

SEPPmail Appliance

Version 12

Benutzerhandbuch mit Ruleset

SEPPmail AG

Industriestrasse 7
CH-5432 Neuenhof

fon +41 56 648 28 38
e-mail info@seppmail.ch

<https://www.seppmail.ch>

SEPPmail - Deutschland GmbH

Ringstraße 1c
DE-85649 Brunnthal

fon +49 8104 8999 030
e-mail info@seppmail.de

<https://www.seppmail.de>

Inhaltsverzeichnis

Part I	Vorwort	18
	1 Haftungsausschluss	19
Part II	Einleitung	20
	1 Dokumentationsvereinbarungen	21
	2 Unterstützung	22
Part III	Die SEPPmail Appliance	23
	1 SEPPmail - Das Unternehmen	23
	1 SEPPmail AG	23
	2 SEPPmail - Deutschland GmbH	24
	2 Vorstellung und Verfahren	25
	1 Produktphilosophie	26
	1 Fünf generische Prinzipien	26
	2 Verschlüsselungstechnologien	28
	1 S/MIME (X.509)	28
	Managed PKI	29
	Güte eines Zertifikates	30
	2 OpenPGP	30
	3 Gateway-to-Gateway (Domänen) Verschlüsselung	31
	Managed Domain Service	31
	4 GINA-Webmail	32
	Standard Prozess	35
	Funktionsablauf	40
	Unterschiedliche Registrierungsarten	41
	Einmal-Passwort / One-Time-Password OTP	42
	E-Mail Passwort / Unique-E-Mail-Password UEP	43
	Authentisierungsanfrage bei Identitätsanbieter (IDP)	44
	E-Mail lesen	46
	Sicheres Antworten	47
	Abmelden	49
	Account-Basierte Funktionen	50
	Self-Service Password Management (SSPM)	53
	(optional) Initiales Schreiben von Nachrichten	56
	(optional) Schlüsselverwaltung	57
	(optional) Selbstlöschung	58
	(optional) Schlüsselsuche	60
	Administration und Management	61
	5 Mobile Computing Support	62
	Interne Nutzer von mobilen Endgeräten	62
	Externe Empfänger von verschlüsselten E-Mails auf mobilen Endgeräten	63
	Kompatibilitätsmatrix für Empfänger von GINA-Web-Mails	64
	6 TLS	65
	3 Verschlüsselungshierarchie	66
	4 LDAP Key-Lookup für S/MIME und OpenPGP	67
	5 Elektronische Signaturen	68

6 Remote-Administration mittels Web-Portal	70
7 SEPPmail Microsoft Outlook Add-In	71
8 Kompatibilität zu anderen Secure E-Mail Systemen	72
9 Kompatibilität zu diversen Regularien	73
1 Regelung zum sicheren Austausch von EDIFACT Übertragungsdateien	73
2 Verordnung zur Schaffung barrierefreier Informationstechnik (BITV 2.0)	75
3 Aufbau und Architektur	76
1 Appliance	76
1 Hardware Modelle	76
2 Virtualisierte Versionen	77
2 Sizing	78
3 Software	79
4 Zentrales Regelwerk (Rule-Engine)	80
5 Architekturen	81
1 Im vollen Mailstrom (empfohlen)	81
Kleine Umgebungen	81
Mit zwischengeschalteter Schutzkomponente	82
Parallel zur Schutzkomponente	83
Routing auf der SEPPmail Appliance	84
2 Ausschließlich kryptographisch behandelte E-Mails	86
3 Schnittstellen	87
6 Hochverfügbarkeit, Loadbalancing	88
1 Multi Master LDAP	88
2 Queue-Less-Betrieb	88
3 Failover und Loadbalancing	89
7 System Management	90
1 Administration	90
2 Rollenrechte	91
3 Backup / Restore	92
4 System Update	93
5 SysLog	94
6 Systemüberwachung	95
7 Report	96
8 Mandantenfähigkeit - Public / Private Cloud Implementierung	98
9 Steuern der Appliance	99
1 Betreffzeilen Schlüsselwörter / x-header	99
2 Microsoft Outlook Vertraulichkeit	100
3 SEPPmail Microsoft Outlook Add-In	100
4 Sicherheit	101
1 Ciphers	103
5 Zusätzliche Features	105
1 Protection Pack (PP)	106
2 Large File Transfer (LFT)	107
1 Einliefern/Versenden via Standard E-Mail Client	109
2 Einliefern/Versenden via GINA-Webmail	110
3 Einliefern/Versenden via SEPPmail Microsoft Outlook Add-In	111
4 Einliefern/Versenden via API	112
5 Einliefern/Versenden durch organisationsfremde (externe) Sender an interne Empfänger	113
3 Internal Mail Encryption (IME)	114

	1 Allgemeines zur Ende zu Ende Verschlüsselung	114
	Umgebung einer „nicht gesicherten“ E-Mail Kommunikation im Unternehmen	114
	Technische Voraussetzungen einer Ende zu Ende Verschlüsselung	115
1	Bedarfsanalyse	116
	Ende zu Ende Kommunikation nach außen	117
	2 SEPPmail IME unter ausschließlicher Verwendung der GINA-Technologie	118
	3 SEPPmail IME 1.0	119
	Ablauf	120
	4 SEPPmail IME 2.0	121
	Voraussetzungen	121
	Rollout / Deployment	122
	Ablauf	123
	Ergebnis / Vorteile	124
	4 Central Disclaimer Management (CDM)	125
	6 Lizenzen	126
	1 Basissysteme und Lizenz	126
	1 Protection Pack	126
	2 Signatur und Verschlüsselung	127
	3 Large File Transfer (LFT)	128
	4 Internal Mail Encryption (IME)	129
	5 Central Disclaimer Management (CDM)	130
Part IV	Inbetriebnahme der Secure E-Mail Gateway Appliance	131
	1 Bevor Sie beginnen	131
	2 Integration der SEPPmail Appliance in die vorhandene E-Mail Umgebung (Standard Konfiguration)	132
	3 Benötigte Informationen zur Inbetriebnahme	133
	4 Firewall / Router einrichten	135
	5 Basiskonfiguration in wenigen Schritten	139
	1 Netzwerkeinstellungen und Systemregistrierung	139
	1 Initialer Verbindungsaufbau	139
	Virtuelle Appliance	139
	Hardware Appliance	140
	Consolen Login	141
	2 Login als Administrator	143
	3 Netzwerkeinstellungen der SEPPmail Appliance	144
	4 Netzwerkkonfiguration prüfen	145
	5 Das System registrieren	146
	2 Das System auf den neusten Stand bringen	147
	3 Wichtige Sicherheitsmaßnahmen	148
	1 Administrator Kennwort ändern	148
	2 Festlegen des HTTPS Protokolls für den sicheren Zugriff zum System	149
	3 Backup Benutzer erstellen	150
	4 Eingabe der Postmaster Adresse für den Empfang von Systemmeldungen	151
	5 Ruleset generieren	152
	6 Vorbereiten der GINA-Technologie	153
	7 Integration in die bestehende E-Mail Infrastruktur	154

	1 Zu verwaltende E-Mail Domänen einrichten	154
	2 Ausgehenden E-Mail Verkehr steuern	155
	3 Mail Relaying	156
	4 SSL Zertifikat einbinden	157
	1 SSL Zertifikat selbst erstellen	157
	2 Bestehendes SSL Zertifikat einbinden	159
	3 SSL Zertifikat von einer öffentlichen Zertifizierungsstelle anfordern	161
	5 E-Mail Datenfluss umstellen	163
	6 Steuern der Appliance	164
	1 Betreffzeilen Schlüsselwörter / (X-)Header	164
	2 Microsoft Outlook Vertraulichkeit	166
	3 SEPPmail Microsoft Outlook Add-In	167
	8 Clustern mehrerer Systeme	168
	1 Allgemein	168
	2 Hochverfügbarkeits-Cluster	171
	3 Loadbalancing Cluster	173
	1 Aufteilen des Ein- und Ausgehenden Verkehrs	173
	2 Nutzen des DNS Round Robin Verfahrens	175
	3 Nutzen eines externen Loadbalancers	177
	4 Geo-Cluster	179
	5 Frontend/Backend Cluster	180
	6 GINA Satellit	181
	7 Unterstützen externer redundanter Systeme	183
	9 Einrichten zusätzlicher Features	184
	1 Protection Pack (PP)	184
	2 Self Service Password Management (SSPM)	185
	3 Large File Transfer (LFT)	186
	4 Internal Mail Encryption (IME)	187
	5 Central Disclaimer Management (CDM)	188
Part V	Administrative Aufgaben	189
	1 Rudimentäre Systembefehle	189
Part VI	SEPPmail Microsoft Outlook Add-In	190
	1 X-Plattform-Add-In für Microsoft 365	190
	1 Einleitung	190
	2 Bezug	192
	3 Systemanforderungen	194
	2 COM Add-In für MS Exchange / Outlook on premises	195
	1 Einleitung	195
	2 Download	196
	3 Systemanforderungen	197
	4 Installation	198
	1 Interaktive Installation	198
	2 Silent Installation	200
	3 Deinstallation	202
	5 Registry	203

	6 Schaltflächen für den Versand von E-Mails	208
	7 Large File Transfer	209
	8 Interne Verschlüsselung	210
	9 Berechtigungssteuerung per LDAP	212
	10 AddIn Verwaltung	212
	11 Versionsverlauf	212
Part VII	Referenz der Menüpunkte	216
	1 Allgemein	216
	2 Übersicht der Menüpunkte	217
	3 Login / Logout	219
	4 Home	220
	5 System	224
	6 Mail System	247
	1 List Disclaimer	259
	1 Edit Disclaimer	261
	2 List Template	263
	1 Edit Template	264
	3 Add / Edit Managed Domain	266
	1 Import OpenPGP Key(s)	280
	2 Import PKCS#12 certificate structure(s)	280
	4 Extended Postfix MTA Settings	281
	5 Add TLS Domain	282
	7 Mail Processing	286
	1 Encryption Policy	313
	1 Add/Edit Encryption Policy	314
	8 SSL	319
	1 Request Or Create New Certificate (Authority)	322
	1 Certificate Signing Request (CSR)	324
	2 Import An Existing Certificate (Authority)	326
	9 CA	328
	1 Sign Certificate Request	338
	10 MPKI	339
	1 Deutsches Forschungsnetz	341
	2 Digicert	344
	3 Bundesdruckerei D-Trust	346
	4 GlobalSign	349
	5 GlobalTrust	352
	6 QuoVadis Trustlink	355
	7 Simple Certificate Enrollment Protocol	358
	8 Sectigo	360
	9 SwissSign	364
	11 Administration	369
	1 Register This Device	376

2 Restore	379
3 Bulk Import OpenPGP Keys	379
4 Bulk Import PKCS#12 Certificate Structure	380
12 Cluster	383
13 Logs	388
1 Mails Currently In Queue	391
2 Other Logs	392
14 Statistics	394
15 Users	396
1 User 'user@domain.tld'	398
1 X.509 Certificate 'details'	404
2 OpenPGP Key 'details'	408
2 Create User Account	410
3 Change Password Policy	411
4 Advanced Settings	411
16 Groups	413
17 GINA Domains	416
1 Create New GINA Domain	422
2 Change GINA Settings For	423
1 Layout	453
2 Edit Translations For Language	459
18 GINA Accounts	462
1 Account Details	464
19 LFT Accounts	466
20 OpenPGP Public Keys	467
1 Import OpenPGP Key(s)	468
2 OpenPGP Key 'details'	469
21 X.509 Certificates	471
1 Import X.509 Certificate(s)	473
2 X.509 Certificate 'details'	474
3 Advanced Settings	478
22 X.509 Root Certificates	480
1 Import X.509 Root Certificate(s)	483
2 Advanced Settings	485
3 Certificate Details	486
23 Domain Certificates	489
1 S/MIME domain certificates	490
2 OpenPGP domain keys	492
24 Customers	494
1 Create New / Edit Settings For Customer	496
1 Manage Assigned GINA Accounts	500
2 Delete Customer	501

1 Allgemeine Informationen	504
1 Syntax	505
2 Variablen	506
3 Kontrollstrukturen - if/else Anweisungen	507
4 Makros	509
5 Reguläre Ausdrücke	511
6 X-Header	514
2 Allgemeine Befehle	516
1 incoming()	516
2 internal()	516
3 external()	517
4 getheader()	518
5 notify()	520
6 setvar()	522
3 Vergleichende Befehle	523
1 check_sender()	523
2 compare()	525
3 compareattr()	527
4 comparebody()	529
5 empty()	530
6 from_managed_domain()	531
7 member_of()	532
8 rmatch()	532
9 rmatchsplit()	533
4 Logging	534
1 log()	534
2 logheader()	535
3 logsubject()	536
5 Verwalten von Benutzern	537
1 authenticated()	537
2 createaccount()	539
3 createkeys()	540
4 member_of()	541
5 setuserattr()	542
6 Handhaben von Nachrichten	544
1 archive()	544
2 autoreply()	545
3 bounce()	548
4 deliver()	549
5 disclaimer()	550
6 drop()	552
7 flag()	553
8 reject()	554
9 reprocess()	554

10 Manipulieren von Envelope und Header	556
1 add_rcpt()	556
2 normalize_header()	557
3 replace_rcpt()	558
4 replace_sender()	560
5 rmheader()	562
6 setheader()	563
7 splitrecipients()	565
8 tag_subject()	566
9 tagsubject()	566
11 Kryptographische Behandlung	567
1 OpenPGP	567
attachpgpkey()	567
pgp_encrypted()	568
Domänen basiert	569
decrypt_domain_pgp()	569
domain_pgp_keys_avail()	570
encrypt_domain_pgp_inline()	571
encrypt_domain_pgp_mime()	572
Benutzer basiert	573
decrypt_pgp()	573
pgp_keys_avail()	574
pgp_secret_keys_avail()	575
encrypt_pgp()	576
encrypt_pgp_inline()	576
encrypt_pgp_mime()	577
pgp_signed()	578
validate_pgp_sig()	579
delete_pgp_sig()	580
sign_pgp_mime()	581
2 S/MIME	582
smime_encrypted()	582
Domänen basiert	583
decrypt_domain_smime()	583
domain_smime_keys_avail()	584
encrypt_domain_smime()	585
Benutzer basiert	586
decrypt_smime()	586
smime_keys_avail()	587
encrypt_smime()	588
smime_signed()	589
validate_smime_sig()	590
delete_smime_sig()	591
has_smime_key()	592
sign_smime()	593
3 GINA	595
encrypt_webmail()	595
change_webmail_sender()	597
pack_mail()	598
unpack_mail()	599
webmail_keys_avail()	600
webmail_keys_gen()	601
4 TLS	602
force_tls_domain()	603
12 Content Management	604

	1 iscalendar()	604
	2 issпам()	605
	3 partoftype()	606
1	Liste von MIME Typen	607
	Liste der Dateitypen (veraltet)	611
	Liste von Dateigruppen (veraltet)	613
	4 vscan()	614
	5 whitelist_recipients()	615
	7 Zugriff auf externe LDAP-Verzeichnisse	616
	1 ldap_init()	616
	2 ldap_read()	617
	3 ldap_compare()	620
	4 ldap_getcerts()	625
	5 ldap_getpgpkeys()	627
	8 Vordefinierte Platzhalter	629
	1 Allgemein	629
	1 @CUSTOMDELIVER@	629
	2 Benutzerverwaltung	630
	1 @CREATEPGPKEYS@	630
	3 Signatur	631
	1 @NOSIGNTEXT@	631
	2 @TAGSIGNED@	631
	3 @TAGSIGNEDINVALID@	632
	4 @REMOVETAGDECRYPTED@	633
	5 @REMOVETAGS@	633
	6 @REMOVETAGSIGNED@	633
	7 @REMOVETAGSIGNEDINVALID@	634
	4 Verschlüsselung	635
	1 @TRIGGERTEXT@	635
	2 @NOENCTEXT@	635
	3 @KEYSERVER@	635
	4 @TAGDECRYPTED@	635
	5 @REMOVETAGDECRYPTED@	636
	5 LFT	637
	1 @LARGEFILETEXT@	637
	2 @NOLARGEFILETEXT@	637
	3 @REMOVELFMTAGS@	637
	6 Header Tagging	638
	1 @TAGHEADERENCRYPTED@	638
	2 @TAGHEADERDECRYPTED@	638
	9 Vordefinierte Makros	638
	1 Allgemein	639
	1 \$archive	639
	2 Verwalten von Benutzern	640
	1 \$createanyuser	640
	2 \$createcustomuser	640
	3 \$createwebuser	641
	3 Tagging	642
	1 \$removelfmtags	642
	4 Verschlüsselung	642
	1 \$keyserver	642

Part IX	HowTo / FAQ	643
1	Admin: Admins sollen keine „Daily Reports“ erhalten	644
2	Admin: Anmelden nach Passwort-Wechsel mit Sonderzeichen nicht möglich	645
3	Admin: API Funktionen	646
4	Admin: API Test mit „Postman“	647
5	Admin: Erkennen kryptographisch behandelter E-Mails	653
6	Admin: „Factory reset“ funktioniert nicht	654
7	Admin: Gruppenzuordnung im Menü „Users“	655
8	Admin: Klonen von SEPPmail Appliances	656
9	Admin: Mehrere SMTP-Authentifizierungen verwalten	657
10	Admin: Menü „Administration“ öffnet nicht	659
11	Admin: Unerwartetes Verhalten bei E-Mails mit vielen Empfängern	660
12	Admin: Wiederholte Logouts aus der Administrationsoberfläche	661
13	Admin: Vertrauen für gesammelte Root Zertifikate herstellen	662
14	Allgemein: Anzeige der für den Empfänger verfügbaren Verschlüsselungsverfahren	663
15	Allgemein: E-Mails werden mit „452.3.1 Insuffizient System Storage abgewiesen“	664
16	Allgemein: Automatisches Einsammeln von OpenPGP Public Keys	664
17	Allgemein: E-Mails als Anhang einer leeren Träger-E-Mail	665
18	Allgemein: E-Mails werden mangels TLS vom annehmenden Server abgewiesen	666
19	Allgemein: E-Mails über ablaufende Zertifikate	667
20	Allgemein: Entfernen von (X-)Header oder den darin enthaltenen Informationen	669
21	Allgemein: Kalenderanfragen kommen als HTML-Datei mit PGP im Dateinamen an	669
22	Allgemein: Kalenderanfragen kommen zerstört beim Empfänger an	670
23	Allgemein: Kennzahlen der SEPPmail Appliance	671
24	Allgemein: Langsames Verarbeiten von E-Mails	672

25 Allgemein: Mehrere Aktionen mit einem Schlüsselwort triggern	673
26 Allgemein: Mehrere Schlüsselwörter als Trigger für eine Aktion	674
27 Allgemein: Permanentes Synchronisieren mit Zeitserver (NTP)	675
28 Allgemein: Rückmelden der ausgeführten kryptographischen Aktionen	676
29 Allgemein: SEPPmail Appliance NDRs werden nicht zugestellt	677
30 Allgemein: Text Codierung (ungleich UTF-8)	678
31 AntiSpam: Dienst startet nicht	679
32 AntiSpam: Funktionen / Engine	680
33 AntiVirus: Funktionen / Engine	681
34 AntiVirus: Wo erfolgt der Scan	682
35 Backup: Kopieren von SEPPmail Appliance Backups	683
36 Backup: Quiescing	684
37 Backup: Volume Shadow Copy for Linux	685
38 Benutzer: Anlage / Zertifikatsbezug auf Basis des Envelope- oder Sender-Eintrags	685
39 Benutzer: Anlage mittels LDAP Abfrage	687
40 Benutzer: Berechtigung mittels LDAP Abfrage	689
41 Benutzer: Einschränken des LFT berechtigten Personenkreises	692
42 CDM: Personalisierte Grußformel automatisiert erstellen	694
43 Cluster: Doppel-Bezug von Zertifikaten verhindern	700
44 Cluster: Failover (CARP) funktioniert nicht	701
45 Cluster: GINA-Satellite Konfiguration	702
1 Variante 1	703
2 Variante 2	704
3 Variante 2a	709
46 Cluster: Priorität bei der Replikation	714
47 Cluster: Replikation arbeitet nicht wie erwartet	715
48 Cluster: Replikations-Intervalle	716
49 Cluster: Replizierte Daten	717
50 Cluster: Sendende IP Adresse im Cluster	718
51 Cluster: Update Reihenfolge der Cluster Maschinen	719

52 Cluster: Verfügbarkeit der GINA-Interfaces prüfen	720
53 Cluster: Virtuelle IP-Adressen (CARP) funktionieren nicht.	721
54 DATEV: Austausch von Domänenschlüsseln mit DATEV-Kunden	722
55 E-Mail Fluss: „ERROR: Missing mandatory headers Date and From“	723
56 E-Mail Fluss: Verarbeiten von E-Mails an Sub-Domänen	724
57 ESX: Netzwerkadapter wird nicht erkannt	725
58 ESX: Abstürzte / Einfrieren der Maschine	725
59 GINA: 403 Forbidden / Server Name Indication (SNI)	726
60 GINA: Anmelden interner Benutzer	727
61 GINA: Apple E-Mail App zeigt GINA-Mail unverschlüsselt an	728
62 GINA: Einrichten eines Bewerberportals	729
63 GINA: Lesebestätigung auch bei Schlüsselwort	730
64 GINA: Öffnen des HTML-Anhangs einer GINA-Nachricht in iOS schlägt fehl	731
65 GINA: Paralleles Verwenden von „Account login“ und „Unique e-mail password“	732
66 GINA: Session / Verbindungs-Abbrüche	733
67 GINA: Session Timeouts	734
68 GINA: SMS-Anbieter	735
69 GINA: „Kopie an mich selbst“: Vertauschter Absender/Empfänger	737
70 Hyper-V: Hardware Einstellungen	738
71 IBM Notes: Schaltfläche für verschlüsseltes Senden erzeugen	739
72 IME: Interne E-Mails verschlüsseln	740
1 IME 1.0	740
2 IME 2.0	741
1 Vorbereitung	741
Infrastruktur	741
GAL Eintrag erstellen	742
SEPPmail Appliance	743
Windows- / Outlook-Client	744
2 Eingehende E-Mails umverschlüsseln	745
73 IME: Verzögerter Start von MS Outlook	746
74 IronPort: Anbinden der SEPPmail Appliance	747
75 Konfig: Anbinden von LDAP Datenbeständen	750

76	Konfig: Angabe von mehreren E-Mail Servern	751
77	Konfig: Bounce von E-Mails nicht authentifizierter Benutzer	752
78	Konfig: Custom commands for outgoing e-mails AFTER encryption	753
79	Konfig: Queueless Mode	754
80	Konfig: Migrieren von „on premises“ zu einem MSP Mandanten	755
81	Konfig: Re-Inject mails to sending mailserver	757
82	LFT: Schwellwerte Ungenauigkeiten	758
83	LFT: Datenablage im Cluster	759
84	LFT: Download von LFT-Nachrichten in einem E-Mail Format	760
85	LFT: Größenbeschränkungen für LFT-Nachrichten	761
86	LFT: Mindestgröße für eine LFT-Disk/Partition	762
87	LFT: Unerwarteter LFT-Versand	763
88	LFT: Verhalten bei Ablauf der LFT-Nachricht	764
89	LFT: Versand einer „normalen“ E-Mail anstatt einer LFT-Nachricht	765
90	LFT: Versand mit Passwort trotz Einstellung „Plain“	766
91	Lizenz: Lizenzdaten aktualisieren (adhoc / Turnus)	767
92	Logs: Mehrere Einträge zu einer E-Mail	768
93	Mandanten: Signieren von E-Mails zwischen Mandanten	769
	1 Variante 1	770
	2 Variante 2	771
	3 Variante 3	773
	4 Variante 4	775
94	Mandanten: GINA zwischen Mandanten erzwingen	777
95	Mandanten: Absichern der Verbindung zwischen SEPPmail Appliance und E-Mail Server	779
96	Mandanten: Umstellen auf Mandantenfähigkeit	780
97	Mandanten: Verschlüsseln von E-Mails zwischen Mandanten	781
98	Monitoring: Partitionen zum Teil bis zu 100% ausgelastet	782
99	MS Azure: Installation	783
100	MS Azure: Migrieren von on premises	784
101	MS Azure: Sizing	785

102	MS Azure: Temporär hohe Auslastung der Datenbank Partition	786
103	MS Exchange: Verify recipient addresses using SMTP-Lookups	787
104	MS Office365: Anbinden von Exchange Online mit ATP / EOP	789
	1 Faktoren für eine reibungslose Integration	790
	2 Technischer Überblick	791
	3 Konfigurationsschema	792
	1 Eingehender E-Mail Fluss	792
	2 Ausgehender E-Mail Fluss	793
	3 Interner E-Mail Fluss	794
	4 Vorbereitung	795
	1 Allgemein	795
	2 Zertifikate	796
	5 SEPPmail Appliance Konfiguration	797
	1 Mail System	797
	Managed domains	799
	2 Mail Processing	801
	6 Exchange Online Konfiguration	802
105	MS Office365: Folgende Nachricht konnte nicht gesendet werden	803
106	MS Office365: Fehler ATTR35 bei der Übergabe an Exchange Online	804
107	MS Office365: Verteilerlisten Alias-Adressen und Weiterleitungen	805
108	MS Outlook: Der Name Ihrer digitalen ID kann im zugrunde liegenden Sicherheitssystem nicht gefunden werden.	807
109	SEPPmail Microsoft Outlook Cross-Platform-Add-In: Ablageort der LOG-Dateien	808
110	SEPPmail Microsoft Outlook Cross-Platform-Add-In: Wiederholtes Deaktivieren durch Outlook	809
111	MPKI: Beauftragen/Anbinden SwissSign	809
112	MPKI: Bezogene Zertifikate für weitere Zwecke einsetzen	812
113	MPKI: Bezug von Zertifikaten funktioniert nicht mehr	813
114	MPKI: DigiCert versendet Validierungs-E-Mails	814
115	MPKI: Umstellen des Zertifikatsanbieters (CA)	815
116	Schnittstellen: legacy.app	816
117	Sicherheit: Path traversal attack	817
118	Sicherheit: RC4 Attacken möglich / alte TLS Version	818

119	Sicherheit: TLS 1.0 abschalten	819
120	Sicherheit: TLS Zertifikat kann nicht validiert werden	820
121	Sicherheit: Zertifikat für TLS gesicherte SMTP-Anfragen	821
122	Signatur: Auswirkung von Änderungen im Header von E-Mails auf eine Signatur	822
123	Signatur: Log-Meldung „Warning: Could not find certificate chain. Add certificates to x.509 root certificates“ beim Signieren	823
124	Signatur: Signieren aller ausgehenden E-Mail mit einem einzigen Domänenzertifikat	824
125	Signatur: Unterschiedliche Prüfergebnisse	825
126	Signatur: Verwendeter Schlüssel bei Microsoft Vertreterregelung	827
127	Signatur: Zum Signieren verwendetes Zertifikat	828
128	Signatur: Gründe einer ungültigen Signatur	829
	1 Barracuda	830
129	Sophos UTM: Erneute Virenprüfung nach dem Entschlüsseln	831
	1 Vorbereitung auf Sophos UTM	831
	2 Erforderliche Aktionen auf der SEPPmail Appliance	832
130	Verschlüsselung: Globales Unterdrücken oder Forcieren kryptographischer Aktionen	834
131	Verschlüsselung: Domänenverschlüsselung mit einem Dritthersteller-System	835
132	Verschlüsselung: Domänenverschlüsselung zu einer anderen SEPPmail Appliance	836
133	Verschlüsselung: Domänenzertifikat mit Aussteller (Issuer)	837
134	Verschlüsselung: E-Mails von Google nicht lesbar	838
135	Verschlüsselung: Lokal abliegende E-Mails erneut entschlüsseln	839
136	Verschlüsselung: Outlook Confidential Flag trotz gegenteiliger Einstellung gesetzt	840
137	Verschlüsselung: TLS als gültige Verschlüsselungsvariante	841
138	Verschlüsselung: Verwenden abgelaufener OpenPGP-Schlüssel	842
139	Verschlüsselung: Verwendetes Zertifikat	843
140	Zertifikate: SwissSign: Einlösen von Vouchers	844

141	Zertifikate: Unterstützen von SAN Zertifikaten	847
142	Aktuelle Sicherheitslücken / Exploits	848
1	Amnesia 33	849
2	Vulnerability in LibreSSLv3.2.2 (CVE-2020-1971)	850
3	GLIBC	850
4	Heartbleed	850
5	Poodle	850
143	Regularien	851
1	EDIFACT	851
1	Zu implementierende Prüfungen	851
2	Erforderliche Maßnahmen auf der SEPPmail Appliance	851
	Erstellen einer E-Mail Vorlage	851
	Im HTML-Format	852
	Im Text-Format	854
	Erstellen von Custom Commands	855
	Custom macros and commands for all e-mails BEFORE processing	855
	Custom commands for incoming e-mails BEFORE decryption	860
	Custom commands for outgoing e-mails BEFORE encryption	861
Part X	Versionsverlauf (englisch)	863

1 Vorwort

Die SEPPmail AG behält sich vor, am Inhalt dieses Dokuments jederzeit und unangekündigt, Änderungen vorzunehmen. Sofern nicht anders vermerkt, sind Namen und Daten von Personen oder Unternehmen, die in diesem Dokument als Anwendungsbeispiele verwendet werden, frei erfunden. Das Herstellen einer angemessenen Zahl von Kopien dieses Dokuments ist gestattet, jedoch nur für den internen Gebrauch. Zu anderen Zwecken darf dieses Dokument weder kopiert noch reproduziert werden; weder teilweise noch vollständig, nicht elektronisch, mechanisch oder auf irgendeine andere Weise, außer mit ausdrücklicher, schriftlicher Genehmigung der SEPPmail AG.

Der Inhalt dieses Dokuments kann möglicherweise verändert worden sein, falls dieses nicht direkt von SEPPmail AG bezogen wurde. Auch wenn dieses Dokument mit der größten Sorgfalt angefertigt wurde, übernimmt die SEPPmail AG keine Verantwortung für etwaige Fehler oder Unvollständigkeiten. Das Benutzen dieses Dokuments beinhaltet die Zustimmung zu dessen Gebrauch ohne Mangelgewähr und ohne jegliche Garantien. Jeglicher Gebrauch der hier aufgeführten Informationen erfolgt auf eigenes Risiko.

Gemäß aktueller deutscher Rechtschreibung wird im Dokument das „generische Maskulinum“ verwendet, um etwaige geschlechtsspezifische Diskriminierungen auszuschließen.

PGP und Pretty Good Privacy sind gesetzlich geschützte Warenzeichen der PGP Corporation, gültig in den USA und anderen Ländern. Java und alle Java-basierten Marken sind Warenzeichen Oracle Corporation, gültig in den USA und anderen Ländern. UNIX ist ein eingetragenes Warenzeichen unter der Verfügung der X/Open Company, gültig in den USA und anderen Ländern. Microsoft, Internet Explorer, Windows, Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8 und Windows 10 sind entweder eingetragene Warenzeichen oder gesetzlich geschützte Warenzeichen der Microsoft Corporation, gültig in den USA und anderen Ländern. Netscape und Netscape Navigator sind gesetzlich geschützte Warenzeichen der Netscape Communications Corporation, gültig in den USA und anderen Ländern. Google Chrome ist ein gesetzlich geschütztes Warenzeichen der Google Inc., gültig in den USA und anderen Ländern. Alle etwaigen anderen hier aufgeführten Warenzeichen sind Eigentum ihrer jeweiligen Besitzer und werden hier ohne die Absicht der Markenverletzung verwendet.

OpenBSD ist ein Betriebssystem, das unter dem Berkeley Copyright vertrieben wird (www.openbsd.org).

Postfix ist ein open source E-Mail Server (www.postfix.org).

OpenSSL ist eine Anwendung, die unter einer Apache ähnlichen Lizenz vertrieben wird (www.openssl.org). LibreSSL ist eine vom OpenBSD-Team von nicht benötigten Bestandteilen befreite Abspaltung von OpenSSL und wird unter der OpenBSD Lizenz vertrieben (www.libressl.org).

Apache Webserver und Apache Tomcat werden unter dem Apache Software Foundation Copyright entwickelt (www.apache.org).

OpenLDAP ist eine Implementierung des LDAP, die als freie Software unter der, BSD-Lizenz ähnlichen, OpenLDAP Public License veröffentlicht wird (www.openldap.org).

GnuPG ist Software, die unter der GNU Public License vertrieben wird (www.gnupg.org).

SpamAssassin ist ein Filterprogramm, mit dem unerwünschte E-Mails (Spam) automatisch aussortiert werden können und ist als freie Software unter den Bedingungen der Version 2 der Apache-Lizenz freigegeben (www.spamassassin.org).

ClamAV ist ein unter der GPL stehendes von der Sourcefire Inc. (www.sourcefire.com) entwickeltes Virenschutzprogramm (www.clamav.net).

Hinweise auf kommerzielle Produkte, Verfahren oder Dienstleistungen, durch Nennung des Produkt- oder Herstellernamens oder auf beliebige andere Weise, kommen nicht notwendigerweise einer Billigung, Empfehlung oder Favorisierung durch die SEPPmail AG gleich.

Einfuhr, Ausfuhr und Benutzung dieser und anderer Verschlüsselungsprodukte sind möglicherweise gesetzlich eingeschränkt.

In diesem Dokument vom Verfasser geäußerte Ansichten und Meinungen drücken nicht notwendigerweise jene der SEPPmail AG aus und dürfen nicht zum Zweck der Werbung oder der Produktempfehlung benutzt werden. Verweise auf Internetadressen sind vor der Drucklegung gründlich geprüft worden. Aufgrund des ständigen Wandels der

Internetinhalte kann die SEPPmail AG aber keine Garantie für das Vorhandensein und den Inhalt der angegebenen Quellen übernehmen. Sollten Sie in dieser Anleitung fehlerhafte Links finden, teilen Sie uns diese bitte unter Angabe des betroffenen Links und der Versionsnummer dieser Anleitung an die Adresse info@seppmail.de mit.

Druck: September 2021, CH-5432 Neuenhof

1.1 Haftungsausschluss

Vertragspartner für den Endkunden ist sein Vertriebspartner, beziehungsweise Systemhaus. Als SEPPmail Vertragspartner stehen diesem jeweils die Endbenutzer-Lizenzvereinbarung <https://downloads.seppmail.com/wp-content/uploads/docu/SEPPmail-EULA.pdf> (siehe insbesondere §9 und §10) und der Dienstleistungsvertrag Wartung und Support <https://downloads.seppmail.com/wp-content/uploads/docu/Maintenance-and-Support.pdf> (insbesondere Punkte 2.5, 2.6, 3.3 und 4.4) zur Verfügung.

Allgemein weisen wir darauf hin, dass Fehlkonfigurationen zur Nicht-Lesbarkeit von E-Mails und zu Einschränkungen des E-Mail-Verkehrs bis hin zum Erliegen desselben führen können.

2 Einleitung

Willkommen zur Secure E-Mail Lösung von SEPPmail

Das vorliegende Handbuch soll vollumfänglich über das Produkt SEPPmail Appliance sowie die darin verwendeten Komponenten informieren.

Damit der für die jeweilige Lesergruppe relevante Teil leichter zu finden ist, wurde es in folgende Teilbereiche gegliedert:

Teil I  18

Teil II

Teil III  23

Teil IV  131

Teil V  189

Teil VI  190

Teil VII  216

Teil VIII  504

Teil IX  643

Teil X  863

2.1 Dokumentationsvereinbarungen

Um die Dokumentation übersichtlicher zu gestalten, werden unterschiedliche Schreibweisen und Symbole verwendet. Eine Übersicht der verwendeten Symbole und Schreibweisen für zum Beispiel Programmiercode, Menüpunkte oder Schaltflächen ist in der folgenden Tabelle dargestellt:

	Hinweis auf mögliche Fehlerquellen oder Abschnitte in denen besondere Sorgfalt bei der Konfiguration notwendig ist.
	Wichtiger Hinweis
Kapitelverweis	Verweis auf ein Kapitel in dieser Dokumentation
Menü	Menüpunkt
Untermenü	Untermenü
Sektion	Sektion
Abschnitt	Abschnitt
Teilabschnitt	Teilabschnitt
'Option'	Option
Eingabe	Spezielle Eingabefelder, Eingabewerte
Schaltfläche	Schaltfläche
Tabellenüberschrift	Tabellenüberschrift
AdminGUI Link	Link in einer Tabelle auf ein Untermenü
Positivmeldung	Positive Rückmeldung des Systems
Informationsmeldung	Informative Rückmeldung des Systems
Fehlermeldung	Negative Rückmeldung des Systems
<code>command() ;</code>	Programmiercode
<code>@function@</code>	Programmierfunktion
<i>(neu in X.X.X)</i> <i>(entfällt in X.X.X)</i> <i>(geändert in X.X.X)</i> <i>(verschoben in X.X.X)</i>	Neuerungen und Änderungen seit der letzten Vollversion werden jeweils mit dem Hinweis gekennzeichnet. Somit kann im Dokument jeweils nach den entsprechenden Stellen gesucht werden. Die komplette Revision History ist in diesem Handbuch (siehe Versionsverlauf ⁸⁶³), beziehungsweise auf der Administrationsoberfläche der SEPPmail Appliance selbst (siehe auch View release notes ³⁶⁹) einzusehen.

Da insbesondere in den technisch relevanten Teilen (ab Teil IV) sehr viel mit Verweisen gearbeitet wird, empfiehlt sich für Administratoren das Handbuch in elektronischer Form zu verwenden.

2.2 Unterstützung

Die Unterstützung für Endkunden und Partner orientiert sich am Vertriebsmodell der SEPPmail. So steht dem Endkunden in erster Instanz sein Systemhaus beziehungsweise Systemintegrator zur Verfügung. Ein zertifizierter SEPPmail Partner verfügt über wenigstens einen SEPPmail Certified System Engineer und ist somit kompetenter Ansprechpartner, sowohl für infrastrukturelle, wie auch projektspezifische Fragen und Probleme.

Bei tiefergehenden Fragen steht dem Partner wiederum sein Distributor als Ansprechpartner zur Verfügung. Der Distributor verfügt über Mitarbeiter, welche umfangreiche Erfahrung mit dem Thema Sichere E-Mail im Allgemeinen sowie SEPPmail im Speziellen haben. Sollten seitens des Distributors Fragen offen bleiben, besteht für ihn die Möglichkeit den SEPPmail Support einzubinden beziehungsweise den direkten Kontakt zum Partner oder Kunden herzustellen, falls notwendig.

Ebenso werden über diesen Kanal neue Anforderungen an das Produkt entgegengenommen.

Als erste Hilfestellung dient das Kapitel [HowTo / FAQ](#) ⁶⁴³ in diesem Handbuch.

3 Die SEPPmail Appliance

3.1 SEPPmail - Das Unternehmen

3.1.1 SEPPmail AG

Das in der Schweiz ansässige, international tätige und inhabergeführte Unternehmen SEPPmail ist Hersteller im Bereich „Secure Messaging“. Dessen patentierte, mehrfach prämierte Technologie für den spontanen sicheren E-Mail Verkehr (GINA) verschlüsselt elektronische Nachrichten und versieht diese auf Wunsch mit einer digitalen Signatur. Die Secure E-Mail Lösungen sind weltweit erhältlich und leisten einen nachhaltigen Beitrag zur sicheren Kommunikation mittels elektronischer Post. Dadurch maximiert SEPPmail die Kommunikationssicherheit von hunderten von Benutzern. Das Unternehmen wurde 2001 gegründet und verfügt demnach über langjährige Erfahrungen im sicheren Versenden digitaler Nachrichten.

Die Produktphilosophie gründet sich auf vier Hauptmerkmale:

- ein Höchstmaß an Sicherheit
- hohen Benutzerkomfort
- hohe Stabilität
- geringer Administrationsaufwand.

SEPPmail AG hat mit seinem CEO, Herrn Stefan Klein, den „Erfinder“ dieser Lösung on board, der seit 2001 die Entwicklung dieses Produktes forciert und begleitet. Dabei stellt er sicher, dass die Produktphilosophie über all die Jahre beibehalten wird. So reifte das Produkt mit den Kundenanforderungen, wobei die individuellen Anforderungen immer dem Gesamtprodukt beigelegt und somit allen Kunden zugänglich gemacht werden.

SEPPmail AG
Industriestrasse 7
CH-5432 Neuenhof

<https://www.seppmail.ch>

3.1.2 SEPPmail - Deutschland GmbH

Das deutsche Unternehmen SEPPmail - Deutschland GmbH wurde im August 2015 gegründet um Vertrieb, Marketing und den Kundensupport über die Grenzen der Schweiz hinaus nachhaltig innerhalb Europas zu festigen und weiter auszubauen.

Mit Gründen der SEPPmail - Deutschland GmbH wurde neben dem Entwicklungsstandort Schweiz auch in Leipzig ein neues Entwicklungszentrum aufgebaut.

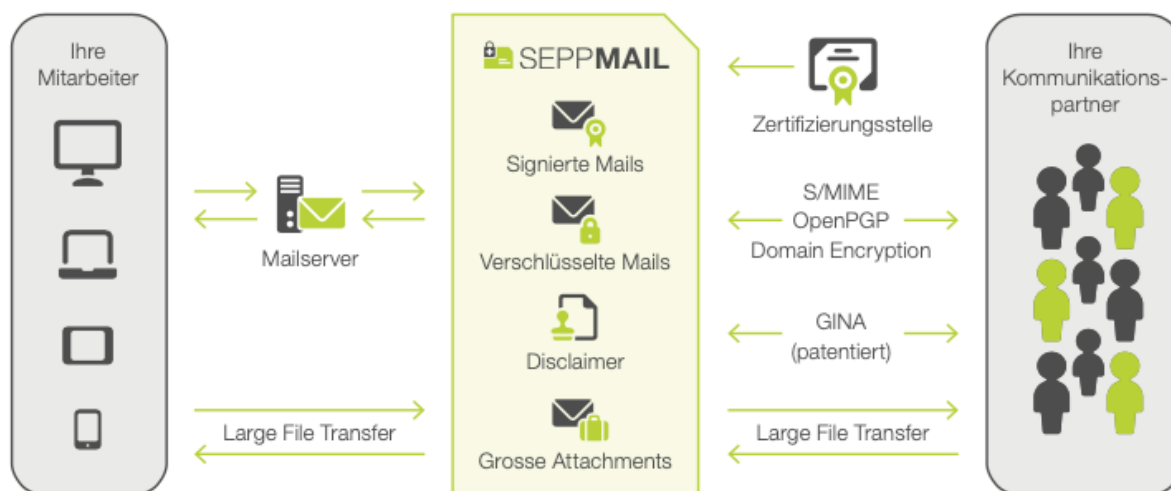
Der Vertrieb ist zweistufig über Distribution und einem gut ausgebildeten Partnernetzwerk etabliert.

Günter Esch ist seit 1. Oktober 2011 als Country Manager für Deutschland und Österreich bei SEPPmail tätig. Seit August 2015 zeichnet er als Geschäftsführer verantwortlich für die SEPPmail - Deutschland GmbH sowie das Betreuen bestehender und neuer Kunden, das Bearbeiten strategischer Märkte und dem gezielten Ausbau des Channels. Der diplomierte Maschinenbau-Ingenieur ist seit über 25 Jahren in der internationalen IT- und IT-Security-Branche aktiv.

SEPPmail - Deutschland GmbH
Ringstraße 1c
DE-85649 Brunnthal

<https://www.seppmail.de>

3.2 Vorstellung und Verfahren



Das SEPPmail Secure E-Mail Gateway ist eine konsequente All-in-One-Lösung für den wirtschaftlichen und effizienten Einsatz für

- das zentrale Verwalten von Zertifikaten und E-Mail-Signaturen (SIG);
- das Ver- und Entschlüsseln von E-Mails (ENC);
- den einfachen und sicheren Versand großer Dateien (LFT);
- ein zentrales E-Mail-Disclaimer-, beziehungsweise Fußnoten-Management des gesamten Unternehmens (CDM).

3.2.1 Produktphilosophie

Die Produktphilosophie gründet sich auf zwei Hauptmerkmale: ein Höchstmaß an Sicherheit in Kombination mit hohem Benutzerkomfort. Zu Letzterem zählen insbesondere ein stabiler Betrieb und möglichst geringe Administrationsaufwände.

Die SEPPmail Appliance unterstützt alle am Markt befindlichen Standard-Technologien (siehe [S/MIME \(X.509\)](#) ^[28], [OpenPGP](#) ^[30], [Gateway-to-Gateway \(Domänen\) Verschlüsselung](#) ^[31], [TLS](#) ^[65]) für das Absichern des E-Mail Verkehrs mittels Verschlüsselung und Signatur.

Darüber hinaus hat SEPPmail mit seinem patentierten GINA-Verfahren (siehe [GINA-Web-Mail](#) ^[32]) eine Technologie entwickelt, welche den Absender in die Lage versetzt, einem gänzlich „unbekannten“ Empfänger spontan - ohne vorherigem Schlüsselaustausch - eine verschlüsselte E-Mail zu senden. Der Empfänger benötigt für das Entschlüsseln, sowie gegebenenfalls das Verfassen einer sicheren Antwort, ausschließlich Standardkomponenten. Das heißt ein beliebiger E-Mail Client (dies kann auch ein Web-Mail Client sein), ein beliebiger Internet-Browser und der Zugang zum Internet ist ausreichend, unabhängig vom Endgerät.

Durch die Kombination dieser Verfahren wird der verschlüsselte Versand der als vertraulich gekennzeichneten E-Mails zu 100% gewährleistet. Ermöglicht wird dies über das Ruleset (siehe [Zentrales Regelwerk](#) ^[80]), mittels welchem die SEPPmail Appliance entscheidet, welches das für den Empfänger geeignetste Verfahren ist. Beginnend mit dem Prüfen, ob ein beglaubigter öffentlicher S/MIME Schlüssel (Zertifikat) des Empfängers für das Verschlüsseln zur Verfügung steht, kaskadiert das System über [OpenPGP](#) ^[30], [Domänenverschlüsselung](#) ^[31] bis hin zu [GINA-Webmail](#) ^[32] (siehe [Verschlüsselungshierarchie](#) ^[66]).

GINA kommt also nur dann zum Einsatz, wenn aufgrund fehlenden Schlüsselmaterials kein Standard-Verfahren angewendet werden kann oder das Verfahren vom Versender ganz bewusst - zwecks Erhalt einer verbindlichen Lesebestätigung - gewählt wird.

Die SEPPmail Appliance besteht aus „nur“ einem Hauptprodukt, welches jeweils für alle Kunden bereit gestellt wird. Einzelne Features, welche von Kunden gewünscht werden und in das Gesamtkonzept in punkto Sicherheit und Benutzerkomfort passen, werden kostenfrei von SEPPmail implementiert und kommen somit allen Kunden zu Gute.

Die Lösung wird komplett als, auf OpenBSD basierende Firmware geliefert. Damit entfällt das aufwendige Installieren und Warten von Einzelkomponenten, wie zum Beispiel Datenbanken oder Funktionsmodulen. Das Update erfolgt auf Knopfdruck für das gesamte System.

3.2.1.1 Fünf generische Prinzipien

1. Angemessenes Absichern von Geschäftsdaten

Das Absichern wird durch den Einsatz bewährter Verschlüsselungstechnologien (S/MIME, OpenPGP, GINA und TLS) sowie durch das Härten der Appliance garantiert.

2. Kosteneffizienter Betrieb

Kosteneffizienz wird durch den Appliance – Ansatz, einem hohen Automatisierungs- und Standardisierungsgrad und insbesondere einem sehr niedrigen Support Aufwand der GINA-Technologie im Vergleich zu anderen Methoden (PDF oder Web-Mailer) erreicht.

3. Hohe Anzahl von Kunden und Geschäftspartnern erreichbar

Die Massentauglichkeit der SEPPmail Appliance und insbesondere des integrierten Spontankommunikationsverfahrens - die patentierte GINA-Technologie - zeigt sich mit „Incmail“. Incmail ist der „Volksverschlüsselungsdienst“ der Schweizerischen Post, welcher auf der GINA-Technologie basiert. Vermutlich werden in keinem anderen Projekt auch nur annähernd so viele Kunden bedient beziehungsweise so viele E-Mails mit alternativen Methoden verschlüsselt. Vor allem im B2B Bereich findet die Domänenverschlüsselung immer mehr Verbreitung, da hier der gesamte E-Mail Verkehr zwischen den teilnehmenden Unternehmen zuverlässig und völlig transparent abgesichert werden kann (siehe [Gateway-to-Gateway \(Domänen-\) Verschlüsselung](#) ^[31]).

4. Hoher Grad von Akzeptanz

Vor allem bei der Spontankommunikation, für welche immer ein alternatives und somit nicht transparentes, Verfahren zum Einsatz kommt, ist die Akzeptanz dieses Verfahren sehr hoch. Auch in diesem Punkt kann die GINA-Technologie überzeugen, wie Tests in unabhängigen Benutzerlaboren ebenso zeigen, wie der Einsatz bei der Schweizerischen Post.

5. Erfüllen der geschäftlichen und rechtlichen Rahmenbedingungen

Bei der GINA-Technologie werden E-Mails generell vollständig verschlüsselt ausgeliefert. Somit gelangt die E-Mail in den Verantwortungsbereich des Empfängers. Rechtliche Probleme wie bei den sogenannten „sicheren“ Web-Mailern, bei welchem eine E-Mail bis zum Abholen durch den Empfänger vorgehalten werden, entstehen somit nicht.

3.2.2 Verschlüsselungstechnologien

Grundsätzlich kommen beim Verschlüsseln zwei Verfahren zum Einsatz, das symmetrische und asymmetrische Verschlüsseln. Dabei hat jedes Verfahren seine Vor- und Nachteile.

Symmetrisch

Beim symmetrischen Verschlüsseln wird mit einem Schlüssel verschlüsselt. Der Kommunikationspartner muss für das Entschlüsseln im Besitz desselben Schlüssels sein. Das heißt jedoch, dass für jeden Kommunikationspartner ein eigener Schlüssel verwendet werden muss. Problematisch sind dabei der sichere Austausch der Schlüssel und das Verwalten der Schlüssel bei vielen Kommunikationspartnern.

Diese Art des Verschlüsseln ist wenig rechenintensiv und somit schnell und ressourcenschonend.

Asymmetrisch

Beim asymmetrischen Verschlüsseln wird ein Schlüsselpaar verwendet, welches aus einem öffentlichen Teil (public key) und einem privaten Teil (private oder secret key) besteht. Der öffentliche Schlüssel ist mit einem Vorhängeschloss, der private Schlüssel dem dazu passenden Schlüssel vergleichbar. Somit muss dem Absender eines zu verschlüsselnden Dokumentes nur der „public key“ des Empfängers bekannt sein. Nur der Empfänger wird in der Lage sein, das Dokument mit dem dazu passenden „privaten Schlüssel“ wieder zu entschlüsseln.

Somit kann der „public key“ ohne weitere Sicherheitsmaßnahmen an jeden beliebigen Kommunikationspartner gegeben werden und ist somit mehrfach verwendbar.

Dieses Verfahren ist allerdings sehr rechenintensiv und deshalb langsam und ressourcenraubend.

Hybrid

Mit dem hybriden Verfahren werden die Vorteile aus symmetrischer und asymmetrischer Verschlüsselung genutzt. So wird das zu verschlüsselnde Dokument ressourcenschonend und schnell symmetrisch mit einem sogenannten Session-Key, welcher nur einmalig zum Einsatz kommt, verschlüsselt. Der Austausch des symmetrischen Session-Keys erfolgt mittels asymmetrischer Verschlüsselung. Aufgrund dieser Vorteile hat sich dieses Verfahren für die Dokumentenverschlüsselung durchgesetzt und kommt in den Standardverfahren **S/MIME (X.509)**^[28] und **OpenPGP**^[30] zum Einsatz.

Mit diesen Standardverfahren verschlüsselte, eingehende E-Mails werden durch die SEPPmail Appliance automatisiert entschlüsselt. Somit bleibt dieser Vorgang für den E-Mail Empfänger komplett transparent. Die E-Mail gelangt unverschlüsselt in die Mailbox des Empfängers und kann - wie bisher - ohne Zusatzaufwand gelesen werden.

Um zusätzlich, zu der durch das Verschlüsseln erlangten Vertraulichkeit einer E-Mail, auch die Authentizität des Absenders sowie die Integrität des E-Mail Inhalts zu gewährleisten, sind diese häufig zusätzlich mit **Elektronische Signaturen**^[68] versehen. Diese basieren letztendlich auf dem asymmetrischen Verschlüsselungsverfahren, welches natürlich von den hybriden Technologien ebenfalls beherrscht wird.

3.2.2.1 S/MIME (X.509)

S/MIME ist wohl das am weitest verbreitete Standardverfahren für die abgesicherte E-Mail-Kommunikation. Das liegt vor allem an der zugrundeliegenden, hierarchisch aufgebauten Vertrauensstruktur. Durch diese Struktur lassen sich **Elektronische Signaturen**^[68] automatisiert überprüfen. Voraussetzung hierfür ist, dass die Signatur-Zertifikate von einer vertrauenswürdigen Zertifizierungsstelle, auch CA (Certificate Authority) genannt, ausgestellt wurden.

Durch dieses automatische Herstellen des Vertrauens kann wiederum der öffentliche Schlüssel (Zertifikat) des Signierenden in der Signatur mitgeliefert werden. Dieses wird für das Prüfen der Integrität des Inhalts und der Authentizität des Absenders bei eingehenden E-Mails ebenso benötigt, wie für das Verschlüsseln an den Signierenden bei ausgehenden E-Mails.

CA und Zertifikat sind in etwa mit einem Passamt und den von ihm ausgestellten Pässen vergleichbar.

Ist auf der SEPPmail Appliance die ausstellende CA eines Signatur-Zertifikates nicht bekannt, so wird das Wurzelzertifikat dieser CA aus der Signatur eingesammelt und der Administrator benachrichtigt. Dieser legt im Anschluss fest, ob dem CA Zertifikat und somit der Zertifizierungsstelle, zukünftig vertraut werden soll (halbautomatischer Vorgang).

Wurde der CA bereits das Vertrauen ausgesprochen, sammelt die SEPPmail Appliance beim Überprüfen der Signaturen die (gültigen!) Zertifikate der Kommunikationspartner ein, sodass diese im Anschluss für das Verschlüsseln bereit stehen.

S/MIME eignet sich sowohl für die personenbezogene, als auch für die domänenbezogene (siehe [Gateway-to-Gateway \(Domänen-\) Verschlüsselung](#) ^[31]) Verschlüsselung.

3.2.2.1.1 Managed PKI



Die SEPPmail Appliance beinhaltet eine vollständige PKI und verwaltet User Schlüssel beziehungsweise Zertifikate zentral im System. E-Mail Zertifikate können von beliebigen CAs eingespielt werden. Zu den wichtigsten CAs stellt SEPPmail jedoch Konnektoren zur Verfügung:

aktive Konnektoren

- D-Trust Bundesdruckerei (Deutschland)
- Deutsches Forschungsnetz Zertifizierungsstelle des Deutschen-Forschungsnetzes
- DigiCert akkreditierte US amerikanische Zertifizierungsstelle mit Sitz in Lehi / Utah
- GlobalSign akkreditierte Zertifizierungsstelle mit Sitz in Großbritannien
- GlobalTrust akkreditierte Zertifizierungsstelle mit Sitz in Österreich
(neu in 12.0)
- QuoVadis Trustlink International akkreditierte Schweizer CA
- SCEP Protokoll, durch welches CAs diverser Hersteller – auch Microsoft – angebunden werden können. Dabei handelt es sich jedoch (noch) um keinen Standard (RFC).
- SECTIGO akkreditierte US amerikanische Zertifizierungsstelle mit Sitz in Roseland / New Jersey
(vormals Comodo)
- SwissSign Zertifizierungsstelle der Schweizerischen Post

in Vorbereitung

- A-Trust akkreditierte Zertifizierungsdiensteanbieter für qualifizierte Zertifikate in Österreich und Liechtenstein
- Entrust akkreditierte US amerikanische Zertifizierungsstelle mit Sitz in Dallas / Texas

Über diese Konnektoren können E-Mail- und gegebenenfalls Personenzertifikate automatisiert von den entsprechenden CAs bezogen werden. Das jeweils zum Tragen kommende Verfahren kann dabei unterschiedlich sein. In der Appliance werden die so bezogenen Zertifikate den Usern automatisiert zugeordnet und zur Signatur herangezogen.

Der Bezug von Zertifikaten für die E-Mail-Konten ist daher flexibel und individuell konfigurierbar.

Bei Anlage eines neuen Benutzers - dies kann wahlweise automatisch, zum Beispiel durch Anfordern von Verschlüsselung oder Signatur, oder manuell erfolgen - kann gewählt werden, ob ein E-Mail Zertifikat automatisch ausgestellt werden soll. Dieses kann dann von der internen (Zwischen-)Zertifizierungsstelle oder auch (Sub-)CA oder über die MPKI Schnittstelle bezogen werden. Bei Bedarf sind auch beide Varianten parallel möglich.

Wird das Zertifikat über die MPKI bezogen, so wird das Schlüsselpaar in der Regel auf der SEPPmail Appliance generiert und nur der öffentliche Schlüssel zum Signieren an die vertrauenswürdige Zertifizierungsstelle (trusted CA) übermittelt. Der sensible private Schlüssel verlässt bei diesem Verfahren zu keiner Zeit die Appliance und liegt dort – wie das gesamte Schlüsselmaterial – in einem gesicherten Bereich ab.

Auch das Erneuern der Zertifikate ist vollautomatisiert möglich. Dabei wird in der Regel ein Überschneidungszeitraum eingerichtet, sodass bereits vor Ablauf eines Zertifikates ein neues generiert wird. Durch diese Überschneidung ist gewährleistet, dass den Kommunikationspartner spätestens zum Ablauf des alten Zertifikates bereits ein neues, gültiges Zertifikat für das Verschlüsseln vorliegt.

Für den MPKI Funktionsablauf finden Sie in unseren [YouTube Channel](#) ein entsprechendes [Erklärvideo](#).

3.2.2.1.2 Güte eines Zertifikates

Um eine SEPPmail Appliance mit Zertifikaten zu bestücken, sollte geklärt sein, in welcher Qualität diese gewünscht sind.

SSL Zertifikat

Zunächst wird für das Absichern der SSL Strecke, welche durch die GINA-Funktionalität etabliert wird, im Regelfall zwingend ein SSL-Zertifikat notwendig. Damit die gängigen Browser keinen Sicherheitsverstoß beim Aufruf der GINA-Oberfläche melden, sollte dieses Zertifikat von einer offiziellen Zertifizierungsstelle kommen und den FQDN - also den Namen, unter welchem das GINA-Oberfläche zu erreichen ist - beinhalten.

E-Mail Zertifikat

Zertifikate, welche für das Signieren (und Verschlüsseln) von E-Mails geeignet sind, werden in unterschiedlichen Güteklassen von den Ausstellern (CAs) angeboten. Eine einheitliche Klassifizierung gibt es dabei leider nicht. Die Zertifikate unterscheiden sich jedoch in Ihrer Aussagekraft.

Beim einfachsten Zertifikat wird lediglich die Existenz der E-Mail-Adresse bestätigt. Somit wird mit dieser Art des Zertifikates durch die Signatur bestätigt, dass die E-Mail

- während des Transportes nicht verändert wurde
- von der benannten Absenderadresse stammt

In der nächst höheren Zertifikatsgüte wird zusätzlich der Absender namentlich benannt. Das heißt für das Ausstellen dieses Zertifikates musste sich der Inhaber in irgend einer Form ausweisen. Bei Einsatz einer MPKI (siehe [Managed PKI](#) ^[29]) bestätigt die beantragende Organisation, dass sie nur Zertifikate für Ihre Mitarbeiter ausstellt. Somit bestätigt dieses zusätzlich

- die Person des Absenders und dessen Organisation

Diese Zertifikate könnten in der Regel für zusätzliche Zwecke verwendet werden, wie zum Beispiel dem Signieren von Dokumenten wie in etwa PDF-Dateien.

Für das Ausstellen eines qualifizierten Zertifikats - wie z.B. beim Personalausweis in Deutschland, der SuisseID in der Schweiz oder der Bürgerkarte in Österreich - muss die Identität der beantragenden Person zuverlässig festgestellt werden. Hierfür muss die Person entweder mit Ihrem Ausweis persönlich vorstellig werden oder ein alternatives Verfahren, wie zum Beispiel PostIdent in Deutschland, kommt zum Einsatz. Eine automatisches Ausstellen über eine [Managed PKI](#) ^[29] ist somit unmöglich!

Selbst signierte Zertifikate sind für das Signieren von E-Mails ungeeignet, da die Zertifikatskette beim Kommunikationspartner in der Regel nicht bekannt ist und somit kein Vertrauen hergestellt werden kann.

3.2.2.2 OpenPGP

Entgegen der hierarchischen Vertrauensstruktur von [S/MIME](#) ^[28], basiert OpenPGP auf einem anarchistischen Vertrauensmodell, das aus Vertrauensketten besteht (ich vertraue jemandem, dem jemand vertraut dem ich vertraue). Ein 100%iges Zuordnen eines öffentlichen Schlüssels zu einer Person ist somit nicht automatisch möglich. Das heißt, nur über ein manuelles Validieren, zum Beispiel durch Prüfen des Fingerabdrucks (Hash) und Abgleich desselbigen über einen anderen Kommunikationskanal (zum Beispiel Telefon), kann ein eindeutiges Vertrauen hergestellt werden.

SEPPmail Appliance bietet innerhalb der GINA-Technologie für den Kommunikationspartner die Möglichkeit, sein Schlüsselmaterial hochzuladen. Da das Authentisieren des Benutzers in diesem Fall durch das Anmelden an GINA bereits erfolgt ist, entfällt mit dieser Variante die Notwendigkeit des erneuten Prüfens des Schlüssels.

OpenPGP eignet sich sowohl für die personenbezogene, als auch für die domänenbezogene (siehe [Gateway-to-Gateway \(Domänen-\) Verschlüsselung](#) ^[31]) Verschlüsselung.

3.2.2.3 Gateway-to-Gateway (Domänen) Verschlüsselung

Eine Grundfunktionalität aller SEPPmail Appliances ist die Domänenverschlüsselung. Bei dieser Art der Verschlüsselung wird zwischen den Kommunikationspartnern jeweils ein, für die ganze E-Mail Domäne gültiger, öffentlicher S/MIME (oder OpenPGP) Schlüssel manuell ausgetauscht. Dieses Verfahren funktioniert somit auch mit Gateways anderer Hersteller, sofern diese das Verfahren unterstützen. Somit können E-Mails zwischen diesen E-Mail Domänen, auch ohne jeweils persönlichem Schlüsselmateriale der einzelnen Benutzer, inhaltlich verschlüsselt ausgetauscht werden.

Jede auf der SEPPmail Appliance eingerichtete Domänenverschlüsselung steht grundsätzlich allen Benutzern - egal ob diese auf der Appliance als User angelegt sind oder nicht - zur Verfügung. Das heißt, dass hiermit der gesamte E-Mailverkehr zwischen zwei Domänen inhaltlich abgesichert wird.

Diese Verschlüsselungstechnologie ist Bestandteil der SEPPmail Appliance Grundlizenz und steht daher allen Absendern zur Verfügung. Eine User-Lizenz ist hierfür nicht erforderlich.

Für den Domänenverschlüsselungs-Funktionsablauf finden Sie in unseren [YouTube Channel](#) ein entsprechendes [Erklärvideo](#).

3.2.2.3.1 Managed Domain Service

Der Managed Domain Service ist ein SEPPmail Add-On zur Domänenverschlüsselung ³¹⁾. Dabei werden für teilnehmende Kunden die, auf jeder SEPPmail Appliance automatisch generierten, öffentlichen S/MIME Domänenschlüssel automatisiert zwischen allen SEPPmail Appliances und deren OEM Derivaten ausgetauscht. Somit steht in der Regel zwischen SEPPmail Appliances grundsätzlich die Domänenverschlüsselung ³¹⁾ automatisch zur Verfügung.

Auch der Managed Domain Service steht im Rahmen der Domänenverschlüsselung ³¹⁾ bereits über die Grundlizenz allen Absendern zur Verfügung. Eine User-Lizenz ist auch hierfür nicht erforderlich.

3.2.2.4 GINA-Webmail

Die SEPPmail Appliance verfügt über eine patentierte Technologie zur Spontankommunikation, die GINA-Technologie.

Über diese Technologie ist gewährleistet, dass E-Mails, welche verschlüsselt werden sollen, selbst dann verschlüsselt werden können, wenn der Kommunikationspartner über keine der Standardtechnologien verfügt.

Der Kommunikationspartner benötigt für das Lesen, der mit dieser Technologie verschlüsselten E-Mails lediglich einen Internetzugang, die Möglichkeit E-Mails zu empfangen und einen Web-Browser.

Weitere Anforderungen an die Infrastruktur des Benutzers bestehen nicht.

GINA bietet, im Vergleich zu anderen auf dem Markt verfügbaren Ansätzen für die sichere E-Mail Kommunikation mit beliebigen Partnern, wichtige Vorteile:



	PDF-Ver-schlüsselung	„Normales“ Secure Web-Mail	Selbst-extra-hierendes Archiv	Spezieller Client	
Empfänger kommt mit Standardkomponenten aus (Mail-Client/Browser/Internet)	✗	✓	✗	✗	✓
Passwortwechsel möglich	✗	✓	✗	✗	
Sichere Antwort möglich	✗	✓	✗	✓	
Mail wird sofort und vollständig ausgeliefert	✓	✗	✓	✓	
Corporate Identity individuell anpassbar	✓	✓	✗	✗	
Empfänger kann seinen öffentlichen Schlüssel hinterlegen	✗	✓	✗	✗	
Empfänger kann vorgängig sein Wunschpasswort hinterlegen	✓	✓	✗	✗	
Appliance hält keine Nutzerdaten	✓	✗	✗	✗	
Phishing Resistent	✗	✗	✓	✓	
Resistent gegen Brute Force Attacks	✗	✓	✗	✓	
„E-Mail als Einwurf-Einschreiben“; Lesebestätigung möglich	✗	✓	✗	✗	
Passwort Selfservice	✗	✓	✗	✗	
Two-Factor Authentication	✗	✗	✗	✗	
Queueless Betrieb (kein Datenverlust bei Ausfall)	✗	✗	✗	✗	

a) Schritt 1: Sender - E-Mail verfassen

Der Sender verfasst in seinem Standard E-Mail Client eine E-Mail und klassifiziert diese als zu verschlüsselnd. Hierzu stehen mehrere Möglichkeiten zur Verfügung (Abbildung 1):

- Über die E-Mail Client Bordmittel als „vertraulich“ markieren ①
- Über ein unternehmensweit definiertes Schlüsselwort ②
Im Standard lautet dieses Schlüsselwort [confidential]. Diese Methode ist auf allen E-Mail Clients verfügbar und wird häufig auch für System-User, also dem maschinellen Ansteuern verwendet.
- Über das kostenfreie **SEPPmail Microsoft Outlook Add-In** ③.
In diesem kann gewählt werden zwischen
 - a) „Verschlüsseln“
Initiiert das Verschlüsseln mit der für den Empfänger geeignetsten Technologie (siehe auch **Verschlüsselungshierarchie** 66).
 - b) „Verschlüsseln mit Lesebestätigung“
Erzwingt die GINA-Technologie in Verbindung mit der Client seitigen Lesebestätigungsanforderung. Dadurch wird eine, durch den Empfänger nicht zu unterdrückende, Lesebestätigung ausgelöst. Dieses Verfahren ist mit einem Einschreiben mit Rückschein vergleichbar!

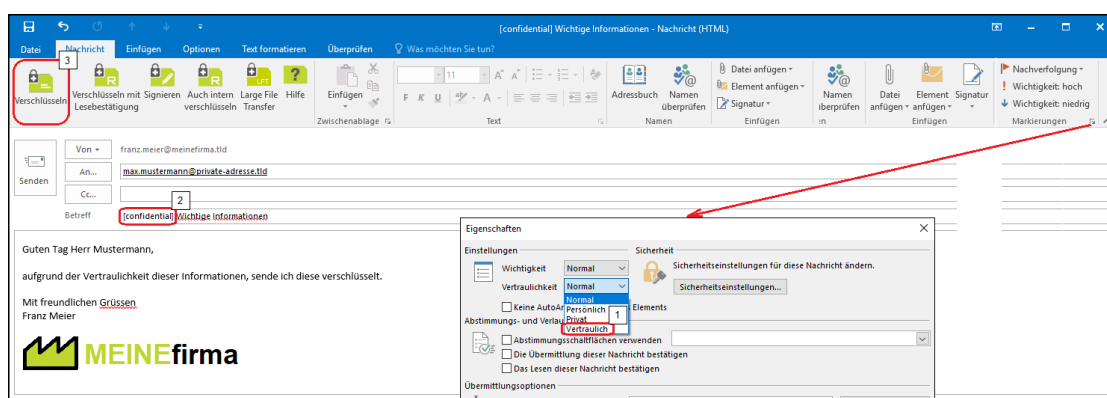


Abbildung 1

Im Anschluss wird die E-Mail wie gewohnt versendet.

b) Schritt 2: Sender - Verschlüsseln

Die so gekennzeichnete E-Mail gelangt über den E-Mail Server auf die SEPPmail Appliance. Diese wertet die gesetzten Kennzeichen aus und führt die dadurch initiierten Aktionen aus.

Kommt, aufgrund fehlenden Schlüsselmaterials oder erzwungener Lesebestätigung, GINA zum Einsatz, so wird wie folgt weiter verfahren:

Sofern nicht bereits vorhanden, wird für die betroffene Empfänger-E-Mail-Adresse - je nach Verfahren - ein GINA-Account oder Hilfs-Account angelegt, wobei ein individueller, passwortgeschützter AES256 Schlüssel generiert und der Empfänger-E-Mail-Adresse hinterlegt wird.

Abhängig vom gewählten GINA-Verfahren unterscheiden sich die weiteren Schritte:

1. **Standard Prozess** 35
2. **Einmal-Passwort / One-Time-Password OTP** 42
3. **E-Mail Passwort / Unique-E-Mail-Passwort UEP** 43
4. **Authentisierungsanfrage bei Identitätsanbieter (IDP)** 44

Dabei ist das Anwenden der Authentisierungsanfrage bei einem externen Identitätsanbieter (4.) vermutlich die für den Empfänger komfortabelste Lösung.

3.2.2.4.1 Standard Prozess

Das im GINA Standard Prozess benötigte Initialpasswort des generierten Schlüssels wird wahlweise

- dem Empfänger direkt per SMS an die im Betreff der E-Mail anzugebende Mobilfunk-Nummer übermittelt.
- dem Absender via E-Mail zur Weitergabe an den Empfänger über einen zweiten Kommunikationskanal - SMS (siehe Abbildung 2) oder Telefon (sofern die integrierte SMS-Schnittstelle nicht konfiguriert wurde) - mitgeteilt.

The screenshot shows the SEPPMAIL web interface. At the top left is the SEPPMAIL logo. The main content area is divided into two columns. The left column contains the following text: 'SMS-Versand des sicheren E-Mail Passworts für: max.mustermann@private-adresse.tld', followed by a section 'SMS-Nachricht und Sprache wählen' with two radio button options: 'Sicheres E-Mail Passwort für max.mustermann@private-adresse.tld: ohsh9Phi' (selected) and 'Secure e-mail password for max.mustermann@private-adresse.tld: ohsh9Phi'. Below this is a section 'Geben Sie die Handynummer des Empfängers ein' with a text input field and the instruction 'Bitte geben Sie die Telefonnummer im internationalen Format (z.B. 0041123456789) ein.' At the bottom of the left column, it says 'Dieser Dienst wird bereitgestellt und betrieben von der SEPPmail AG Schweiz' with links for 'Impressum' and 'Datenschutz'. The right column features a large 'SMS senden' button. At the bottom right, it says 'Powered by SEPPmail'.

Abbildung 2

Der GINA-Account bleibt persistent. Somit kann er dauerhaft für weitere E-Mails an diesen Empfänger verwendet werden.

Ist der GINA-Account für den Empfänger vorhanden, wird die komplette E-Mail des Absenders mit dem AES256 Schlüssel des GINA-Accounts des Empfängers verschlüsselt und in einen HTML-Container gepackt. Dabei wird auf aktive Inhalte, wie zum Beispiel JavaScript, aus Sicherheitsgründen komplett verzichtet.

Der HTML-Container wird nun an eine, vom Absender automatisch über die Appliance signierte, Träger-E-Mail angehängen. Diese Träger-E-Mail enthält, neben der im HTML Anhang befindlichen eigentlichen E-Mail, Kurzinformationen für den Empfänger zum Umgang mit dieser Technologie (Abbildung 2a).

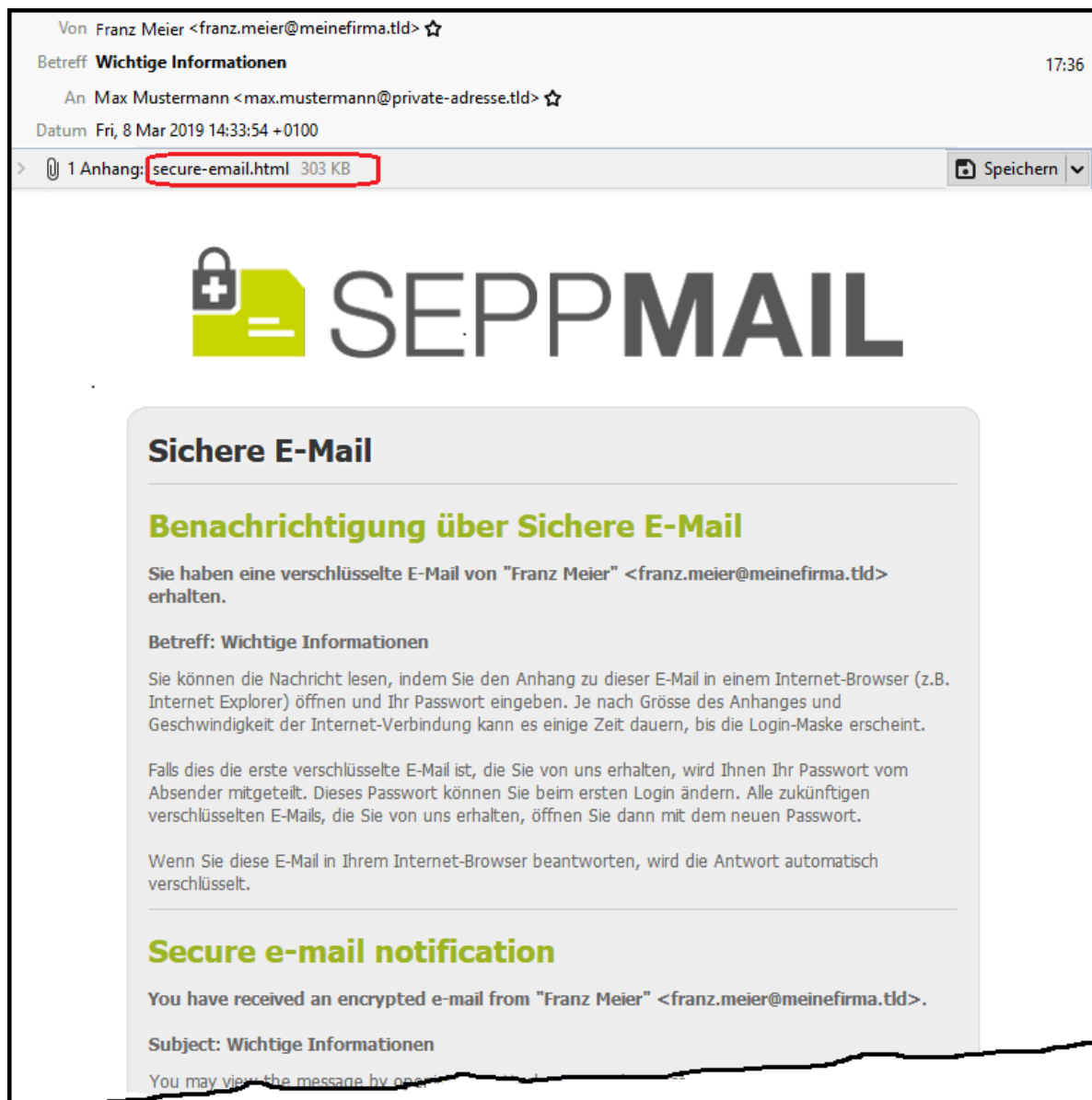


Abbildung 2a

Mit der Träger-E-Mail wird somit auch die im Anhang befindliche eigentliche E-Mail **komplett ausgeliefert und geht somit in den Verantwortungsbereich des Empfängers über** (Abbildung 2a). Auf der Appliance bleiben ausser dem GINA-Account keine Daten zurück.



c) Schritt 3: Empfänger – Anmelden und einmaliges Registrieren

Der Empfänger öffnet den HTML-Anhang (lokal), worauf er bereits die gewünschte Sprache auswählen kann (Abbildung 3).

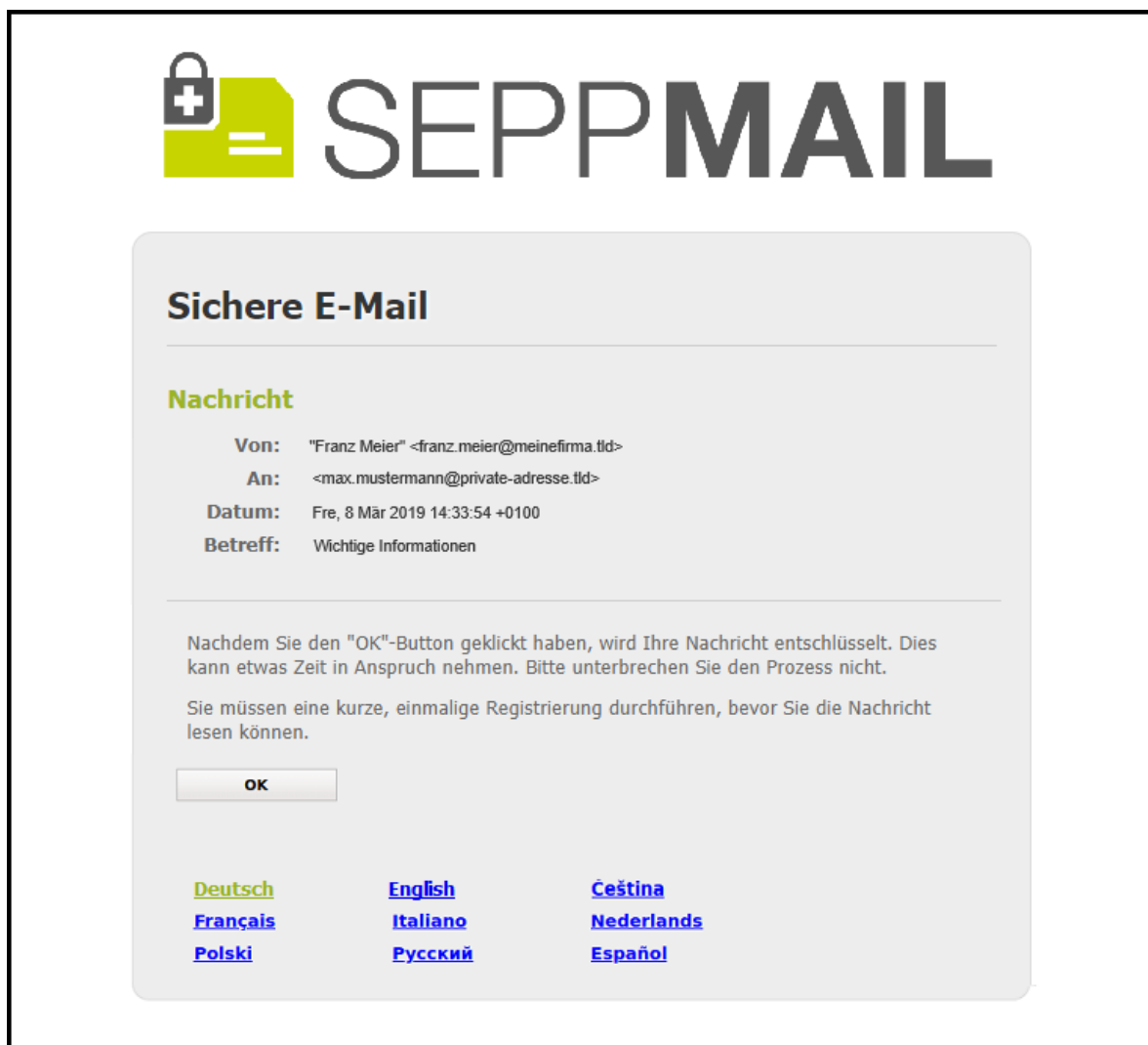


Abbildung 3

Im Anschluss öffnet die GINA-Oberfläche und fordert zur Eingabe des (Initial-)Passwortes auf (Abbildung 3a).

Abbildung 3a

Nur beim initialen Aufruf ist ein **einmaliges** Registrieren (Abbildung 3b) am System erforderlich. Dabei vergibt sich der GINA-Benutzer ein eigenes Passwort. Je nach Sicherheitseinstellung wird zusätzlich eine Sicherheitsfrage + Antwort festgelegt, um das selbstständige Zurücksetzen des Passwortes durch den GINA-Benutzer - ohne jeglichen Hotline-Aufwand (!) - zu ermöglichen. Diese Sicherheitsfrage kann durch den GINA-Benutzer selbst definiert, oder aus den vom Betreiber vorgegeben Sicherheitsfragen ausgewählt werden. Wurde das Initialpasswort bereits per SMS gesendet, so ist das entsprechende Eingabefeld im Registrierungsprozess bereits vorausgefüllt. Die Passwortkriterien, das Anzeigen der optionalen Eingabefelder, sowie gegebenenfalls der AGBs werden durch den Betreiber der SEPPmail Appliance festgelegt.

Die Anzahl der auszufüllenden Felder des Registrierungsprozesses ist maßgeblich von dem vom Betreiber der SEPPmail Appliance festgelegten Passwort-Rücksetzungs-Verfahren abhängig (siehe auch [Self-Service-Password-Management \(SSPM\)](#) ⁵³⁾!).


Anmelden
Suchen

Neuen Benutzer registrieren

Bitte setzen Sie ein neues Passwort.

Bitte geben Sie Ihren Namen und E-Mail-Adresse ein und setzen ein Passwort sowie eine Sicherheitsfrage und -antwort. Bitte lesen und akzeptieren Sie auch die Nutzungsbedingungen

* E-Mail-Adresse:
max.mustermann@private-adresse.tld

Voller Name:
Max Mustermann

Sprache:
Deutsch

Passwortkriterien

☒ Passwort-Mindestlänge: 8
☒ Das Passwort muss mindestens einen Kleinbuchstaben enthalten
☒ Das Passwort muss mindestens einen Grossbuchstaben enthalten
☒ Das Passwort muss mindestens eine Zahl enthalten
☒ Das Passwort muss mindestens ein Sonderzeichen enthalten
☐ Das Passwort darf nicht Ihren Namen oder Ihre E-Mail-Adresse enthalten
☒ Passwort bestätigen

* Neues Passwort:

sicher

* Passwort bestätigen:

Passwort-Rücksetzung

Bitte wählen Sie eine Sicherheitsfrage, deren Antwort nur Ihnen bekannt ist. Sie wird im Passwort-Rücksetzungs-Prozess sowohl online als auch telefonisch von unserem Support-Team verwendet werden.

* Sicherheitsfrage:

Zu welcher Tageszeit wurden Sie geboren?
Geben Sie eine Sicherheitsfrage ein oder wählen Sie:

* Antwort:
Nacht

Handynummer:
004179 1234 567
Bitte geben Sie die Telefonnummer im internationalen Format (z.B. 0041123456789) ein.

* Nutzungsbedingungen akzeptiert:
☒ [Klicken Sie hier, um die Nutzungsbedingungen zu lesen](#)

Weiter
Abbrechen

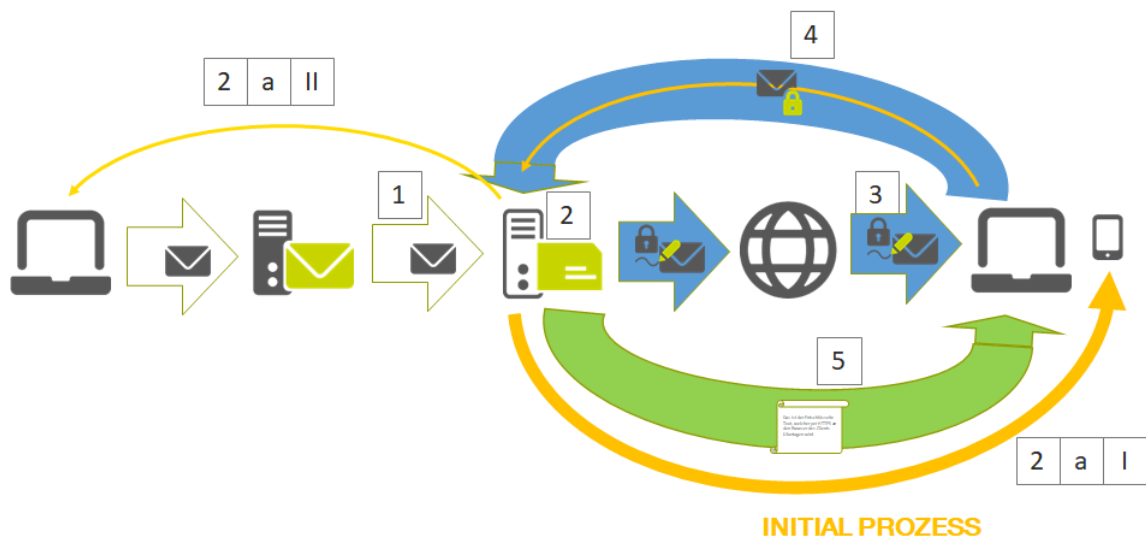
Powered by SEPPmail

Abbildung 3b

Nach erfolgreichem Registrieren gelangt der GINA-Benutzer zum Lesebereich ([E-Mail lesen](#))⁴⁶⁾ der eigentlichen E-Mail.

3.2.2.4.1.1 Funktionsablauf

1. Der Sender verfasst eine E-Mail. Diese wird im Klartext bis zur SEPPmail Appliance übertragen.
2. Kommt, aufgrund fehlenden Schlüsselmaterials oder erzwungener Lesebestätigung, GINA zum Einsatz, so wird die E-Mail mit dem AES256 Schlüssel des GINA-Accounts des Empfängers verschlüsselt und in einen HTML-Container gepackt.
 - a) Ist für die Empfänger E-Mail-Adresse noch kein GINA-Account vorhanden, so wird dieser angelegt. Dabei wird ein individueller, passwortgeschützter AES256 Schlüssel generiert und der Empfänger-E-Mail-Adresse hinterlegt. Das Initialpasswort des generierten Schlüssels wird wahlweise
 - I. dem Empfänger direkt per SMS an die im Betreff (zum Beispiel [sms:0041791234567]) der E-Mail anzugebende Mobilfunk-Nummer gesendet
 - II. dem Absender via E-Mail, zur Weitergabe an den Empfänger über einen zweiten Kommunikationskanal - SMS oder Telefon (sofern die integrierte SMS-Schnittstelle nicht konfiguriert wurde) - mitgeteilt.
3. Die so verschlüsselte E-Mail wird in eine Träger-Mail gepackt und **komplett** an den Empfänger ausgeliefert.
4. Der Empfänger öffnet den Anhang der Träger-Mail, stellt dadurch eine sichere https-Verbindung zur SEPPmail her und übermittelt die ursprüngliche Nachricht aus dem Anhang der Träger-Mail. Im Anschluss wird er aufgefordert, sein initiales Passwort einzugeben, sich zu registrieren und das Passwort zu ändern.
5. Nach dem Entschlüsseln wird die Nachricht über die sichere https-Verbindung im Browser dargestellt.



3.2.2.4.1.2 Unterschiedliche Registrierungsarten

Um gegebenenfalls den Registrierungsprozess für den Kommunikationspartner zu erleichtern, beziehungsweise diesen darauf vorzubereiten, stehen unterschiedliche Registrierungsarten zur Verfügung.

1. Spontaner Kommunikationsbeginn:

Der Sender verfasst eine E-Mail, klassifiziert diese als „Vertraulich“ und versendet sie. Ist die E-Mail nur an einen Empfänger adressiert und ist dessen Mobilfunk-Nummer bekannt, so kann bereits durch Angabe der Nummer im Betreff, in der Form [sms:0049 170 1234 5678] eine entsprechende SMS mit dem Initialpasswort, parallel zum E-Mail Versand, initiiert werden.

Andernfalls wird der Sender über eine GINA-Passwort-Mail aufgefordert, dem Empfänger das Initialpasswort auf parallelem Wege (SMS, Telefon) mitzuteilen.

2. Vorbereitete Kommunikation:

- a) Der Sender versendet eine Einladungs-E-Mail ohne Initialpasswort an den zukünftigen Kommunikationspartner. Diese sollte KEINE vertraulichen Daten beinhalten! Der Empfänger öffnet den HTML-Anhang und der unter **Schritt 3: Empfänger – Anmelden und einmaliges Registrieren** ³⁷⁾ / Abbildung 3a beschriebene Registrierungsprozess startet, ohne vorherige Passwort-Eingabe. Nach abgeschlossenen Registrierungsvorgang kann gesichert kommuniziert werden.
- b) Über einen Link auf der Webseite des SEPPmail Appliance Betreibers gelangt der externe Kommunikationspartner zur GINA-Oberfläche. Über die optionale Funktion „Registrierung“ gelangt der Kommunikationspartner direkt zum Registrierungsprozess. Nach erfolgreichem Registrieren erhält der Kommunikationspartner eine entsprechende Rückmeldung (Abbildung 8) und eine Aktivierungs-E-Mail an die von ihm während des Registrierungsprozesses eingegebene E-Mail Adresse. Erst nach dem Aufruf des Aktivierungs-Links aus dieser E-Mail wird der GINA-Account generiert.



Abbildung 8

3.2.2.4.2 Einmal-Passwort / One-Time-Password OTP

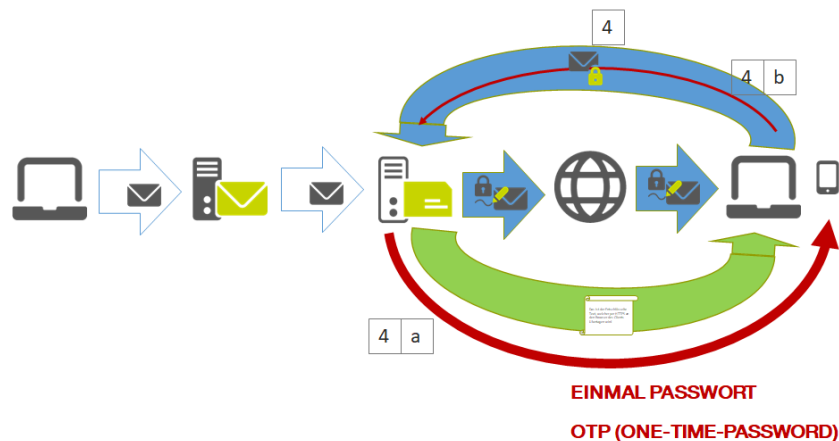
In dieser Variante ist eine Rufnummer des Empfängers, welche SMS empfangen kann, zwingend. Auch hier ist ein Registrierungsprozess (siehe auch **Standard Prozess** [35]) erforderlich, um die SMS-Nummer des Empfängers zu verifizieren.
Für OTP stehen zwei Varianten zur Verfügung:

1. Ausschließlich unter Verwenden von SMS (via SMS only)

Im Registrierungsprozess ist in der Regel nur das Bestätigen der SMS-Nummer erforderlich, wenngleich natürlich optional auch der Anzeigename abgefragt werden kann. Da in diesem Verfahren in der Regel bereits der Versand des initialen Passwortes per SMS erfolgt, muss der Registrierende meist nur noch die vorausgefüllten Daten bestätigen.

Ab diesem Zeitpunkt wird dem GINA-Benutzer bei jedem Öffnen eines GINA-Anhangs (secure-email.html) per SMS ein für dieses Öffnen einmalig gültiges Passwort zugesendet. Das heißt im Vergleich zum GINA-Standard Prozess **Funktionsablauf** [40] ändert sich Punkt 4. wie folgt:

4. Der Empfänger öffnet den Anhang der Träger-Mail, stellt dadurch eine sichere https-Verbindung zur SEPPmail her und übermittelt die ursprüngliche Nachricht aus dem Anhang der Träger-Mail.
 - a) Durch das Einliefern wird ein **Einmal-Passwort** generiert und dem GINA-Benutzer **per SMS** zugestellt
 - b) Mit Eingabe dieses **Einmal-Passworts** wird die E-Mail auf der SEPPmail Appliance entschlüsselt



2. Verwenden von SMS in Kombination mit einem Account (via SMS (account password available))

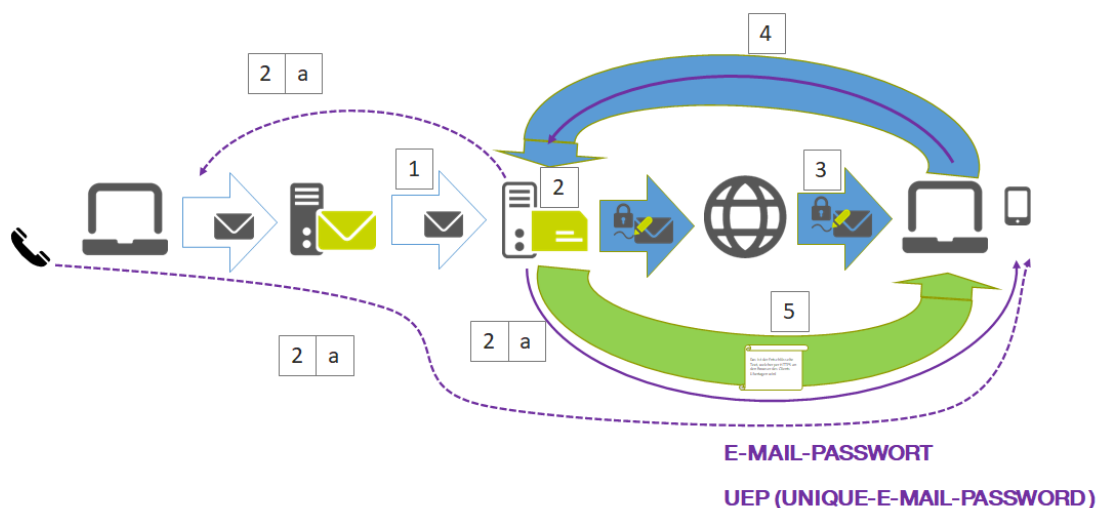
Diese Variante ist eine Kombination aus dem GINA-Standard- und dem OTP-Verfahren. Da ein vollwertiger GINA-Account erzeugt wird, entspricht der Registrierungsprozess dem des **Standard Prozess** [35]. Auch hier wird - wie auch in 1. - jeweils beim Einliefern der GINA-Nachricht ein Einmal-Passwort generiert und per SMS versendet. Jedoch besteht für den GINA-Benutzer zusätzlich die Möglichkeit - quasi als Backup-Verfahren - seine E-Mails jederzeit mit dem beim Registrierungsprozess vergebenen Passwort zu öffnen. Weiterhin ist der GINA-Benutzer aufgrund des vollwertigen Accounts in der Lage, seine eigenen Daten (Name, Passwort, SMS-Nummer usw.) selbst anzupassen.

Daraus resultiert jedoch auch, dass eine GINA-Nachricht nach Verlust des Passwortes für den Empfänger unwiederruflich verloren ist!

Dieses Verfahren wird meist dann verwendet, wenn das sichere Übertragen von Dokumenten zum Beispiel während eines Telefonats mit dem Kommunikationspartner und meist nur einmalig benötigt wird.

Der Ablauf sieht bei diesem Verfahren wie folgt aus:

1. Der Sender verfasst eine E-Mail. Diese wird im Klartext bis zur SEPPmail Appliance übertragen.
2. SEPPmail generiert bei **jedem** GINA-Mail-Versand einen AES256-Key und verschlüsselt damit die E-Mail (symmetrisch).
 - a) Parallel wird dem Empfänger auf einem zweiten Kanal (**direkt via SMS oder indirekt, zum Beispiel via Telefon**) ein – **ausschließlich zu dieser einen E-Mail passendes** – Passwort übermittelt.
3. Die so verschlüsselte E-Mail wird in eine Träger-Mail gepackt und **komplett** an den Empfänger ausgeliefert.
4. Der Empfänger öffnet den Anhang der Träger-Mail, stellt dadurch eine sichere https-Verbindung zur SEPPmail her und übermittelt die ursprüngliche Nachricht aus dem Anhang der Träger-Mail. Im Anschluss wird er aufgefordert, sein **E-Mail bezogenes Passwort** einzugeben. Der Registrierungsprozess entfällt!
5. Nach dem Entschlüsseln wird die Nachricht über die sichere https-Verbindung im Browser dargestellt.



3.2.2.4.4 Authentisierungsanfrage bei Identitätsanbieter (IDP)

Bei diesem Verfahren wird das Authentisieren des GINA-Benutzers über einen „Identitätsanbieter / Identity Provider (IDP)“ durchgeführt.

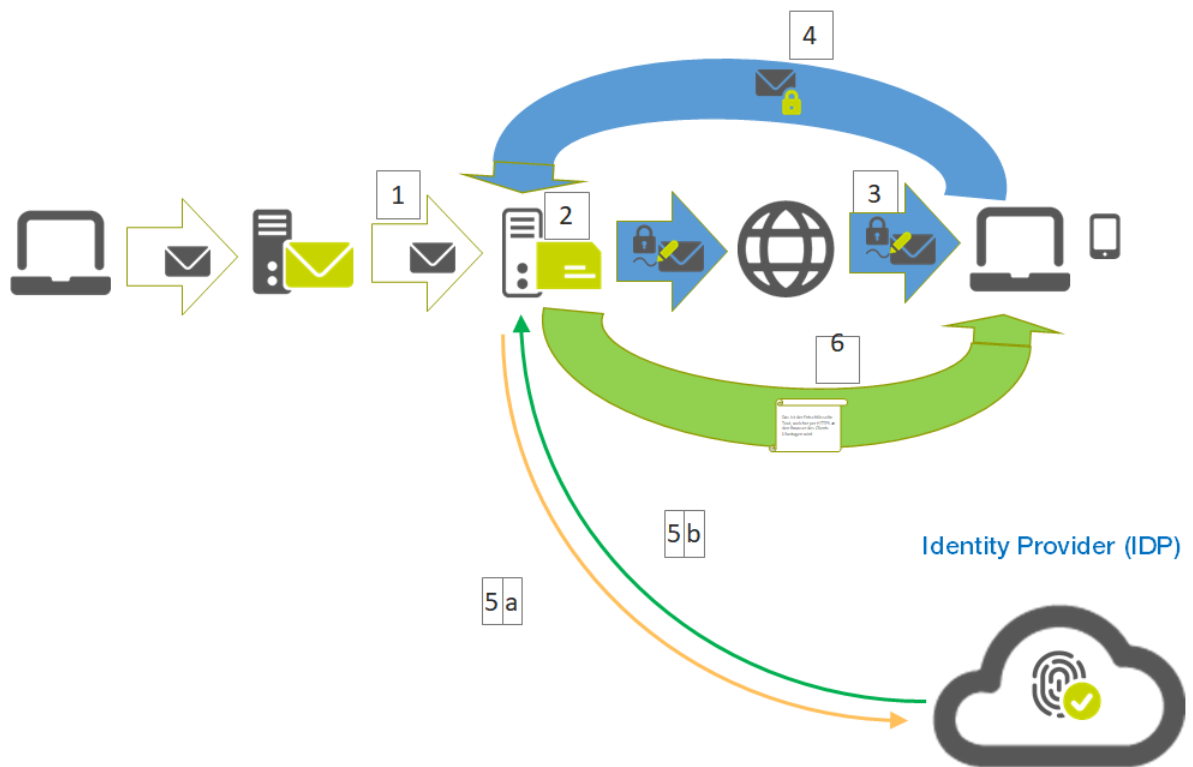
Somit kann der einmalige Registrierungsprozess komplett entfallen, wenngleich ein Account quasi als Backup-Verfahren eingerichtet werden kann.

Wurden vom Betreiber der SEPPmail Appliance externe Identitätsanbieter eingerichtet, so stehen diese dem jeweiligen GINA-Benutzer für das Anmelden zur Verfügung (Abbildung).

Abbildung

Der Ablauf sieht bei diesem Verfahren wie folgt aus:

1. Der Sender verfasst eine E-Mail. Diese wird im Klartext bis zur SEPPmail Appliance übertragen.
2. Kommt, aufgrund fehlenden Schlüsselmaterials oder erzwungener Lesebestätigung, GINA zum Einsatz, so wird die E-Mail mit dem AES256 Schlüssel des GINA-Accounts des Empfängers verschlüsselt und in einen HTML-Container gepackt.
 - a) Ist für die Empfänger E-Mail-Adresse noch kein GINA-Account vorhanden, so wird dieser angelegt. Dabei wird ein individueller, passwortgeschützter AES256 Schlüssel generiert und der Empfänger-E-Mail-Adresse hinterlegt. Ein Initialpasswort ist nicht erforderlich, da die Identität des Empfängers später über den Identitätsanbieter festgestellt wird.
3. Die so verschlüsselte E-Mail wird in eine Träger-Mail gepackt und **komplett** an den Empfänger ausgeliefert.
4. Der Empfänger öffnet den Anhang der Träger-Mail, stellt dadurch eine sichere https-Verbindung zur SEPPmail her und übermittelt die ursprüngliche Nachricht aus dem Anhang der Träger-Mail.
5. Nun wählt der GINA-Benutzer seinen bevorzugten Identitätsanbieter
 - a) Hier authentisiert sich der GINA-Benutzer mit seinen dort hinterlegten Anmeldedaten.
 - b) Wurden die korrekten Anmeldedaten eingegeben, so wird dies vom Identitätsanbieter bestätigt und der GINA-Benutzer gilt somit auch auf der SEPPmail Appliance als authentisiert.
6. Somit wird die Nachricht entschlüsselt und dem GINA-Benutzer über die sichere https-Verbindung im Browser dargestellt.



3.2.2.4.5 E-Mail lesen

Nach erfolgreichem Anmelden, beziehungsweise abschließen des initialen Registrierungsprozesses wird die entschlüsselte E-Mail in der GINA-Web-Oberfläche (Abbildung 4) dargestellt.

Sofern vom Betreiber der SEPPmail Appliance freigeschaltet, bietet die Oberfläche dem GINA-Benutzer die Möglichkeit, die dargestellte E-Mail im Klartext als PDF-, als EML- oder MSG-Datei (Schaltfläche „Speichern als“ Abbildung 4) herunterzuladen.

Wurde die GINA-Oberfläche durch Öffnen einer GINA-Nachricht aufgerufen, so kann über die Schaltfläche „E-Mail lesen“ aus jedem beliebigen Menü wieder zur eigentlichen Nachricht zurückgekehrt werden.

Die GINA-Oberfläche ist bewusst einfach gehalten, um ein intuitives Bedienen zu gewährleisten.

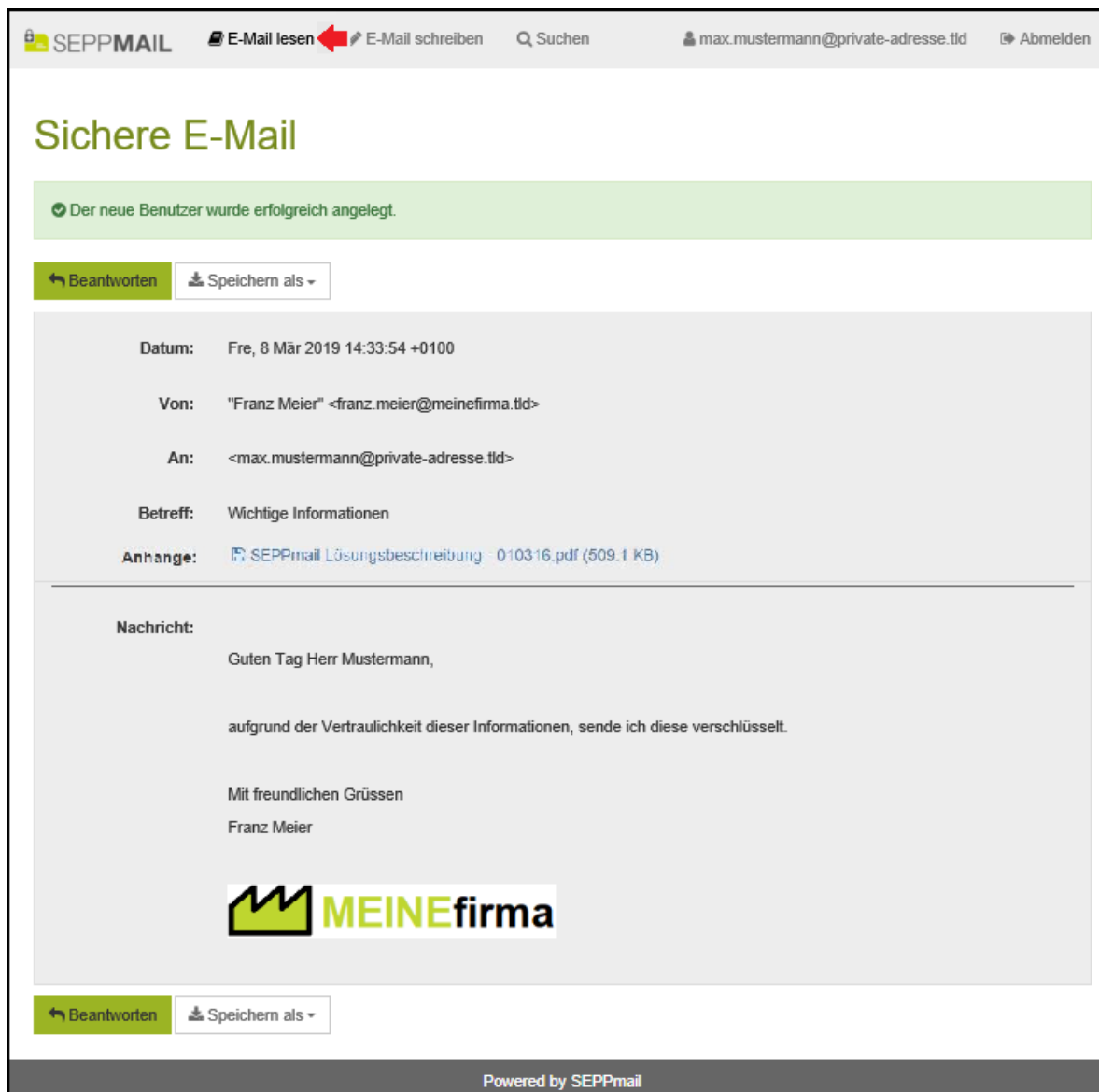


Abbildung 4

Über die Schaltfläche „Beantworten“ ist ein **Sicheres Antworten**^[47] gewährleistet.

3.2.2.4.6 Sicheres Antworten

Unabhängig vom verwendeten GINA-Verfahren, kann auf eine GINA-Nachricht immer auch auf sicherem Wege geantwortet werden.

Wurde vom Empfänger einer GINA-Nachricht diese geöffnet, so kann er über die Schaltfläche „Beantworten“ (Abbildung 4)

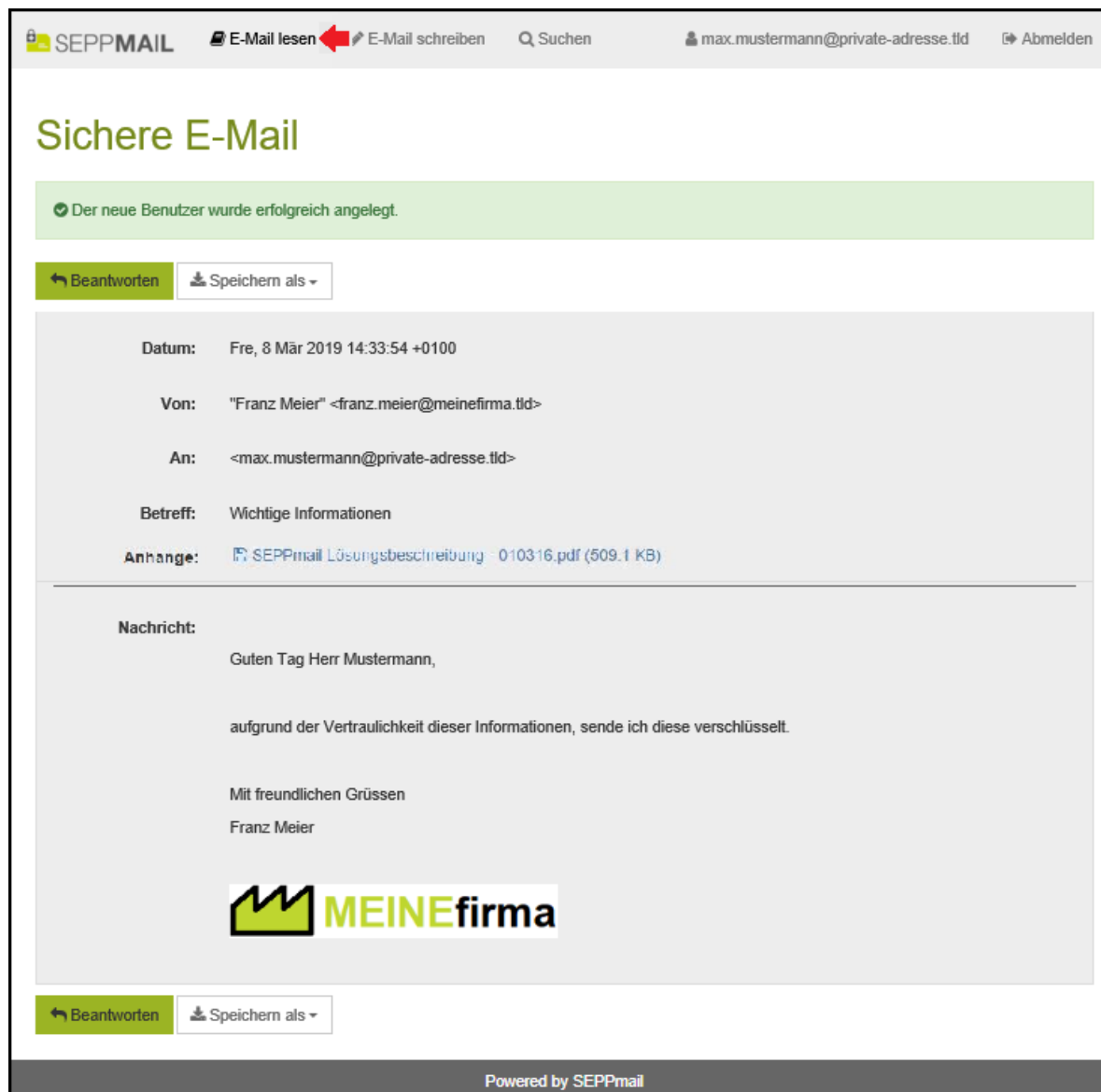


Abbildung 4

dem ursprünglichen Verfasser der Nachricht über einen sicheren Kanal antworten (Abbildung 4a)

SEPPMAIL E-Mail lesen E-Mail schreiben Suchen max.mustermann@private-adresse.tld Abmelden

Sichere E-Mail

Nachricht senden

Von: Max Mustermann <max.mustermann@private-adresse.tld>

An: Franz Meier <franz.meier@meinefirma.tld>

Betreff: Aw: Wichtige Informationen

Anhänge: Datei anhängen

Maximalgröße der Anhänge: 1313.7 MiB

Nachricht:

Guten Tag Herr Meier,
vielen Dank für diese Information.
Mit freundlichen Grüßen
Max Mustermann

> Am Fre, 8 Mär 2019 14:33:54 +0100 schrieb Franz Meier <franz.meier@meinefirma.tld>:
>
> Guten Tag Herr Mustermann,
>
>

☒ Kopie an mich selbst senden
Wenn Sie diese Option nicht setzen, wird Ihre Antwort nicht auf Ihrem lokalen System verfügbar sein.

Nachricht senden

Powered by SEPPmail

Abbildung 4a

Beim Antworten, beziehungsweise Schreiben können natürlich auch Anhänge, in den auf der Appliance durch den Administrator zugelassenen Formaten, beigefügt werden.

Eine Kopie der eigenen Antwort wird dem GINA-Benutzer wieder mittels GINA-Technologie verschlüsselt zurückgeliefert (Abbildung 4b). Somit hat auch er einen Nachweis über seine, via GINA-Oberfläche gesendete, Nachricht.

SEPPMAIL E-Mail lesen E-Mail schreiben Suchen max.mustermann@private-adresse.tld Abmelden

Sichere E-Mail

Die Sichere E-Mail und die Kopie an Sie wurden erfolgreich gesendet.

Powered by SEPPmail

Abbildung 4b

3.2.2.4.7 Abmelden

Durch das Abmelden über die Schaltfläche für das sichere Verlassen der GINA-Oberfläche (Abbildung 5) wird die GINA-Nachricht aus dem Zwischenspeicher der SEPPmail Appliance sowie aus dem Browser-Cache des Empfängers entfernt.



Abbildung 5

Zurück im System des Empfängers bleibt die verschlüsselte Original-GINA-Mail, sowie gegebenenfalls heruntergeladene Klartext-Kopien (siehe auch [E-Mail lesen](#) 46).

3.2.2.4.8 Account-Basierte Funktionen

Bei Account basierten GINA-Varianten (**Standard Prozess** ³⁵⁾, **Einmal-Passwort / One-Time-Passwort OTM** ⁴²⁾ **SMS** (**account password available**) ⁴²⁾ steht dem GINA-Benutzer über das

- **Self-Service-Password-Management (SSPM)** ⁵³⁾

die Möglichkeit zur Verfügung, bei Verlust seines Passwortes dieses selbstständig zurückzusetzen.

Weiterhin besteht für ihn die Möglichkeit, nach dem Anmelden an der GINA-Oberfläche seine Account-Daten selbstständig zu bearbeiten. So kann jeder GINA-Benutzer seinen Namen, Mobilfunknummer und die bevorzugte Sprache (Abbildung 5a) anpassen.

The screenshot displays the 'SEPPMAIL' web interface for editing a user profile. The top navigation bar includes links for 'E-Mail lesen', 'E-Mail schreiben', 'Suchen', and a user profile section for 'max.mustermann@private-adresse.tld' with an 'Abmelden' (Logout) button. The main heading is 'Profil bearbeiten'. Below this, there are three buttons: 'Profil bearbeiten' (highlighted with a red arrow), 'Passwort ändern', and 'Schlüsselverwaltung'. The profile form contains the following fields:

- E-Mail-Adresse:** max.mustermann@private-adresse.tld
- Voller Name:** Max Mustermann
- Sprache:** Deutsch (with a dropdown arrow)
- Handynummer:** 0041791234567

Below the form, a note states: 'Bitte geben Sie die Telefonnummer im internationalen Format (z.B. 0041123456789) ein.' At the bottom of the form are two buttons: 'Speichern' (Save) and 'Profil löschen' (Delete Profile). The footer of the interface reads 'Powered by SEPPmail'.

Abbildung 5a

Ebenso kann der GINA-Benutzer natürlich sein Passwort und - abhängig von der vom Betreiber der SEPPmail Appliance gewählten Passwort Reset Methode (siehe auch [Self-Service-Password-Management \(SSPM\)](#) ⁵³⁾ - auch die Sicherheitsfrage und die dazugehörige Antwort (Abbildung 5b) ändern.

SEPPMAIL E-Mail lesen E-Mail schreiben Suchen max.mustermann@private-adresse.tld Abmelden

Passwort ändern

Profil bearbeiten **Passwort ändern** Schlüsselverwaltung

Passwort ändern Dieses Passwort gilt für alle verschlüsselten Nachrichten, die Sie von uns erhalten. Bitte wählen Sie das Passwort sorgfältig.

Bestehendes Passwort:

Passwortkriterien

- ☐ Passwort-Mindestlänge: 8
- ☐ Das Passwort muss mindestens einen Kleinbuchstaben enthalten
- ☐ Das Passwort muss mindestens einen Grossbuchstaben enthalten
- ☐ Das Passwort muss mindestens eine Zahl enthalten
- ☐ Das Passwort muss mindestens ein Sonderzeichen enthalten
- ☐ Das Passwort darf nicht Ihren Namen oder Ihre E-Mail-Adresse enthalten
- ☐ Passwort bestätigen

Neues Passwort:

Passwort bestätigen:

Passwort-Rücksetzung Bitte wählen Sie eine Sicherheitsfrage, deren Antwort nur Ihnen bekannt ist. Sie wird im Passwort-Rücksetzungs-Prozess sowohl online als auch telefonisch von unserem Support-Team verwendet werden.

Sicherheitsfrage:

Geben Sie eine Sicherheitsfrage ein oder wählen Sie:

Antwort:

Profil bearbeiten **Passwort ändern** Schlüsselverwaltung

Powered by SEPPmail

Abbildung 5b

Sofern dies vom Betreiber der SEPPmail Appliance freigeschaltet ist, stehen dem GINA-Benutzer noch weitere Möglichkeiten innerhalb seines Profils zur Verfügung:

- [\(optional\) Initiales Schreiben von Nachrichten](#) ⁵⁶⁾
- [\(optional\) Schlüsselverwaltung](#) ⁵⁷⁾
- [\(optional\) Selbstlöschung](#) ⁵⁸⁾

- [Self-Service-Password-Management \(SSPM\)](#)  53

3.2.2.4.8.1 Self-Service Password Management (SSPM)

Dem GINA-Benutzer steht die Möglichkeit zum eigenständigen Zurücksetzen seines Passwortes zur Verfügung (Abbildung 6).

The screenshot shows the SEPPMAIL login interface. At the top, there is a navigation bar with the SEPPMAIL logo, links for 'Anmelden', 'Registrierung', and 'Suchen', and a language selector 'Sprache'. The main heading is 'Nutzeranmeldung'. Below this, there are two input fields: 'E-Mail:' and 'Passwort:'. To the right of the 'Passwort:' field, there is a red-bordered button labeled 'Passwort vergessen?'. Below the input fields, there is a green button labeled 'Anmelden'. At the bottom of the page, it says 'Powered by SEPPmail'.

Abbildung 6

Hierfür stehen mehrere Varianten bereit, welche vom SEPPmail Appliance-Betreiber festgelegt werden:

- Auslösen eines Calls beim Administrator oder HelpDesk, welcher dem GINA-Benutzer sein neues Passwort mitteilt.
- Über SSPM. Dabei wird das Passwort vollautomatisiert - das heißt **ohne jegliche HelpDesk Aufwände** - wahlweise per SMS oder Passwort-Reset-E-Mail an den GINA-Mail Empfänger gestellt. Beim darauf folgenden Anmelden wird der GINA-Mail Empfänger zur Neuvergabe eines eigenen Passwortes aufgefordert.

Ob der jeweilige Rücksetzungsprozess zusätzlich durch eine Sicherheitsfrage abgesichert wird, kann vom Betreiber der SEPPmail Appliance festgelegt werden. Für diesen Fall muss der GINA-Mail Empfänger beim Registrieren Sicherheitsfrage und -antwort hinterlegen (siehe **Empfänger – Anmelden und einmaliges Registrieren**³⁷) sowie Abbildung 6a).

The screenshot shows a security question form. It has two main sections. The first section is labeled '* Sicherheitsfrage:' and contains two input fields: 'Zu welcher Tageszeit wurden Sie geboren?' and 'Geben Sie eine Sicherheitsfrage ein oder wählen Sie:'. The second section is labeled '* Antwort:' and contains one input field with the text 'Nacht'.

Abbildung 6a

Der Passwort-Reset-Prozess würde nach dem korrekten Beantworten dieser Sicherheitsabfrage (Abbildung 6b) durch den GINA-Benutzer starten.

Abbildung 6b

Im Detail stehen folgende Reset Optionen zur Verfügung:

Reset by hotline (Standardeinstellung)

- Der Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können.
- Der Benutzer wird aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben.

Reset by hotline, no reminder question/answer

- Der Benutzer wird aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben.
- **Dies funktioniert jedoch nur, wenn die GINA-Oberfläche über eine GINA-E-Mail aufgerufen wurde, also nicht durch die bloße Anmeldung.**

Reset by SMS

- Der Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können.
- Wurde beim Registrieren eine Handynummer für den SMS Reset eingegeben, so wird diese angezeigt. Mit Klicken der Schaltfläche „Senden“ wird der SMS-Passwort-Versand ausgelöst.
- Steht keine Handynummer zur Verfügung, so wird der Benutzer aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben.

Reset by SMS, no reminder question/answer

- Wurde beim Registrieren eine Handynummer für den SMS Reset eingegeben, so wird diese angezeigt. Mit Klicken der Schaltfläche „Senden“ wird der SMS-Passwort-Versand ausgelöst.
- Steht keine Handynummer zur Verfügung, so wird der Benutzer aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben.
- **Dies funktioniert jedoch nur, wenn die GINA-Oberfläche über eine GINA-E-Mail aufgerufen wurde, also nicht durch die bloße Anmeldung.**

Let user choose between hotline and SMS

- Der Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können.

- Wurde beim Registrieren eine Handynummer für den SMS Reset eingegeben, so erscheint eine Auswahl, in welcher der Benutzer zwischen seiner Handynummer (für SMS Reset) und einer einzugebenden Telefonnummer (voreingetragen ist die Handynummer) wählen kann.
- Steht keine Handynummer zur Verfügung, so wird der Benutzer aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben.

Let user choose between hotline and SMS, no reminder question/answer

- Wurde beim Registrieren eine Handynummer für den SMS Reset eingegeben, so erscheint eine Auswahl, in welcher der Benutzer zwischen seiner Handynummer (für SMS Reset) und einer einzugebenden Telefonnummer (voreingetragen ist die Handynummer) wählen kann.
- Steht keine Handynummer zur Verfügung, so wird der Benutzer aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben.
- **Dies funktioniert jedoch nur, wenn die GINA-Oberfläche über eine GINA-E-Mail aufgerufen wurde, also nicht durch die bloße Anmeldung.**

Reset by E-Mail verification

Da diese Variante allein auf dem Medium E-Mail basiert bedeutet dies einen gewissen Einschnitt in die Sicherheit. Aus diesem Grund ist diese Variante von SEPPmail Appliance nur bedingt empfohlen.

- Der Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können.
- Daraufhin wird der Benutzer aufgefordert ein neues Passwort einzugeben und dieses zu verifizieren.
- Der Benutzer erhält daraufhin eine E-Mail mit einem Link zugesendet. Erst durch Aufruf dieses Links erhält das neu vergebene Passwort seine Gültigkeit.

Reset by E-Mail verification, no reminder question/answer

Bereits das alleinige Basieren dieser Variante auf dem Medium E-Mail bedeutet einen gewissen Einschnitt in die Sicherheit (siehe oben).

Weiterhin ist jedoch in dieser Einstellung bereits der Besitz einer GINA-E-Mail ausreichend um das Passwort zurücksetzen zu können. Ein zweiter Faktor Wissen, also die Antwort auf eine Sicherheitsabfrage ist nicht erforderlich. Dies bedeutet einen weiteren Einschnitt in die Sicherheit. Aus diesem Grund ist diese Variante von SEPPmail absolut nicht empfohlen.

- Der Benutzer wird ohne Sicherheitsfrage aufgefordert ein neues Passwort einzugeben und dieses zu verifizieren.
- Der Benutzer erhält daraufhin eine E-Mail mit einem Link zugesendet. Erst durch Aufruf dieses Links erhält das neu vergebene Passwort seine Gültigkeit.
- **Dies funktioniert jedoch nur, wenn die GINA-Oberfläche über eine GINA-E-Mail aufgerufen wurde, also nicht durch die bloße Anmeldung.**

Disable user profile and password management

Diese Einstellung unterbindet das Anlegen eines Profils. Ein Passwort Reset ist nicht möglich. Das Anmelden an der GINA-Oberfläche ist nur durch den Aufruf eines GINA-Anhangs (secure-email.html) möglich. In der Regel kommt diese Einstellung nur bei maschinell generierten GINA Accounts zum Einsatz.

Als Absender von Passwort E-Mails fungiert im Standard die für die jeweilige GINA-Domain eingetragene „Admin E-Mail“ Adresse. Ebenso werden Passwort Reset Anfragen im Normalfall an diese Adresse gesendet. Das heißt an dieser Stelle sollte eine HelpDesk Sammeladresse eingetragen werden.

Steht kein HelpDesk zur Verfügung kann wahlweise auch der Absender, beziehungsweise der initiale Absender der GINA-Mail benachrichtigt werden.

Da sämtliche Texte des Passwort Reset Prozesses ebenfalls anpassbar sind, kann bei Bedarf an geeigneter Stelle zusätzlich eine HelpDesk Telefonnummer mit aufgenommen werden.

3.2.2.4.8.2 (optional) Initiales Schreiben von Nachrichten

Wurde vom Betreiber der SEPPmail Appliance das initiale Schreiben von E-Mails freigegeben, so kann ein GINA-Benutzer nicht nur auf erhaltene Nachrichten antworten, sondern auch initial E-Mails verfassen (Abbildung 4c). Dabei ist zu beachten, dass der Empfänger einer der von der SEPPmail Appliance verwalteten E-Mail Domänen angehören muss!

The screenshot shows the SEPPmail web interface for composing a new email. The top navigation bar includes the SEPPMAIL logo, links for 'E-Mail lesen', 'E-Mail schreiben' (highlighted with a red arrow), 'Suchen', the user email 'max.mustermann@private-adresse.tld', and a 'Abmelden' link. The main heading is 'Sichere E-Mail'. Below it is a green button labeled 'Nachricht senden'. The form fields are as follows:

- Von:** Max Mustermann <max.mustermann@private-adresse.tld>
- An:** A dropdown menu with the text 'Klicken Sie, um eine Empfängeradresse auszuwählen' and a downward arrow. Below it is an empty input field with a green plus icon to its right.
- Cc:** A dropdown menu with the text 'Klicken Sie, um eine Empfängeradresse auszuwählen' and a downward arrow. Below it is an empty input field with a green plus icon to its right.
- Betreff:** An empty text input field.
- Anhänge:** An empty text input field with a 'Datei anhängen' button (represented by a paperclip icon) to its right.

Below the attachment field, there is a blue information icon and the text 'Maximalgrösse der Anhänge: 1313.7 MiB'. The 'Nachricht:' label is to the left of a large, empty text area for the email body. At the bottom of the form, there is a checked checkbox labeled 'Kopie an mich selbst senden' and a small note: 'Wenn Sie diese Option nicht setzen, wird Ihre Antwort nicht auf Ihrem lokalen System verfügbar sein.' A second green 'Nachricht senden' button is located at the bottom left of the form area. The footer of the interface says 'Powered by SEPPmail'.

Abbildung 4c

3.2.2.4.8.3 (optional) Schlüsselverwaltung

Ist vom Betreiber der SEPPmail Appliance die Schlüsselverwaltung für GINA-Benutzer freigeschaltet, so können diese über die gleichnamige Schaltfläche eigenes Schlüsselmaterial (S/MIME Zertifikat - gegebenenfalls auch selbst signiert - oder OpenPGP public key) auf die SEPPmail Appliance hochladen (Abbildung 5c).

Aufgrund des vorangegangenen Authentisierens über GINA, kann dem so auf die Appliance eingebrachten Schlüsselmaterial sofort vertraut werden. Ein Validieren durch den Administrator ist an dieser Stelle nicht notwendig! Bereits mit dem nächsten Verschlüsselungsvorgang an diesen Benutzer würde die SEPPmail Appliance somit dieses Schlüsselmaterial anstatt der GINA-Technologie verwenden, sofern diese nicht explizit angefordert wurde.

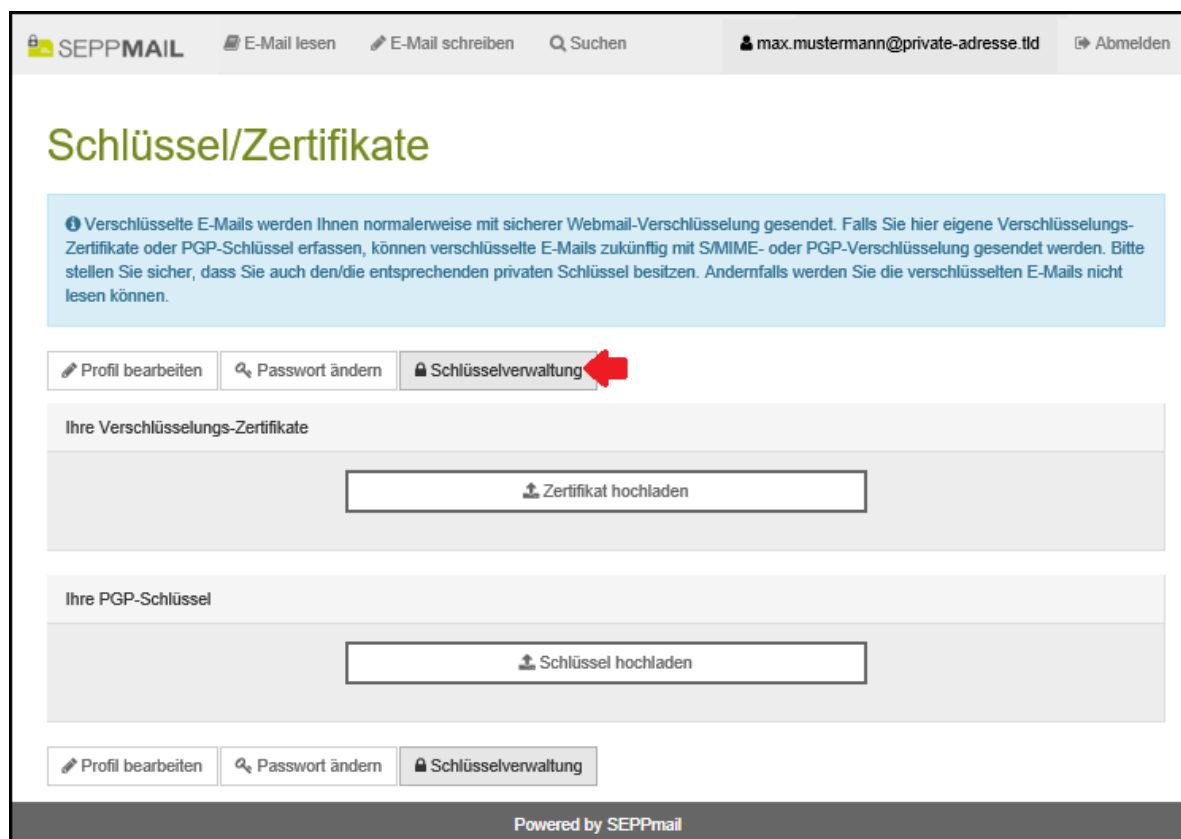


Abbildung 5c

3.2.2.4.8.4 (optional) Selbstlöschung

Sofern dies vom Betreiber der SEPPmail Appliance freigeschaltet ist, kann ein GINA-Benutzer seinen eigenen Account auch löschen.

Hierzu klickt er auf „Profil löschen“ (siehe Abbildung 5e)

SEPPMAIL E-Mail lesen E-Mail schreiben Suchen max.mustermann@private-adresse.tld Abmelden

Profil bearbeiten

Profil bearbeiten Passwort ändern Schlüsselverwaltung

E-Mail-Adresse: max.mustermann@private-adresse.tld

Voller Name: Max Mustermann

Sprache: Deutsch ▼

Handynummer: 0041791234567

Bitte geben Sie die Telefonnummer im internationalen Format (z.B. 0041123456789) ein.

Speichern Profil löschen

Profil bearbeiten Passwort ändern Schlüsselverwaltung

Powered by SEPPmail

Abbildung 5e

Darauffin wird der GINA-Benutzer aufgefordert die zu seinem GINA-Account gehörige E-Mail Adresse zu bestätigen (Abbildung 5g).

Profil löschen

Wollen Sie Ihr Profil wirklich löschen?

Wenn Sie es löschen, können all Ihre bereits empfangenen E-Mails nicht mehr entschlüsselt werden.

Dieser Prozess kann nicht rückgängig gemacht werden.

Falls Sie Ihr Profil weiterhin löschen möchten, bestätigen Sie dies bitte durch die Eingabe ihrer E-Mail Adresse.

E-Mail-Adresse

Abbrechen Bestätigung

Abbildung 5g

Nach dem Bestätigen erscheint eine entsprechende Erfolgsmeldung (Abbildung 5f)

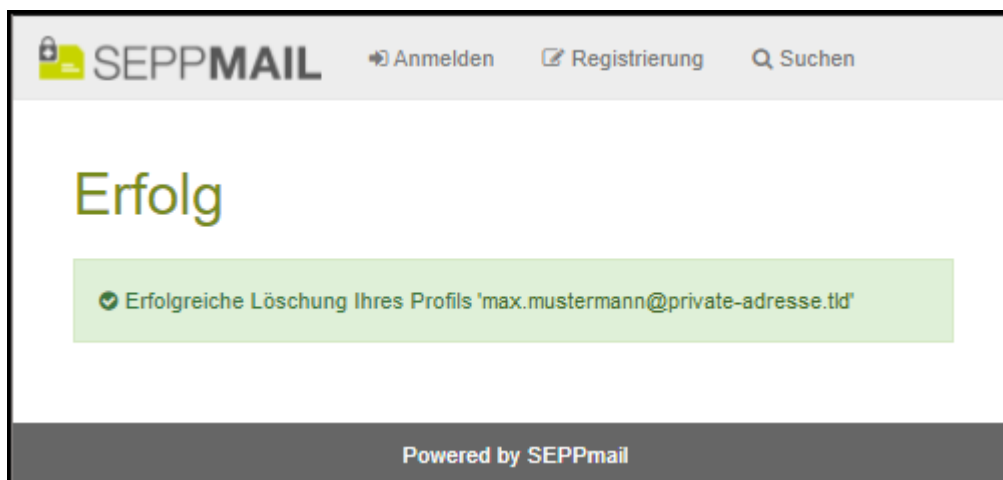


Abbildung 5f

3.2.2.4.9 (optional) Schlüsselsuche

Gibt der Betreiber der SEPPmail Appliance die Schlüsselsuche frei, so ist über die GINA-Oberfläche das Suchen von öffentlichen Schlüsseln der auf der SEPPmail Appliance vorhandenen, internen Benutzer möglich (Abbildung 5d). Ob diese Suche nur authentifizierten GINA-Benutzern oder generell jedem möglich ist, bestimmt der Betreiber der SEPPmail Appliance. Dem so erlangten Schlüsselmateriale kann in jedem Fall vertraut werden, da dieses aus sicherer Quelle stammt und über einen sicheren Kanal (https) heruntergeladen wird.

Abbildung 7

Weiterhin kann optional die Anzeige, beziehungsweise der Download der auf der SEPPmail Appliance vorhandenen öffentlichen Domänenschlüssel (Schaltfläche „Domain-Schlüssel“), sowie des Root-CA Zertifikates der SEPPmail Appliance internen CA - sofern diese aktiv ist - (Link „Zertifizierungsstelle“) freigeschaltet werden.

3.2.2.4.10 Administration und Management

Eine komplette Managementoberfläche für die Administration und das Management der **GINA-Accounts** ⁴⁶² ist integraler Bestandteil der Lösung. Auf diese Oberfläche ist ein rollenbasierter (Helpdesk) Zugriff möglich.

3.2.2.5 Mobile Computing Support

3.2.2.5.1 Interne Nutzer von mobilen Endgeräten

Grundsätzlich sollte innerhalb des internen Netzwerk den Geräten und Kommunikationswegen vertraut werden. Somit sind alle E-Mails im Intranet und am E-Mail Server im Klartext verfügbar. Mobile Endgeräte, welche an den internen E-Mail Server, zum Beispiel via ActiveSync, angebunden sind, kommunizieren somit über den Standard E-Mail Weg. Nachdem sich die SEPPmail Appliance zwischen E-Mail Server und Internet befindet, durchlaufen deshalb auch E-Mails mobiler Endgeräte die SEPPmail Appliance und werden somit dort verarbeitet.

Nachdem die SEPPmail Appliance **Betreffzeilen-Schlüsselwörter** verarbeiten kann, können auch an mobilen Endgeräten verfasste E-Mails - herstellerunabhängig - entsprechend klassifiziert werden. Um das Eingeben dieser Schlüsselwörter am mobilen Endgerät komfortabler zu gestalten, können zusätzlich zu den Standardschlüsselwörtern auch weitere, unternehmensweite Schlüsselwörter definiert werden. So wäre beispielsweise das Verwenden des selbstdefinierten Schlüsselwortes <c> zusätzlich zum Standardschlüsselwort [confidential] für das Verschlüsseln denkbar.

Für die Standard E-Mail Clients von iOS, Android und Windows Phone sind derzeit keine integralen Funktionen für das Klassifizieren von E-Mails bekannt. Sollten solche in zukünftigen Versionen implementiert werden, wird SEPPmail auch diese für das Ansteuern der eigenen Lösung nutzen.

3.2.2.5.2 Externe Empfänger von verschlüsselten E-Mails auf mobilen Endgeräten

Hersteller / Betriebssystem	Zertifikats-Unterstützung durch Vendor gegeben	Bemerkung
Android	ja	Eine Anleitung für das Importieren beziehungsweise Installieren von Zertifikaten ist gegebenenfalls der Dokumentation des Herstellers zu entnehmen.
Windows Phone	?	Keine Dokumentation im Netz vorhanden
Blackberry 10 und höher	ja / nein	Blackberry hat nach Auskunft des Supports bei signierten und verschlüsselten ein grundsätzliches Problem. Ein Zeithorizont für das Beheben dieses Problems ist derzeit nicht bekannt. Das Fehlverhalten von zum Beispiel signierten E-Mails auf BB Endgeräten ist unterschiedlich und nicht vorhersehbar. So kann beispielsweise bei einer Antwort auf eine signierte E-Mail vom BB Client der Antworttext beim Empfänger verschwinden.
iOS (Apple)	ja	Eine Anleitung für das Importieren beziehungsweise Installieren von Zertifikaten ist gegebenenfalls der Dokumentation des Herstellers zu entnehmen.

3.2.2.5.3 Kompatibilitätsmatrix für Empfänger von GINA-Web-Mails

Hersteller / Betriebssystem	Unterstützung	Bemerkung
Android	nativ	mit vollwertigem Browser zum Beispiel Chrome oder Firefox Alternativ steht über den Google Play Store die SEPPmail Reader App (https://play.google.com/store/apps/details?id=com.seppmail.reader&gl=DE) bereit, welche den Benutzerkomfort deutlich erhöht. Hierzu finden Sie in unseren YouTube Channel ein entsprechendes Erklärvideo .
Windows Phone	nativ	
Blackberry 10 und höher	nativ	Für frühere Betriebssystem Versionen kann eine App bereit gestellt werden.
iOS (Apple)	nativ	ab iOS 11 nativ. Alternativ steht über den iTunes Store die SEPPmail Reader App (https://apps.apple.com/de/app/seppmail-reader/id1565769384) bereit, welche den Benutzerkomfort deutlich erhöht. Hierzu finden Sie in unseren YouTube Channel ein entsprechendes Erklärvideo .

3.2.2.6 TLS

Die SEPPmail Appliance nutzt im Normalfall „opportunistisches TLS“. Somit wird immer dann TLS genutzt, wenn der gegenüberliegenden E-Mail Server beziehungsweise MTA (Mail Transfer Agent) dies anbietet. Dabei wird jeweils der maximal möglich Verschlüsselungsgrad angewendet. TLS stellt eine, im Normalfall zusätzliche, Verschlüsselung des Transportweges dar.

Soll TLS erzwungen werden, so steht in der SEPPmail Appliance die Möglichkeit des Verwaltens einzelner Ziele - E-Mail Domänen und/oder E-Mail Server - bereit. Dabei kann zwischen den für Postfix typischen Stufen gewählt werden.

- (none) Keine TLS-Verschlüsselung
- may (Standard) Opportunistisch
- encrypt E-Mails werden nur versendet, falls der Versand mittels TLS-Verschlüsselung möglich ist.
- verify E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich, und das SSL Zertifikat des empfangenden E-Mail Servers gültig ist.
- secure E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich, das SSL Zertifikat des empfangenden E-Mail Servers gültig, der FQDN des E-Mail Servers identisch mit dem im Zertifikat (Antragsteller) eingetragenen Namen (CN) und der Name der E-Mail Domäne identisch mit dem Domänen Namen des E-Mail Servers ist.
- fingerprint E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich ist und das SSL Zertifikat des empfangenden E-Mail Servers dem eingetragenen Fingerprint entspricht.

TLS „gezielt“ als Ersatz für eine Verschlüsselung von E-Mails zu verwenden, ist jedoch nicht zu empfehlen. Dies hat folgende Gründe:

- TLS kann immer nur bis zum nächsten MTA gewährleistet werden. Ob und wie ab diesem MTA weiter verschlüsselt wird, ist für den Absender nicht ersichtlich.
Da immer mehr Firmen Cloud-Dienste für das Filtern von Spam E-Mails verwenden, reicht diese Art des Verschlüsseln in der Regel nicht aus.
- Als tatsächlich sicher sind nur die Stufen „Fingerprint“ oder „DANE“ zu betrachten. Alle anderen Sicherheitsstufen können beispielsweise durch DNS Spoofing - ausgehebelt werden.
- Das Verwalten von TLS Strecken erzeugt hohen Administrationsaufwand

Da TLS als „kleinster gemeinsamer Nenner“ auf praktisch jedem MTA verfügbar ist, kommt diese Art des Verschlüsseln relativ häufig - insbesondere in der Punkt zu Punkt Kommunikation zwischen Unternehmen - zum Einsatz.

Auch diese Verschlüsselungstechnologie ist Bestandteil der SEPPmail Appliance Grundlizenz und muss nicht per User lizenziert werden.

3.2.3 Verschlüsselungshierarchie



Durch die von der SEPPmail Appliance bereit gestellten kryptographischen Technologien und Verfahren ist höchste Sicherheit und Flexibilität in der abgesicherten Kommunikation mit den unterschiedlichen Kommunikationspartnern gewährleistet.

So werden jeweils ausgehende E-Mails mit dem für den Kommunikationspartner am besten geeigneten Verfahren abgesichert. Dabei geht die SEPPmail Appliance im Standard nach folgender Wertigkeit vor:

1. Geprüftes S/MIME Zertifikat des Empfängers
2. Geprüfter öffentlicher OpenPGP Schlüssel des Empfängers
3. Geprüftes S/MIME Domänen Zertifikat der Empfänger Domäne
4. Geprüfter öffentlicher OpenPGP Domänen Schlüssel der Empfänger Domäne
5. *Optional kann eine TLS-Verschlüsselung höher „may“ an dieser Stelle als gültiges Verschlüsselungsverfahren eingebunden werden - wobei diese auch zusätzlich verwendet wird, wenn bereits eines der höher priorisierten Verfahren zum Einsatz kam.*

Sollte aufgrund fehlenden Schlüsselmaterials des Empfängers keines der vorangegangenen (Standard-)Verfahren verfügbar sein, so wird

6. GINA mit hinterlegtem Empfängerpasswort
7. GINA mit Initialpasswort



Hinweis:

Die Verschlüsselungsverfahren der Punkte 3. bis 5. kommen im Normalfall auch bei nicht als zu verschlüsselnd markierten E-Mails zum Einsatz, sofern diese Verfahren verfügbar sind.

Eine gesondertes Lizenzieren ist hierfür nicht erforderlich (siehe [Gateway-to-Gateway \(Domänen Verschlüsselung](#) ^[31] und [TLS](#) ^[65]).

Standard Verschlüsselungsmerkmale für ausgehende E-Mails sind [Betreffzeilen Schlüsselwörter](#) ^[99], Sensitivity Parameter (Vertraulichkeitsmarkierung, siehe auch [Microsoft Outlook Vertraulichkeit](#) ^[100]) sowie spezielle [X-Header](#) ^[100]. Optional können auch zum Beispiel LDAP Abfragen als Merkmale herangezogen werden, wie etwa Microsoft Active Directory (AD) Benutzergruppen.

Sollte eine andere Reihenfolge, oder ein anderer Vorgang gewünscht sein, kann das Ruleset jederzeit entsprechend angepasst werden. Somit können gewünschte Standardisierungen im Umgang mit E-Mails von und an bestimmte Adressen oder Domänen so voreingestellt werden, dass diese Regelungen unabhängig von den Nutzeraktionen Vorrang haben.

Für den abgesicherten Empfang von E-Mails kann dem Kommunikationspartner jeweils ein beliebiges Standardverfahren oder GINA für die Spontankommunikation angeboten werden.

Diese Arten der abgesicherten Kommunikation sind für den internen Benutzer in jedem Falle transparent.

Weiterhin können eingehende E-Mail mit einer digitalen Signatur (siehe auch [Elektronische Signaturen](#) ^[68]) versehen sein. Bestandteil einer S/MIME Signatur ist der öffentliche S/MIME Schlüssel (Zertifikat) des Absenders. Um den Verwaltungsaufwand zu minimieren, speichert die SEPPmail Appliance diese S/MIME Zertifikate nach erfolgreichem Prüfen der Signatur automatisch. Dadurch stehen die so eingesammelten Zertifikate im Anschluss unternehmensweit für das Verschlüsseln von E-Mails an die entsprechenden Kommunikationspartner bereit.

Für den Funktionsablauf der Verschlüsselungshierarchie finden Sie in unseren [YouTube Channel](#) ein entsprechendes [Erklärvideo](#).

3.2.4 LDAP Key-Lookup für S/MIME und OpenPGP

Für den automatisierten Bezug öffentlicher Schlüssel gegebenenfalls noch unbekannter Empfänger aus externen Quellen, steht auf der SEPPmail Appliance weiterhin eine LDAP Lookup Funktion bereit. Beim Erfassen von sogenannten Schlüssel-Servern (Key Server) ist allerdings auf deren Qualität zu achten. Häufig wird über „öffentliche“ Key Server „totes“ Schlüsselmaterial verbreitet. Verwendet der Absender dieses Material, so kann der Empfänger die damit verschlüsselte E-Mail unter Umständen - mangels privatem Schlüssel - nicht lesen.

Umgekehrt kann in der SEPPmail Appliance die Key Server Funktionalität aktiviert werden, um externen Kommunikationspartnern über diesen Weg die Zertifikate der internen Benutzer zur Verfügung zu stellen.

3.2.5 Elektronische Signaturen



Die SEPPmail Appliance beherrscht neben dem Verschlüsseln von E-Mails auch das RFC konforme Signieren. Mit dem Signieren werden die Authentizität des Absenders und die Integrität der Daten in einer E-Mail gewährleistet. Zusätzlich wird mit der Signatur der öffentliche Schlüssel des Absenders verbreitet. Damit werden die Kommunikationspartner in die Lage versetzt, zukünftig verschlüsselt mit dem Signierenden zu kommunizieren.

Das für die Signatur erforderliche Benutzerzertifikat (siehe auch [S/MIME \(X.509\)](#) ^[28]) kann bei Bedarf

- von einer akkreditierten CA über die in der SEPPmail Appliance integrierten Schnittstelle (siehe [Managed PKI](#) ^[29]) automatisch durch die Appliance bezogen
- von der lokal auf der SEPPmail Appliance vorhandenen CA ausgestellt
- manuell - einzeln oder als Bulk-Import - für die jeweiligen Benutzer importiert

werden. Die dazu erforderlichen zentralen Funktionalitäten sind in der SEPPmail Appliance per Standard vorhanden und werden dem Betreiber mit der Verschlüsselungslizenz bereit gestellt.

Automatische Signatur

Ausgehenden E-Mails können durch die SEPPmail Appliance automatisch im Namen des Senders signiert werden. Der Benutzerkreis, für welchen dies gegebenenfalls erfolgen soll, kann bei Bedarf über das Ruleset gesteuert werden.

Manuelle Signatur

Das Signieren von E-Mails durch die SEPPmail Appliance kann auch über die bereits von der Verschlüsselung bekannten Steuerfunktionen ([Steuern der Appliance](#) ^[99]) manuell forciert werden.

Digitale E-Mail Signatur mit einem Firmenzertifikat

Das Signieren von E-Mails mit einem S/MIME-Firmenzertifikat erfüllt auf Unternehmensebene denselben Zweck wie das Signieren mit einem S/MIME-Benutzerzertifikat auf Personenebene. Bei dieser Variante wird nur ein einziges Zertifikat für das Unternehmen benötigt. Da S/MIME-Zertifikate grundsätzlich jedoch nur für eine E-Mail Absenderadresse gültig sind, erhalten alle ausgehenden E-Mails den gleichen (technischen) Absender. Das heißt alle E-Mails des Unternehmens - egal wer im

Unternehmen der Absender ist - erscheinen beim Empfänger mit derselben E-Mail Adresse.

Daraus resultieren einige Probleme:

- Zwar wird beim Empfänger der korrekte (Absender-) Benutzername angezeigt, jedoch wird bei Erfassen des Kontaktes im jeweiligen E-Mail Client unter dem Namen des tatsächlichen Absenders die E-Mail Adresse des technischen Absenders (siehe oben) gespeichert. Beim späteren Verwenden dieses Kontaktes würde als fälschlicherweise die zentrale Absenderadresse aus dem Unternehmenszertifikat adressiert!
- Aufgrund der Häufigkeit des Verwendens dieser einen Absenderadresse besteht eine hohe Wahrscheinlichkeit, dass diese fälschlicherweise als SPAM eingestuft wird. Das hätte im ungünstigsten Fall, dass alle ausgehenden E-Mails des Unternehmens von den Empfängern abgewiesen werden!
- Non Delivery Reports (NDR), also Informations-E-Mails über die Nicht-Zustellbarkeit einer E-Mail, werden generell nicht mehr an den ursprünglichen, sondern an den technischen Absender gesendet. Der eigentliche Absender erhält somit keine Information darüber, wenn seine gesendete E-Mail nicht zugestellt werden konnte!

Fazit:

Diese Art der Signatur ist im produktiven Umfeld absolut nicht zu empfehlen, da über kurz oder lang massive Support Aufwände generiert werden!

Validieren von Signaturen

Die Information ob eine E-Mail signiert ist und zu welchem Ergebnis das Prüfen einer Signatur führte, wird von der SEPPmail Appliance durch ein Kennzeichen im Betreff der E-Mail angezeigt. Im Standard lauten diese Kennzeichen:

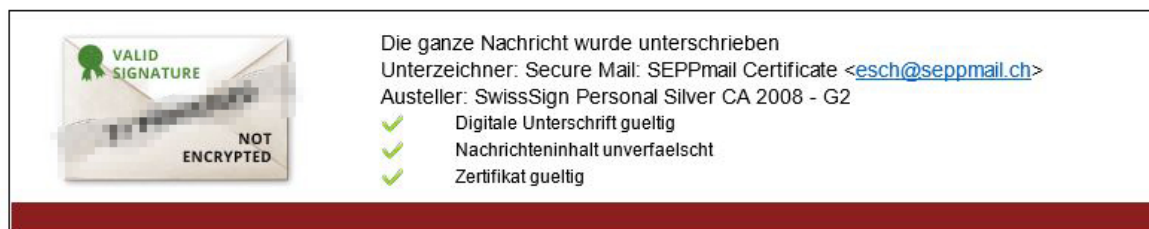
[signed OK] für gültige Signaturen

**[signed
INVALID]** für ungültige Signaturen

Sollte eine aus dem Internet kommende E-Mail bereits über ein entsprechendes Kennzeichen verfügen, so wird dieses noch vor dem Überprüfen der Signatur durch die SEPPmail Appliance entfernt. Somit ist gegebenenfalls das Vortäuschen einer gar nicht vorhandenen gültigen Signatur unmöglich. Der Empfänger bekommt in jedem Fall das korrekte Prüfergebnis angezeigt!

Weiterhin kann der Betreiber der SEPPmail Appliance entscheiden, ob Signaturen nach dem Prüfen und dem damit einhergehenden Kennzeichen im Betreff entfernt oder an der E-Mail belassen werden. Das Entfernen von Signaturen nach erfolgreichem Prüfen kann dabei durchaus sinnvoll sein. So werden dadurch unterschiedlich Ergebnisse beim doppelten Prüfen, an der SEPPmail Appliance und am E-Mail Client, zum Beispiel durch unterschiedliche Vertrauensstellungen oder Fehlen von CA-Zertifikaten, vermieden. Ein weiterer Grund für das Entfernen können mobile Endgeräte sein, welche häufig Probleme im Umgang mit signierten E-Mails haben. So wird meist versucht, beim Antworten direkt am Client zu signieren. Die muss jedoch aufgrund der in der Regel nicht vorhandenen Signaturzertifikate scheitern.

Wie kritisch der Umgang mit Signaturnachrichten an den Empfänger betrachtet werden sollte, zeigt folgendes Beispiel. Eine sichere E-Mail Gateway Appliance erzeugt folgenden E-Mail Footer beim Prüfen der Signatur:



Vordergründig scheint diese Art des Hinweises zu eine E-Mail Signatur sehr informativ:

- E-Mail ist originär
- E-Mail ist unverfälscht
- Zertifikat ist gültig

Aber!

Ein Angreifer könnte diese Fußnote ebenso an seine unsignierte E-Mail anfügen und so eine gefälschte E-Mail von außen einschleusen. Das Gateway, welches dieses Verfahren für das Markieren signierter E-Mails verwendet, könnte diese Fälschung nicht erkennen. Dem Empfänger dieser E-Mail würde somit eine gültige Signatur vorgegaukelt.

3.2.6 Remote-Administration mittels Web-Portal

Sämtliche Verwaltungsmöglichkeiten der SEPPmail Appliance stehen über eine Webbrowser basierte Konfigurationsoberfläche zur Verfügung. Das Verbinden zur Administrationsoberfläche der SEPPmail Appliance erfolgt selbstverständlich SSL verschlüsselt (HTTPS).

3.2.7 SEPPmail Microsoft Outlook Add-In



SEPPmail stellt für Microsoft Outlook kostenfrei Add-Ins bereit, durch welche die jeweils gewünschte kryptographische Aktion durch den Benutzer bequem angefordert werden kann.

Nachdem sich die Technologien bei Outlook 365 und Exchange / Outlook on premises Installationen unterscheiden, wurden für das Office 365 Umfeld folgende, sogenannte Cross-Platform-Add-Ins entwickelt:

-  Verschlüsseln
-  Verschlüsseln mit Lesebestätigung (GINA)
-  Unverschlüsselt

Für Exchange / Outlook on premises Installationen steht ein einzelnes, sogenanntes COM-Add-In bereit. Da Microsoft für die on premises Version einen erweiterten Funktionsumfang bietet, konnten mit dem COM-Add-In weitere, zusätzliche Funktionen realisiert werden:

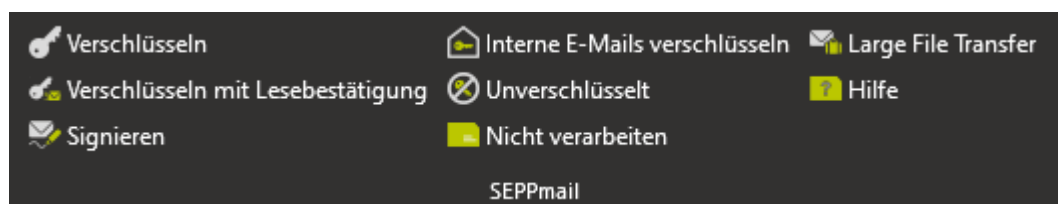


Abb1. COM-Add-In

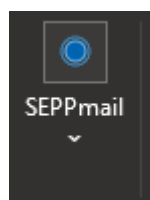


Abb2. COM-Add-In minimiert

Bei allen Add-In Versionen wurde explizit darauf geachtet, diese möglichst einfach zu halten. Eine direkte Kommunikation zwischen Add-Ins und SEPPmail Appliance ist dabei nicht notwendig.

3.2.8 Kompatibilität zu anderen Secure E-Mail Systemen

Aufgrund des Verwendens genormter Techniken und Protokolle, lässt sich die SEPPmail Appliance transparent in jede E-Mail Infrastruktur integrieren. Alle anerkannten und sicheren Standard-Verschlüsselungstechniken sind implementiert. Die Kompatibilität zu den gängigen E-Mail Systemen ist damit sichergestellt und die Installation zusätzlicher Softwarekomponenten entfällt.

Für Empfänger, über keine der Standardtechnologien oder entsprechendes Schlüsselmaterial verfügen, steht die **GINA-Technologie** ³²⁾ für das sichere Übertragen von E-Mails auf der SEPPmail Appliance bereit.

3.2.9 Kompatibilität zu diversen Regularien

3.2.9.1 Regelung zum sicheren Austausch von EDIFACT Übertragungsdateien

(Stand 03/2019)

Von Bundesverband der Energie- und Wasserwirtschaft wird ein Konzeptpapier bezüglich der "Regelung zum Übertragungsweg" jeweils als "Konsolidierte Lesefassung mit Fehlerkorrekturen ausgegeben. Das jeweils aktuelle Dokument kann unter www.edi-energy.de/index.php?id=38 heruntergeladen werden.

Da dieses Dokument in der Vergangenheit zum Teil in verschiedenen Ständen mit der gleichen Versionsnummer publiziert wurde, stellen wir den Link zum Dokument, auf welches sich dieses Kapitel bezieht direkt bereit:

EDI@Energy – Regelungen zum Übertragungsweg

Regelungen zum sicheren Austausch von EDIFACT Übertragungsdateien

Konsultationsfassung

Version:	1.2
Ursprüngliches Publikationsdatum:	01.08.2018
Anzuwenden ab:	01.04.2019
Autor:	BDEW

www.bundesnetzagentur.de/DE/Service-Funktionen/Beschlusskammern/BK06/BK6_81_GPKE_GeLi/Mitteilung_Nr_61/Anlagen/Regelungen_Uebertragungsweg_1.2.pdf?__blob=publicationFile&v=1

Zweck des Dokumentes ist

Zitat:

Dieses Dokument regelt die Sicherheits- und Schutzmechanismen, die im Rahmen des elektronischen Datenaustauschs zwischen den Marktteilnehmern der deutschen Energiewirtschaft für die Übertragungswege AS2 und E-Mail via SMTP in der aktuellen Prozesswelt und im sogenannten Interimsmodell und zu den bereits etablierten Dateiaustauschprozessen in der Marktkommunikation einzuhalten sind. Es wird keine Aussage über die im Zielmodell geltenden Anforderungen an die Übertragungswege getroffen.

SEPPmail nimmt auf Basis des oben genannten Dokumentes, sowie den in diesem Dokument ebenfalls genannten Dokumenten Stellung zu den Punkten, die nicht organisatorischer Natur sind, sondern explizit die in der SEPPmail Appliance bereitgestellten Technologien für die sichere E-Mail Kommunikation betreffen.

Dabei ist festzustellen, dass die SEPPmail Appliance generell alle Konformitätsanforderungen in dieser Hinsicht erfüllt:

- Gesetz zur Digitalisierung der Energiewende (BGBl. I, S. 2034) (GDEW)
- Beschluss BK6-16-200, insbesondere Tenorziffer 5 und BK6-16-200-142 der Bundesnetzagentur
- Verschlüsselung der Marktkommunikation nach Vorgaben des § 75 Abs. 1 i.V.m. § 52 Abs. 1 Messstellenbetriebsgesetz (MsbG).
- Elektronische Marktkommunikation im deutschen Strommarkt nach den Festlegungen
- Geschäftsprozesse zur Kundenbelieferung mit Elektrizität (GPKE)
- Marktprozesse für Erzeugungsanlagen (Strom) (MPES)
- Wechselprozesse im Messwesen (WiM)
- Marktprozesse für die Bilanzkreisabrechnung Strom (MaBiS)
- Technische Richtlinie TR 03116-4 des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT)

Unabhängig davon, kann die SEPPmail Appliance auch Verstöße gegen organisatorische Regelungen zum Übertragungsweg in einer E-Mail erkennen und gegebenenfalls entsprechende Maßnahmen einleiten, wie zum Beispiel

- Benachrichtigen eines zu definierenden E-Mail Empfängers.

- Umleiten der E-Mail in ein zu definierendes E-Mail Postfach (ähnlich einer Quarantäne).
- Abweisen der E-Mail
- und vieles mehr

Nachdem die EDIFACT Konformität bereits durch die E-Mail generierenden Instanzen gewährleistet werden muss, ist dieses zusätzliche Prüfen im Normalfall jedoch nicht notwendig.

Die geänderten Anforderungen aus dem Dokument

Version:	1.3
Ursprüngliches Publikationsdatum:	01.04.2020
Anzuwenden ab:	01.10.2020
Autor:	BDEW

www.edi-energy.de/index.php?id=38&tx_bdew_bdew%5Buid%5D=953&tx_bdew_bdew%5Baction%5D=download&tx_bdew_bdew%5Bcontroller%5D=Dokument&cHash=80debae27afd94199b70243485bfa11f

werden zeitnah umgesetzt, sobald entsprechende Tools für das Umsetzen der geforderten Standards verfügbar sind.

3.2.9.2 Verordnung zur Schaffung barrierefreier Informationstechnik (BITV 2.0)

Die von der SEPPmail Appliance für Endbenutzer bereit gestellten Portale wurden in der Schweiz nach dem europäischen Standard zur barrierefreien Gestaltung von Internetseiten WCAG 2.0 geprüft. Somit wird auch die Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (BITV 2.0) erfüllt.

3.3 Aufbau und Architektur

3.3.1 Appliance

SEPPmail stellt die Appliance sowohl in als hochstabile Industrie-Hardware, wie auch als Image für virtualisierte Umgebungen bereit.

3.3.1.1 Hardware Modelle

- Bis maximal 500 Postfächer, beziehungsweise [Verschlüsselungs-/Signatur](#) ¹²⁷⁾ User.

	SEPPmail Standard	Dimensionen (HxBxT)	19" 1U short rack form factor (43 x 426 x 382 mm)
		Prozessoren	Intel Xeon E3-1220v5 Quad-Core 3.0GHz
		Speicher (RAM)	8 GB 1Rx8 PC4-2133P-E-15 STND
		Festplatte (HDD)	1 TB enterprise class SATA HDD
		Netzwerk Karte (NIC)	1GB Ethernet-Adapter
		Stromversorgung	290W FIO PSU

- Bis maximal 1000 Postfächer, beziehungsweise [Verschlüsselungs-/Signatur](#) ¹²⁷⁾ User.

	SEPPmail Business	Dimensionen (HxBxT)	19" 1U short rack form factor (43 x 426 x 382 mm)
		Prozessoren	Intel Xeon E3-1220v5 Quad-Core 3.0GHz
		Speicher (RAM)	16 GB 1Rx8 PC4-2133P-E-15 STND
		Festplatte (HDD)	1 TB enterprise class SATA HDD
		Netzwerk Karte (NIC)	1GB Ethernet-Adapter
		Stromversorgung	290W FIO PSU

- Bis maximal 5000 Postfächer, beziehungsweise [Verschlüsselungs-/Signatur](#) ¹²⁷⁾ User.

	SEPPmail Advanced	Dimensionen (HxBxT)	19" 1U rack form factor (43 x 426 x 707 mm)
		Prozessoren	Intel Xeon Silver 4112 Quad-Core 2.6GHz
		Speicher (RAM)	16GB 1Rx4 PC4-2933Y-R Smart Kit
		Festplatte (HDD)	2x 300 GB SAS 15K (RAID)
		Netzwerk Karte (NIC)	1GB 332i Ethernet-Adapter
		Stromversorgung	500W FS Plat

- Ab 5000 Postfächer, beziehungsweise [Verschlüsselungs-/Signatur](#) ¹²⁷⁾ User.

Die maximal mögliche Anzahl von Verschlüsselungs-/Signatur User, beziehungsweise Postfächer pro Maschine ist im Einzelfall zu prüfen. Durch die Kaskadierbarkeit des Systems ist die Anzahl der User frei skalierbar.

	SEPPmail Enterprise	Dimensionen (HxBxT)	19" 1U rack form factor (43 x 426 x 707 mm)
		Prozessoren	Intel Xeon Silver 4112 Quad-Core 2.6GHz
		Speicher (RAM)	32GB 1Rx4 PC4-2933Y-R Smart Kit
		Festplatte (HDD)	2x 300 GB SAS 15K (RAID)
		Netzwerk Karte (NIC)	1GB 332i Ethernet-Adapter
		Stromversorgung	500W FS Plat

Die angegebenen Empfehlungen für die Anzahl der Postfächer basieren auf Durchschnittswerten für E-Mail-Durchsatz und -Größen pro Postfach und können daher im Einzelfall stark abweichen (siehe auch [Sizing](#) ⁷⁸⁾).

3.3.1.2 Virtualisierte Versionen

Analog zu den [Hardware Modellen](#) ⁷⁶ stehen auch virtuelle Versionen der SEPPmail Appliance zur Verfügung. In der Hauptsache werden dabei zwei Formate unterschieden



Open Virtualization Format (OVF) für zum Beispiel

- ESX (VMware)
- HyperVisor (Virtual-Machine-Monitor, kurz VMM)
- KVM (Kernel-based Virtual Machine)
- QUEMU (Quick Emulator)
- Proxmox VE (Proxmox Virtual Environment; kurz PVE)
- Xen

Virtual Hard Disk (VHD / VHDX) für

- Hyper-V (Microsoft)

Die Systemanforderungen für die virtuellen Appliance-Größen sind ebenfalls im Kapitel [Sizing](#) ⁷⁸ aufgeführt.

3.3.2 Sizing

Unverbindliche Erfahrungswerte für das Dimensionieren der Lösung sowie dem Festlegen von System-Ressourcen für Virtualisierungs-Host-Systeme.

	Basic	Standard	Business	Advanced	Enterprise
Maximalanzahl Postfächer / User	50	500	1000	5000	unlimitiert ¹
Maildurchsatz pro Stunde ²	2500	10000	30000	60000	90000
Maximalgröße (MB) LFT bei Einliefern per SMTP (begrenzt durch Mailqueue)	500 Bei Einliefern per GINA begrenzt lediglich der verfügbare LFT Speicher				
	Spezifikationen Virtual Appliances³				
Speicher (RAM) in GB	4	6	8	12	18-32
	mindestens empfohlen				4
Anzahl Prozessorkerne	2	2	4	8	12-16
	mindestens empfohlen				4
Festplatte / System in GB	30				
Anzahl Netzwerk-Ports	1	1	1	1	1
	bis auf 4 erweiterbar				
Verfügbarer LFT Speicher in GB ⁵	abhängig von der Größe der zugewiesenen zusätzlichen virtuellen Disk / Partition (mind. 30GB)				
	Spezifikationen Hardware Appliances				
	Die Hardware Spezifikationen sind dem Kapitel Hardware Modelle ⁷⁶ zu entnehmen				
Verfügbarer LFT Speicher in GB ⁵	-	950	950	250	250
	durch Hinzufügen zusätzlicher Platten erweiterbar				

¹ Bei Hardware ist durch die begrenzten Ressourcen das Limit bei etwa 15000 Postfächern. Bei virtuellen Appliances kann das Limit gegebenenfalls durch Hinzufügen weiterer Ressourcen erhöht werden (siehe auch ⁴). In jedem Fall kann jedoch die Anzahl unterstützter Postfächer durch Kaskadieren mehrerer Appliances beliebig erhöht werden.

² Bei einer angenommenen durchschnittlichen E-Mail Größe von 200 kByte

³ Da einige Ressourcen in virtuellen Umgebungen nicht mit physikalischen vergleichbar sind (Speicher/Prozessoren), können diese im Bedarfsfall entsprechend angepasst werden. Weiterhin ist zu beachten, dass die genannten Werte Mindestanforderungen sind. Insbesondere bei weiteren aktiven Features, wie zum Beispiel dem [Protection Pack \(PP\)](#) ¹⁰⁶, müssen an dieser Stelle gegebenenfalls mehr Ressourcen bereit gestellt werden

⁴ Die Maximalanzahl der möglichen Postfächer kann durch skalieren von Prozessorkernen und RAM erhöht werden. Jedoch zeigt sich in der Praxis, dass durch Überschreiten der oben genannten maximalen Werte kaum noch Steigerungen erreicht werden können. Für diesen Fall können jedoch mehrere Appliances kaskadiert werden.

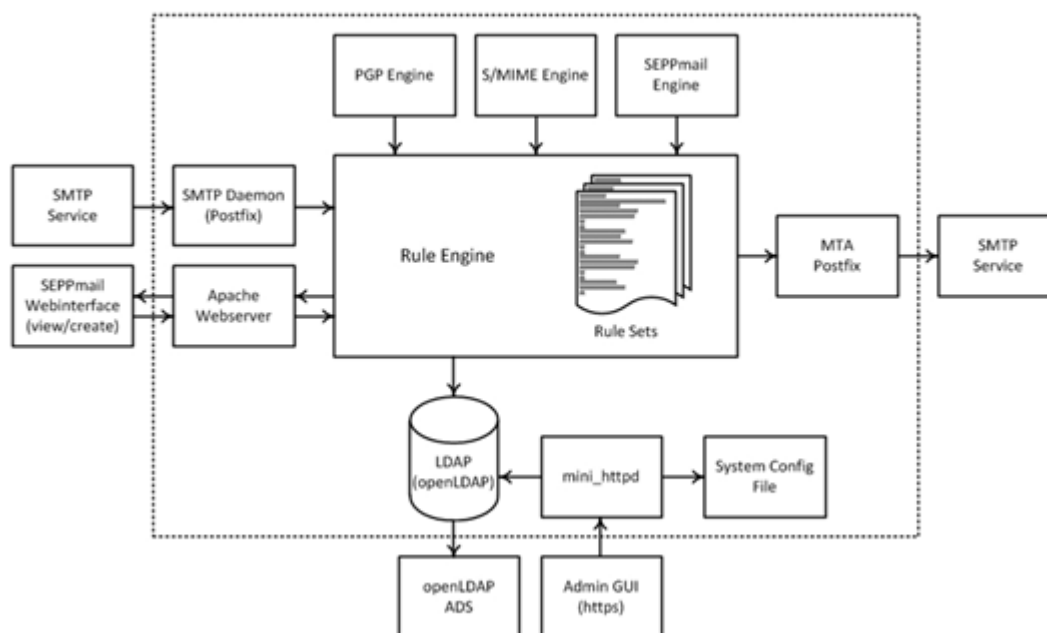
⁵ Je nach Plattengröße, werden bis zu 4 GB für das Erweitern der „/tmp“ Partition verwendet.

3.3.3 Software

Die Software der SEPPmail Appliance basiert auf dem Betriebssystem OpenBSD. Dieses hat sich über die Jahre als extrem zuverlässig und widerstandsfähig gegen Angriffe erwiesen. Darüber hinaus wurde das Betriebssystem durch SEPPmail zusätzlich gehärtet. So wurden alle nicht benötigten Libraries entfernt. Weiterhin wurden ausschließlich die funktional notwendigen Module implementiert. Die Firmware hat in der komprimierten Version (Betriebssystem und Applikation) eine Größe von unter 200MB.

Durch dieses Konzept ist auch der Aufbau Payment Card Industry Data Security Standard, kurz PCI – konformer Infrastrukturen möglich (Passwortregeln, SIEM, Samhain-Integration, verschlüsseltes Dateisystem und so weiter).

Schematischer Aufbau



3.3.4 Zentrales Regelwerk (Rule-Engine)

Die Rule-Engine der SEPPmail Appliance gleicht einem Workflow-System. Über dieses Regelwerk wird bestimmt, wie jede einzelne E-Mail zu verarbeiten ist.

Bei eingehenden E-Mails wird zunächst überprüft, ob diese kryptographisch behandelt sind. Aufgrund des Ergebnisses werden dann entsprechende Aktionen ausgelöst, wie zum Beispiel Entschlüsseln und /oder Prüfen einer vorhandenen [Elektronischen Signatur](#) ^[68].

Weiterhin stehen für das Überprüfen eingehender E-Mails optional noch weitere Funktionen, wie beispielsweise Spam- und Virenschutz (siehe [Protection Pack](#) ^[106]) bereit.

Ausgehende E-Mails kommen in der Regel klassifiziert (siehe [Steuern der Appliance](#) ^[99]) auf der SEPPmail Appliance an. Die SEPPmail Appliance prüft diese Kriterien und führt die sich daraus ergebenden Aktionen aus. Aber auch fest definierte Merkmale wie Absender oder Empfänger einer E-Mail können Auslöser für entsprechende Aktionen sein. Weiterhin können Kriterien aus Drittsystemen, wie zum Beispiel die Gruppenzugehörigkeit eines Absenders im Microsoft Active Directory (AD), über eine LDAP-Anbindung, als Auslöser herangezogen werden. Auszulösende Aktionen sind in der Regel das Verschlüsseln und Signieren von E-Mails. Aber auch das Anhängen eines Disclaimers, das Setzen einer auf den Absender personalisierten Fußnote (siehe [Central Disclaimer Management \(CDM\)](#) ^[125]), das Versenden von großen Dateien (siehe [Large File Transfer \(LFT\)](#) ^[128]) und vieles mehr ist möglich.

Konfigurierbar ist dieses zentrale Regelwerk ebenfalls über die Browser basierte Administrationsoberfläche. Somit kann auf einfachem Wege die in einem Unternehmen benötigte Security Policy individuell umgesetzt werden, wenngleich das Standard Ruleset bereits in 90% aller Installationen den Vorgaben der jeweiligen Unternehmen entspricht.

Für sehr spezielle Anforderungen besteht weiterhin die Möglichkeit programmatisch in den E-Mail Verarbeitungsprozess einzugreifen. Hierfür steht eine sehr einfach gehaltene, proprietäre Skriptsprache zum Einsatz, welche im Handbuch detailliert dokumentiert ist.

3.3.5 Architekturen

3.3.5.1 Im vollen Mailstrom (empfohlen)

Generell wird empfohlen, die SEPPmail Appliance immer in den vollen E-Mail Strom zu integrieren. Das heißt, jede ein- und jede ausgehende E-Mail wird durch die SEPPmail Appliance verarbeitet.

Somit wird jede eingehende E-Mail gegebenenfalls entschlüsselt, beziehungsweise eine eventuell vorhandene Signatur geprüft und für den internen E-Mail Empfänger entsprechend gekennzeichnet (im Standard [secure], [signed OK], [signed INVALID])

Weiterhin werden Zertifikate von eingehender, signierter E-Mails gesammelt und stehen somit bei Bedarf für das Verschlüsseln an diese Kommunikationspartner unternehmensweit bereit.

Bei ausgehenden E-Mails kann der **Managed Domain Service** ³¹ genutzt werden. Das Entscheiden, ob und wie E-Mails beim Versand behandelt werden (verschlüsseln, signieren, mit Disclaimer versehen, etcetera) werden, geschieht zentral über das Ruleset der SEPPmail Appliance oder individuell durch die E-Mail über die bekannten Mechanismen (siehe **Steuern der Appliance** ⁹⁹).

3.3.5.1.1 Kleine Umgebungen

Für gewöhnlich wird die Appliance in kleineren Umgebungen als zusätzliche Stufe zwischen E-Mail Server und Internetzugang (Router) in den E-Mail Strom gesetzt. Wird in dieser Konstellation kein externer AntiSpam Dienst genutzt, so ist das optional erhältliche **Protection Pack** ¹⁰⁶ zum Schutz vor Spam und Viren dringend zu empfehlen. Andernfalls droht bei Spam Attacken der E-Mail Verkehr zum Erliegen zu kommen.



3.3.5.1.2 Mit zwischengeschalteter Schutzkomponente

Dabei werden ausgehende E-Mails zunächst an der Appliance - je nach Kennzeichen - verschlüsselt/signiert und im Anschluss nicht mehr direkt in das Internet gesendet, sondern an die Schutzkomponente übergeben. Eingehende E-Mails werden zunächst durch die Schutzkomponente entgegengenommen und geprüft (hier ist zu beachten, dass bei verschlüsselten E-Mails ein Prüfen auf Viren nicht möglich ist!) und anschließend an die SEPPmail Appliance geleitet. Kryptographisch behandelte E-Mails werden nun auf der SEPPmail Appliance entsprechend Verarbeitet (entschlüsseln und/oder prüfen von Signaturen, gegebenenfalls auch Header Tagging und so weiter) ausgeführt. Abschließend gibt die Appliance die E-Mail an den E-Mail Server weiter.



Hinweis:

Auch in dieser Konstellation kann der Einsatz des optionalen **Protection Pack** ¹⁰⁶ der SEPPmail Appliance durchaus sinnvoll sein. Somit kann auch bei verschlüsselten E-Mails, welche am Spam Filter nicht auf Viren geprüft werden können, die Zweistufigkeit des Virenschutzes gewährleistet werden.

3.3.5.1.3 Parallel zur Schutzkomponente

Stellt die Schutzkomponente spezielle Routing Funktionen bereit, so können ausgehende E-Mails am Spam Filter auf Viren geprüft werden, bevor sie gegebenenfalls an der Appliance verschlüsselt/signiert werden. Eingehende verschlüsselte E-Mails werden zunächst zum Entschlüsseln an die SEPPmail Appliance geleitet und anschließend zur Virenprüfung zurück an die Schutzkomponente geliefert. Somit können auch verschlüsselte E-Mails durch die Schutzkomponente auf Viren geprüft werden.



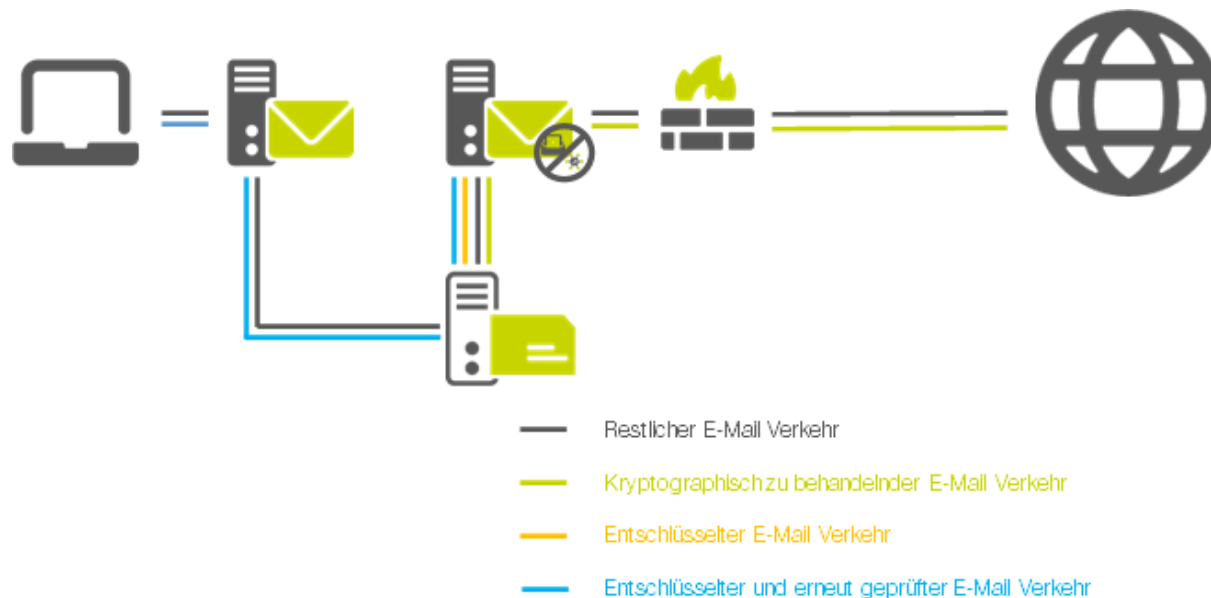
Achtung:

Die eingesetzte Schutzkomponente muss diese Konfiguration unterstützen, da andernfalls unweigerlich eine „mail-loop“ entsteht und der E-Mail Verkehr somit zum Erliegen kommt. Unterstützt die Schutzkomponente dieses Routing nicht, kann unter Umständen ein spezielles Routing auf der SEPPmail Appliance ⁸⁴⁾ Abhilfe schaffen.

3.3.5.1.4 Routing auf der SEPPmail Appliance

Unterstützt die Schutzkomponente keine speziellen Routing-Funktionen, so kann dennoch mittels Header-Tagging ein zweifacher Durchlauf einer ursprünglich verschlüsselt eingehenden E-Mail durch die Schutzkomponente gewährleistet werden, ohne eine sogenannte Loop zu erzeugen. Die SEPPmail Appliance übernimmt dabei das Routing.

Eingehend:



Dabei wird zunächst der gesamte eingehende E-Mail Verkehr von der Schutzkomponente an die SEPPmail Appliance weitergeleitet. Die SEPPmail Appliance verarbeitet diese E-Mails. Alle unverschlüsselten E-Mails werden nach dem Verarbeiten an den E-Mail Server übergeben.

Durch die SEPPmail Appliance entschlüsselte E-Mails werden mit einem speziellen X-Header versehen und erneut an die Schutzkomponente übergeben. Nach dem Prüfen auf Malware durch die Schutzkomponente übergibt diese die E-Mail erneut an die SEPPmail Appliance. Diese erkennt aufgrund des zuvor gesetzten X-Headers, dass die E-Mail bereits im ersten Durchlauf verarbeitet wurde und sendet diese ohne weitere Aktionen an den E-Mail Server.

Ausgehend:



Somit wird mit ausgehenden E-Mails letztendlich wie bereits im Szenario Mit zwischengeschalteter Schutzkomponente ⁸² beschrieben verfahren.

3.3.5.2 Ausschließlich kryptographisch behandelte E-Mails

In komplexeren Umgebungen besteht unter Umständen der Bedarf, ausschließlich kryptographisch zu behandelnde E-Mails über die SEPPmail Appliance zu routen.

Im folgenden Szenario fällt die Möglichkeit der zentralen Entscheidung, ob und wie E-Mails beim Versand verschlüsselt/signiert werden, an der SEPPmail Appliance weg. Dieses Steuern wird von der vorgeschalteten Schutzkomponente übernommen.

Soll das individuelle Steuern von Aktionen auf dem Client erhalten bleiben, muss die Schutzkomponente die via **Betreffzeilen Schlüsselwörter** ^[99], **SEPPmail Microsoft Outlook Add-In** ^[100], IBM Notes Schablone oder Groupwise Vorlage vorgenommenen Markierungen interpretieren können.

Eingehend muss die AntiSpam-Komponente zuverlässig erkennen können, ob eine E-Mail kryptographisch behandelt ist, um diese korrekt zu routen.



Hinweis:

Bei dieser Art der Konfiguration geht - zumindest ausgehend - die **Managed Domain Service** ^[31] Funktion verloren, da nur an der SEPPmail Appliance bekannt ist, ob der Kommunikationspartner ebenfalls über eine SEPPmail Appliance verfügt und am Service teilnimmt.



Achtung:

Die eingesetzte Schutzkomponente muss diese Konfiguration unterstützen, da andernfalls unweigerlich eine „mail-loop“ entsteht und der E-Mail Verkehr somit zum Erliegen kommt.

3.3.5.3 Schnittstellen

Eine Liste der zu gewährleistenden Kommunikationswege, über welche die SEPPmail Appliance kommuniziert, ist in einer Kurzzusammenfassung im Quick-Install Guide (siehe <https://downloads.seppmail.com/index.php/outlook-plugin/>) als auch ausführlich im Kapitel **Firewall / Router einrichten** ¹³⁵ des Handbuchs zu finden.

3.3.6 Hochverfügbarkeit, Loadbalancing

Die Cluster- und Loadbalancing-Funktionalität ist im Grundsystem der SEPPmail Appliance integriert. Mit wenigen Schritten kann ein Cluster zwischen zwei oder mehr Geräten aufgebaut werden, bei Bedarf auch über verschiedene Standorte hinweg. Dabei werden alle betriebsrelevanten Daten (Systemparameter, Nutzerdaten und Schlüsselmaterial) über alle Systeme synchronisiert. Da auf der SEPPmail Appliance E-Mails generell nur für die Dauer des Verarbeitens in der E-Mail gehalten werden, ist ein Synchronisieren der Nutzdaten (E-Mails) nicht erforderlich. Auch hier zeigt sich der sparsame Umgang mit Systemressourcen (Bandbreite).

Die Systeme sind so ausgelegt, dass bei einem Totalausfall eines Systems oder gegebenenfalls eines ganzen Standortes, der oder die verbleibenden Systeme, auch standortübergreifend, den Betrieb reibungslos aufrechterhalten können. Sobald der Regelbetrieb wiederhergestellt ist, werden alle Systeme wieder automatisch abgeglichen.

3.3.6.1 Multi Master LDAP

Ein SEPPmail Appliance Cluster besteht aus zwei oder mehr SEPPmail Appliances. Jedes Mitglied des Clusters, beziehungsweise jede Instanz ist Teil des Multi-Master LDAP Verbundes. Im LDAP sind alle für den alleinigen Betrieb einer Instanz notwendigen Daten abgelegt.

Der Einsatz von Multi-Master LDAP ermöglicht deshalb auf einfache und elegante Art allen Instanzen, mit minimaler Verzögerung, die gleiche Datenbasis bereit zu halten.

Des Weiteren ist über den LDAP-Synchronisierungsprozess ein Betrieb des Clusters über reine IP Netzwerke, gegebenenfalls auch standortübergreifend über verteilte Rechenzentren hinweg, möglich. Spezielle Protokolle sind hierfür nicht notwendig.

3.3.6.2 Queue-Less-Betrieb

Generell werden auf der SEPPmail Appliance E-Mails nur für die Dauer des Verarbeitens in der E-Mail gehalten. Durch den Queue-Less-Betrieb wird das zurückbleiben von E-Mails in der E-Mail-Queue der SEPPmail Appliance selbst für diesen kurzen Zeitraum verhindert. Eine E-Mail wird dem abgebenden Relay erst dann als empfangen quittiert, wenn der Empfang bereits durch das nachfolgende Relay bestätigt wurde.

Dieses Verfahren erleichtert gegebenenfalls die Fehlersuche im E-Mail System, da in der Regel die Suche auf den im E-Mail Fluss vorgelagerten Systemen ausreichend ist. Hauptvorteil ist jedoch bei Hardware Appliances, dass bei einem Ausfall noch nicht zugestellte E-Mails niemals verloren gehen können. Somit kann die Hardware ausgetauscht werden, ohne Datenverlust fürchten zu müssen.

3.3.6.3 Failover und Loadbalancing

Über die in der SEPPmail Appliance integrierte Cluster Funktion können zwei oder mehrere Geräte einfach in einen Multimaster Cluster zusammengeführt werden. Hierfür ist einzig eine TCP-Verbindung zwischen den Geräten erforderlich, um eine gemeinsame Datenbasis auf allen Cluster Partnern zu halten.

Failover kann dann über unterschiedliche Verfahren realisiert werden, das

- Verwenden von DNS via MX oder Round Robin für das Ansprechen der Systeme.
- Definieren von ausschließlich lokal gültigen MX Einträgen, für das Erreichen des nächsten Hops.
- Definieren von virtuellen IP-Adressen, wodurch alle Cluster Partner über die gleiche IP Adresse erreichbar sind.

Loadbalancing kann ebenfalls durch unterschiedliche Verfahren umgesetzt werden, das

- Aufteilen des E-Mail Stroms (zum Beispiel ein-/ausgehend) auf unterschiedliche, virtuelle IP-Adressen getrennt.
- Definieren von MX-Records mit gleicher Priorität auf virtuelle IP-Adressen oder DNS Round Robin.
- Verwenden des in der SEPPmail Appliance integrierten Loadbalancer: Erreicht eine Maschine den voreingestellten Last-Schwellwert, werden weitere Anfragen automatisch an die vordefinierten weiteren Cluster Partner weitergegeben. Dies funktioniert auch über verteilte Standorte

Für den Zugriff auf das Webportal (GINA) kann über virtuelle IP- Adressen oder DNS Round Robin natürlich ebenfalls Failover und Loadbalancing gewährleistet werden.

3.3.7 System Management

3.3.7.1 Administration

Der administrative Zugriff erfolgt in der Regel über eine SSL gesicherte Verbindung auf einen, separat in der SEPPmail Appliance integrierten, Web-Server (Administrationsoberfläche).

Alternativ können diverse administrative Aktionen auch über eine sogenannte Rest-API vorgenommen werden. Dies ermöglicht beispielsweise in größeren Umgebungen das On-/Off-Boarding von Mitarbeitern beim Ein-/Austritt.

3.3.7.2 Rollenrechte

Die SEPPmail Appliance verfügt über ein integriertes Rollen-Rechtesystem. Dieses ist in der folgenden Tabelle abgebildet:

Rolle	Zugriff
admin	Vollzugriff
administrationadmin	Systemrelevante Konfigurationseinstellungen (Lizenz, Update, Backup, Importfunktionen, Boot)
backup	Das Backup der Appliance wird täglich verschlüsselt an die E-Mail Adressen aller Backup Benutzer gesendet
caadmin	Interne Certificate Authority (CA)
clusteradmin	Cluster Einstellungen
domainkeysadmin	Domänen Schlüssel Verwaltung
groupsadmin	Gruppenverwaltung (diese beinhaltet sowohl die hier beschriebenen Rollen, wie auf optional selbst erstellte Gruppen zur Verwendung im Ruleset)
homeadmin	Übersicht des Systemstatus
logsadmin	Logs
mailprocessingadmin	Rule engine
mailsystemadmin	Anbindungseinstellungen und einfache AntiSpam Einstellungen
mpkiadmin	Managed Public Key Infrastructure (MPKI)-Einstellungen
multiplecustomersadmin	Mandanteneinstellungen in multitenant Systemen
pgpkeysadmin	OpenPGP Schlüsselverwaltung
readonlyadmin	lesender Zugriff auf alle Menüs
readonlyuser	lesender Zugriff auf die Menüs, in welchem ein Benutzer zusätzlich Mitglied ist
ssladmin	SSL Einstellungen
statisticsadmin	Statistik Grafiken
systemadmin	Systemeinstellungen (Netzwerkinterfaces)
usersadmin	Interne Benutzerverwaltung
webmailaccountsadmin	GINA-Benutzer Verwaltung
webmaildomainsadmin	GINA-Domänen Verwaltung
webmaillogsadmin	GINA-Web-Mail Logs
x509certificatesadmin	X.509 Zertifikatsverwaltung
x509rootcertificatesadmin	X.509 Wurzel-Zertifikatsverwaltung

Tabelle 1

3.3.7.3 Backup / Restore

Das System wird täglich automatisch gesichert. Nachdem auf der SEPPmail Appliance keine Nutzdaten (E-Mails) gespeichert werden, beschränkt sich der Inhalt der Sicherung ausschließlich auf Konfiguration und Schlüsselmaterial. Das Datenvolumen dieser Sicherungen bleibt somit selbst nach jahrelangem Betrieb der SEPPmail Appliance extrem gering. Die Sicherungsdatei wird automatisch verschlüsselt und im Standard einmal täglich per E-Mail an den oder die BackupOperator(s) gesendet.

Dank der geringen Größe, kann im Disaster-Fall die volle Funktionalität des Systems innerhalb kürzester Zeit wiederhergestellt werden. Das Wiederherstellen eines Systems erfolgt alleine durch das Einspielen der Backup-Datei. Nach einem Neustart der so wiederhergestellten SEPPmail Appliance steht diese wieder im vollen Funktionsumfang bereit.

Das Wiederherstellen einer Cluster Maschine erfolgt automatisch per Replikation, durch das Aufnehmen der neuen Maschine in den bestehenden Cluster.

3.3.7.4 System Update

Das System sucht regelmäßig automatisch nach anstehenden Versionsupdates und Patches. Steht ein Update bereit, so wird dies in der Administrationsoberfläche angezeigt. Weiterhin wird der Administrator per E-Mail darüber benachrichtigt. Dieser entscheidet, ob er das Update nur abholen und beim nächsten Systemstart oder sofort installieren möchte.

Nachdem die SEPPmail Appliance Firmware ist, wird bei einem Update immer das gesamte Core-System ausgetauscht. Dies schließt Kompatibilitätsprobleme zwischen einzelnen, benötigten Komponenten, wie zum Beispiel Datenbanken und Modulen aus und macht das System test- und reproduzierbar. Konfiguration und Schlüsselmateriale bleiben beim Update Vorgang natürlich erhalten.

Im Cluster-Betrieb können die einzelnen Cluster Partner im laufenden Betrieb nacheinander - und somit ohne Unterbrechen des E-Mail Verkehrs - aktualisiert werden.

3.3.7.5 SysLog

Die SEPPmail Appliance bietet die Möglichkeit ihre gesamten Logs an SysLog-Server für ein zentrales Überwachen/Archivieren zu liefern. Die RFC 3164 Konformität ist gegeben.

Neben den E-Mail Ereignissen können bei Bedarf auch alle Administrationsoberflächen- wie auch GINA-Ereignisse in einem PCI konformen Format eingerichtet werden (zum Beispiel CEF - Format für ArcSight).

3.3.7.6 Systemüberwachung

Für das Überwachen der SEPPmail Appliance steht sowohl die Möglichkeit des Anbindens via SNMP als auch Nagios bereit.

3.3.7.7 Report

Ein Status Report wird einmal täglich von der Appliance per E-Mail an den Statistik-Verantwortlichen versendet. Dieser beinhaltet je eine graphische Statistik zu Durchsatz (Received - Sent - Encrypted - Decrypted), Technologie (GINA - S/MIME - OpenPGP - Domain), optional Spam (incoming - Spam - Blacklisted - Greylisted), Prozessor- und Speicherauslastung, sowie Domänen- und Benutzerstatistiken im csv-Format.

Sofern administrative Aufgaben vonnöten sind, wird dieser Report als "IMPORTANT" klassifiziert und zusätzlich an die definierten Appliance Administratoren gesendet. Dies ist zum Beispiel dann der Fall, wenn aus S/MIME Signaturen eingesammelte, unbekannte Wurzel-Zertifikate bezüglich ihrer Vertrauenswürdigkeit klassifiziert werden sollten oder ein Update der Appliance ansteht.

SEPPmail Daily Report for Device ID 000c-295a-25e2

Notifications and Warnings

NOTE: There is a new version available: Installed version is 8.5, latest version is 9.0

Root Certificates

NOTE: There are 23 Root Certificates with undefined state.

To get rid of this message, log in to your appliance and click on "X.509 Root Certificates"
Sort the certificates in the table by "Trust state" by clicking on the header of this column.
Click on each entry with a "?" and decide if you want to trust the certificate or not.
A good way to decide if you want to trust a certificate is to download it and to check if your PC trusts the certificate.

Watchdog messages

Mon Aug 7 08:00:02 CEST 2017 Last successful managed domain certificates refresh at Thu Aug 3 06:15:17 2017

GINA accounts

Currently locked

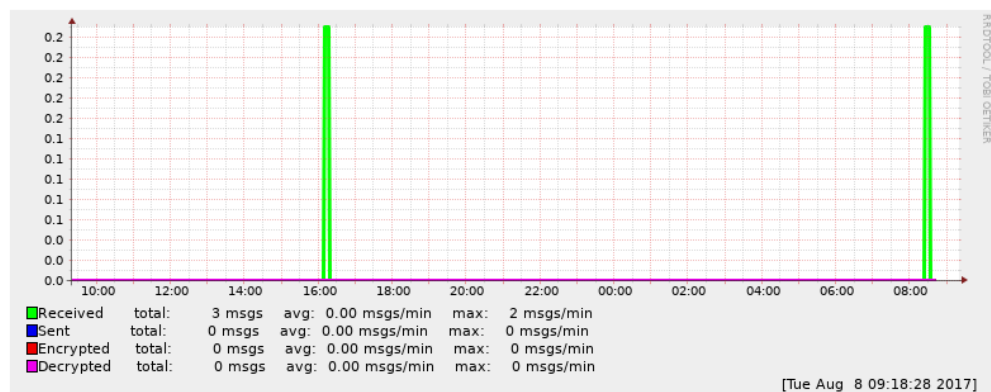
pgp_smime@customer1.local locked by admin
nokey@mailpartner.external locked by bad password policy

Daily lock history

pgp_smime@customer1.local Tue Aug 8 09:16:34 2017: locked by admin
nokey@mailpartner.external Tue Aug 8 09:17:31 2017: locked by bad password policy

Statistics

Throughput Visualisation



3.3.8 Mandantenfähigkeit - Public / Private Cloud Implementierung

SEPPmail Appliances sind grundsätzlich mandantenfähig.

Somit wird Unternehmensrechenzentren und Managed Service Providern (MSP) ermöglicht, den Service „Sichere E-Mail“ auch für eigenständige Unternehmenseinheiten und/oder unterschiedliche kleinere oder größere Kunden (Mandanten) anzubieten. Dabei unterliegt der Betrieb der Appliance dem Provider.

Durch eine ebenfalls nach Mandanten getrennte Konfigurationsoberfläche kann über optional jeweils einzurichtende Mandanten-Administratoren, der jeweilige Mandant spezifische Aufgaben selbst übernehmen, wie zum Beispiel

- Vornehmen von GINA-Einstellungen und -Layouts [416]
- Prüfen von Log-Dateien
- Verwalten von SEPPmail Appliance-Benutzern [396] (für das Signieren/Verschlüsseln)
- Verwalten von GINA-Benutzern [462]
- Verwalten von LFT-Benutzern [466] (optional)

Die Art und Weise, wie E-Mails verarbeitet werden, wird jedoch grundsätzlich global verwaltet und ist somit für jeden Mandanten im Großen und Ganzen identisch. Das bedeutet der MSP macht seinen Kunden Vorgaben bezüglich der Verarbeitungsweise von E-Mails!

Diese globalen Vorgaben werden im **Zentralen Regelwerk (Ruleset)** [80] definiert und enthalten zum Beispiel:

- Merkmale für das Steuern der Appliance
 - Tags (zum Beispiel [confidential], [sign] und so weiter)
 - E-Mail Header (Sensitivity-Parameter welcher zum Beispiel aus dem Outlook Vertraulichkeits-Flag resultiert)
 - X-Header (zum Beispiel aus dem kostenfreien SEPPmail **Microsoft Outlook Add-In** [71])
- Kennzeichen für das Rückmelden durchgeführter Aktionen
 - Tags (zum Beispiel [secure], [signed OK] und so weiter)
 - Header (Setzen des Sensitivity-Parameter (Vertraulichkeits-Flag))
- Automatisches Erzeugen von SEPPmail Appliance Benutzern
- MPKI, also von welcher Zertifizierungsstelle die S/MIME Zertifikate automatisiert bezogen werden

Ist das Individualisieren der Verfahrensweisen im Umgang mit E-Mail (Ruleset Einstellungen, unterschiedliche MPKI) für Mandanten unumgänglich, so kann dies auf zwei Arten gelöst werden:

- Installieren von mehreren Instanzen mit unterschiedlichen Rulesets und Aufteilen der Mandanten gemäß jeweils passender Konfiguration
- Das Standard-Ruleset so anpassen, dass die unterschiedlichen Regelbedürfnisse pro Mandant in diesem abgebildet werden (siehe auch **Zentrales Regelwerk (rule engine)** [80]). Dies führt unter Umständen zu einem sehr komplexen Ruleset.

3.3.9 Steuern der Appliance

Die von der Appliance durchzuführenden gewünschten Aktionen - zum Beispiel Signieren und/oder Verschlüsseln - können als globale Aktion an der Appliance oder über vordefinierte Merkmale individuell am Client (siehe [Betreffzeilen Schlüsselwörter](#) ^[99], [Microsoft Outlook Vertraulichkeit](#) ^[100], [SEPPmail Microsoft Outlook Add-In](#) ^[100], gegebenenfalls auf IBM Notes über das Anpassen der Mail-Schablone) ausgelöst werden.

Automatisierte Steuerungsmöglichkeiten sind über fest definierte Regeln zum Beispiel anhand von Absender- und/oder Empfänger Adressen und Domänen möglich. Auch ein Gruppieren von Benutzern ist zu diesem Zweck möglich. Weiterhin können über LDAP-Abfragen entsprechende Trigger Merkmale von Drittsystemen übernommen werden.

3.3.9.1 Betreffzeilen Schlüsselwörter / x-header

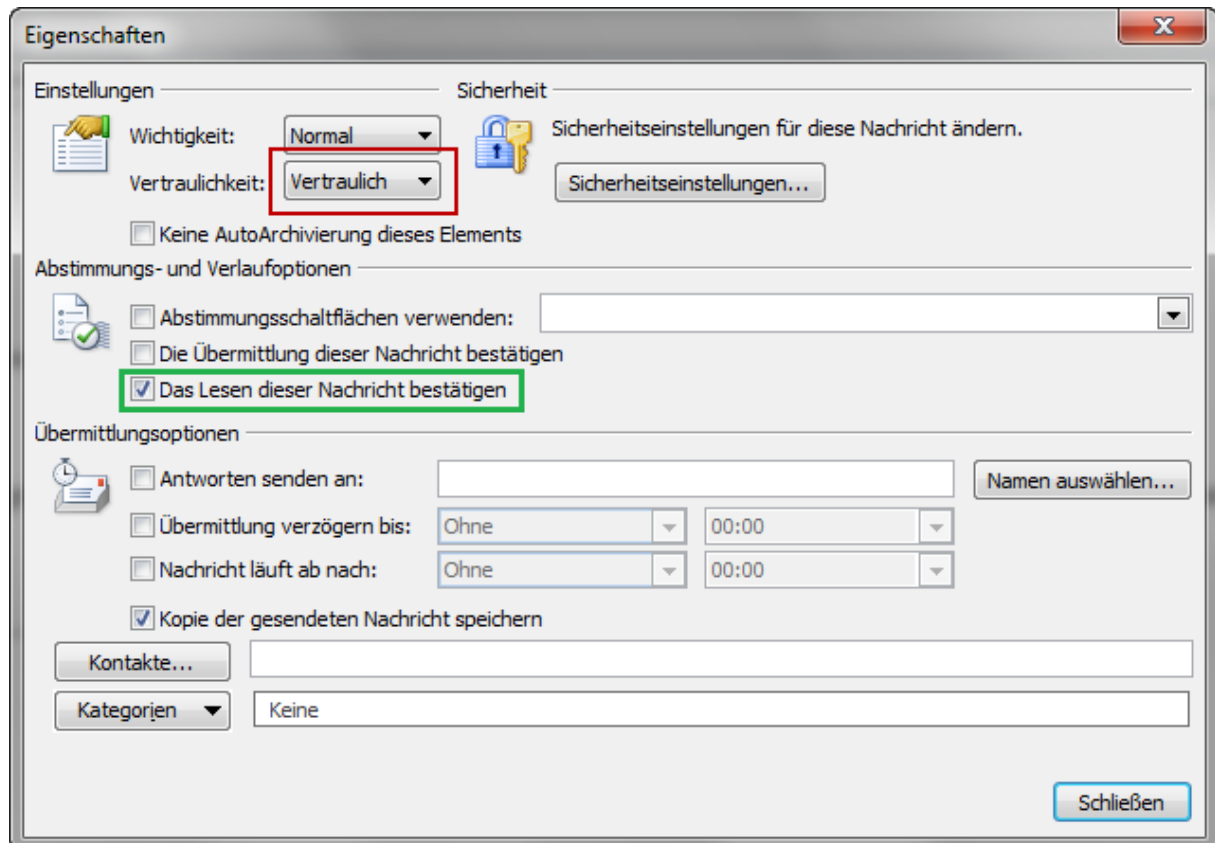
Das Verwenden von Betreffzeilen Schlüsselwörtern - welche bei Bedarf individuell angepasst werden können - gewährleistet die Unabhängigkeit vom eingesetzten E-Mail Client beim Steuern der Appliance. Ebenso können (X-)Header für das Ansteuern von, auf der SEPPmail Appliance auszuführenden, Aktionen ausgewertet werden. Diese X-Header werden im Standard vom [Microsoft Outlook Add-In](#) ^[71] verwendet, können aber auch in anderen E-Mail Clients, wie etwa IBM Notes mittels angepasster Mail Schablonen oder Novell Groupwise über Vorlagen gesetzt werden.

3.3.9.2 Microsoft Outlook Vertraulichkeit

Eine weitere Möglichkeit die SEPPmail Appliance zu steuern ist über die Vertraulichkeitseinstellung bei Microsoft Outlook.

Dabei wird die eingestellte Vertraulichkeit der E-Mail (siehe Abbildung **roter Rahmen**) ausgewertet. Steht diese auf „**Vertraulich**“ so wird das Verschlüsseln der E-Mail angefordert (siehe [Verschlüsselungshierarchie](#) ^[66]).

Wird hingegen „**Privat**“ verwendet, so wird die GINA-Technologie erzwungen. Damit mit der so erzwungenen GINA-Technologie die verlässliche Lesebestätigung einher geht, muss zusätzlich die Lesebestätigung (siehe **grüner Rahmen**) angefordert werden.



Nachrichtenoption »Vertraulich« in Outlook

3.3.9.3 SEPPmail Microsoft Outlook Add-In

Um den Benutzerkomfort zu steigern steht für Microsoft Outlook kostenfrei das [SEPPmail Microsoft Outlook Add-In](#) ^[71] zum Download bereit.

3.4 Sicherheit

Sicherheitskonzept des Betriebssystems OpenBSD

Die SEPPmail Appliance hat das, an sich als gut gesichert bekannte Betriebssystem, zusätzlich im „Bottom-up“ Verfahren gehärtet. Dabei wurden alle nicht notwendigen Libraries entfernt und nur unbedingt notwendigen Funktionen behalten.

Bei der Lösung handelt es sich um „echte“ Firmware: Bei einem Update wird das Gesamtsystem aktualisiert. Damit ist dieses auch test- und reproduzierbar.

(siehe auch www.openbsd.org/papers/asiabsdcon2015-pie-slides.pdf)

Sicherheitskonzept Core Application

Bei der Appliance handelt sich um eine gekapselte Applikation. Alle Schnittstellen nach außen sind möglichst einfach gehalten. Nur die absolut notwendigen Schnittstellen wurden implementiert. Die Firmware ist gepackt mit allen zugehörigen Applikationen unter 200 MB groß.

Sicherheitskonzept GINA-Webinterface

Das Webinterface wurde absichtlich sehr einfach gehalten und nur mit den absolut notwendigen, aber ausreichenden Funktionen versehen. Dabei wurden alle Board-Mittel für das Absichern des Web-Servers - etwa zur Abwehr von „Denial of Service“ (DoS) Attacken - ausgeschöpft. Weiterhin werden zur Eingabe nur genau vordefinierte Datenfelder akzeptiert. Jedes Datenfeld wird beim Einliefern auf Gültigkeit geprüft. Somit ist ein Einschleusen schädlichen Codes unmöglich. Der gehärtete, gekapselte Web-Server läuft als unprivilegierter User.

Schutz der Daten

- CA-Schlüssel, Private Schlüssel, Session Schlüssel, GINA-Benutzer Schlüssel
 - Die Hauptmaschinen sind so gekapselt in der DMZ platziert, dass keinerlei direkter Zugriff von außen möglich ist.
 - Sollte der Wunsch/Forderung bestehen, dass die PKI-Daten ausschließlich im Intranet abgelegt werden, kann die Lösung aufgetrennt werden. Dabei werden für den Web-Zugriff (GINA) eigene Maschinen (Satelliten) ohne eigene Datenhaltung in der Internet DMZ verwendet.
 - In der Regel macht das Sicherheitskonzept der Appliance in Kombination mit den vorhandenen Überwachungsmöglichkeiten (Samhain, Audit Log, SNMP etcetera) ein HSM unnötig. Sollte dennoch ein zusätzliches Sichern von privaten Schlüsseln gewünscht sein, ist das Anbinden einer HSM (zum Beispiel Safenet oder Thales) möglich.
 - Auf Wunsch kann das System gemäß PCI-DSS (Payment Card Industry Data Security Standard) gehärtet werden. Dabei wird das gesamte System - Platten und Kernel - nochmals mittels AES XTS 256 verschlüsselt. (siehe auch www.openbsd.org/papers/eurobsdcon2015-softraid-boot.pdf)
- Pin/Passwörter
 - Passwörter dienen dem Zugriff eines externen Empfängers auf seine GINA-E-Mail beziehungsweise nachgelagert dem AES256 Schlüssel auf der Appliance zum Entschlüsseln seiner E-Mail. Letzterer verlässt die gut geschützte SEPPmail Appliance niemals.

Zertifizierungen

Die Appliance kann auch für den Betrieb in PCI-DSS (Payment Card Industry Data Security Standard) - konformen Umgebungen konfiguriert werden. Zum Beispiel hat die Lufthansa Systems ein PCI-DSS – konformes Gesamtsystem mit einer SEPPmail Appliance als Kernsystem aufgebaut. Im Oktober 2014 wurde das System zum ersten Mal und seither jährlich mit positivem Abschluss geprüft.

Aus Herstellersicht ist derzeit aus unterschiedlichen Gründen fraglich, ob und welche „standardisierten“ Zertifizierungen sinnvoll sind. Der Markt der „Sicherheitszertifizierer“ wächst schnell und ist unübersichtlich. Einige ausländische Unternehmen verlangen zudem Einblicke in den Sourcecode. Dies können wir aus sicherheitsrelevanten Gründen nicht zulassen.

Die von der Lufthansa Systems durchgeführte Prüfung auf PCI-DSS-Compliance ist unseres Erachtens deutlich strenger und daher höher zu bewerten, da diese neben einem normalen PenTest sehr harte Vorgaben bezüglich Zugangsrechte und Protokoll der Administrationstätigkeit verlangt und prüft.

Aktuelle Sicherheitslücken oder Exploits

SEPPmail reagiert - falls betroffen - auf bekanntwerdende Sicherheitslücken oder Exploits innerhalb kürzester Zeit mit einem Sicherheitsupdate. Dieses wird allen Kunden über den normalen Update-Mechanismus bereit gestellt. Aufgrund der eingesetzten Komponenten und deren Härtung, ist die SEPPmail Appliance jedoch von vielen Sicherheitslücken erst gar nicht betroffen. So stellten beispielsweise „Heartbleed“ oder „Poodle“ keine Gefahr für die Lösung dar.

3.4.1 Ciphers

Für eingehende HTTPS-Verbindungen

		insecure ciphers	
Protokoll	Version	disallow	allow
TLS	1.3	nein	nein
TLS	1.2	ja	ja
TLS	1.1	nein	ja
TLS	1.0	nein	ja
SSL	3	nein	nein
SSL	2	nein	nein

	insecure ciphers	
Cypher Suites	disallow	allow
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS 256	ja	ja
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH secp256r1 (eq. 3072 bits RSA) FS 256		
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS 128		
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS 256		
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS 128		
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS 128	nein	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS 256		
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS 128		
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS 256		
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits FS 128		
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS 128		
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits FS 256		
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS 256		
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) 128		
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK 256		
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK 128		
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK 256		
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK 128		
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK 256		

Browser-Kompatibilität	insecure ciphers	
	disallow	allow
Android	ab 4.4.2	ja
Chrome	ab 49 / XP SP3	
	ab 65 / Win 7	
Firefox	ab 31.3.0 ESR / Win 7	
	ab 47 / Win 7	
	ab 49 / XP SP3	
IE	ab 11	
Edge	ab 13	
Safari	ab 7 / iOS 7.1	
	ab 6 / iOS 6.0.1	

S/MIME

Die SEPPmail Appliance kann bei S/MIME Verschlüsselung wahlweise für die Inhaltsverschlüsselung (Session Key)

- Triple DES
- AES-128 CBC
- AES-192 CBC
- AES-256 CBC

(siehe gegebenenfalls auch IETF RFC 3565) verwenden.

Für die Schlüsselverschlüsselung steht optional das Padding Verfahren RSA-OAEP (siehe IETF RFC 3447) zur Verfügung.

Für die S/MIME Signatur stehen als Hash-Algorithmen

- SHA-1
- SHA-256
- SHA-512

(siehe auch IETF RFC 5754) zur Verfügung. Optional steht hier das Padding-Verfahren RSA-PSS (siehe IETF RFC 4056) zur Verfügung.

Schlüssellängen sind derzeit bis 4096 Bit möglich.

OpenPGP

Für OpenPGP steht sowohl PGP Inline als auch PGP/MIME mit folgenden Ciphers

- --personal-cipher-preferences 'AES256 TWOFISH AES192 AES'
- --personal-digest-preferences 'SHA512 SHA384 SHA256'

bevorzugt zur Verfügung. Das tatsächlich verwendete Verfahren ist jedoch von dem, vom Kommunikationspartner bereit gestellten Schlüsselmaterial abhängig.

3.5 **Zusätzliche Features**

Die SEPPmail Appliance bietet zusätzliche Features, welche auf Wunsch, beziehungsweise bei Bedarf, lizenziert und verwendet werden können.

3.5.1 Protection Pack (PP)



Ein weiteres optionales Feature der SEPPmail Appliance ist das Protection Pack, welches Virus-, Spam- und Phishing-Schutz bietet.

Ist die SEPPmail Appliance aus dem Internet direkt, ohne vorgelagerte Schutzkomponenten per MX-Record zu erreichen, so empfiehlt sich der Einsatz dieser Komponente dringend. Andernfalls droht bei Spam-Attacken ein Überlasten der SEPPmail Appliance sowie gegebenenfalls der nachgelagerten Systeme. Selbst bei vorgelagerten Schutzkomponenten ist das Scannen von verschlüsselten E-Mails auf Viren nicht möglich. Nachdem an der SEPPmail Appliance E-Mails entschlüsselt werden, können Sie dort auch auf Viren geprüft werden. Weiterhin kann durch Aktivieren des Virenschutzes gegebenenfalls die Zweistufigkeit des Virenschutzes gewährleistet werden. Realisiert wird der Schutz mittels Black-, White- und Greylisting, Real-Time Blackhole List (RBL), sowie der integrierten Komponenten SpamAssassin und ClamAV. Zusätzlich bietet die SEPPmail Appliance eine proprietäre Anti-Spoofing Funktion.

Dabei arbeitet das Protection Pack generell inline rejection. Dies bedeutet, dass der Absender in jedem Fall benachrichtigt wird, wenn seine E-Mail abgewiesen wird. Dieses Verhalten ist sowohl in Bezug auf (Rechts-)Sicherheit, Workflow und insbesondere Bedienerfreundlichkeit deutlich sinnvoller als die klassische und höchstens historisch sinnvolle „Quarantänefunktion“.

Derzeit erfährt das Protection Pack eine komplette Überarbeitung, sowohl bezüglich der eingestetzten Basiskomponenten, als auch einer deutlich erweiterten Funktionalität. Aus Marketinggründen wird dann eventuell - trotz kontroverser Empfehlung - auch eine Quarantänefunktion zur Verfügung stehen. Die überarbeitete Version des Protection Packs wird für 2022 erwartet.

3.5.2 Large File Transfer (LFT)



Ein weiteres optionales Feature der SEPPmail Appliance ist der Large File Transfer, kurz LFT.

Neben den üblicherweise kleinen Datenmengen in E-Mails besteht immer häufiger der Bedarf auch relativ große Datenmengen zu übermitteln. Hierzu zählen beispielsweise Fotos, Filme und Daten zu Kampagnen der Marketing-, CAD Daten der Entwicklungs- oder Datenbank-Dumps der IT- Abteilung. Das Übermitteln dieser Datenmengen per E-Mail scheitert meist an den vom Empfänger, gelegentlich aber auch bereits an den vom eigenen E-Mail System vorgegebenen Grenzwerten.

Der Sender ist somit gezwungen, ein alternatives, für ihn geeignet erscheinendes Übermittlungsverfahren zu verwenden. Dabei wird häufig auf Internetdienste zurückgegriffen oder das Entstehen einer sogenannten „Schatten-IT“ ist vorprogrammiert. Dadurch werden häufig hochsensible Daten über nicht kontrollierte, beziehungsweise kontrollierbare Wege transportiert (zum Beispiel Dropbox).

Als letzte Alternative bleiben dann meist nur noch zeit- und kostenbehaftete Vorgänge wie zum Beispiel der traditionelle Postweg.

SEPPMail stellt mit LFT ein Verfahren zur Verfügung, bei welchen über die bewährte GINA Technologie (siehe [GINA Webmail](#) ^[32]) eine Einladung zum Abholen der großen Daten gesendet wird. Dabei kann zentral oder optional durch den einzelnen Absender entschieden werden, ob der Zugriff durch den Empfänger mittels Passwort abgesichert werden soll. Der Übertragungsweg ist in jedem Fall abgesichert.

Auf der Appliance selbst sind nur drei Parameter notwendig, wenngleich weitere Einstellungen möglich sind:

- Standardverfahren für den Versand von LFT-Nachrichten, mit oder ohne Passwort.
- Verweildauer (in Tagen) von LFT-Nachrichten, um ein unkontrolliertes Anwachsen des bereitgestellten Speichers zu vermeiden. Nach Ablauf der eingestellten Frist wird eine LFT-Nachricht automatisch gelöscht. Der Absender wird 24 Stunden vor Ablauf der Frist informiert, sofern der oder einer der Empfänger die Daten noch nicht abgeholt haben sollte.
- Schwellwert (in KiB), ab welchem die SEPPmail Appliance ausgehende E-Mails als LFT-Nachrichten senden soll.

Optional

- Maximale Größe (in KiB), welche eine LFT-Nachricht erreichen darf. Wird keine Größe definiert, darf eine LFT-Nachricht ein Viertel des zur Verfügung stehenden LFT-Speichers einnehmen.
- Standardverfahren für LFT-Antworten, mit oder ohne Passwort. Wurden an einen externen Empfänger mittels LFT secure Verfahren große Daten gesendet, so kann dieser Empfänger über seinen GINA-Account jederzeit auch große Daten an interne Empfänger senden. Diese Antworten können auch nach innen über LFT gesendet werden¹, um gegebenenfalls Größenbeschränkungen des nachgelagerten E-Mail Servers zu umgehen.
- Schwellwert (in KiB), ab welchem die SEPPmail Appliance LFT-Antworten ebenfalls über diese Technologie nach innen senden soll.
- Parameter für das Anbinden eines eigenen LFT-Archiv Servers via SCP, beziehungsweise SFTP.

¹Wird das LFT Verfahren nach innen hin angewendet, so wird dem internen Empfänger eine [LFT-Lizenz](#) ^[128] zugewiesen.

Versand großer Dateien

Für das Versenden großer Datenmengen via LFT stehen fünf Möglichkeiten zur Verfügung:

1. [Standard E-Mail Client](#) ^[109]
2. [GINA-Webmail](#) ^[110]

3. SEPPmail Microsoft Outlook Add-In  ¹¹¹
4. API  ¹¹² (Schnittstelle für das programmatische Anliefern von Daten)
5. Einliefern/Versenden durch organisationsfremde (externe) Sender an interne Empfänger  ¹¹³

3.5.2.1 Einliefern/Versenden via Standard E-Mail Client

Wurde vom Betreiber des E-Mail Systems keine, oder eine entsprechend hohe Größeneinschränkung für E-Mails definiert, steht dem Nutzen des Standard E-Mail Clients zum Versenden von großen Daten nichts im Weg.

Sender:

Der Sender verfasst eine E-Mail mit einem oder mehreren Anhängen (Abbildung 1, ①) und versendet diese. Überschreitet die Gesamtgröße dieser E-Mail den auf der SEPPmail Appliance festgelegten Schwellwert, so wird die E-Mail verschlüsselt in einem gesonderten Datenbereich der Appliance abgelegt. Gleichzeitig wird eine Einladung ② zum Download dieser übergroßen E-Mail mittels GINA-Technologie versendet. Das heißt, die LFT Benachrichtigungs-E-Mail enthält – im Gegensatz zur GINA E-Mail – im anhängenden HTML-Container nicht die gesamte E-Mail, sondern lediglich den Sicherheits-Token zur Abholung der Daten. Somit ist die LFT Benachrichtigungs-E-Mail nur wenige kByte groß.

Empfänger:

Für den externen Empfänger ist die Bedienung – unabhängig vom Einlieferungsverfahren - analog zur GINA-Technologie. Einzig durch das Ablaufdatum im Betreff ist für ihn ein Unterschied erkennbar. Wurde beim Versand das LFT-Verfahren ohne Passwort gewählt, zeigt sich ein weiterer Unterschied. Die E-Mail wird sofort nach Öffnen des HTML-Containers aus der Träger-E-Mail im GINA Web-Interface, ohne vorherige Passwort-Eingabe, angezeigt. Wie gewohnt können nun aus dem GINA Web-Interface die Anhänge und gegebenenfalls der E-Mail-Text heruntergeladen werden ③.

Diese Variante hat folgende Vorteile:

- Beibehalten der Arbeitsprozesse da ausschließlich dem Sender bekannte Werkzeuge (Outlook) zum Einsatz kommen.
- LFT Nachrichten sind in den Logs des E-Mail Servers zu sehen.
- LFT Nachrichten bleiben **nachvollziehbar**.

Schema-Skizze:

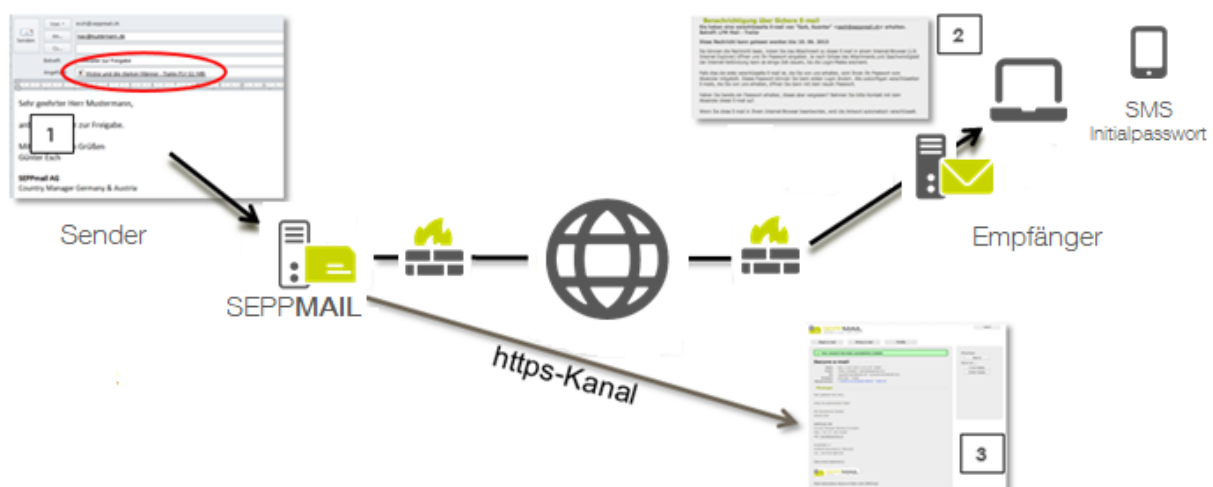


Abbildung 1

3.5.2.2 Einliefern/Versenden via GINA-Webmail

Ist die maximale E-Mail Größe in der firmeninternen Infrastruktur relativ stark limitiert, ist ein Versenden großer Datenmengen über E-Mail nicht möglich. Aus diesem Grund kann auf das **GINA-Webmail** ³²⁾ auch von intern zugegriffen werden, um große Daten direkt – am limitierenden E-Mail Server vorbei – durch Nutzen der LFT-Technologie zu versenden. Dabei kann der Anmeldeprozess für den Sender durch das Anbinden der Appliance, zum Beispiel an eine Microsoft Windows Infrastruktur, erleichtert werden. Durch dieses Anbinden ist das Windows Passwort auch für das Anmelden am GINA Web-Interface gültig.

Ein weiterer Grund für den direkten Versand über das GINA Web-Interface können besonders kritische und sensible Daten, wie zum Beispiel Kreditkarteninformationen sein. Das hierfür erforderliche Einhalten des PCI (Payment Card Industry Data Security Standard) Standards kann über reine E-Mail Systeme nicht gewährleistet werden.

SENDER:

Der Anwender öffnet dafür die HTTPS abgesicherte GINA-Webmail Seite in seinen Browser. Dort verfasst er seine Nachricht und fügt die zu übermittelnden sensiblen oder großen Daten an (Abbildung 2 ①). Die so erzeugte Nachricht wird verschlüsselt auf dem LFT-Datenspeicher der SEPPmail Appliance abgelegt. Die LFT Benachrichtigungs-E-Mail an den Empfänger ② wird ausgelöst.

Diese Variante hat folgende Vorteile:

- E-Mail Server, sowie eventuell angebundene Archiv-Systeme bleiben von großen Datenmengen verschont
- Unabhängig vom eingesetzten E-Mail Client und Standort des Senders
- PCI konform

Schema-Skizze:

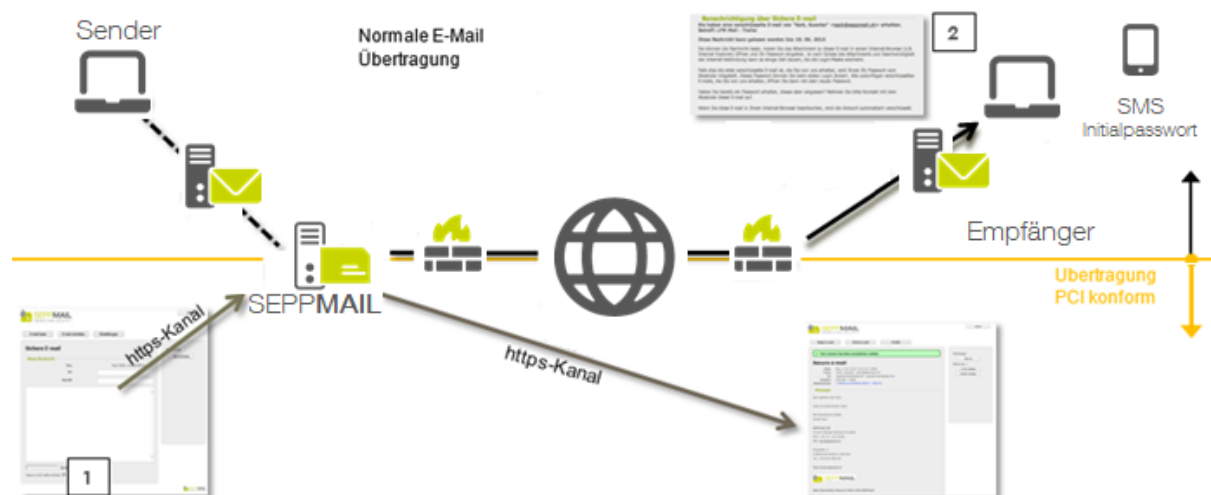


Abbildung 2

3.5.2.3 Einliefern/Versenden via SEPPmail Microsoft Outlook Add-In

Bei Einsatz von MS Outlook ist die wohl komfortabelste Variante das Verfassen einer Nachricht in Outlook und dem direkten Einliefern der großen Dateianhänge zur SEPPmail Appliance. Dabei trennt das **SEPPmail Microsoft Outlook Add-In** (bei entsprechender Konfiguration) die Dateianhänge ab und überträgt diese über einen gesicherten Kanal direkt zur SEPPmail Appliance (Abbildung 3 ①). In der eigentlichen E-Mail verbleibt lediglich eine Information über die Anhänge (Dateiname, -datum, -größe, -prüfsumme), um einen eindeutigen und nachvollziehbaren Nachweis über diese Anhänge in der E-Mail zu haben. Die E-Mail wird nun ohne Anhänge, aber mit den entsprechenden Informationen zu diesen Anhängen, über den E-Mail Server zur SEPPmail Appliance gesendet (Abbildung 3 ②). Dadurch bleiben die Informationen zu den Anhängen auch später, zum Beispiel bei archivierten E-Mails erhalten. Die SEPPmail Appliance fügt nun die eigentliche E-Mail und die bereits übertragenen Anhänge wieder zusammen und stellt die gesamte Nachricht über die LFT-Technologie für den Empfänger bereit.

Diese Variante hat folgende Vorteile:

- Beibehalten der Arbeitsprozesse, da ausschließlich dem Sender bekannte Werkzeuge (MS Outlook) zum Einsatz kommen.
- E-Mail Server, sowie eventuell angebundene Archiv-Systeme bleiben von großen Datenmengen verschont.
- LFT Nachrichten sind in den Logs des E-Mail Servers zu sehen.
- LFT Nachrichten bleiben nachvollziehbar.

Schema-Skizze:

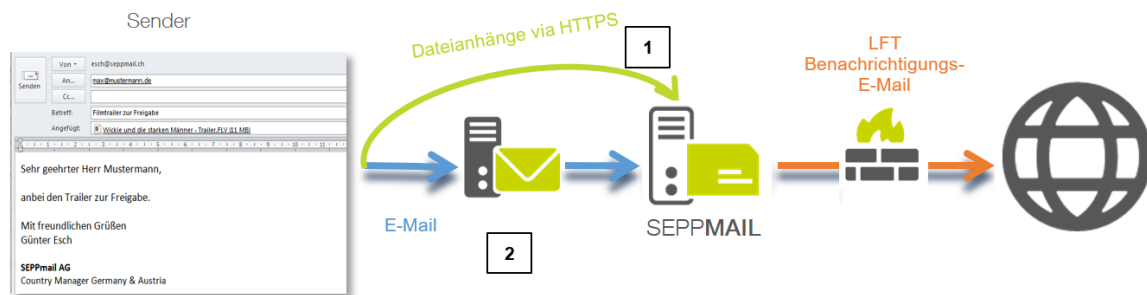


Abbildung 3

3.5.2.4 Einliefern/Versenden via API

Ab Version 10 beinhaltet die SEPPmail Appliance weiterhin eine API für das Anliefern großer Daten für den anschließenden Versand via LFT. Damit können in erster Linie auch maschinell erzeugte Daten von Dritt-Systemen bequem über die LFT-Technologie versendet werden. Folgendes Datenformat kommt dabei zum Einsatz:
JSON Payload mittels POST Request und JSON Payload in Response

LFT - Einliefern von einem externen Sender außerhalb der Organisation

Für Organisationsfremde (externer Sender) können via LFT zwei Varianten für das Einliefern großer Daten bereitgestellt werden:

1. Der Empfänger greift auf eine ihm übermittelte 12 oder passwortgeschützte LFT E-Mail zurück und nutzt die Antwortfunktion im GINA Web-Interface. Das heißt ein interner Mitarbeiter des Unternehmens könnte den jeweils externen Sender durch eine Einladungs-E-Mail per GINA-Technologie zum Einliefern großer Daten berechtigen.
2. Der SEPPmail Betreiber stellt die GINA Selbstregistrierungsfunktion bereit. Sinnvollerweise wird in diesem Fall ein Link zum GINA Web-Interface des jeweiligen Unternehmens auf dessen Internet-Seite publiziert. Nach erfolgreichem Registrieren ist der externe Sender in der Lage, über das GINA Web-Interface Nachrichten, auch mit großen Datenanhängen an Empfänger der internen E-Mail Domänen zu senden.

Der interne Empfänger erhält daraufhin die bekannte LFT Benachrichtigungs-E-Mail. Da für diesen Prozess nach intern das Verschlüsseln meist nicht erforderlich ist, kann bereits global für eingehende LFT-Nachrichten die unverschlüsselte Variante gewählt werden, sodass die Passworтеingabe nach Öffnen des HTML-Containers für den Zugriff auf das GINA Web-Interface entfällt.

Sollte für LFT-Nachrichten nach innen dennoch das Absichern mittels Passwort gewünscht sein, so können hierfür optional die jeweiligen Netzwerk (Windows) Passwörter der Benutzer verwendet werden. Zu diesem Zweck ist ein Anbinden der SEPPmail Appliance an ein externes LDAP – für Windows also an das Active Directory - möglich.

ANMERKUNG:

LFT in Verbindung mit dem Selbstregistrierungsprozess bietet zum Beispiel die Möglichkeit EUDSGVO-konform Bewerbungen zu empfangen und mit Bewerbern zu kommunizieren. Darüber hinaus ist über diesen Weg das Einschleusen von Malware unterbunden.

3.5.2.5 Einliefern/Versenden durch organisationsfremde (externe) Sender an interne Empfänger

Für Organisationsfremde (externer Sender) können via LFT zwei Varianten für das Einliefern großer Daten bereitgestellt werden:

1. Der Empfänger greift auf eine ihm übermittelte GINA- oder passwortgeschützte LFT-Nachricht zurück und nutzt die Antwortfunktion im GINA Web-Interface. Das heißt ein interner Mitarbeiter des Unternehmens könnte den jeweils externen Sender durch eine Einladungs-E-Mail per GINA-Technologie zum Einliefern großer Daten berechtigen.
2. Der SEPPmail Betreiber stellt die GINA Selbstregistrierungsfunktion bereit. Sinnvollerweise wird in diesem Fall ein Link zum GINA Web-Interface des jeweiligen Unternehmens auf dessen Internet-Seite publiziert. Nach erfolgreichem Registrieren ist der externe Sender in der Lage, über das GINA Web-Interface Nachrichten, auch mit großen Datenanhängen an Empfänger der internen E-Mail Domänen zu senden.

Der interne Empfänger erhält daraufhin die bekannte LFT Benachrichtigungs-E-Mail. Da für diesen Prozess nach intern das Verschlüsseln meist nicht erforderlich ist, kann bereits global für eingehende LFT-Nachrichten die unverschlüsselte Variante gewählt werden, sodass die Passwordeingabe nach Öffnen des HTML-Containers für den Zugriff auf das GINA Web-Interface entfällt.

Sollte für LFT-Nachrichten nach innen dennoch das Absichern mittels Passwort gewünscht sein, so können hierfür optional die jeweiligen Netzwerk- (meißt Windows) Passwörter der Benutzer verwendet werden. Zu diesem Zweck ist ein Anbinden der SEPPmail Appliance an ein externes LDAP-Verzeichnis - für Windows also an das Active Directory - möglich.

ANMERKUNG:

LFT in Verbindung mit dem Selbstregistrierungsprozess bietet zum Beispiel die Möglichkeit, EUDSGVO-konform Bewerbungen zu empfangen und mit Bewerbern zu kommunizieren. Darüber hinaus ist über diesen Weg das Einschleusen von Malware unterbunden.

3.5.3 Internal Mail Encryption (IME)

Prinzipiell vertraut SEPPmail Appliance dem internen Netzwerk. Das heißt zwischen Appliance und E-Mail Server wird in der Regel inhaltlich unverschlüsselt gesendet. Jedoch kann und sollte die Strecke zwischen SEPPmail Appliance und E-Mail-Server verschlüsselt werden.

Diese Vorgehensweise bietet mehrere Vorteile:

- In einem angeschlossenen E-Mail-Archiv werden die E-Mails unverschlüsselt abgelegt. Somit
 - a) kann im Archiv nach E-Mail Inhalten gesucht werden.
 - b) werden die Daten gesetzeskonform archiviert
 - c) ist ein Schlüsselmanagement obsolet.
- E-Mails können zentral auf schädliche Inhalte wie Viren und Malware durchsucht werden.

3.5.3.1 Allgemeines zur Ende zu Ende Verschlüsselung

3.5.3.1.1 Umgebung einer „nicht gesicherten“ E-Mail Kommunikation im Unternehmen

Bei einer ordnungsgemäßen Installation eines E-Mail Systems, geschieht die Kommunikation zwischen E-Mail Client (wie zum Beispiel Microsoft Outlook) und E-Mail-Server (wie Microsoft Exchange) bereits über verschlüsselte Strecken. Ebenso bei mobilen Endgeräten, welche innerhalb eines Firmennetzwerkes zum Beispiel via Active Sync mit dem E-Mail-Server kommunizieren. Somit sind alle Verbindungen zwischen den Kommunikationspartnern bereits gesichert. Einen Angriffspunkt könnte jedoch

- a. der E-Mail-Server darstellen, auf welchem ein Administrator die Möglichkeit eines unbefugten Zugriffs hätte. Um dem zu entgegen, kann der E-Mail-Server selbst verschlüsselt und der Zugriff mittels Vier-Augen-Prinzip gesichert werden.
- b. der E-Mail-Client sein, sobald Zugriff erlangt beziehungsweise gestattet (Vertreter) wurde . Liegt das Zertifikat für eine Ende zu Ende lokal ab, so ist selbst dann ein unbefugter Zugriff nicht ausgeschlossen.

3.5.3.1.2 Technische Voraussetzungen einer Ende zu Ende Verschlüsselung

Ist ein Absichern der Strecken, sowie des E-Mail-Servers nicht möglich, so sollten E-Mails bereits am E-Mail-Client inhaltlich verschlüsselt werden. Dies setzt das Implementieren einer entsprechenden Lösung auf den Endgeräten (PCs, Notebooks, mobile Endgeräte) des Unternehmens voraus. Weiterhin muss für jeden Benutzer zur Laufzeit lokal sein Schlüsselpaar, für das Durchführen kryptographischer Aktionen (Signieren/Verschlüsseln) bereit stehen. Dieses Schlüsselpaar sollte aus Sicherheitsgründen automatisiert vom Endgerät entfernt werden, sobald sich der Benutzer abmeldet.

Sind diese Gegebenheiten erfüllt, so sind die kryptographischen Vorgänge für den Nutzer transparent und laufen im Hintergrund ab.

Vorteile:

- Echte Ende zu Ende Verschlüsselung innerhalb des Unternehmens und mit externen Kommunikationspartnern, welche ebenfalls über die entsprechende Technologie und Schlüsselmaterial verfügen.
- Je nach Zertifikatsgüte und eingesetzter Infrastruktur ist eine Qualifizierte E-Mail-Signatur (Stufe „hoch“ gemäß EU-Verordnung 910/2014 (eIDAS)) möglich.

Nachteile

- Komplizierte Verteilmechanismen für den Bezug und das Aktualisieren des Schlüsselmaterials bis zum Client (hoher Verwaltungsaufwand / Kosten)
- Die Suche nach E-Mail-Inhalten im Archiv ist aufgrund der verschlüsselten Ablage nicht möglich. Um E-Mails aus dem Archiv wieder öffnen zu können, ist ein akkurates Schlüsselmanagement unerlässlich.
- Nur eine **Verschlüsselungstechnologie** [28] ist verfügbar (**S/MIME** [28] oder **OpenPGP** [30]). Die Technologie muss vom Kommunikationspartner ebenfalls unterstützt werden.
- Ein spontaner oder genereller Austausch von vertraulichen Information mit Kommunikationspartnern, von denen bislang kein Schlüsselmaterial bekannt ist oder welche über keine **Verschlüsselungstechnologie** [28] verfügen, ist nicht möglich.
- Eine Vertreterregelung mit Schutz der sensiblen Inhalte ist nicht möglich.
- Zentrale Schutzmechanismen wie Viren- und Content-Scanning und damit Data Loss Prevention (DLP) sind nicht möglich.

Somit ist abzuwägen, ob der Nutzen einer internen E-Mail Verschlüsselung die Inkaufnahme der Nachteile rechtfertigt. Die SEPPmail Appliance fügt sich in den SMTP-Strom im Perimeter eines Unternehmens ein. Somit verlagert sich die kryptographische Komplexität aus dem Unternehmen und konzentriert sich an zentraler Stelle. Dies ermöglicht ein einfaches und effizientes Verwalten.

Sofern das Bedürfnis nach internem Datenschutz überwiegt, muss der Ansatz hierfür wesentlich weitgreifender gefasst werden. Für diesen Fall sollte ein ganzheitliches Konzept erstellt werden, in welchem nicht nur der E-Mail-Kanal, sondern alle Komponenten des internen Netzes, wie zum Beispiel Datenbank-, File- und Folder-Verschlüsselung und so weiter, betrachtet werden. Wird ein solches Konzept konsequent umgesetzt, so ist - aus den unter **Umgebung einer „nicht gesicherten“ E-Mail Kommunikation im Unternehmen** [114] beschriebenen Gegebenheiten - eine E-Mail Ende zu Ende Verschlüsselung (zumindest intern) nur noch bedingt notwendig.

Die Interne Mail Encryption Lösung von SEPPmail eliminiert alle oben aufgeführten Nachteile. Soll das intern verschlüsselte Material von der SEPPmail Appliance unverschlüsselt in ein Archiv ausgeleitet werden, so ist der Zugriff auf das Archiv entsprechend zu schützen!

3.5.3.1.3 Bedarfsanalyse

In den meisten Fällen stellt sich bei einer Bedarfsanalyse heraus, dass sich der Bedarf einer auch intern geschützten Kommunikation meist auf wenige Personen beschränkt, zum Beispiel Mitglieder der Geschäftsführung oder Personalabteilung. Für diesen eingeschränkten Personenkreis einen entsprechenden Schlüsselschutz zu etablieren ist von administrativen Aufwand eher gering und durchaus zu empfehlen.

3.5.3.1.4 Ende zu Ende Kommunikation nach außen

Wie aus Punkt [Technische Voraussetzungen einer Ende zu Ende Verschlüsselung](#) ^[115] unter „Nachteile“ hervorgeht, ist eine echte Ende zu Ende Verschlüsselung mit externen Kommunikationspartnern nur dann möglich, wenn deren öffentliche Schlüssel bereits am Sendegerät vorliegen. Umgekehrt muss den externen Kommunikationspartnern jeweils der öffentliche Schlüssel des internen Absenders bereitstehen.

Die SEPPmail Appliance ist in der Lage sich automatisch auf die Gegebenheiten des internen und externen Empfängers einzustellen und die jeweils geeignetste Technologie für das Absichern der zu sendenden E-Mail automatisch auszuwählen.

Dabei stehen folgende Technologien bereit:

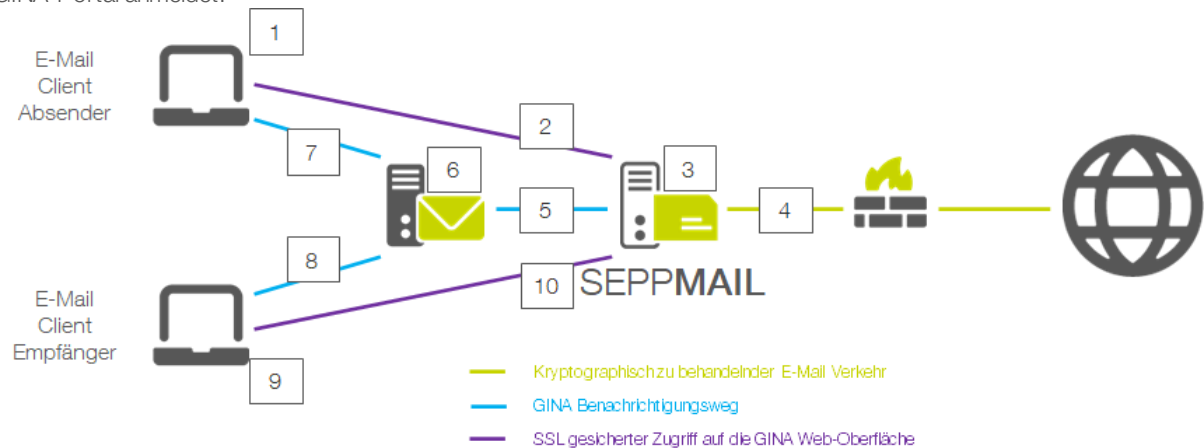
- S/MIME
- OpenPGP
- Domainverschlüsselung
- GINA (patentierte Technologie zur spontanen Kommunikation mit jedermann)

(siehe auch [Verschlüsselungshierarchie](#) ^[66])

In der Regel leitet ein E-Mail-Server interne E-Mails nicht nach außen. Da ein Verschlüsselungs-Gateway jedoch im E-Mail-Strom zwischen E-Mail-Server und Internet steht, müssen gegebenenfalls auch interne E-Mails nach außen bis zum Verschlüsselungs-Gateway geleitet werden, um dieses für eine interne E-Mail-Verschlüsselung nutzen zu können.

3.5.3.2 SEPPmail IME unter ausschließlicher Verwendung der GINA-Technologie

Diese Variante basiert allein auf der GINA-Technologie, wobei sich der Absender bereits für den Versand der E-Mail am GINA-Portal anmeldet.



1. Am E-Mail Client (1) wird eine SSL Verbindung (2) zum GINA-Portal der SEPPmail Appliance (3) aufgebaut.
2. Nach Anmelden am GINA-Portal wird im Web-Mailer direkt eine E-Mail an interne (und gegebenenfalls externe) Benutzer adressiert und versendet.
3. Die SEPPmail Appliance leitet die so erzeugten, bekannten GINA-Mails (5) an den internen E-Mail Server (6), sowie für eventuell adressierte externe Benutzer (4) mit dem bestmöglichen Verfahren verschlüsselt (siehe [Verschlüsselungshierarchie](#)) in das Internet.
4. Der interne E-Mail Server (6) leitet die GINA-Mails an den/die Empfänger (8) sowie den Absender (7).
5. Die Empfänger (9) sowie der Absender (1) können die E-Mail im E-Mail Client öffnen und gelangen durch Öffnen des verschlüsselten HTML-Anhanges über die SSL verschlüsselte Strecke [(10) beziehungsweise (2)] zum bekannten GINA-Web-Mailer (3) mit dessen Hilfe die ursprüngliche E-Mail aus dem HTML-Anhang entschlüsselt und gelesen werden kann.

Vorteil dieser Lösung ist die absolute Unabhängigkeit von den dazwischen eingesetzten Komponenten wie E-Mail-Client oder E-Mail-Server.

Nachteil dieses Konzeptes ist der fehlende Zugriff auf Adresslisten und Datenbanken.

3.5.3.3 SEPPmail IME 1.0

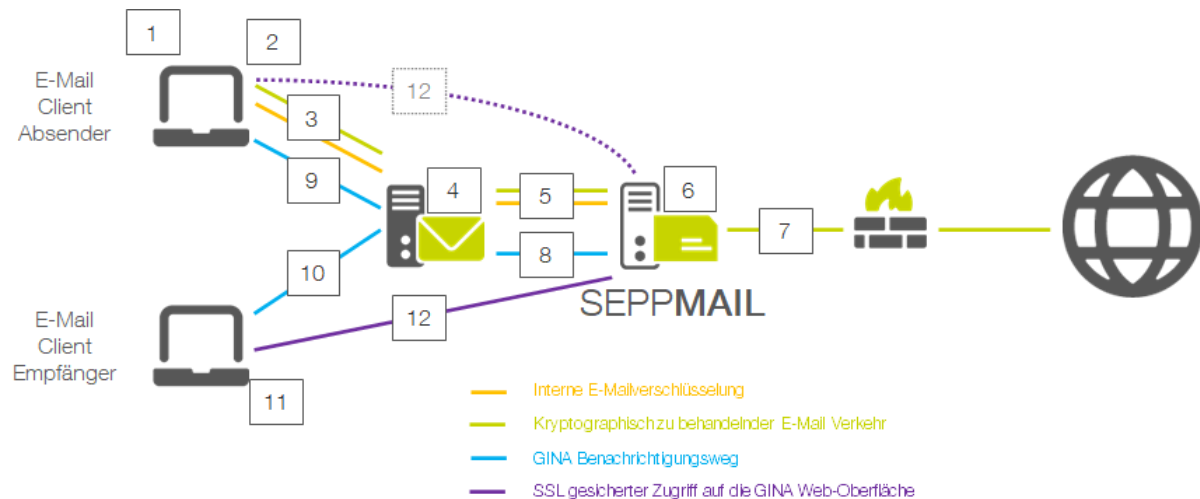
SEPPmail löst die beschriebene Anforderung durch eine vollständige E-Mail Verschlüsselung mit Hilfe des SEPPmail Microsoft Outlook Add-In und dem Nutzen aller Standardfunktionalitäten, welche Outlook zur Verfügung stellt.

Dabei

- setzt das SEPPmail Microsoft Outlook Add-In die Empfangsadressen im E-Mail Header um und ersetzt diese durch eine statische Sonderadresse
- erhält der Absender seine E-Mail, in der Regel im GINA verschlüsselt (es sei denn ein S/MIME Zertifikat wäre für ihn im Zertifikatsspeicher für ausgehende E-Mails hinterlegt), zurück
- ist die E-Mail auf der Strecke bis zur SEPPmail Appliance inhaltlich unverschlüsselt

3.5.3.3.1 Ablauf

IME 1.0 basiert auf der GINA-Technologie in Verbindung mit dem SEPPmail Microsoft Outlook Add-In. Der Vorteil dieser Lösung liegt zum einen in der Outlook-Integration, zum anderen erleichtert sie das Realisieren von Vertreterregelungen, da die intern verschlüsselten E-Mails auch verschlüsselt im Outlook abgelegt bleiben. Somit können diese nur vom originären Empfänger mit dessen Passwort entschlüsselt und somit gelesen werden. Die folgende Grafik zeigt den funktionalen Ablauf:



IME 1.0 Abbildung 1

1. Am E-Mail Client (1) wird eine neue E-Mail – an einen oder mehrere interne und gegebenenfalls externe Empfänger - erzeugt.
2. Diese wird über das SEPPmail Microsoft Outlook Add-In (2) als „zu verschlüsselnd“ und „intern zu verschlüsselnd“ markiert und modifiziert.
3. Die modifizierte E-Mail (3) wird an den E-Mail Server (4) geleitet.
4. Durch die vorgenommene Modifikation behandelt der E-Mail Server (4) die E-Mail an die internen Empfänger wie eine Internet E-Mail (5) und leitet diese somit an die SEPPmail Appliance (6) weiter.
5. Die SEPPmail Appliance (6) leitet die E-Mails an die externen Empfänger (7) mit dem jeweils bestmöglichen Verfahren verschlüsselt (siehe [Verschlüsselungshierarchie](#)) in das Internet.
6. Für die internen Empfänger generiert die SEPPmail Appliance – sofern nicht bereits vorhanden - neue, interne GINA-Benutzer und versendet an diese sowie an den Absender die bekannte GINA-E-Mail (8) über den internen E-Mail Server (4).
Wurde vom Absender die interne E-Mail Verschlüsselung gewählt, jedoch nur externe Empfänger adressiert, so erhält an dieser Stelle natürlich nur er seine ausgehende E-Mail als GINA-E-Mail.
7. Der interne E-Mail Server stellt die GINA-E-Mail(s) (9)/(10) für den Absender (1) und den/die Empfänger (11) bereit.
8. Das SEPPmail Microsoft Outlook Add-In (2) entfernt die noch unverschlüsselte E-Mail aus dem „Gesendet“ Ordner des Absenders (1). Dieser erhält an deren statt die GINA verschlüsselte E-Mail (9).
9. Der Absender (1) sowie die Empfänger (11) verbinden sich durch Öffnen des in der GINAE--Mail befindlichen html-Anhangs mit dem GINA-Portal (12) der SEPPmail Appliance (6), wo die E-Mail nach Anmelden mit den persönlichen Zugangsdaten gelesen werden kann.

3.5.3.4 SEPPmail IME 2.0

IME 2.0 erweitert den Funktionsumfang um eine inhaltlich verschlüsselte Kommunikation vom E-Mail Client bis zur SEPPmail Appliance.

Dabei wird

- eine Träger-E-Mail mit konfigurierbarer IME-Empfängeradresse erstellt
- die eigentliche E-Mail verschlüsselt als Anlage zur Träger-E-Mail bis zur SEPPmail Appliance übertragen
Durch die Träger-E-Mail wird gewährleistet, dass die Header- und somit Routing-Informationen auf dem Übertragungsweg nicht manipuliert werden können.
- die E-Mail über die SEPPmail Appliance mit dem für den Empfänger - egal ob intern oder extern - geeignetsten Verfahren (siehe [Verschlüsselungshierarchie](#) ⁶⁶⁾) verschlüsselt und ausgeliefert.

3.5.3.4.1 Vorbedingungen

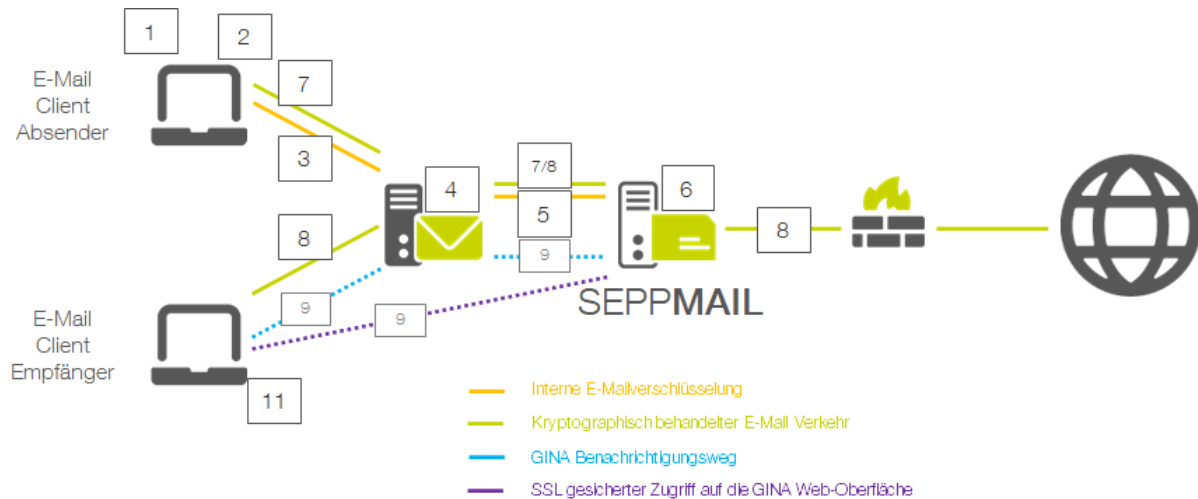
- Die SEPPmail Appliance steht im E-Mail-Strom zwischen E-Mail-Server und Internet.
- IME ist lizenziert und aktiviert.
- Das SEPPmail Microsoft Outlook Add-In ist installiert und die IME-Empfänger-Adresse, zum Beispiel [domain-confidentiality-authority@ime.domain.tld](#) konfiguriert. Dies ist die Sonderadresse, die den E-Mail-Server veranlasst, die E-Mail nach extern - also zur SEPPmail Appliance - zu routen.
Dabei eröffnen sich folgende Möglichkeiten:
 - Die offizielle Firmendomäne kann hinterlegt werden (zum Beispiel @ime.meinefirma.tld)
 - Durch die Wahl der „IME“ Subdomain können Zertifikate für die IME Empfängeradresse ausgestellt und gegebenenfalls auch extern per DNS propagiert werden.
 - Über den Nutzernamen der IME Empfängeradresse könnten zusätzliche Gruppen- oder Nutzer-Regeln im Custom Ruleset auf der SEPPmail Appliance festgelegt werden:
Ein „topsecret@ime.meinefirma.tld“ kann zum Beispiel strenger behandelt werden, als „memo@ime.meinefirma.tld“
- Das interne Domänenzertifikat für die Verschlüsselung der E-Mails bis zur SEPPmail Appliance. Dieses wird in der SEPPmail Appliance generiert und im Windows Standard Zertifikatsspeicher am Client abgelegt.
- Ein persönliches Zertifikat für das Verschlüsseln, Entschlüsseln und gegebenenfalls Signieren der E-Mails im Outlook Client des lokalen Senders. Dieses Zertifikat wird für den verschlüsselten Rückkanal der versendeten E-Mail verwendet. Ist dieses Zertifikat auf der SEPPmail Appliance nicht bekannt, wird im Rückkanal GINA verschlüsselt. Details dazu im [Ablauf](#) ¹²³⁾ Punkt 5.

3.5.3.4.2 Rollout / Deployment

Ein Rollout der beiden lokalen (internes Domänen- sowie persönliches-) Zertifikate am E-Mail-Client kann über die Microsoft Standardmethoden bewerkstelligt werden. Die SEPPmail Appliance muss den privaten Schlüssel des internen Senders nicht kennen.

Das benötigte **SEPPmail Microsoft Outlook Add-In**  steht als MSI-Paket zur Verfügung und kann silent, bereits vorkonfiguriert ausgerollt oder nachträglich individuell via Microsoft GPOs (Group Policy Objects) konfiguriert werden.

3.5.3.4.3 Ablauf



IME 2.0 Abbildung 1

1. Eine auch intern zu verschlüsselnde E-Mail wird im Outlook (1) verfasst, durch die entsprechende **Schaltfläche des Add-Ins** (208) als intern zu verschlüsselnd markiert und versendet.
2. Das SEPPmail Microsoft Outlook Add-In (2) erzeugt nun eine neutrale Träger-E-Mail, welche nur den Absender und das Datum erkennen lässt. Der Betreff wird mit einem Standardtext befüllt. Der Empfänger dieser Träger-E-Mail ist immer die im SEPPmail Microsoft Outlook Add-In konfigurierte **IME-Empfänger-Adresse** (210). Dieser Träger-E-Mail wird die ursprüngliche E-Mail komplett als Container angefügt, welcher mit dem lokalen Zertifikat signiert und mit dem internen Domänenzertifikat (siehe **Vorbedingungen** (121)) verschlüsselt wurde. Damit wird eine Manipulation des Inhaltes und der Header unmöglich. Das Ablegen der E-Mail im „Gesendete Elemente“ Ordner wird zunächst unterdrückt (siehe auch Punkt 6.)
3. Die E-Mail wird durch die am Exchange Server (4) unbekannte IME-Sub-Domäne zur SEPPmail Appliance (6) weitergeleitet (3/5).
4. An der SEPPmail Appliance (6) wird nach dem Entschlüsseln die Signatur der Träger-E-Mail geprüft und die Träger-E-Mail verworfen.
5. Die eigentliche E-Mail aus dem Container (siehe Punkt 1.) wird nun dem ursprünglichen Absender (7), sowie allen Empfängern mit den geeignetsten Verschlüsselungsverfahren gemäß **Verschlüsselungshierarchie** (66) ausgeliefert (8).
Sofern für interne Benutzer (11) also kein persönliches Schlüsselmaterial verteilt wurde (siehe **Vorbedingungen** (121)), würde nach intern mittels GINA-Technologie (9) verschlüsselt.
6. Das SEPPmail Microsoft Outlook Add-In erkennt beim Absender, dass es sich um eine Kopie seiner gesendeten E-Mail handelt (7) und verschiebt diese vom „Posteingang“ in den „Gesendete Elemente“ Ordner.

3.5.3.4.4 Ergebnis / Vorteile

Der E-Mail Inhalt sowie die Routing-Informationen werden bereits auf dem Transportweg zur SEPPmail Appliance über den internen E-Mail-Server vor Manipulation oder Extraktion geschützt. Die E-Mail wird in jedem Falle verschlüsselt an INTERNE und EXTERNE Empfänger mit der am besten geeigneten **Verschlüsselungstechnologie** ²⁸⁾ ausgeliefert. Ebenso wird eine sichere Kopie der E-Mail in den „Gesendete Elemente“ Ordner des ursprünglichen Absenders zurückgeliefert.

Wird dabei - gegebenenfalls partiell - für das Verschlüsseln an interne Empfänger die GINA-Technologie verwendet, so

1. werden schützenswerte E-Mails zusätzlich mit einem Passwort geschützt und bleiben auch am Client verschlossen,
2. kann ein Vertreter die E-Mail-Eingänge prüfen, ohne dass er Zugang zu den verschlüsselten E-Mails erlangt,
3. kann einem Mitarbeiter - sollte dies erforderlich werde - der Zugang zu den vertraulichen E-Mails im Nachhinein verwehrt werden, indem zentral auf der SEPPmail Appliance das Passwort geändert wird.
Für dieses Ändern kann ein Vier-Augen-Prinzip etabliert werden,
4. können selbst E-Mails im Archiv durch das Zurücksetzen des Passworts auf der SEPPmail Appliance wieder geöffnet werden. Ein unter Umständen aufwändiges wiederherstellen des Schlüsselmaterials ist nicht erforderlich.

3.5.4 Central Disclaimer Management (CDM)



Mit dem Central Disclaimer Management (CDM) kann die SEPPmail Appliance Ihre E-Mails sowohl mit zentralen Firmen- (Disclaimer), wie auch - unter Zuhilfenahme von externen LDAP-Datenbeständen (wie zum Beispiel das Microsoft Active Directory - kurz AD) - personalisierten Absender- (Footer) Informationen ergänzen.

Dies ist insbesondere möglich, da ein durch die SEPPmail Appliance hinzugefügter Disclaimer auch bei Antworten korrekt positioniert wird, also unterhalb der Antwort und nicht am Ende der E-Mail. Dabei ist unerheblich, ob eine E-Mail im Text- oder HTML-Format, beziehungsweise mit welchem der gängigen E-Mail Clients (Microsoft Outlook, Mozilla Thunderbird und Apple Mail) sie verfasst wurde.

Zentrale Firmen-Disclaimer, können verwendet werden um einheitlichen Text wie zum Beispiel Adresse und Firmeninhaber an E-Mails anzuhängen.

Beispiel Disclaimer im Textformat:

Meine Firma AG - Musterstrasse 1, 98765 Musterstadt - www.meinefirma.tld

Footer können verwendet werden, um absenderindividuelle Informationen, wie Name, Telefondurchwahl, E-Mail Adresse und so weiter an E-Mails anzuhängen.

Beispiel Footer im Textformat:

Mit freundlichen Grüßen
Max Mustermann

Telefon 0049 123 456 700
Durchwahl 0049 123 456 780
Mobil 0049 170 1234 5678
E-Mail max.mustermann@meinefirma.tld

Meine Firma AG - Musterstrasse 1, 98765 Musterstadt - www.meinefirma.tld

Beispiel Footer im HTML-Format:

Mit freundlichen Grüßen
Max Mustermann

max.mustermann@meinefirma.tld | phone 0049 123 456 700 | direct 0049 123 456 780



Sitz der Gesellschaft: Musterstrasse 1 | 98765 Musterstadt
UID: DE 987 654 321
IBAN DE98 7654 3210 0000 1234 56

Geschäftsführung: Franz Meier
HRB 123456 - Musterstadt
BIC SPKOEFFXXX

3.6 Lizenzen

3.6.1 Basissysteme und Lizenz

SEPPmail bietet die SEPPmail Appliance Basissysteme entweder als Hardware (siehe [Hardware Modelle](#) ⁷⁶⁾) oder als virtuelle (siehe [Virtualisierte Versionen](#) ⁷⁷⁾) Appliance an.

Die eingesetzte Firmware ist auf beiden Systemen identisch. Somit sind auch gemischte (Cluster-)Systeme aus physikalischen und virtuellen Appliances möglich.

Mit dem Basissystem wird auch die Basislizenz erworben, welche bereits die [Domänenverschlüsselung](#) ³¹⁾, sowie den [Managed Domain Service](#) ³¹⁾ für das gesamte Unternehmen beinhaltet.

Weiterhin zwingend erforderlich für den Betrieb der SEPPmail Appliance ist ein jährlicher, beziehungsweise dreijähriger Wartungsvertrag (Maintenance) für das Basissystem / Lizenz.

3.6.1.1 Protection Pack

Optional kann für jede Instanz (SEPPmail Appliance) das Protection-Pack (PP) erworben werden.

Der jährliche Betrag beinhaltet das Freischalten der integrierten AntiSpam und AntiVirus Funktionalität.

Diese Funktionalitäten werden durch verschiedene Filtermechanismen sowie dem Einsatz der Produkte SpamAssassin und ClamAV realisiert, deren Integration in den jeweils aktuellen Versionen gewährleistet wird.



Hinweis:

Für Systeme welche ohne vorgelagerte Schutzkomponenten direkt mit dem Internet kommunizieren, wird das Protection Pack dringend empfohlen.

Andernfalls gilt es den gegebenenfalls durch Spam E-Mails zusätzlichen Ressourcenverbrauch beim Dimensionieren der SEPPmail Appliance zu beachten!

Schritt 1 zur passenden Lizenz:

Auswahl der gewünschten Appliance(s) für das Basissystem und die dazugehörige jährliche, beziehungsweise dreijährige Wartung. Optional kann pro Basissystem die Wartung um das Protection-Pack (PP) erweitert werden.

3.6.2 Signatur und Verschlüsselung

Soll das kryptographische Behandeln von E-Mails an der SEPPmail Appliance auf Benutzerebene stattfinden, so ist für **jede sendende E-Mail Adresse** - unabhängig vom kryptographischen Verfahren - eine User-Lizenz zu erwerben. Das impliziert natürlich, dass auch nur diese Nutzer personenbezogen verschlüsselte E-Mails über die SEPPmail Appliance entschlüsseln können. Denn nur für diese Benutzer kann auf der Appliance das benötigte, benutzerbezogene Schlüsselmaterial vorgehalten werden.

Diese benutzerbezogenen Lizenzen sind fest an die E-Mail Adresse des Benutzers gebunden und werden nur dann wieder freigestellt, wenn die E-Mail Adresse stillgelegt wird, zum Beispiel wenn der Mitarbeiter das Unternehmen verlässt. Werden E-Mails von einer auf der Appliance stillgelegten E-Mail Adresse versendet, so werden diese weder signiert noch verschlüsselt (auch nicht über die Domänenverschlüsselung^[31]).

Soll die betroffene E-Mail Adresse und damit auch die allgemein gültige Domänenverschlüsselung^[31] (ohne personenbezogenes S/MIME, OpenPGP und GINA), weiter aktiv bleiben, ist das nur durch das vollständige Löschen des Users auf der SEPPmail Appliance möglich. Wurde diesem User ein Zertifikat (selbstsigniert oder offiziell) zugewiesen, so wird dieses zunächst revoziert und anschließend gelöscht. Über das Revozieren der Zertifikate wird externen Kommunikationspartnern in der Regel automatisiert die Ungültigkeit des Zertifikates mitgeteilt. Somit ist ein Verschlüsseln an die entsprechende E-Mail Adresse - anders als beim bloßen Stilllegen - durch den Kommunikationspartner mit diesem Zertifikat nicht mehr möglich.

Schritt 2 zur passenden Lizenz:

Auswahl der Anzahl benötigter Signatur- und Verschlüsselungslizenzen (pro sendender E-Mail Adresse), zuzüglich dem zwingend erforderlichen, jährlichen, beziehungsweise dreijährigen SW Care Pack.

3.6.3 Large File Transfer (LFT)

LFT kann als Standalone-, sowie als Add-On zur Secure-E-Mail-Lösung betrieben werden. Somit können LFT Lizenzen in unterschiedlichen Mengen zu den Signatur- und Verschlüsselungslizenzen bezogen werden. LFT Lizenzen sind concurrent Lizenzen. Das heißt, eine LFT Lizenz wird nach 30 Tagen der Inaktivität freigegeben und kann somit durch einen anderen Benutzer verwendet werden. LFT Lizenzen werden ausschließlich für interne Benutzer vergeben, welche eine LFT-Nachricht versenden oder empfangen.

Sind keine Lizenzen frei, so wird eine übergroße E-Mail als „normale“ SMTP-E-Mail versendet.

Schritt 3 zur passenden Lizenz:

Auswahl der Anzahl gewünschter LFT-Lizenzen, zuzüglich dem zwingend erforderlichen, jährlichen, beziehungsweise dreijährigen LFT Care Pack.

3.6.4 Internal Mail Encryption (IME)

Die unter **Internal Mail Encryption (IME)** ¹¹⁴ erläuterte Lösungserweiterung für das Verschlüsseln von E-Mails innerhalb der unternehmensinternen Infrastruktur, ist ohne Wartung einmalig pro Signatur- und Verschlüsselungslizenz zu erwerben.

Schritt 4 zur passenden Lizenz:

Auswahl von IME Lizenzen in der selben Anzahl wie Signatur- und Verschlüsselungslizenzen, sofern dieses Modul gewünscht wird.

3.6.5 Central Disclaimer Management (CDM)

Die unter **Central Disclaimer Management (CDM)** ¹²⁵ erläuterte Lösungserweiterung für das Verwalten globaler Disclaimer sowie individualisierter Fußnoten, ist in der gleichen Anzahl zu erwerben, wie sendende Postfächer im Unternehmen vorhanden sind.

Schritt 5 zur passenden Lizenz:

Auswahl von CDM Lizenzen, sofern dieses Modul gewünscht wird.

4 Inbetriebnahme der Secure E-Mail Gateway Appliance

4.1 Bevor Sie beginnen

Bei Hardware:

Bitte überprüfen Sie den Verpackungsinhalt auf Vollständigkeit. Der Lieferumfang besteht aus:

Anzahl	Beschreibung
1	SEPPmail-Hardware Appliance
1	Quick Install Guide
1	Kaltgerätekabel (240V)

Bei virtuellen Images:

Unmittelbar nach dem Importieren des Images in den Virtualisierungs-Host, sollten die Spezifikationen aus der **Size**-Tabelle entsprechend des bestellten Appliance-Typs angepasst werden.

Sollte der Lieferumfang bei Ihnen unvollständig sein oder sollten bei der Installation der SEPPmail Appliance Probleme oder Fragen auftauchen, kontaktieren Sie bitte SEPPmail oder Ihren SEPPmail Appliance Fachhändler.

Eine Liste mit den Kontaktangaben der jeweiligen Fachhändler auf der SEPPmail Webseite - <https://www.seppmail.ch> zu finden.

4.3 Benötigte Informationen zur Inbetriebnahme

Folgende Informationen Ihrer E-Mail Umgebung sind vor dem Inbetriebnehmen der SEPPmail Appliance bereitzustellen:

Benötigte Information	Ihre Angabe
Interne IP-Adresse(n) der Appliance: Interne IP-Adresse(n) und Subnetzmaske(n), unter welcher die SEPPmail Appliance im internen Netzwerk erreichbar sein wird. In der Standardkonfiguration ist eine IP-Adresse ausreichend. Bei Bedarf können jedoch für unterschiedliche Funktionen (SMTP, Administrationszugriff, Cluster ^[363] -Kommunikation, Web-Zugriff) jeweils eigene Netze verwendet werden. Siehe auch System ^[224] IP addresses ^[225] .	
Standard Gateway IP-Adresse: Standard-Gateway IP-Adresse Ihrer Firewall oder Ihres Routers, über welche die SEPPmail Appliance die Verbindung mit dem Internet herstellen kann. Siehe auch System ^[224] Routing ^[228] Default gateway ^[228] .	
Hostname der Appliance: Frei wählbarer Hostname Ihrer SEPPmail Appliance, zum Beispiel securemailgateway. Dieser ist normalerweise im internen DNS-Server aufgeführt. Diese Einstellung entspricht der internen Sicht. Sie muss also nicht den Daten, wie sie vom Internet her Gültigkeit haben, entsprechen. Siehe auch System ^[224] Name ^[228] Hostname ^[228] .	
Interne Domäne: Beispiele sind: ihrefirma.local oder ihredomain.tld und so weiter. Diese Einstellung entspricht der internen Sicht. Sie muss also nicht den Daten, wie sie vom Internet her Gültigkeit haben, entsprechen. Siehe auch System ^[224] Name ^[228] Domain ^[228] .	
DNS-Server: Die Eingabe von bis zu drei IP-Adressen von DNS-Servern ist möglich. Dabei kann es sich sowohl um externe, als auch interne DNS-Server handeln. Werden interne DNS-Server verwendet, so müssen diese Anfragen für externe Adressen entsprechend weiterleiten. Siehe auch System ^[224] DNS ^[229] .	
MX, Hostname und IP-Adresse(n) des bestehenden internen E-Mail Servers: Hostname oder IP-Adresse, unter welcher der bestehende interne E-Mail Server im internen Netzwerk angesprochen werden kann. Siehe auch ADD MANAGED DOMAIN ^[266] Settings ^[266] Forwarding server ^[266] , beziehungsweise Mail System ^[247] Relaying ^[254] .	
E-Mail Domänen: Domänen der E-Mail Adressen Ihrer Organisation, zum Beispiel firma.ch, firma.com Siehe auch ADD MANAGED DOMAIN ^[266] .	
Postmaster Adresse An diese Adresse werden Systembenachrichtigungen (zum Beispiel Watchdog Meldungen) gesendet. Weiterhin wird sie für Backup- und Systembenachrichtigungs E-Mails als Absender verwendet. Siehe auch Mail System ^[247] SMTP settings ^[252] Postmaster address ^[253] .	
Öffentlicher DNS-Eintrag oder öffentliche IP-Adresse der Appliance: Name oder die IP-Adresse, unter welchem Ihre SEPPmail Appliance aus dem Internet - als Webserver - erreichbar sein wird (siehe auch CHANGE GINA SETTINGS FOR [DEFAULT] ^[423] Secure GINAHost ^[423] Hostname ^[423]). Oft ist dies die Adresse der Firewall oder eines Reverse-Proxies / Web-Application-Firewall. In einfachen Installationen kann dazu die IP-Adresse verwendet werden, unter welcher der Internet-Router von extern erreichbar ist. Diese Information sind wie folgt herauszufinden:	

Benötigte Information	Ihre Angabe
1. Öffnen der Eingabeaufforderung auf einem Windows-PC 2. Eingabe des Befehls „nslookup“ und mit „Enter“ bestätigen 3. Es erscheint „>“ Zeichen (Prompt) 4. Eingabe des Befehls „set querytype=mx“ und mit „Enter“ bestätigen 5. Eingabe der E-Mail Domäne der eigenen Organisation (zum Beispiel ihredomain.com) und mit „Enter“ bestätigen 6. Alle verfügbaren E-Mail Server werden als „mail exchanger =“ angezeigt Servernamen hinter dem Begriff „mail exchanger“ mit der geringsten MX-Preference-Nummer haben die höchste Priorität bei der Namensauflösung.	
SSL Zertifikat: Für den Zugriff auf GINA via HTTPS, beziehungsweise für die optionale TLS-Verschlüsselung ist ein SSL Zertifikat erforderlich. Dies kann auch ein Wildcard Zertifikate sein. Dieses sollte jedoch von einer akkreditierten CA stammen.	
Admin E-Mail Adresse(n): Wird für den Empfang von Passwort Rücksetzungsanfragen von GINA-Benutzern benötigt. Werden mehrere GINA-Domains verwendet, so ist unter Umständen das Einrichten mehrerer Admin-E-Mail Adressen sinnvoll. Siehe auch CHANGE GINA SETTINGS FOR [DEFAULT] [423] Admin [424] Admin e-mail [424].	
<u>Optional:</u>	
SysLog-Server: Wird für das Übermitteln von Log-Einträgen an zentrale SysLog-Server benötigt. Siehe auch System [224] Syslog settings [235].	
SNMP-Server: Wird für das Überwachen der SEPPmail Appliance via SNMP benötigt. Siehe auch System [224] SNMP daemon [241].	
Nagios-Server: Wird für das Überwachen der SEPPmail Appliance über Nagios benötigt. Siehe auch System [224] NRPE daemon [243].	
Proxy-Server: Sind Zugriffe ins Internet für die entsprechenden Systemfunktionen nicht direkt möglich, so können diese über Proxy-Server hergestellt werden. Siehe auch System [224] Proxy settings [236], MPKI proxy settings [236] und OCSP / CRL check settings [236] Proxy server [239].	
Zeit-Server: Dient der Synchronisation der SEPPmail Appliance Systemzeit mit einem Zeitserver (für Cluster [383]-Konfigurationen zwingend!). Siehe auch System [224] Time and Date [240] Server [240].	
Virtuelle IP-Adressen: Durch virtuelle IP-Adressen kann ein Cluster [383] dynamisch angesprochen werden. Siehe auch System [224] IP ALIAS addresses [226], beziehungsweise Clustern mehrerer Systeme [168] ff.	
SMS-Dienst: Soll der GINA SMS-Passwort Versand beziehungsweise Self-Service Password Management (SSPM) [53] via SMS verwendet werden, so sind die Zugangsdaten für einen SMS-Dienst oder einen lokalen SMS-Server erforderlich. Siehe auch GINA Domains [416] SMS passwords [418] [418].	

Benötigte Informationen zum Einrichten der SEPPmail Appliance

4.4 Firewall / Router einrichten

Für eine korrekte Funktion der SEPPmail Appliance sind folgende Kommunikationswege zu gewährleisten:

Funktion / Feature	Port	Quelle	Ziel	Beschreibung
Managed Domain Service ³¹ Lizenzänderungen Systemupdate ⁹³ Support	TCP 22 (SSH)	Appliance	update.seppmail.ch support.seppmail.ch	Sollte der Zugriff über Port 22 nicht möglich sein, so besteht die Möglichkeit die Verbindung über einen Proxy-Server herzustellen (siehe auch System ²²⁴ Proxy settings ²³⁶).
E-Mail Kommunikation	TCP 25 (SMTP)	E-Mail Server	Appliance	Wird für den Versand ausgehender E-Mails vom internen E-Mail Server an die SEPPmail Appliance benötigt (siehe unter anderem auch Mail System ²⁴⁷ Relaying ²⁵⁴).
		Appliance	E-Mail Server	Wird für den Versand eingehender E-Mails von der SEPPmail Appliance an den internen E-Mail Server benötigt (siehe auch Mail System ²⁴⁷ Managed domains ²⁴⁷ Server IP Address).
		Internet	Appliance	Wird für den direkten Empfang von E-Mails aus dem Internet benötigt
		Smarthost		Wird für den Empfang von E-Mails über einen Smarthost benötigt
		Appliance	Internet	Wird für den direkten Versand von E-Mails in das Internet benötigt (siehe Mail System ²⁴⁷ Outgoing server ²⁵⁰ Use built-in mail transport agent ²⁵⁰).
			Smarthost	Wird für den Versand von E-Mails über einen Smarthost benötigt (siehe Mail System ²⁴⁷ Outgoing server ²⁵⁰ Use the following SMTP server ²⁵⁰).
Namensauflösung	TCP/UDP 53 (DNS)	Appliance	Name-Server (intern)	Ermöglicht die Namensauflösung über einen/mehrere interne DNS-Server (siehe System ²²⁴ DNS ²²⁹).
			Name-Server (extern)	Ermöglicht die Namensauflösung über einen/mehrere externe DNS-Server (siehe System ²²⁴ DNS ²²⁹).
			Internet	Ermöglicht die Namensauflösung für die Einstellung Use built-in DNS Resolver ²²⁹ (siehe System ²²⁴ DNS ²²⁹).
GINA	TCP 443 (HTTPS)	Internet	Appliance	Wird für das Herstellen der SSL verschlüsselten Kommunikation über HTTPS zur SEPPmail Appliance benötigt, welche für das Nutzen der GINA-Technologie verwendet wird.
Administrationszugriff	TCP 8080 (HTTP) und/oder TCP 8443 (HTTPS)	Admin PC (Internet)	Appliance	Wird für den Zugriff auf die web-basierte Administrationsoberfläche benötigt. Es wird empfohlen, nur die SSL verschlüsselte Verbindung (HTTPS) über Port TCP/8443 zuzulassen.

Funktion / Feature	Port	Quelle	Ziel	Beschreibung
				 Achtung: Wird in mandantenfähigen Systemen der Zugriff für die Mandanten-Admins aus dem Internet gestattet, so sollte dieser aus Sicherheitsgründen durch einen vorgeschalteten Proxy oder eine Firewall auf die IPs der Mandanten eingeschränkt werden!
Protection Pack ^[126] (optional)	TCP 80/443/ 873/ 2703 UDP 24441	Appliance	Internet	Wird für Updates des Protection Packs (AntiVirus/AntiSpam) benötigt (siehe unter anderem Mail System ^[247] Antispam ^[255] und Blacklists ^[258]).
Fetchmail (optional)	TCP 995 (POP3S) 993 (IMAPS) 110 (POP3) 143 (IMAP)	Appliance	Internet	Wird benötigt, sofern für SEPPmail Appliance-Benutzer E-Mail über eines der benannten Protokolle via Fetchmail abgeholt werden (siehe Mail System ^[247] Managed domains ^[247] Fetch mail from remote POP3 server ^[249] Interval in minutes: beziehungsweise Users ^[396] USER 'USER@DOMAIN.TLD' ^[398] Remote POP3 ^[402]).
Cluster Kommunikation (optional)	TCP 22 (SSH)	Appliance	Appliance	Wird für die Synchronisation von Appliances im Cluster ^[383] -Verbund benötigt. (siehe Clustern mehrerer Systeme ^[168] beziehungsweise Cluster ^[383]).
		Frontend	Backend	Wird für das Aufteilen der Appliance in Funktionsgruppen benötigt (siehe Frontend/Backend Cluster ^[180] , GINA Satellite ^[181] beziehungsweise Cluster ^[383] Add this device as frontend server (no local database) ^[383]).
	TCP 25 (SMTP)	GINA -Frontend	E-Mail-Server	Wird für die Konstellation GINA Satellite ^[181] benötigt. Die unter E-Mail Kommunikation dieser Tabelle genannten, weiteren Kommunikationsbeziehungen sind dann nicht erforderlich.
Zeit-synchronisation (optional, im Cluster zwingend)	UDP 123 (NTP)	Appliance	Internet	Wird für die Zeitsynchronisation mit Zeitservern im Internet benötigt (siehe System ^[224] Time and Date ^[240] Set remote NTP server ^[240]).
			Time-Server (intern)	Wird für die Zeitsynchronisation mit internen Zeitservern benötigt (siehe System ^[224] Time and Date ^[240] Automatically synchronize via NTP).
System-überwachung (optional)	UDP 161 (snmp)	internes Netz	Appliance	Wird für das Überwachen der SEPPmail Appliance via SNMP benötigt (siehe System ^[224] SNMP Daemon ^[241]).
	TCP 5666 (NRPE)			Wird für das Überwachen der SEPPmail Appliance via Nagios benötigt (siehe System ^[224] NRPE Daemon ^[241]).

Funktion / Feature	Port	Quelle	Ziel	Beschreibung
SysLog (optional)	UDP 514 TCP 6514	Appliance	SysLog Server	Wird für das Weiterleiten von Log-Einträgen an einen SysLog-Server benötigt (siehe System ^[224] Syslog settings ^[235]).
MPKI (optional)	TCP 443 (HTTPS)	Appliance	Internet	Wird ein Managed Public Key Infrastructure (MPKI ^[339]) Connector verwendet, so wird der Zugang zur Certification Authority (CA) über eine HTTPS Strecke hergestellt. Sollte der Zugriff über Port 443 nicht möglich sein, so besteht die Möglichkeit die Verbindung über einen Proxy-Server herzustellen (siehe auch System ^[224] MPKI proxy settings ^[238]).
OCSP / CRL check (optional)	TCP 443 (HTTPS) 80 (HTTP)	Appliance	Internet	Für Zertifikatsprüfungen via OCSP / CRL (siehe System ^[224] OCSP / CRL check settings ^[238]) wird der Zugriff via Port 443 (selten Port 80) zur CA benötigt. Die Möglichkeit eines entsprechenden Proxy-Eintrags besteht.
Abfrage externer Keyserver (optional)	TCP/UDP 389 (LDAP) und/oder TCP/UDP 636 (LDAPS)	Appliance	Internet	Ermöglicht LDAP Abfragen an LDAP-Server im Internet, welche zum Beispiel von vielen CAs für das Bereitstellen von öffentlichen Schlüsseln betrieben werden (siehe Mail Processing ^[286] Ruleset generator ^[287] Key server ^[309]).
			LDAP-Server (intern)	Ermöglicht LDAP Abfragen an interne LDAP-Server zur Abfrage von öffentlichen Schlüsseln interner Benutzer zum Beispiel für Interne E-Mail Verschlüsselung (IME) (siehe Mail Processing ^[286] Ruleset generator ^[287] Key server ^[309]).
Keyserver Abfrage von intern (optional)	TCP/UDP 388,387 (LDAP) und/oder TCP/UDP 635 (LDAPS)	internes Netz	Appliance	Ermöglicht LDAP Abfragen an den in die Appliance integrierten Schlüssel-Server (Key Server) zur Abfrage von öffentlichen Schlüsseln externer Kommunikationspartner, zum Beispiel für eine End-to-End Verschlüsselung (siehe Mail Processing ^[286] Miscellaneous options ^[287] Enable LDAP server on port 388, 387 and 635 to distribute collected S/MIME certificates to internal users ^[287]).
Keyserver Abfrage von extern (optional)	TCP/UDP 1389 (LDAP) und/oder TCP/UDP 1636 (LDAPS)	internes Netz	Appliance	Ermöglicht LDAP Abfragen an den in die Appliance integrierten Key Server zur Abfrage von öffentlichen Schlüsseln interner Benutzer. Diese Schlüssel können zum Beispiel für das Realisieren einer internen E-Mail Verschlüsselung verwendet werden (siehe auch System ^[224] Key server ^[234]).
		Firewall		Ermöglicht LDAP Abfragen an den in die Appliance integrierten Key Server zur Abfrage von öffentlichen Schlüsseln interner Benutzer. Damit können unter Anderem (insbesondere bei Verwenden von selbst signierten Zertifikaten) diese Schlüssel externen Kommunikationspartnern zur Verfügung gestellt

Funktion / Feature	Port	Quelle	Ziel	Beschreibung
				werden (siehe auch System [224] Key server [234]).
Self Service Password Management (SSPM) [53] (optional)	TCP 5061	Appliance	Internet	Wird von vielen SMS-Gateways für den SMS-Versand via Internet verwendet. Dies wird benötigt, sofern Self-Service Password Management (SSPM) [53] per SMS über einen externen SMS Dienst eingestellt wird. Im Bedarfsfall ist der korrekte Port direkt beim Anbieter zu erfragen.

Regeln für das Gewährleisten der Netzwerkkommunikation der SEPPmail Appliance

4.5 Basiskonfiguration in wenigen Schritten

Dieses Kapitel beschreibt, wie in wenigen Schritten die Basis-Konfiguration der SEPPmail Appliance vorgenommen wird.

4.5.1 Netzwerkeinstellungen und Systemregistrierung

Nachfolgend wird das Integrieren der SEPPmail Appliance in die vorhandene Infrastruktur beschrieben. Hierfür werden die in [Benötigte Informationen zur Inbetriebnahme](#) ^[139] gesammelten Informationen benötigt.

4.5.1.1 Initialer Verbindungsaufbau

Ziel ist das initiale Erreichen der Webbrowser basierten Administrationsoberfläche, über welche ausnahmslos die weitere Konfiguration erfolgt.

Die SEPPmail Appliance bezieht generell beim initialen Starten dynamisch eine IP-Adresse auf dem ersten Interface, sofern hierfür die Gegebenheiten in der vorhandenen Netzwerk-Infrastruktur existent sind. Ist dies der Fall, kann - sofern die bezogene IP-Adresse bekannt ist - direkt mit [Login als Administrator](#) ^[143] fortgefahren werden.



Achtung:

Kann dynamisch keine IP-Adresse bezogen werden, so startet die Appliance mit der IP 192.168.1.60. Sollte sich die Appliance in einem Subnetz befinden, in welchem diese Adresse bereits vergeben ist, sollte für den initialen Start die Verbindung zum Netzwerk unterbunden werden.

Der initiale Zugang zur Vergabe einer statischen IP-Adresse ist in den folgenden Kapiteln [Hardware Appliance](#) ^[140] und [Virtuelle Appliance](#) ^[139] beschrieben.

4.5.1.1.1 Virtuelle Appliance

Bei einer virtuellen Appliance ist das Consolen Fenster des erstmalig gestarteten SEPPmail Appliance Images auf dem Host-System zu öffnen.

Im Anschluss ist für das Setzen einer statischen IP-Adresse wie in Punkt [Consolen Login](#) ^[141] beschrieben vorzugehen.

4.5.1.1.2 Hardware Appliance

Zur erstmaligen Konfiguration der Netzwerkparameter der SEPPmail Appliance Hardware besteht die Möglichkeit einen Bildschirm und Tastatur anzuschließen und die IP-Adresse temporär an der Console auf den gewünschten Wert zu ändern. Das weitere Vorgehen für diese Methode ist im Punkt [Consolen Login](#) ^[141] beschrieben.

Alternativ kann die SEPPmail Appliance Hardware über ein Crossover-Kabel oder über einen Hub direkt mit einem Computer verbunden werden.

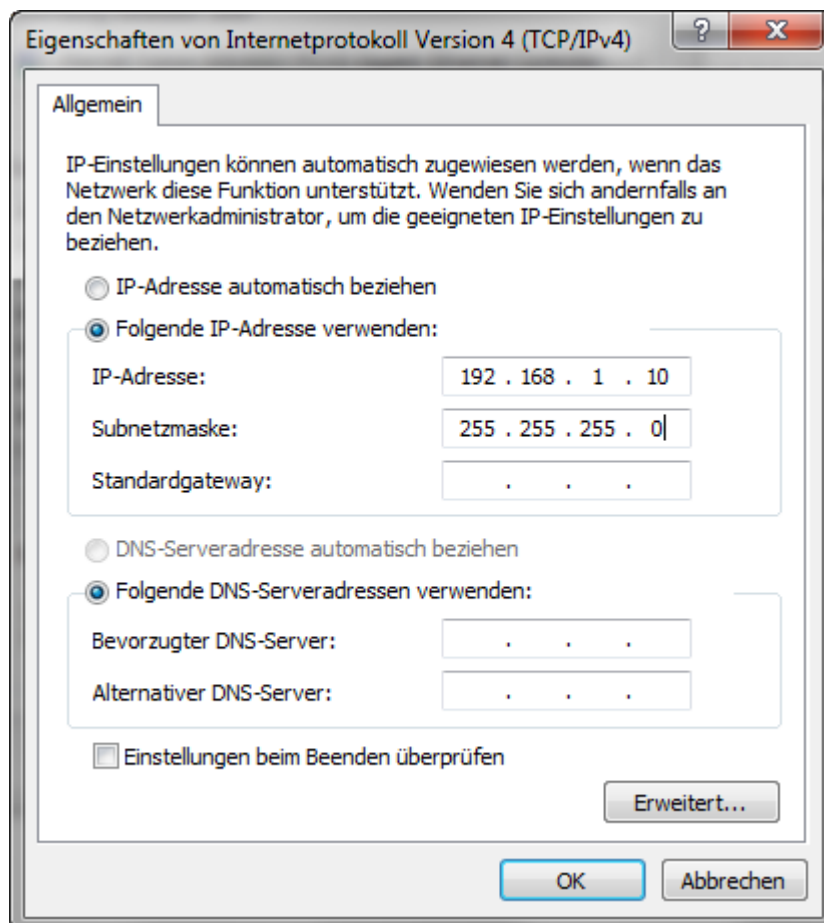
Hierfür müssen sich beide Geräte im gleichen IP Subnetz befinden. Gegebenenfalls muss hierfür die IP-Adresse des Computers auf eine IP-Adresse zwischen 192.168.1.1/24 - 192.168.1.254/24, Netzwerkmaske 255.255.255.0 geändert werden.



Hinweis:

Die Adresse 192.168.1.60 ist bereits für die SEPPmail Appliance reserviert. Dies ist die Standard IP-Adresse im Auslieferungszustand.

Beispiel einer entsprechenden Netzwerkeinstellung anhand der Windows Oberfläche



Das weitere Vorgehen ist im Punkt [Login als Administrator](#) ^[143] beschrieben.

4.5.1.1.3 Consolen Login

Ist die SEPPmail Appliance fertig hochgefahren, so erscheint ein Login Prompt:

```
*** Starting SEPPmail system ***
Nologin-Ifconfig-Hostname-Route-Nameserver-Clock-Syslog-Cluster-Logrotate-vmtool
s-LDAP-License-Comment-Templates-Ruleset-Proxy-MPKIPProxy-OCSPcheck-Loadbalance-s
nmp-nrpe-Fetchmail-GUI-Statistics-Backup-Firmware-ImportIdif-Restore-ExternalCA-
CA-Webmail-keyserver-Postfix-Daemons-done

*****
***   INITIAL SETUP: Login with admin/admin to set a temporary IP address   ***
*****

OpenBSD/i386 (smtp.securemail.local) (ttyC0)

login: _
```

Nach dem Anmelden mit

Standard-Benutzername: admin
Standard-Kennwort: admin

wird zur Eingabe der IP-Adresse (in diesem Beispiel 172.16.161.50) aufgefordert

```
*****
***   You can now enter basic network settings. These settings are           ***
***   only temporary: You must access the Web GUI and adjust them           ***
***   under 'system' to make them permanent.                               ***
*****

Enter an IP address (e.g. 192.168.1.60): _
```

Weiterhin ist das Subnetz (in diesem Beispiel 255.255.255.0) und Gateway Adresse (in diesem Beispiel 172.16.161.1) einzugeben

```
*****
***   You can now enter basic network settings. These settings are           ***
***   only temporary: You must access the Web GUI and adjust them           ***
***   under 'system' to make them permanent.                               ***
*****

Enter an IP address (e.g. 192.168.1.60): 172.16.161.50
Enter a network mask (e.g. 255.255.255.0): 255.255.255.0
Enter the default gateway (e.g. 192.168.1.1): 172.16.161.1_
```



Hinweis:

Im Standard bezieht die Appliance initial dynamisch eine IP Adresse - ausschließlich (!) - auf „Interface 1“ (siehe [IP Addresses](#)²²³⁾).

Somit ist die Administrationsoberfläche gegebenenfalls auch ohne die oben genannte Consolen Eingabe zu erreichen.

Dies ist meist bei der Installation in Cloud-Umgebungen von Interesse.

Abschließend wird die URL für das Administrator Login angezeigt:

```
IP Address for interface vic0 set to 172.16.161.50/255.255.255.0, gateway set to
172.16.161.1

*****
***  You should now be able to access the device with your browser:  ***
***  https://172.16.161.50:8443                                     ***
*
*****

OpenBSD/i386 (SECUREMAIL.) (ttyC0)

login: _
```

Nun ist das Web-Administrationsportal der SEPPmail Appliance - bis zum Reboot - über die angezeigte URL im Browser zu erreichen (siehe [Login als Administrator](#) ¹⁴³).

Bei Bedarf kann das „Initial network setup“ erneut über die [Rudimentären Systembefehle](#) ¹⁸⁹ aufgerufen werden.

4.5.1.2 Login als Administrator

Sämtliche Verwaltungsmöglichkeiten der SEPPmail Appliance stehen über eine Webbrowser basierte Konfigurationsoberfläche zur Verfügung.

Im Auslieferungszustand kann die Konfigurationsoberfläche wie folgt erreicht werden:

- Hardware Appliance
 - über CrossOver Kabel oder Hub via
 - LAN1 - <https://192.168.1.60:8443>
 - LAN2 - <https://192.168.2.60:8443>
- virtuelle und Hardware Appliances
 - bei welchen die IP-Adresse über die Console geändert wurde:
 - LAN1 - <https://<Ihre temporär vergebene IP>:8443>
 - bei welchen die IP-Adresse dynamisch bezogen wurde:
 - LAN1 - <https://<dynamische IP>:8443>

Der Standard-Benutzername lautet: admin
Das Standard-Kennwort lautet: admin



Hinweis:

Erst durch das Registrieren der SEPPmail Appliance wird eine temporäre, 30-tägige Testlizenz bezogen beziehungsweise eine bereits vorhandene Kauflizenz aktiviert. (siehe [Das System registrieren](#) ¹⁴⁶).

Nach erfolgreichem Registrierungsprozess verschwindet die Meldung **No valid license found - Please obtain a valid license.**

Bei Aufruf der Konfigurationsoberfläche im Webbrowser erscheint eine Warnung, dass die Webseite unsicher sei. Der Aufruf der Seite muss trotz dieser Meldung fortgesetzt werden.



Hinweis:

Die Meldung erscheint in der Regel nur bis ein gültiges SSL Zertifikat installiert wurde (siehe Menüpunkt [SSL](#) ³¹⁹).

4.5.1.3 Netzwerkeinstellungen der SEPPmail Appliance

Um die Netzwerkparameter der SEPPmail Appliance persistent zu konfigurieren, müssen diese in der Konfigurationsoberfläche unter dem Menüpunkt **System** eingetragen und gesichert werden, es sei denn die Option **Virtualisation tools** **Microsoft Azure** **Enable Microsoft Azure guest agent** wäre aktiv.

In der **Sektion IP addresses**

ist für das **Interface 1** die IP-Adresse und die zugehörige Subnetzmaske gemäß des vorhandenen Netzwerkes einzugeben



Hinweis:

Die Definition der Netzmaske wird nach der Classless Inter-Domain Routing (CIDR) Notation festgelegt.

- Die Netzmaske 255.255.255.255 entspricht „/32“ (einzelne IP-Adresse)
- Die Netzmaske 255.255.255.0 entspricht „/24“ (Klasse-C Netzwerk)
- Die Netzmaske 255.255.0.0 entspricht „/16“ (Klasse-B Netzwerk)
- Die Netzmaske 255.0.0.0 entspricht „/8“ (Klasse-A Netzwerk)

In der **Sektion Name**

sind die Felder **Hostname** und **Domain** zu füllen.

Dabei ist der Hostname frei wählbar, zum Beispiel securemailgateway. Der Domain-Name entspricht der DNS-Domäne, in welcher sich die Appliance befindet (zum Beispiel meinefirma.local oder ihredomain.com).

Diese Einstellungen sind die interne Sicht, sie müssen also nicht den Daten, wie sie vom Internet her Gültigkeit hätten, entsprechen.

In der **Sektion DNS**

kann zwischen dem Verwenden der Root-DNS-Server im Internet (**Use built-in DNS resolver**) oder eines explizit anzugebenden DNS-Server gewählt werden (**Use the following DNS servers**)

Wird die Einstellung **Use built-in DNS resolver** verwendet, kann das Auflösen von Namen unter Umständen etwas länger dauern, wodurch die Performanz des Systems beeinträchtigt werden kann.

Bei Angabe eines DNS-Servers (**Primary**) ist darauf zu achten, dass dieser auch Domänen Namen im Internet auflösen kann. Falsche Einträge können zu einem sehr langsamen Antwortverhalten der Konfigurationsoberfläche sowie Problemen bei der Kommunikation mit Drittsystemen führen. Über die Eingabefelder **Alternate 1** und **Alternate 2** können bei Bedarf weitere, alternative DNS-Server eingegeben werden. Dadurch würde bei Ausfall des **Primary** Servers würde der **Alternate 1** übernehmen, sollte auch dieser ausfallen der **Alternate 2**.

In der **Sektion Routing**

wird das zum Subnetz passende **Default gateway** eingetragen. Diese Eingabe wird benötigt um Netze außerhalb des Eigenen zu erreichen.

Die Eingaben sind abschließend über die Schaltfläche **Save** zu sichern.

4.5.1.4 Netzwerkkonfiguration prüfen

Um sicherzustellen, dass die vorgenommenen Netzwerkeinstellungen der SEPPmail Appliance korrekt sind, ist in der Konfigurationsoberfläche **Administration** ³⁶⁹ **Update** ³⁶⁹ auf **View release notes** zu klicken.

Falls eine der beiden folgenden Meldungen erscheint,

- **You already have the latest version installed**
- **There is a new version available: Installed version is alteVersionsnummer, latest version is neueVersionsnummer**

war die Netzwerkkonfiguration erfolgreich.

Erscheint die Meldung

- **ERROR: unable to connect to update server. Make sure that the device can make connections to the internet on port 22.**

ist eine Verbindung in das Internet über Port TCP/22 (SSH) nicht möglich. Die Netzwerkeinstellungen der SEPPmail Appliance sowie die Firewall- beziehungsweise Router-Einstellungen sind erneut zu prüfen (siehe **Firewall / Router einrichten** ¹³⁵).

Rudimentäre Netzwerkfunktionen für Basistests, stehen gegebenenfalls auch über das Command Line Interface (CLI) zur Verfügung (siehe **Rudimentäre Systembefehle** ¹⁸⁹).

4.5.1.5 Das System registrieren

Das Registrieren der SEPPmail Appliance erfolgt im Web-Administrationsportal unter **Administration**  **License and registration**  durch Klicken von **Register this device...**.

Mit dem Registrieren

- virtueller Appliances
 - wird bei Eingabe des **Activation code**  am Ende der Registrierungsseite eine Kauflizenz aktiviert. Der **Activation code**  entspricht der Device ID (xxxx-xxxx-xxxx) auf dem „**SEPPmail License Certificate**“.
 - wird ohne Eingabe des **Activation code**  am Ende der Registrierungsseite automatisch eine 30-tägige Testlizenz bezogen
- von Hardware Appliances wird die Lizenz aktiviert. Die Eingabe eines **Activation code**  ist weder erforderlich noch möglich.

Erscheint die Meldung **Registration successful**, so wurde der Registrierungsprozess erfolgreich abgeschlossen.

4.5.2 Das System auf den neusten Stand bringen

In **Administration**  **Update**  sind die verschiedenen Update Optionen zu finden.

Ist die SEPPmail Appliance bereits auf dem aktuellen Stand, so ist die Meldung

You already have the latest version installed

zu sehen. Andernfalls wird die aktuell auf der SEPPmail Appliance installierte, sowie die auf dem Update-Server bereitgestellte Version angezeigt

There is a new version available: Installed version is <alteVersionsnummer>, latest version is <neueVersionsnummer>

In diesem Fall ist die Appliance so oft über die Schaltfläche **Perform update (reboot automatically)** zu aktualisieren, bis die Meldung „**You already have the latest version installed**“ erscheint. Durch erneutes Klicken auf **Perform update (reboot automatically)** wird gegebenenfalls der Update-Fortschritt in % angezeigt.

Nach jedem Update erfolgt ein Neustart der SEPPmail Appliance.

4.5.3 Wichtige Sicherheitsmaßnahmen

In den kommenden Abschnitten werden folgende Sicherheitsmaßnahmen beschrieben:

- [Ändern des Administrator-Passworts](#) ^[148]
- [Festlegen des HTTPS-Protokolls für den sicheren Zugriff auf die Appliance](#) ^[149]
- [Erstellen eines Backup Users zur regelmäßigen Sicherung der Appliance](#) ^[150]
- [Eingabe der Postmaster Adresse für den Empfang von Systemmeldungen](#) ^[151]

4.5.3.1 Administrator Kennwort ändern

Aus Sicherheitsgründen sollte das Kennwort des Benutzers „admin“ unbedingt geändert und auf einen entsprechend komplexen Wert gesetzt werden.

Das Ändern des Passwortes kann sowohl über [Login](#) ^[219] [Change password](#) ^[219] als auch in den Benutzerdetails des Benutzers „admin“ (siehe [Users](#) ^[396]) erfolgen (siehe [USER 'USER@DOMAIN.TLD'](#) ^[396] [User data](#) ^[396] [Password](#) ^[396]).

4.5.3.2 Festlegen des HTTPS Protokolls für den sicheren Zugriff zum System

In **System** sind nach dem Klicken von **Advanced view** weitere Konfigurationsoptionen sichtbar. In den Sektionen **Admin GUI** und **GINA GUI** werden die Zugriffsoptionen auf die Appliance (**HTTP** oder **HTTPS**) eingestellt.

Aus Sicherheitsgründen wird empfohlen, die Option **HTTP** zu deaktivieren und sowohl für die Konfigurationsoberfläche wie auch für den Zugriff auf das/die GINA-Domain(s) nur **HTTPS** zuzulassen. Das ungesicherte **HTTP**-Protokoll sollte nur dann zum Einsatz kommen, wenn bereits eine vorgelagerte Komponente den SSL Tunnel terminiert und die Verbindung zwischen dieser Komponente und der SEPPmail Appliance über ein gesichertes Netzwerk stattfindet.

4.5.3.3 Backup Benutzer erstellen

Der Backup Prozess der SEPPmail Appliance erstellt täglich automatisiert eine Sicherung. Für die Funktion dieses Prozesses sind zwei Schritte notwendig:

1. Backup Kennwort setzen

Da die Backups der Appliance grundsätzlich verschlüsselt werden, ist die Eingabe eines Backup Kennwortes zwingend. Das Setzen erfolgt unter **Administration**  **Backup**  mittels **Change password**.

2. Zuordnen eines Users zur Gruppe Backup

Nach dem automatischen Erstellen des Backups wird dieses an alle Mitglieder der Gruppe Backup gesendet. Das Zuordnen von Benutzern zu dieser Gruppe erfolgt über **Groups**  **backup (Backup operator)**  über die Schaltfläche **Edit...**.

Soll für diesen Zweck ein eigener Benutzer angelegt werden, so ist darauf zu achten, dass dieser eine gültige E-Mail Adresse in der, beziehungsweise einer der internen E-Mail Domänen besitzt. Das Ziehen einer Verschlüsselungslizenz für diesen Benutzer kann gegebenenfalls durch aktivieren der Optionen **May not encrypt mails**  und **May not sign mails**  unterbunden werden (siehe **USER 'USER@DOMAIN.TLD'**  **User Data** .

4.5.3.4 Eingabe der Postmaster Adresse für den Empfang von Systemmeldungen

Damit Systembenachrichtigungen der SEPPmail Appliance (Watchdog Meldungen) versendet werden können, ist die Eingabe einer entsprechenden E-Mail Adresse für den Empfang dieser Meldungen unter **Mail System** ^[247] **SMTP settings** ^[252] **Postmaster address** ^[253] erforderlich.

4.5.3.5 Ruleset generieren

Damit die SEPPmail Appliance ihren Dienst aufnehmen kann, ist ein Ruleset zu generieren. Das Standard Ruleset wird durch Klicken von **Generate ruleset** unter **Mail Processing**  **SMTP ruleset**  erzeugt und kann bei Bedarf im Nachgang im **Ruleset generator**  noch individualisiert werden.

4.6 Vorbereiten der GINA-Technologie

Um auch mit Kommunikationspartnern, welche selbst über kein Schlüsselmaterial verfügen sicher kommunizieren zu können, kommt die GINA-Technologie zum Einsatz.

Für das initiale Einrichten dieses Verfahrens ist zunächst die Erreichbarkeit der SEPPmail Appliance aus dem Internet - in der Regel per SSL Port 443 (siehe [Firewall / Router einrichten](#)^[135]) - zu gewährleisten.

Weiterhin sollte auf der SEPPmail Appliance ein gültiges SSL Zertifikat einer akkreditierten Certification Authority (CA) eingebunden sein (siehe [SSL](#)^[319]).

Die eigentlichen Einstellungen für das GINA-Web-Interface sind über [GINA Domains](#)^[416], beziehungsweise [CHANGE GINA SETTINGS FOR](#)^[423] vorzunehmen.

4.7 Integration in die bestehende E-Mail Infrastruktur

Die Basis-Einrichtung der SEPPmail Appliance ist mit dem Abarbeiten der vorangegangenen Punkte abgeschlossen.

Für eine Minimalkonfiguration zum Austausch sicherer E-Mails sind die, in den folgenden Punkten beschriebenen weiteren Schritte notwendig.

4.7.1 Zu verwaltende E-Mail Domänen einrichten

Die E-Mail Domänen auf welche die neue SEPPmail Appliance reagieren soll, sind unter **Mail System**^[247] **Managed domain**^[247] durch Klicken von **Add managed domain...** einzugeben.

Im Folgemenü **ADD MANAGED DOMAIN**^[266] wird unter **Settings**^[266] **Domain name**^[266] der Name der E-Mail Domäne eingegeben.

Als **Forwarding server**^[266] wird in der Regel der Groupware-Server angegeben, an welchen die E-Mails intern weitergeleitet werden.

Die Einstellung **S/MIME domain keys**^[274] ist abhängig von der globalen Einstellung des übergeordneten Menüs. Mit dieser Einstellung wird über die Teilnahme am **Managed Domain Service**^[31] entschieden.

Mit **GINA domain**^[270] wird die für diese **Managed domain**^[247] zu verwendende GINA-Seite gewählt. Da zum Zeitpunkt des Ersteinrichtens ausschließlich die [default] GINA existent ist, sollte die Einstellung zunächst so belassen werden und kann bei Bedarf im Nachgang geändert werden.

4.7.2 Ausgehenden E-Mail Verkehr steuern

Das Abgeben der ausgehenden E-Mails in das Internet wird in der Regel global unter **Mail System**^[247] **Outgoing server**^[250] gesteuert. Soll die SEPPmail Appliance E-Mails direkt an externe E-Mail Empfänger im Internet abgeben, so ist die Option **Use built-in e-mail transport agent**^[250] zu wählen. Sollte an ein vorgelagertes System weitergeleitet werden, so ist die Option **Use the following SMTP server**^[250] zu wählen. Dann ist unter **Server name**^[250] der entsprechende Name oder die IP-Adresse dieses Systems einzutragen. Erfordert dieses System eine Authentifizierung, so ist der erforderliche Benutzername unter **User ID**^[250] und das Kennwort unter **Password**^[250] einzugeben.



Hinweis:

Bei Verwenden der Einstellung **Use built-in e-mail transport agent**^[250] wird dringend empfohlen das optionale **Protection Pack**^[106] zu lizenzieren und aktivieren, sofern für den eingehenden E-Mail Verkehr nicht etwa ein externer AntiSpam-Dienst vorgeschaltet ist. Andernfalls ist mit erheblichen Beeinträchtigungen, bis hin zum Erliegen des Mailflusses durch SPAM-Attacken zu rechnen (siehe auch **Kleine Umgebungen**^[81]).

4.7.3 Mail Relaying

Damit das interne Groupware System in der Lage ist, ausgehende E-Mails an die SEPPmail Appliance abzugeben, ist die IP-Adresse des, beziehungsweise unter Umständen auch das Netz in dem die Groupware-Server stehen zu berechtigen.

Dies erfolgt durch den Eintrag der IP(s) beziehungsweise des oder der Netze in die dafür vorgesehenen Felder unter **Mail System**^[247] **Relaying**^[254].

4.7.4 SSL Zertifikat einbinden

Das erforderliche Vorgehen ist im Kapitel des Menüpunktes **SSL** ³¹⁹ beschrieben. Die folgenden Seiten liefern lediglich eine Kurzbeschreibung zur Inbetriebnahme.

4.7.4.1 SSL Zertifikat selbst erstellen

Die SEPPmail Appliance ermöglicht es, ein eigenes SSL Maschinen oder Wildcard Zertifikat über die Konfigurationsoberfläche zu erstellen. Für eine Testinstallation ist es nicht zwingend erforderlich ein kostenpflichtiges SSL Zertifikat zu beschaffen. Das Zertifikat kann auf der SEPPmail Appliance automatisch generiert und signiert werden.

Hierfür ist in das Menü **SSL** ³¹⁹ zu wechseln und die Schaltfläche **Request or create new certificate...** zu klicken.

Im erscheinenden Menü sind die hier aufgeführten Felder zwingend auszufüllen:

Sektion **Issue to** ³²²

Parameter	Beschreibung
Name or IP (CN)	IP-Adresse oder Hostname unter welchem die SEPPmail Appliance aus dem Internet erreichbar ist. Bei einem selbst signierten Zertifikat muss der hier angegebene Werte dem Namen in der URL entsprechen unter der die SEPPmail Appliance angesprochen wird. Beispiel: Soll die SEPPmail Appliance unter der URL https://securewebmail.example.tld angesprochen werden, so lautet der im Feld Name or IP (CN) anzugebende Hostname securewebmail.example.tld. beziehungsweise *.example.tld sofern ein Wildcard Zertifikat erstellt werden soll.
E-Mail	Eine gültige E-Mail Adresse innerhalb der Firma, unter der eine zuständige Person erreicht werden kann.
Country (C)	Land, in dem die Organisation ihren Sitz hat.

Sektion **Attributes** ³²³

Parameter	Beschreibung
Key size (bits)	In der Regel ist die maximale Schlüssellänge zu wählen um den aktuellen Sicherheitsstandards zu entsprechen.
Signature	Für das Erstellen eines selbst signierten Zertifikates ist Create self-signed certificate auszuwählen.

Um das Erstellen des SSL Zertifikats auszuführen, ist auf die Schaltfläche **Create** zu klicken. Mit dem Rückmelden folgender Zertifikatsdetails

- die Seriennummer des Zertifikats (**Serial No.**)
- die Gültigkeitsdauer (**Validity**)
- den Fingerprint (**SHA1 Fingerprint**)

ist der Vorgang abgeschlossen.

**Hinweis:**

Auch das Erstellen eines **Wildcard oder SAN (Subject Alternate Name) SSL Zertifikats** ist möglich. Wildcard Zertifikate gelten nicht nur für einen dedizierten Host sondern können für mehrere Hosts einer Domäne verwendet werden. SAN Zertifikate hingegen können mehrere Hostnames enthalten.

Beispiel:

Ein SSL Zertifikat mit dem Namen GINAtest.testdomain.tld kann nur für diesen einen Host verwendet werden. Andernfalls wird eine Zertifikatsfehlermeldung im Webbrowser angezeigt. Ein Wildcard SSL Zertifikat kann auf beliebigen Hosts einer Domäne verwendet werden, zum Beispiel GINAtest.testdomain.tld, webmail.testdomain.tld oder secmail.testdomain.tld.

Um ein Wildcard SSL Zertifikat zu erzeugen, geben Sie den Hostnamen mit einem führenden Stern „*“ ein, zum Beispiel „*.testdomain.net“.

Detaillierte Informationen sind unter [REQUEST OR CREATE NEW CERTIFICATE \(AUTHORITY\)](#)  zu finden.

4.7.4.2 Bestehendes SSL Zertifikat einbinden

Für den produktiven Betrieb der SEPPmail Appliance inklusive GINA-Technologie empfiehlt sich dringend das Verwenden eines trusted SSL Maschinen- oder Wildcard- Zertifikates für den SSL gesicherten Zugriff auf das GINA-Web-Mail System.

Für das Einbinden eines gekauften trusted SSL Zertifikates ist in das Menü **SSL**  zu wechseln und die Schaltfläche **Import existing certificate...** zu klicken.

Im erscheinenden Menü ist in **Upload existing certificate**  das Einbinden auf zwei Arten - abhängig vom vorliegenden Zertifikatsformat (pem oder PKCS#12 also p12 oder pfx) - möglich.

Parameter	Beschreibung
PKCS12 file	Über die Internet-Browser Schaltfläche „Datei auswählen“ wird die PKCS#12-Datei (diese hat die Endung .p12 oder .pfx) ausgewählt.
PKCS12 password	Nachdem eine PKCS#12-Datei den Privaten Schlüssel enthält, ist diese Passwort geschützt. Das Passwort muss vor dem Import der oben ausgewählten PKCS#12-Datei in dieses Eingabefeld eingegeben werden.
PEM file	Über die Internet-Browser Schaltfläche „Datei auswählen“ wird die PEM-Datei (diese hat auch die Endung .pem) ausgewählt.  Achtung: Bei Import einer PEM Datei ist darauf zu achten, dass der darin enthaltene Private Schlüssel nicht in verschlüsselter Form vorliegt!
PEM text	In dieses Feld wird sowohl der Private, als auch der Öffentliche Schlüssel und gegebenenfalls die Intermediate Zertifikate als Text eingefügt. Falls der Private Schlüssel durch ein Kennwort geschützt ist, muss dieses zuvor entfernt werden. Die Eingabe sollte demnach in etwa so aussehen: <pre>-----BEGIN PRIVATE KEY----- # Privater Schlüssel -----END PRIVATE KEY----- -----BEGIN CERTIFICATE----- # Öffentlicher Schlüssel -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- # Eventuell benötigtes Zwischenzertifikat -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- # Eventuell weitere benötigte Zwischenzertifikate -----END CERTIFICATE-----</pre>

Hinweis:

Egal welche Methode für den Import der SSL Schlüsselpaars zum Einsatz kommt, ist immer darauf zu achten, dass alle notwendigen Zwischenzertifikate für eine vollständige Zertifikatskette beinhaltet sind. Eine unvollständige Zertifikatskette führt beim Prüfen der Zertifikate durch die Gegenstelle immer dann zu Problemen, wenn dieser die fehlenden Zwischenzertifikate nicht bereits bekannt sind. Internet-Tools - wie zum Beispiel CheckTLS - zeigen dann, dass die Zertifikatskette nicht vollständig ist und melden somit ein unbekanntes Zertifikat.

Das Wurzel-Zertifikat der Stammzertifizierungsstelle darf nicht mit hinzugefügt werden, da die Gegenstelle diesem ohnehin vertrauen muss! Wird es dennoch hinzugefügt, melden einige Prüfwerkzeuge Fehler wie etwa „Chain issues - Contains anchor“.

Nicht jede PKCS12- beziehungsweise PEM-Datei enthält die komplette Zertifikatskette. In diesem Fall müssen die benötigten Zwischenzertifikate gegebenenfalls anderweitig besorgt und in das zu importierende Zertifikat eingebettet werden.



Über die Schaltfläche **Upload key and certificate** wird das SSL Zertifikat in die Appliance hochgeladen.

Detaillierte Informationen sind unter **REQUEST OR CREATE NEW CERTIFICATE (AUTHORITY)**  zu finden.

4.7.4.3 SSL Zertifikat von einer öffentlichen Zertifizierungsstelle anfordern

Für den produktiven Betrieb der SEPPmail Appliance inklusive GINA-Technologie empfiehlt sich dringend das Verwenden eines trusted SSL Maschinen- oder Wildcard- Zertifikates für den SSL gesicherten Zugriff auf das GINA-Web-Mail System.

Für das Anfordern und anschließende Einbinden eines gekauften trusted SSL Zertifikates ist in das Menü **SSL** ^[319] zu wechseln und die Schaltfläche **Request or create a new certificate...** zu klicken.

Im erscheinenden Untermenü **REQUEST OR CREATE NEW CERTIFICATE** ^[322] sind die hier aufgeführten Felder zwingend auszufüllen:

Sektion **Issue to** ^[322]

Parameter	Beschreibung
Name or IP (CN)	IP-Adresse oder Hostname unter der die SEPPmail Appliance aus dem Internet erreichbar ist. Bei einem selbstsignierten Zertifikat muss der hier angegebene Werte dem Namen in der URL entsprechen unter der die SEPPmail Appliance angesprochen wird. Beispiel: Soll die SEPPmail Appliance unter der URL https://securewebmail.example.tld angesprochen werden, so lautet der im Feld Name or IP (CN) anzugebende Hostname securewebmail.example.tld. beziehungsweise *.example.tld sofern ein Wildcard Zertifikat erstellt werden soll.
E-Mail	Eine gültige E-Mail Adresse innerhalb der Firma, unter der eine zuständige Person erreicht werden kann.
Country (C)	Land, in dem die Organisation ihren Sitz hat.

Sektion **Attributes** ^[323]

Parameter	Beschreibung
Key size (bits)	In der Regel ist die maximale Schlüssellänge zu wählen um den aktuellen Sicherheitsstandards zu entsprechen.
Signature	Für das Anfordern eines trusted SSL Zertifikat ist Create certificate signing request auszuwählen.

Um ein Schlüsselpaar zu erzeugen und den Antrag auf Signieren des öffentlichen Schlüssels (certificate signing request, kurz CSR) zu erstellen, ist **Create** zu klicken. In der grünen Statusleiste oben im Menü erscheint nun **Certificate request created** und das Folgemenü **CERTIFICATE SIGNING REQUEST (CSR)** ^[324] öffnet. Dort sind die zuvor gemachten Eingaben unter **Details** ^[324] und der generierte CSR unter **Request** ^[324] zu sehen.

Nach dem Hochladen des CSR zur Zertifizierungsstelle und dem anschließenden Erhalt des Zertifikates durch diese, kann das Zertifikat in die Appliance hochgeladen werden. Wurde zwischenzeitlich das Menü gewechselt, so gelangt man durch Wechseln in **SSL** ^[319] und anschließendem Klicken der Schaltfläche **Download and import signed certificate...**, wieder in das Sub-Menü für den Zertifikatsimport. Dieser erfolgt durch Einfügen des/der Zertifikat/e (siehe **Hinweis**) unter **Import** ^[324] und abschließenden Klicken von **Import certificate**.

**Hinweis:**

Falls oben in der Statusleiste des Menüs die gelb hinterlegte Information **Remember to import the signed certificate** angezeigt wird, so wurde zuvor bereits ein Zertifikatsantrag erstellt.

Das neu erstellte SSL Zertifikat sollte zusammen mit den gegebenenfalls zusätzlich benötigten Zwischen- oder auch Intermediate-Zertifikate(n) zur Stammzertifizierungsstelle oder auch Root CA in der Reihenfolge

1. Public Key des eigenen SSL Maschinen Zertifikats
2. Public Key von einer oder mehreren Zwischen-Zertifikaten

eingefügt werden. Das Wurzel-Zertifikat der Stammzertifizierungsstelle darf nicht mit eingefügt werden.

Im Fehlerfall ist das SSL Maschinen Zertifikat nicht zu nutzen. Ebenfalls kann dies zu Problemen beim Zugriff auf die Konfigurationsoberfläche führen. Für diesen Fall sollte sicherheitshalber vor dieser Aktion temporär der HTTP Port über **System**^[224] **Advanced view** **Admin GUI**^[230] **HTTP port**^[230] für den Zugriff auf die Administrationsoberfläche (<http://<Appliance>:8080>) freigegeben werden.

Um das neue SSL Zertifikate zu aktivieren ist ein Neustart der SEPPmail Appliance - zum Beispiel über die Schaltfläche **Reboot...**, welche unter **Administration**^[369] **Maintenance**^[370] **Reboot**^[372] zu finden ist - erforderlich.

Detaillierte Informationen sind unter **REQUEST OR CREATE NEW CERTIFICATE (AUTHORITY)**^[322] zu finden.

4.7.5 E-Mail Datenfluss umstellen

Um den sicheren E-Mail Verkehr mit der SEPPmail Appliance zu ermöglichen, müssen folgende Änderungen am bestehenden E-Mail Server vorgenommen werden:

In das Internet:

1. SEPPmail Appliance als Smarthost definieren

Die SEPPmail Appliance wird nach dem Integrieren in die bestehende E-Mail Umgebung die Rolle eines SMTP-Gateways übernehmen. Der E-Mail Server übermittelt somit E-Mails nicht mehr direkt nach extern, beziehungsweise an das gegebenenfalls bereits vorhandene SMTP-Gateway (zum Beispiel Spam-Filter), sondern (neu) nun an die SEPPmail Appliance.

Das Umstellen muss auf dem bestehenden E-Mail Server erfolgen, in dessen Konfiguration der interne **Name** ^[228] beziehungsweise **IP Address** ^[225] der SEPPmail Appliance als Smarthost eingetragen werden muss. Auf der SEPPmail Appliance sind die **Relaying** ^[254] Einstellungen zu beachten.

2. Autorisieren der SEPPmail Appliance für den E-Mail Versand

- a. Ist die SEPPmail Appliance direkt mit dem Internet verbunden, so sind die korrekten Firewall-beziehungsweise Router-Einstellungen zu gewährleisten (siehe Abschnitt **Firewall / Router einrichten** ^[135]).
- b. Ist der SEPPmail Appliance zum Internet hin noch ein weiterer Smarthost (zum Beispiel ein Spam-Filter) vorgeschaltet, so ist der interne Hostname beziehungsweise die IP-Adresse der SEPPmail Appliance auf diesem Smarthost in die Liste der autorisierten E-Mail Relay Systeme einzutragen. Die Appliance ist entsprechend einzustellen (siehe **Ausgehenden E-Mail Verkehr steuern** ^[155]).

Aus dem Internet:

3. Umstellen des MX-Eintrages

War der E-Mail Server bislang direkt mit dem Internet verbunden, so muss der vorhandene MX-Eintrag zukünftig nicht mehr auf den Hostnamen beziehungsweise die IP-Adresse des E-Mail Servers, sondern (neu) auf die SEPPmail Appliance zeigen.

4. Umstellen des Smarthost

Nimmt ein Smarthost die E-Mails aus dem Internet entgegen und leitete diese bislang direkt an den E-Mail Server weiter, so muss dieser die E-Mails zukünftig an die SEPPmail Appliance abgeben.



Achtung:

Mit dem Anpassen wird die SEPPmail Appliance in den E-Mail Datenfluss integriert. Alle E-Mails werden nach dem Umstellen an die SEPPmail Appliance gesendet.

Das Umstellen des E-Mail Datenflusses darf erst dann erfolgen, wenn alle anderen Konfigurationsschritte der SEPPmail Appliance abgeschlossen sind. Andernfalls ist eine Beeinträchtigung des E-Mail Verkehrs bis hin zum Erliegen desselbigen nicht ausgeschlossen.

4.7.6 Steuern der Appliance

Die von der Appliance durchzuführenden, gewünschten Aktionen - zum Beispiel Signieren und/oder Verschlüsseln - können als globale Aktion an der Appliance oder über vordefinierte Merkmale individuell am Client (siehe [Betreffzeilen Schlüsselwörter](#) ^[167], [Microsoft Outlook Vertraulichkeit](#) ^[166], [SEPPmail Microsoft Outlook Add-In](#) ^[167], gegebenenfalls auch [IBM Notes: Schaltfläche für verschlüsseltes Senden erzeugen](#) ^[739]) ausgelöst werden.

Auch ein automatisiertes Steuern kann bei Bedarf über fest definierte Regeln, zum Beispiel anhand von Absender- und/oder Empfänger Adressen und Domänen (siehe [ENCRYPTION POLICY](#) ^[313]) realisiert werden. Auch ein Gruppieren von Benutzern (siehe [Groups](#) ^[413]) ist zu diesem Zweck möglich. Weiterhin können über LDAP-Abfragen entsprechende Merkmale (Trigger) von Drittsystemen übernommen werden. Diese Optionen stehen über sogenannte **Custom commands** ^[264] des Menüs **Mail Processing** ^[286] der Sektion **Ruleset generator** ^[287] bereit.



Achtung:

Um auf der Appliance keine undefinierten Zustände zu erzeugen, sind entgegengesetzte Steuermerkmale unbedingt zu vermeiden!

Mit dem initialen in Betrieb nehmen der SEPPmail Appliance ist bereits ein vordefiniertes Regelwerk mit den entsprechenden Standard-Merkmalen (Trigger) für das Steuern der SEPPmail Appliance vorhanden. Die Konfigurationsmöglichkeiten für das Steuern der SEPPmail Appliance sind im Detail im unter **Mail Processing** ^[286] **Ruleset generator** ^[287] zu finden.



Achtung:

Für eine korrekte Funktion der Appliance, muss initial ein Ruleset generiert werden (siehe **Mail Processing** ^[286] **SMTP ruleset** ^[286] **Generate ruleset**, beziehungsweise **Ruleset generator** ^[287] **Save and create ruleset**).

4.7.6.1 Betreffzeilen Schlüsselwörter / (X-)Header

Das Verwenden von Betreffzeilen Schlüsselwörtern (siehe Tabelle 1) - welche bei Bedarf individuell angepasst werden können - gewährleistet die Unabhängigkeit vom eingesetzten E-Mail Client beim Steuern der Appliance. Ebenso können (X-)Header (ebenfalls Tabelle 1) für das Ansteuern von, auf der SEPPmail Appliance auszuführenden, Aktionen ausgewertet werden. Diese X-Header werden im Standard vom [SEPPmail Microsoft Outlook Add-In](#) ^[167] verwendet, können aber auch in anderen E-Mail Clients, wie etwa IBM Notes mittels angepasster Mail Schablonen (siehe auch [IBM Notes: Schaltfläche für verschlüsseltes Senden erzeugen](#) ^[739]) oder Novell Groupwise über Vorlagen gesetzt werden.

Betreffzeilen Schlüsselwort	(X-)Header / Wert	
[plain]	x-smpain / yes	Unterdrücken jeglicher kryptographischer Aktion.
[confidential]	sensitivity / companyconfidential x-smenc / yes	Auslösen des Verschlüsseln (Verschlüsselungshierarchie ^[667]).
[priv]	sensitivity / private x-smwebmail / yes	Auslösen des Verschlüsseln mittels GINA-Technologie (Stichwort Lesebestätigung)  Hinweis: Wird im E-Mail Client zusätzlich zum Erzwingen der GINA-Technologie eine Lesebestätigung (Disposition-Notification-To Header) angefordert, so wird über diese Technologie eine verlässliche Lesebestätigung angefordert. Das heißt der Empfänger kann das Auslösen dieser Lesebestätigung - anders als zum Beispiel

Betreffzeilen Schlüsselwort	(X-)Header / Wert	
		in MS-Outlook - nicht unterdrücken. Das SEPPmail Microsoft Outlook Add-in ^[167] fordert automatisch zur GINA-Technologie eine Lesebestätigung (Disposition-Notification-To Header) an.
[emptypw]		Unterdrücken der Notwendigkeit zur Eingabe eines Initialpasswortes bei GINA-Mails (Sicherheitstechnisch bedenklich)
[sms:<internationale Vorwahl><Mobilfunknummer>]		Optionale Angabe der Mobilfunknummer für das Übermitteln des Initialpasswortes einer GINA-E-Mail per SMS. Format: [sms:0041791234567] oder [sms:+41791234567]
[zip]		Versenden des verschlüsselten E-Mail Teils einer GINA-Mail im ZIP- anstatt im HTML-Format. Dies wird zum Beispiel benötigt, wenn der Empfänger Outlook Web Access (OWA) 2003 verwendet, da GINA-Mails im HTML-Format aus OWA 2003 nicht entschlüsselt werden können.
[noenc]	x-smnoenc / yes	Unterdrücken des Verschlüsseln der E-Mail, sofern „Verschlüsseln“ im Ruleset als Standard definiert wurde
[sign]	x-smsign / yes	Auslösen des Signierens der E-Mail.
[nosign]	x-smnosign / yes	Unterdrücken des Signierens der E-Mail, sofern „Signieren“ im Ruleset als Standard definiert wurde
[lfm]	x-smlfm / yes	Aktivieren des Large File Transfer (LFT) ^[107] , unabhängig von der E-Mail Größe*
[nolfm]		Unterdrücken des Large File Transfer (LFT) ^[107] , auch bei Überschreiten des eingestellten Schwellwertes (Size (in KiB) above which outgoing messages are treated as large files) ^[440] .

Tabelle 1

**Achtung:**

Das gleichzeitige Verwenden konkurrierender Schlüsselwörter und (X-)Header, als Trigger innerhalb einer E-Mail, kann in einem undefinierten Zustand enden und ist deshalb unbedingt zu vermeiden!

4.7.6.2 Microsoft Outlook Vertraulichkeit

Eine weitere Möglichkeit die SEPPmail Appliance zu steuern ist über die Vertraulichkeitseinstellung bei Microsoft Outlook.

Dabei wird die eingestellte Vertraulichkeit der E-Mail (siehe Abbildung 1 **roter Rahmen**) ausgewertet. Steht diese auf „**Vertraulich**“ so wird das Verschlüsseln der E-Mail angefordert (siehe [Verschlüsselungshierarchie](#) ^[66]).

Wird hingegen „**Privat**“ verwendet, so wird die GINA-Technologie erzwungen (siehe [Betreffzeilen Schlüsselwörter / X-Header](#) ^[99], Tabelle 1, Sensitivity Header). Damit mit der so erzwungenen GINA-Technologie die verlässliche Lesebestätigung einher geht, muss zusätzlich die Lesebestätigung (siehe Abbildung 1 **grüner Rahmen**) angefordert werden.

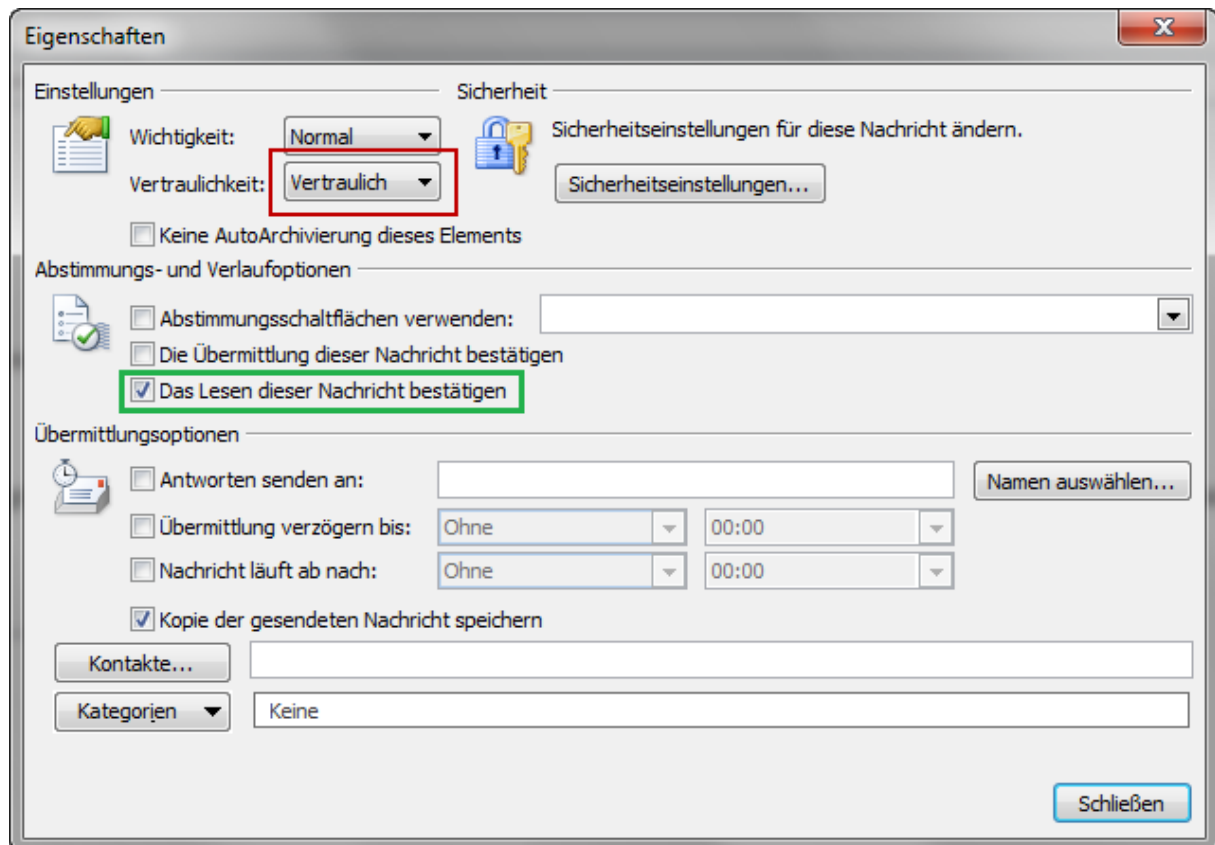


Abbildung 1

4.7.6.3 SEPPmail Microsoft Outlook Add-In

Um den Benutzerkomfort zu steigern steht für Microsoft Outlook das **SEPPmail Microsoft Outlook Add-In** ¹⁹⁰ zum kostenfreien Download unter <https://downloads.seppmail.com/index.php/outlook-plugin/>, beziehungsweise im Microsoft AppStore (<https://appssource.microsoft.com/>) bereit.

4.8 Clustern mehrerer Systeme

Dieses Kapitel beschreibt die grundsätzliche Funktionsweise von Clustern und zeigt die Möglichkeiten des Einbindens von SEPPmail Appliances auf.

Die SEPPmail Appliance verfügt über alle notwendigen Funktionen für ein eigenständiges Clustering und Loadbalancing. Natürlich ist das Einbinden in Infrastrukturen mit bereits vorhandenen externen Loadbalancern beziehungsweise Loadbalancing Verfahren ebenso möglich.

4.8.1 Allgemein

Ein Cluster bezeichnet einen Rechnerverbund aus mehreren vernetzten Computersystemen. Diese miteinander vernetzten Computersysteme sind zwar physisch getrennt, werden aber logisch als eine Einheit betrachtet. So ist es möglich, dass ein Cluster als ein einziges logisches System angesprochen werden kann, tatsächlich aber aus mehreren physikalischen Systemen besteht.

Das Einrichten beziehungsweise das Hinzufügen von Maschinen zu einem Cluster erfolgt - wie in „Abbildung 1“ dargestellt - im Menü **Cluster** ³⁸³.

Replikation der Cluster-Konfiguration

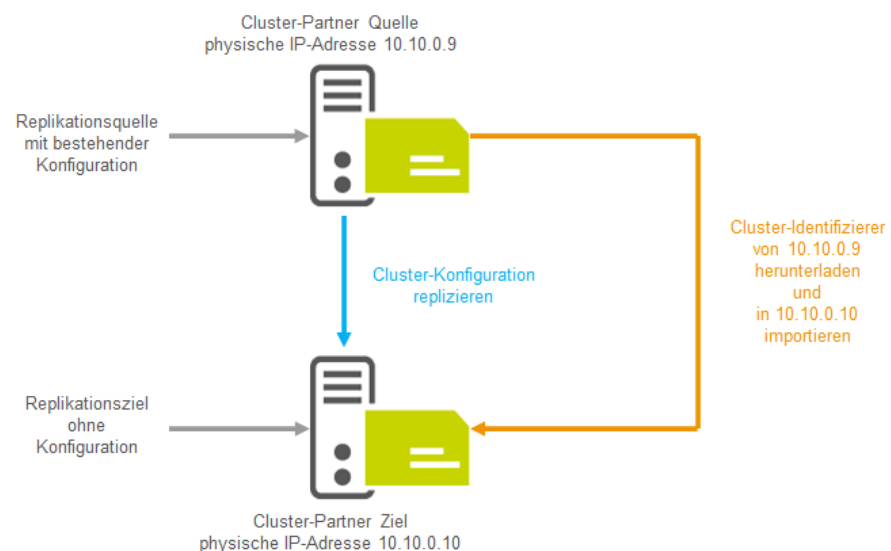


Abbildung 1 - Einrichten eines Clusters

Bei einem bestehenden Cluster synchronisieren alle Cluster-Mitglieder ihre Konfigurationsdatenbanken ohne merklichen Zeitverlust. Das heißt alle Cluster-Mitglieder sind gleichberechtigt. Konfigurationsänderungen werden somit sofort übernommen, egal an welchem cluster member sie vorgenommen werden (siehe „Abbildung 1.1“)

Replikation im Cluster

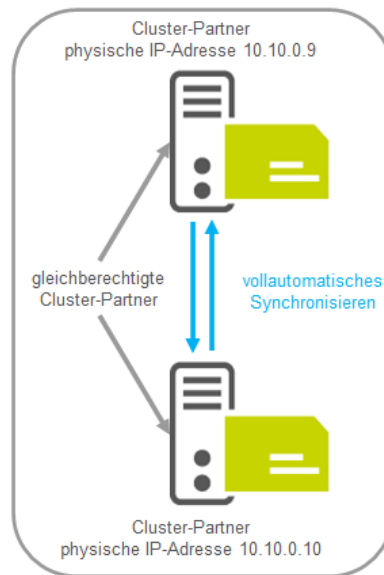


Abbildung 1.1 - Replikation im Cluster

Für das Einrichten beziehungsweise den Betrieb eines Clusters gibt es mehrere Beweggründe. Je nach Zielsetzung unterstützt die SEPPmail Appliance verschiedene Betriebsarten, welche wie folgt unterschieden werden:

1. **Hochverfügbarkeits-Cluster** ^[17]
Diese Art des Clusters dient dem Gewährleisten der Ausfallsicherheit
2. **Loadbalancing-Cluster** ^[17]
Ein Loadbalancing Cluster dient der Lastverteilung auf mehrere Maschinen. Dabei können unterschiedliche Verfahren zum Einsatz kommen.
3. **Geo-Cluster** ^[17]
Repliziert Konfigurationsdatenbanken auf geographisch voneinander getrennten Systemen.
4. **Frontend-/Backend-Cluster** ^[18]
Bei Frontend-/Backend-Clustern verfügt das Frontend-System über keine eigene Datenbank, sondern wird bei Bedarf vom Backend-System mit Daten gespeist. Somit kann die Frontend-Maschine in einer Demilitarisierten Zone (DMZ) betrieben werden, in welcher keine Datenhaltung erlaubt ist.
5. **Secure Web-Mail Satellite** ^[18]
Abtrennen der GINA-Technologie vom E-Mail verarbeitenden System (Stichwort DMZ-Struktur).
6. **Unterstützen externer redundanter Systeme** ^[18]

Dabei sind auch Kombinationen aus den verschiedenen Betriebsarten möglich.

Die zumeist benötigten virtuellen IP-Adressen (IP Alias Adressen) für das Ansprechen eines Clusters als logische Einheit ist in **System** ^[22] **Advanced View** **IP ALIAS addresses** ^[22] vorzunehmen.



Hinweis:

Virtuelle IP-Adressen dienen ausschließlich dem Ansprechen eines Clusters von außen. Wird eine E-Mail von einer Cluster-Maschine versandt, so geschieht dies immer mit der physikalischen IP-Adresse der jeweiligen Maschine.

**Hinweis:**

Beim Dimensionieren der Anzahl und Leistungsfähigkeit der Systeme in einem Cluster ist immer darauf zu achten, dass bei Ausfall eines Systems das oder die verbleibende(n) System(e) die dadurch entstehende Mehrlast verarbeiten kann/können.

4.8.2 Hochverfügbarkeits-Cluster

Die Ausfallsicherheit der SEPPmail Appliance kann durch das Bilden eines Clusters erhöht werden.

Die SEPPmail Appliance besitzt eine integrierte Cluster-Funktionalität auf Basis des CARP Protokolls (siehe auch http://de.wikipedia.org/wiki/Common_Address_Redundancy_Protocol).

Um einen Cluster zu bilden sind mindestens zwei SEPPmail Appliances erforderlich die sich gegenseitig überwachen. Fällt ein System aus beziehungsweise antwortet dieses nicht mehr auf Überwachungsanfragen, so übernimmt das zweite System dessen Funktion. Ist das ausgefallene System wieder verfügbar beziehungsweise es antwortet wieder auf Überwachungsanfragen, so übernimmt es wieder seine ursprüngliche Aufgabe.

Diese Funktion kann mit bis zu neun SEPPmail Appliances abgebildet werden, wodurch eine sehr hohe Ausfallsicherheit erreicht werden kann.

Ein Hochverfügbarkeits-Cluster kann sowohl mit SEPPmail Appliances auf Hardware Basis wie auch auf Basis von virtualisierten Appliances abgebildet werden. Ein Mischbetrieb beider Systeme ist ebenso möglich.

Funktion eines Hochverfügbarkeits-Clusters

Bei diesem Verfahren werden einem Cluster eine oder mehrere virtuelle IP-Adresse(n) mit verschiedenen Prioritäten zugeordnet. Jedes Cluster Member System hat unabhängig von der zugewiesenen virtuellen Cluster IP-Adresse eine jeweils eigene eindeutige IP-Adresse. Über diese eigene eindeutige IP-Adresse kann jedes Cluster Member System explizit angesprochen werden.

Beispiel:

In der folgenden Abbildung ist die virtuelle Cluster IP-Adresse des Clusters 10.10.0.1. Die Cluster Member Systeme haben in unserem Beispiel die IP-Adressen **10.10.0.9** und **10.10.0.10**.

Hochverfügbarkeits-Cluster

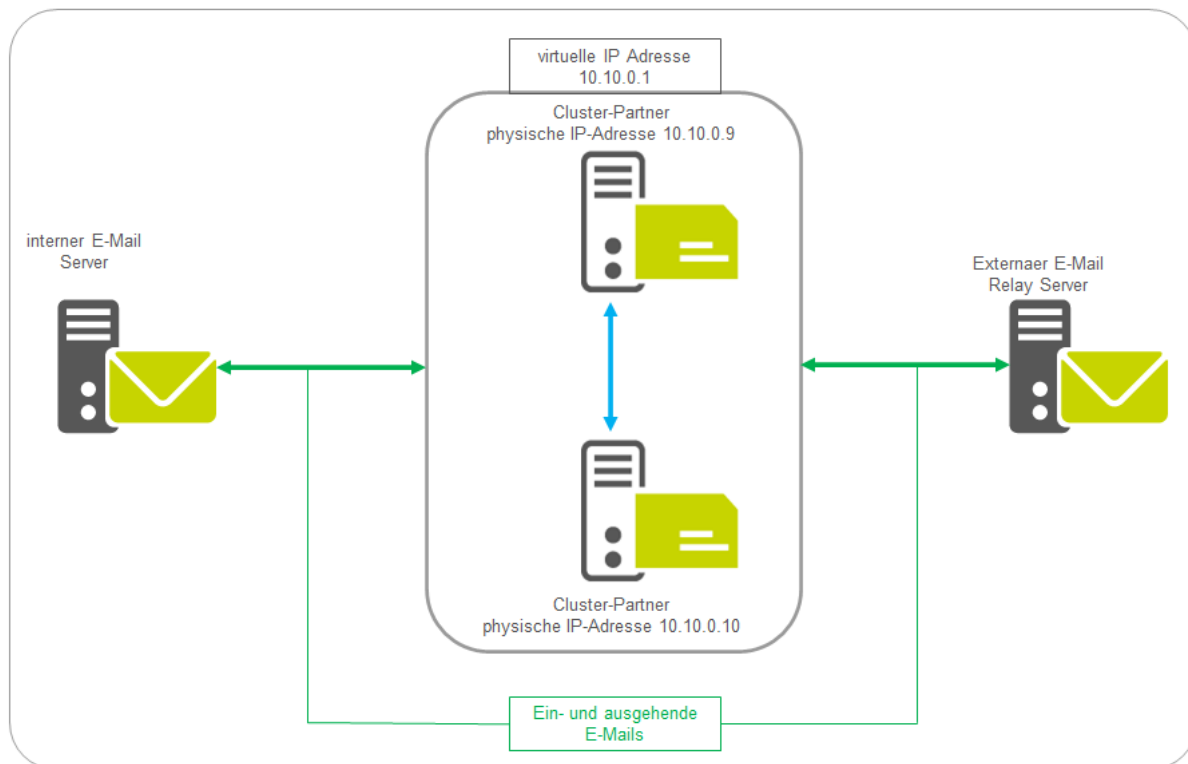


Abbildung 2 - Schematische Darstellung eines Hochverfügbarkeits-Clusters

Das Cluster selbst wird von anderen Systemen, zum Beispiel einem internen E-Mail Server oder einem vorgelagerten E-Mail Relay-Server (Gateway) über die eingerichtete(n) virtuelle(n) IP-Adresse(n) angesprochen. Im Beispiel oben ist das die IP-Adresse **10.10.0.1**.

Wird das Cluster selbst über seine Cluster IP-Adresse angesprochen, so reagiert immer das Cluster Member System mit der höchsten Priorität auf die angesprochene virtuelle Cluster IP-Adresse. Alle anderen Cluster Member Systeme mit niedrigerer Priorität reagieren nicht auf die virtuelle Cluster IP-Adresse, solange ein Cluster Member System mit einer höheren Priorität verfügbar ist.

Fällt das Cluster Member System mit der höchsten Priorität aus, so übernimmt automatisch ein Cluster Member System mit der nächst niedrigeren Priorität die virtuelle Cluster IP-Adresse inklusive der Funktion des ausgefallenen Cluster Member Systems.

Die Prioritäten sind in der folgenden Reihenfolge geordnet:

1. Primary
2. Secondary
3. Backup

Das Einrichten der Priorität des jeweiligen Cluster Member Systems ist in **System**  **Advanced view** **IP ALIAS addresses**  **Priority** vorzunehmen.

4.8.3 Loadbalancing Cluster

Ein Loadbalancing innerhalb eines Clusters kann durch mehrere Verfahren erreicht werden. Dabei bietet SEPPmail ein in die Appliance integriertes Verfahren an. Ebenso kann das Verteilen der Last auf die einzelnen Cluster Member eines SEPPmail Appliance Clusters durch externe Loadbalancer oder Loadbalancing Verfahren erfolgen. Die gängigsten werden an dieser Stelle aufgeführt:

- **Aufteilen des Ein- und Ausgehenden Verkehrs** ^[173]
auf je ein Cluster Member System. Das Abgeben von E-Mails an den/die anderen Cluster-Partner tritt dabei erst bei Erreichen eines entsprechenden Lastzustandes in Kraft.
- **Nutzen des DNS Round Robin Verfahrens** ^[175]
- **Nutzen eines externen Loadbalancers** ^[177]

Das Failover-Verhalten des Clusters wird durch diese Konfigurationen nicht verändert.

4.8.3.1 Aufteilen des Ein- und Ausgehenden Verkehrs

Das Aufteilen des ein- und ausgehenden E-Mail Datenflusses erfolgt - wie in „Abbildung 3“ dargestellt - durch eine statische Konfiguration, in welcher neben den physikalischen IP-Adressen der Appliances mit zwei weiteren, virtuellen IP-Adressen (IP Alias Addresses) gearbeitet wird. Dabei existieren zwei SEPPmail Appliances die mit entgegengesetzter Priorität auf die zwei virtuellen IP-Adressen reagieren. Dadurch erhält jeweils das eine System alle eingehenden und das andere alle ausgehenden E-Mails.

Im Detail

Ausfallsicherheit

Jede SEPPmail Appliance hat eine eigene, physikalische IP-Adresse über welche nur dieses System angesprochen werden kann. Diese Adresse wird in der Regel für die individuelle Konfiguration der Appliance und für das Synchronisieren der Appliances untereinander (blaue Pfeile „Abbildung 1“) verwendet. In „Abbildung 3“ sind dies die IP-Adressen **10.10.0.9** und **10.10.0.10**.

Zusätzlich werden zwei virtuelle IP-Adressen eingerichtet, um die beiden SEPPmail Appliances logisch zu jeweils einer Gruppe zusammenzufassen. In „Abbildung 3“ sind diese virtuellen IP-Adressen (Gruppen) farblich getrennt dargestellt. Dabei wird die **virtuelle IP-Adresse 10.10.0.1 (grün)** vom internen E-Mail Server für das Versenden **ausgehender E-Mails** angesprochen. Da diese **virtuelle IP-Adresse** von der Maschine mit der physikalischen IP **10.10.0.9 primär** bedient wird, fließt der gesamte ausgehende E-Mail Verkehr im Normalbetrieb über dieses System. Die **virtuelle IP-Adresse 10.10.0.2 (orange)** wird vom externen E-Mail Server oder auch einem vorgelagerten E-Mail Relay (zum Beispiel Firewall) für das Empfangen **eingehender E-Mails** angesprochen. Da diese **virtuelle IP-Adresse** von der Maschine mit der physikalischen IP **10.10.0.10 primär** bedient wird, fließt der gesamte eingehende E-Mail Verkehr im Normalbetrieb über dieses System.

In „Abbildung 3“, **grün dargestellt**, ist die **virtuelle IP-Adresse 10.10.0.1** für alle ausgehenden E-Mails zuständig. Hier ist das Cluster Member System mit der IP-Adresse **10.10.0.9** als **Primary** eingerichtet und reagiert immer als erstes System, wenn die **virtuelle IP-Adresse 10.10.0.1** angesprochen wird. Das Cluster Member System mit der IP-Adresse **10.10.0.10** ist als **Secondary** eingerichtet und reagiert nur dann, wenn der Cluster Member **Primary** - also das System mit der IP **10.10.0.9** - nicht verfügbar ist.

In „Abbildung 3“, **orange dargestellt**, ist die **virtuelle IP-Adresse 10.10.0.2** für alle eingehenden E-Mails zuständig. Hier ist das Cluster Member System mit der IP-Adresse **10.10.0.10** als **Primary** eingerichtet (entgegengesetzt der vorherigen Darstellung) und reagiert somit immer als erstes System, wenn die **virtuelle IP-Adresse 10.10.0.2** angesprochen wird. Das Cluster Member System mit der IP-Adresse **10.10.0.9** ist als **Secondary** eingerichtet und reagiert nur dann, wenn der Cluster Member **Primary** - also das System mit der IP **10.10.0.10** - nicht verfügbar ist.

Das heißt, fällt in diesem Konstrukt eine Maschine aus, so übernimmt die jeweils andere Maschine deren Aufgabe. Am Beispiel der „Abbildung 3“ würde also bei Ausfall des Systems mit der physikalischen IP **10.10.0.9** - welches primär den ausgehenden E-Mail Verkehr über die **virtuelle IP-Adresse 10.10.0.1** annimmt - ausfallen, so würde das **sekundär** für die **virtuelle IP-Adresse 10.10.0.1** konfigurierte System - also das mit der IP **10.10.0.10** - den ausgehenden E-Mail Verkehr zusätzlich übernehmen.

Loadbalancing

Um gegebenenfalls Lastspitzen abfangen zu können, bietet die SEPPmail Appliance in einer solchen Umgebung weiterhin die Möglichkeit, bei Erreichen eines definierten Lastzustandes am **Primary** System Last an das **Secondary** System abzugeben (siehe auch [System](#) ^[224] [Advanced view](#) [SMTP loadbalancer](#) ^[227]).

Zusammenfassung

Jede einzelne SEPPmail Appliance kann über zwei verschiedene virtuelle IP-Adressen angesprochen werden und reagiert mit jeweils unterschiedlichen Prioritäten einmal als **Primary** und einmal als **Secondary**. Dadurch ist der Betrieb beim Ausfall eines Cluster Member Systems weiterhin möglich. Das verbliebene Cluster Member System übernimmt dann zusätzlich die Arbeit des nicht mehr verfügbaren Systems und wird alle ein- und ausgehenden E-Mails verarbeiten.

Für das Bereitstellen der GINA-Technologie, beziehungsweise deren Oberfläche kann eine weitere virtuelle Cluster IP-Adresse **10.10.0.1** angesprochen werden. In Abhängigkeit der Cluster Member Prioritäten wird im Beispiel in Abbildung 3 das Cluster Member System mit der IP-Adresse **10.10.0.9** antworten, da dies mit der Priorität „Primary“ eingerichtet ist. Ist dieses System nicht verfügbar, so wird das Cluster Member System mit der IP-Adresse 10.10.0.10 antworten, da dies mit der Priorität „Secondary“ eingerichtet ist.

Das Einrichten der virtuellen IP-Adressen und das Zuweisen den Prioritäten des jeweiligen Cluster Member Systems ist in [System](#) ^[224] [Advanced view](#) [IP ALIAS addresses](#) ^[226] vorzunehmen.

Lastenausgleichs-Cluster - statisch

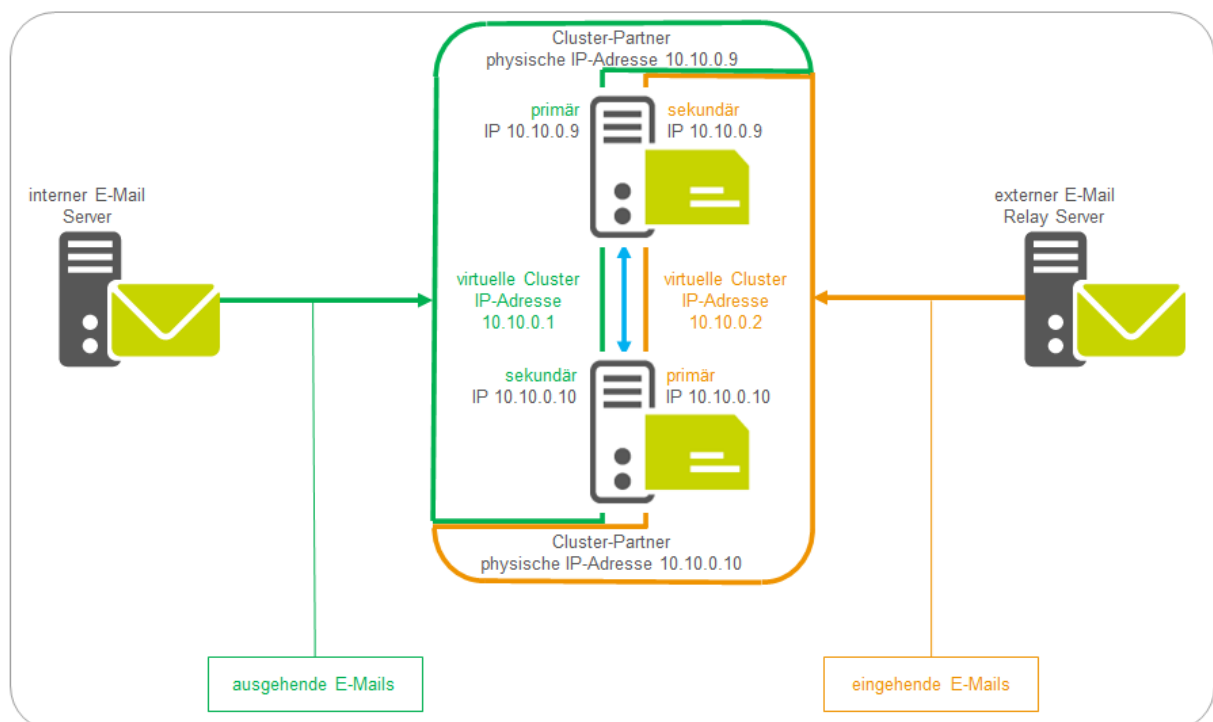


Abbildung 3 - Schematische Darstellung des statischen Aufteilens für ein- und ausgehenden E-Mails

4.8.3.2 Nutzen des DNS Round Robin Verfahrens

In der Konfiguration des internen und externen E-Mail Servers wird nicht mehr eine virtuelle Cluster IP-Adresse für den E-Mail Versand angegeben sondern jeweils ein Hostname, zum Beispiel „securemail.meinefirma.tld“ der bei ein- und ausgehenden E-Mails angesprochen wird. Im DNS ist es möglich zu jedem Hostnamen mehrere IP-Adressen anzugeben. Dadurch kann eine einfache Lastverteilung erreicht werden.

Fragt nun zum Beispiel der interne E-Mail Server den für den E-Mail Versand angegebenen Hostnamen (securemail.meinefirma.tld) des SEPPmail Appliance Clusters beim DNS-Server an, so werden immer alle - diesem Hostnamen zugeordneten - IP-Adressen, also **10.10.0.1** und **10.10.0.2** zurückgeliefert, dies aber jedes Mal in unterschiedlicher Reihenfolge. Der interne E-Mail Server wird im Normalfall die erste vom DNS-Server gelieferte IP-Adresse für den Versand der E-Mail verwenden.

Durch das Verwenden virtueller IP-Adressen in diesem Aufbau, wird die Ausfallsicherheit gewährleistet, da in diesem Fall bei Ausfall einer Maschine die verbleibende Maschine beide (virtuelle) IP-Adressen bedienen wird. „Abbildung 3“ zeigt eine logische Darstellung des Szenarios.

Im Detail

Jede SEPPmail Appliance hat eine eigene, physikalische IP-Adresse über welche nur dieses System angesprochen werden kann. Diese Adresse wird in der Regel für die individuelle Konfiguration der Appliance und für das Synchronisieren der Appliances untereinander (blaue Pfeile „Abbildung 4“) verwendet. In „Abbildung 4“ sind dies die IP-Adressen **10.10.0.9** und **10.10.0.10**.

Zusätzlich werden zwei virtuelle IP-Adressen eingerichtet, um die beiden SEPPmail Appliances logisch zu jeweils einer Gruppe zusammenzufassen. In „Abbildung 4“ sind diese virtuellen IP-Adressen (Gruppen) farblich getrennt dargestellt.

Der interne und der externe E-Mail Server sprechen für den Versand von ein- und ausgehenden E-Mails an das SEPPmail Appliance Cluster System einen Hostnamen (SEPPmail.meinefirma.tld) statt virtueller IP-Adressen an. Wird eine Anfrage für diesen Hostnamen an den DNS-Server gestellt, so wird der Hostname in alle eingerichteten IP-Adressen aufgelöst.

Im Beispiel entsprechen die aufgelösten IP-Adressen den virtuellen Cluster IP-Adressen wie in „Abbildung 4“ dargestellt.

Dabei sind die Rollen Primary und Secondary, für das Verarbeiten dieser virtuellen IP-Adressen auf den beiden Systemen entgegengesetzt konfiguriert (Stichwort Ausfallsicherheit).

Die **virtuelle IP-Adresse 10.10.0.1 (grün)** und die **virtuelle IP-Adresse 10.10.0.2 (orange)** dargestellt, werden dem Hostnamen (SEPPmail.meinefirma.tld) zugeordnet.

Wird dieser Hostname am DNS-Server abgefragt, so gibt dieser bei jeder ersten Anfrage

```
securemail.meinefirma.tld 1800 IN A 10.10.0.1
securemail.meinefirma.tld 1800 IN A 10.10.0.2
```

zurück. Bei jeder zweiten Anfrage wird der DNS-Server die zugeordneten IP-Adressen in umgekehrter Reihenfolge

```
securemail.meinefirma.tld 1800 IN A 10.10.0.2
securemail.meinefirma.tld 1800 IN A 10.10.0.1
```

zurückgeben. Da das anfragende System in der Regel die jeweils zuerst gelieferte IP-Adresse verwendet, werden die Anfragen zahlenmäßig verteilt (Lastverteilung).

Zusammenfassung

Beim Versand von ein- und ausgehenden E-Mails über den SEPPmail Appliance Cluster wird statt einer virtuellen Cluster IP-Adresse ein Hostname im jeweiligen E-Mail Server angegeben. Dieser wird dann zur Laufzeit in die zugehörigen IP-Adressen aufgelöst. So können der interne und der externe E-Mail Server ein- und ausgehende E-Mails wahlweise an eine dieser aufgelösten IP-Adressen senden. Durch den Einsatz virtueller Cluster IP-Adressen reagieren die Cluster Member Systeme je nach Priorität, wodurch die Ausfallsicherheit gewährleistet wird.

Durch die DNS Round-Robin-Funktion kann für den ein- und ausgehenden E-Mail Datenfluss eine Lastverteilung erreicht werden.

Quelle: Wikipedia, http://de.wikipedia.org/wiki/Lastverteilung_per_DNS

Das Einrichten der virtuellen IP-Adressen und das Zuweisen den Prioritäten des jeweiligen Cluster Member Systems ist in **System** ^[224] **Advanced view** **IP ALIAS addresses** ^[225] vorzunehmen.

Lastenausgleichs-Cluster – DNS Round-Robin-Verfahren

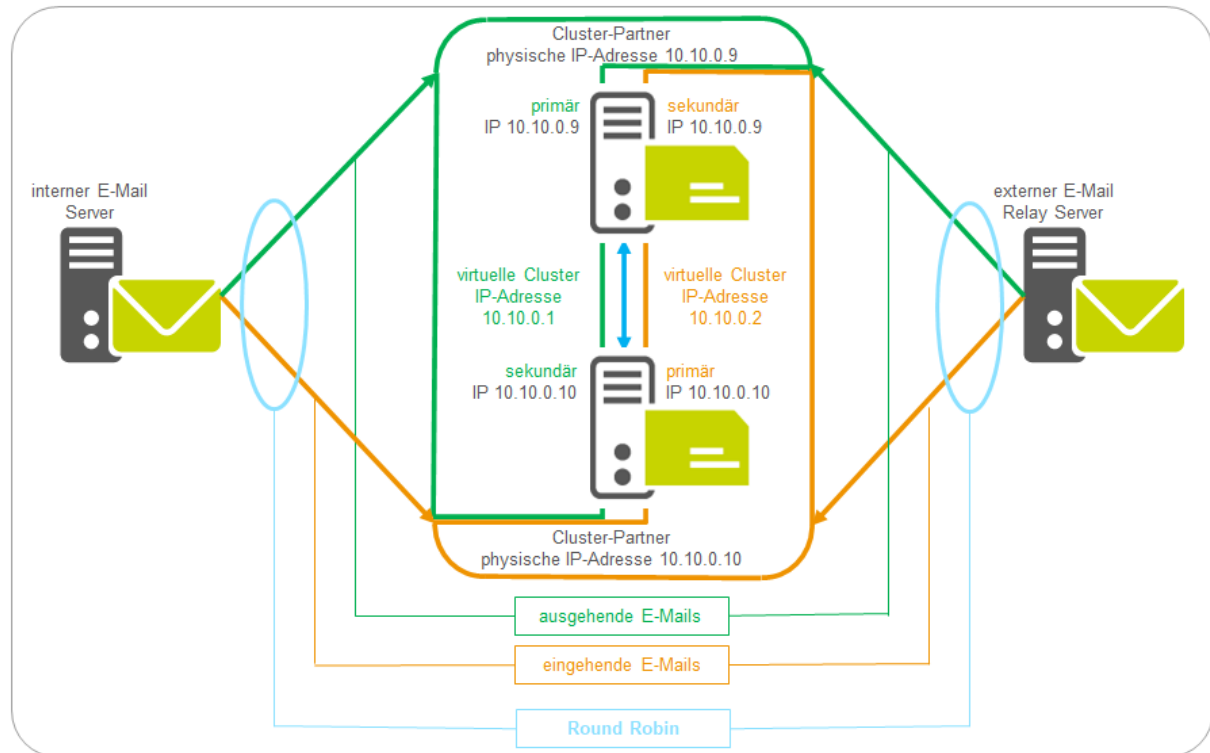


Abbildung 4 - Schematische Darstellung des Verteilens der Last durch das DNS Round-Robin-Verfahren für ein- und ausgehende E-Mails

4.8.3.3 Nutzen eines externen Loadbalancers

Bei Einsatz externer Loadbalancer sind diese für das gleichmäßige Verteilen der Last an die SEPPmail Appliance Cluster Member Systeme verantwortlich (siehe „Abbildung 5“). Ebenso müssen diese externen Loadbalancing Systeme den Ausfall eines Cluster Member Systems erkennen und somit für die Ausfallsicherheit des Gesamtsystems sorgen.

Im Detail

Die Cluster-Funktionalität der SEPPmail Appliance wird in diesem Szenario lediglich für die Synchronisation der Konfiguration zwischen den Cluster Member Systemen verwendet. Das **Entscheiden**, welches System auf ein- und ausgehende E-Mails reagiert wird **durch vorgelagerte Loadbalancer** getroffen. Diese verteilen je nach Konfiguration und Lastsituation die E-Mails wahlweise an ein bestimmtes Cluster Member System. Hierbei wird jedes Cluster Member System - im Gegensatz zu den anderen Cluster Varianten - über seine eigene, physikalische IP-Adresse angesprochen. In „Abbildung 5.1“ sind dies die IP-Adressen **10.10.0.9** und **10.10.0.10**.

Zu beachten ist an dieser Stelle das Realisieren des SSL Zugriffs für GINA (hellgrün dargestellt). Kann dieser nicht wie in „Abbildung 5.1“ dargestellt von einem externen Loadbalancer mit verarbeitet werden, so besteht bei Bedarf die Möglichkeit, diesen Zugriff über eine virtuelle Cluster IP-Adresse (siehe „Abbildung 5.2“) - im Beispiel **10.10.0.1** - zu realisieren. In Abhängigkeit der Cluster Member Prioritäten wird im Beispiel der „Abbildung 5.2“ das Cluster Member System mit der IP-Adresse 10.10.0.9 antworten, da dies mit der Priorität „**Primary**“ eingerichtet ist. Ist dieses System nicht verfügbar, so wird das Cluster Member System mit der IP-Adresse 10.10.0.10 und der Priorität „**Secondary**“ die Funktion übernehmen.

Lastenausgleichs-Cluster mit externem Loadbalancer

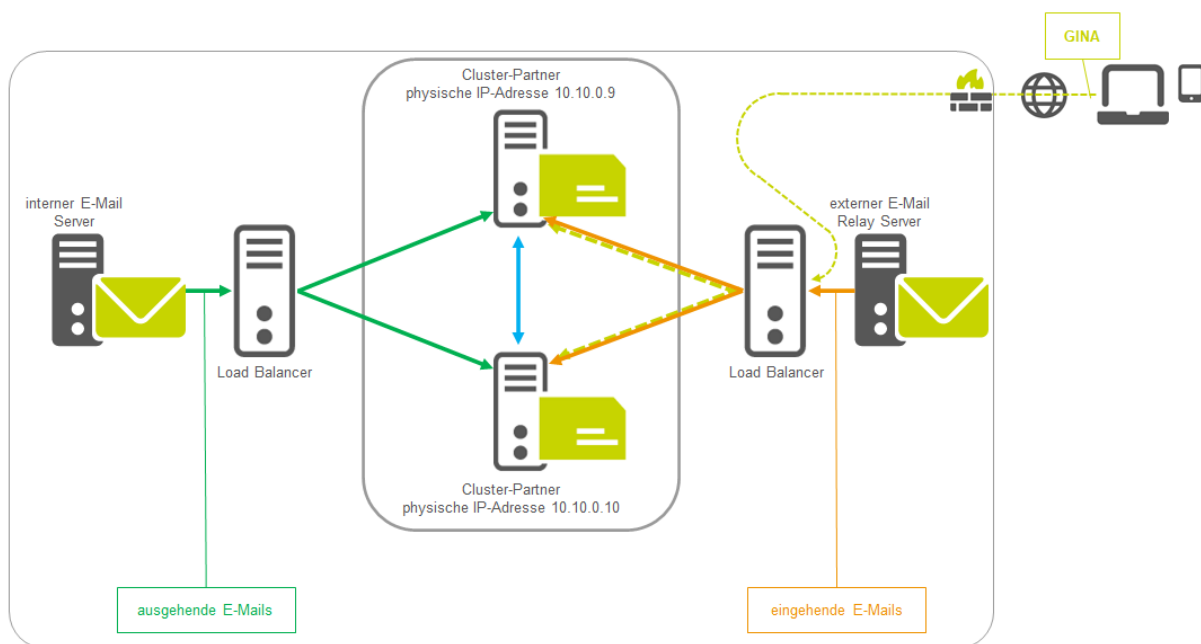


Abbildung 5.1 - Schematische Darstellung des dynamischen Aufteilens der Last für ein- und ausgehende E-Mails durch einen externen Loadbalancer

Lastenausgleichs-Cluster mit externem Loadbalancer und virtueller IP für GINA Zugriff

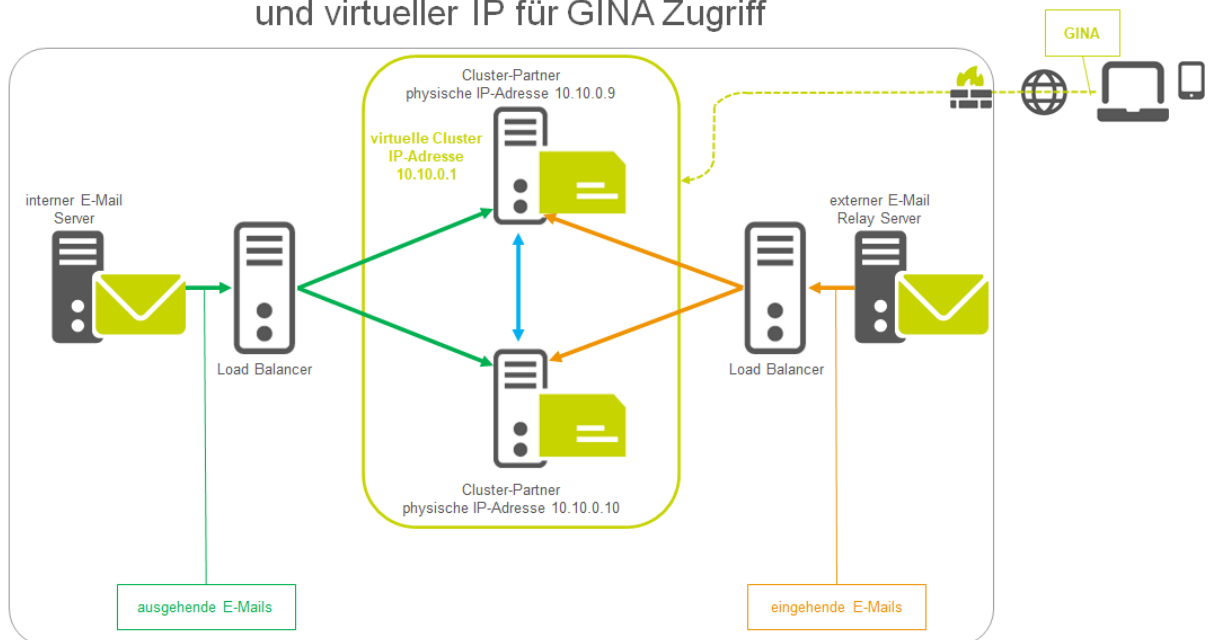


Abbildung 5.2 - Schematische Darstellung des dynamischen Aufteilens der Last für ein- und ausgehende E-Mails durch einen externen Loadbalancer unter Verwendung einer virtuellen IP-Adresse für GINA

4.8.4 Geo-Cluster

Ein Geo-Cluster (auch „Multisite System“ genannt) dient dem Replizieren von Konfigurationsdatenbanken zwischen geographisch voneinander getrennten SEPPmail Appliances, zum Beispiel zwischen verschiedenen Standorten eines Unternehmens.

Beispiel

Ein Unternehmen ist weltweit tätig und betreibt aus diesem Grund mehrere Rechenzentren auf verschiedenen Kontinenten. Die Unternehmensstandorte selbst sind alle durch ein VPN verbunden und haben in jedem Rechenzentrum einen Zugang zum Internet. Innerhalb dieses internen Unternehmensnetzwerks besteht ein E-Mail Transportsystem, zum Beispiel auf Basis von Microsoft Exchange oder IBM Domino. Die nach extern gesendeten E-Mails können je nach intern abgebildeter Richtlinie an verschiedenen Internetzugängen des Unternehmens ins Internet versendet werden. So können beispielsweise bei Ausfall eines Internetzugangs an einem Standort die E-Mails dieses Standortes über den Internet Zugang des anderen Standortes versendet werden, sofern die VPN-Verbindung zwischen den Standorten von diesem Ausfall nicht betroffen ist.

In einem derartigen Konstrukt muss das notwendige kryptographische Verarbeiten der E-Mails an allen Internetzugängen gleichermaßen funktionieren. Um dies zu gewährleisten, müssen die Konfigurationsdatenbanken sowie das Schlüsselmaterial an allen Kryptographie-Gateways - SEPPmail Appliance - identisch gehalten werden.

Dies wird durch die Geo-Cluster Funktion der SEPPmail Appliance realisiert, so dass stets die konsistente Konfiguration aller Systeme gewährleistet ist.

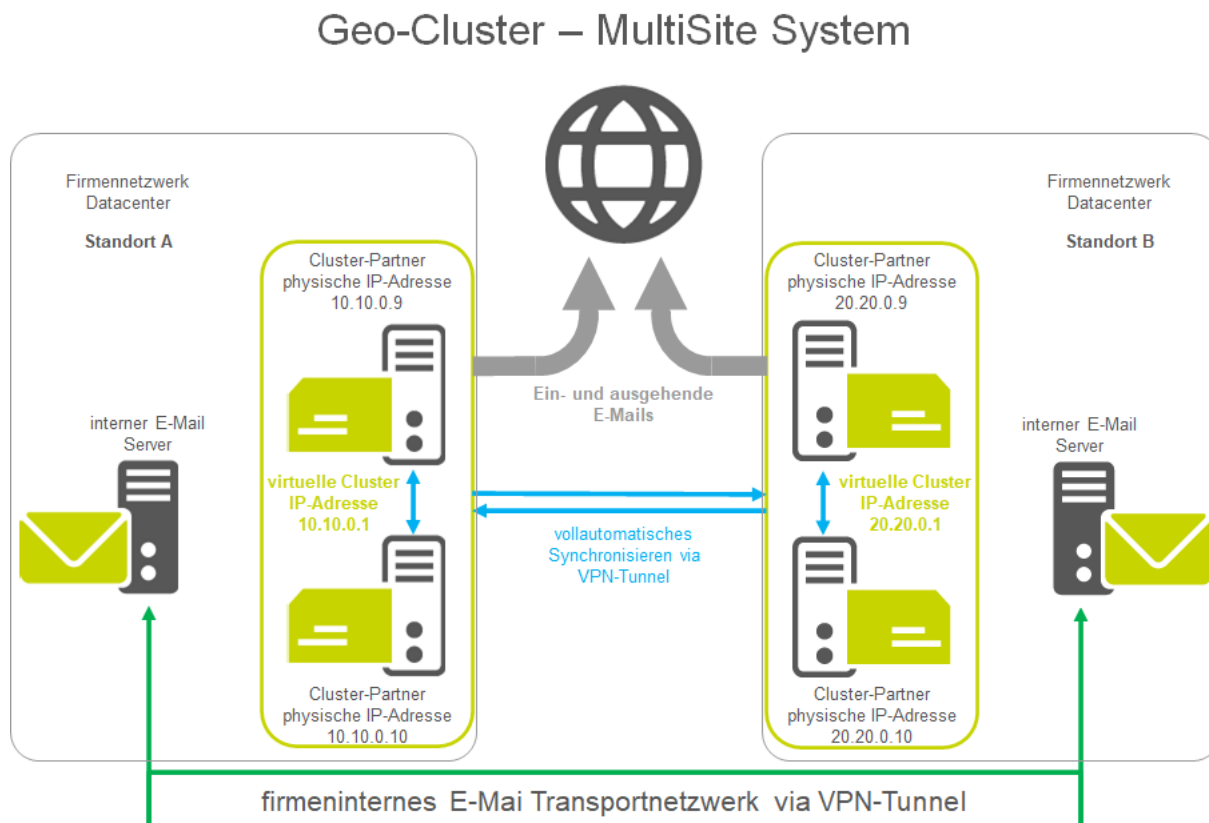


Abbildung 6 - Schematische Darstellung einer Geo-Cluster Struktur

4.8.5 Frontend/Backend Cluster

Ist aufgrund einer DMZ (DeMilitarisierte Zone) Struktur die Datenhaltung - insbesondere die Schlüsselverwaltung - innerhalb des Netzwerk-Standortes des E-Mail verarbeitenden Systems nicht erlaubt, so ermöglicht der Frontend-/Backend-Cluster das Trennen der Datenbank vom E-Mail verarbeitenden System.

Das heißt bei dieser speziellen Form eines SEPPmail Appliance Clusters existiert auf dem als Frontend konfigurierten System keine Konfigurationsdatenbank. Die zur Laufzeit benötigten Konfigurationsdaten werden ausschließlich auf dem Backend-System - welches die Konfigurationsdatenbank und somit auch das Schlüsselmaterial beherbergt - vorgehalten und auf Anfrage vom Frontend System auf dieses im Push-Verfahren geschoben (lila Pfeile in „Abbildung 7“).

Durch Abschluss der am Frontend System angeforderten Aktion - zum Beispiel Ver- oder Entschlüsseln - werden die hierfür angeforderten Konfigurationsdaten automatisch verworfen/gelöscht.

Frontend-Backend Trennung

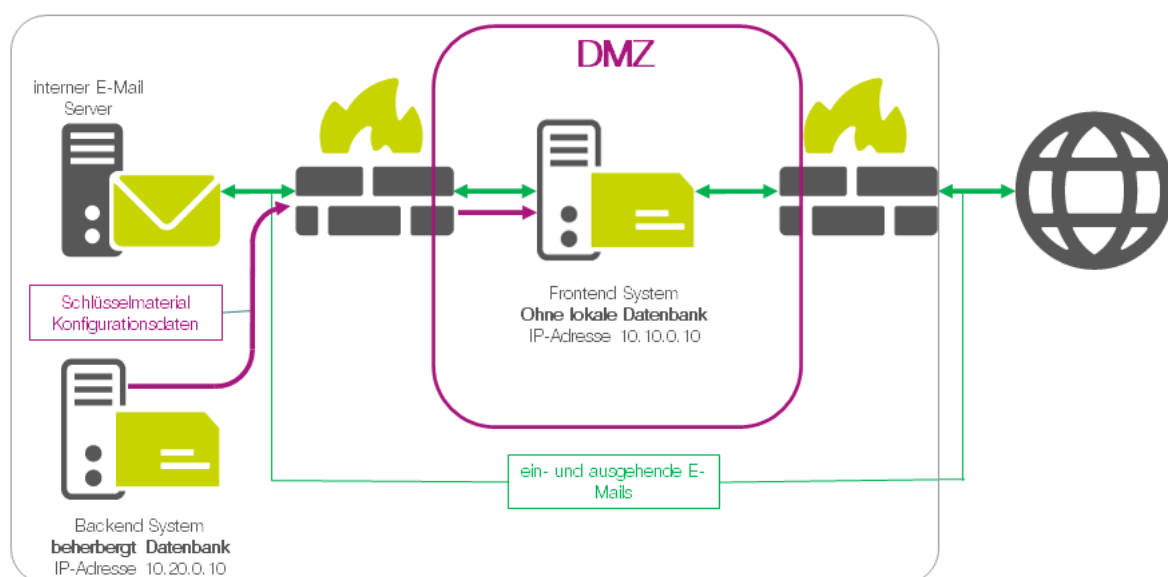


Abbildung 7 - Schematische Darstellung einer Frontend-/Backend-Cluster Struktur

Eine Sonderfall tritt in dieser Konstellation bei gleichzeitig aktivem **Large File Transfer (LFT)** ^[107] auf. Da ein Bereitstellen der großen Datenmengen einer LFT-Nachricht bei Anfrage durch den externen Empfänger über den SSH Tunnel vom Backend an den Frontend unweigerlich zu Geschwindigkeitseinbußen führen würde, muss auf dem Frontend-System ebenfalls Plattenspeicher für LFT bereitgestellt werden. Das Frontend-System erhält dabei die Synchronisation zum Backend aufrecht, sodass dennoch keine weiteren Portfreigaben (siehe auch **Firewall / Router einrichten**) ^[138] erforderlich sind.

4.8.6 GINA Satellit

Da E-Mail Systeme üblicherweise nur über SMTP Port 25 kommunizieren, ist unter Umständen aufgrund einer vorhandenen DMZ (DeMilitarisierte Zone) Struktur die für die GINA-Technologie benötigte Kommunikation über SSL Port 443 nicht möglich. Um dennoch die GINA-Technologie Nutzen zu können, ohne die Sicherheits-Infrastruktur aufweichen zu müssen, ist ein Abspalten dieser Technologie über das GINA Satelliten System und somit das Platzieren außerhalb der DMZ möglich. Hierfür stehen generell zwei Varianten zur Verfügung.

Variante 1

Diese entspricht im Wesentlichen dem **Frontend/Backend Cluster** ¹⁸⁰, bei welchem das Frontend-System ausschließlich die GINA-Funktion übernimmt.

Variante 2

Die Kommunikation zwischen dem Basis System und dem Satelliten System erfolgt dabei via SMTP Port 25 (lila Pfeil in „Abbildung 8“). Zum Internet hin wird das GINA-Web-Interface - meist getrennt durch eine Web Application Firewall (WAF) - über SSL Port 443 bereit gestellt.

GINA Satellit

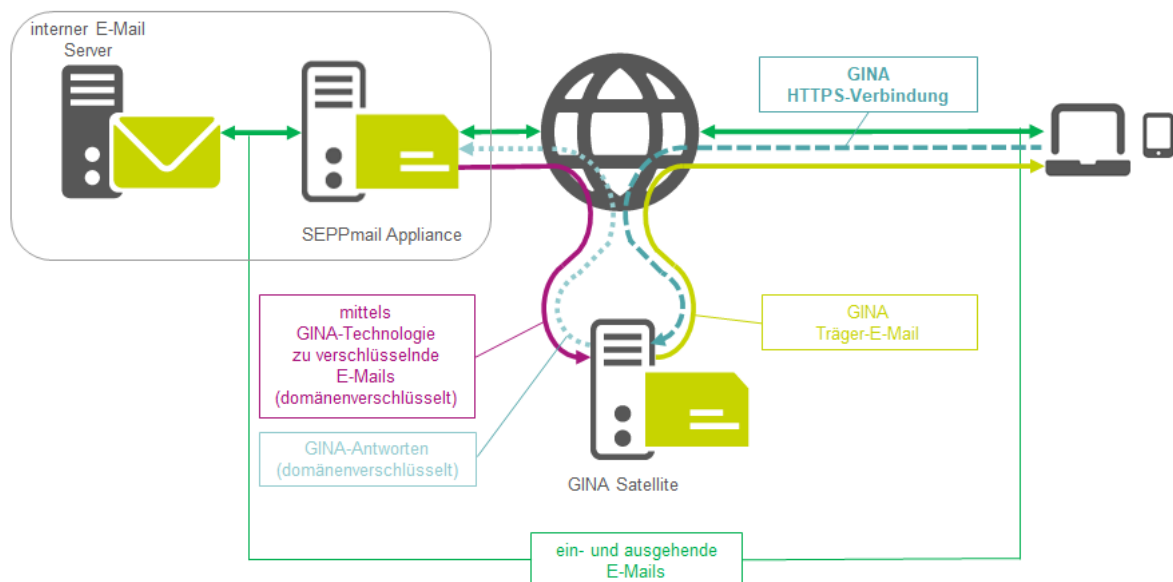


Abbildung 8 - Schematische Darstellung einer Secure Web-Mail Satellite Struktur

(neu in 12.0)

Variante 2a

Soll der GINA-Satellit als reiner Web-Server betrieben werden, das heißt der Zugriff auf die Maschine ist von außen zwar möglich, jedoch darf das System selbst nicht nach außen kommunizieren, so können E-Mails nach dem Verarbeiten auf dem Satelliten-System dort zwischengespeichert werden. Das Backend System würde in diesem Fall die auf dem Satelliten-System zwischengespeicherten E-Mails via POP3s abholen (siehe **oranger Pfeil** in „Abbildung 8a“).

4.8.7 Unterstützen externer redundanter Systeme

Einsatz mit redundanten internen und externen MTAs (Mail Transport Agent)

In der SEPPmail Appliance Konfiguration kann sowohl als externer MTA (E-Mail Relay) (siehe **Mail System** ^[247] **Outgoing server** ^[250] **Server name** ^[250]) wie auch pro interner E-Mail Domäne (E-Mail Server) (siehe **Mail System** ^[247] **Managed domain** ^[247] **ADD/EDIT MANAGED DOMAIN** ^[266] **Settings** ^[266] **Forwarding server** ^[266]) jeweils nur ein Host angegeben werden. Sollen mehrere Systeme angesprochen werden können, so muss dies über DNS MX-Einträge geschehen.

Steht lokal kein DNS-Server zur Verfügung, welcher MX-Einträge für die anzubindenden Server bereit stellt, so können hierfür im Menü **System** ^[224] unter **Advanced view** **DNS** ^[229] **add local zone** ^[229] lokale (pseudo) Einträge definiert und verwendet werden.

Lastenausgleichs-Cluster mit redundanten internen und externen MTAs

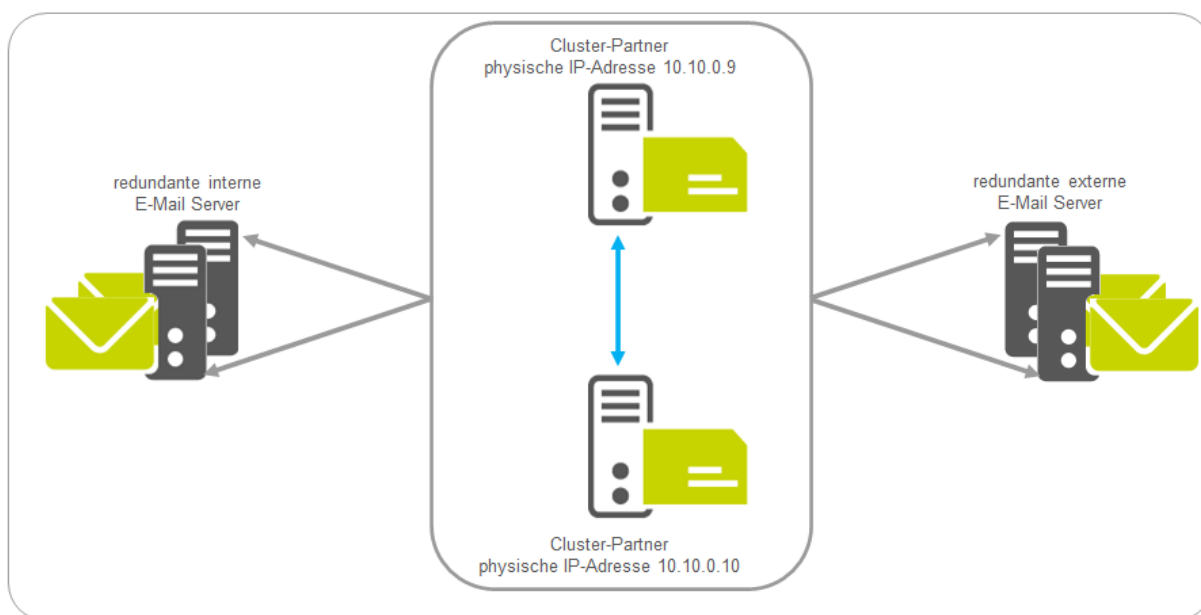


Abbildung 9 - Schematische Darstellung für den Einsatz von redundanten internen und externen MTAs

4.9 Einrichten zusätzlicher Features

Die SEPPmail Appliance bietet neben der Hauptfunktion des kryptographischen Behandelns von E-Mails zusätzliche Features an, um

- die Sicherheit zu erhöhen
 - [Protection Pack](#) ^[184]
 - [Internal Mail Encryption \(IME\)](#) ^[187]
- den Verwaltungsaufwand zu minimieren
 - [Self-Service Password Management \(SSPM\)](#) ^[53]
 - [Central Disclaimer Management \(CDM\)](#) ^[188]
- den Funktionsumfang zu erweitern
 - [Large File Transfer \(LFT\)](#) ^[186]

Diese optionalen Features müssen separat lizenziert werden.

4.9.1 Protection Pack (PP)

Das Protection Pack bietet zusätzlichen Schutz vor Spam E-Mails und Viren.

Das Einrichten der zugehörigen Einstellungen sind in [Mail System](#) ^[24] in den Sektionen [Antispam](#) ^[255], [Blacklists](#) ^[258] und [Manual blacklisting / whitelisting](#) ^[258] und [Mail Processing](#) ^[286] in der Sektion [Ruleset generator](#) ^[287] im Abschnitt **Protection Pack (Anti-Spam / Anti-Virus)** ^[303] zu finden.



Achtung:

Ob und in welchem Stand Virensignaturen nach der Installation bereits zur Verfügung stehen, ist unter [Home](#) ^[220] [Antivirus](#) ^[222] **Signature version** ^[222] zu sehen.

4.9.2 Self Service Password Management (SSPM)

Das Self Service Passwort Management erlaubt GINA-Benutzern selbstständig Ihr Passwort zurückzusetzen, wenn dieses verloren ging. Ein Eingreifen des Administrators ist somit nicht notwendig. Für das Konfigurieren des eigenständigen Zurücksetzens sind zunächst die Details der jeweiligen **GINA-Domain**^[416], welche durch Klicken des jeweiligen **GINA name**^[416] der Sektion **Domains**^[416] zu erreichen sind zu öffnen. Im Folgemenü **CHANGE GINA SETTINGS FOR**^[423] finden sich unter **Account login**^[447] folgende Möglichkeiten für das Zurücksetzen:

- über eine Bestätigungs-E-Mail (**Reset by Email verification**^[448])
- über eine Bestätigungs-E-Mail ohne Sicherheitsfrage (**Reset by Email verification, no reminder question/answer**^[448])
- per SMS (**Reset by SMS**^[449])
- per SMS ohne Sicherheitsfrage (**Reset by SMS, no reminder question/answer**^[449])
- über eine Auswahl durch den Benutzer (**Let user choose between hotline and SMS**^[449])

Soll die Möglichkeit des Zurücksetzens per SMS angeboten werden, so ist über **GINA Domains**^[416] **SMS passwords**^[418] die Konfiguration für den SMS Versand vorzunehmen.

4.9.3 Large File Transfer (LFT)

Large File Transfer ermöglicht mittels GINA-Technologie das Übertragen großer Dateien, über das übliche E-Mail Limit hinaus.

Diese zusätzliche Funktion steht in den Details jeder einzelnen GINA-Domain, welche jeweils über [GINA Domains](#)^[416] [Domains](#)^[416] zu erreichen ist, in der [Sektion Large File Transfer](#)^[439] zur Verfügung.

4.9.4 Internal Mail Encryption (IME)

Die Internal Mail Encryption dient dem Verschlüsseln von E-Mails innerhalb des eigenen Unternehmens (E-Mail Domänen).

Diese Funktion wird in mehreren verschiedenen Ausprägungen angeboten (siehe auch [Internal Mail Encryption \(IME\)](#) ^[114]).

Wird eine Variante gewählt, welche sich der GINA-Technologie bedient, ist das Aktivieren der **External authentication** ^[271] in den Detailsinstellungen der jeweiligen **Managed Domains** ^[247] (siehe [Mail System](#) ^[247]) empfehlenswert.

Andernfalls muss sich der interne Benutzer als GINA-Benutzer registrieren, bevor er diese Funktion nutzen kann. Wird GINA auch für das Versenden interner E-Mail verwendet sind dann zusätzlich folgende Optionen in den Einstellungen der jeweiligen GINA Domain in der **Sektion Extended settings** ^[431] (siehe [CHANGE GINA SETTINGS FOR](#) ^[423]) zu Aktivieren:

- Allow account self-registration in GINA portal without initial mail ^[432]
- Allow GINA users to write new mails (not reply) ^[434]

Sollten diese Optionen für den Zugriff von extern nicht gewünscht sein, so muss gegebenenfalls für den Zugriff von intern ein eigenes GINA-Interface (siehe [GINA Domains](#) ^[416] **Domains** ^[416] [CREATE NEW GINA DOMAIN](#) ^[422]) eingerichtet werden.

4.9.5 Central Disclaimer Management (CDM)

Mit dem Central Disclaimer Management (CDM) kann die SEPPmail Appliance Ihre E-Mails sowohl mit zentralen Firmen- (Disclaimer), wie auch - unter Zuhilfenahme von externen LDAP-Datenbeständen (wie zum Beispiel das Microsoft Active Directory - kurz AD) - personalisierten Absender- (Footer) Informationen ergänzen. Diese Fußnoten werden sowohl im Text- wie auch HTML-Format unterstützt.

Die Fußnoten können jeweils mittels **Mail System**  **Edit mail disclaimer...**  eingerichtet und den jeweiligen **Managed domains**  unter **Mail System**  **Managed domains**  **ADD/EDIT MANAGED DOMAIN**  **Settings**  **Disclaimer**  zugeordnet werden.

5 Administrative Aufgaben

Administrative Aufgaben wurden durch das effektive Design der SEPPmail Appliance auf ein Minimum reduziert. Sollten dennoch Aufgaben anfallen, so werden die Mitglieder der Gruppen **admin**^[413] und **statisticsadmin**^[415] (siehe **Groups**^[413]) darüber benachrichtigt. Weiterhin werden Benachrichtigungen über Probleme des Systems per Watchdog Meldung an die **Postmaster address**^[253] (siehe **Mail System**^[247] **SMTP settings**^[286]) gesendet.

Je nach Konfiguration des Systems lassen sich so die administrativen Aufgaben auf folgende Tätigkeiten beschränken:

- Eingreifen bei Problemen (Watchdog Meldung)
- Aktualisieren der Appliance (siehe **Administration**^[369] **Update**^[369])
- Erneuern des SSL Zertifikats bei Ablauf (siehe **SSL**^[319])
- Einstufen der Vertrauenswürdigkeit von **X.509 Root Certificates**^[480]

Sollte die Anlage von Benutzern (siehe **Mail Processing**^[286] **Ruleset generator**^[287] **User creation**^[289]) sowie der Bezug von Zertifikaten (siehe **Mail Processing**^[286] **Ruleset generator**^[287] **Key generation**^[291]) nicht automatisiert sein, so fallen hierfür natürlich weitere Aufgaben an.

5.1 Rudimentäre Systembefehle

Für rudimentäre Tests und Support-Aufgaben steht durch das Anmelden an der Console (bei Hardware über Bildschirm und Tastatur oder ein entsprechendes Remote Hardware Management System, beziehungsweise bei virtuellen Appliances über das Consolen Fenster der Maschine im Virtualisierungs-Host) mit

Standard-Benutzername: support
Standard-Kennwort: support

das „Recovery console menu“ mit den folgenden Optionen bereit:

(neu in 12.0) Option "Test mail"

```
===== Recovery console menu =====
```

```
0) Logout
1) Open support connection
2) Update appliance: You already have the latest version installed
3) Restart web services
4) Restart all services
5) Ping target
6) Port probe
7) DNS lookup
8) Trace route
9) Test mail
10) Initial network setup
11) Reboot
```

Enter an option: _

In Option **2)** wird angezeigt, ob ein Update vorhanden ist (update available, install latest version) oder nicht (You already have the latest version installed). Erscheint keine Meldung, so kann die Verbindung zum Update-Server nicht hergestellt werden.

Wird die Option trotz aktuellem Firmware Stand dennoch gewählt, so wird die aktuelle Firmware erneut heruntergeladen und installiert.

Ist die Appliance noch nicht registriert, so wird beim Update-Versuch eine entsprechende Meldung ausgegeben.

Wird während des Updates „Enter“ gedrückt, so wird der Update-Fortschritt angezeigt.

Option **6)** stellt eine Verbindung zu einem in der Folge anzugebenden Host auf einem ebenfalls anzugebenden Port her (telnet).

Hinweis:

Eine Verbindung nach außen kann nur dann getestet werden, wenn kein Proxy zwischengeschaltet ist. Ist für eine Verbindung in das Internet ein Proxy erforderlich, (siehe auch **Proxy Settings**^[236], **MPKI Proxy Settings**^[238], und **OCSP / CRL Check Settings**^[238]) so kann nur jeweils die Verbindung bis zu diesem Proxy direkt getestet werden.

Wird die Verbindung über einen Proxy hergestellt, so wird die Port 22 Verbindung über HTTPS getunnelt.

für das Testen dieser Verbindung sollte nach Aufruf dieser Option unter

Enter Server:

die IP

127.0.0.1

und unter

Enter Port:

die Nummer:

23

eingetragen werden.

Als Antwort sollte

Connection to 127.0.0.1 23 port [tcp/telnet] succeeded!

gezeigt werden.

Falls nicht, kann die SEPPmail Appliance die Verbindung zum Proxy Server nicht herstellen. Dann wären die Proxy Einstellungen erneut zu prüfen.

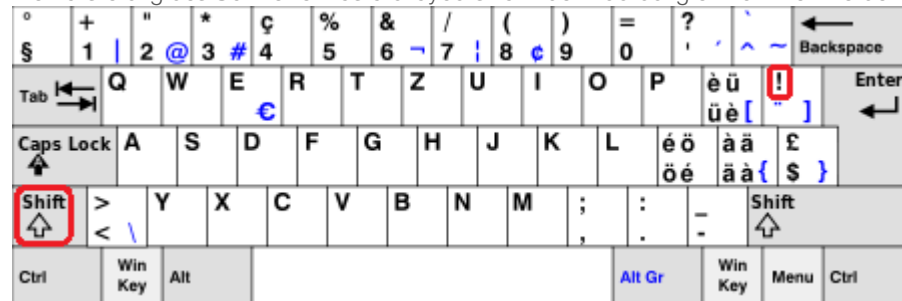
Falls diese Prüfung erfolgreich ist, die Verbindung in der Administrationsoberfläche jedoch nicht zustande kommt ist anzunehmen, dass die Anfrage am Proxy hängen bleibt.

Option **9)** sendet eine Testmail. Wird die Testmail erfolgreich gesendet, werden im Anschluß die Logdaten angezeigt. In der Anzeige der Logdaten kann gescrollt werden (oben / unten). Durch Drücken von "q" wird dieser Modus beendet.

Hinweis:

Im CLI ist das Schweizer Tastatur Layout zu beachten.

Die Darstellung des Schweizer Tastaturlayouts kann der Abbildung entnommen werden:



6 SEPPmail Microsoft Outlook Add-In

6.1 X-Platform-Add-In für Microsoft 365

6.1.1 Einleitung

Die SEPPmail Cross-Platform-Add-Ins wurden speziell für Outlook 365 entwickelt.

Aufgrund der gegenüber der on premises Version von Outlook eingeschränkten Entwicklungsmöglichkeiten existieren für Outlook 365 drei separate Add-Ins für

-  Verschlüsseln
-  Verschlüsseln mit Lesebestätigung (GINA)

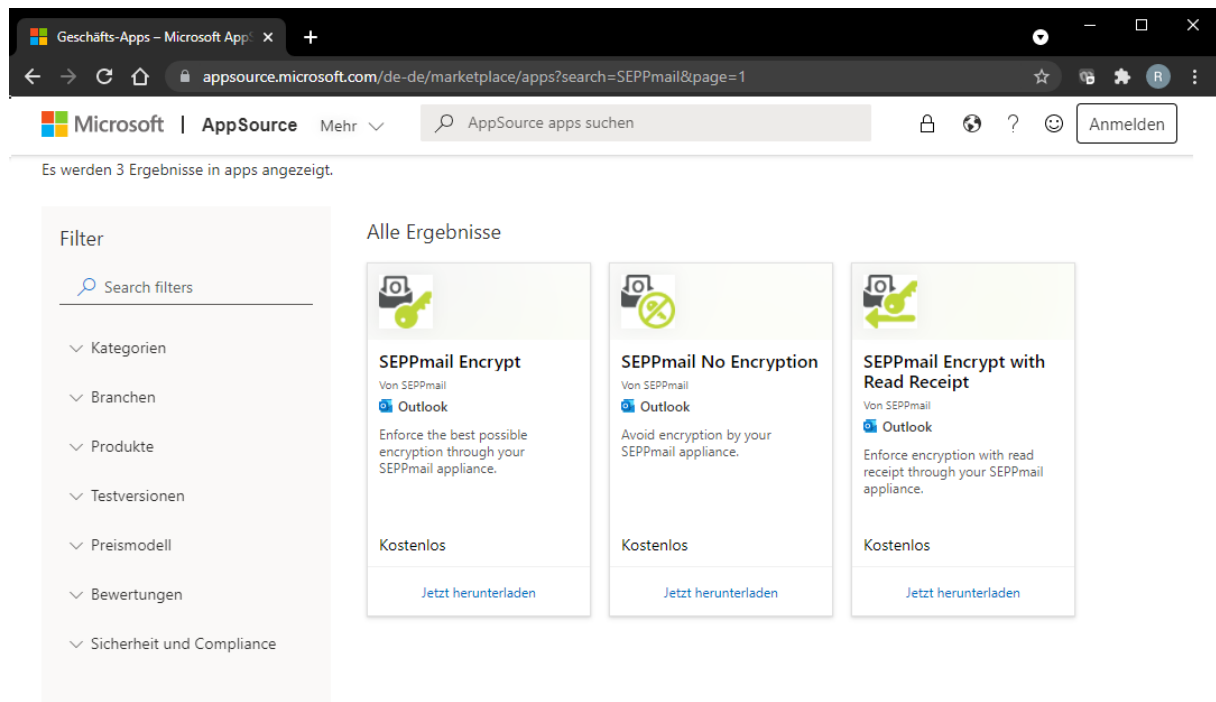


Unverschlüsselt

Diese entsprechen in Ihrer Funktion 1:1 denen des [COM Add-In für MS Exchange / Outlook on premises](#) ^[195] (siehe [Schaltflächen für den Versand von E-Mails](#) ^[208] ^[208]). Die weiteren Funktionen, welche gegebenenfalls bereits aus dem [COM Add-In für MS Exchange / Outlook on premises](#) ^[195] bekannt sind, sind wegen der oben genannten Einschränkungen leider nicht möglich.

6.1.2 Bezug

Die X-Plattform-Add-Ins sind im Microsoft AppStore (<https://appssource.microsoft.com/>) über eine Suche nach „seppmail“ zu finden und können dort bezogen werden (siehe Abbildung).



Für das Installieren der Add-Ins ist ein Microsoft Account erforderlich. Die Vorgehensweisen zur Installation des Add-Ins unterscheiden sich dabei abhängig von der Art des Accounts.

Zum Zeitpunkt des Erstellens dieses Kapitels standen zu diesem Vorgang folgende Hilfe-Artikel bei Microsoft zur Verfügung:

Beim „Personal“ Account (Hotmail, Live, Outlook) können die Add-Ins direkt in die eigene outlook.com Mailbox integriert werden.

Verwenden von Add-Ins in Outlook im Web

<https://support.microsoft.com/de-de/office/verwenden-von-add-ins-in-outlook-im-web-8f2ce816-5df4-44a5-958c-f7f9d6dabdc9>

Verwenden von Add-Ins in Outlook.com

<https://support.microsoft.com/de-de/office/verwenden-von-add-ins-in-outlook-com-a5672109-e4f3-4119-abea-72323e9653cf>

Für Business/Edu Accounts (also mit eigener Maildomain und M365 Subscription) stehen folgende Artikel bereit:

Installieren oder Entfernen von Add-Ins für Outlook für die Organisation

<https://docs.microsoft.com/de-de/exchange/clients-and-mobile-in-exchange-online/add-ins-for-outlook/install-or-remove-outlook-add-ins>

Bereitstellen der Add-Ins im M365 Admin-Center

<https://docs.microsoft.com/de-de/microsoft-365/admin/manage/manage-deployment-of-add-ins?view=o365-worldwide>

Weiterhin existieren allgemeine Artikel für das für das Aktivieren, beziehungsweise Deaktivieren der Add-Ins:

Aktivieren eines deaktivierten Addins

<https://support.microsoft.com/de-de/office/aktivieren-eines-add-ins-in-outlook-f%C3%BCr-windows-f2ec3c07-59ce-4fd4-912d-460aa0bd009d>

6.1.3 Systemanforderungen

Voraussetzung für eine erfolgreiche Integration des X-Platform-Add-Ins ist API-Version 1.8, welche ausschließlich von Exchange Online unterstützt wird.

Für die on premises Varianten ist das **COM Add-In für MS Exchange / Outlook on premises** ¹⁹⁵ zu verwenden.

Weitere Informationen hierzu sind gegebenenfalls direkt bei Microsoft unter <https://docs.microsoft.com/de-de/office/dev/add-ins/reference/requirement-sets/outlook-api-requirement-sets> zu finden.

6.2 COM Add-In für MS Exchange / Outlook on premises

6.2.1 Einleitung

Das SEPPmail Microsoft Outlook Add-In kann auf Microsoft Windows PC Systemen mit Microsoft Outlook installiert werden. Das Installieren kann sowohl interaktiv, als auch im Silent-Mode erfolgen. Je nach gewählter Installation stehen unterschiedliche Einstellungen (Parameter) zur Verfügung, um die Funktionalität des Add-Ins zu beeinflussen.

Das Add-In stellt in jedem (abgekoppelten!) Outlook Fenster zum Verfassen einer E-Mail (Neu, Weiterleiten, Antworten) Schaltflächen für das Steuern der kryptographischen Aktionen der SEPPmail Appliance zur Verfügung. Abhängig von den bei der Installation gewählten Einstellungen erscheinen unterschiedlich viele Schaltflächen, mit unterschiedlichen Standard-Einstellungen (gedrückt / nicht gedrückt).

(neu in 2.0.7)

Weiterhin werden eigene Kategorien angelegt, welche entsprechend des gewählten Verfahrens auch für gesendete E-Mails im Ordner „Gesendete Elemente“ gesetzt werden. Das versetzt den Absender in die Lage, auch später nachzuvollziehen ob eine E-Mail kryptographisch behandelt oder unbehandelt versendet wurde.

Die Zustände der Schaltflächen werden beim späteren Versenden einer E-Mail entweder

- als Steuer-Informationen in X-Header geschrieben.
- optional bei Verwenden des „Subject-Mode“ als Schlüsselwort in die Betreffzeile der E-Mail integriert.

Hinweis:

Bei Verwenden des „Subject-Mode“ werden eventuell manuell der Betreffzeile hinzugefügte Steuerbefehle (siehe „subject-mod Schlüsselwörter“ in Tabelle [Registry](#) ^[203]) entfernt, um eventuell entgegengesetzte, doppelte oder ungewollte Anweisungen zu vermeiden.



Da E-Mail Server unter Umständen X-Header abschneiden, bietet der „Subject-Mode“ hierfür eine Alternative.

Die durch das Add-In im „Subject-Mode“ hinzugefügten Schlüsselwörter sind auch im „Gesendete Elemente“ Ordner des Absenders zu sehen. Das versetzt diesen in die Lage, auch später nachzuvollziehen zu können, ob eine E-Mail kryptographisch behandelt oder unbehandelt versendet wurde. Ein Kategorisieren der ausgehenden E-Mails findet in diesem Modus nicht statt.

Da E-Mails bei adressierten internen Empfängern in der Regel durch den E-Mail Server direkt zugestellt werden, also gar nicht bis zur SEPPmail Appliance gelangen, sind diese Steuerbefehle auch im „Posteingang“ dieser Empfänger zu sehen.

Das zentrale SEPPmail Appliance System ist bei Eingang der E-Mail in der Lage beide Informationen auszuwerten. Weiterhin steht eine (optionale) Schaltfläche für den Aufruf einer Hilfe-Seite im Standard-Webbrowser zur Verfügung. Ebenso kann bei Bedarf eine Warnung beim Versenden von unverschlüsselten E-Mails ausgegeben werden.



Hinweis:

Die Warnung wird immer dann ausgegeben, wenn mittels Add-In keine Verschlüsselung angefordert wurde.

Die betreffende E-Mail kann jedoch unter Umständen an der SEPPmail Appliance dennoch verschlüsselt werden, sofern dort weitere, automatisierte Verschlüsselungskriterien konfiguriert wurden. Im Standard wäre das zum Beispiel eine [Domänenverschlüsselung](#) ^[314].

Die Anwendung ist mehrsprachig und passt sich der jeweiligen Sprache der Microsoft Outlook-Oberfläche an. Ist diese nicht verfügbar, wird Englisch als Standardsprache für das Add-In verwendet. Derzeit sind folgende Sprachen verfügbar:

- Deutsch
- Englisch
- Französisch
- Italienisch

6.2.2 Download

Das MS Outlook Add-In können Sie auf der folgenden Webseite in der jeweils aktuellen Version herunterladen:

[Download](#)

6.2.3 Systemanforderungen

Systemanforderung ist eine jeweils von Microsoft unterstützte Version von Microsoft Outlook für Windows auf einem unterstützten Microsoft Windows Client Betriebssystem.

6.2.4 Installation

Die Installation besteht aus zwei Dateien:

- Setup.exe
ist erforderlich um auf Windows 7,8,10 bei eingeschaltetem UAC (User Account Control = Benutzerkontensteuerung), per Rechtsklick „Als Administrator“ auswählen zu können. Prüft vor dem Ausführen der .msi-Datei ob die Voraussetzungen für die Installation (zum Beispiel NET Framework) vorhanden sind.
- SEPPmailOutlookAdd-InSetup.msi
führt die eigentliche Installation durch und kann auch direkt gestartet werden, wenn entsprechende Rechte vorhanden sind (zum Beispiel inaktives UAC und Admin-Rechte) beziehungsweise am Terminalserver bereits in den Install-Mode gewechselt wurde.

6.2.4.1 Interaktive Installation

Beispiel:

1. Rechtsklick auf setup.exe und „Als Administrator ausführen“ beziehungsweise „Run as administrator“ auswählen.

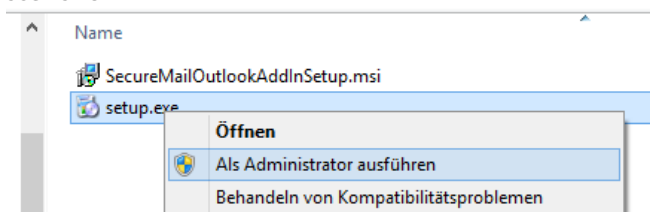


Abbildung 1

2. Die Sicherheitsabfrage von Windows mit „Ja“ beantworten, um die Installation zu starten.
3. Die Installation startet und folgendes Fenster erscheint:

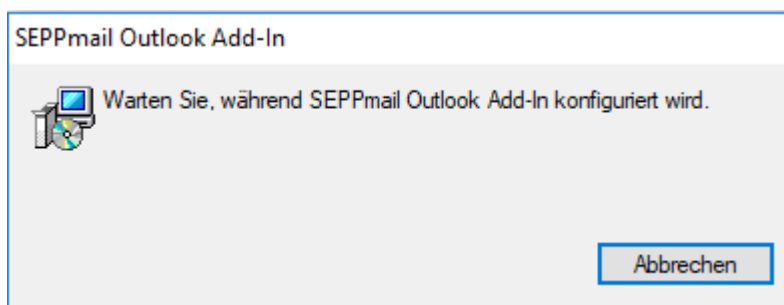


Abbildung 2

4. Ein weiteres Fenster erscheint, in welchem das Erscheinungsbild des Add-In im Menüband (Ribbon) von MS Outlook angepasst wird.
 - a. Rechts zur Auswahl stehen unter **„Bitte wählen Sie die Funktionen aus, welche in Outlook zur Verfügung stehen sollen“** jeweils die anzuzeigenden Schaltflächen sowie deren Standardzustand (an/aus).
 - b. Links kann zunächst unter **„TAG Einstellungen“** gewählt werden, wie das Add-In die Anweisungen an die SEPPmail Appliance übergibt (siehe [Betreffzeilen Schlüsselwörter / X-Header](#)). Wird der „Subject-Mode“ gewählt, so werden anstatt der üblicherweise vom Add-In verwendeten X-Header Schlüsselwörter in den Betreff eingefügt. Weiterhin kann dann gewählt werden, ob die Betreffzeilen Schlüsselwörter im Betreff an das Ende (Standard) oder an den Anfang gesetzt werden sollen. Die unterhalb bei „TAGs“ eingetragenen Schlüsselwörter müssen von der SEPPmail Appliance

entsprechend verarbeitet werden (siehe auch **Mail Processing**^[286] **Ruleset generator**^[287]). Voreingestellt sind die auf der SEPPmail Appliance verwendeten Standard-Schlüsselwörter.

- c. Weiterhin können - sofern die entsprechenden **Features**^[109] auf der SEPPmail Appliance aktiv geschaltet sind - die hierfür benötigten Angabe getätigt werden
- i. Für **Large File Transfer (LFT)**^[107] in der Variante 3 ist die Angabe des FQDN der SEPPmail Appliance erforderlich. Dies ist in der Regel der **Hostname**^[416] der [default] GINA (siehe **GINA Domains**^[416] **Domains**^[416]), beispielsweise
securemail.meinefirma.tld
beziehungsweise ein Aneinanderreihung der Hostnames der [default] GINA und der jeweils zu verwendenden GINA, beispielsweise
securemail.meinefirma.tld/mandant1
Bei Verwenden von **virtual hosting**^[417] ist jeweils nur der FQDN aus dem **Hostname**^[416] der jeweils zu verwendenden GINA einzutragen.
- Weiterhin kann für das Hochladen der LFT Daten auch eine unsichere Verbindung (HTTP) zugelassen werden (nicht empfohlen!).
- ii. Für die **Internal Mail Encryption (IME)**^[114] muss je nach Version der entsprechende Eintrag, wie in diesem Kapitel unter **Interne Verschlüsselung**^[210] beschrieben, vorgenommen werden.
- d. In den „**Sontige Einstellungen**“ können weitere Konfigurationen vorgenommen werden, wie
- i. eine Warnung ausgeben, wenn keine Verschlüsselung im Add-In gewählt wurde
1. diese Meldung für bestimmte Zieldomänen unterdrücken
- ii. eine definierbare „Hilfe“ Schaltfläche (siehe auch **Registry**^[203]) einblenden
- iii. ausschließlich maschinenbasierte Einstellungen zulassen (siehe ebenfalls **Registry**^[203])

Abbildung 3

6.2.4.2 Silent Installation

Alternativ kann die Installation über die Kommandozeile mit diversen Parametern gestartet werden.



Hinweis:

Die Kommandozeile muss als Administrator gestartet werden!

Beispiel

```
msiexec /q /i "SEPPmailOutlookAdd-InSetup.msi" NoGUI=true
SMWarning=false SMEncrypt=true SMSign=true SMWebMail=true SMHelp=true
SMEncryptSelected=false SMSignSelected=false SMWebmailSelected=false /li
.\log.txt
```

msiexec-Parameter:

Parameter	Beschreibung
/q	Installation ohne User Interface (nur in Verbindung mit "NoGUI=true" !)
/i	Installation eines MSI Paketes
/li .\log.txt	log.txt mit Basis Informationen im aktuellen Verzeichnis erzeugen

MSI-Parameter von SEPPmailOutlookAdd-InSetup.msi

Parameter	Standard	Beschreibung
NoGUI	false	Zwingend erforderlich für die Silent-Installation
InsecureLFTUploadConnection	false	Erlaubt das Hochladen der LFT Daten auch über eine unsichere Verbindung (HTTP).
InternalRecipient	ime@imepseudomain.local	Eintrag, wie in diesem Kapitel unter Interne Verschlüsselung [210] beschrieben
LFTSEPPmailHostname	leer	Angabe des FQDN der SEPPmail Appliance
LMonly	false	Registry-Werte nur in „HKLM“, nicht in „HCU“ speichern ein-/ausschalten
PlaceSubjectFlagsAtStart	false	Legt fest, ob Steuerbefehle am Anfang des Betreffs eingefügt werden. Im Standard (false) werden Steuerbefehle am Ende des Betreffs angefügt. Diese Einstellung ist nur relevant, wenn „subject-mod“ aktiviert ist.
SMEncrypt	true	Schaltfläche „Verschlüsseln“ ein-/ausblenden
SMEncryptSelected	false	Schaltfläche „Verschlüsseln“ im Standard aktiv/inaktiv setzen
SMHelp	true	Schaltfläche „Hilfe“ ein-/ausblenden
SMInternalEncryption	false	Schaltfläche „Auch Intern verschlüsseln“ ein-/ausblenden
SMInternalEncryptionSelected	false	Schaltfläche „Auch Intern verschlüsseln“ im Standard aktiv/inaktiv setzen
SMLargeFileTransfer	false	Schaltfläche „Large File Transfer“ ein-/ausblenden
SMLargeFileTransferBypass (entfällt mit 2.0.10)	false	Schaltfläche „LFT Attachments hochladen“ ein-/ausblenden
SMLargeFileTransferSelected	false	Schaltfläche „Large File Transfer“ im Standard aktiv/inaktiv setzen
SMNoEncryption	true	Schaltfläche „Unverschlüsselt“ ein-/ausblenden
SMNoEncryptionSelected	false	Schaltfläche „Unverschlüsselt“ im Standard aktiv/inaktiv setzen
SMSign	true	Schaltfläche „Signieren“ ein-/ausblenden
SMSignSelected	false	Schaltfläche „Verschlüsseln mit Lesebestätigung“ im Standard aktiv/inaktiv setzen

Parameter	Standard	Beschreibung
SMWarning	true	Funktion zur Ausgabe einer Warnmeldung, wenn keine Verschlüsselung gewählt wurde, ein-/ausschalten
SMWarningDomainWhitelist	leer	Durch Leerzeichen getrennter Eintrag von Ziel-E-Mail-Domänen, welche von der Warnung ausgenommen werden sollen.
SMWebmail	true	Schaltfläche „Verschlüsseln mit Lesebestätigung“ ein-/ausblenden
SMWebmailSelected	true	Schaltfläche „Verschlüsseln mit Lesebestätigung“ im Standard aktiv/inaktiv setzen
subject-mod	false	Wird die Subject-Ergänzung aktiviert, werden keine Header-Felder geschrieben, sondern Steuerbefehle als Zeichenfolgen an den Betreff ergänzt. Beim Senden werden zunächst eventuell noch vorhandene Steuerbefehle (z.B. „[confidential]“, etcetera) aus dem Betreff entfernt und anschließend gemäß der durch die Schaltflächen im Add-in vorgenommenen Einstellungen an den Betreff ergänzt. Der Benutzer sieht den erweiterten Betreff im Ordner „Gesendete Objekte“ und kann die Steuerbefehle für jede E-Mail nachvollziehen. Im Local Machine Teil der Registry werden die folgenden Werte ergänzt, mittels derer die Zeichenfolgen, die als Steuerbefehle verwendet werden sollen, konfiguriert werden können: - s-smenc = [confidential] - s-smlfm = [lfm] - s-smnoenc = [noenc] - s-smplain = [plain] - s-smsign = [sign] - s-smwebmail = [priv]
Tooltips	true	Tooltips für Buttons ein-/ausschalten

6.2.4.3 Deinstallation

Die Deinstallation des MS Outlook Add-In erfolgt interaktiv über die **Systemsteuerung** im Menü **Programme und Funktionen**.

Interaktiv am Beispiel Windows 7/8/10

Rechtsklick auf den Eintrag **SEPPmail Outlook Add-In** -> **Deinstallieren** (siehe Abbildung 1).

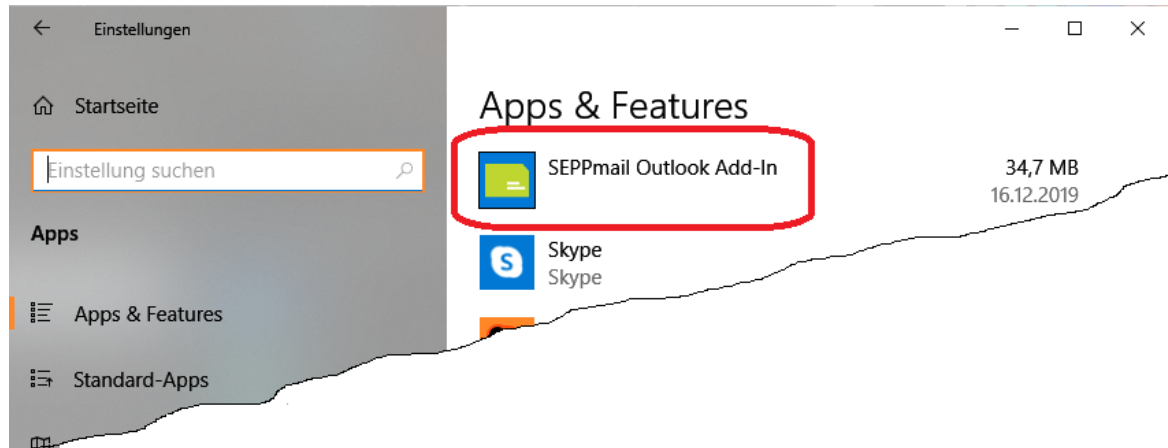


Abbildung 1

Weiterhin ist die Deinstallation auch Silent per MSI über den Befehl

`MsiExec.exe /x {A5B1FA06-7E16-4645-AFC1-0A7CDAFA77E3} /qn`
oder über das Add-In Setup

`setup /s /v" /x {A5B1FA06-7E16-4645-AFC1-0A7CDAFA77E3} /qn"`
möglich.

Dabei ist zu beachten, dass diese Befehle mit Administrator-Rechten ausgeführt werden müssen.

6.2.5 Registry

Das Add-In macht im Standard sowohl maschinenbezogene Eintragungen in den Registry Hive HKEY_LOCAL_MACHINE (HKLM) wie auch in die benutzerbezogenen Hives HKEY_CURRENT_USER (HCU). Um zum Beispiel unternehmensweit Standard Vorgaben der Schaltflächen Einstellungen zu erzwingen, lässt sich das Speichern Benutzer bezogener Einstellungen (HCU) optional abschalten.

Die Schaltflächen Einstellungen werden bei neuen Benutzern aus den Maschineneinstellungen (HKLM) in die Benutzereinstellungen (HCU) übernommen. Ebenso werden Änderungen der Maschineneinstellungen bei bestehenden Benutzern übernommen.

Folgend werden die Registry-Werte für das Add-In im Bereich

HKEY_LOCAL_MACHINE\Software\SEPPmail\OutlookAdd-In

bei **32 bit** Maschinen beziehungsweise

HKEY_LOCAL_MACHINE\Software\Wow6432Node\SEPPmail\OutlookAdd-In

bei **64 bit** Maschinen und Ihre jeweilige Funktion beschrieben:

Schaltfläche	Registry			Beschreibung
	Name	Typ REG_	Data Standard	
 Verschlüsseln	SMEncrypt	DWORD	0/1	Blendet die Schaltfläche aus bzw. ein
	SMEncryptSelected	DWORD	0/1	Setzt die Schaltfläche im Standard auf inaktiv/aktiv
	s-smenc	SZ	[confidential]	subject-mod Schlüsselwort
 Verschlüsseln mit Lesebestätigung	SMWebmail	DWORD	0/1	blendet die Schaltfläche aus bzw. ein
	SMWebmailSelected	DWORD	0/1	setzt die Schaltfläche im Standard auf inaktiv/aktiv
	s-smwebmail	SZ	[priv]	subject-mod Schlüsselwort
 Signieren	SMSign	DWORD	0/1	blendet die Schaltfläche aus bzw. ein
	SMSign Selected	DWORD	0/1	setzt die Schaltfläche im Standard auf inaktiv/aktiv
	s-smsign	SZ	[sign]	subject-mod Schlüsselwort
 Interne E-Mails verschlüsseln	SMInternalEncryption	DWORD	0/1	blendet die Schaltfläche aus bzw. ein
	SMInternalEncryption Selected	DWORD	0/1	Setzt die Schaltfläche im Standard auf inaktiv/aktiv
	InternalRecipient	SZ	ime@ime pseudo domain.local	gibt die Pseudo-Empfängeradresse für IME an (siehe auch Interne Verschlüsselung [210]).
 Unverschlüsselt	SMNoEncryption	DWORD	0/1	blendet die Schaltfläche aus bzw. ein
	SMNoEncryption Selected	DWORD	0/1	setzt die Schaltfläche im Standard auf inaktiv/aktiv
	s-smnoenc	SZ	[noenc]	subject-mod Schlüsselwort
<i>(neu in 2.0.7)</i>  Nicht verarbeiten	SMPlain	DWORD	0/1	blendet die Schaltfläche aus bzw. ein
	SMPlainSelected	DWORD	0/1	setzt die Schaltfläche im Standard auf inaktiv/aktiv
	s-smplain	SZ	[plain]	subject-mod Schlüsselwort
<i>(geändert in 2.0.10)</i>  Large File Transfer	SMLargeFileTransfer	DWORD	0/1	blendet die Schaltfläche aus bzw. ein
	SMLargeFileTransfer Selected	DWORD	0/1	setzt die Schaltfläche im Standard auf inaktiv/aktiv
	s-smlftm	SZ		subject-mod Schlüsselwort
	SMLargeFileTransfer Bypass	DWORD	0/1	durch Aktivieren wird das LFT Bypass Verfahren eingeschaltet
	LFTSEPPmail Hostname	SZ		FQDN, beziehungsweise Pfad für Large File Transfer (LFT) [107] in der Variante 3.

				Dies ist in der Regel der Hostname^[416] der [default] GINA (siehe GINA Domains^[416] Domains^[416]), beispielsweise securemail.meinefirma.tld beziehungsweise eine Aneinanderreihung der Hostnames der [default] GINA und der jeweils zu verwendenden GINA, beispielsweise securemail.meinefirma.tld/mandant1 Bei Verwenden von virtual hosting^[417] ist jeweils nur der FQDN aus dem Hostname^[416] der jeweils zu verwendenden GINA einzutragen.
	InsecureLFTUpload Connection	DWORD	0/1	durch Aktivieren werden unsichere, also nicht SSL verschlüsselte Verbindungen für das Übertragen von Dateien vom Client auf die Appliance zugelassen.
(entfällt in 2.0.10)  LFT Attachments hochladen	<i>SMLargeFileTransferBypass Selected</i>	<i>DWORD</i>	<i>0/1</i>	<i>setzt die Schaltfläche im Standard auf inaktiv/aktiv</i>
 Hilfe	SMHelp	DWORD	0/1	blendet die Schaltfläche aus bzw. ein
	Web Site	SZ	https:// www. seppmail.ch	Webseite welche bei Anklicken der Hilfe Schaltfläche aufgerufen werden soll
	<i>(neu in 2.0.9)</i> Categorize	DWORD	0/1	mit Aktivieren dieses Wertes werden die E-Mails beim Verarbeiten kategorisiert (siehe auch Einführung ^[195]).
	<i>(neu in 2.0.7)</i> CategorizeHistory	DWORD	0/1	mit Aktivieren dieses Wertes werden jeweils auch die E-Mails kategorisiert, welche seit dem letzten Outlook Start verarbeitet wurden (siehe auch Einführung ^[195]).
	LMOnly	DWORD	0/1	das Aktivieren von LMOnly deaktiviert das benutzerbezogene Speichern von Einstellungen in HCU
	PlaceSubjectFlags AtStart	DWORD	0/1	legt fest, ob Steuerbefehle am Anfang des Betreffs eingefügt werden. Im Standard (false) werden Steuerbefehle am Ende des Betreffs angefügt. Diese Einstellung ist nur relevant, wenn "subject-mod" aktiviert ist.
	SMWarning	DWORD	0/1	sofern aktiv, wird bei nicht angeforderter Verschlüsselung eine Warnmeldung vor dem Senden der E-Mail ausgegeben.
	<i>(neu in 1.6.8)</i> SMWarningDomain Whitelist	SZ		Durch Leerzeichen getrennter Eintrag von Ziel-E-Mail-Domänen, welche von der Warnung ausgenommen werden sollen.
	subject-mod	DWORD	0/1	durch Aktivieren des Subject-Mode werden Betreffzeilen Schlüsselwörter ^[164] statt X-Header zur Steuerung der Appliance verwendet.
	ToolTips	DWORD	0/1	de- bzw. aktiviert die Tooltips für die Schaltflächen
	UsageTimeStamp	SZ	JJJJ,MM,DD,hh,mm,ss	Wird mit der Zeit des letzten Andersns der Konfiguration belegt und für den Vergleich HKLM/HCU benötigt

Tabelle 1

Davon werden folgende Werte gegebenenfalls in den Bereich

HKEY_CURRENT_USER\Software\SEPPmail\OutlookAdd-In

übernommen:

Schaltfläche	Registry		
	Name	Typ REG_	Data
 Verschlüsseln	SMEncrypt	DWORD	0/1
	SMEncryptSelected	DWORD	0/1
 Verschlüsseln mit Lesebestätigung	SMWebmail	DWORD	0/1
	SMWebmailSelected	DWORD	0/1
 Signieren	SMSign	DWORD	0/1
	SMSignSelected	DWORD	0/1
 Interne E-Mails verschlüsseln	(neu in 2.0) SMInternalEncryption	DWORD	0/1
	SMInternalEncryption Selected	DWORD	0/1
	InternalRecipient	SZ	ime@ime pseudo domain.local
 Unverschlüsselt	SMNoEncryption	DWORD	0/1
	SMNoEncryptionSelected	DWORD	0/1
 Nicht verarbeiten	(neu in 2.0.7) SMPlain	DWORD	0/1
	SMPlainSelected	DWORD	0/1
 Large File Transfer	(geändert in 2.0.10) SMLargeFileTransfer	DWORD	0/1
	SMLargeFileTransferSelected	DWORD	0/1
	SMLargeFileTransferBypass	DWORD	0/1
	LFTSEPPmail Hostname	SZ	
	InsecureLFTUpload Connection	DWORD	0/1
 LFT Attachments hochladen	(entfällt in 2.0.10) ~~SMLargeFileTransferBypass Selected~~	~~DWORD~~	~~0/1~~
 Hilfe	SMHelp	DWORD	0/1
	Web Site	SZ	https://www.seppmail.ch
	(neu in 2.0.9) Categorize	DWORD	0/1
	(neu in 2.0.7) CategorizeHistory	DWORD	0/1

	PlaceSubjectFlagsAtStart	DWORD	0/1
	SMWarning	DWORD	0/1
	SMWarningDomainWhitelist	SZ	
	subject-mod	DWORD	0/1
	Tooltips	DWORD	0/1
	UsageTimeStamp	SZ	JJJJ,MM,DD,hh,mm,ss wird mit der aktuellen Zeit belegt. Ist der UsageTimeStamp von HCU neuer als der in HKLM, werden immer die Werte aus HCU vom Add-In verwendet.

Tabelle 2

Werden durch Aktivieren des **subject-mod** statt der X-Header **Betreffzeilen Schlüsselwörter** ¹⁶⁴ verwendet, so ist darauf zu achten, dass die Schlüsselwörter denen in der Appliance im Punkt **Mail Processing** ²⁸⁶ **Ruleset generator** ²⁸⁷ konfigurierten gleichen.

X-Header	Registry	
	Name	Schlüsselwort (Standard)
x-smenc	s-smenc	[confidential]
x-smsign	s-smsign	[sign]
x-smwebmail	s-smwebmail	[priv]
x-smnoenc	s-smnoenc	[noenc]
x-smplain	s-smplain	[plain]
x-smifm	s-smifm	[ifm]

Tabelle 3

Optional sind gegebenenfalls noch weitere Registry-Keys möglich (siehe [Berechtigungssteuerung per LDAP](#) ²¹²).

6.2.6 Schaltflächen für den Versand von E-Mails

Beim Versand von E-Mails sind je nach Einstellung die in Tabelle 1 angeführten Schaltflächen zu sehen und sind per Standard Aktiv beziehungsweise Inaktiv.

Je nach Zustand der Schaltflächen, wird der Header der E-Mail beziehungsweise bei aktiviertem Subject-Mode die Betreffzeile wie folgt ergänzt:

Schaltfläche	X-Header	Schlüsselwort (Standard)	Header
 Verschlüsseln	x-smenc: yes	[confidential]	
 Verschlüsseln mit Lesebestätigung	x-smwebmail: yes	[priv]	Disposition-Notification-To: <Absender SMTP Adresse>
 Signieren	x-smsig: yes	[sign]	
 Interne E-Mails verschlüsseln	siehe Kapitel: Interne Verschlüsselung ²¹⁰		
 Unverschlüsselt	x-smnoenc: yes	[noenc]	
 Nicht verarbeiten	x-smpain: yes	[plain]	
 Large File Transfer	x-smlfm: yes	[lfm]	
 Hilfe	öffnet den in der Registry definierten Hilfe-Link aus		

Tabelle 1

6.2.7 Large File Transfer

Generell kann über das Add-In mit der **Schaltfläche** [208] „Large File Transfer“ das Verwenden dieser Technologie erzwungen werden.

Für die Variante **Einliefern/Versenden via Standard E-Mail Client** [109] bedeutet dies, dass eine E-Mail unabhängig vom eingestellten Schwellwert (siehe auch **Size (in KiB) above which outgoing messages are treated as large files (set to 0 to treat all outgoing messages as large files)** [440]) als LFT-Nachricht versendet wird. Dazu muss lediglich während des **Installation** [198]prozesses die „Schaltfläche: Large File Transfer“ aktiviert werden.

Mit der Option **Einliefern/Versenden via SEPPmail Microsoft Outlook Add-In** [111] besteht die Möglichkeit, große Anhänge direkt, also am E-Mail Server vorbei, auf die SEPPmail Appliance hochzuladen, um den E-Mail Server nicht unnötig zu belasten und gegebenenfalls E-Mail-Größenbeschränkungen zu umgehen.

Für diese Funktion muss dem Add-In die URL für den Upload mitgeteilt werden. Dies erfolgt während des Installationsprozesses, beziehungsweise über den **Registry** [203] Wert „LFTSEPPmailHostname“ und entspricht in der Regel dem **Hostname** [416] des **GINA name** [416] [default].

Alternativ kann hier natürlich auch ein Hostname oder eine IP-Adresse angegeben werden, über welche die SEPPmail Appliance im internen Netz erreicht werden kann.

Dies ist insbesondere bei **Frontend/Backend Clustern** [180] wichtig, da das Einliefern auf ein Frontend-System über diese Variante nicht möglich ist. Das heißt, in diesem Fall müsste über die unter „LFTSEPPmailHostname“ eingetragenen FQDN/IP-Adresse das Backend System erreicht werden, über welches dann der LFT Versand stattfindet. Der LFT Download durch den Empfänger ist dann auch wieder am Frontend-System möglich.



Hinweis:

Werden ein oder mehrere Dateianhänge auf diese Art und Weise hochgeladen, die zugehörige E-Mail dann jedoch nicht versendet, so wird mit Ablauf der zum Übertragen aufgebauten „GINA-Session“ (spätestens nach 50 Minuten) der Upload verworfen.

6.2.8 Interne Verschlüsselung

Mit der Funktion „Interne Verschlüsselung“ können E-Mails an ein internes Postfach über die SEPPmail Appliance umgeleitet, dort verschlüsselt und an den internen E-Mail Server zur Auslieferung zurückgegeben werden. Dazu müssen einige Voraussetzungen erfüllt sein. Der Registry-Konfigurationswert „InternalRecipient“ muss eine E-Mail Adresse enthalten, welche nicht der eigenen E-Mail Domäne(n) zugeordnet und auch im Internet nicht existent ist. Somit wird gewährleistet, dass der E-Mail Server diese E-Mail als extern erkennt an die SEPPmail Appliance weiterleitet. Weiterhin ist sicherzustellen, dass an keinem, zwischen Outlook Client und SEPPmail Appliance stehendem System X-Header entfernt werden.

Im Standard lautet der Eintrag unter „InternalRecipient“ „ime@imepseudodomain.local“. Damit wird das [IME 1.0](#) ^[119] Verfahren festgelegt:

Beim Versand einer E-Mail werden die ursprünglichen Empfänger (To, CC, BCC) der E-Mail zunächst vom SEPPmail Microsoft Outlook Add-In in die X-Header „X-SM-ORIGTO“, „X-SM-ORIGCC“ und „X-SM-ORIGBCC“ übernommen. Als Empfänger wird ausschließlich der in der Registry hinterlegte „InternalRecipient“ eingefügt. Weiterhin wird eine technische Markierung „Interne Verschlüsselung“ gesetzt. Die SEPPmail Appliance erkennt anhand der Empfängeradresse „ime@imepseudodomain.local“, dass es sich um eine (auch) intern zu verschlüsselnde E-Mail handelt. Das heißt die Empfänger aus den X-Headern „X-SM-ORIGTO“, „X-SM-ORIGCC“ und „X-SM-ORIGBCC“ werden wiederhergestellt, die X-Header gelöscht, der ursprüngliche Absender als weiterer Empfänger hinzugefügt. Nun wird die E-Mail für die Empfänger verschlüsselt (mit S/MIME, sofern für den/die Empfänger entsprechendes Schlüsselmaterial auf der SEPPmail Appliance vorhanden ist, andernfalls mittels GINA-Technologie) und versendet.

Geht die so verschlüsselte E-Mail beim ursprünglichen Sender ein, so erkennt das SEPPmail Microsoft Outlook Add-In anhand des X-Headers „X-ESWmail-InternalEncrypt-sentcopy“, dass es sich eigentlich um die gesendete, Intern zu verschlüsselnde E-Mail handelt und verschiebt diese - natürlich ebenfalls verschlüsselte E-Mail - in den „Gesendete Elemente“ Ordner. Dabei wird die technische Markierung „Interne Verschlüsselung“ entfernt. Wird eine E-Mail im Ordner „Gesendete Elemente“ abgelegt, welche die technische Markierung „Interne Verschlüsselung“ gesetzt hat, so wird die E-Mail gelöscht. Damit wird gewährleistet, dass die ursprünglich gesendete, noch unverschlüsselte E-Mail aus dem Ordner „Gesendete Elemente“ entfernt wird.

Wird der Wert von „InternalRecipient“ geändert, so wird damit [IME 2.0](#) ^[121] festgelegt:

Wird die interne Verschlüsselung aktiviert, so legt das SEPPmail Microsoft Outlook Add-In beim Versand die verfasste E-Mail in einer signierten und verschlüsselten Container-E-Mail ab, welche dann an die für die SEPPmail Appliance konfigurierte „InternalRecipient“-Adresse (in der Regel [domain-confidentiality-authority@ime.<ihremangeddomain.tld>](#)) gesendet wird.

Die SEPPmail Appliance entpackt dann die Container-E-Mails, welche an die eingetragene „InternalRecipient“ Adresse gesendet wurden, verschlüsselt diese mit dem für die eigentlichen Empfänger vorliegenden Schlüsselmaterial (siehe auch [Verschlüsselungshierarchie](#) ^[66]) und sendet sie an die ursprünglichen Empfänger.

Die hierfür benötigten Zertifikate sind im Client bereitzustellen.

Zum einen ist das das unter [Mail System](#) ^[247] [Managed domains](#) ^[247] [ADD/EDIT MANAGED DOMAIN](#) ^[266] [Internal Mail Encryption](#) ^[276] zu erstellende Zertifikat für das Verschlüsseln. Um das Zertifikat anschließend mit dem [SEPPmail Microsoft Outlook Add-In](#) ^[190] nutzen zu können, wird in der Regel in der „Global Adress List (GAL)“ des Exchange Servers ein Kontakt mit der E-Mail Adresse aus dem CN dieses IME-Zertifikates und diesem Zertifikat selbst angelegt. Meist wird das Zertifikat des Kontaktes dadurch in den maschinenbezogenen Zertifikatsspeicher der Clients unter „Andere Personen“ „Zertifikate“ übernommen.

Hinweis:

Der Ordner „Andere Personen“ wird im Standard erst dann im Zertifikatsspeicher angelegt, wenn für einen Kontakt im Outlook-Adressbuch ein Zertifikat importiert wurde oder ein Eintrag im Exchange in der Global Adress List (GAL) erzeugt wurde.

Der in der Regel im GAL zu erzeugende Kontakt sollte mit einem Sonderzeichen, zum Beispiel einem Unterstrich „_“ beginnen. Hintergrund ist, dass das [SEPPmail Microsoft Outlook Add-In](#) ^[190] beim Start von MS Outlook automatisch nach diesem Eintrag sucht. Steht der Eintrag aufgrund des alphabetischen Sortierens relativ weit am Ende der GAL, kann diese Suche mitunter sehr lange dauern. Als Folge würde sich auch der Start von MS Outlook entsprechend verzögern.

Dies wiederum könnte ein automatisches Deaktivieren des [SEPPmail Microsoft Outlook Add-In](#) ^[190] zur Folge haben, sofern dem nicht durch entsprechende Konfigurationsmaßnahmen entgegengewirkt wurde.



Zum anderen ein - in der Regel selbst signiertes - S/MIME Schlüsselpaar des Absenders für das Signieren, welches in der Regel im benutzerbezogenen Zertifikatsspeicher unter „Eigene Zertifikate“ „Zertifikate“ bereitgestellt wird.

Details hierzu sind dem HowTo [Interne E-Mails verschlüsseln](#) ⁷⁴⁰ zu entnehmen.

6.2.9 Berechtigungssteuerung per LDAP

Bei Bedarf kann eine Berechtigungssteuerung aktiviert werden, welche abhängig vom ausgewählten Absender-Postfach das Verwenden der SEPPmail Appliance Verschlüsselungsfunktionen gewährt oder unterbindet.

Hierfür ist der Eintrag weiterer Registry-Keys erforderlich. Durch diese wird die Verbindung zum, sowie die Abfrage im LDAP definiert, wie der folgenden Tabelle zu entnehmen ist

Name	Typ REG_	Data (Beispiel)	Beschreibung
LDAPPermissionCheckActive	DWORD	0/1	Steuert, ob die Berechtigungssteuerung grundsätzlich aktiviert ist.
LDAPServerAddress	SZ	myldap.local	Adresse des LDAP Servers
LDAPUsername	SZ	tech_ldap	Benutzer der zur Abfrage des LDAPs berechtigt ist. Ist kein Eintrag vorhanden, so wird der aktuell angemeldete Benutzer verwendet.
LDAPPassword	SZ	password	Passwort dieses Benutzers. Ist kein Eintrag vorhanden, so wird das Passwort des aktuell angemeldeten Benutzers verwendet.
LDAPAuthenticationTypes	SZ	secure fast bind	Zu verwendendes Authentifizierungsverfahren für die LDAP Anmeldung. Mehrere Werte können kommagetrennt angegeben werden. Mögliche Werte sind unter https://msdn.microsoft.com/de-de/library/system.directoryservices.authenticationtypes(v=vs.110).aspx aufgelistet. Ist der Eintrag nicht vorhanden oder leer wird NTLM als Authentifizierungsverfahren (secure) verwendet.
LDAPOrganizationalUnit	SZ	OU=Users, DC=test, DC=server, DC=tld	LDAP Organisations Einheit, für welche die Abfrage ausgeführt wird
LDAPQuery	SZ	(&(mail={0}) (SEPPmailPermission=*))	LDAP Abfrage, in welcher anstelle des Platzhalters {0} die ausgewählte Absender-Adresse eingesetzt wird, sofern diese vorhanden und berechtigt ist. Andernfalls wird kein Ergebnis geliefert

6.2.10 AddIn Verwaltung

Für das zentrale Verwalten der SEPPmail Microsoft Outlook Add-In Einstellungen in Microsoft Netzwerken, bieten wir zusätzlich ein ADMX-Template an. Somit können die Einstellungen bequem per Group Policies (GPO) ausgebracht werden.

Die Vorlage steht ebenfalls zum [Download](#)  zur Verfügung.

6.2.11 Versionsverlauf

2.0.15

(neu in 2.0.15)

- Update auf Add-in Express 9.5.4661: behebt Abstürze auf ARM-Architekturen und auf Multi-Monitor Systemen mit verschiedenen DPI Einstellungen

2.0.14

(neu in 2.0.14)

- interne Verbesserungen

2.0.13

(neu in 2.0.13)

- interne Verbesserungen

2.0.12

(neu in 2.0.12)

- korrigiert das Verhalten bei der Suche nach vorhandenem IME Kontakt

2.0.11

(neu in 2.0.11)

- LFT: SEPPmail Hostname kann nun "http://" oder "https://" vorgestellt werden. Standard ist "https://"
- IME: IME Kontaktname wird ein "_" vorgestellt um die Suchzeit in der Global Address LIST (GAL) zu verkürzen
- Parsen von E-Mail Adressen verbessert
- Auslesen der Registry-Werte bei 64-Bit Office Versionen verbessert

2.0.10

(neu in 2.0.10)

- Öffnen von Attachments für LFT Bypass im read-only Modus
- Zusammenfassen der Schaltflächen "LFT" und "LFT Bypass"

2.0.9

(neu in 2.0.9)

- Schaltfläche "Verschlüsseln" wird bei gesetztem Outlook-Vertraulichkeits-Flag nicht mehr automatisch aktiviert
- Warnung vor dem unverschlüsselten Versand wird für IME Mails unterdrückt
- Schaltfläche "Verschlüsseln" und "Signieren" unabhängig voneinander
- Suche nach vorhandenen IME Kontakt bei der Installation verbessert
- Automatisches aktivieren der Schaltfläche "Auch intern verschlüsseln" beim Antworten auf eine IME Mail

2.0.8

(neu in 2.0.8)

- Verhalten der "Unverschlüsselt" Schaltfläche korrigiert
- Wiederkehrende Login-Aufforderungen abgestellt

2.0.7

(neu in 2.0.7)

- Installer in Deutscher Sprache verfügbar
- SMInternalEncryption Parameter für "silent" Installation via msixexec korrigiert
- Schaltfläche "Unverschlüsselt" in "Unverschlüsselt" ("No encryption") und "Nicht verarbeiten" ("Plain") aufgeteilt
- OEM Brandings ermöglicht(auf Anfrage)
- Kategorisieren von E-Mails, welche seit dem letzten Outlook Start verarbeitet wurden im Standard deaktiviert. Aktivieren erfolgt über den Registry Wert CategorizeHistory=1
- Optionales automatisches Aktivieren der Schaltfläche "Verschlüsseln", sofern auf eine E-Mail mit gesetztem Vertraulichkeits-Flag (Header sensitivity=companyconfidential) geantwortet wird, nur wenn "Verschlüsseln" für das AddIn aktiviert ist
- Verhalten beim Versenden von Serienbriefen aus Word, sowie bei Kalendereinladungen verbessert

2.0.6

(neu in 2.0.6)

- interne Verbesserungen

2.0.5

(neu in 2.0.5)

- Funktion "Senden an > E-Mail-Empfänger" über die rechte Maustaste im Windows Explorer ermöglicht
- Anbinden an Exchange mit und ohne Exchange-Cache-Modus ermöglicht
- Outlook Kategorisierung gesendeter E-Mails verbessert

2.0.4*(neu in 2.0.4)*

- Registry-Keys in CURRENT USER werden per Standard erstellt

2.0.3*(neu in 2.0.3)*

- Upgrade Verhalten verbessert (Registry Einträge bleiben erhalten)

2.0.2*(neu in 2.0.2)*

- IME Antwortverhalten verbessert

2.0.1*(neu in 2.0.1)*

- Trennen der Verhaltensweisen zwischen IME 1.0 und IME 2.0 verbessert

2.0*(neu in 2.0)*

- Schaltflächen im MS Outlook Menüband (Ribbon) für das Kategorisieren von E-Mails und dem damit verbundenen Triggern kryptographischer Aktionen beziehungsweise Zusatzfunktionen erweitert
- Large File Transfer (LFT) Bypass Mode implementiert
- Internal Mail Encryption (IME) 2.0 implementiert
- Whitelisting von Domänen für das Unterdrücken der Warnung bei nicht gewählter Verschlüsselung implementiert
- Log-Verhalten nach APPDATA\SEPPmail\Outlook AddIn\ verbessert
- Installationsmechanismus unter Beibehalten einer eventuell bereits bestehenden Konfiguration überarbeitet
- "silent" Installationen um den Parameter NoGUI erweitert
- Fehlerbehandlung verbessert

1.6.5*(neu in 1.6.5)*

- Improvement: Fehlerbehandlung & Logging verbessert

1.6.4*(neu in 1.6.4)*

- Bugfix: Der Installationspfad einer Dritthersteller-Bibliothek wurde korrigiert, so dass diese nun wieder korrekt geladen wird.

1.6.3*(neu in 1.6.3)*

- Bugfix: Beim Versenden von Arbeitsmappen aus Excel heraus erscheint Dialog nun nicht mehr hinter Excel Fenster (Austausch von Drittherstellerkomponente)

1.6.2*(neu in 1.6.2)*

- Improvement: Das Header-Flag "X-SMLFM" wurde in "X-SMLFT" geändert.
- Improvement: Es wurden aussagekräftige Fehlermeldungen für den Fall ergänzt, dass Zertifikate zur Signierung und Verschlüsselung nicht gefunden werden können.

1.6.1*(neu in 1.6.1)*

- Bugfix: Die Optionen/Parameter "LargeFileTransfer" und "LargeFileTransferSelected" werden nun korrekt aus dem Setup übernommen.

1.6.0*(neu in 1.6.0)*

- Improvement: Das Add-in unterstützt nun die „Large File Transfer“ Funktion

1.5.9*(neu in 1.5.9)*

- Bugfix: Bei der Add-in Initialisierung ist nun eine weitere Sonderbehandlung für den Start via SimpleMAPI umgesetzt, durch die Schaltflächen beim Start korrekt ausgeblendet werden.
- Improvement: Logdateien werden nun rollierend geschrieben und nach 30 Tagen automatisch entfernt.

1.5.8

(neu in 1.5.8)

- Bugfix: Re-Initialisierung der Schaltflächen für neue E-Mails funktioniert nun wieder ordnungsgemäß.

1.5.7

(neu in 1.5.7)

- Improvement: Es wurde eine Konfigurationsmöglichkeit (Registry) für den LDAPAuthentifizierungsmodus implementiert

1.5.6

(neu in 1.5.6)

- Bugfix: Re-Initialisierung der Schaltflächen mit vorkonfigurierten Werten wird für neue E-Mails nun korrekt durchgeführt.

1.5.5

(neu in 1.5.5)

- Bugfix: Die Add-in-Funktionalität ist nun auch verfügbar, wenn eine E-Mail über "Senden an" (Simple MAPI) erzeugt wird
- Improvement: Die Funktionalität der Schaltflächen kann per LDAP-Konfiguration abhängig von der Absender-Adresse gesperrt/entsperrt werden.
- Improvement: E-Mails, die mit "interner Verschlüsselung" versendet werden, werden nun in eine Container-E-Mail gelegt, und diese an den "InternalRecipient" versendet.

1.5.4

(neu in 1.5.4)

- Improvement: Position der Steuerbefehle in Betreff (Anfang/Ende) ist nun über SetupParameter und Registry konfigurierbar.

1.5.3

(neu in 1.5.3)

- Bugfix: Kleinere Kompatibilitätsmängel behoben.

1.5.2

(neu in 1.5.2)

- Bugfix: Das Problem beim Versand von Mails auf 64 Bit Systemen wurde behoben.

1.5.1

(neu in 1.5.1)

- Improvement: Die Lauffähigkeit des Add-ins wurde unter Outlook 2010 und 2013 (x86 und x64) geprüft.
- Improvement: Das Verhalten der Schaltfläche „interne Verschlüsselung“ wurde so angepasst, dass sie auch anwählbar ist, wenn die Schaltfläche „Verschlüsseln“ nicht zuvor ausgewählt ist. In dem Fall wird die Schaltfläche „Verschlüsseln“ automatisch mit ausgewählt.

1.5.0

(neu in 1.5.0)

- Improvement: Das Add-in bietet nun eine polnische Lokalisierung.
- Improvement: Die Setup-Einstellung „Warning message for unencrypted or unsigned outgoing e-mails“ ist nun standardmäßig deaktiviert.
- Improvement: Der Standardwert für "InternalRecipient" wurde auf "ime@imepseudodomain.local" geändert.
- Improvement: Tooltips werden nun standardmäßig angezeigt.
- Bugfix: Die Option "Fenster der Originalnachricht beim Antworten und Weiterleiten schließen." kann nun zusammen mit dem Add-in verwendet werden.
- Bugfix: Ein Outlook-Fehlverhalten, das bei bestimmten Build-Versionen dazu führt, dass Tooltips (und andere Beschriftungen) nicht korrekt angezeigt werden, wird nun umgangen.

7 Referenz der Menüpunkte

7.1 Allgemein

Grundsätzlich sollte in der Administrationsoberfläche vom Navigieren mittels „Vor“ und „Zurück“ Schaltflächen beziehungsweise vom Aktualisieren mittels entsprechende Schaltfläche des Browsers oder F5-Taste abgesehen werden.

Das SEPPmail-Logo dient in der Administrationsoberfläche als Navigationsanker zur zentralen Seite ([Home](#)  **220**). Ein Aktualisieren der aktuellen Seite kann durch erneutes Klicken auf das entsprechende Menü der Menüleiste oder den Menü Namen unterhalb des SEPPmail-Logo angestoßen werden.

Sortierungen in Listen und Tabellen können jeweils durch Klicken auf **unterstrichene Spaltenüberschriften** vorgenommen werden.

Sektionen können durch Klicken auf das Minus (-) am rechten Rand aus-, beziehungsweise über das Plus (+) eingeblendet werden.

7.2 Übersicht der Menüpunkte

Die Konfigurationsoberfläche der SEPPmail Appliance ist in die in der folgenden Tabelle kurz beschriebenen Menüs aufgeteilt. Dementsprechend ist dieser Teils des Handbuchs gegliedert.

Menü	Beschreibung
 Login/Logout 219	Anmelden an der Konfigurationsoberfläche, Ändern des persönlichen Kennworts für die Konfigurationsoberfläche.
 Home 220	Anzeige administrativer Daten (Systemstatus, System- und Benutzerlizenz, aktuelle Softwareversion, statistische Daten zur Systemauslastung, ...).
 System 224	Grundlegende Systemkonfiguration (IP-Adresse, Host- und Domainname, Routing, System-Datum und Uhrzeit, ...).
 Mail System 247	Konfiguration des SEPPmail Appliance E-Mail Systems (E-Mail Domänen, E-Mail Routing, Access Control, TLS, AntiSpam, Blacklists/Whitelists, ...).
 Mail Processing 286	Konfiguration des Regelwerks für das Verarbeiten von E-Mails (kryptographische Aktionen, Fußnoten (disclaimer/footer), Schutz-Regeln (AntiVirus/AntiSpam),...).
 SSL 319	Konfiguration des SSL Maschinen Zertifikats (für Secure Web-Mail Server, TLS, ...).
 CA 328	Konfiguration der internen Zertifizierungsstelle (optional).
 MPKI 339	Konfiguration des Konnektors für das Anbinden externer (akkreditierter) Zertifizierungsstellen,
 Administration 369	Administrationsoptionen für die SEPPmail Appliance.
 Cluster 383	Konfiguration für einen SEPPmail Appliance Cluster (optional).
 Logs 388	Anzeige von Logdateien (E-Mail, GINA, System, ...).
 Statistics 394	Anzeige von statistischen Daten bezüglich E-Mail-Verarbeitung und System.
 Users 396	Verwalten von SEPPmail Appliance Benutzerkonten.
 Groups 413	Verwalten von SEPPmail Appliance Gruppen.
 GINA Domains	Verwalten von GINA-Domänen.
 GINA Accounts 462	Verwalten von automatisch erzeugten GINA-Konten.
 LFT Accounts 466	Verwalten von automatisch erzeugten LFT-Konten.
 OpenPGP Public Keys 467	Verwalten öffentlicher OpenPGP-Schlüssel von Kommunikationspartnern.
 X.509 Certificates 477	Verwalten der S/MIME X.509-Zertifikaten (öffentliche Schlüssel) von Kommunikationspartnern.

 X.509 Root Certificates 	Verwalten von X.509-Wurzel-Zertifikaten und deren Vertrauensstatus.
 Domain Certificates 	Verwalten der OpenPGP und S/MIME Domänen Schlüssel von Kommunikationspartnern.
 Customers 	Verwalten der Mandanten (optional).

Referenz der Menüpunkte in der SEPPmail Appliance Konfigurationsoberfläche

7.3 Login / Logout

Der Menüpunkt **Login**^[219] ermöglicht das Abmelden von der SEPPmail Appliance Konfigurationsoberfläche, beziehungsweise den Kennwortwechsel des angemeldeten Benutzers. In der folgenden Tabelle werden die einzelnen Parameter beschrieben.

 **Sektion Login** (erscheint nur nach erfolgreichem „Log out“)

Parameter	Beschreibung
 User	Eingabe der User ID oder der dem User ^[396] zugeordneten E-Mail Adresse (Groß-/Kleinschreibung wird nicht berücksichtigt!) Das Anmelden an der Administrationsoberfläche ist prinzipiell für jeden auf der SEPPmail Appliance angelegten Benutzer möglich, sofern diesem ein Passwort zugewiesen wurde (siehe USER 'USER@DOMAIN.TLD' ^[396]). Ob und welche Menüs für den jeweiligen Benutzer sichtbar sind hängt von dessen Gruppenzugehörigkeit ab (siehe Groups ^[413]).
 Password	Dient der Passwort Eingabe.

 **Sektion Change password**

Parameter	Beschreibung
 The password must:	Gibt die Passwort Stärke der vorgegebenen Konfiguration (siehe Users ^[396] Password policy... CHANGE PASSWORD POLICY ^[414]). Zum Anmelden an der Konfigurationsoberfläche wählen Sie die Schaltfläche Log in .
 Old password	Um sicherzustellen, dass die berechtigte Person den Passwortwechsel durchführt, ist zunächst das aktuelle Passwort einzugeben.
 New password	Dient dem Passwort Wechsel des angemeldeten Benutzers. Das Passwort muss zwei mal angegeben werden um eine fehlerhafte Eingabe zu vermeiden und den Vorgaben von The password must: entsprechen.
 Log out.	Abmelden von der Konfigurationsoberfläche.
	Ändert das Passwort wie unter Change password ^[219] eingegeben.
	 Change password

7.4 Home

Das Menü Home öffnet nach dem Anmelden an der Konfigurationsoberfläche. Es zeigt grundlegende Informationen zur SEPPmail Appliance an.

Diese Ansicht wird alle 20 Sekunden automatisiert erneuert. Selbst wenn die Appliance nicht verfügbar sein sollte (zum Beispiel nach einem Update) wird weiterhin versucht diese zu erreichen. Sobald die Maschine wieder erreichbar ist, wird der Login Bildschirm angezeigt.

Sektion **System status**

Diese Sektion zeigt den aktuellen Systemstatus der SEPPmail Appliance an. Dieser sollte

All systems are stable and running.

lauten. Sollten wichtige Konfigurationseinträge fehlen, werden diese hier ebenso in rot angezeigt, wie Probleme auf dem System. Letztere resultieren jeweils aus Watchdog Meldungen.

Sektion **System**

Zeigt die Systemdaten der Appliance an.

Parameter	Beschreibung
 Device type	Typ der aktuellen Appliance, zum Beispiel SEPPmail 5000 (VMware Virtual Appliance).
 Device ID	Gerätelizenznummer (diese befindet sich auch auf dem Lizenzdokument)
 Firmware version	Aktuell auf dem System installierte Softwareversion.
 Current time	Aktuelle SEPPmail Appliance Uhrzeit im Format WWW MMM DD hh:mm:ss JJJJ zum Zeitpunkt des Seitenaufrufs.
 RAM usage	Aktuelle Speicherauslastung (momentan genutzt / insgesamt verfügbar)
 Swap usage	Aktuelle Größe des Auslagerungsbereichs (momentan genutzt / insgesamt verfügbar)  Hinweis: Generell sollte die Appliance Speicher nicht auslagern. Ist dies dennoch regelmäßig der Fall, so sollte mehr RAM zugewiesen werden.
 Load averages	Lastdurchschnitt als Anzahl der auszuführenden Arbeitsschritte im Vergleich zur Anzahl der ausgeführten Arbeitsschritte im gegebenen Zeitintervall (1, 5, 15 Minuten)
 Uptime	Laufzeit des Systems nach dem letzten Neustart.

Sektion **License**

In dieser Sektion wird der Lizenzstatus, wie lizenzierte Komponenten, deren Anzahl und Laufzeit angezeigt.

Parameter	Beschreibung
 License type	Hier werden Informationen zur System- und Benutzerlizenz angezeigt.
 License ID	Lizenznummer der SEPPmail Appliance.
 License holder	Eigentümer der SEPPmail Appliance Lizenz.
 Issue date	Ausstellungsdatum der Lizenz.
 Comment	Zusätzliche Informationen zur Lizenz.
 Last refresh	Zeigt den Stand der Anzeige der Lizenzdaten an. Mit  werden die Lizenzdaten aktualisiert.
 Encryption/Signature licenses	Anzahl der erworbenen Benutzerlizenzen ^[127] . In Klammern wird die Anzahl der noch verfügbaren Benutzerlizenzen angezeigt. Weiterhin werden die Lizenzen gegliedert angezeigt: Wie viele Benutzer unter Users ^[396] angelegt, wie viele davon auf „inactive“ (siehe USER 'USER@DOMAIN.TLD' ^[398] User data ^[398] Encryption settings) gesetzt und wie viele aufgrund von Inaktivität für mindestens drei Monate freigegeben wurden.
 Large File Transfer (LFT) licenses	Anzahl der erworbenen Benutzerlizenzen für die Funktion Large File Transfer ^[107] . In Klammern wird die Anzahl der noch verfügbaren Benutzerlizenzen angezeigt.  Hinweis: Auf den Hardware Appliances ab 1000B steht für LFT interner Speicher zur Verfügung. Die 500B benötigt eine externe USB-Platte. Bei virtuellen Appliances muss für das Verwenden von LFT auf dem Host-System eine weitere Hard Disk von mindestens 30GB zugeordnet, und das System neu gestartet werden. Andernfalls erscheint die Meldung Note: You have LFT licenses, however your device has no disk to store Files. Please add an USB (or virtual) disk. (siehe auch Sizing ^[78])
 Multitenancy	Anzahl der erworbenen Mandantenlizenzen
 Software Care Pack	Anzeige des Ablaufdatums der Lizenz für Software Updates ^[126] .
 Device Care Pack	Anzeige des Ablaufdatums des Device Care Packs ^[126] .
 Protection Pack (AntiSpam/AntiVirus)	Anzeige des Ablaufdatums der Lizenz für das Protection Pack ^[126] (AntiVirus und AntiSpam).
 Internal Mail Encryption	Lizenz für interne Verschlüsselung ^[129] (active / not licensed).
 Central Disclaimer	Lizenz für Central Disclaimer Management ^[130] (active / not licensed).

Parameter	Beschreibung
Management	
 Self-Service Password Management	Lizenz für Self-Service Passwort Management (active / not licensed).

Sektion **AntiVirus**

Zeigt den Status des integrierten Virenschanners an

Parameter	Beschreibung
 Inactive	Falls keine Protection Pack ^[126] Lizenz vorhanden ist.

nur bei aktiver **Protection Pack** ^[22] **License** ^[220]

 ClamAV engine	Anzeige der ClamAV Scan Engine Version
 Signature version	Anzeige der ClamAV Virensignatur Version  Achtung: Sofern - insbesondere bei Neuinstallationen - noch keine Virensignaturen vorhanden sind, werden alle E-Mails blockiert, bis diese zur Verfügung stehen. In diesem Fall erscheint an dieser Stelle die Meldung: NO VALID SIGNATURES FOUND Signature update can take up to 15 minutes. NOTE: If you activated antivirus in 'Mail Processing' all mails will be rejected until valid signatures are available If this message does not disappear make sure that the appliance is allowed to make connections on port 80 to the internet or that a http proxy is specified
 Signature date	Anzeige des ClamAV Virensignatur Datums

Sektion **Mail statistics**

Zeigt eine Kurzübersicht der verarbeiteten E-Mail an.

Parameter	Beschreibung
 Mails processed	Anzahl aller insgesamt vom System übertragenen E-Mails (empfangen, gesendet).
 Mails processed (S/MIME)	Anzahl aller insgesamt via S/MIME verarbeiteten E-Mails (entschlüsselt, verschlüsselt).
 Mails processed (OpenPGP)	Anzahl aller insgesamt via OpenPGP verarbeiteten E-Mails (entschlüsselt, verschlüsselt).
 Mails processed (DOMAIN)	Anzahl aller insgesamt via Domänenverschlüsselung ^[31] verarbeiteten E-Mails (entschlüsselt, verschlüsselt).

Parameter	Beschreibung
 GINA mails	Anzahl aller insgesamt versendeten Secure Web-Mails über das GINA-Subsystem.
 Mails currently in queue	Anzahl aller E-Mails in der Warteschlange.

Sektion **Disk statistics**

Zeigt die Auslastung der einzelnen Systempartitionen an.

Parameter	Beschreibung
 Database	Zeigt die Auslastung des Datenbank Volumes (/var/ldap.ENCRYPTED) im System. Bei einer Auslastung von 75% wird die Anzeige rot und eine Watchdog-Meldung wird ausgegeben.
 Mail queue	Zeigt die Auslastung des E-Mail Warteschlangen Volumes (/var/mailqueue) im System. Bei einer Auslastung von 60% wird die Anzeige rot und eine Watchdog-Meldung wird ausgegeben.
 Log	Zeigt die Auslastung des Volumes für die Log-Dateien (/var/log) im System. Bei einer Auslastung von 75% wird die Anzeige rot und eine Watchdog-Meldung wird ausgegeben.
 Temp	Zeigt die Auslastung des Volumes für temporäre Dateien (/tmp) im System. Bei einer Auslastung von 90% wird die Anzeige rot und eine Watchdog-Meldung wird ausgegeben.

nur bei aktiven **Large File Transfer (LFT) licenses**

 LFT store	Zeigt die Auslastung des Large File Transfer Volumes (/var/lftm) im System. Bei einer Auslastung von ??% wird die Anzeige rot und eine Watchdog-Meldung wird ausgegeben.

7.5 System

Das Menü **System**^[224] kann in zwei Ansichten betrachtet werden. Die grundlegenden Basiseinstellungen sind in der Ansicht **Normal View** zu sehen. Diese Ansicht ist die Standardansicht bei Aufruf des Menüs. Eine vollständige Übersicht aller Einstellungen ist in der Ansicht **Advanced View** zu sehen.



Hinweis:

Bei **System**^[224] handelt es sich um maschinenbezogene Einstellungen. Das heißt, diese werden nicht im **Cluster**^[383] synchronisiert und müssen somit im Bedarfsfall auf jedem Cluster Partner einzeln vorgenommen werden.



Achtung:

Sollen in einem Cluster Änderungen an der Netzwerkconfiguration vorgenommen werden, so ist der Cluster zunächst aufzulösen (siehe auch **Remove From Cluster**^[385]). Nach Abschluss der Änderungen muss der Cluster dann wieder neu gebildet werden (siehe auch **Prepare For Cluster**^[383], beziehungsweise **Add This Device To Existing Cluster**^[383]).



Advanced View

Durch betätigen der Schaltfläche **Advanced view** werden die erweiterten Parameter angezeigt. Um die erweiterte Darstellung des Menüpunkts **System** wieder zusammenzufassen ist in der erweiterten Darstellung die Schaltfläche **Normal view** zu betätigen.



Normal View

In diesem Menü werden die wichtigsten Parameter der LAN-Anbindung der SEPPmail Appliance eingerichtet. Die hier eingetragenen Daten dienen auch als Grundeinstellung für viele weitere Einstellungen des SEPPmail Appliance-Systems.

Die folgenden Tabellen beschreiben den **Advanced view**, da dieser alle Einstellungen des **Normal view** beinhaltet.



Sektion **Comment** (optional)

Eingabefelder zur Beschreibung beziehungsweise zur Identifikation der SEPPmail Appliance. Diese Parameter werden zum Beispiel als Betreff in der automatischen Datensicherung sowie von SNMP verwendet. Ansonsten sind diese rein informativ. Die Einträge sind frei wählbar und jeweils optional.

Parameter	Beschreibung
 System description	Kurzbeschreibung des Systems. Diese wird auch als Titel im Browser beziehungsweise Browser-Tab der Administrationsoberfläche angezeigt.
 System location	Standort des Systems
 System object ID	Eigene ID des Systems
 System contact	Ansprechperson für das System

Parameter	Beschreibung
 System name	Name des Systems

Sektion IP addresses

Parameter	Beschreibung
 ☒ Interface 1	Im Standard ist diese Option aktiv. Eingabemaske für IP-Adresse mit Subnetzmaske (sofern die Einstellung Virtualisation tools ^[246] Microsoft Azure ^[246] Enable Microsoft Azure guest agent ^[246] nicht aktiv ist) und den Medientyp der physischen Netzwerk Schnittstelle LAN1 bzw. eth0 oder auch vic0. In den meisten Umgebungen sollte der Medientyp auf dem Standardwert autoselect belassen bleiben. Für jede physisch vorhandene Netzwerk-Schnittstelle wird jeweils eine Schnittstellen-Konfiguration angezeigt. Die hier angezeigte Schnittstellen-Nummer entspricht der folgenden Netzwerk-Schnittstelle: Interface 1 - LAN1 bzw. eth0 oder auch vic0 bei virtuellen Appliances
 ☐ Interface 2 - 4 (optional)	Diese Optionen sind im Standard inaktiv. Wie bei Interface 1 jedoch jeweils für Interface 2 - LAN2 bzw. eth1 oder auch vic1 Interface 3 - LAN3 bzw. eth2 oder auch vic2 Interface 4 - LAN4 bzw. eth3 oder auch vic3
 ☐ Team / bond interfaces (optional)	Diese Option ist im Standard inaktiv. Durch das Verwenden dieser Einstellung können mehrere Interfaces gebündelt und logisch wie eines verwendet werden. Dabei gibt es unterschiedliche Verfahren:
 broadcast	Dient der Ausfallsicherheit. Nutzung mehrerer Switches gleichzeitig möglich.
 failover	Dient der Ausfallsicherheit. Nur ein Interface ist aktiv, bei Ausfall wird auf das nächste übergegangen. Nutzung mehrerer Switches möglich.
 lacp	Basiert auf 802.3ad. Dient der Lastverteilung sowie Ausfallsicherheit. Bündeln mehrerer Schnittstellen für das Erhöhen der möglichen Bandbreiten. Anbindung an nur einen Switch mit entsprechender Protokollunterstützung möglich.
 loadbalance	Dient der Lastverteilung. Jeder Gegenstelle im Netzwerk ein zu nutzendes Interface zugewiesen.
 roundrobin	Basiert auf 802.3ad. Dient der Lastverteilung sowie Ausfallsicherheit. Verfügbare Interfaces werden in Senderichtung wechselweise genutzt, in Empfangsrichtung kann maximal die Geschwindigkeit eines einzelnen Interfaces genutzt werden.
 Custom hosts file entries: (optional)	Ermöglicht eine lokalen Namensauflösung. Hierfür muss eine Kombination von IP-Adressen und Hostname/n eintragen werden. Format: 62.2.145.228 update.seppmail.ch support.seppmail.ch

Parameter	Beschreibung
	193.239.220.29 pool.ntp.org

Sektion IP ALIAS addresses (optional)

Werden mehrere SEPPmail Appliances in einem Cluster-Verbund betrieben (siehe auch [Clustern mehrerer Systeme](#)¹⁶⁸ ff.), so können diese gemeinsam über eine oder auch mehrere virtuelle IP-Adressen angesprochen werden. Die Stellung der einzelnen Maschine innerhalb dieses Verbundes wird über die Priorität (**Priority**²²⁷) definiert.



Hinweis:

Um die Funktion des CARP-Protokolls - welches die Basis für das Bereitstellen virtueller IP-Adressen bildet - zu gewährleisten, müssen bei virtuellen Appliances gegebenenfalls folgende Einstellungen vorgenommen werden:

- **Microsoft Hyper-V**

Option „Spoofing von MAC-Adressen aktivieren“ in der Konfiguration der virtuellen Netzwerkkarte aktivieren.

Diese Option ist in den Hyper-V Einstellungen der virtuellen Maschine unter „Netzwerkkarte - > Erweiterte Features“ zu finden.

- **ESX**

„promiscuous mode“ in der Konfiguration der virtuellen Netzwerkkarte aktivieren.

Diese Option ist in den ESX Einstellungen wie folgt vorzunehmen:

1. Im „vSphere Web Client“ zum entsprechenden „Host“ navigieren
2. Anwählen der Registerkarte „Verwalten“
3. Anwählen „Virtuelle Switches“ in der Auswahl rechts der Registerkarte
4. Anwählen des umzustellenden „Switches“
5. Anwählen der Option „Einstellungen bearbeiten“ durch Klick auf das Bleistift-Symbol
6. Anwählen „Sicherheit“ in der Auswahl rechts des Fensters
7. Option „Promiscuous-Modus“ über das Auswahlmenü auf „Akzeptieren“ stellen und mit „OK“ bestätigen



Je nach ESX Version kann es sein, dass die Sicherheitseinstellungen gesplittet wurden. Für diesen Fall sollten auf dem vSwitch die Optionen

- Promiscuous Mode
- Gefälschte Übertragung
- MAC Adressänderung

aktiv sein, damit CARP / VRRP korrekt arbeitet.

Hinweis:

Die genannten Einstellungen sind bei jedem physikalischen Switch ebenfalls aktiv, so dass hier kein Sicherheitsrisiko zu erwarten ist.

Sollte diese Einstellung aus revisionstechnischen Gründen dennoch nicht möglich sein, so muss entweder

- auf virtuelle IP-Adressen verzichtet und ein Fail-Over über andere Mittel sichergestellt werden.
- einen separaten vSwitch für die SEPPmail Appliances erstellt werden.



**Hinweis:**

Virtuelle IP-Adressen dienen ausschließlich dem Ansprechen eines Clusters von außen. Wird eine E-Mail von einer Cluster-Maschine versandt, so geschieht dies immer mit der physikalischen IP-Adresse der jeweiligen Maschine.

Parameter	Beschreibung												
 ☐ IP alias 0-3	Im Standard sind diese Optionen inaktiv. An dieser Stelle können virtuelle IP-Adressen definiert werden, welche in der Regel bei Cluster Konfigurationen (siehe auch Clustern mehrerer Systeme ¹⁶⁸ ff.) zum Einsatz kommen (siehe Menü Cluster ³⁸³). Hierzu ist es erforderlich für jeden Alias 1. eine IP-Adresse 2. die Netzwerkmaske 3. die VHID (Virtual Host Identification) 4. das Interface an welches der Alias gebunden werden soll 5. die Priorität der Schnittstelle im Verbund (Primary, Secondary, Backup) anzugeben. <table><tr><th>IP-Adresse</th><th>Subnetz</th><th>VHID</th><th>Interface</th><th>Password</th><th>Priority</th></tr><tr><td>Angabe der virtuellen IP-Adresse auf welche die Systeme gemeinsam reagieren sollen.</td><td>Angabe des Subnetzes als CIDR Notation, zum Beispiel /24 für C-Klasse</td><td>Die VHID (Virtual Host Identification) muss bei allen Maschinen, welche ebenfalls auf die eingetragene virtuelle IP reagieren sollen gleich sein.</td><td>Angabe der Netzwerk Schnittstelle (siehe Sektion IP addresses), an welche die virtuelle IP gebunden werden soll.</td><td>Optionales CARP-Passwort. Wird ein Passwort gesetzt, so muss dieses auf allen Cluster Partnern identisch sein.</td><td>Stellung der einzelnen Maschine innerhalb dieses Verbundes. Mögliche Werte: Primary Secondary Backup</td></tr></table>  Achtung: Aufgrund des Designs von VRRP/CARP, werden bei selber VHID und unterschiedlichen Passwörtern unterschiedliche „Cluster“ erstellt. Das kann im ungünstigsten Fall zu doppelten IP-Adressen im Netzwerk führen. Zu erkennen ist dies, wenn mehrere Maschinen für denselben IP ALIAS den Status MASTER haben. Aus diesem Grund ist bei Verwenden eines CARP-Passwortes unbedingt darauf zu achten, dass an allen Maschinen dasselbe Passwort verwendet wird!	IP-Adresse	Subnetz	VHID	Interface	Password	Priority	Angabe der virtuellen IP-Adresse auf welche die Systeme gemeinsam reagieren sollen.	Angabe des Subnetzes als CIDR Notation, zum Beispiel /24 für C-Klasse	Die VHID (Virtual Host Identification) muss bei allen Maschinen, welche ebenfalls auf die eingetragene virtuelle IP reagieren sollen gleich sein.	Angabe der Netzwerk Schnittstelle (siehe Sektion IP addresses), an welche die virtuelle IP gebunden werden soll.	Optionales CARP-Passwort. Wird ein Passwort gesetzt, so muss dieses auf allen Cluster Partnern identisch sein.	Stellung der einzelnen Maschine innerhalb dieses Verbundes. Mögliche Werte: Primary Secondary Backup
IP-Adresse	Subnetz	VHID	Interface	Password	Priority								
Angabe der virtuellen IP-Adresse auf welche die Systeme gemeinsam reagieren sollen.	Angabe des Subnetzes als CIDR Notation, zum Beispiel /24 für C-Klasse	Die VHID (Virtual Host Identification) muss bei allen Maschinen, welche ebenfalls auf die eingetragene virtuelle IP reagieren sollen gleich sein.	Angabe der Netzwerk Schnittstelle (siehe Sektion IP addresses), an welche die virtuelle IP gebunden werden soll.	Optionales CARP-Passwort. Wird ein Passwort gesetzt, so muss dieses auf allen Cluster Partnern identisch sein.	Stellung der einzelnen Maschine innerhalb dieses Verbundes. Mögliche Werte: Primary Secondary Backup								

**Sektion SMTP loadbalancer** (optional)

Dient der Lastverteilung bei Betrieb eines Clusters.

Parameter	Beschreibung
 ☐ Enable load balancer	Im Standard sind diese Optionen inaktiv. Das SMTP Loadbalancing reicht erst nach Erreichen der definierten gleichzeitigen Verbindungen (siehe number of active connections before balancing) E-Mails an

Parameter	Beschreibung
	die eingetragenen Cluster-Partner (siehe Distribute load to the following cluster members) weiter.
 Distribute load to the following cluster members	An dieser Stelle werden die IP-Adressen der Cluster-Partner für das Loadbalancing eingegeben. Die IP-Adressen werden im Eingabefeld durch ein Leerzeichen getrennt.
 number of active connections before balancing (default: 4):	Definition der Anzahl gleichzeitiger Verbindungen, ab welcher E-Mails an die eingetragenen Cluster-Partner weitergeleitet werden sollen. Das heißt im Standard (4) wird die fünfte Verbindung an den ersten - unter Distribute load to the following cluster members eingetragenen - Cluster-Partner weitergegeben, die neunte Verbindung an den zweiten und so weiter.

Sektion **Name**

Der Name des Systems setzt sich aus dem Hostnamen und der Domäne zusammen, zum Beispiel securemail.meinefirma.tld.

Diese Einstellungen sind die interne Sicht, sie müssen also nicht den Daten, wie sie vom Internet her Gültigkeit hätten, entsprechen.

Parameter	Beschreibung
 Hostname	Eingabe des Host-Namens der SEPPmail Appliance, zum Beispiel securemail
 Domain	Eingabe der Domäne des SEPPmail Appliance Systems, zum Beispiel meinefirma.tld.

Hinweis:



Mit dem hier eingetragenen Hostname meldet sich die SEPPmail Appliance auch beim „HELO“. Prüfen Gegenstellen im Rahmen von AntiSpam oder TLS^[282] - insbesondere in Microsoft 365 Infrastrukturen (siehe gegebenenfalls auch **Anbinden von MS Office365 unter Beibehaltung von ATP / EOP**^[789]) den Namen im „HELO“ Kommando, so muss dieser unter Umständen einen vollständigen FQDN enthalten und mit dem Antragsteller (siehe **Name (CN)**^[319], beziehungsweise **Subject Alternate Name (SAN)**^[320] des unter **SSL**^[319] eingetragenen Zertifikats übereinstimmen.
Bei Bedarf kann in der Option **SMTP server HELO string**^[253] ein vom hier eingetragenen Hostname abweichender Name angegeben werden.

Sektion **Routing**

Parameter	Beschreibung
 Default gateway	Angabe der Gateway-Adresse passend zum Netzwerksegment (IP und Netzmaske wie sie unter IP addresses ^[225] eingegeben wurden). An dieses Gateway werden alle Datenpakete weitergeleitet, welche an Zieladressen außerhalb des lokalen Netzwerksegments gesendet werden sollen.
 Static routes (optional)	Sollten Verbindungen zu Netzen hergestellt werden müssen, welche nicht über das default gateway erreichbar sind, so können an dieser Stelle die entsprechenden Netze mit ihrem Subnetz jeweils unter Destination und das jeweils dorthin führende Gateway

Parameter	Beschreibung
	angegeben werden. Diese statischen IP-Routen haben Priorität vor dem Verwenden des Standard-Routers (default gateway). Nach dem Speichern einer statischen Route wird jeweils ein weiteres Eingabefeld eingeblendet.

Sektion DNS

Parameter	Beschreibung
 ☒ Use built-in DNS resolver	Standardeinstellung. Bei diesem Parameter versucht das System die DNS-Namensauflösung immer mit Hilfe der DNS-Root-Nameserver im Internet. Ist dieser Parameter ausgewählt, so kann das Auflösen von DNS-Namen gegebenenfalls sehr lange dauern und die Reaktion der SEPPmail Appliance dadurch verzögert werden. Diese Einstellung ist in der Regel dann zu wählen, wenn die SEPPmail Appliance direkt - also ohne zwischengeschaltetes Relay - in das Internet sendet.
 ☐ Use the following DNS servers	DNS-Anfragen für Adressen, für welche die SEPPmail Appliance nicht selbst zuständig ist, werden an übergeordnete DNS-Name-Server weitergeleitet. Dazu sollte SEPPmail Appliance die DNS-Anfrage zunächst an einen internen DNS-Server im eigenen Netzwerk oder die DNS-Server Ihres Internet Providers weitergeben, welche hier spezifiziert werden können.
 ☐ Disable early refresh of cache records (cache prefetch)	Diese Option ist im Standard inaktiv. Deaktiviert das Vorab-Befüllen des DNS-Zwischenspeichers. Dadurch kann das Auflösen von Namen länger dauern, das Ergebnis ist jedoch gegebenenfalls aktueller.
 ☐ Prefer IPv6 addresses in replies	Diese Option ist im Standard inaktiv. Bevorzugt IPv6 Antworten des DNS-Servers.
 Primary	Eingabe des ersten DNS-Server, an welchen die SEPPmail Appliance DNS-Anfragen weiterleiten soll.
 Alternate 1 (optional)	Ist der primäre DNS-Server nicht verfügbar oder antwortet nicht wird die DNS-Anfrage an den hier eingetragenen, alternativen DNS-Server weitergeleitet.
 Alternate 2 (optional)	Sind weder der primäre noch der erste alternative DNS-Server verfügbar, so wird die DNS-Anfrage an den hier eingetragenen, zweiten alternativen DNS-Server weitergeleitet.
 Search domain(s) (optional)	Suchliste mit Domänen Namen, welche bei einer DNS-Anfrage nacheinander abgefragt werden.
 add local zone (optional)	Lokale Zonen werden verwendet, wenn jeweils mehrere Forwarding- und/oder SMTP-Server angesprochen werden sollen, für das Auflösen der hierfür benötigten MX-Records jedoch kein lokaler DNS-Server zur Verfügung steht. Nach dem Speichern wird jeweils ein weiteres Eingabefeld eingeblendet. In den unten dargestellten Beispiel Eintragungen würde für die Domäne pseudo.local vorrangig in mail1.pseudo.local mit der IP-Adresse 10.0.0.11 aufgelöst da dieser die Präferenz 10 aufweist. Sollte der Server mail1.pseudo.local nicht erreichbar sein, wird der Eintrag mit der Präferenz 20, also mail2.pseudo.local mit der IP-Adresse 10.0.0.12 verwendet.

Parameter	Beschreibung				
	Domain name:	Pseudo Domänen Name, welcher intern in der SEPPmail Appliance als MX-Record aufgelöst werden soll, zum Beispiel pseudo.local .			
	host:	Hostname, zum Beispiel mail1	mx:	Präferenz, zum Beispiel 10	ip: IP-Adresse des ersten E-Mail Servers, zum Beispiel 10.0.0.11
	host:	Hostname, zum Beispiel mail2	mx:	Präferenz, zum Beispiel 20	ip: IP-Adresse des zweiten E-Mail Servers, zum Beispiel 10.0.0.12

Sektion **Admin GUI**

Definiert die Einstellungen für den Zugriff auf die Administrationsoberfläche.

Parameter	Beschreibung
 ☐ HTTP port	Diese Option ist im Standard inaktiv und mit dem Wert 8080 vorbelegt. Ermöglicht den unverschlüsselten Zugriff auf die Konfigurationsoberfläche über das HTTP Protokoll.
 ☒ HTTPS port	Im Standard ist diese Option aktiv und mit dem Wert 8443 vorbelegt. Ermöglicht den verschlüsselten Zugriff auf die Konfigurationsoberfläche über das HTTPS Protokoll. Das für den Zugriff verwendete Zertifikat ist unter SSL [319] zu sehen.
 Admin GUI session timeout:	Im Standard ist diese Option mit dem Wert 1800 vorbelegt. Zeit in Sekunden bis zum automatischen Logout aus der Konfigurationsoberfläche bei Inaktivität. Nach einem automatischen Logout wird bei erneutem Login das zuletzt geöffnete Konfigurationsmenü angezeigt.
 Bind to IP addresses (use space to separate multiple IPv4 or IPv6 addresses)	Durch Angabe der IP Adresse eines bestimmten Netzwerk Interfaces (siehe IP addresses [225] Interface <n>) kann der Zugriff auf die Administrationsoberfläche auf diese(s) Netzwerk Interface(s) beschränkt werden. Die Eingabe mehrerer Adressen ist durch Trennen mittels Leerzeichen möglich. Wird zusätzlich der SMTP-Verkehr auf ein anderes Interface gebunden (siehe Mail System [247] SMTP settings [252] SMTP bind address [253]), so wird dadurch ein sauberes Trennen des administrativen und des Nutzdatenverkehrs (E-Mails) erreicht (Stichwort Administrationsnetz).

Sektion **GINA GUI**

Definiert die Einstellungen für den Zugriff auf das GINA-Portal.



Hinweis:

Unabhängig von den in den folgenden Optionen eingestellten Ports, wird der im html-Anhang einer GINA-E-Mail enthaltene Link immer auf den Standard HTTPS Port 443 verweisen. Nur so kann gewährleistet werden, dass die Verbindung zwischen GINA-Empfänger und dem GINA-Portal nicht von einer Firewall blockiert wird. Die Einstellbarkeit der Ports soll ausschließlich dem Ermöglichen eines internen Portforwardings dienen.

Parameter	Beschreibung
 ☐ HTTP port	Diese Option ist im Standard inaktiv und mit dem Wert 80 vorbelegt. Ermöglicht den unverschlüsselten Zugriff auf die Web-Mail Schnittstelle der SEPPmail Appliance (GINA) über das HTTP Protokoll. Achtung: Das HTTP-Protokoll sollte nicht für einen Zugriff auf die Web-Mail Schnittstelle aus dem Internet oder aus einem anderen unsicheren Netzwerk verwendet werden. Hierdurch würde das Protokollieren von Webbrowser Verbindungen zur Web-Mail Schnittstelle der SEPPmail Appliance durch unbefugte Dritte ermöglicht. Diese Einstellung wird in der Regel nur dann benötigt, wenn bereits eine vorgeschaltete Komponente den SSL Tunnel zum GINA-Portal terminiert. 
 ☒ HTTPS port	Im Standard ist diese Option aktiv und mit dem Wert 443 vorbelegt. Ermöglicht den verschlüsselten Zugriff auf die Web-Mail Schnittstelle der SEPPmail Appliance (GINA) über das HTTPS Protokoll. Sollte die SEPPmail Appliance HTTPS Anfragen nicht direkt aus dem Internet entgegennehmen, so kann der Port angepasst werden, um zum Beispiel ein Portforwarding einer vorgeschalteten Sicherheitskomponente zu nutzen. Achtung: Der Link innerhalb der „secure-email.html“ aus der GINA-Träger-E-Mail ist statisch auf Port 443 gesetzt. Nur durch das Verwenden des HTTPS-Standard-Ports kann an dieser Stelle der zuverlässige Verbindungsaufbau zurück zur SEPPmail Appliance - auch durch gegebenenfalls zwischengeschaltete Firewalls hindurch - gewährleistet werden. Das für den Zugriff verwendete Zertifikat ist unter SSL ^[319], beziehungsweise bei aktiviertem „Virtual hosting“ (siehe GINA Domains ^[416] GINA settings ^[416] unter CHANGE GINA SETTINGS FOR ^[423] Secure GINA host ^[423] zu sehen. 
 ☐ Enable local https proxy, redirect unknown requests to (optional)	Diese Option ist im Standard inaktiv. Stellt den Zugang zum Web-Mail Subsystem (GINA-Portal) nicht mehr direkt sondern über den lokalen SEPPmail Appliance Reverse-Proxy her. Alle nicht für das Web-Mail bestimmten Anfragen werden dadurch an die eingetragene Server-Adresse weitergeleitet. Hierdurch kann zum Beispiel der Zugang zu einem internen OWA-(Outlook Web Access) Server mit nur einer externen IP-Adresse gewährleistet werden. Ebenfalls können ActiveSync Verbindungen zum internen Microsoft Exchange Server durch den Reverse-Proxy weitergeleitet werden. Hinweis: Hier darf ausschließlich die IP-Adresse oder der FQDN eingetragen werden, über welche(n) der nachfolgende Server erreichbar ist, keine komplette URL: richtig 192.168.1.10 oder mycompany.local falsch 192.168.1.10/owa oder mycompany.local/owa 

Parameter	Beschreibung
	 Achtung: Diese Einstellung hebt eine auch unter CHANGE GINA SETTINGS FOR ⁴²³ Extended settings ⁴³¹ Default Forward Page ⁴³¹ vorgenommene Einträge aus. Weiterhin können bei RPC over HTTPS (zum Beispiel Outlook Anywhere) unter Umständen Probleme auftreten.
 ☐ Enable high-performance mode (RAM usage increases considerably)	Diese Option dient dem Beschleunigen der GINA.  Hinweis: Das Verwenden dieser Option erhöht den Speicherbedarf (RAM) und sollte nur bei Bedarf aktiviert werden.

Sektion RestAPI (neu in 12.1)

Definiert die Einstellungen für den API Zugriff (siehe auch **API Funktionen** ⁶⁴⁶), beziehungsweise <https://docs.seppmail.com/api/> auf die SEPPmail Appliance.

Parameter	Beschreibung
 ☐ enabled	Diese Option ist im Standard inaktiv. Schaltet den API Zugriff grundsätzlich ein.
 HTTPS port	Im Standard ist dieses Eingabefeld mit dem Wert 8445 vorbelegt. Gibt den Port für API Zugriffe an. Die zugriffe finden grundsätzlich SSL gesichert über das HTTPS Protokoll statt.
 RESTAPI keys	
 New API Token	Wurde noch keine Konfiguration vorgenommen, so ist dies die erste und einzige Anzeige. Andernfalls steht dieses Feld unterhalb der bereits eingerichteten Zugänge.
 ☐ Active	Diese Option ist im Standard inaktiv. Aktiviert den zu generierenden Zugang automatisch nach dem Erstellen.
 Display name	Im Standard ist dieses Eingabefeld leer. Hier sollte ein aussagekräftiger Name für den einzurichtenden Zugang.
 API token	Im Standard ist dieses Eingabefeld leer. Ein Token kann über Generate weiter unten im Abschnitt generiert werden. Alternativ kann hier auch eine Zeichenfolge eingegeben werden.
 API secret	Im Standard ist dieses Eingabefeld leer. Mit dem Generieren eines API token via Generate wird auch ein API secret generiert. Alternativ kann auch hier eine Zeichenfolge eingegeben werden. Mittels  wird dieses Secret angezeigt
 Access	In den Teilabschnitten dieser Option werden die Zugriffsberechtigungen für den anzulegenden Zugang vergeben.
 Modules 	Im Auswahl-Menü... https://app.swaggerhub.com/apis-docs/SEPPmail/seppmail_rest_api/

Parameter		Beschreibung
	Search	steht über das Eingabefeld eine Suchfunktion für die verfügbaren Berechtigungen zur Verfügung.
	(un)select all	können mittels select all , beziehungsweise unselect all alle Berechtigungen gleichzeitig aktiviert oder deaktiviert werden.
	Customers	Berechtigt für den Zugriff auf die API-Befehle zu „customer“ (siehe https://app.swaggerhub.com/apis-docs/SEPPmail/seppmail_rest_api/customer) für Tenant Einstellungen (vergleiche auch Customers ^[494] ^[494]).
	Groups	Berechtigt für den Zugriff auf die API-Befehle zu „group“ (siehe https://app.swaggerhub.com/apis-docs/SEPPmail/seppmail_rest_api/group) für Gruppen Einstellungen (vergleiche auch Groups ^[413] ^[494]).
	Info / Encryption Info	Berechtigt für den Zugriff auf die API-Befehle zu „info“ (siehe https://app.swaggerhub.com/apis-docs/SEPPmail/seppmail_rest_api/info). Damit können die für eine oder mehrere Zieladressen verfügbaren Verschlüsselungs-Modi ausgelesen werden.
	Mail System / Domain	Berechtigt für den Zugriff auf die API-Befehle zu „mail system / managed domain“ (siehe https://app.swaggerhub.com/apis-docs/SEPPmail/seppmail_rest_api/mail%20system) für Einstellungen rund um Managed Domains ^[247] (vergleiche auch Add Managed Domain ^[266] , beziehungsweise Edit Managed Domain ^[266] ^[494]).
	Mail System / Templates and Disclaimers	Berechtigt für den Zugriff auf die API-Befehle zu „mail system / template“ für das Bearbeiten von E-Mail Vorlagen (vergleiche auch Edit Template ^[264] ^[494] , beziehungsweise „mail system / disclaimer“ (siehe https://app.swaggerhub.com/apis-docs/SEPPmail/seppmail_rest_api/mail%20system) für das Bearbeiten von Disclaimern (vergleiche auch Edit Disclaimer ^[267] ^[494]).
	Statistics	Berechtigt für den Zugriff auf die API-Befehle zu „statistics“ (siehe https://app.swaggerhub.com/apis-docs/SEPPmail/seppmail_rest_api/statistics) für Statistik Abfragen (vergleiche auch Statistics ^[394] , beziehungsweise Daily Report ^[96]).
	Users	Berechtigt für den Zugriff auf die API-Befehle zu „user“ (siehe https://app.swaggerhub.com/apis-docs/SEPPmail/seppmail_rest_api/user) für Einstellungen Rund um die SEPPmail Appliance-Benutzer (vergleiche auch Users ^[396] ^[494]).
	Webmail Accounts	Berechtigt für den Zugriff auf die API-Befehle zu „webmail“ (siehe https://app.swaggerhub.com/apis-docs/SEPPmail/seppmail_rest_api/webmail) für Einstellungen Rund um die GINA-Empfänger (vergleiche auch GINA Accounts ^[462] ^[494]).
	MSP token	☐ Diese Option ist im Standard inaktiv. Wird die Option aktiviert, so wird ein Token mit Zugriff auf alle bestehenden und zukünftigen Tenants generiert. Die Option Assigned tenants bleibt deshalb ausgegraut.
	Assigned tenants 	Im Auswahl-Menü...
	Search	steht über das Eingabefeld eine Suchfunktion für die verfügbaren Tenants zur Verfügung.
	select all	können mittels select all alle verfügbaren Tenants gleichzeitig ausgewählt werden.
	Default Customer	Der Tenant "Default Customer" ([default] vergleiche Customers ^[494] ^[494]) steht in jedem mandantenfähigen System zur Verfügung
		 Hinweis: Nur bei aktivierter mandantenfähigkeit (siehe Customers ^[494]) sichtbar.

Parameter	Beschreibung
 <Customer>	Für jeden angelegten Tenant existiert jeweils ein eigenes Auswahlkästchen
	Durch Klicken von Generate wird ein API token sowie ein zugehöriges API secret generiert. Über Add wird der der Zugang übernommen.
Wurden bereits Zugangsdaten eingerichtet, so werden diese wie angelegt angezeigt:	
 Active	Im Standard hat diese Option den beim Erstellen eingestellten Status. Aktiviert / Deaktiviert den jeweiligen Zugang.
 Display name	Der Display name ist bei bestehenden Zugängen nicht veränderbar.
 API token	Der API token ist bei bestehenden Zugängen nicht veränderbar Über  kann der API token in die Zwischenablage kopiert werden.
 API secret	Das API secret kann bei Bedarf gewechselt werden. Über die Schalter Mittels  wird das aktuelle Secret angezeigt.  kann das API secret in die Zwischenablage kopiert werden.  kann ein neues API secret generiert werden.
 Access	In den Teilabschnitten dieser Option können die Zugriffsberechtigungen für jeweiligen Zugang angepasst werden. Die Beschreibung zu den Teilabschnitten ist identisch zu New API token ^[232] Access ^[232] oberhalb und wird deshalb hier nicht erneut gelistet.

Sektion **Key server**

Ermöglicht das maschinelle Abfragen öffentlicher Schlüssel der lokalen Benutzer.

Parameter	Beschreibung
 Enable S/MIME and PGP key server on port 1389 (LDAP) and 1636 (LDAPS)	Diese Option ist im Standard inaktiv. Aktiviert die Key Server Funktion der SEPPmail Appliance. Hierdurch werden die öffentlichen Schlüssel - sowohl S/MIME als auch OpenPGP - der SEPPmail Appliance Users ^[395] für andere Systeme per LDAP via Port 1389, beziehungsweise LDAPS via Port 1636 zugänglich gemacht. Für die gesicherte Kommunikation via LDAPS wird das im Menü SSL ^[319] eingetragene Zertifikat verwendet. Eine Abfrage ist wie folgt möglich: URI <Protokoll>://<FQDN aus CHANGE GINA SETTINGS FOR ^[423] [default] Secure GINA host ^[423] Hostname ^[423] > BindDN / BindPW wird nicht benötigt BaseDN wird nicht benötigt, wenngleich dc=keyserver funktioniert.

Parameter	Beschreibung										
	 Hinweis: Für das Verwenden dieser Key Server Funktion wird das Vorschalten einer Firewall mit entsprechendem Port-Mapping empfohlen: <table><tr><th>Quelle</th><th>Port</th><th>Ziel</th><th>Port</th></tr><tr><td rowspan="2">Internet</td><td>389 (LDAP)</td><td rowspan="2">SEPPmail Appliance</td><td>1389 (LDAP)</td></tr><tr><td>636 (LDAPS)</td><td>1636 (LDAPS)</td></tr></table>	Quelle	Port	Ziel	Port	Internet	389 (LDAP)	SEPPmail Appliance	1389 (LDAP)	636 (LDAPS)	1636 (LDAPS)
Quelle	Port	Ziel	Port								
Internet	389 (LDAP)	SEPPmail Appliance	1389 (LDAP)								
	636 (LDAPS)		1636 (LDAPS)								

Sektion Console login (optional)

Definiert die Einstellungen für den Zugriff auf die Console (CLI) der Appliance.

Parameter	Beschreibung
 ☐ Disable console root login	Diese Option ist im Standard inaktiv. Deaktiviert den Konsolenzugang (CLI) der SEPPmail Appliance.  Hinweis: Bitte beachten Sie beim Aktivieren dieses Parameters, dass in diesem Fall ein gewollter Zugang zum System im Fehlerfall ebenfalls nicht mehr möglich ist.
 ☐ Redirect console to serial port	Diese Option ist im Standard inaktiv. Ermöglicht den Zugriff auf das Command Line Interface (CLI) über den seriellen Port.  Hinweis: Für die serielle Verbindung muss die Baudrate 115200 gewählt werden. Weitere Einstellungen sollten nicht erforderlich sein.

Sektion Syslog settings (optional)

Ermöglicht das Weiterleiten von Log-Einträgen an einen SysLog-Server. Mehrere Server können jeweils durch Semikolon „;“ getrennt eingetragen werden. Im Standard wird der Port UDP/514 für das Übertragen der Meldungen verwendet.

Bei Bedarf können Protokoll sowie Ziel-Port optional in der Form **[protocol]host[:port]** mit angegeben werden, zum Beispiel tcp://192.168.10.60:1514.

Parameter	Beschreibung
 Forward maillog and authlog to this syslog server	SysLog-Server an welchen die SEPPmail Appliance Mail-, Authentifizierungs- und System-Log-Protokolle senden soll.

Parameter	Beschreibung
 Forward GUI audit log to this syslog server	SysLog-Server an welchen die SEPPmail Appliance Log-Protokolle der Aktionen aus der Administrationsoberfläche senden soll.
 Forward GINA log to this syslog server:	SysLog-Server an welchen die SEPPmail Appliance GINA-Protokolle senden soll.
 ☐ Disable logging to local maillog	Diese Option ist im Standard inaktiv. Deaktiviert sowohl das lokale Schreiben des Mail Logs, als auch die relevanten Statistiken.

Sektion **Log cleanup** (optional)

Parameter	Beschreibung
 ☐ Automatically delete log archives older than days	Diese Option ist im Standard inaktiv und mit dem Wert 1095 vorbelegt. Löscht automatisch alle Logs ³⁸⁸, welche älter als die eingestellte Anzahl von Tagen sind. Durch das automatische Löschen der Log-Archive kann • ein „Volllaufen“ der Log-Partition vermieden werden. • Revisionsvorgaben bezüglich des Vorhaltens von Daten entsprochen werden. Als Eingabe werden Werte von 1 bis 3650 akzeptiert. Dabei wird bei der Angabe von Werten ≥ 30 die Standard-Log-Rotation verwendet. Bei dieser wird das E-Mail-Log bei Erreichen einer Größe von 30 MB, das GINA-Log bei Erreichen einer Größe von 10 MB zunächst archiviert und jeweils eine neue Log-Datei begonnen. Da somit nicht Tag genau gelöscht werden kann, eignet sich dieses Verfahren in erster Linie, um ein Volllaufen der Log-Partition zu verhindern. Bei Einstellen eines Wertes ≤ 29 rotiert das Log hingegen täglich. Somit eignet sich dieses Verfahren zum Beispiel für das Einhalten von Revisionsvorgaben bezüglich des Zeitraumes für das Vorhalten von Daten.  Hinweis: In mandantenfähigen Systemen ist zu beachten, dass diese Logs somit auch nicht mehr für den Mandanten Admin auf der Appliance zur Verfügung stehen.

Sektion **Proxy settings** (optional)

Hier müssen nur dann entsprechende Einstellungen vorgenommen werden, wenn ein direkter Zugriff der Appliance per SSH (siehe **Use direct connection on port 22 outgoing (preferred)**) in das Internet nicht möglich ist.



Hinweis:

Die hier vorgenommenen Einstellungen werden gegebenenfalls auch für den Bezug von Signatur-Dateien des Protection Packs verwendet.

Wird die Verbindung über einen Proxy hergestellt, so wird die Port 22 Verbindung über HTTPS getunnelt.

Über das "Recovery console menu" (siehe **Rudimentäre Systembefehle** ¹⁸⁹ Option "6) Port probe") kann dann der Zugang nicht mehr direkte getestet werden.

Hiefür ist nach Aufruf der Option unter

Enter Server:

die IP

127.0.0.1

und unter

Enter Port:

die Nummer:

23

einzugeben.

Als Antwort sollte

Connection to 127.0.0.1 23 port [tcp/telnet] succeeded!

gezeigt werden.

Falls nicht, kann die SEPPmail Appliance die Verbindung zum Proxy Server nicht herstellen. Dann wären die Proxy Einstellungen erneut zu prüfen.

Falls diese Prüfung erfolgreich ist, die Verbindung in der Administrationsoberfläche jedoch nicht zustande kommt ist anzunehmen, dass die Anfrage am Proxy hängen bleibt.

Parameter	Beschreibung
 Proxy server	Hostname oder IP-Adresse des Proxy-Servers, über welchen die SSH Kommunikation geleitet werden soll.
 Proxy port	Ziel Port des Proxy-Servers, zum Beispiel 8080 oder 8081
 Proxy user (optional)	Benutzername für das Anmelden am Proxy-Server sofern diese notwendig ist.
 Proxy password (optional)	Kennwort für das Anmelden am Proxy-Server
 Use direct connection on port 22 outgoing (preferred)	Standardeinstellung. Diese Option muss aktiviert werden, wenn eine SSH-Verbindung direkt und ohne Umweg über einen Proxy-Server ins Internet möglich ist.
 Connect through SOCKS 4 proxy	Diese Option muss aktiviert werden, um SSH-Verbindungen durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, die Verbindung jedoch über einen SOCKS-Proxy (Version 4) ins Internet möglich ist.
 Connect through SOCKS 5 proxy	Diese Option muss aktiviert werden, um SSH-Verbindungen durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, die Verbindung jedoch über einen SOCKS-Proxy (Version 5) ins Internet möglich ist.
 Connect through HTTP proxy	Diese Option muss aktiviert werden, um SSH-Verbindungen durch einen HTTP-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, die Verbindung jedoch über einen HTTP-Proxy ins Internet möglich ist.
 Connect through Telnet proxy	Diese Option muss aktiviert werden, um SSH-Verbindungen durch einen Telnet-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, die Verbindung jedoch über einen Telnet-Proxy ins Internet möglich ist.
 Use port 80 instead of 22	Diese Option muss aktiviert werden, wenn eine HTTP-Verbindung direkt ins Internet möglich ist. Die SSH-Verbindung verwendet dann den Port TCP 80 (HTTP) statt TCP 22 (SSH).

Sektion **MPKI proxy settings** (optional)

Hier müssen nur dann entsprechende Einstellungen vorgenommen werden, wenn ein direkter Zugriff der jeweiligen **MPKI** ^[339] Schnittstelle auf die ausstellende Zertifizierungsstelle nicht möglich ist.

Parameter	Beschreibung
 MPKI proxy server	Hostname oder IP-Adresse des Proxy-Servers, über welchen die Kommunikation zur Zertifizierungsstelle via HTTPS Port 443 aufgebaut werden soll.
 MPKI proxy port	Ziel Port des Proxy-Servers, zum Beispiel 8080 oder 8081
 MPKI proxy user (optional)	Benutzername für das Anmelden am Proxy-Server sofern diese notwendig ist.
 MPKI proxy password (optional)	Kennwort für das Anmelden am Proxy-Server
  Use direct connection (preferred)	Standardeinstellung. Diese Option muss aktiviert werden, wenn die Verbindung zur Zertifizierungsstelle direkt und ohne Umweg via HTTPS Port 443 über einen Proxy-Server ins Internet möglich ist.
  Connect through SOCKS 4 proxy	Diese Option muss aktiviert werden, um Verbindungen zur Zertifizierungsstelle durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang ins Internet reglementiert ist, die Verbindung jedoch über einen SOCKS-Proxy (Version 4) ins Internet möglich ist.
  Connect through SOCKS 5 proxy	Diese Option muss aktiviert werden, um Verbindungen zur Zertifizierungsstelle durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang ins Internet reglementiert ist, die Verbindung jedoch über einen SOCKS-Proxy (Version 5) ins Internet möglich ist.
  Connect through HTTP proxy	Diese Option muss aktiviert werden, um Verbindungen zur Zertifizierungsstelle durch einen HTTP-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang ins Internet reglementiert ist, die Verbindung jedoch über einen HTTP-Proxy ins Internet möglich ist.

Sektion **OCSP / CRL check settings** (optional)

Über diese Sektion kann das Prüfen der Zertifikatsgültigkeit über Sperrlisten („certificate revocation list“ kurz „CRL“) und / oder das Online Certificate Status Protocol (OCSP) aktiviert werden. Für den Abruf dieser Informationen wird jeweils Zugriff zur ausstellenden Certification Authority (CA) benötigt. Hat die Appliance keine direkten Zugriff auf das Internet, so kann an dieser Stelle zusätzlich die Verbindung über einen Proxy-Server konfiguriert werden.



Hinweis:

Benötigt das GINA Zertifikat (siehe **SSL** ^[319]) Stapling (siehe gegebenenfalls auch https://de.wikipedia.org/wiki/Online_Certificate_Status_Protocol_stapling), muss für die korrekte Funktion die Option **Connect through HTTP proxy** aktiv sein. Bei Verwenden dieser Einstellung werden eventuelle Einträge unter **Proxy user**, beziehungsweise **Proxy password** nicht an den eingetragenen **Proxy server** übergeben.

Parameter	Beschreibung
  Enable	Im Standard ist diese Option aktiv. Aktiviert das Prüfen von Zertifikaten via OCSP / CRL.

Parameter	Beschreibung
OCSP / CRL checks for S/MIME certificates.	Hinweis: Zertifikate werden automatisch immer dann geprüft, wenn sie zur Verwendung herangezogen werden, jedoch maximal einmal pro Stunde. Die ausstellende Zertifizierungsstelle meldet gemäß RFC 2560 zurück, wann Ihrerseits die • letzte Revokations-Überprüfung stattfand (This Update) • die nächste Revokations-Überprüfung stattfindet (Next Update) (ist Next Update nicht vorhanden, bedeutet dies, dass seitens der Zertifizierungsstelle permanent neue Revokations-Informationen bereit gestellt werden) • die Zeit wann diese Anfrage signiert wurde (Produced At). Die Ergebnisse der Prüfungen sind jeweils in den Zertifikatsdetails in den Menüs X-509 Certificates^[47] und X.509 Root Certificates^[48] zu finden
 Proxy server	Hostname oder IP-Adresse des Proxy-Servers, über welchen die HTTP / HTTPS Kommunikation zur Zertifizierungsstelle hin hergestellt werden soll.
 Proxy port	Ziel Port des Proxy-Servers, zum Beispiel 8080 oder 8081
 Proxy user (optional)	Benutzername für das Anmelden am Proxy-Server sofern diese notwendig ist.
 Proxy password (optional)	Kennwort für das Anmelden am Proxy-Server
  Use direct connection	Standardeinstellung. Diese Option muss aktiviert werden, wenn eine HTTP- / HTTPS-Verbindung direkt und ohne Umweg über einen Proxy-Server ins Internet möglich ist.
  Connect through SOCKS 4 proxy	Diese Option muss aktiviert werden, um HTTP- / HTTPS-Verbindungen durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via HTTP / HTTPS ins Internet reglementiert ist, die Verbindung jedoch über einen SOCKS-Proxy (Version 4) ins Internet möglich ist.
  Connect through SOCKS 5 proxy	Diese Option muss aktiviert werden, um HTTP- / HTTPS-Verbindungen durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via HTTP / HTTPS ins Internet reglementiert ist, die Verbindung jedoch über einen SOCKS-Proxy (Version 5) ins Internet möglich ist.
  Connect through HTTP proxy	Diese Option muss aktiviert werden, um HTTP- / HTTPS-Verbindungen durch einen HTTP-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via HTTP / HTTPS ins Internet reglementiert ist, die Verbindung jedoch über einen HTTP-Proxy ins Internet möglich ist.


Achtung:

Zertifikate werden nur dann nicht verwendet, wenn diese per OCSP oder CRL geprüft werden konnten und revoziert sind.
Kann ein Zertifikat nicht per OCSP oder CRL geprüft werden, so wird es dennoch verwendet.



Sektion **Time zone**

Parameter	Beschreibung
 Auswahl der Zeitzone	Auswahl der für den Standort der SEPPmail Appliance gültigen Zeitzone. Der Wechsel zwischen Sommer- und Winterzeit wird automatisch durchgeführt.

Sektion **Time and date**

Parameter	Beschreibung
 ☐ No time sync	Mit dieser Einstellung wird ausschließlich die interne Systemzeit verwendet. Diese kann über Set date and time manually entsprechend eingestellt werden. Ein automatische Abgleich mit anderen Systemen findet nicht statt!
 ☒ Use virtual host time or attached sensor	Mit der Einstellung würde die Zeit bei virtuellen Appliances mit dem Host System abgeglichen, sofern dies vom Host System unterstützt wird. Bei Hardware Systemen würde der entsprechende Sensor für den Abgleich herangezogen werden.
 ☐ Set remote NTP server	Standardeinstellung. Datum und Uhrzeit werden gegen den unter Server angegebenen Zeitserver über das Protokoll NTP, Zielport UDP 123, synchronisiert.  Hinweis: Diese Option ist für das Einrichten eines Cluster^[383] auf allen Cluster Members zwingend erforderlich. Dabei müssen auf allen Cluster Partnern dieselben Zeitserver in derselben Reihenfolge eingetragen werden. Die ausgewählte Zeitzone (siehe Time zone^[239]) spielt für die Synchronisation im Cluster keine Rolle.
 Server	Im Standard vorbelegt mit pool.ntp.org. Hostname oder IP-Adresse eines Zeitservers. Mehrere Server können jeweils durch Leerzeichen getrennt eingetragen werden. Wird ein Ziel im Internet angegeben, so ist der Zugang dorthin zu gewährleisten (siehe Firewall / Router einrichten^[135]). Gegebenenfalls ist die Angabe eines Host-Namens, der in mehrere Zeitserver aufgelöst wird (pool), für das Gewährleisten der Verfügbarkeit von Vorteil. Werden Internet Zeitserver verwendet, so sollten möglichst lokale Server verwendet werden, beispielsweise de.pool.ntp.org anstatt nur pool.ntp.org.
 ☐ Periodic updates	Diese Option ist im Standard inaktiv. Periodically adjust the clock to avoid drift in virtual machines hat ein periodisches Nachstellen der Uhrzeit mit dem Virtualisierungs-Host zur Folge.  Hinweis: Insbesondere bei Hyper-V Guest Systemen ist vereinzelt ein permanenter Clock-Drift von mehreren Sekunden pro Minute festzustellen, selbst wenn das Host-System nicht unter Last steht. Weicht die Uhrzeiten des Systems zu sehr ab, so stellt NTP die Korrektur der Systemzeit ein, da NTP zu hohe Differenzen seiner eingangs eingestellten Zeit als Fehlerfall ansieht.
 ☐ Set date and time manually	Steht kein NTP-Zugang zur Verfügung, so kann an dieser Stelle das aktuelle Datum und die aktuelle Uhrzeit manuell eingegeben werden.
 Date	aktuelles Datum im Format: dd.mm.yyyy

Parameter	Beschreibung
 Time	aktuelle Uhrzeit im Format: hh:mm:ss

Sektion `SNMP daemon` (optional)

Wird weder bei **snmp v1/2 Read-only Community** noch bei **snmp v1/2 Read-write Community** eine Eingabe gemacht, so wird **SNMP v1/2 deaktiviert**.

Für die **SNMP v3 Verschlüsselung** wird **AES** für die **Authentifikation**, **SHA** als Algorithmus verwendet.



Hinweis:

Beim Überwachen von Partitions-Auslastungen ist zu beachten, dass nur die Partitionen berücksichtigt werden, welche auch unter **Home** [\[220\]](#) **Disk statistics** [\[223\]](#) aufgeführt sind. Alle anderen Partitionen sind read-only und bis zu 100% belegt. Ein Überwachen dieser Partitionen würde somit zu permanenten Meldungen führen.

Parameter	Beschreibung
 ☐ Enable SNMP	Diese Option ist im Standard inaktiv. Aktiviert den SNMP Daemon auf der SEPPmail Appliance. Somit können über das SNMP Protokoll mit Tools, wie zum Beispiel snmpwalk, Informationen über die SEPPmail Appliance abgerufen werden.
 Listen address	IP-Adresse - IPv4 oder IPv6 - zu der sich das SNMP-Monitoring verbindet. Dies ist in der Regel die IP-Adresse der SEPPmail Appliance. Die Eingabe mehrerer Adressen ist nicht möglich.
 snmp v1/2 read-only community	Passwort für den Nur-Lese Zugriff auf die SNMP-Daten.
 snmp v1/2 read-write community	Passwort für den Schreib-Lese Zugriff auf die SNMP-Daten.
 snmp v3 user	Benutzername für den SNMP v3 Zugriff
 snmp v3 password	Passwort (User- und Privacy) für den SNMP v3 Zugriff. Dieses muss mindestens acht Zeichen lang sein.
 Download MIBs	Über die Schaltfläche können die Management Information Bases (MIB) der SEPPmail Appliance als ZIP-Datei heruntergeladen werden. Zusätzlich stehen folgende OIDs für das Überwachen weiterer Funktionen zur Verfügung: .1.3.6.1.4.1.8072.1.3.2.1.0 = INTEGER: 10 .1.3.6.1.4.1.8072.1.3.2.2.1.3.11.109.97.105.108.115.80.103.112.68.101.99.0 = STRING: mailsPgpDec .1.3.6.1.4.1.8072.1.3.2.2.1.3.11.109.97.105.108.115.80.103.112.69.110.99.0 = STRING: mailsPgpEnc .1.3.6.1.4.1.8072.1.3.2.2.1.3.13.109.97.105.108.115.83.109.105.109.101.68.101.99.0 = STRING: mailsSmimeDec .1.3.6.1.4.1.8072.1.3.2.2.1.3.13.109.97.105.108.115.83.109.105.109.101.69.110.99.0 = STRING: mailsSmimeEnc

Parameter	Beschreibung
	.1.3.6.1.4.1.8072.1.3.2.2.1.3.14.109.97.105.108.115.68.111.109.97.105.110.68.101.99.0 = STRING: mailsDomainDec .1.3.6.1.4.1.8072.1.3.2.2.1.3.14.109.97.105.108.115.68.111.109.97.105.110.69.110.99.0 = STRING: mailsDomainEnc .1.3.6.1.4.1.8072.1.3.2.2.1.3.14.109.97.105.108.115.80.114.111.99.101.115.115.101.100.0 = STRING: mailsProcessed .1.3.6.1.4.1.8072.1.3.2.3.1.1.18.109.97.105.108.101.117.101.65.99.116.105.118.101.0 = STRING: mailsInQueueActive .1.3.6.1.4.1.8072.1.3.2.3.1.1.20.109.97.105.108.101.117.101.68.101.102.101.114.114.101.100.0 = STRING: mailsInQueueDeferred .1.3.6.1.4.1.8072.1.3.2.2.1.3.20.109.97.105.108.101.117.101.73.110.99.111.109.105.110.103.0 = STRING: mailsInQueueIncoming .1.3.6.1.4.1.8072.1.3.2.3.1.1.11.109.97.105.108.115.80.103.112.68.101.99.0 = STRING: 17 .1.3.6.1.4.1.8072.1.3.2.3.1.1.11.109.97.105.108.115.80.103.112.69.110.99.0 = STRING: 14 .1.3.6.1.4.1.8072.1.3.2.3.1.1.13.109.97.105.108.115.83.109.105.109.101.68.101.99.0 = STRING: 0 .1.3.6.1.4.1.8072.1.3.2.3.1.1.13.109.97.105.108.115.83.109.105.109.101.69.110.99.0 = STRING: 0 .1.3.6.1.4.1.8072.1.3.2.3.1.1.14.109.97.105.108.115.68.111.109.97.105.110.68.101.99.0 = STRING: 0 .1.3.6.1.4.1.8072.1.3.2.3.1.1.14.109.97.105.108.115.68.111.109.97.105.110.69.110.99.0 = STRING: 2 .1.3.6.1.4.1.8072.1.3.2.3.1.1.14.109.97.105.108.115.80.114.111.99.101.115.115.101.100.0 = STRING: 6409 .1.3.6.1.4.1.8072.1.3.2.2.1.3.18.109.97.105.108.101.117.101.65.99.116.105.118.101.0 = STRING: 0 .1.3.6.1.4.1.8072.1.3.2.2.1.3.20.109.97.105.108.101.117.101.68.101.102.101.114.114.101.100.0 = STRING: 0 .1.3.6.1.4.1.8072.1.3.2.3.1.1.20.109.97.105.108.101.117.101.73.110.99.111.109.105.110.103.0 = STRING: 0  Hinweis: Die genannten OIDs geben jeweils eine Zeichenkette (STRING) mit dem entsprechenden Wert zurück. Dies ist auf ein Custom-MIB Format von net-snmp zurückzuführen. Die eigentlichen Werte werden über eine zweite, verwandte OID bereit gestellt, z.B.: .1.3.6.1.4.1.8072.1.3.2.2.1.3.11.109.97.105.108.115.80.103.112.68.101.99.0 -> "mailsPgpDec" .1.3.6.1.4.1.8072.1.3.2.3.1.1.11.109.97.105.108.115.80.103.112.68.101.99.0 -> Wert für mailsPgpDec

Parameter	Beschreibung
	 Hinweis: Bedeutung der Strings mailsInQueueIncoming -- new message queue mailsInQueueActive -- messages scheduled for delivery mailsInQueueDeferred -- messages postponed for later delivery

Sektion **NRPE daemon** (optional)

In dieser Sektion wird die Konfiguration des NRPE (Nagios Remote Plugin Executor) für das Überwachen der SEPPmail Appliance via Nagios vorgenommen.



Hinweis:

Beim Überwachen von Partitions-Auslastungen ist zu beachten, dass nur die Partitionen berücksichtigt werden, welche auch unter **Home** [Disk statistics](#) ^[223] aufgeführt sind. Alle anderen Partitionen sind read-only und bis zu 100% belegt. Ein Überwachen dieser Partitionen würde somit zu permanenten Meldungen führen.

Parameter	Beschreibung
 Enable Nagios Remote Plugin Executor	Diese Option ist im Standard inaktiv. Aktiviert den Nagios Daemon auf der SEPPmail Appliance für das Überwachen des Systems.
 Listen address	Eingabe der IP-Adresse - IPv4 oder IPv6 - zu der sich der NRPE Client verbinden soll. Die Eingabe mehrerer Adressen ist nicht möglich. Wird keine Eingabe vorgenommen, so horcht der Daemon auf allen vorhandenen Interfaces (siehe IP addresses ^[224]). (entspricht dem Parameter „server_address=“ in der NRPE Konfigurationsdatei „nrpe.cfg“)
 Listen port (above 1024)	Port auf welchem die SEPPmail Appliance NRPE Anfragen erwartet. Im Standard lautet dieser 5666. Wird ein anderer als der Standard Port verwendet, so ist darauf zu achten, dass dieser nicht durch einen anderen Dienst verwendet wird und höher als 1024 ist. Sollte irrtümlich ein bereits besetzter Port verwendet werden, würde Watchdog gegebenenfalls melden, dass der Dienst nicht läuft. (entspricht dem Parameter „server_port=“ in der NRPE Konfigurationsdatei „nrpe.cfg“)
 Allowed hosts/networks	Eingabe der zur Abfrage berechtigten IP Adressen beziehungsweise Subnetze. Die Eingabe erfolgt in der Form 192.168.0.0/24 beziehungsweise 2a00::/112. Mehrere Einträge können jeweils Komma getrennt vorgenommen werden. Wird keine Eingabe vorgenommen, so werden Anfragen von jeder beliebigen Adresse angenommen. (entspricht dem Parameter „allowed_hosts=“ in der NRPE Konfigurationsdatei „nrpe.cfg“)
 Advanced settings	Mit Aktivieren der Option Allow remote command arguments nimmt die SEPPmail Appliance auch die mit den Anfragen des NRPE Clients übergebenen Argumente an. (entspricht dem Parameter „dont_blame_nrpe=1“ in der NRPE Konfigurationsdatei „nrpe.cfg“)

Parameter	Beschreibung
	 Achtung: Das Aktivieren dieser Option kann zu Sicherheitsrisiken führen, wie • nicht autorisiertes Auslesen von publizierten Werten • Auslesen von eigentlich privaten Werten, die durch eine schwache Sicherheitslücke in der Kommandoausführung möglich werden • Ausführen von Drittprogrammen, die durch eine schwere Sicherheitslücke in der Kommandoausführung möglich werden

Folgende Nagios PlugIns sind in der SEPPmail Appliance für das Verwenden mit variablen Parametern integriert. Die Möglichkeit zum Verwenden variabler Parameter wird durch das Aktivieren der Option **Allow remote command arguments** freigeschaltet. Die jeweils zum Befehl aufgeführten Parameter sind zwingend zu übergeben.



Command	Parameter	Beschreibung
check_disk	-w \$ARG1\$	Schwellwert (in %) für freien Plattenspeicher, bei dessen Unterschreiten die Meldung „warning“ ausgegeben wird (zum Beispiel „20%“).
	-c \$ARG2\$	Schwellwert (in %) für freien Plattenspeicher, bei dessen Unterschreiten die Meldung „critical“ ausgegeben wird (zum Beispiel „10%“).
	-p \$ARG3\$	Pfad des zu überprüfenden Dateisystems (zum Beispiel „/var/log“).
check_swap	-w \$ARG1\$	Schwellwert (in %) für freien Auslagerungsspeicher (swap), bei dessen Unterschreiten die Meldung „warning“ ausgegeben wird (zum Beispiel „60%“).
	-c \$ARG2\$	Schwellwert (in %) für freien Auslagerungsspeicher (swap), bei dessen Unterschreiten die Meldung „critical“ ausgegeben wird (zum Beispiel „40%“).
check_mailq	-w \$ARG1\$	Schwellwert für die Anzahl von E-Mails in der Warteschlange (queue), bei dessen Überschreiten die Meldung „warning“ ausgegeben wird (zum Beispiel „1000“).
	-c \$ARG2\$	Schwellwert für die Anzahl von E-Mails in der Warteschlange (queue), bei dessen Überschreiten die Meldung „critical“ ausgegeben wird (zum Beispiel „1500“).
check_load	-w \$ARG1\$	Schwellwerte für die Systemauslastung [avg1,avg5,avg15], bei dessen Überschreiten die Meldung „warning“ ausgegeben wird (zum Beispiel „15,20,20“).
	-c \$ARG2\$	Schwellwerte für die Systemauslastung [avg1,avg5,avg15], bei dessen Überschreiten die Meldung „critical“ ausgegeben wird (zum Beispiel „20,25,35“).
check_procs	-w \$ARG1\$	Schwellwert für die Anzahl von Prozessen, bei dessen Überschreiten die Meldung „warning“ ausgegeben wird (zum Beispiel „5“).
	-c \$ARG2\$	Schwellwert für die Anzahl von Prozessen, bei dessen Überschreiten die Meldung „critical“ ausgegeben wird (zum Beispiel „10“).
	-s \$ARG3\$	Angabe der Prozesse, welche überwacht werden sollen (zum Beispiel „Z“ für Zombie Prozesse).
check_tcp	-H \$ARG1\$	Angabe der IP-Adresse, zu welcher die TCP Verbindung geprüft werden soll (zum Beispiel „localhost“).
	-p \$ARG2\$	Angabe des Ports, welcher geprüft werden soll (zum Beispiel „25“).
check_telnet	-H \$ARG1\$	Angabe der IP-Adresse, zu welcher die Telnet Verbindung geprüft werden soll (zum Beispiel „localhost“).

Command	Parameter	Beschreibung
	-P \$ARG2\$	Angabe des Ports, welcher geprüft werden soll (zum Beispiel „25“).
	-M \$ARG3\$	Angabe des Banner Strings (siehe auch), welcher geprüft werden soll (zum Beispiel „ESMTP“).

Tabelle: PlugIns mit variablen Parametern

Die weiterhin integrierten PlugIns können auch bei deaktivierter Option **Allow remote command arguments** verwendet werden. Sie sind **ausschließlich ohne Angabe von Parametern** zu verwenden.

Command	Vorgabe Parameter	Beschreibung
check_disk_tmp_static	-w 10%	Vergleiche Tabelle PlugIns mit variablen Parametern Command check_disk
	-c 5%	
	-p /tmp	
check_disk_db_static	-w 25%	
	-c 10%	
	-p /var/ldap.ENCRYPTED	
check_disk_log_static	-w 25%	
	-c 10%	
	-p /var/log	
check_disk_mq_static	-w 40%	
	-c 10%	
	-p /var/mailqueue	
check_mailq_static	-w 100	Vergleiche Tabelle PlugIns mit variablen Parametern Command check_mailq
	-c 250	
	-M postfix	
check_telnet_static	-H localhost	Vergleiche Tabelle PlugIns mit variablen Parametern Command check_telnet
	-P 25	
	-M ESMTP	
check_zombie_procs_static	-w 5	Vergleiche Tabelle PlugIns mit variablen Parametern Command check_procs
	-c 10	
	-s Z	
check_load_static	-w 5,10,15	Vergleiche Tabelle PlugIns mit variablen Parametern Command check_load
	-c 20,25,30	

Tabelle: PlugIns mit statischen Parametern

Sektion **Virtualisation tools** (optional)

Diese Sektion ist nur auf virtuellen Appliances verfügbar.

Parameter	Beschreibung
 ☒ Enable VMware tools	Im Standard ist diese Option aktiv. Ein OS-Kernel mit integrierten VMware Tools wird verwendet. Diese Tools können in einigen wenigen Konstellationen unter ESX, sowie mit einigen Backup Tools, welche „quiescing“ verwenden, zu Problemen führen. Aus diesem Grund besteht die Möglichkeit, diese zu deaktivieren. Eine hier vorgenommene Änderung wird erst nach einem Neustart der SEPPmail Appliance aktiv.
 Microsoft Azure	
 ☐ Enable Microsoft Azure guest agent	Diese Option ist im Standard inaktiv. Aktiviert den Microsoft Azure Linux-Agent. Damit stehen die Überwachungsfunktionen des Azure Fabric Controller zur Verfügung. Das Setzen von Einstellungen über diesen Weg ist nicht möglich.
 ☐ Fetch network information for the first interface from DHCP on every startup	Diese Option ist im Standard inaktiv. Durch Aktivieren dieser Option besteht die Möglichkeit, bei jedem Neustart der Appliance dynamisch eine IP Adresse - ausschließlich (!) - auf Interface 1 (siehe IP Addresses ²²⁵) zu beziehen.  Hinweis: Wurden unter Name ²²⁸ noch keine Einträge für Hostname und Domain vorgenommen, so werden diese dynamisch per DHCP bezogen. Sind die Einträge vorhanden, so werden diese über den Agent an Microsoft Azure übergeben.



Hinweis:

Das Unterstützen von Xen und QEMU Tools ist per Standard gegeben.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

7.6 Mail System

Im Menüpunkt **Mail System**^[247] werden grundlegende Einstellungen des SEPPmail Appliance E-Mail Systems vorgenommen.

Die gegebenenfalls in der folgenden Sektion benötigten E-Mail-Disclaimer, beziehungsweise E-Mail-Vorlagen können jeweils über die Schaltflächen **Edit mail disclaimer...**^[261] (ist das **Central Disclaimer Management (CDM)**^[125] nicht lizenziert, so ist diese Schaltfläche ausgegraut), beziehungsweise **Edit mail templates...**^[264] vorab erzeugt oder bearbeitet werden.



Hinweis:

Sollen Fußnoten verwendet werden, so ist unbedingt darauf zu achten, dass diese noch auf dem Groupware System oder durch die SEPPmail Appliance gesetzt werden. Werden Fußnoten bei ausgehenden E-Mails durch ein nachgelagertes System angehängt, so würde eine eventuell bereits vorhandene E-Mail-Signatur zerstört.

Sektion **Managed domains**

Definiert die E-Mail Domänen welche verwaltet werden sollen.

Über den **Filter...** steht eine Suchfunktion innerhalb der Spalte **Domain Name** der folgenden Tabelle bereit. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Spalte	Beschreibung
 Domain name	Liste aller auf der SEPPmail Appliance angelegten E-Mail Domänen. Für diese Domänen werden E-Mails angenommen und entsprechend verarbeitet.
 Server IP address	Zeigt die IP-Adresse, den Hostnamen oder den MX-Eintrag des internen Groupware Systems sowie den Port an, an welches eingehende E-Mails für den jeweils oben genannten Domain name weitergeleitet werden.
 TLS level	Zeigt an, welche Art der TLS-Transportverschlüsselung zum Groupware-Server (Server IP address) verwendet wird.
 Smarthost	Zeigt den Smarthost an, an welchen E-Mails der jeweiligen Managed domain ^[247] in das Internet gesendet werden sollen (Sender Based Routing).
 GINA	Zeigt die GINA-Domain an, welche für die jeweilige E-Mail Domäne festgelegt wurde (siehe auch CHANGE GINA SETTINGS FOR ^[423]).
 Disclaimer	Zeigt an, welcher Disclaimer gegebenenfalls an ausgehende E-Mails der jeweiligen E-Mail Domäne angefügt werden soll (siehe auch Mail System ^[247] Edit mail disclaimer... ^[259] , beziehungsweise LIST DISCLAIMER ^[259]).
 Postmaster	Zeigt die für diese Domäne gültige Postmaster-Adresse an (siehe auch ADD/EDIT MANAGED DOMAIN ^[266] Settings ^[266] Postmaster address). Ist kein Eintrag vorhanden, wird der Standard-Eintrag aus SMTP settings ^[252] verwendet.
 SEPPmail Managed Domain Encryption	Zeigt an, ob die jeweilige Managed domain ^[247] am Managed Domain Service ^[31] teilnimmt (Status managed / unmanaged , siehe auch ADD/EDIT MANAGED DOMAIN ^[266] Settings ^[266] S/MIME Domain keys <i>Automatically create and publish S/MIME domain keys for this domain</i>) und ob der auf dem SEPPmail Lizenz-, beziehungsweise Key-Server freigeschaltete Schlüssel vom lokalen Schlüssel abweicht (Status mismatch , siehe auch ADD/EDIT MANAGED DOMAIN ^[266] S/MIME domain encryption ^[274]). Wurde das automatische Generieren und Übertragen von Domänenschlüsseln zur Teilnahme am Managed Domain Service ^[31] global in dieser Sektion über Create S/MIME domain keys for managed domain encryption and send public

Spalte	Beschreibung
	key to vendor pool: (siehe unten) abgeschaltet, so erscheint zusätzlich die Warnung Autopublish globally switched off.
 MPKI	Zeigt an, ob die jeweilige Managed domain [247] für den automatischen Bezug von User Zertifikaten via MPKI [339] eingerichtet ist (siehe auch Connectors [339] MPKI managed domains [340]). Mögliche Status: On Off <i>wird nur bei aktiver Multitenancy [221] License [220] angezeigt</i>
 Customer	Name des Mandanten, dem diese E-Mail Domäne zugeordnet wurde (siehe auch Customers [494]).

Über die Schaltfläche **Add managed domain...** werden weitere E-Mail Domänen hinzugefügt. Diese E-Mail Domänen müssen passend zu den E-Mail Adressen Ihres Unternehmens sein. Weitere Informationen für das Verwalten von E-Mail Domänen sind unter **ADD/EDIT MANAGED DOMAIN** [266] zu finden.

**Hinweis:**

Wird beim Anlegen einer Domäne dieser die **Server IP address (Forwarding server IP or MX name)** „DISCARD“ (ohne Anführungszeichen) eingetragen, so werden alle E-Mails welche an diese Domäne adressiert sind verworfen.
Somit kann zum Beispiel der Versand von Bounce-E-Mails von internen Systemen an unbekannte Adressen vermieden werden.

Parameter	Beschreibung
 Create S/MIME domain keys for managed domain encryption and send public key to vendor pool: ☐	Mit dieser Einstellung wird die Teilnahme am Managed Domain Service [31] global festgelegt.
 On for all domains	Standardeinstellung. Generell für alle Managed domains [247] aktiv. Die Hinweise aus S/MIME domain keys [267] in EDIT MANAGED DOMAIN [266] sind zu beachten!
 Off for all domains	Generell für alle Managed domains [247] abgeschaltet. Ist diese Einstellung gewählt, erscheint in der Spalte SEPPmail Managed Domain Encryption der oben genannten Tabelle zu jeder Managed domain [247] die Warnung Autopublish globally switched off.  Hinweis: Generell ist diese Einstellung nicht zu empfehlen, da der mit dem Erwerb der Basis-Lizenz [120] kostenfrei enthaltene Managed Domain Service [31] nicht genutzt wird. In Umgebungen, in welchen aus infrastrukturellen Gründen für keine der eingerichteten Managed domains [247] der gesamte E-Mail-Verkehr über die SEPPmail Appliance geleitet wird, kann diese Einstellung jedoch sinnvoll sein.

Parameter	Beschreibung
	 Hinweis: Soll grundsätzlich, also auch für den Versand, nicht am Managed Domain Service ^[31] teilgenommen werden, so ist zusätzlich zu dieser Auswahl unter Domain Certificates ^[489] Managed S/MIME domain certificates ^[489] die Option Auto-update S/MIME domain certificates ^[489] gleich nach der Installation zu deaktivieren.
 Use domain settings	Mit dieser Einstellung kann pro Managed domain ^[247] (siehe ADD/EDIT MANAGED DOMAIN ^[266] Settings ^[266] S/MIME domain keys) entschieden werden, ob teilgenommen werden soll oder nicht.  Hinweis: Diese Einstellung kann in MSP Umgebungen mit unterschiedlichen Kundenanforderungen bezüglich des Managed Domain Service ^[31] sinnvoll sein. Ein weiterer Anwendungsfall könnte das Aufschalten einzelner Test-User, zum Beispiel im Rahmen eines PoCs sein. Die Teilnahme kann dann zunächst unterbunden und bei Produktivschalten der gesamten Managed domain ^[247] im Nachgang aktiviert werden.
 ☐ Fetch e-mail from remote POP3 server. Interval in minutes	Diese Option ist im Standard inaktiv. E-Mails von Benutzern mit eingerichteten POP3 / IMAP Zugangsdaten (siehe Users ^[396] USER 'USER@DOMAIN.TLD' ^[396] Remote POP3 ^[402]) werden durch die SEPPmail Appliance jeweils im eingestellten Zeitintervall abgeholt. Die so abgeholten E-Mails werden im Anschluss durch die SEPPmail Appliance verarbeitet und an den entsprechenden Forwarding server (siehe Tabelle unter Mail System ^[247] Managed domains ^[247] Spalte Server IP address) weitergeleitet.  Hinweis: Beim Abholen von E-Mails werden nacheinander die Protokolle in der Priorität IMAPS, POP3S, IMAP und POP3 verwendet. Kommt ein SSL/TLS gesichertes Protokoll zum Einsatz, so werden die Zertifikate der Gegenstellen bezüglich deren Vertrauenswürdigkeit gemäß der Einträge unter X.509 Root Certificates ^[480] eingestuft.
 ☒ Verify recipient addresses using SMTP-lookups	Im Standard ist diese Option aktiv. E-Mails für eine Managed domain ^[247] werden nur dann angenommen, wenn die E-Mail Adresse - also auch der Namensteil - des Empfängers auch auf dem Forwarding server (siehe Tabelle unter Mail System ^[247] Managed domains ^[247] Spalte Server IP address) bekannt ist. Dies impliziert, dass der Forwarding server ebenfalls den Namensteil einer E-Mail und nicht nur den Domänenteil vor der Annahme prüft. (Mit der Schaltfläche Flush recipient cache now wird der Zwischenspeicher gelöscht, in welchem die bereits erfolgreich gefundenen Empfängeradressen vorgehalten werden.)  Hinweis: Damit diese Einstellung problemlos funktioniert, ist darauf zu achten, dass der Forwarding server keinen SPAM Schutz aktiviert hat. Unter Umständen ist mit Problemen zu rechnen, wenn der nachgelagerte (Forwarding-)Server nicht der E-Mail Server sondern ein weiteres, zwischengeschaltetes E-Mail Relay ist. Im Detail wird durch diesen Parameter im Postfix bei smtpd_recipient_restrictions die Option reject_unverified_recipient gesetzt. Das heißt, für das Prüfen wird versucht eine Nachricht zu senden und nicht etwa Befehle wie „SMTP VRFY“ verwendet. Bei vorgelagerten Schutzkomponenten sollten diese bereits ein entsprechendes Prüfen übernehmen. Die Option wäre in diesem Falle zu deaktivieren.

Sektion **Outgoing server**

Definiert die Art des Weiterleitens ausgehender E-Mails.



Hinweis:

Das hier eingestellte ausgehende Routing wird gegebenenfalls durch die TLS Einstellungen übersteuert (siehe nächste Sektion **TLS settings** ^[251]).

Parameter	Beschreibung						
 Use built-in mail transport agent	Standardeinstellung. Ausgehende E-Mails in Richtung Internet werden direkt durch die SEPPmail Appliance an den Ziel E-Mail Server des E-Mail Empfängers adressiert. Die Appliance muss für diese Einstellung direkt den Übergang zum Internet bilden. Hinweis: Bei Verwenden dieser Einstellung wird dringend empfohlen das optionale Protection Pack ^[105] (PP) zu lizenzieren und aktivieren, sofern für den eingehenden E-Mail Verkehr nicht etwa ein externer AntiSpam-Dienst vorgeschaltet ist. Andernfalls ist mit erheblichen Beeinträchtigungen, bis hin zum Erliegen des Mailflusses durch SPAM-Attacken zu rechnen.						
 Use the following SMTP server	Sollen ausgehende E-Mails in Richtung Internet nicht direkt zugestellt werden, empfiehlt sich das Verwenden eines E-Mail Relay-Servers (smart host). Alle ausgehenden E-Mails werden an diesen E-Mail Relay-Server übertragen, welcher dann die E-Mails in Richtung Empfänger weiterleitet. Der E-Mail Relay-Server kann ein Interner Server aber auch ein Server beim E-Mail Provider sein.						
 Server name	Als Eingabe wird folgendes akzeptiert: <table border="0"> <tr> <td>IP-Adresse</td><td>einzelne IP-Adresse (in eckige Klammern [] zu setzen).</td></tr> <tr> <td>Hostname</td><td>wird ein Hostname verwendet, so ist dieser in eckige Klammern [] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt!</td></tr> <tr> <td>MX-Name</td><td>MX-lookup wird ausgeführt (siehe gegebenenfalls auch System ^[224] DNS ^[225] add local zone)</td></tr> </table> Optional ist bei Angabe einer IP-Adresse, eines Host-Namens oder eines MX-Namens zusätzlich die Angabe eines individuellen Ports möglich. Dieser wird direkt im Anschluss mit einem Doppelpunkt „:“ getrennt angegeben, also „[IP-Adresse]:Port“, „[Hostname]:Port“ oder „MX-Name:Port“. Wird kein Port angegeben, so wird der Standard SMTP Port TCP25 verwendet.	IP-Adresse	einzelne IP-Adresse (in eckige Klammern [] zu setzen).	Hostname	wird ein Hostname verwendet, so ist dieser in eckige Klammern [] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt!	MX-Name	MX-lookup wird ausgeführt (siehe gegebenenfalls auch System ^[224] DNS ^[225] add local zone)
IP-Adresse	einzelne IP-Adresse (in eckige Klammern [] zu setzen).						
Hostname	wird ein Hostname verwendet, so ist dieser in eckige Klammern [] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt!						
MX-Name	MX-lookup wird ausgeführt (siehe gegebenenfalls auch System ^[224] DNS ^[225] add local zone)						
 Server requires authentication	Diese Option ist im Standard inaktiv. E-Mail Relay-Server bei einem Provider benötigen vor dem Übertragen von E-Mails meist eine Anmeldung. Verwenden Sie hierzu die entsprechenden Anmeldedaten.						
 User ID	Benutzername für das Anmelden am unter Server name angegebenen SMTP server.						
 Password	Zur User ID gehöriges Kennwort.						

Parameter	Beschreibung
 Additional credentials for managed domains:	Werden für einzelne Managed domains ^[266] dedizierte Smarthost ^[247] s benötigt, welche eine Anmeldung erfordern, so können die benötigten Zugangsdaten hier entsprechend konfiguriert werden.
 Add smarthost	Über Add smarthost werden die benötigten Zugangsdaten eingegeben. Nach dem Speichern eines Eintrags, erscheint dieser jeweils in einer in einer neuen Zeile als Smarthost .
 Smarthost	Bereits eingetragene Smarthost Zugangsdaten.
 hostname:	Angabe des Smarthost (vergleiche Server name des Abschnitts Use the following SMTP server ^[250])
 username:	Benutzername für das Anmelden am unter hostname: angegebenen Smarthost .
 password:	Zum username gehöriges Kennwort.
 Domain:	Im Auswahlfeld sind alle Managed domains ^[247] aufgelistet. Durch Auswählen der Managed domains ^[266] (Mehrfachauswahl ist durch Klicken mit gedrückter „Strg“ Taste möglich) werden die Zugangsdaten auf diese beschränkt. In der Regel ist das dann notwendig, wenn in einem Managed Service Provider (MSP) Umfeld mehrere Mandanten denselben Smarthost mit unterschiedlichen Credentials ansprechen sollen.

Sektion TLS settings (optional)

An dieser Stelle werden TLS-Verbindungen nach außen - also in Richtung Internet - aufgelistet beziehungsweise eingerichtet.

Wurde in der **Sektion Outgoing server** ^[250] die Option **Use the following SMTP server** gewählt, so kann hier zu dem unter **Server name** eingetragenen Server die TLS-Verschlüsselung fest definiert werden.

Wurde die Option **Use built-in e-mail transport agent** gewählt, so kann hier bei Bedarf zu bestimmten E-Mail Servern im Internet die Route und die Art der TLS Verschlüsselung fest definiert werden.



Hinweis:

Wird hier keine Konfiguration vorgenommen, so gilt die Einstellung „may“, das heißt die SEPPmail Appliance wird zu allen Kommunikationspartnern eine TLS-verschlüsselte Verbindung aufbauen, sofern die Gegenstelle dies unterstützt (opportunistisch).

Für die TLS Verschlüsselung wird das unter **SSL** ^[319] eingebundene Zertifikat verwendet.

Über den **Filter...** steht eine Suchfunktion innerhalb der Spalte **Domain Name** der folgenden Tabelle bereit. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Neue TLS-Verbindungen werden über die Schaltfläche **Add TLS domain...** eingerichtet.

Parameter	Beschreibung
 Domain name	Liste aller auf der SEPPmail Appliance angelegten E-Mail Domänen, für welche eine TLS-Verbindung konfiguriert wurde auf.

Parameter	Beschreibung
	 Hinweis: Ist hier ein Punkt „.“ eingetragen und - dann zwingend - eine Server IP address, so werden alle über das „Sender Based Routing“ (siehe ADD/EDIT MANAGED DOMAIN ²⁶⁶) Settings ²⁶⁶ Send ALL outgoing mails from this domain to the following SMTP server (optional)) an diese IP Adresse gerouteten E-Mails mit dem eingestellten TLS level dorthin verschlüsselt.
 Server IP address	Zeigt die IP-Adresse, den Hostnamen oder den MX-Eintrag für den jeweils oben genannten Domain name an.  Hinweis: Das heißt alle E-Mails an die unter Domain name genannte E-Mail Domäne werden direkt an diese Adresse geroutet! Ausnahme bildet der Punkt „.“ unter Domain name, durch welchen das Routing an dieser Stelle nicht beeinflusst wird.
 Server port	Zeigt den Port an, welcher für die TLS-verschlüsselte Verbindung zur oben genannten Server IP address verwendet wird. Im Standard ist das 25.
 TLS level	Zeigt an, welche Art der TLS-Transportverschlüsselung von der SEPPmail Appliance zum angegebenen E-Mail Server für die jeweilige E-Mail Domäne verwendet wird.
 Fingerprint	Wurde als TLS level Fingerprint gewählt, so werden hier die eingetragenen Fingerprints der Zertifikate angezeigt..

Um bestehende TLS-Verbindungen zu verwalten ist auf den jeweiligen „Domain Name“ zu klicken.

Weitere Informationen für das Verwalten von TLS E-Mail Domänen stehen im Kapitel zum Untermenü [ADD TLS DOMAIN](#) ²⁸² zur Verfügung.

Sektion SMTP settings

Definiert spezifische Einstellungen für das SMTP-Protokoll.



Hinweis:

Alle in dieser Sektion vorhandenen Einstellungen, mit Ausnahme der **Postmaster address** ²⁵³ sind maschinenbezogen und werden somit in einem **Cluster** ³⁸³ **nicht** synchronisiert. Im Bedarfsfall müssen diese Einstellungen somit auf jedem **Cluster** ³⁸³ Partner einzeln vorgenommen werden.

Parameter	Beschreibung
 max. message size (KiB) (optional)	In diesem Feld wird die maximale Größe einer E-Mail in Kibibyte definiert, die durch die SEPPmail Appliance per SMTP übertragen werden darf. E-Mails, welche diese Größe überschreiten werden abgelehnt. Wird hier eine Beschränkung festgelegt, so ist darauf zu achten, wie diese gegebenenfalls mit dem Groupware-Server beziehungsweise des optional zum Internet hin vorgeschalteten Systems zusammenpasst. Sollte die SEPPmail Appliance über den MX-Record im Internet direkt angesprochen werden ist der Eintrag eines Limits zwingend. Dieses darf die angezeigte Größe (siehe Note: cannot exceed xxxxx KiB) nicht überschreiten. Der eingegebene Wert kommt auch bei der Anzeige der Maximalgröße von Anhängen bei GINA- (nicht LFT !!!) Antworten beziehungsweise Initial-E-Mails zum Tragen. Folglich wird dort nichts angezeigt, wenn dieser Wert nicht definiert wurde. LFT-E-Mails welche über das GINA-Portal eingeliefert werden sind von dieser Einschränkung nicht betroffen.

Parameter	Beschreibung
	 Achtung: Wird ein Anhang via SMTP versendet, so kann dieser bei base64 Kodierung auf 4/-3 seiner ursprünglichen Größe anwachsen! Weiterhin erfolgt die Angabe in Kibibyte (siehe auch http://de.wikipedia.org/wiki/Byte)!
 Postmaster address	Eingabe der E-Mail Adresse des lokalen Administrators der SEPPmail Appliance. Alle von der SEPPmail Appliance erzeugten Statusmeldungen wie zum Beispiel Watchdog Meldungen, aber auch die Daily Report [96]s (siehe auch Groups [413] admin [413] und statisticsadmin [415]) werden an diese E-Mail Adresse gesendet, sofern diese den Status "IMPORTANT" haben, was bedeutet, dass eine administrative Aktion auf der Appliance vonnöten ist.  Hinweis: Die Postmaster address muss gesetzt werden um Systembenachrichtigungen empfangen zu können. Weiterhin wird diese Adresse als Absender für den Versand von Backups und Systemmeldungen verwendet. Dies ist der einzige Eintrag dieser Sektion, welcher in einem Cluster [383] synchronisiert wird.
 SMTP server banner string (optional)	Festlegen des Namens, mit welchem sich die SEPPmail Appliance beim Aufbau einer SMTP-Verbindung von außen meldet. Bleibt der Eintrag leer, so wird der unter System [224] Name [228] eingetragene Name verwendet.
 SMTP server HELO string (optional)	Festlegen, mit welchen Namen sich die SEPPmail Appliance, beim Versand von E-Mails beim gegenüberliegenden SMTP-Server melden soll (HELO/EHLO-Befehl). Die Appliance wird sich im Normalfall mit dem unter System [224] Name [228] eingegebenen Namen melden. Handelt es sich hierbei zum Beispiel um einen aus dem Internet nicht erreichbaren Namen (zum Beispiel Domäne „local“) so kann es erforderlich sein, hier den aus dem Internet erreichbaren Namen (FQDN) einzutragen. Somit wird gewährleistet, dass E-Mail Server welche mit der Einstellung „Require fully qualified domain name in HELO command“ [257] arbeiten E-Mails von der SEPPmail Appliance auch annehmen. Das heißt die Einstellung ist meist nur dann relevant, wenn in der Sektion Outgoing server [250] dieses Menüs die Einstellung Use built-in e-mail transport agent aktiv ist.
 SMTP bind address (use with care!) (optional)	Festlegen der IP-Adresse einer Netzwerk-Schnittstelle, über die alle E-Mails empfangen werden (normalerweise nicht notwendig). Die SEPPmail Appliance bindet im Normalfall alle vorhandenen Netzwerk Interfaces. Sind mehrere Interfaces aktiv, jedoch nur eines davon soll für SMTP Verbindungen zur Verfügung stehen, so kann dessen IP-Adresse hier eingetragen werden.  Hinweis: Fällt das Interface der hier eingetragenen IP-Adresse aus, so ist die Appliance per SMTP nicht mehr erreichbar. Somit würde auch der E-Mail Verkehr unterbrochen.
 TLS encryption	
 ☐ Require TLS	Diese Option ist im Standard inaktiv. Durch Aktivieren dieser Option werden eingehend ausschließlich TLS-gesicherte Verbindungen angenommen.

Parameter	Beschreibung
encryption 	Hinweis: Insbesondere bei Verwenden von SMTP-Auth für das Einliefern von E-Mails des Groupware-Servers auf der SEPPmail Appliance (siehe auch Mehrere SMTP-Authentifizierungen verwalten [657]) wird das Aktivieren dieser Option empfohlen.
 Server name indication	
 ☐ Send SNI with SMTP request <i>(neu in 12.1)</i>	Diese Option ist im Standard inaktiv. Durch Aktivieren dieser Option wird bei jeder TLS verschlüsselten, ausgehenden SMTP-Verbindung im Client-Hello Paket der Name des Ziel-Servers mitgesendet. So kann der annehmende Zielservers das entsprechende Zertifikat auswählen, sofern dieser mehrere Domänen verwaltet und verschiedene Zertifikate nutzt.
 Extended settings (use with care)	Extended postfix MTA settings... öffnet das Folgemenü EXTENDED POSTFIX MTA SETTINGS [281], über welches bei Bedarf die Postfix Parameter und somit der SMTP Mailfluss beeinflusst werden können. Änderungen in EXTENDED POSTFIX MTA SETTINGS [281], werden erst nach zusätzlichem Speichern mittels Save in Mail System [247] aktiv.  Achtung: In der Regel sind Änderungen an den EXTENDED POSTFIX MTA SETTINGS [281] nicht notwendig. Bei unsachgemäßem Verwenden kann der E-Mail Fluss zum Erliegen kommen!

Sektion Relaying

Definition der für den Versand von E-Mails in das Internet berechtigten Systeme.

Parameter	Beschreibung
 Relaying allowed:	An dieser Stelle können die IP-Adresse(n) oder Subnetz(e) eingetragen werden, von welcher/m die SEPPmail Appliance E-Mails an externe Empfänger annehmen soll. Optional kann im Feld Comment: ein benutzerdefinierter Kommentar für jeden Eintrag hinzugefügt werden. Nach dem Speichern wird jeweils ein weiteres Eingabefeld eingeblendet.  Hinweis: In der Regel sind hier die IP-Adressen der eingetragenen Forwarding server (siehe Tabelle unter Mail System [247] Managed domains [247] Spalte Server IP address) zu berechnen. Um ein sogenanntes „open relay“ zu verhindern, sollte hier im Normalfall keinesfalls der Outgoing server [250] mit aufgelistet sein.
 Add relaying for	Dieses Feld dient der Eingabe weiterer Relay Adressen beziehungsweise Subnetzen. Nach dem Speichern werden jeweils weitere Eingabefelder eingeblendet.

Sektion Exchange Online Relaying

Parameter	Beschreibung
 ☐ Allow relaying for Exchange Online servers (remember to set correct tenant Ids for managed domains)	Diese Option ist im Standard inaktiv. Durch Aktivieren dieser Option wird allen Microsoft Office Outlook 365 Server erlaubt, über die SEPPmail Appliance zu relayen. Die jeweils aktuellen IPv4, beziehungsweise IPv6 Netze werden dabei nachfolgend aufgelistet (siehe auch https://endpoints.office.com/endpoints/Worldwide?ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7 und https://docs.microsoft.com/de-de/office365/enterprise/office-365-germany-endpoints#exchange-online für die IPs der deutschen Cloud).  Hinweis: Wird eine E-Mail von einem der hier aufgeführten Netze an eine nicht-Managed domain^[247] adressiert, so wird automatisch geprüft, ob - der Domänenteil der Absender-E-Mail-Adresse als Managed domain^[247] hinterlegt ist (andernfalls würde die E-Mail mit einem SMTP-Code 4xx abgelehnt, um ein Debugging zu ermöglichen). - in dieser Managed domain^[247] die korrekte Tenant-ID (siehe EDIT MANAGED DOMAIN^[266] Settings^[266] Exchange Online Integration) hinterlegt ist.

Sektion AntiSpam



Hinweis:

Die AntiSpam Optionen sind erst nach Erwerb des optionalen **Protection Packs**^[126] verfügbar. Ist der SEPPmail Appliance ein weiteres Relay - zum Beispiel Spamfilter - vorgeschaltet, so sollte vom Aktivieren von AntiSpam Funktionen abgesehen werden. Die AntiVirus Funktionen sollten in jedem Fall genutzt werden.

Parameter	Beschreibung
 Recommended settings	
 ☐ Use greylisting	Diese Option ist im Standard inaktiv. Durch diese Funktion werden eingehende externe E-Mails - d.h. E-Mails welche von keiner unter Relaying^[254] eingetragener IP oder Subnetz kommen - nicht mehr unmittelbar, sondern erst beim zweiten Zustellversuch angenommen. Dies soll bewirken, dass von SPAM-Versendern verwendete Methoden zum direkten Übertragen von E-Mails erfolglos bleiben. Der Empfang von gewünschten E-Mails wird durch diese Funktion nicht verhindert, sondern - bei unbekannten Absendern - lediglich zeitlich verzögert. Der E-Mail Server des Absenders wird nach einer kurzen Zeit einen erneuten Zustellversuch unternehmen. Die E-Mail wird dann angenommen.

Parameter	Beschreibung
	 Hinweis: Diese Funktion ist nur wirksam, wenn die SEPPmail Appliance eingehende E-Mails aus dem Internet direkt empfängt (in der Regel bei Verwenden der Einstellung Outgoing server^[250] Use built-in e-mail transport agent). Bereits von einem anderen E-Mail Server empfangene und weitergeleitete SPAM E-Mails können durch diese Funktion nicht vermieden werden Erklärung zum greylisting Greylisting ist eine Methode für das Bekämpfen von SPAM E-Mails. Bei dieser Funktion wird davon ausgegangen, dass E-Mail Server und E-Mail Clients sich an den RFC-Standard für SMTP halten. SPAM-Versender halten sich oft nicht an den RFC-Standard. So werben sie das temporäre Abweisen nicht immer aus, wodurch ein weiterer Zustellversuch unterbleibt. Um eventuelle Einschränkungen durch übermäßiges, einmaliges Abweisen gewünschter E-Mails zu vermeiden, wird empfohlen die Option Greylist learning only (no e-mail rejection) aus den optional settings für zwei bis vier Wochen ab Inbetriebnahme zu aktivieren. Hierdurch wird die SEPPmail Appliance bezüglich des Greylistings in einem Lernmodus versetzt und weist keine E-Mails temporär zurück.  Hinweis: Nachdem inzwischen die meisten SPAM-Versender ebenfalls eine E-Mail mehrfach versenden, bietet greylisting heute kaum noch Schutz. Aus diesem Grund sollte abgewägt werden, ob die Nachteile (verzögerte Zustellung) nicht höher als der Nutzen sind.  Hinweis: Da für das greylisting eine Kombination aus Sender Domäne und Hostname verwendet wird, kann dies bei Cloud-Diensten, wie zum Beispiel Microsoft Office365 zu enormen Verzögerungen führen. Aus diesem Grund wurden die wichtigsten Cloud-Sender (Office365, gmail, alibaba und so weiter) bereits in die default whitelist des greylisting-daemons aufgenommen.
 ☐ Use AntiSpam Engine (Note: remember to activate in ruleset)	Diese Option ist im Standard inaktiv. Aktiviert den SPAM-Filter auf der SEPPmail Appliance. Die Konfiguration des SPAM-Filters wird im Abschnitt Protection Pack^[303] der Sektion Ruleset generator^[287] des Menüs Mail Processing^[286] durchgeführt.  Achtung: Wird diese Option deaktiviert, obwohl im Menü Mail Processing^[286] die Spam-Prüfung aktiv geschaltet ist, so würde keine Spam-Erkennung stattfinden.
 ☐ Use ClamAV antivirus Engine (Note: remember to activate in ruleset)	Diese Option ist im Standard inaktiv. Aktiviert den Virens Scanner auf der SEPPmail Appliance. Die Konfiguration des Virens Scanners wird im Abschnitt Protection Pack^[303] der Sektion Ruleset generator^[287] des Menüs Mail Processing^[286] durchgeführt.

Parameter	Beschreibung
	 Achtung: Wird diese Option deaktiviert, obwohl im Menü Mail Processing ^[286] der Virenskan aktiv geschaltet ist, so würden E-Mails generell als „Virus-frei“ weitergeleitet.
 Enable unofficial signatures for ClamAV	Im Standard ist diese Option aktiv. Aktiviert zu den Standard AntiVirus Signaturen des ClamAV weitere Drittanbieter Signaturen geladen.  Hinweis: Folgende Ziele werden bei Aktivieren der Option angesprochen: Sanesecurity: rsync://rsync.sanesecurity.net www.sanesecurity.net Linux Malware Detect: http://cdn.rfxn.com Yara-Rule Project: https://raw.githubusercontent.com Die Auflösung von rsync.sanesecurity.net erfolgt zu einem beliebigen Mirror und ist mit einer OpenPGP Signatur gesichert. Die Quelle ist in folgendem Link einzusehen: https://github.com/extremeshok/clamav-unofficial-signs/blob/master/config/master.conf#L533-L534
 Require HELO command	Diese Option ist im Standard inaktiv. Aktiviert das Prüfen eines, vom absendenden E-Mail Server gesendeten, HELO Kommandos. Wird das Kommando nicht gesendet, so wird die Entgegennahme der E-Mails verweigert (bounced).
 PTR check (reverse DNS lookup)	Diese Option ist im Standard inaktiv. E-Mails von Servern, zu deren IP-Adresse keinen gültiger DNS-Eintrag vorhanden ist, werden abgewiesen. SPAM-Versender benutzen häufig E-Mail Server ohne gültigen DNS-Eintrag.
 Check if sender domain is valid	Diese Option ist im Standard inaktiv. Überprüfen die Auflösbarkeit des Domänenteil einer E-Mail Adresse via DNS. Schlägt das Auflösen fehl, so wird die E-Mail abgewiesen (bounced).  Hinweis: Diese Einstellung bleibt von einem eventuellen whitelisting (siehe Sektion Manual blacklisting / whitelisting ^[258]) unberührt!
 Require valid hostname in HELO command	Diese Option ist im Standard inaktiv. E-Mails werden ausschließlich von Servern angenommen, welche sich im HELO Kommando mit einem gültigen - das heißt im DNS auflösbaren - Hostnamen melden. Dies könnte auch ein NetBIOS Name sein.
 Require fully qualified hostname in HELO command	Diese Option ist im Standard inaktiv. E-Mails werden ausschließlich von Servern angenommen, welche sich im HELO Kommando mit ihrem vollständigen, im DNS auflösbaren FQDN (fully qualified domain name) identifizieren. Der FQDN erfordert mindestens eine Punkt„.“, also zum Beispiel „SEPPmail.tld“.
 Limit incoming connections for SMTP per IP	Diese Option ist im Standard inaktiv. Limitiert die Anzahl der parallelen Verbindungen auf zehn pro IP-Adresse. Hierdurch kann das Überlasten der SEPPmail Appliance durch einzelne Server vermieden werden.

Parameter	Beschreibung
 ☐ Enable SPF checks	Diese Option ist im Standard inaktiv. Aktiviert die Sender Policy Framework Funktion. Dabei wird der optional im DNS eingetragene SPF-Record geprüft. Ist der sendende Server für die entsprechende E-Mail Domäne dort nicht hinterlegt, so wird die E-Mail abgewiesen (bounced).
 optional settings	
 ☐ Greylist learning only (no e-mail rejection)	Diese Option ist im Standard inaktiv. Greylisting-Lernmodus. Dabei wird die Datenbank mit den für den Greylisting-Betrieb benötigten Informationen aufgebaut. Bei Neuinstallationen wird empfohlen diese Option zwei bis vier Wochen zu verwenden, um in der Startphase keine Engpässe durch das Greylisting zu verursachen.
 ☐ Strict PTR check (reverse DNS lookup)	Diese Option ist im Standard inaktiv. Aktiviert eine doppelte DNS Prüfung. Zunächst wird geprüft, ob zur IP-Adresse ein gültiger DNS Eintrag vorhanden ist um im Anschluss zu prüfen, ob die DNS-Abfrage die ursprüngliche IP ausgibt.

Sektion **Blacklists**

Parameter	Beschreibung
 Add Blacklist (RBL)	E-Mail Server werden aufgrund von SPAM-Aktivitäten in sogenannte Blacklists aufgenommen. Diese Listen werden durch verschiedene Anbieter im Internet gepflegt. Um E-Mails von Servern welche in diesen Listen aufgeführt sind abzuweisen, müssen die URLs der gewünschten Realtime Blackhole Lists (RBL) eingetragen werden. Nach dem Speichern wird jeweils ein weiteres Eingabefeld eingeblendet.

Sektion **Manual blacklisting / whitelisting**

In diesem Menüpunkt kann der Empfang von externen E-Mails von bestimmten IP-Adressen beziehungsweise -Netzwerken blockiert (blacklisted) oder explizit zugelassen (whitelisted) werden. Whitelist Einträge werden auch von der Spam-Prüfung ausgenommen.

Parameter	Beschreibung			
 add access entry	Für das Blockieren oder Zulassen wird das IP-Netzwerk, die Aktion und einen Kommentar in die entsprechenden Eingabefelder eingetragen.			
	network:	action:		comment:
	IP-Adresse mit CIDR Suffix	accept	akzeptiert die Annahme (whitelist)	Aussagekräftiger Kommentar, weshalb die Regel eingetragen wurde und wen diese betrifft.
		reject	verweigert die Annahme (blacklist)	
	Beispiel:			

Parameter	Beschreibung		
	network:	action	comment:
	186.56.148.224/28	reject	weist alle E-Mails ab, welche aus dem IP-Adressbereich 186.56.148.224/24 - also 186.56.148.224 bis 186.56.148.239 - kommen.
	fe80::220/124	accept	akzeptiert alle E-Mails, welche aus dem IP-Adressbereich fe80::220/124 - also fe80::220 bis fe80::22f - kommen.
 Hinweis: E-Mails von whitelisted IP-Adressen beziehungsweise IP-Adressbereichen werden selbst dann entgegengenommen, wenn vom sendenden E-Mail Server kein gültiges HELO Kommando übergeben wird.			

**Hinweis:**

Externe Adressen, an welche E-Mails von intern versendet wird (mit Ausnahme sogenannter Non-Delivery-Reports (NDR)), werden automatisch für sechs Monate ab dem letzten Versand whitelisted, und somit als reale Kommunikationspartner gekennzeichnet.

**Achtung:**

Bei E-Mails von whitelisted IP-Adressen werden jegliche AntiSpam Funktionen (siehe **Antispam** ^[255], sowie **Mail Processing** ^[266], **Ruleset generator** ^[267], **Protection Pack** ^[303]) unterbunden.
Der Virensan bleibt davon unberührt.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

7.6.1 List Disclaimer

Dieses Sub-Menü wird aus **Mail System** ^[247] über **Edit mail disclaimer...** aufgerufen.

An dieser Stelle können individuelle Fußnoten erstellt (**Add** ^[261]), beziehungsweise vorhandene Fußnoten bearbeitet , kopiert  oder gelöscht  werden.

Die bereits vorhandene Standardvorlage [default] sollte im Normalfall nicht angepasst werden. Sie dient vielmehr als Vorlage für weitere Fußnoten und kann bei Bedarf kopiert und angepasst werden.

Die gelisteten Fußnoten werden in der Regel der entsprechenden **Managed domain** ^[247], in deren Detailmenü **ADD/EDIT MANAGED DOMAIN** ^[266] unter **Settings** ^[266] **Disclaimer** zugeordnet.

**Hinweis:**

Das Positionieren eines Disclaimers kann alternativ auch manuell in einer E-Mail selbst erfolgen. Hierzu ist einer E-Mail an der Stelle, an welcher der Disclaimer positioniert werden soll, eine Zeile mit dem Text

##MAILDISCLAIMER##

hinzuzufügen.

(erweitert in 12.0)

Durch Angabe von

##MAILDISCLAIMER_<disclaimer>##

(wobei <disclaimer> dem gewünschten Disclaimer aus **LIST DISCLAIMER**^[259] entspricht), kann nicht nur die Position, sondern auch explizit der zu verwendende Disclaimer ausgewählt werden.

Fußnoten stehen immer sowohl im Text- als auch im HTML-Format zur Verfügung. Beim E-Mail Versand wird das passende Format anhand des E-Mail Formats automatisch ausgewählt.

Soll eine Fußnote über die Schaltfläche  gelöscht werden, so ist vorher unbedingt zu überprüfen, dass diese keiner **Managed domain**^[247] (siehe **Mail System**^[247]) zugeordnet ist oder eventuell in **Custom commands**^[308] der **Sektion Ruleset generator**^[287] des Menüs **Mail Processing**^[286] verwendet wird.



Hinweis:

Durch Verwenden von LDAP Abfragen, zum Beispiel des zur sendenden E-Mail Adresse gehörenden Benutzerobjektes in einem Microsoft Active Directory (AD), kann nicht nur eine allgemein, unternehmensweit gültige, sondern eine für jeden einzelnen Absender individuelle Fußnote erstellt werden.

Ebenso ist das granularere Verwenden von Disclaimern anhand von Merkmalen des Absenders im LDAP - wie zum Beispiel einer AD-Gruppenzugehörigkeit - möglich. So können beispielsweise eigene Disclaimer pro Abteilung zum Einsatz kommen.

7.6.1.1 Edit Disclaimer

Dieses Sub-Menü wird aus **LIST DISCLAIMER** über **Add**, beziehungsweise  aufgerufen.



Hinweis:

Durch Auslesen von Informationen aus LDAP-Verzeichnissen, wie zum Beispiel dem Microsoft Active Directory (AD) mittels `ldap_read()`, und anschließendem Verwenden der damit erzeugten Variablen im Disclaimer Text (siehe **Disclaimer as HTML** beziehungsweise **Disclaimer as Text**), ist nicht nur ein allgemeingültiger (Firmen-)Disclaimer möglich, sondern selbst eine auf den jeweiligen Absender personalisierte Fußnote (Footer).

Dies ist insbesondere möglich, da ein durch die SEPPmail Appliance hinzugefügter Disclaimer auch bei Antworten korrekt positioniert wird, also unterhalb der Antwort und nicht am Ende der E-Mail.



Sektion Disclaimer settings

Parameter	Beschreibung
 Name	Gibt den Namen des Disclaimers an. Dieser muss eindeutig sein.
 Advanced	Gibt an in welchen Formaten ein Disclaimer verfügbar sein soll.
 ☒ Add HTML part	Im Standard ist diese Option aktiv. Aktiviert den HTML Disclaimer aus Disclaimer as HTML im HTML-Part einer E-Mail.
 ☒ Add text part	Im Standard ist diese Option aktiv. Aktiviert den HTML Disclaimer aus Disclaimer as Text im Text-Part einer E-Mail.
 ☐ Force parts	Diese Option ist im Standard inaktiv. Ist in der Original-E-Mail kein Text oder HTML Part vorhanden, an welchen der Disclaimer angehängt werden könnte, so wird durch Aktivieren dieser Option ein entsprechend leerer Part erzeugt. Im Regelfall ist diese Option nur bei maschinell generierten E-Mails in speziellen Fällen von Bedeutung.
 ☐ Force UTF-8	Diese Option ist im Standard inaktiv. Erzwingt das UTF-8 Format um eventuelle Kodierungsprobleme zu vermeiden.  Hinweis: Outlook verwendet in der Regel das minimal notwendige Charset. Sind zum Beispiel keine Umlaute (oder sonstige Sonderzeichen) in der E-Mail, so würde das Charset us-ascii genutzt. Da SEPPmail Appliance eine E-Mail so wenig wie möglich manipuliert, würden bei Verwenden der Disclaimer-Funktion eventuell im Disclaimer enthaltene Umlaute oder Sonderzeichen in das bereits vorhandene Charset überführt. Dies würde ohne die Einstellung Force UTF-8 zwangsläufig zur fehlerhaften Darstellung dieser Sonderzeichen führen.



Sektion Disclaimer as HTML preview

Zeigt eine Vorschau des unter **Disclaimer as HTML** eingegebenen HTML Codes an.



Sektion Disclaimer as HTML

Bei neu erstellten Disclaimers ist im Eingabefeld bereits ein Standard Code enthalten, welcher einen deutschen und englischen Standarttext beinhaltet. **Dieser kann den individuellen Bedürfnissen angepasst oder vollständig ersetzt werden.**

Ebenso können dem HTML-Disclaimer Dateien als Inlines im Code hinzugefügt werden, welche über die Content-ID (siehe Tabelle unten) zu erreichen sind.

Inlines

Dateien, welche im HTML-Code des Eingabefeldes verwendet werden sollen. Diese können ausgewählt und über **Add** hochgeladen werden. Im Anschluss erscheinen die hochgeladenen Dateien in der Tabelle.

Name	Content-Type	Content-ID
Name der hochgeladenen Datei.	Datei- / Mime- Typ der Datei. Beispielsweise <i>image/x-png</i> für eine Bilddatei im PNG-Format	ID (cid) unter welcher die Datei im HTML Code abgerufen werden kann. Wird beispielsweise einer hochgeladenen Bilddatei die ID <i>picture1</i> vergeben, so ist diese im HTML Code über <code></code> zu erreichen. Im Standard ist nach dem Hochladen die Content-ID identisch mit dem Dateinamen, kann aber durch Klicken auf den „Name“n angepasst werden.  Hinweis: Werden Inlines unter Disclaimer as HTML nicht referenziert, so erscheint die Meldung cid is not referenced in HTML and will not be added to the Disclaimer

Sektion Disclaimer as text

Bei neu erstellten Disclaimers ist im Eingabefeld **bereits ein Standardtext in deutsch und englisch vorhanden. Dieser kann den individuellen Bedürfnissen angepasst oder vollständig ersetzt werden.**

Sektion Attachments

Optional können Dateien, welche jeder E-Mail angehängt werden sollen, ausgewählt und über **Add** hochgeladen werden. Im Anschluss erscheinen die hochgeladenen Dateien in der Tabelle.

Name	Content-Type	Content-ID
Name der hochgeladenen Datei.	Datei- / Mime- Typ der Datei. Beispielsweise <i>image/x-png</i> für eine Bilddatei im PNG-Format	ID (cid) unter welcher die Datei im HTML Code abgerufen werden kann. Wird beispielsweise einer hochgeladenen Bilddatei die ID <i>picture1</i> vergeben, so ist diese im HTML Code über <code></code> zu erreichen. Im Standard ist nach dem Hochladen die Content-ID identisch mit dem Dateinamen, kann aber durch Klicken auf den „Name“n angepasst werden.

Sektion Info

Zeigt die unter **Disclaimer as HTML** und **Disclaimer as Text** verfügbaren **Variablen** an. Verfügbar sind die internen **Variablen** sowie solche, welche mit `ldap_read()` geschrieben werden.

7.6.2 List Template

Dieses Sub-Menü wird aus **Mail System** [247] über **Edit mail template...** aufgerufen.

E-Mail Vorlagen sind vordefinierte Nachrichten, welche in definierten Fällen automatisiert versendet werden. Absender solcher Nachrichten ist immer die unter **Mail System** [247] **SMTP settings** [252] beziehungsweise **Managed domains** [247] **ADD/EDIT MANAGED DOMAIN** [266] **Settings** [266] eingegebene **Postmaster address**. Generell finden diese Vorlagen Verwendung in Bounce-Mails, wie sie in **Managed domains** [247] **ADD/EDIT MANAGED DOMAIN** [266] **Bounce templates** [270] dann auch auszuwählen sind. Weiterhin können hier erzeugte Vorlagen auch innerhalb von **Custom commands** [308] der **Sektion Ruleset generator** [287] des Menüs **Mail Processing** [286] abgerufen werden.

Im Standard stehen die Basisvorlagen bounce_noauth, bounce_noenc und bounce_noseckey zur Verfügung.

Diese Basisvorlagen können, sollten aber im Normalfall nicht angepasst werden. Sie dienen vielmehr als Basis für weitere Vorlagen - zum Beispiel individuell angepasst an Mandanten - und können entsprechend kopiert werden.

Neu Vorlagen können über **Add** [264] erzeugt, vorhandene über  bearbeitet,  kopiert oder  gelöscht werden.

Soll eine E-Mail Vorlage über die Schaltfläche  gelöscht werden, so ist vorher unbedingt zu überprüfen, dass diese keiner **Managed domain** [247] (siehe **Mail System** [247]) zugeordnet ist oder eventuell in **Custom commands** [308] der **Sektion Ruleset generator** [287] des Menüs **Mail Processing** [286] verwendet wird.



Hinweis:

Bei der Anlage neuer Vorlagen kann über den Namen gesteuert werden, ob die Original-E-Mail als Anhang angefügt wird oder nicht.

Wird im Namen der Vorlage „attachmail“ gefunden, so wird die ursprüngliche E-Mail beim Versand mit angefügt.

Bei Bounce-E-Mails sollte aus Sicherheitsgründen niemals die gesamte, ursprüngliche E-Mail mit angehängen werden.

7.6.2.1 Edit Template

Dieses Sub-Menü wird aus **LIST TEMPLATE** [263] mittels **Add** [264], beziehungsweise  aufgerufen.

Sektion **Template settings**

Parameter	Beschreibung
 Name	Gibt den Namen der Vorlage an. Dieser muss eindeutig sein.  Hinweis: Enthält der Name der Vorlage „attachmail“, so wird die ursprüngliche E-Mail beim Versand einer Email mit dieser Vorlage - zum Beispiel einer Bounce-Nachricht (siehe auch EDIT MANAGED DOMAIN [266] Bounce templates [270], bounce() [548] oder notify() [520]) als „original-mail.eml“ mit angefügt.
 Subject	Der Standard Betreff der Vorlagen lautet „Undelivered Mail Returned to Sender“. Soll ein anderer Betreff verwendet werden, so ist dieser hier einzugeben.
 Advanced	Gibt an in welchen Formaten ein Disclaimer verfügbar sein soll.
 ☒ Add HTML part	Im Standard ist diese Option aktiv. Mit dieser Option steht der Disclaimer (auch) im HTML Format zur Verfügung, so wie er unter Disclaimer as HTML eingetragen ist.
 ☒ Add text part	Im Standard ist diese Option aktiv. Mit dieser Option steht der Disclaimer (auch) im Text Format zur Verfügung, sowie er unter Disclaimer as Text eingetragen ist.

Sektion **Template as HTML preview**

Zeigt eine Vorschau des unter **Template as HTML** eingegebenen HTML Codes an.

Sektion **Template as HTML**

Im Regelfall werden automatisierte Benachrichtigungs-E-Mails wie bounce-Mails ausschließlich im Textformat versendet.

Dennoch kann bei Bedarf auf HTML ausgewichen werden, sofern zum Beispiel Aussehen und Text durch unterschiedliche HTML-Tags zur Formatierung (zum Beispiel Absätze, Schriftgröße oder Schriftfarbe) individuell angepasst werden sollen oder die SEPPmail zum Beispiel als **Auto-Responder** fungieren soll.

Bei neu erstellten Vorlagen ist im Eingabefeld bereits ein Standard Code enthalten, welcher einen deutschen und englischen Standarttext beinhaltet. Dieser kann den individuellen Bedürfnissen angepasst oder vollständig ersetzt werden.

Ebenso können HTML-Vorlagen Dateien als Inlines im Code hinzugefügt werden, welche über die Content-ID (siehe Tabelle unten) zu erreichen sind.

Inlines

Dateien, welche im HTML-Code des Eingabefeldes verwendet werden sollen. Diese können ausgewählt und über **Add** hochgeladen werden. Im Anschluss erscheinen die hochgeladenen Dateien in der Tabelle.

Name	Content-Type	Content-ID
Name der hoch-	Datei- / Mime- Typ der Datei.	ID (cid) unter welcher die Datei im HTML Code abgerufen werden kann.

Name	Content-Type	Content-ID
geladenen Datei.	Beispielsweise <i>image/x-png</i> für eine Bilddatei im PNG-Format	Wird beispielsweise einer hochgeladenen Bilddatei die ID <i>picture1</i> vergeben, so ist diese im HTML Code über <code></code> zu erreichen. Im Standard ist nach dem Hochladen die Content-ID identisch mit dem Dateinamen, kann aber durch Klicken auf den „Name“n angepasst werden.  Hinweis: Werden Inlines unter Template as HTML nicht referenziert, so erscheint die Meldung cid is not referenced in HTML and will not be added to the Disclaimer

Sektion **Template as text**

Bei neu erstellten Vorlagen ist im Eingabefeld **bereits ein Standardtext in deutsch und englisch vorhanden. Dieser kann den individuellen Bedürfnissen angepasst oder vollständig ersetzt werden.**

Sektion **Attachments**

Optional können Dateien, welche jeder E-Mail angehängt werden sollen, ausgewählt und über **Add** hochgeladen werden. Im Anschluss erscheinen die hochgeladenen Dateien in der Tabelle.

Name	Content-Type	Content-ID
Name der hochgeladenen Datei.	Datei- / Mime- Typ der Datei. Beispielsweise <i>image/x-png</i> für eine Bilddatei im PNG-Format	ID (cid) unter welcher die Datei im HTML Code abgerufen werden kann. Wird beispielsweise einer hochgeladenen Bilddatei die ID <i>picture1</i> vergeben, so ist diese im HTML Code über <code></code> zu erreichen. Im Standard ist nach dem Hochladen die Content-ID identisch mit dem Dateinamen, kann aber durch Klicken auf den „Name“n angepasst werden.

Sektion **Info**

Zeigt die unter **Template as HTML** und **Template as Text** verfügbaren **Variablen**⁵⁰⁶ an. Verfügbar sind die internen **Variablen**⁵⁰⁶ sowie solche, welche mit `ldap_read()`⁶¹⁷ geschrieben werden.

7.6.3 Add / Edit Managed Domain

Dieses Sub-Menü wird aus **Mail System** ^[247] **Managed domains** ^[247] durch klicken auf einen **Domain Name** ^[247] zum Editieren, beziehungsweise über **Add managed domain...** für das Anlegen einer neuen **Managed domain** ^[247] aufgerufen.

Sektion Settings

Parameter	Beschreibung						
 Domain name	Name der E-Mail Domäne, für welche durch die SEPPmail Appliance E-Mails angenommen und verarbeitet werden sollen. Diese Einstellung ist nur beim Anlegen einer neuen Managed domain ^[247] - das heißt wenn das Menü über die Schaltfläche Add managed domain... aufgerufen wurde - editierbar (siehe ADD MANAGED DOMAIN ^[266] Settings ^[266]).						
 Forwarding server	Angabe des E-Mail Servers, an welchen die für den oben genannten Domain Name eingehenden E-Mails nach dem Verarbeiten durch die SEPPmail Appliance weitergeleitet werden sollen. Als Eingabe wird folgendes akzeptiert: <table border="0"> <tr> <td>IP-Adresse</td><td>einzelne IP-Adresse (in eckige Klammern [] zu setzen).</td></tr> <tr> <td>Hostname</td><td>wird ein Hostname verwendet, so ist dieser in eckige Klammern [] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt!</td></tr> <tr> <td>MX-Name</td><td>MX-lookup wird ausgeführt (siehe gegebenenfalls auch System ^[224] DNS ^[229] add local zone)</td></tr> </table> Optional ist bei Angabe einer IP-Adresse, eines Host-Namens oder eines MX-Namens zusätzlich die Angabe eines individuellen Ports möglich. Dieser wird direkt im Anschluss mit einem Doppelpunkt „:“ getrennt angegeben, also „[IP-Adresse]:Port“, „[Hostname]:Port“ oder „MX-Name:Port“. Wird kein Port angegeben, so wird der Standard SMTP Port TCP25 verwendet.	IP-Adresse	einzelne IP-Adresse (in eckige Klammern [] zu setzen).	Hostname	wird ein Hostname verwendet, so ist dieser in eckige Klammern [] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt!	MX-Name	MX-lookup wird ausgeführt (siehe gegebenenfalls auch System ^[224] DNS ^[229] add local zone)
IP-Adresse	einzelne IP-Adresse (in eckige Klammern [] zu setzen).						
Hostname	wird ein Hostname verwendet, so ist dieser in eckige Klammern [] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt!						
MX-Name	MX-lookup wird ausgeführt (siehe gegebenenfalls auch System ^[224] DNS ^[229] add local zone)						
 Header Check	Unter Mails from this domain must have a header kann ein X-Header angegeben werden, dessen erwarteter Wert bei with the following value: eingetragen wird. Wird nun versucht von der aktuellen Managed domain ^[247] eine E-Mail zu senden, so muss diese den hier angegebenen X-Header mit dem entsprechenden Wert enthalten (Groß-/ Kleinschreibung beachten!). Andernfalls wird die E-Mail nicht angenommen. Der entsprechende X-Header wird nach dem Prüfen entfernt.						
 Exchange Online Integration	Durch Eingabe der Office 365 Tenant ID (siehe auch https://docs.microsoft.com/de-de/onedrive/find-your-office-365-tenant-id) wird das Relaying aus Office 365 (siehe Exchange Online Relaying ^[255]) für die entsprechende Managed domain ^[247] auf den jeweiligen Office 365 Mandanten beschränkt.  Hinweis: Ist das Eingabefeld leer und wurde dennoch aus einem der unter Exchange Online Relaying ^[255] eingetragenen Netze eine E-Mail mit einer Absender-E-Mail-Adresse der jeweiligen Managed domain ^[247] abgesetzt, so wird die Office 365 Tenant ID des Absenders ausgegeben, zum Beispiel (HINT: Tenant ID detected in mail flow is XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXX)						
 Allowed sending servers for this domain	An dieser Stelle können die IP-Adresse(n) oder Subnetz(e) eingetragen werden, welche im Namen der jeweiligen Managed domain ^[247] senden dürfen. Dadurch wird zum Beispiel in mandantenfähigen Systemen unterbunden, dass ein Mandant im Namen eines anderen						

Parameter	Beschreibung
(leave empty to allow all relaying networks)	E-Mails senden kann. Wird hier kein Eintrag vorgenommen, so darf jede unter Mail System ^[247] Relaying ^[254] eingetragene Adresse im Namen dieser Managed domain ^[247] senden. In der Regel wird der Eintrag der IP-Adresse(n) des/r eingetragenen Forwarding server (siehe Tabelle unter Mail System ^[247] Managed domains ^[247] Spalte Server IP address) entsprechen.  Hinweis: Dieser Eintrag übersteuert nicht die unter Mail System ^[247] Relaying ^[254] vorhandenen Einträge, sondern schränkt diese lediglich pro Managed domain ^[247] ein! Somit müssen die hier eingetragenen IP-Adressen zusätzlich unter Mail System ^[247] Relaying ^[254] vorhanden sein. Nach dem Speichern wird jeweils ein weiteres Eingabefeld eingeblendet.  Hinweis: Wird aufgrund dieser Einstellung eine E-Mail abgewiesen, so erscheint im Log (siehe Logs ^[388] Mail log (last 500) ^[389]) die Meldung: IP xxx.xxx.xxx.xxx is not allowed to send mails for domain <IhreFirma.tld> Relaying denied due to allowed domain settings in Managed domain ^[247] Message Rejected. (550 Mail not accepted)
 Send ALL outgoing mails from this domain to the following SMTP server (optional)	Mit der Eingabe eines Ziel Servers (Eingabeformat identisch zu Mail System ^[247] Managed domain ^[247] ADD/EDIT MANAGED DOMAIN ^[266] Settings ^[266] Forwarding server IP or MX name) wird für die jeweilige Managed domain ^[247] der Outgoing server ^[250] (siehe Mail System ^[247]) übersteuert (sender based routing). Eventuell benötigte TLS-Einstellungen können unter Mail System ^[247] TLS settings ^[257] Add TLS domain... ADD TLS DOMAIN ^[262] vorgenommen werden.
 Postmaster address	Wird hier eine E-Mail Adresse angegeben, so wird diese für den Versand von Bounce- und Benachrichtigungs-E-Mails der jeweiligen Managed domain ^[247] als Absender (FROM-Header) verwendet.
 S/MIME domain keys	Abhängig von der globalen Auswahl unter Mail System ^[247] Managed domain ^[247] Create S/MIME domain keys for managed domain encryption and send public key to vendor pool: werden unterschiedlich Status angezeigt.
 Globally on	Wird angezeigt, wenn global die Einstellung „ON for all domains“ gewählt wurde. Mit diesen Einstellungen wird die Teilnahme am Managed Domain Service ^[31] aktiviert. Mit dem Aktivieren wird für die jeweilige Managed domain ^[247] automatisch ein selbst signiertes X.509 S/MIME Domänen Zertifikat (siehe S/MIME domain encryption ^[274]) erzeugt und an den zentralen SEPPmail Lizenz-, beziehungsweise Key-Server übertragen. Das jeweils neu erzeugte S/MIME Domänen Zertifikat (also ausschließlich der öffentliche Schlüssel !!!) wird danach automatisch an alle SEPPmail Appliances verteilt, so dass alle Unternehmen, welche eine SEPPmail Appliance betreiben ohne jeglichen weiteren Aufwand E-Mails ausschließlich mindestens domänenverschlüsselt untereinander austauschen. Dieser Service ist bereits in der Basis-Lizenz ^[126] enthalten und erfordert keine zusätzlichen Encryption-Lizenzen.

Parameter	Beschreibung
 Create S/MIME domain keys for managed domain encryption for this domain and send public key to vendor pool	Im Standard ist diese Option aktiv. Wird angezeigt, wenn global die Einstellung „Use domain settings“ gewählt wurde. Managed domains^[247] mit aktiver Option globale    Hinweis: In der Regel werden die erzeugten S/MIME-Domänenzertifikate automatisiert durch SEPPmail zur Teilnahme am Managed Domain Service^[31] freigeschaltet. Gegebenenfalls kann das Freischalten durch eine entsprechende E-Mail an support@seppmail.de beschleunigt werden. Hinweis: Wird der Haken im Nachhinein gesetzt und sind bereits Zertifikate vorhanden, so wird das Zertifikat mit der längsten Laufzeit übertragen. Wird ein weiteres Zertifikat generiert, wird dieses aufgrund der längeren Laufzeit ebenfalls übertragen. Soll dieses neu generierte Zertifikat anstatt des bereits bestehenden Zertifikates zur Teilnahme am Managed Domain Service^[31] freigeschaltet werden, so muss dies ebenfalls über eine E-Mail an support@seppmail.de explizit mitgeteilt werden. Achtung: Die Teilnahme am Managed Domain Service^[31] sollte erst erfolgen, wenn der gesamte eingehende E-Mail Strom für die jeweilige Managed domain^[247] über die SEPPmail Appliance geleitet wird. Andernfalls gelangen unter Umständen über den Service verschlüsselte E-Mails unbearbeitet - also weiterhin verschlüsselt - bis zum Empfänger! Wurde bereits ein S/MIME-Domänenzertifikat erzeugt, bevor der E-Mail Strom für die jeweilige Managed domain^[247] über die SEPPmail Appliance geleitet wird, ist unbedingt der Support durch eine E-Mail an support.seppmail.ch darüber zu informieren, dass das entsprechende Domänenzertifikat <u>nicht</u> freigeschaltet werden darf. Ist der E-Mail Fluss komplett umgestellt, muss das Aktivieren für den Managed Domain Service^[31] erneut durch eine E-Mail an support.seppmail.ch angezeigt werden. Wird eine, am Managed Domain Service^[31] teilnehmende Managed domain^[247] - zum Beispiel wegen Umfirmierung - eliminiert, ist dies ebenfalls durch eine E-Mail an support.seppmail.ch

Parameter	Beschreibung
	anzuzeigen. Das entsprechende Domänenzertifikat wird dann von SEPPmail revoziert, und die E-Mail Domäne somit vom Managed Domain Service ^[31] wieder ausgeschlossen. Ebenso müssten nach einem Umstellen der globalen Einstellung auf Off for all domains alle bereits teilnehmenden Domänen gegebenenfalls an support.seppmail.ch für das Ausschließen vom Managed Domain Service ^[31] gemeldet werden.
 Globally off	Wird angezeigt, wenn global die Einstellung OFF for all domains gewählt wurde.  Hinweis: Wurde die globale Einstellung OFF for all domains erst aktiviert, nachdem der Managed Domain Service ^[31] für die jeweilige Managed domain ^[247] bereits etabliert wurde, so steht der an den SEPPmail Lizenz-, beziehungsweise Key-Server übermittelte Schlüssel bis zum Widerruf über eine E-Mail an support@seppmail.de weiterhin den Kommunikationspartnern zur Verfügung. Eingehende Managed Domain Service ^[31] verschlüsselte E-Mails werden weiterhin entschlüsselt.  Hinweis: Der Versand von E-Mails via Managed Domain Service ^[31] bleibt von dieser Einstellung unberührt. Soll dieser ebenfalls unterbunden werden, so ist zusätzlich zu dieser Einstellung unter Domain Certificates ^[489] Managed S/MIME domain certificates ^[489] die Option Auto-update S/MIME domain certificates gleich nach der Installation (!) zu deaktivieren.
 Disclaimer (geändert in 12.0)	Für das Verwenden des Central Disclaimer Management (CDM) ^[125] ist eine entsprechende Lizenz erforderlich. Disclaimer (Ausschlussklauseln) beziehungsweise personalisierte Fußnoten können über das Menü Mail System ^[247] Edit mail disclaimer... ^[259] erzeugt und editiert werden. Ist eine Lizenz vorhanden, wird der Disclaimer gemäß folgender Auswahl angehängt.  Hinweis: Wird eine granularere Einstellung für das Anfügen eines Disclaimers benötigt, zum Beispiel pro Abteilung anstatt pro Managed domains ^[247], so ist dies problemlos über Custom commands ^[308] möglich (siehe auch <code>disclaimer()</code> ^[550]). Das Positionieren eines Disclaimers kann alternativ auch manuell in einer E-Mail selbst erfolgen. Hierzu ist einer E-Mail an der Stelle, an welcher der Disclaimer positioniert werden soll, eine Zeile mit dem Text ##MAILDISCLAIMER## hinzuzufügen. (erweitert in 12.0) Durch Angabe von ##MAILDISCLAIMER_<disclaimer>## (wobei <disclaimer> dem gewünschten Disclaimer aus LIST DISCLAIMER ^[259] entspricht), kann nicht nur die Position, sondern auch explizit der zu verwendende Disclaimer ausgewählt werden.

Parameter	Beschreibung
	Soll die Disclaimer Funktion auch innerhalb der GINA-Träger-E-Mails verwendet werden, so kann dies über Custom commands [308] realisiert werden (siehe auch <code>disclaimer()</code> [550]).
 Initial disclaimer 	Auswahl des Disclaimers für neue, ausgehende E-Mails.
 Reply disclaimer  <i>(neu in 12.0)</i>	Auswahl des Disclaimers für ausgehende Antwort-E-Mails.  Hinweis: Der Disclaimer in Antwort-E-Mails wird direkt nach der Antwort - nicht erst am Ende der E-Mail (!) - angehängt. Somit ist das Verwenden der erweiterten Disclaimer Funktion insbesondere auch für das Erstellen personalisierter Fußnoten geeignet!
 GINA domain 	Über die Auswahl können die für die angegebene E-Mail Domäne zu verwendenden GINA-Einstellungen ausgewählt werden. Diese können über das Menü GINA Domains [416] Domains [416] erzeugt und editiert werden. Wird hier „-DISABLED-“ gewählt, so steht für die ausgewählte Managed domain [247] keine GINA-Technologie zur Verfügung. Das heißt auch, dass bei angeforderter Verschlüsselung und fehlendem öffentlichen Schlüssel des Empfängers die E-Mail abgewiesen (bounced) wird (siehe auch Bounce templates [270] No public key). Bei mandantenfähigen Systemen muss hier zwingend die - beziehungsweise eine der - für den Kunden dediziert eingerichtete GINA-Domain ausgewählt werden, sofern die GINA-Technologie nicht mittels „-DISABLED-“ abgeschaltet wurde.
 Assigned to customer (nur bei Mandanten-fähigen Systemen)	Zuordnung zu einem unter Customers [494] bereits angelegten Kunden in einem mandantenfähigen System. Das Zuordnen zu einem Kunden ist nur beim Anlegen einer neuen Managed domain [247] - das heißt wenn das Menü über die Schaltfläche Add managed domain... aufgerufen wurde - möglich.

Sektion **Bounce templates**

In dieser Sektion können individualisierte Bounce Templates angegeben werden, welche zuvor über **Mail System** [247] **Edit mail templates...** [263] erzeugt wurden.

Parameter	Beschreibung
 No authentication	Im Standard ist bounce_noauth ausgewählt. Zeigt die gewählte Bounce Vorlage für angefordertes Verschlüsseln/Signieren durch nicht vorhandene Benutzer (Users [396]).
 No public key	Im Standard ist bounce_noenc ausgewählt. Zeigt die gewählte Bounce Vorlage für fehlgeschlagenes Verschlüsseln.  Hinweis: Sofern die SEPPmail Appliance in einer Standardkonfiguration unter Verwendung der Verschlüsselungshierarchie [66] betrieben wird, kommt dieses Template nie zum Einsatz, da bei fehlendem Schlüsselmaterial mittels GINA-Technologie verschlüsselt wird.

Parameter	Beschreibung
 No private key	Im Standard ist bounce_noseckey ausgewählt. Zeigt die gewählte Bounce Vorlage bei fehlendem Schlüsselmaterial des internen Senders.  Hinweis: Dieses Template kommt zum Einsatz, wenn ein interner Sender zwar Signatur anfordert, jedoch kein gültiges S/MIME Schlüsselpaar auf der SEPPmail Appliance für diesen Sender verfügbar ist (siehe Users USER 'USER@DOMAIN.TLD' [398] S/MIME [401] oder generiert werden kann (siehe Mail Processing [286] Ruleset generator [287] Key generation [291]).
 Policy not applicable	Im Standard ist bounce_policy ausgewählt. Diese Vorlage wird generell für alle Abweisungen aufgrund einer ENCRYPTION POLICY [313] verwendet, sofern in der jeweiligen ENCRYPTION POLICY [313] nicht explizit eine andere Vorlage gewählt wurde. Wird also eine ENCRYPTION POLICY [313] für mehr als eine Managed domain [247] verwendet, so würde jeweils die Vorlage der jeweiligen Managed domain [247] anstatt einer ENCRYPTION POLICY [313] bezogenen Vorlage verwendet werden. Die Reihenfolge ist dann in aufsteigender Wertigkeit: • Standard Template • Domain Template • Policy Template.
 Send OpenPGP keys	Im Standard ist sendpgpkeys ausgewählt. Die hier ausgewählte Vorlage übersteuert gegebenenfalls die globale Auswahl der Option Mail Processing [286] Miscellaneous options [287] Send new OpenPGP public keys to users when a key is created with template [287].

Sektion External authentication

Definiert die Einstellungen für das Authentisieren an der GINA-Oberfläche über externe Benutzerdaten.

Parameter	Beschreibung
 LDAP	Wird die GINA-Technologie auch intern eingesetzt, zum Beispiel für Large File Transfer (LFT) [107] oder Interne E-Mail Verschlüsselung (IME) [114], so ermöglicht diese Option das Authentisieren der Benutzer der jeweiligen Managed domain [247] gegen ein externes LDAP im organisationsinternen Netz (zum Beispiel Active Directory). Dadurch wird Benutzern aus der jeweiligen Managed domain [247] ermöglicht, sich an der GINA-Oberfläche mit Ihrer E-Mail Adresse und dem im LDAP hinterlegten Passwort (im Falle AD also das Windows Passwort) anzumelden. <u>Funktionsweise:</u> Wird aufgrund oben genannter Konfiguration die E-Mail Adresse (die Hauptadresse, kein E-Mail Alias!) des sich anmeldenden Benutzers (GINA-Accounts) und somit dessen DN in der LDAP Datenbank gefunden, so wird mit diesem DN und dem vom Benutzer im GINA-Portal eingegebenen Passwort ein neuerlicher Verbindungsversuch unternommen. Ist dieser Versuch erfolgreich, so gilt die Authentifizierung am GINA-Portal ebenfalls als erfolgreich. Dabei führt die SEPPmail Appliance einen eigenen Zähler für falsche Passwort-Eingaben. Schlägt das externe Authentisieren öfter fehl als maximal zugelassen, wird der Account lokal temporär deaktiviert. Dabei findet keine Interaktion mehr mit dem externen Server statt. Das Deaktivieren ist also ausschließlich lokal. Somit kann ein SEPPmail Appliance

Parameter	Beschreibung
	Administrator einen deaktivierten GINA Account ^[462] in der SEPPmail Appliance Administrationsoberfläche jederzeit wieder aktivieren oder dauerhaft deaktivieren. Weiterhin besteht die Möglichkeit einzelne GINA Accounts ^[462] von der externen Authentisierung auszunehmen. In diesem Fall wird jeweils wieder das lokale Passwort für das Login verwendet (siehe auch GINA Accounts ^[462] GINA User Details ^[464] User data ^[464] External authentication).
 ☐ Authenticate GINA users from this domain to external LDAP server (eg. Active Directory)	Diese Option ist im Standard inaktiv. Aktiviert die „externe LDAP Authentisierung“.
 ☐ Automatically create GINA account if user exists on external LDAP server	Diese Option ist im Standard inaktiv. Wird diese Option aktiviert, so wird - sofern nicht bereits vorhanden - automatisiert ein GINA Account ^[462] bei erfolgreichem Authentisieren via LDAP angelegt. Der Registrierungsprozess beim initialen Anmelden entfällt somit für den GINA-Benutzer. Voraussetzung hierfür ist, dass die GINA Domain ^[416], an welcher sich der jeweilige Benutzer anmeldet, auch dieser Managed domain ^[247] zugeordnet ist. Auf mandantenfähigen Systemen sind zwingend die Hinweise in Customers Notes ^[495] bezüglich der GINA-Domain Zuordnung zu beachten. Wird die Option im Nachhinein deaktiviert, so werden die bereits vorhandenen Accounts beim nächsten Anmelden aufgefordert sich zu registrieren.  Hinweis: Wird über dieses Verfahren ein GINA Account ^[462] angelegt, so wird - sofern nicht bereits vorhanden - auch automatisiert ein User ^[396] angelegt. Hierfür wird wiederum eine freie Signatur und Verschlüsselung ^[127] lizenz (siehe Encryption/Signature licenses ^[227]) benötigt. Ist diese Option nicht aktiviert, so müssen die GINA Account ^[462]s weiterhin auf der SEPPmail Appliance registriert werden. Dabei muss ein lokales Passwort gesetzt werden. Dieses Passwort wird jedoch nicht für das Authentisieren verwendet, solange die External Authentication aktiviert ist. Während des initialen Registrierens des Accounts wird ein entsprechender Hinweis angezeigt. Wird beim Anmelden an der GINA-Oberfläche das lokale statt dem im LDAP hinterlegten Passwort verwendet, dann - und nur dann! - erhält der Benutzer einen entsprechenden Hinweis (siehe GINA Domains ^[416] Domain ^[416] GINA Edit CHANGE GINA SETTINGS FOR ^[423] Language settings ^[448] Edit translations Edit translation file ^[460] Advanced view Edit translation file ^[460] msgid „ext_auth_enabled“).
 Server	Angabe der/s LDAP-Server(s), gegen welchen authentisiert werden soll. Als Eingabe wird der Hostname oder die IP-Adresse akzeptiert. Mehrere Server können jeweils durch Leerzeichen getrennt eingetragen werden. Die Server werden in der angegebenen Reihenfolge verarbeitet, bis einer von ihnen entweder OK oder INVALID_CREDENTIALS (falsches Passwort) zurückgibt. Bei allen andern Antworten (oder Fehler im Verbindungsaufbau) wird der nächste Server in der Liste versucht.
 Port	Im Standard vorbelegt mit 636 Gibt den Port an, auf welchem der externe LDAP-Server Anfragen entgegen nimmt. Standard LDAP Port ist 389, beziehungsweise 636 für LDAPS (siehe auch TLS required).

Parameter	Beschreibung	
 ☒ TLS required	Im Standard ist diese Option aktiv. Erzwingt das Verschlüsseln der Verbindung zum LDAP-Server mittels TLSv1 oder höher (LDAPS oder LDAPS+STARTTLS).	
 Bind DN	Eingabe des vollständigen Distinguished Name (DN) des read-only Accounts, welcher zur Suche des unter External user attributes Search base E-Mail attribute in der LDAP Datenbank berechtigt ist.	
 Bind password	Passwort für das authentisieren des unter Bind DN eingegebenen Accounts.	
 External user attributes	LDAP objectClass	Im Standard vorbelegt mit *. Eingabe der LDAP-Klasse der Benutzerobjekte am externen LDAP-Server.
	Search base	Suchpfad: Gibt den Zweig des LDAP Verzeichnisses an, in welchem die zu authentisierenden Benutzer Anhand der Suchparameter „LDAP ObjectClass“ und „E-Mail Attribute“ gesucht werden sollen. Hinweis: Das Authentisieren funktioniert auch für verschachtelte OUs („rekursiv“). Als „Search base“ ist dann die oberste, für den „Bind DN“ erreichbare Stufe anzugeben. Der „Bind DN“ muss die Berechtigung zur rekursiven Suche besitzen. Existieren im LDAP Verzeichnis Baum unter der „globalen“ - das heißt der weiter oben liegenden - „Search base“ mehrere Objekte, auf die der Standard-Suchparameter zutrifft (mail=\$email) (objectClass=*) und es werden ungeeignete Objekte zurück geliefert, so muss die „LDAP object class“ so angepasst werden, dass die Suche nur noch diejenigen Einträge zurück liefert, welche tatsächlich für das Authentisieren geeignet sind. Gegebenenfalls sollte über einen externen LDAP Browser in der „globalen“ Search Base nach - zum Beispiel - „(&(mail=max.mustermann@ihre-firma.tld) (objectClass=*))“ gesucht werden. Kommt hier unter Anderem ein - für das Authentisieren nicht geeigneter - Eintrag zurück, so liegt hier das Problem. Über die zurückgegebenen Einträge kann dann eine geeignete objectClass (zum Beispiel objectClass=inetOrgPerson) gesucht werden, so dass nur noch geeignete Einträge gefunden werden.
	Email attribute (Default: "mail")	Im Standard vorbelegt mit "mail". Angabe des Attributes der LDAP Datenbank, unter welchem die E-Mail Adresse des zu authentisierenden Benutzers in der angegebenen Search base gespeichert ist.  Achtung: Das Authentifizieren mittels anderer Werte als der E-Mail Adresse, wie zum Beispiel dem Windows Anmeldenamen aus dem Attribut sAMAccountName, ist nicht möglich!
 Customer Login Test	User	E-Mail Adresse eines in der angegebenen Search base vorhandenen Benutzers

Parameter	Beschreibung				
	<table border="1"> <tr> <td>Password</td><td>Passwort der unter User eingegebenen Benutzers</td></tr> <tr> <td>Test connection</td><td>Über die Schaltfläche Test connection wird ein Verbindungstest angestoßen. Das Ergebnis wird in der Statusleiste (oben) ausgegeben</td></tr> </table>  Hinweis: Mit dem Verbindungstest werden die Verbindungsdaten nicht gespeichert. Sofern also Änderungen vorgenommen wurden, müssen diese über Save changes (ganz unten rechts im Submenü) gespeichert werden.	Password	Passwort der unter User eingegebenen Benutzers	Test connection	Über die Schaltfläche Test connection wird ein Verbindungstest angestoßen. Das Ergebnis wird in der Statusleiste (oben) ausgegeben
Password	Passwort der unter User eingegebenen Benutzers				
Test connection	Über die Schaltfläche Test connection wird ein Verbindungstest angestoßen. Das Ergebnis wird in der Statusleiste (oben) ausgegeben				

**Hinweis:**

Um einen eventuellen, externen Angreifer die Art des Authentisierungsverfahrens nicht Preis zu geben, bleibt der Link „Passwort vergessen?“ auch bei aktivierter, externer Authentisierung in der GINA-Anmeldemaske erhalten.

**Sektion OpenPGP domain encryption****Hinweis:**

Diese Sektion ist nur im Editier-Modus vorhanden.

In dieser Sektion werden die OpenPGP Domänen-Schlüssel angezeigt, sofern vorhanden.

Key ID	Subkey ID(s) <i>(neu in 12.1)</i>	User ID	Issued on	Expires on
<u>Zeigt die Key ID des/der OpenPGP-Domänen-Key(s) an</u>	Zeigt die Key IDs aller vorhandenen Subkeys an.	Zeigt die zur Key ID zugehörige User ID an. Wurde der Key durch die Appliance generiert, so lautet er in der Regel OpenPGP Domain Encryption <domain-confidentiality-authority@ihredomain.tld>	Ausstelldatum des Keys JJJJ-MM-TT	Ablaufdatum des Keys JJJJ-MM-TT

Durch Klicken der **Key ID** wird ein Untermenü mit Details zum Key geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

Über die Schaltfläche **Import OpenPGP key...** kann ein bereits vorhandenes Schlüsselpaar importiert werden (siehe Untermenü **IMPORT OPENPGP KEY** ²⁸⁶⁾).

Über die Schaltfläche **Generate new OpenPGP key** wird ein neues Schlüsselpaar auf der Appliance generiert. *(geändert in 12.1)* Dabei kann die Laufzeit (**Validity in days**) des so erzeugten Schlüssels frei definiert werden und ist mit 825 Tagen vorgelegt.

**Sektion S/MIME domain encryption**

**Hinweis:**

Diese Sektion ist nur im Editier-Modus vorhanden.

In dieser Sektion werden die S/MIME Domänen-Schlüssel angezeigt, sofern vorhanden.

Fingerprint	Issued on	Expires on	Managed Domain Encryption
Zeigt den/die Fingerprint/s des/der S/MIME Domänen-Schlüssel an.  Hinweis: Ist unter Settings ^[266] im Abschnitt S/MIME domain keys ^[267] eine der Optionen Globally on ^[267] oder Create S/MIME domain keys for managed domain encryption for this domain and send public key to vendor pool ^[268] aktiviert, so ist hier mindestens ein Zertifikat zu sehen.	Ausstelldatum des Keys JJJJ-MM-TT	Ablaufdatum des Keys JJJJ-MM-TT	Zeigt an, ob ein Schlüssel freigeschaltet ist und verwendet wird. Mögliche Status: • managed by SEPPmail verwendet für die automatisch verwaltete Domänenverschlüsselung (siehe auch Managed Domain Service ^[31] und Status managed aus SEPPmail domain encryption ^[247]) • unmanaged siehe auch Status unmanaged, beziehungsweise mismatch aus SEPPmail domain encryption ^[247] Beim Status mismatch wird in der Statusleiste eine entsprechende Warnung ausgegeben! Unabhängig vom Status können die Schlüssel gegebenenfalls in Benutzung für eine manuell eingerichtete Domänenverschlüsselung (siehe auch S/MIME domain certificates ^[490]) sein.

Durch Klicken des **Fingerprints** wird ein Untermenü mit Details zum Key geöffnet (vergleiche **X.509 CERTIFICATE 'details'** ^[404]). Dieses bietet die Möglichkeit den öffentlichen Schlüssel (Zertifikat) herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

**Hinweis:**

Wird in den Zertifikatsdetails unter **Key usage** der Haken der Option **Allow signing** entfernt, so wird das entsprechende Zertifikat bei einer Zertifikatssuche in GINA nicht mit angezeigt (siehe auch **CHANGE GINA SETTINGS FOR** ^[423] **Extended settings Allow download of public domain keys/domain certificates (Note: You must assign "Use GINA Settings" under Mail System Settings / Managed Domains)**)

Über die Schaltfläche **Import S/MIME key...** kann ein bereits vorhandenes Schlüsselpaar importiert werden (siehe Untermenü **IMPORT PKCS#12 CERTIFICATE STRUCTURE** ^[280]).

Der Schlüsselaustausch zwischen SEPPmail Appliances erfolgt bei aktivierter Option **Automatically create and publish S/MIME domain keys for all domains** über den **Managed Domain Service** ^[31] automatisch. Somit wird sichergestellt, dass alle SEPPmail Appliances untereinander Domänen verschlüsselt kommunizieren.

Über die Schaltfläche **Generate S/MIME key** wird ein neues Schlüsselpaar auf der Appliance generiert. (*geändert in 12.1*) Dabei kann die Laufzeit (**Validity in days**) des so erzeugten Schlüssels frei definiert werden und ist mit 825 Tagen vorbelegt.

**Hinweis:**

Wurde bereits vor dem Generieren des Domänenzertifikats die interne CA ^[328] eingerichtet, so werden beim Erstellen die dort eingetragenen Attribute verwendet.

Das kann insbesondere dann sinnvoll sein, wenn ein Kommunikationspartner mit einem Gateway eines anderen Herstellers detailliertere Angaben im Domänenzertifikat fordert, obwohl dies laut RFC nicht erforderlich ist.

Generell werden SAN Zertifikate generiert, welche im **Subject Alternative Name** zunächst den Domänen Namen und im Anschluss die E-Mail Adresse eingetragen hat, also beispielsweise `meinefirma.tld domain-confidentiality-authority@meinefirma.tld`

**Sektion Internal mail encryption****Hinweis:**

Diese Sektion ist nur im Editier-Modus vorhanden.

Fingerprint	Issued on	Expires on
Zeigt den/die Fingerprint/s des/der S/MIME Domänen-Schlüssel, welche für die Interne Mail Verschlüsselung ab IME 2.0 ^[127] benötigt werden, an.	Ausstelldatum des Keys JJJJ-MM-TT	Ablaufdatum des Keys JJJJ-MM-TT

Über die Schaltfläche **Import S/MIME key...** kann ein bereits vorhandenes Schlüsselpaar importiert werden (siehe Untermenü **IMPORT PKCS#12 CERTIFICATE STRUCTURE** ^[280]).

Generate new S/MIME key erzeugt ein neues Schlüsselpaar für die Interne Mail Verschlüsselung. *(geändert in 12.1)*
Dabei kann die Laufzeit (**Validity in days**) des so erzeugten Schlüssels frei definiert werden und ist mit 825 Tagen vorbelegt.

Nach Erstellen eines Schlüsselpaares, kann das Zertifikat durch Klicken auf den Fingerprint exportiert werden.

Um das Zertifikat anschließend mit dem **SEPPmail Microsoft Outlook Add-In** ^[190] nutzen zu können, wird in der Regel in der „Global Adress List (GAL)“ des Exchange Servers ein Kontakt mit der E-Mail Adresse aus dem CN dieses Zertifikates und diesem Zertifikat selbst angelegt. Meist wird das Zertifikat des Kontaktes dadurch in den maschinenbezogenen Zertifikatsspeicher der Clients unter „Andere Personen“ „Zertifikate“ übernommen.

**Hinweis:**

Der Ordner „Andere Personen“ wird im Standard erst dann im Zertifikatsspeicher angelegt, wenn für einen Kontakt im Outlook-Adressbuch ein Zertifikat importiert wurde oder ein Eintrag im Exchange in der Global Adress List (GAL) erzeugt wurde.

Der in der Regel in der GAL zu erzeugende Kontakt sollte mit einem Sonderzeichen, zum Beispiel einem Unterstrich „_“ beginnen. Hintergrund ist, dass das **SEPPmail Microsoft Outlook Add-In** ^[190] beim Start von MS Outlook automatisch nach diesem Eintrag sucht. Steht der Eintrag aufgrund des alphabetischen Sortierens relativ weit am Ende der GAL, kann diese Suche mitunter sehr lange dauern. Als Folge würde sich auch der Start von MS Outlook entsprechend verzögern.

Dies wiederum könnte ein automatisches Deaktivieren des **SEPPmail Microsoft Outlook Add-In** ^[190] zur Folge haben, sofern dem nicht durch entsprechende Konfigurationsmaßnahmen entgegengewirkt wurde.

**Sektion DKIM settings (optional)**

Parameter	Beschreibung
 Generate a DKIM key pair for this domain	Diese Option ist im Standard inaktiv. Durch Setzen des Hakens und anschließendem Speichern via Save changes wird für die jeweilige Managed Domain ein DKIM Schlüsselpaar generiert. Ab diesem Zeitpunkt werden alle ausgehenden E-Mails der Managed domain mit einer DKIM Signatur versehen. Achtung: Damit die DKIM Signatur vom Empfänger geprüft werden kann, ist der öffentliche Teil des DKIM Schlüssels zwingend als Text-Eintrag im DNS zu publizieren. Die vorzunehmenden Anpassungen für eine DNS-Zonendatei sind dabei dem Feld Before enabling, make sure that the following TXT entry exists in your DNS zone file: zu entnehmen. Bei einigen Internet Service Providern (ISP) kann die Zonendatei nicht direkt editiert werden. Hier ist meist zunächst die Eingabe in der Form default._domainkey.<manged domain> also zum Beispiel default._domainkey.meinefirma.tld gefolgt von einem weiteren Eingabefeld, in welchem der Inhalt des Feldes entry for 'default._domainkey.customer1.local' as text: einzufügen ist. Wird der erstellte Texteintrag vom DNS korrekt publiziert, so sollte das dritte Feld wie folgt überschrieben sein found a valid DNS entry for this DKIM key: Andernfalls ist das Feld mit DNS entry missing or invalid: überschrieben. Im Feld selbst ist der Texteintrag zu sehen, wie er von der SEPPmail Appliance ausgelesen wird. 

Sektion **TLS settings** (optional)

Soll zum nachgelagerten Groupware-System für eine E-Mail Domäne (siehe Tabelle unter **Mail System** ²⁴⁷) **Managed domains** ²⁴⁷ Spalte **Server IP address**) eine TLS verschlüsselte Verbindung aufgebaut werden, so kann die TLS Verschlüsselung an dieser Stelle konfiguriert werden.

Das Einrichten von TLS-Verbindungen ist im Kapitel zum Untermenü **ADD TLS DOMAIN** ²⁸² beschrieben.

Sektion **Domain statistics**



Hinweis:

Diese Sektion ist nur im Editier-Modus vorhanden.

In dieser Statistik werden nur diejenigen Kryptographie-Technologien angezeigt, welche auf der SEPPmail Appliance bereits zum Einsatz kamen.

Parameter	Beschreibung
 Number of accounts in this domain	Anzahl der auf der SEPPmail Appliance angelegten Benutzer (entspricht User-Lizenzen)
 S/MIME encrypted e-mails sent	Anzahl der versendeten E-Mails, welche mittels S/MIME-Technologie verschlüsselt wurden.
 S/MIME encrypted e-mails received	Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie verschlüsselt waren.
 OpenPGP encrypted e-mails sent	Anzahl der versendeten E-Mails, welche mittels OpenPGP-Technologie verschlüsselt wurden.
 OpenPGP encrypted e-mails received	Anzahl der empfangenen E-Mails, welche mittels OpenPGP-Technologie verschlüsselt waren.
 S/MIME Domain encrypted e-mails sent	Anzahl der versendeten E-Mails, welche mittels S/MIME-Technologie domänenverschlüsselt wurden.
 S/MIME Domain encrypted e-mails received	Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie domänenverschlüsselt waren.
 OpenPGP Domain encrypted e-mails sent	Anzahl der versendeten E-Mails, welche mittels OpenPGP-Technologie domänenverschlüsselt wurden.
 OpenPGP Domain encrypted e-mails received	Anzahl der empfangenen E-Mails, welche mittels OpenPGP-Technologie domänenverschlüsselt waren.
 S/MIME signed e-mails sent	Anzahl der versendeten E-Mails, welche mittels S/MIME-Technologie signiert wurden.
 S/MIME signed e-mails received	Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie signiert waren.
 GINA encrypted e-mails sent	Anzahl der versendeten E-Mails, welche mittels GINA-Technologie verschlüsselt wurden.

Alle vorgenommenen Änderungen werden über die Schaltfläche **Save changes** gespeichert.
Das Löschen einer Domain erfolgt über **Delete domain**.

**Hinweis:**

Verfügt die Domäne über einen Domänenschlüssel (siehe, [S/MIME domain encryption](#)^[274] beziehungsweise [OpenPGP domain encryption](#)^[274]), so erscheint in der **Statusleiste** eine entsprechende Warnung und das Löschen muss durch Drücken von **Delete domain** erneut bestätigt werden.

**Achtung:**

Nimmt die Domäne mit einem der S/MIME Schlüssel aktiv am [Managed Domain Service](#)^[31] (Status **managed** in **SEPPmail domain encryption**^[247]) teil, so erscheint selbst nach dem zweiten Drücken von **Delete domain** eine weitere Warnung in der **Statusleiste**, welche darauf hinweist.

Vor dem Löschen durch ein weiteres Klicken auf **Delete domain muss zwingend durch ein Ticket an support@seppmail.de das Beenden der Teilnahme am [Managed Domain Service](#)^[31] angezeigt werden!**

Andernfalls werden E-Mails von SEPPmail Appliances an diese Domäne weiterhin mittels [Managed Domain Service](#)^[31] verschlüsselt, können vom Empfänger jedoch mangels privaten Schlüssel nicht mehr entschlüsselt werden.

7.6.3.1 Import OpenPGP Key(s)

Dieses Sub-Menü wird aus **EDIT MANAGED DOMAIN** ^[268] **OpenPGP domain encryption** ^[274] aufgerufen.

Sektion **Key Data**

Parameter	Beschreibung
 Passphrase	Eingabe für die Passphrase mit welcher der private OpenPGP Schlüssel bei Export verschlüsselt wurde.
 Key file	Über die Schaltfläche „Datei auswählen“ wird die OpenPGP Schlüsseldatei ausgewählt, welche importiert werden soll. Diese muss das komplette Schlüsselpaar, also privaten und öffentlichen Schlüssel enthalten.
 or key as string	Alternativ zur Auswahl einer Schlüssel Datei kann der Schlüssel als Text in dieses Feld kopiert werden

Über die Schaltfläche **Import** wird der Vorgang abgeschlossen.

7.6.3.2 Import PKCS#12 certificate structure(s)

Dieses Sub-Menü wird aus **EDIT MANAGED DOMAIN** ^[268] **S/MIME domain encryption** ^[274] aufgerufen.

Sektion **Certificate data**

Parameter	Beschreibung
 Passphrase	Eingabe für die Passphrase mit welcher der private S/MIME Schlüssel bei Export in eine PKCS#12 Datei verschlüsselt wurde.
 PKCS#12 file	Über die Schaltfläche „Datei auswählen“ wird die S/MIME Schlüsseldatei ausgewählt, welche importiert werden soll. Diese muss das komplette Schlüsselpaar, also privaten und öffentlichen Schlüssel enthalten. PKCS#12 Dateien haben die Dateiendung .p12 oder auch .pfx.

Über die Schaltfläche **Import** wird der Vorgang abgeschlossen.

7.6.4 Extended Postfix MTA Settings

Dieses Sub-Menü wird aus **Mail System** ^[247] **Managed domains** ^[247] aufgerufen.



Achtung:

In der Regel sind Änderungen an den **EXTENDED POSTFIX MTA SETTINGS** ^[281] nicht notwendig!
Sollten in komplexen Infrastrukturen dennoch Anpassungen notwendig sein, so sind diese mit Bedacht vorzunehmen, da das Eintragen von fehlerhaften Werten zum Erliegen des Systems, beziehungsweise des E-Mail Flusses führen kann. postfix Kenntnisse werden vorausgesetzt.



Hinweis:

Bei den **EXTENDED POSTFIX MTA SETTINGS** ^[281] handelt es sich um maschinenbezogene Einstellungen. Das heißt, diese werden nicht im **Cluster** ^[383] synchronisiert und müssen somit im Bedarfsfall auf jedem Cluster Partner einzeln vorgenommen werden.



Sektion MTA settings

Spalte	Beschreibung
 Tag	Gibt den postfix Parameter an, welcher angepasst werden soll. Erklärungen zu den einzelnen Parametern sind unter www.postfix.org/postconf.5.html nachzulesen.
 Postfix default setting	Gibt den postfix Standardwert des jeweiligen Tag an.
 Appliance default setting	Gibt den SEPPmail Appliance Standardwert des jeweiligen Tag an, sofern dieser vom postfix Standard abweicht.
 Appliance dynamic setting	Gibt die Parameter an, welche über andere Konfigurationsfelder der SEPPmail Appliance konfiguriert und somit überschrieben wurden.
 Custom setting	Eingabefeld für das manuelle Anpassen des jeweiligen Parameters.  Achtung: Die Eingabe falscher Werte kann zu unerwünschten Auswirkungen, beziehungsweise Verhalten der Appliance, bis hin zum Erliegen des E-Mail Flusses oder des Systems führen.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

7.6.5 Add TLS Domain

Dieses Sub-Menü wird aus **Mail System**^[247] **TLS settings**^[251] aufgerufen.

Sektion **Domain info**

Parameter	Beschreibung						
 Domain name	In der Regel wird hier der Name der E-Mail Domäne des Kommunikationspartners eingetragen. Diese Einstellung ist nur beim Anlegen einer neuen TLS-Verbindung - das heißt wenn das Menü über die Schaltfläche Add TLS Domain... aufgerufen wurde - editierbar.						
 Optional forwarding server address	Wird an dieser Stelle kein Eintrag vorgenommen, so wird der unter Domain Name angegebene Name per MX aufgelöst. Als Eingabe wird folgendes akzeptiert: <table> <tr> <td>IP-Adresse</td><td>einzelne IP-Adresse</td></tr> <tr> <td>Hostname</td><td>wird ein Hostname verwendet, so ist dieser in eckige Klammern [] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt</td></tr> <tr> <td>MX-Name</td><td>MX-lookup wird ausgeführt (siehe gegebenenfalls auch System^[224] DNS^[229] add local zone)</td></tr> </table> Optional ist bei Angabe einer IP-Adresse oder eines Host-Namens zusätzlich die Angabe eines individuellen Ports möglich. Dieser wird direkt im Anschluss mit einem Doppelpunkt „:“ getrennt angegeben, also „IP-Adresse:Port“ oder „Hostname:Port“. Wird kein Port angegeben, so wird der Standard SMTP Port TCP25 verwendet.  Hinweis: Der hier optional eingegebene Server übersteuert das eingestellte Standard Routing (siehe Mail System^[247] Outgoing server^[250]) zu der unter Domain name angegebenen Zieldomäne. Das heißt alle E-Mails an die unter Domain name genannte E-Mail Domäne werden direkt an die hier eingegebene Adresse geroutet!	IP-Adresse	einzelne IP-Adresse	Hostname	wird ein Hostname verwendet, so ist dieser in eckige Klammern [] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt	MX-Name	MX-lookup wird ausgeführt (siehe gegebenenfalls auch System ^[224] DNS ^[229] add local zone)
IP-Adresse	einzelne IP-Adresse						
Hostname	wird ein Hostname verwendet, so ist dieser in eckige Klammern [] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt						
MX-Name	MX-lookup wird ausgeführt (siehe gegebenenfalls auch System ^[224] DNS ^[229] add local zone)						

Sektion **TLS settings**

Über die TLS settings wird der Grad der Prüfungen für eine TLS-Verbindung zum Ziel-Server im Internet, zum **Outgoing server**^[250] (siehe **Mail System**^[247]) beziehungsweise zu den jeweiligen Groupware- also **Forwarding server** (siehe Tabelle unter **Mail System**^[247] **Managed domains**^[247] Spalte **Server IP address**) eingestellt.



Hinweis:

Mit dieser Einstellung wird lediglich TLS **zur** Ziel-Domäne beziehungsweise **zum** Ziel-Server konfiguriert.

Das Entgegennehmen einer eingehenden Verbindung kann nicht eingestellt werden. Unter anderem vermittelt deshalb TLS häufig eine „falsche“ Sicherheit.

Für das Entgegennehmen von TLS Verbindungen wird das unter **SSL^[319] eingebundene Zertifikat verwendet.**

**Hinweis:**

Wird hier keine Konfiguration vorgenommen, so gilt die Einstellung „may“ (siehe folgende Tabelle). Das heißt, unterstützt das nachgelagerte E-Mail System TLS, so wird die SEPPmail Appliance eine TLS-verschlüsselte Verbindung dorthin aufbauen.

TLS-Einstellung	Beschreibung
  None	Keine TLS-Verschlüsselung.
  May	E-Mails werden über einen TLS-verschlüsselten Kanal versendet, falls der empfangende E-Mail Server TLS-Verschlüsselung unterstützt.
  Encrypt	E-Mails werden nur versendet, falls der Versand mittels TLS-Verschlüsselung möglich ist.
  Verify	E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich und das SSL Zertifikat des empfangenden E-Mail Servers gültig ist (Ausgestellt von einer vertrauenswürdigen CA und nicht abgelaufen/revoziert).
  Secure	E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich, das SSL Zertifikat des empfangenden E-Mail Servers gültig, der FQDN des E-Mail Servers identisch mit dem im Zertifikat (Antragsteller) eingetragenen Namen (CN) und der Name der E-Mail Domäne identisch mit dem Domänen Namen des E-Mail Servers ist. Somit wird ein MX-Spoofing verhindert. Das Verwenden von Wildcard-Zertifikaten ist an dieser Stelle nicht möglich. Beispiel: 1. Versand einer E-Mail an max.mustermann@partner.tld a. MX-Lookup ergibt MX-Lookup ergibt partner.tld MX preference=10, mail exchanger=mail1.partner.tld partner.tld MX preference=20, mail exchanger=mail2.partner.tld b. Jeder dieser Server hat in seinem für TLS verwendeten Zertifikat als CN seinen FQDN eingetragen. c. Der Domainname aller hosts (mail1, mail2) lautet auf partner.tld und stimmt somit mit dem Domainname der E-Mail Domäne überein. => Überprüfung bei der Einstellung „secure“ ist erfolgreich 2. Annahme: Das Unternehmen mit der E-Mail Domäne kommunikationspartner.tld betreibt diese Domäne auch mit einer anderen Länderdomäne (com). Versand einer E-Mail an erika.mustermann@kommunikationspartner.com a. MX Lookup ergibt partner.com MX preference=10, mail exchanger=mail2.partner.tld partner.com MX preference=20, mail exchanger=mail4.partner.tld a. Der Domainname der E-Mail Domäne partner.com stimmt nicht mit dem der Mailserver – partner.tld – überein => Die Überprüfung schlägt fehl Fazit: Für die E-Mail Domäne partner.tld kann der TLS Security Level auf „secure“ belassen bleiben. Sollte der Security Level „verify“ für die Maildomäne partner.com nicht ausreichend sein, so muss der Level „Fingerprint“ verwendet werden. Hierzu sind die Fingerprints aller Mailserver (mail1 und mail2.kommunikationspartner.com) einzutragen.

TLS-Einstellung	Beschreibung
	 Hinweis: Wird anstatt eines MX Lookups ein Host direkt adressiert, so entfällt das Prüfen des Übereinstimmens des Hostnamens aus dem Domänenteil der E-Mail Adresse mit dem Mail Exchanger. Das heißt, würde in „2.Annahme“ als Forwarding Server anstatt „kommunikationspartner.com“ zum Beispiel „[mail2.partner.tld]“ eingetragen, so wäre die Überprüfung bei der Einstellung „secure“ erfolgreich. Dies ist insbesondere bei Office 365 Anbindungen relevant.
 Fingerprint	E-Mails werden nur versendet, die Gegenstelle TLS unterstützt und das vorgezeigte Zertifikat den im eingabefeld eingetragenen Fingerprint besitzt. Stehen für die Ziel-Domäne mehrere E-Mail Server zur Verfügung, so können deren Fingerprints getrennt durch Pipe „ “ eingetragen werden,

Die vorgenommenen Änderungen werden über die Schaltfläche **Save changes** gespeichert.

Erklärende Anmerkungen:

Überprüfen des empfangenden E-Mail Servers auf die Verwendung eines Wildcard-SSL Zertifikats

Ob ein E-Mail Server ein Wildcard-SSL Zertifikat verwendet kann sehr einfach mit dem Kommandozeilentool **OpenSSL** durchgeführt werden.

Beispiel:

```
# openssl s_client -starttls smtp -crlf -connect xxx.xxx.xxx.xxx:25
```

Im Beispiel steht xxx.xxx.xxx.xxx für die tatsächliche IP-Adresse des Zielservers. Alternativ kann der Hostname des Zielservers verwendet werden.

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25
```

Das Ergebnis der Abfrage wird wie unten dargestellt aussehen. Anhand des Zertifikats-Subject im Parameter **CN** kann festgestellt werden, ob es sich um ein Wildcard-SSL Zertifikat handelt. Im Beispiel wurde in der Antwort der Wert **CN=*.psmtp.com** zurückgegeben. Somit handelt es sich um ein Wildcard-Zertifikat „*“, welches für alle Hosts der Domain **psmtp.com** verwendet werden kann. Ebenfalls interessant ist der **Parameter X509v3 Subject Alternative Name:**. Als Wert wird hier **DNS:*.psmtp.com** zurückgegeben. In diesem Feld können noch weitere Domains enthalten sein.

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25 | openssl x509 -text -noout
```

```
depth=1 C = US, O = Google Inc, CN = Google Internet Authority
```

```
.
```

```
Certificate:
```

```
.
```

```
Subject: C=US, ST=California, L=Mountain View, O=Google Inc, CN=*.psmtp.com
```

```
.
```

```
.
```


X509v3 Subject Alternative Name:
DNS:*.psmtp.com

Die Darstellung der Ausgabe wurde auf die wesentlichen Informationen reduziert.

Auslesen des SHA1-Fingerprint aus dem SSL Zertifikat des empfangenden E-Mail Servers

Einen Schritt zuvor wurde beschrieben, wie das vom empfangenden E-Mail Server verwendete SSL Zertifikat ausgelesen werden kann. Dabei ist es nicht relevant, ob es sich hierbei um ein Wildcard-Zertifikat handelt oder nicht.

Der Fingerprint eines SSL Zertifikats kann relativ einfach mit dem Kommandozeilentool **OpenSSL** ausgelesen werden.

Beispiel:

```
# openssl s_client -starttls smtp -crlf -connect xxx.xxx.xxx.xxx:25 | openssl x509 -noout -fingerprint
```

Auch in diesem Beispiel steht xxx.xxx.xxx.xxx für die tatsächliche IP-Adresse des Zielservers, welche alternativ durch den Hostnamen des Zielservers ersetzt werden kann.

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25 | openssl x509 -noout -fingerprint
```

Die daraus resultierende Ausgabe sollte wie folgt aussehen:

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25 | openssl x509 -noout -fingerprint
```

```
depth=1 C = US, O = Google Inc, CN = Google Internet Authority
```

```
verify error:num=20:unable to get local issuer certificate
```

```
verify return:0
```

```
250 HELP
```

```
SHA1 Fingerprint=DD:9A:EC:66:E2:43:81:B9:20:2B:75:DB:30:C8:67:CC:9B:B0:D1:99
```

```
read:errno=0
```

In der Ausgabe wird der benötigte SHA1 Fingerprint angezeigt. Dieser Wert kann nun in die Konfiguration übernommen werden.

7.7 Mail Processing

Im Menüpunkt **Mail Processing**^[285] wird das Regelwerk der SEPPmail Appliance konfiguriert. Dieses Regelwerk ist mit einem Workflow System vergleichbar und stellt das zentrale Element der SEPPmail Appliance dar.

Um spezielle Verschlüsselungsmethoden zu einzelnen Zielen einzurichten, steht über **Edit policy table...** das Sub-Menü **ENCRYPTION POLICY**^[313] zur Verfügung. Über dieses können - gegebenenfalls mandantengetrennt - entsprechende Regeln definiert werden.

Sektion SMTP ruleset

Zeigt die Erstelltdaten des aktiven Rulesets an.

Parameter	Beschreibung
 Version	Zeigt die Firmware Version, mit welcher das aktuelle Ruleset erstellt, beziehungsweise hochgeladen wurde.
 Creator	Zeigt den User, welcher das aktuelle Ruleset aktiviert hat
 Date	Zeigt das Aktivierungsdatum des aktuellen Rulesets.
 Type	Zeigt, wie das Ruleset erstellt wurde.
 Generator	Über Generate ruleset mit den unter Ruleset generator ^[287] angezeigten, beziehungsweise vorgenommenen Einstellungen.
 Upload	Über Upload ruleset
 Details	Über Show ruleset wird der Ruleset Code angezeigt

Generate ruleset generiert ein Ruleset mit den unter **Ruleset generator**^[287] angezeigten, beziehungsweise vorgenommenen Einstellungen.



Hinweis:

Ist ein Ruleset vom **Type** „Upload“ aktiv, so wird **Generate ruleset** grau dargestellt. Um den **Type** auf „Generator“ ändern zu können, muss im **Ruleset Generator**^[287] zweimal **Save** geklickt werden!

Upload ruleset... importiert einen, gegebenenfalls unter Zuhilfenahme der **Referenz der Regelwerk-Anweisungen**^[504] manuell geschriebenen Code aus der ausgewählten Datei.

Im Regelfall ist dies nicht zu empfehlen, da dieses Regelset dann auch unter Umständen bei Versionsupdates angepasst werden muss. Sinnvoller ist in der Regel, individuelle Anpassungen über **Custom commands**^[308] des **Ruleset generator**^[287] entsprechend im Code zu platzieren.



Achtung:

Das Ruleset muss nach der initialen Installation wenigstens einmal generiert werden.

Sektion Miscellaneous options

Sonstige Einstellungen.

Parameter	Beschreibung
 Enable LDAP server on port 388, 387 and 635 to distribute collected S/MIME certificates to internal users: ☐	Ermöglicht den Zugriff auf die auf der SEPPmail Appliance bekannten Verschlüsselungszertifikate externer Kommunikationspartner, welche unter X.509 Certificates ^[47] gelistet sind. Hinweis: Dies ermöglicht zum Beispiel Absendern, welche mittels Zusatzhardware am Client direkt verschlüsseln müssen, auf das eingesammelte Schlüsselmaterial der SEPPmail Appliance über ein LDAP-Adressbuch zuzugreifen. 
 Off	Standardeinstellung.
 Server	Aktiviert die LDAP Key Server Funktion der SEPPmail Appliance, für die unter X.509 Certificates ^[47] vorhandenen Zertifikate.
 ☐ Send new OpenPGP public keys to users when a key is created with template ☐	Diese Option ist im Standard inaktiv und mit der Auswahl „sendpgpkeys“ vorbelegt. Wird für einen Benutzer auf der SEPPmail Appliance ein OpenPGP Schlüsselpaar erzeugt - egal ob manuell oder automatisch (siehe Sektion Ruleset generator ^[28]) dieses Menüs unter Key generation ^[29] die Option Issue local OpenPGP keys for users ^[29] - so wird durch Aktivieren dieser Option der öffentliche Schlüssel des automatisch generierten Schlüsselpaares unter Verwendung der ausgewählten E-Mail Vorlage (siehe auch LIST TEMPLATE ^[26]) an den neu erzeugten Benutzer gesendet. Dadurch wird dieser Benutzer in die Lage versetzt, seinen öffentlichen Schlüssel selbst an Kommunikationspartner weiterzugeben. Diese werden dadurch wiederum in die Lage versetzt, OpenPGP verschlüsselt mit diesem Benutzer zu kommunizieren. Die für den Versand verwendete E-Mail Vorlage kann bei Bedarf pro Managed Domain ^[24] individuell übersteuert werden (siehe Send OpenPGP keys ^[27]). Der Absender dieser E-Mail ist der globale Postmaster ^[25], falls kein individueller Postmaster ^[24] hinterlegt wurde. Hinweis: Das Verteilen des öffentlichen OpenPGP Schlüssels an Kommunikationspartner impliziert immer, dass die Prüfsumme (Hash) dieses Schlüssels vor dem Verwenden durch den Kommunikationspartner auf einem zweiten Kanal - zum Beispiel per Telefon - im Nachgang geprüft wird. Dies ist erforderlich, um die Integrität des Schlüssels sicherzustellen. Aus diesem Grund wird empfohlen, das Bereitstellen von OpenPGP Schlüsseln über die GINA-Technologie zu realisieren (siehe CHANGE GINA SETTINGS FOR ^[42] Extended settings ^[43] Enable S/MIME certificate / OpenPGP key search and management in GINA). 

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

Sektion Ruleset generator

Mit dem **Ruleset generator** wird quasi ein „Workflow System“ für eingehende und ausgehende E-Mails definiert.

**Achtung:**

Beim Einsatz von Frontend Servern (siehe **Cluster**^[383] **Add this device as frontend server**^[385]) muss jede Änderung im **Ruleset generator** durch erneutes Speichern am Frontend Server (**Generate ruleset**) bekannt gemacht werden.

Die in dieser Sektion vorhandenen Eingabefelder für **Betreffzeilen Schlüsselwörter**^[164] (text in subject) sind mit „regular expressions“ zu befüllen. Das heißt Sonderzeichen müssen mit einem backslash „\“ als solche gekennzeichnet werden. Ein Aneinanderreihen mehrerer Schlüsselwörter ist durch das Trennen mit dem pipe-Zeichen „|“ möglich.

Beispiel:

Soll als **Betreffzeilen Schlüsselwörter**^[164] <abc> verwendet werden so ist diese wie folgt einzugeben: \<abc>
Soll sowohl das **Betreffzeilen Schlüsselwörter**^[164] <abc> als auch [def] verwendet werden so ist diese wie folgt einzugeben: \<abc>|[def]
(siehe auch **Reguläre Ausdrücke**^[514])

Groß-/Kleinschreibung wird bei der Eingabe des Schlüsselwortes in der Betreffzeile ignoriert.

Bei Verwenden des MS Outlook Add-In im Betreffzeilen-Modus ist darauf zu achten, dass bei Änderungen der Schlüsselwörter in der Appliance, diese entweder als zusätzliche Werte hinzugefügt werden, oder die Werte im Add-In an die Werte der Appliance angepasst werden müssen.

**Hinweis:**

Generell werden bei eingehenden E-Mails - also solche, die nicht von einer **Managed domain**^[247] stammen - alle hier definierten Schlüsselwörter entfernt.
Das heißt, von außen können weder Steuerbefehle an die Appliance übergeben werden, noch können von der Appliance durchgeführte kryptographische Aktionen (Entschlüsseln, Prüfen von Signaturen) vorgetäuscht werden.

**Achtung:**

Um auf der Appliance keine undefinierten Zustände zu erzeugen, ist das gleichzeitige Verwenden unterschiedlicher, sowie insbesondere entgegengesetzter Steuermerkmale (Schlüsselwörter, (X-)Header) in ausgehenden E-Mails unbedingt zu vermeiden!
Weiterhin können mit einem Schlüsselwort nicht zwei Aktionen gleichzeitig angesteuert werden.

Parameter	Beschreibung
General settings	
☒ Do not touch mails with the following text in subject:	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[plain\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird diese kryptographisch unbehandelt weitergeleitet. Das Ruleset wird nicht weiter durchlaufen. Dies ergibt unter Umständen Sinn, wenn all diese Voraussetzungen gegeben sind: • Einstellung Always use S/MIME or OpenPGP if user keys are available an der SEPPmail Appliance aktiv • Absender weiß, dass der Empfänger temporär nur auf einem Mobilien Endgerät empfangen kann • Inhalt der E-Mail ist nicht vertraulich
<i>Add-disclaimer to all outgoing and internal emails</i>	(in 12.0 nach Edit managed domain "X" ^[266] Settings ^[266] Disclaimer ^[269] Initial disclaimer ^[270] <i>inverschoben</i>)
<i>Also add disclaimer to replies (in-reply-to header set)</i>	(in 12.0 nach Edit managed domain "X" ^[266] Settings ^[266] Disclaimer ^[269] Reply disclaimer ^[270] <i>verschoben</i>)
☒ Reproces	Im Standard ist diese Option aktiv. Ermöglicht einem Empfänger eine verschlüsselte E-Mail aus seinem Postfach erneut an die SEPPmail Appliance zum Entschlüsseln zu senden. Hierfür ist die verschlüsselte E-Mail als Anhang

Parameter	Beschreibung
s mails sent to reprocess @ decrypt.re process	in eine neue (Träger-)E-Mail zu packen und an die Adresse „reprocess@decrypt.reprocess“ zu senden. Auf der SEPPmail Appliance wird die Träger-E-Mail verworfen und die darin befindliche, ursprünglich verschlüsselte Nachricht erneut verarbeitet und zugestellt. Dies setzt natürlich voraus, dass der für das Entschlüsseln benötigte private Schlüssel der SEPPmail Appliance bekannt ist. Anwendungsbeispiele könnten sein: • Direktes Weiterleiten verschlüsselter E-Mails an den internen E-Mail Server bei Ausfall der Appliance • Migration von lokalem Schlüsselmaterial auf den Clients hin zur SEPPmail Appliance bei gleichzeitigen zurückbleiben von verschlüsselten E-Mails in den Postfächern der Empfänger Ebenso ermöglicht dieser Befehl OpenPGP verschlüsselte Dateien aus dem Datei-System durch Senden als E-Mail Anlage an diese Adresse zu entschlüsseln.
 Place new tags at the beginning of the subject	Diese Option ist im Standard inaktiv. Durch das Aktivieren dieses Punktes werden von der Appliance gesetzte Kennzeichen (siehe zum Beispiel Add this text to message subject after decryption oder Add this text to message subject if S/MIME signature check succeeds;) anstatt am Ende des Betreffs an den Anfang gesetzt.
 Log message metadata	Im Standard ist diese Option aktiv. Aktiviert das Anzeigen des Betreffs in Logs ^[388]. Dies erleichtert zwar oft die Fehleranalyse, ist aber gelegentlich aus revisionstechnischen Gründen untersagt.
 User creation	
  Achtung: Die hier beschriebenen Verhaltensweisen für das automatische Generieren von Usern (siehe auch Users ^[396]) gelten nur dann zu 100%, wenn diese nicht durch Custom commands ^[308] übersteuert werden. Für das Generieren von neuen Benutzern wird die SMTP-Adresse des FROM-Headers herangezogen.	
 Do not create accounts (also disables custom commands for user creation)	Benutzer müssen auf der Appliance manuell - gegebenenfalls auch durch Bulk-Imports (siehe Administration ^[369] Bulk Import ^[374] Import X.509 keys and certificates beziehungsweise Import OpenPGP key pairs) - angelegt werden.  Hinweis: Wird diese Einstellung gewählt, so ist sicherzustellen, dass kein Absender, welcher in der SEPPmail Appliance nicht bereits als Benutzer angelegt ist, Merkmale (Schlüsselwort, Add-In, Header) für das kryptographische Behandeln von E-Mails verwendet. In dieser Konstellation würde die Anforderung ignoriert und somit die E-Mail ohne die gewünschte kryptographische Aktion versendet. Dieses Verhalten kann bei Bedarf durch Custom Commands ^[308] dahingehend geändert werden, dass E-Mails in dieser Konstellation abgewiesen werden (siehe Bounce von E-Mails nicht authentifizierter Benutzern ^[752]).
 Create accounts for new users if user tries to sign / encrypt	Standardeinstellung. Absender, welche über ein entsprechendes Merkmal eine E-Mail als zu verschlüsselnd oder zu signierend markieren und noch nicht als Benutzer (siehe Users ^[396]) auf der SEPPmail Appliance vorhanden sind, werden automatisch angelegt. Bei Verwenden dieser Option ist darauf zu achten, dass genügend freie Benutzerlizenzen vorhanden sind (siehe Home ^[220] Licenses ^[220] Encryption/Signature licenses ^[221]). Bei Überschreiten des Lizenzkontingents werden E-Mails mit dem Hinweis „license violation“ abgewiesen (bounced) und eine Watchdog-Meldung erzeugt.

Parameter	Beschreibung
	 Hinweis: Kommen Custom Commands ^[308] zum Einsatz, so werden diese in der Reihenfolge Custom Commands for outgoing e-mails BEFORE encryption ^[308], Custom commands for user creation ^[308] abgearbeitet.
 Create accounts for all users	Jeder Absender, der über die SEPPmail Appliance eine E-Mail sendet, wird als Benutzer angelegt, sofern noch nicht vorhanden. Dabei spielt es keine Rolle, ob Verschlüsseln/Signieren angefordert wurde oder nicht. Diese Einstellung ist geeignet, um zum Beispiel generell alle E-Mails aus einem Unternehmen zu signieren. Ein weiterer Anwendungsfall wäre, wenn die SEPPmail Appliance nicht direkt im E-Mail Strom steht, sondern bereits über eine vorgelagerte Komponente entschieden wird, welche E-Mails kryptographisch zu behandeln sind und nur diese an die SEPPmail Appliance übergeben werden.  Hinweis: Kommen Custom Commands ^[308] zum Einsatz, so werden diese in der Reihenfolge Custom commands for user creation ^[308], Custom Commands for outgoing e-mails BEFORE encryption ^[308] abgearbeitet.
 Processing of outgoing mails that are not from a managed domain (based on FROM-Header)	 Hinweis: Hierbei handelt es sich in der Regel um Kalendereinträge, welche von externen Kommunikationspartnern empfangen und vom internen Postfach an einen anderen externen Kommunikationspartner weitergeleitet werden. Nachdem Outlook/Exchange mit verschlüsselten Kalendereinträgen nicht umgehen kann, sollten Kalendereinträge generell nicht verschlüsselt werden. Dies impliziert jedoch auch, dass in Kalendereinträgen keine vertraulichen Daten übermittelt werden sollten.
 Process normally	Standardeinstellung. Mit dieser Option wird kein Unterschied zwischen ausgehenden E-Mails von Fremd- oder Managed domains ^[247] (siehe Mail System ^[247] Managed domain ^[247]) gemacht. Das heißt, sollte eine E-Mail im FROM-Header eine Adresse enthalten, welche nicht von einer Managed domain ^[247] stammt, so werden - sofern eine Option zur automatischen Benutzeranlage (siehe oben) gewählt ist - gegebenenfalls auch für Absender fremder Adressen User generiert.  Hinweis: Diese Einstellung kann unter Umständen sinnvoll sein, um eine Firmenrichtlinie strikt durchzusetzen. So werden dann auch E-Mails, welche zum Beispiel durch eine automatische Weiterleitungsregel gesendet werden und deshalb den ursprünglichen (Fremd-)Absender im FROM-Header beinhalten, gegebenenfalls zwingend verschlüsselt.  Achtung: Folgende Punkte sind bei dieser Einstellung zu beachten: 1. Unter Umständen wird durch diese Einstellung versucht, ein Zertifikat der lokalen CA ^[328] beziehungsweise ein OpenPGP Schlüssel für den (Fremd-)User zu erstellen. Der Bezug von Zertifikaten für Fremd-User via MPKI ^[339] wird unterbunden. 2. Wird weiterhin mangels Schlüsselmaterials des Empfängers GINA als Verschlüsselungstechnologie verwendet, wird das Initialpasswort - unter Umständen sogar unverschlüsselt - nach außen an den (Fremd-)

Parameter	Beschreibung
	User gesendet. Dies bedeutet auch, dass - je nach Einstellung - beim Passwort-Rücksetzungsprozess gegebenenfalls auch der externe (Fremd-)User adressiert würde. 3. In mandantenfähigen Systemen kann der generierte Benutzer nicht automatisch einem Mandanten zugeordnet werden, da die (Fremd-)E-Mail Domäne nicht zugeordnet sein kann. Dies bedeutet auch, dass Log-Einträge solcher E-Mails nur durch Mitglieder der Gruppe (Groups^[413] admin^[413]) zu sehen sind, nicht jedoch vom Mandanten Admin (siehe Customers^[494] Customer Management^[496] Customer administrators^[496]).
 Immediately deliver unchanged	Durch diese Option werden E-Mails von Fremd-Absendern immer unverändert, also „plain“ (vergleiche auch General settings^[288] Do not touch mails with the following text in subject:) versendet. Achtung: Durch diese Einstellung werden unter Umständen ursprünglich verschlüsselte E-Mails im Anschluss im Klartext in das Internet gesendet! In mandantenfähigen Systemen kann der Log-Einträge solcher (Fremd-)E-Mails nicht automatisch einem Mandanten zugeordnet werden, da die (Fremd-)E-Mail Domäne nicht zugeordnet sein kann. Dies bedeutet, dass Log-Einträge solcher E-Mails nur durch Mitglieder der Gruppe (Groups^[413] admin^[413]) zu sehen sind, nicht jedoch vom Mandanten Admin (siehe Customers^[494] Customer Management^[496] Customer administrators^[496]). 
 Reject	Durch diese Option werden E-Mails von Fremd-Absendern immer abgewiesen.
 Key generation	
	 Hinweis: Beim automatischen Generieren eines neuen Users^[396] wird das eingestellte Schlüsselmateriel generiert. Dieses wird dann über den - im nachfolgenden Hinweis beschriebenen - Prozess aktuell gehalten.
	 Hinweis: Ein automatisches, nächtliches Versorgen aller Users^[396] (unabhängig von der User creation^[289] Einstellung) mit Schlüsselmateriel, beziehungsweise das vorzeitige Verlängern von in Kürze ablaufendem Schlüsselmateriel, kann jeweils für lokale S/MIME und OpenPGP Schlüssel in den CA^[328]-Einstellungen (Settings^[330]), beziehungsweise für externe Zertifikate gegebenenfalls in den jeweiligen MPKI^[339]-Einstellungen (Settings) vorgenommen werden (siehe Option Automatically create certificates for active users without certificates, beziehungsweise Automatically renew expiring certificates if validity days left less than). Dieses automatische Verlängern funktioniert unabhängig von den hier eingestellten Optionen.
	 Hinweis: Steht für einen User zur Laufzeit kein gültiges Schlüsselmateriel zur Verfügung (zum Beispiel, weil er manuell angelegt oder aufgrund längerer Abwesenheit über den automatischen nächtlichen Prozess nicht versorgt wurde), würde jeweils bei aktiver Einstellungen auch zur Laufzeit beim Versand einer E-Mail das entsprechende Schlüsselmateriel erzeugt werden. Da für diesen Prozess die Funktion der User creation^[289] verwendet wird, werden eventuell vorhandene Custom commands^[308] for user creation verarbeitet.

Parameter	Beschreibung
	Dabei wird die E-Mail zunächst temporär abgewiesen (420 An encryption key for your account will be available shortly). Mit dem nächsten Zustellungsversuch des abgebenden Systems, sollte dann das benötigte Schlüsselmateriale bereitstehen, sodass die E-Mail wie erwartet verarbeitet werden kann.
 ☐ Issue local OpenPGP keys for users	Diese Option ist im Standard inaktiv. Generiert automatisch ein OpenPGP Schlüsselpaar.
 ☐ Issue local S/MIME certificates for users	Diese Option ist im Standard inaktiv. Generiert automatisch ein S/MIME-Schlüsselpaar. Der öffentliche Schlüssel wird von der lokalen CA  signiert (Self-Signed-Certificate).
 ☐ Issue   S/MIME certificates for users	Diese Option ist im Standard inaktiv. Generiert automatisch ein S/MIME-Schlüsselpaar. Der öffentliche Schlüssel wird von der unter  eingestellten CA signiert.  Hinweis: Diese Option erscheint nur dann, wenn unter  auch eine CA ausgewählt wurde.
 Encryption	
 Achtung: Bei S/MIME verschlüsselten E-Mails sind als „Content-Type“ des Headers jeweils zwei Ausdrücke möglich, nämlich „application/x-pkcs7-mime“ Dieser Ausdruck fand bereits vor Entstehen des Standards weite Verbreitung und ist deshalb weiterhin üblich (siehe auch RFC2311). „application/pkcs7-mime“ Dieser Ausdruck entspricht RFC5751 und ist ebenso üblich. Die SEPPmail Appliance verarbeitet bei eingehenden E-Mails beide Ausdrücke gleichermaßen. Bei ausgehenden E-Mails wird die Variante a. verwendet. Bei empfangenden Drittsystemen ist darauf zu achten, dass diese ebenfalls beide Varianten gleichermaßen verarbeiten, auch um Inkompatibilitäten von anderer Seite zu vermeiden.	
 Incoming e-mails	
 ☒ Add this text to message subject after decryption	Im Standard ist diese Option aktiv und hat das Schlüsselwort <code>\[secure\]</code> hinterlegt. Eingehende, durch die SEPPmail Appliance entschlüsselte E-Mails werden im Betreff mit dem hinterlegten Schlüsselwort gekennzeichnet.

Parameter	Beschreibung
 Set confidential flag after decryption:	Diese Option ist im Standard inaktiv. Bei eingehenden, durch die SEPPmail Appliance entschlüsselten E-Mails wird der Header „Sensitivity“ mit dem Wert „Company-Confidential“ gesetzt.
 Reject mails if S/MIME decryption fails	Im Standard ist diese Option aktiv. Eingehende, verschlüsselte E-Mails werden abgewiesen (bounced), sofern sie durch die SEPPmail Appliance nicht entschlüsselt werden konnten. Hinweis: Da die SEPPmail Appliance eine E-Mail einem eventuell vorgelagerten System erst dann als angenommen meldet, wenn die E-Mail ausgeliefert werden kann, ist diese Funktion auch zum Beispiel nach einem externen SPAM-Filter problemlos verfügbar. Hinweis: Durch Aktivieren dieser Aktion wird auch eine eventuell teilweise Ende-zu-Ende Verschlüsselung (zum Beispiel mittels Smart-Card) unterbunden.
 Outgoing e-mails	
	 Hinweis: Werden ausgehend bereits S/MIME verschlüsselte E-Mail an die SEPPmail Appliance gesendet, so werden diese unbehandelt weitergeleitet, da bei S/MIME kein doppeltes verschlüsseln möglich ist.
 Always encrypt mails with the following text in subject:	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[confidential\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird diese verschlüsselt. Hinweis: Wird an dieser Stelle das Schlüsselwort aus Incoming e-mails Add this text to message subject after decryption verwendet, beziehungsweise zusätzlich hinzugefügt - also \[confidential\]\[secure\] - so würden alle Antworten auf ursprünglich verschlüsselt empfangene E-Mails zwangsweise verschlüsselt. Da somit das Verschlüsseln von Antworten auch auf ursprünglich domänenverschlüsselte E-Mails angefordert wird, ist hier Vorsicht im Zusammenhang mit dem automatischen Generieren von Benutzern (siehe UserCreation²⁸⁹) Create accounts for new users if user tries to sign / encrypt²⁸⁹) geboten! Achtung: Das, beziehungsweise die hier verwendeten Schlüsselwörter müssen sich von denen für die Signatur (siehe Signing Outgoing e-mails „S/MIME sign outgoing mails with the following text in subject:“) unterscheiden.

Parameter	Beschreibung
 Always encrypt mails with Outlook "confidential" flag set	Im Standard ist diese Option aktiv. Wird in einer ausgehenden E-Mail der Header „Sensitivity“ mit dem Wert „Company-Confidential“ gefunden, so wird die E-Mail verschlüsselt.
 Always use GINA technology for mails with the following text in subject:	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[priv\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird das Verschlüsseln mittels GINA-Technologie ^[32] erzwungen.  Hinweis: Wird im E-Mail Client zusätzlich zum Erzwingen der GINA-Technologie eine Lesebestätigung (Disposition-Notification-To Header) angefordert, so wird über diese Technologie eine verlässliche Lesebestätigung angefordert. Das heißt der Empfänger kann das Auslösen dieser Lesebestätigung - anders als zum Beispiel in MS-Outlook - nicht unterdrücken (entspricht einem Einschreiben mit Rückschein).
 Always use GINA technology for mails with Outlook "private" flag set	Diese Option ist im Standard inaktiv. Wird in einer ausgehenden E-Mail der Header „Sensitivity“ mit dem Wert „Private“ gefunden, so wird das Verschlüsseln mittels GINA-Technologie ^[32] erzwungen.  Hinweis: Diese Option kann zu Problemen führen, wenn als privat markierte Kalendereinträge versendet werden, da diese dann automatisch GINA-verschlüsselt würden.
 Create GINA users with empty password if the following text is in the subject:	Diese Option ist im Standard inaktiv und hat das Schlüsselwort \[emptypw\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird bei initialem Verwenden der GINA-Technologie kein Initial-Password benötigt. Dadurch wird im Einzelfall die GINA-Variante 2a (siehe Unterschiedliche Registrierungsarten ^[41]) aktiviert.
 Always use S/MIME or OpenPGP if user keys are available	Im Standard ist diese Option aktiv. Ausgehende E-Mails werden immer verschlüsselt, sofern der SEPPmail Appliance ein öffentlicher Schlüssel - egal ob S/MIME (siehe X.509 Certificates ^[47]) oder OpenPGP (siehe OpenPGP Public Keys ^[46]) - des Kommunikationspartners (Empfängers) vorliegt.  Hinweis: Bei aktiver Option gilt zu beachten, dass der Versender der E-Mail auf der SEPPmail Appliance jeweils als Benutzer angelegt sein oder werden muss, wenn er an einen entsprechenden Kommunikationspartner sendet. Die hieraus entstehende Wechselwirkung bei eingestelltem, automatischen Generieren von Benutzern (siehe UserCreation ^[28]) Create accounts

Parameter	Beschreibung
	for new users if user tries to sign / encrypt^[289] ist zu beachten!
 ☐ Exclude calendar entries and RTF mails (winmail.dat)	Diese Option ist im Standard inaktiv. Kalendereinträge sowie RTF formatierte E-Mails werden vom automatischen Verschlüsseln der übergeordneten Option ausgenommen.  Hinweis: Outlook / Exchange mit lokaler Verschlüsselung kann nicht mit verschlüsselten Kalendereinträgen umgehen. Somit handelt es sich hierbei um eine Kompatibilitätseinstellung für eben diese Systeme. Ist die zu verarbeitende E-Mail RTF-formatiert, so würde im entsprechenden Log-Eintrag (siehe Logs^[388]) die Meldung „Calendar entry could not be found, but detected RTF-formatted MIME parts“ erscheinen.
 ☐ Always use GINA encryption if account exists and no S/MIME or OpenPGP key is known	Diese Option ist im Standard inaktiv. Ausgehende E-Mails werden immer mittels GINA-Technologie verschlüsselt, sofern der SEPPmail Appliance kein öffentlicher Schlüssel - weder S/MIME noch OpenPGP - bekannt ist, jedoch ein GINA Account^[462] für den Kommunikationspartner (Empfänger) vorliegt.
 ☐ Do not encrypt outgoing mails with the following text in subject:	Diese Option ist im Standard inaktiv und hat das Schlüsselwort \[noenc\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird ein eventuelles Verschlüsseln in jedem Fall unterdrückt. Andere kryptographische Aktionen (Signieren) sind davon nicht betroffen.
 ☐ Consider internally routed mails as encrypted	Diese Option ist im Standard inaktiv. E-Mails, welche von einer Managed domains^[247] zu einer Anderen gesendet werden, werden als „sicher“ markiert (siehe auch Incoming e-mails Add this text to message subject after decryption).  Hinweis: Dies ist insbesondere auf mandantenfähigen Systemen von Interesse, da das Standardverhalten bei der Kommunikation zwischen den Mandanten - und somit Managed domains^[247] - systembedingt anders ist, als bei der Kommunikation von und zu externen Kommunikationspartnern. Wird beispielsweise eine E-Mail vom Absender eines Mandanten an einen anderen Mandanten auf der gleichen SEPPmail Appliance als zu verschlüsselnd markiert, so ergäbe es keinen Sinn diese zu verschlüsseln und anschließend sofort wieder zu entschlüsseln. Nachdem jeder Mandant über einen sicheren Kanal (TLS) an die Appliance angebunden ist, spricht in der Regel nichts dagegen, E-Mails zwischen Mandanten generell als sicher zu markieren, da das Verfahren der Domänenverschlüsselung^[31] ähnelt.

Parameter	Beschreibung
	 Achtung: Vor dem Aktivieren dieser Option ist unbedingt sicher zu stellen – gegebenenfalls zusätzlich durch vorgeschaltete Schutzinstanzen –, dass weder aus dem Internet, noch von Managed domains [247] anderer, auf der SEPPmail Appliance verwalteten Mandanten, E-Mails mit gefälschtem Absender auf die SEPPmail Appliance gelangen (siehe gegebenenfalls auch Mail System [247] Managed domains [247] ADD/EDIT MANAGED DOMAIN [266] Settings [266] Allowed outgoing sending servers).
 ☐ Consider "forced TLS" as encrypted	Diese Option ist im Standard inaktiv. TLS Verschlüsselung wird für Zieldomänen, welche unter Mail System [247] TLS settings [257] mit einer höheren Sicherheitseinstellung als „may“ eingetragen wurden, als gültige E-Mail Verschlüsselungsoption anerkannt. Somit ändert sich bei diesen Zieldomänen die Verschlüsselungshierarchie [66] wie folgt (siehe Punkt 5.): 1. Geprüftes S/MIME Zertifikat des Empfängers 2. Geprüfter öffentlicher OpenPGP Schlüssel des Empfängers 3. Geprüftes S/MIME Domänen Zertifikat der Empfänger Domäne 4. Geprüfte öffentlicher OpenPGP Domänen Schlüssel der Empfänger Domäne 5. TLS-Verschlüsselung höher „may“ - wobei diese auch zusätzlich verwendet wird, wenn bereits eines der höher priorisierten Verfahren zum Einsatz kam. Sollte keines der vorangegangenen (Standard-)Verfahren verfügbar sein 6. GINA mit hinterlegtem Empfängerpasswort 7. GINA mit Initialpasswort  Achtung: Das Aktivieren dieser Option setzt voraus, das die SEPPmail Appliance den Übergang zum Internet bildet, also die Ziel-E-Mail Domänen direkt adressiert. Weiterhin ist zu Beachten, dass TLS eine Leitungsver Schlüsselung und keine Inhaltsverschlüsselung darstellt.
 ☐ Prefer RSA-OAEP for S/MIME encryption	Diese Option ist im Standard inaktiv. Verwenden von OAEP global als Padding-Verfahren für das Verschlüsseln via S/MIME (siehe gegebenenfalls auch https://de.wikipedia.org/wiki/PAdd-Ing_(Informatik) und https://de.wikipedia.org/wiki/Optimal_Asymmetric_Encryption_PAdd-Ing). OAEP funktioniert abwärtskompatibel.
 ☐ Use default cipher for S/MIME encryption: 	Diese Option ist im Standard inaktiv. Bei Aktivieren kann über dieses Auswahl-Menü der Algorithmus des bei S/MIME Verschlüsselung verwendeten Session-Keys gewählt werden. Bleibt diese Einstellung deaktiviert, so wird Triple-DES verwendet.  Hinweis: Für OpenPGP wird automatisch die maximal mögliche Schlüssellänge aus dem öffentlichen Schlüssel des Kommunikationspartners ermittelt und verwendet.
 Triple DES	Niedrigster Sicherheitsstandard aber höchste Kompatibilität (zum Beispiel auch zu Outlook 2003 und früher, Secure-E-Mail-Gateway Herstellern, welche nur diesen Cipher bei Domänenverschlüsselung [37] unterstützen oder vom Empfänger eingesetzte Hardware (zum Beispiel Kartenleser)).
 AES-	Wird zum Teil noch gefordert (zum Beispiel EDIFACT)

Parameter	Beschreibung
128	
 AES-192	Wird zum Teil noch gefordert (zum Beispiel EDIFACT)
 AES-256	Standardeinstellung. Aktueller Sicherheitsstandard. Sollte von allen gängigen E-Mail Clients in deren jeweils aktuellen Version unterstützt werden.
 OpenPGP method for recipient encryption ☒	Gibt die Methode für die OpenPGP Verschlüsselung auf Basis personenbezogener Schlüssel (siehe auch OpenPGP Public Keys ^[467] Local OpenPGP Keys ^[467] an.  Hinweis: Für das Entschlüsseln - also für eingehende E-Mails - unterstützt die SEPPmail Appliance generell beide OpenPGP Verschlüsselungsvarianten (Inline und MIME).
 Inline PGP	Bei Inline PGP wird jeder Anhang einer E-Mail - wobei auch der Mail-Body ein Anhang ist - separat verschlüsselt. <u>Vorteil:</u> Inline PGP wird von den meisten Open Source Produkten unterstützt und erhöht somit die Kompatibilität bei den Kommunikationspartnern. <u>Nachteil:</u> Formatierungsprobleme, zum Beispiel werden bei Inline-Tabellen zwar die Inhalte der Tabelle angezeigt, jedoch nicht die Tabelle selbst.  Achtung: Aufgrund eventuell einhergehender Sicherheitsprobleme (Stichwort: EFAIL) sollte das Inline-Verfahren nicht mehr benutzt werden.
 PGP/MIME	Standardeinstellung. Bei PGP/MIME wird die gesamte E-Mail verschlüsselt (wie auch bei S/MIME). <u>Vorteil:</u> Keine Formatierungsprobleme. <u>Nachteil:</u> Eventuell Kompatibilitätsprobleme und somit Nichtlesbarkeit der E-Mail beim Kommunikationspartner
 OpenPGP method for domain encryption ☒	Gibt die Methode für die OpenPGP Verschlüsselung auf Basis von Domänen Schlüsseln (siehe auch OpenPGP domain keys ^[492] Manual OpenPGP Domain Keys ^[492] an.  Hinweis: Für das Entschlüsseln - also für eingehende E-Mails - unterstützt die SEPPmail Appliance generell beide OpenPGP Verschlüsselungsvarianten (Inline und MIME).

Parameter		Beschreibung
	 Inline PGP	siehe OpenPGP method for recipient encryption ^[297] , Inline PGP ^[297]
	 PGP/MIME	siehe OpenPGP method for recipient encryption ^[297] , PGP/MIME ^[297]
 Signing		
  Achtung: Bei S/MIME signierten E-Mails sind als „Content-Type“ des Headers jeweils zwei Ausdrücke möglich, nämlich a. „application/x-pkcs7-signature“ Dieser Ausdruck fand bereits vor Entstehen des Standards weite Verbreitung und ist deshalb weiterhin üblich (siehe auch RFC2311). b. „application/pkcs7-signature“ Dieser Ausdruck entspricht RFC5751 und ist ebenso üblich. Die SEPPmail Appliance verarbeitet bei eingehenden E-Mails beide Ausdrücke gleichermaßen. Bei ausgehenden E-Mails wird die Variante a. verwendet. Bei empfangenden Drittsystemen ist darauf zu achten, dass diese ebenfalls beide Varianten gleichermaßen verarbeiten, auch um Inkompatibilitäten von anderer Seite zu vermeiden.		
  Hinweis: Bei der S/MIME Signatur wird eine Prüfsumme über den E-Mail body sowie die MIME Header gebildet. Das heißt, sofern Änderungen an diesen Teilen der E-Mail vorgenommen werden, wird das Zielsystem die Signatur als ungültig einstufen. Ausgenommen von der Prüfsumme sind hingegen die E-Mail Header, wie zum Beispiel from, sender, reply-to, to, cc, subject sowie beliebige X-Header.		
 Incoming e-mails		
  Hinweis: Die in den S/MIME Signaturen enthaltenen Zertifikate werden eingesammelt und unter X.509 Certificates^[471] für das Verschlüsseln ausgehender E-Mails bereitgestellt, sofern diese a) als gültig eingestuft wurden. Das heißt sie ■ stammen von einer als vertrauenswürdig eingestuften CA (siehe X.509 Root Certificates^[480]) ■ haben das Ablaufdatum noch nicht überschritten ■ wurden nicht für ungültig erklärt (siehe System^[224] OCSP / CRL check settings^[224]) ■ verwenden keinen ungültigen Signatur Algorithmus (siehe auch X.509 Certificates^[471] Advanced Settings^[485] Policies^[479] Refuse import of certificates with a signature algorithm using sha1 or lower^[479]) b) die X.509 Zertifikatserweiterung „Schlüsselverwendung (Key Usage)“ mit dem Wert „Schlüsselverschlüsselung: (key encipherment)“ aufweisen.		
  Add this text to message subject if S/MIME signatur		Im Standard ist diese Option aktiv und hat das Schlüsselwort \[signed\sOK\] hinterlegt. Eingehende, S/MIME signierte E-Mails, deren Signaturen durch die SEPPmail Appliance geprüft und als in Ordnung befunden wurden, werden mit dem angegebenen Schlüsselwort im Betreff gekennzeichnet.

Parameter	Beschreibung
☒ e check succeeds:	Hinweis: Damit eine S/MIME E-Mail Signatur als „gültig“ befunden wird, a) darf diese E-Mail auf dem Weg vom Absender bis zum Empfang und Prüfung durch die SEPPmail Appliance nicht verändert worden sein. b) muss das Signatur-Zertifikat des Absenders gültig sein, c) muss für das Verifizieren des Absenders die E-Mail Adresse des FROM-, beziehungsweise SENDER-Headers mit dem Antragsteller des Zertifikats übereinstimmen. Hinweis: Die SEPPmail Appliance erkennt sowohl Klartext- als auch Opaque-Signaturen und kann diese verifizieren. Da E-Mail-Clients jedoch häufig beim Erkennen von Opaque-Signaturen Probleme haben, empfiehlt sich bei häufigem Empfang von E-mails, welche mit diesem Verfahren signiert wurden, die Signaturen nach erfolgreichem Prüfen zu entfernen (siehe „Remove signature if S/MIME signature check succeeds“).
☐ Remove signature if S/MIME signature check succeeds	Diese Option ist im Standard inaktiv. Entfernt die S/MIME E-Mail Signatur nach erfolgreicher Prüfung. Achtung: Verwendet der Kommunikationspartner beim Signieren RSA-PSS (siehe auch Option Prefer RSA-PSS for S/MIME signatures bei Outgoing e-mails), so wird ein nachfolgender E-Mail Client eine zerstörte Signatur anzeigen, sofern er nicht damit umgehen kann. Um dies zu vermeiden, empfiehlt es sich, die Signatur nach erfolgreichem Prüfen abzuschneiden. Hinweis: Das Entfernen der E-Mail Signatur kann beim Einsatz mobiler Endgeräte - zum Beispiel via Microsoft ActiveSync - als E-Mail Clients von Vorteil sein, da diese häufig nicht mit diesen Signaturen umgehen können.
☒ Add this text to message subject if S/MIME signature fails:	Im Standard ist diese Option aktiv und hat das Schlüsselwort <code>\[signed\sINVALID\]</code> hinterlegt. Eingehende, signierte E-Mails, deren Signaturen durch die SEPPmail Appliance geprüft und als ungültig befunden wurden, werden mit dem angegebenen Schlüsselwort im Betreff gekennzeichnet. Zusätzlich wird unter Logs <code>[388]</code> Mail log <code>[389]</code> ein entsprechender OpenSSL-Fehler ausgegeben.
☐ Remove signature if S/MIME signature check fails	Diese Option ist im Standard inaktiv. Entfernt die S/MIME E-Mail Signatur nach fehlgeschlagener Prüfung. Hinweis: Bei aktiver Option ist keine weitere Prüfung der Signatur auf dem E-Mail Client, also auch durch den Benutzer, möglich. Somit kann dieser nicht selbstständig feststellen, weshalb eine Signatur als ungültig eingestuft wurde.
☐ Add this text to message subject if	Diese Option ist im Standard inaktiv und hat das Schlüsselwort <code>\[signed\sok\]</code> hinterlegt. Eingehende, OpenPGP MIME signierte E-Mails, deren Signaturen durch die SEPPmail Appliance geprüft und als gültig befunden wurden, werden mit dem angegebenen Schlüsselwort im Betreff gekennzeichnet.

Parameter	Beschreibung
OpenPGP signature succeeds:	 Hinweis: Aufgrund der fehlenden hierarchischen Struktur von OpenPGP kann die Authentizität des Absenders nicht zuverlässig geprüft werden. Somit eignet sich die OpenPGP Signatur ausschließlich für das Sicherstellen der Integrität einer E-Mail und hat deshalb auch rechtlich keinerlei Aussagekraft. Weiterhin muss für das erfolgreiche Prüfen einer OpenPGP Signatur der öffentliche Schlüssel des Absenders auf der SEPPmail Appliance bekannt sein (siehe OpenPGP Public Keys^[467]).
 ☐ Add this text to message subject if OpenPGP signature fails:	Diese Option ist im Standard inaktiv und hat das Schlüsselwort \[signed\INVALID\ hinterlegt. Eingehende, OpenPGP signierte E-Mails, deren Signaturen durch die SEPPmail Appliance geprüft und als ungültig befunden wurden, werden mit dem angegebenen Schlüsselwort im Betreff gekennzeichnet.
 ☐ Support triple wrapping (neu in 12.1)	Diese Option ist im Standard inaktiv. Aktiviert die „Triple Wrapping“ Unterstützung (siehe RFC2634). Hinweis: Diese Technologie wird zum Beispiel per Standard bei S/MIME behandelten E-Mails aus den Google Plattformen verwendet. Damit S/MIME behandelte E-Mails von Absendern mit Google E-Mail Adressen gelesen werden können, muss diese Option aktiv sein. Hinweis: Bei „triple wrapped“ E-Mails (optional S/MIME signiert - S/MIME-verschlüsselt - S/MIME signiert) wird die äußere Signatur nach dem Prüfen stets entfernt. War das Prüfergebnis der äußeren Signatur negativ, so wird die E-Mail generell als „ungültig signiert“ gekennzeichnet. Beinhaltet die verschlüsselte E-Mail wieder eine Signatur, so wird die E-Mail nur dann als „gültig signiert“ gekennzeichnet, wenn sowohl die äußere, als auch die innere Signatur gültig ist.
 Outgoing e-mails	
	 Hinweis: Sofern die Zertifikatskette nicht bereits in den Zertifikaten, welche für das Signieren verwendet werden vorhanden ist, wird diese während des Signierens durch die Appliance ergänzt. Dies setzt voraus, dass der Appliance die komplette eigene Zertifikatskette - inklusive der Zwischenzertifikate - bekannt, also unter X.509 Root Certificates^[480] als vertrauenswürdig eingestuft ist.
	 Hinweis: Für das Anziehen des privaten Signaturschlüssels wird in der Regel der Sender aus dem FROM-Header der E-Mail herangezogen (siehe gegebenenfalls auch authenticated()^[537]). Dadurch funktioniert zum Beispiel auch die Vertreterregelungen „Senden im Auftrag von“ in Microsoft Outlook mit anderen E-Mail Clients beim Empfänger, ohne dass ein Eingriff via Custom commands^[308] notwendig wäre (siehe auch Signatur: Verwendeter Schlüssel bei Microsoft Vertreterregelung^[827]). Ist der Sender des FROM-Headers nicht intern - also keiner Managed domain^[247] zuzuordnen - so wird auf das Vorhandensein des SENDER-Headers geprüft. Ist dieser

Parameter	Beschreibung
	vorhanden und der darin enthaltene Sender intern, so wird dieser für das Anziehen des Signaturschlüssels verwendet. Dadurch werden Probleme beim Weiterleiten von Kalendereinladungen vermieden.  Hinweis: Für das Signieren wird jeweils der Schlüssel / das Zertifikat des Absenders mit der längsten Gültigkeit herangezogen. Generell gilt jedoch, per MPKI ausgestellte Zertifikate werden bevorzugt für das Signieren verwendet („Bonus“ von 10 Jahren). Damit wird verhindert, dass „Umsteiger“, welche zunächst Zertifikate einer selbst signierten Zertifizierungsstelle (diese stellt in der Standard-Einstellung Zertifikate mit einer Laufzeit von zehn Jahren aus) im Einsatz hatten, weiterhin mit diesen Zertifikaten anstatt der über die MPKI bezogenen Trusted Zertifikate (diese werden in der Regel mit einer Laufzeit von nur einem Jahr ausgestellt) signieren.  Hinweis: Die SEPPmail Appliance signiert E-Mails ausschließlich mittels Klartext-Signatur. Dadurch wird - im Gegensatz zur Opaque-Signatur - gewährleistet, dass signierte E-Mails auch mit E-Mail-Clients gelesen werden können, welche kein S/MIME beherrschen (häufig mobile Endgeräte).
 ☒ S/MIME sign outgoing mails with the following text in subject:	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[sign\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird diese S/MIME signiert.  Achtung: Das, beziehungsweise die hier verwendeten Schlüsselwörter müssen sich von denen für die Verschlüsselung (siehe Encryption/Decryption Outgoing e-mails Always encrypt mails with the following text in subject:) unterscheiden.
 ☐ Sign all outgoing mails if S/MIME certificate available	Im Standard ist diese Option aktiv. Signiert alle ausgehenden E-Mails (keine Kalendereinträge sowie oder RTF formatierte Nachrichten!) von SEPPmail Appliance Benutzern (Users ³⁹⁶) mit gültigem S/MIME Zertifikat.  Hinweis: Da mit der S/MIME Signatur jeweils das Zertifikat des Absenders mitgesendet wird, wird dieses durch das Aktivieren dieser Option möglichst vielen Kommunikationspartnern zur Verfügung gestellt. Dadurch werden diese wiederum in die Lage versetzt S/MIME verschlüsselt mit dem Absender zu kommunizieren. Weiterhin wird hierdurch die Integrität und Authentizität jeder E-Mail automatisiert bestätigt.
 ☐ OpenPGP sign messages when encrypting with OpenPGP and sender has a secret key	Diese Option ist im Standard inaktiv. E-Mails, bei welchen aufgrund der Verschlüsselungshierarchie ⁶⁶ OpenPGP zum Einsatz kommt, werden automatisch OpenPGP signiert, sofern der Absender im Besitz eines gültigen OpenPGP Schlüsselpaares auf der Appliance ist.  Hinweis: Aufgrund der fehlenden hierarchischen Struktur von OpenPGP kann die Authentizität des Absenders nicht zuverlässig geprüft werden. Somit eignet sich die OpenPGP Signatur ausschließlich für das Sicherstellen der Integrität einer E-Mail und hat deshalb auch rechtlich keinerlei Aussagekraft. Weiterhin muss für das erfolgreiche Prüfen einer OpenPGP Signatur dem Empfänger der öffentliche Schlüssel des Absenders (siehe Users ³⁹⁸) bekannt sein.

Parameter	Beschreibung
 ☒ Do not S/MIME sign outgoing mails with the following text in subject:	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[nosign\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird das automatische S/MIME Signieren (siehe „Sign all outgoing mails if S/MIME certificate available“) in jedem Fall unterdrückt. Andere kryptographische Aktionen (Verschlüsseln) sind davon nicht betroffen.  Hinweis: Das Unterdrücken der E-Mail Signatur kann beim Einsatz mobiler Endgeräte durch den Empfänger von Vorteil sein, da mobile Endgeräte häufig nicht mit diesen Signaturen umgehen können.
 ☐ Use opaque signature	Diese Option ist im Standard inaktiv. In der Regel werden E-Mail Signaturen im Klartext angehängt. Somit kann eine signierte E-Mail, auch ohne Prüfen der Signatur und damit mit jedem x-beliebigen E-Mail Client, gelesen werden. Bei der Opaque Signatur wird der E-Mail Inhalt und die Signatur gemeinsam in einem MIME-Part gespeichert. Somit können Opaque signierte E-Mails ausschließlich mit S/MIME-fähigen E-Mail-Clients gelesen werden.
 ☐ Use triple wrapping (neu in 12.1)	Diese Option ist im Standard inaktiv. Aktiviert das „Triple Wrapping“ (siehe RFC2634) beim Senden von E-Mails.  Hinweis: Bei S/MIME behandelten E-Mails wird diese Technologie zum Beispiel auf den Google Plattformen vorausgesetzt. Wurde kein „Triple Wrapping“ verwendet, so werden S/MIME behandelte E-Mails unter Umständen mit zum Beispiel folgendem Fehler "554 5.7.5 To prevent known S/MIME vulnerabilities, Gmail does not accept S/MIME encrypted messages without an accompanying valid S/MIME signature." abgewiesen oder sind gegebenenfalls im Web-Mailer des Empfängers nicht lesbar. Unterstützt das System des Kommunikationspartners kein „Triple Wrapping“, so kann diese Einstellung unter Umständen zu Problemen führen. Gegebenenfalls ist im Einzelfall das Einrichten einer Encryption Policy ^[313] hilfreich.
 ☐ Use default digest for S/MIME signing: 	Diese Option ist im Standard inaktiv. Bei Aktivieren kann über dieses Auswahl-Menü der zu verwendende Hash-Algorithmus beim Signieren ausgewählt werden. Bleibt diese Einstellung deaktiviert, so wird SHA-256 verwendet.
 SHA-1	Niedrigster Sicherheitsstandard aber höchste Kompatibilität. Sollte nicht mehr verwendet werden, da dieses Verfahren als unsicher gilt.
 SHA-256	Standardeinstellung (empfohlen). Aktueller Sicherheitsstandard. Wird in der Regel von den aktuellen E-Mail Client-Produkten bei der Signaturprüfung unterstützt.
 SHA-512	Höchster Sicherheitsstandard. Dieser kann jedoch unter Umständen auf Empfängerseite zu Kompatibilitätsproblemen führen

Parameter	Beschreibung
 Prefer RSA-PSS for S/MIME signatures	Diese Option ist im Standard inaktiv. Verwenden von PSS global als Padding-Verfahren für das Signieren via S/MIME (siehe gegebenenfalls auch https://de.wikipedia.org/wiki/PAdd-Ing_(Informatik) und https://de.wikipedia.org/wiki/Probabilistic_Signature_Scheme). Hinweis: PSS für die Signatur eines Zertifikates benötigt ein entsprechendes Zertifikat des Ausstellers. Dies ist jedoch nicht relevant für die Signieren einer E-Mail unter Verwendung von PSS.  Wird PSS beim Empfänger nicht unterstützt - dies ist bislang bei allen E-Mail Clients der Fall (!) - so wird die Signatur als ungültig erklärt. Von einem flächendeckenden Einsatz von PSS für das Signieren wird deshalb abgeraten.
 Large files (nur mit entsprechender Large File Transfer (LFT) ^[107] Lizenz (siehe auch Home ^[220] Licenses ^[220] Large File Transfer ^[221] (LFT) licenses), sowie per GiNA Domains ^[416] aktiviertem Large File Transfer ^[439] funktionsfähig.	
 Always use large file processing for mails with the following text in subject:	Im Standard ist diese Option aktiv und hat das Schlüsselwort <code>\[lftm\]</code> hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird diese - unabhängig von der Größe - mittels Large File Transfer (LFT) ^[107] Technologie versendet. Dies impliziert eine gültige Large File Transfer (LFT) ^[128] Lizenz
 Do not use large file processing for mails with the following text in subject:	Diese Option ist im Standard inaktiv und hat das Schlüsselwort <code>\[nolftm\]</code> hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird das Verwenden der LFT ^[128] Technologie selbst dann unterdrückt, wenn der eingestellte Größenschwellwert (siehe CHANGE GiNA SETTINGS FOR ^[423] Large File Transfer ^[439] Outgoing policy ^[440] Size (in KiB) above which messages are treated as large files (set to 0 to treat all messages as large files) ^[440] überschritten wird.
 Protection Pack (nur mit entsprechender Protection Pack (PP) ^[106] Lizenz (siehe auch Home ^[220] Licenses ^[220] Protection Pack (AntiSpam / AntiVirus) ^[221]), sowie unter Mail System ^[247] Antispam ^[255] entsprechend aktivierter Funktionen funktionsfähig.	
 Check mails for viruses and send infected mails to (leave empty to reject infected mails):	Diese Option ist im Standard inaktiv. Aktiviert die Viren-Scan-Funktion. Infizierte E-Mails werden an die optional einzugebende E-Mail Adresse umgeleitet (Quarantäne). Bleibt das Eingabefeld für die E-Mail Adresse leer, so werden infizierte E-Mails abgewiesen (bounced). Achtung: Wird an dieser Stelle ein Postfach angegeben, so ist zu beachten, dass infizierte E-Mails unverschlüsselt an diese Adresse gesendet werden. Dementsprechend wird bei Angabe einer Adresse aus einer Managed Domain ^[247] Note: Infected emails are sent unencrypted to the quarantine. beziehungsweise bei Angabe einer externen E-Mail Adresse 

Parameter	Beschreibung
	Note: In case of an infection, you are sending an unencrypted email to an unmanaged domain! Hinweis:  Generell sollten infizierte E-Mails abgelehnt und nicht an eine E-Mail Adresse umgeleitet werden. Wird die E-Mail abgelehnt, so bleibt sie im Verantwortungsbereich des Absenders. Wird sie hingegen umgeleitet, gelangt sie in den Verantwortungsbereich des Empfängers. Dies kann bei zeitkritischen E-Mails, welche in der Quarantäne verbleiben, problematisch sein. Achtung:  Ist die Option Use ClamAV antivirus Engine (Note: remember to activate in ruleset)^[256] aus Mail System^[247] Antispam^[255] deaktiviert, so würden E-Mails als „Virus-frei“ weitergeleitet. Dateien, welche 1 GB überschreiten werden nicht gescannt um Timeouts zu vermeiden. Ein entsprechender Log Eintrag wird generiert.
 Exclude the following signatures from test (regular expression, e.g. "(Eicar-Test-Signature) (Heuristics\\.Encrypted\\.PDF)"):	Diese Option ist im Standard inaktiv. Für den Fall, dass ClamAV nach einem Signatur-Update sogenannte „false positive“ Meldungen erzeugt, können an dieser Stelle Ausnahmen vom Virenscan definiert werden. Dies können • heuristische Teil-Prüfungen sein (siehe gegebenenfalls www.clamav.net) • einzelne Viren Namen, wie sie dem Log zu entnehmen sind (als Regulärer Ausdruck, das heißt Sonderzeichen müssen als solche markiert werden (siehe Reguläre Ausdrücke^[51]), sein. Im Standard verwendet die Scan Engine die ClamAV Signaturen sowie weitere Signaturen von Sanesecurity (http://sanesecurity.com) (siehe Mail System^[247] AntiSpam^[255] Enable unofficial signatures for ClamAV^[257]).
 Send notification to this e-mail address if a virus was found:	Diese Option ist im Standard inaktiv. Versendet Benachrichtigungen über Viren-Funde an die angegebene E-Mail Adresse.
 Block windows executable files in mails	Diese Option ist im Standard inaktiv. E-Mails, welche ausführbare Windows Dateiformate enthalten werden abgelehnt (rejected). Hinweis:  Im engeren Sinne sind „Executables“ Binärdateien, die nativ ausgeführt werden können. Skript Dateiformate, für deren Ausführung auf dem Betriebssystem ein entsprechender Interpreter benötigt wird (wie etwa Java-Script) sind von dieser Option nicht berührt (siehe nächste Option!).
 Search inside unency	Im Standard ist diese Option aktiv. Bei aktiver Option wird auch in ZIP Archiven nach ausführbaren Windows Dateiformaten gesucht.

Parameter	Beschreibung
☐ pted zip archives	 Achtung: Durch die Suche innerhalb von ZIP Archiven kann das Prüfen mitunter sehr lange dauern und somit zu Timeouts führen.
☐ Block (most) script files in mails (e.g. .js files)	Diese Option ist im Standard inaktiv. E-Mails, welche übliche, ausführbare Skript Dateiformate enthalten werden abgelehnt (rejected).
☒ Search inside unencrypted zip archives	Im Standard ist diese Option aktiv. Bei aktiver Option wird auch in ZIP Archiven nach ausführbaren Skript Dateiformaten gesucht.  Achtung: Durch die Suche innerhalb von ZIP Archiven kann das Prüfen mitunter sehr lange dauern und somit zu Timeouts führen.
	 Hinweis: Die folgenden SPAM Prüfungen werden generell übersprungen, sofern die sendende IP-Adresse unter Mail System ^[247] Manual blacklisting / whitelisting ^[258] gelistet ist.
☐ Check incoming mails for spam and add the following text to the subject to identify spam:	Diese Option ist im Standard inaktiv und hat das Schlüsselwort [SPAM] hinterlegt. Als SPAM klassifizierte E-Mails werden mit dem angegebenen Text in der Betreffzeile versehen und an den Empfänger weitergeleitet. Basis der Klassifizierung ist der angegebene Tag level (siehe nächste Option).  Achtung: ist die Option Use antispam Engine (Note: remember to activate in ruleset) ^[258] aus Mail System ^[247] Antispam ^[255] deaktiviert, so würde keine Spam-Erkennung stattfinden. E-Mails, welche 5 MB überschreiten werden nicht geprüft um Timeouts zu vermeiden. Ein entsprechender Log Eintrag wird generiert.
 Tag level: ☐	Auswahl, des Schwellwertes für die SPAM-Erkennung. Je niedriger dieser Wert (0.5 bis 19.5) gesetzt wird, desto strenger sind die Kriterien für die SPAM-Erkennung. Im Standard ist der Wert „2“ gewählt. Bei niedrigen Werten erhöht sich das Risiko von Falscherkennungen, so dass gegebenenfalls auch legitime E-Mails als SPAM erkannt und markiert werden.
☐ Check incoming mails for spam and redirect spam to (leave	Diese Option ist im Standard inaktiv. Als SPAM klassifizierte E-Mails werden an die optional einzugebende E-Mail Adresse umgeleitet (Quarantäne). Bleibt das Eingabefeld für die E-Mail Adresse leer, so werden die klassifizierten E-Mails abgewiesen (bounced). Basis für die SPAM-Erkennung ist der angegebene Spam level (siehe nächste Option).

Parameter	Beschreibung
empty to reject spam):	Infizierte E-Mails werden an die optional einzugebende E-Mail Adresse gesendet (Quarantäne). Bleibt das Eingabefeld für die E-Mail Adresse leer, so werden infizierte E-Mails abgewiesen (bounced). Hinweis: Generell sollten SPAM E-Mails abgelehnt und nicht an eine E-Mail Adresse umgeleitet werden. Wird die E-Mail abgelehnt, so bleibt sie im Verantwortungsbereich des Absenders. Wird sie hingegen umgeleitet, gelangt sie in den Verantwortungsbereich des Empfängers. Dies kann bei zeitkritischen E-Mails, welche in der Quarantäne verbleiben, problematisch sein. Achtung: ist die Option Use antispam Engine (Note: remember to activate in ruleset) ^[256] aus Mail System ^[247] Antispam ^[255] deaktiviert, so würde keine Spam-Erkennung stattfinden. E-Mails, welche 5 MB überschreiten werden nicht geprüft um Timeouts zu vermeiden. Ein entsprechender Log Eintrag wird generiert.
 Spam level:	Auswahl, des Schwellwertes für die SPAM-Erkennung. Je niedriger dieser Wert (0.5 bis 19.5) gesetzt wird, desto strenger sind die Kriterien für die SPAM-Erkennung. Im Standard ist der Wert „4“ gewählt. Bei niedrigen Werten erhöht sich das Risiko von Falscherkennungen, so dass gegebenenfalls auch legitime E-Mails als SPAM erkannt und umgeleitet beziehungsweise abgelehnt (bounced) werden.
 Reject incoming mails with spoofed sender domain preventing processing of internal mails	Diese Option ist im Standard inaktiv. Stammt der Absender im Envelope oder FROM Header (oder SENDER Header, sofern vorhanden) einer eingehenden E-Mail aus einer Managed domain ^[247] wird die E-Mail abgewiesen. Achtung: Mit dieser Option wird sämtlicher interner E-Mail Verkehr, also von Managed domains ^[247] an Managed domains ^[247], unterbunden. Dies spielt im Normalfall keine Rolle, da interne E-Mails vom E-Mail Server direkt zugestellt werden und nicht bis zur SEPPmail Appliance gelangen. Insbesondere in MSP Umgebungen werden jedoch E-Mails von den Managed domains ^[247] eines Kunden an Managed domains ^[247] anderer Kunden gesendet, sodass diese Option hier keinesfalls aktiviert werden sollte.
 Reject mails if from header does not contain a valid e-mail address	Diese Option ist im Standard inaktiv. Enthält der FROM-Header (und SENDER Header, sofern vorhanden) einer E-Mail keine gültige E-Mail Adresse, so wird die E-Mail abgewiesen. Achtung: Dies kann dazu führen, dass System-E-Mails ebenfalls abgewiesen werden, da diese häufig ohne Absender gesendet werden.
 Header tagging Durch das „Header Tagging“ wird das Setzen eines erweiterten, sogenannten X-Headers und einen zugehörigen Wert für unterschiedliche Situationen (siehe folgende Optionen) durch die SEPPmail Appliance ermöglicht. Diese erweiterten Informationen können durch nachgelagerte Komponenten ausgewertet werden. Ein Beispiel für so eine zusätzliche, nachgelagerte, E-Mail verarbeitende Komponente könnte ein Data Loss Prevention (DLP) System sein.	

Parameter	Beschreibung
	 Hinweis: Die X-Header • X-SM-incoming • X-SM-outgoing • X-SM-internal • X-SM-encrypted • X-SM-decrypted werden per Standard immer gesetzt mit dem Wert „yes“ befüllt, wenn die entsprechende Situation eintritt, unabhängig von den folgenden, optionalen Einstellungen.
 ☐ Set header to value for all incoming and internal mails	Diese Option ist im Standard inaktiv. Setzt den angegebenen X-Header mit dem zugeordneten Wert für alle eingehenden und internen (siehe auch Set header to value for all internal mails) E-Mails.
 ☐ Set header to value for all outgoing mails	Diese Option ist im Standard inaktiv. Setzt den angegebenen X-Header mit dem zugeordneten Wert für alle ausgehenden E-Mails.
 ☐ Set header to value for all internal mails	Diese Option ist im Standard inaktiv. Setzt den angegebenen X-Header mit dem zugeordneten Wert für alle internen E-Mails, also von einer Managed domain an eine Managed domain .
 ☐ Set header to value For all mails that have been encrypted	Diese Option ist im Standard inaktiv. Setzt den angegebenen X-Header mit dem zugeordneten Wert für alle E-Mails, welche durch die SEPPmail Appliance verschlüsselt wurden.
 ☐ Set header to value For all	Diese Option ist im Standard inaktiv. Setzt den angegebenen X-Header mit dem zugeordneten Wert für alle E-Mails, welche durch die SEPPmail Appliance entschlüsselt wurden.

Parameter	Beschreibung
mails that have been decrypted	
 Archiving	
 ☐ Send a copy of ALL mails to the following address:	Diese Option ist im Standard inaktiv. Sendet eine 1:1 Kopie aller über die SEPPmail Appliance transportierten E-Mails - noch vor dem Ver-, beziehungsweise nach dem Entschlüsseln - an die angegebene E-Mail Adresse.
 Custom commands Über Custom Commands können, über den in den Regelwerk-Anweisungen  definierten Befehlssatz, spezifische Anforderungen an entsprechender Stelle im Ruleset eingefügt werden.	
  Hinweis: Beim Speichern von Custom Commands wird ein Syntax Check durchgeführt. Somit wird ein ungültiges Regelwerk nicht aktiviert.	
 ☐ Custom commands for incoming e-mails BEFORE decryption:	Diese Option ist im Standard inaktiv. Fügt den im Eingabefeld vorhandenen Code an der Stelle im Ruleset für eingehende E-Mails VOR dem Entschlüsseln ein.
 ☐ Custom commands for incoming e-mails AFTER decryption:	Diese Option ist im Standard inaktiv. Fügt den im Eingabefeld vorhandenen Code an der Stelle im Ruleset für eingehende E-Mails NACH dem Entschlüsseln ein.
 ☐ Custom commands for outgoing e-mails BEFORE encryption:	Diese Option ist im Standard inaktiv. Fügt den im Eingabefeld vorhandenen Code an der Stelle im Ruleset für ausgehende E-Mails VOR dem Verschlüsseln ein.
 ☐ Custom commands for e-mails from GINA:	Diese Option ist im Standard inaktiv. Fügt den im Eingabefeld vorhandenen Code an der Stelle im Ruleset für eingehende GINA-Mails ein.
 ☐ Custom commands	Diese Option ist im Standard inaktiv. Ersetzt den Code für das unter User creation  ausgewählte Standardverfahren für das Generieren neuer Benutzer. Ist die Option aktiv, so wird dieser Code bei Auswahl von

Parameter	Beschreibung
for user creation:	- Do not create accounts (also disables custom commands for user creation) ^[289] nie - Create accounts for new users if user tries to sign / encrypt ^[289] nur beim Versuch zu verschlüsseln/signieren - Create accounts for all users ^[290] immer durchlaufen. Achtung: Da diese Option das ausgewählte Standardverfahren für das Generieren neuer Benutzer ersetzt, würde bei aktivierter Option ohne eingegebenen Code niemals ein Benutzer angelegt! Aus diesem Grund ist das Eingabefeld dieser Option mit dem Standard-Code für das Generieren von neuen Benutzern vorbelegt. Sofern der hier eingetragene Code nicht angepasst wurde (also dem Standard entspricht), würde dieser bei Bedarf mit einem Firmware-Update ebenfalls aktualisiert. Um gegebenenfalls nach dem manuellen Anpassen den Standard-Code wieder zu erhalten, muss der Inhalt des Eingabefeldes gelöscht und das Ruleset mittels Save neu generiert werden. 
 Custom macros and commands for all e-mails BEFORE processing:	Diese Option ist im Standard inaktiv. An dieser Stelle können Makros ^[509] - also Code-Blöcke, welche einmalig definiert und im Anschluss beliebig oft in den Custom commands verwendet werden können - erstellt werden. Diese werden im Ruleset (siehe SMTP ruleset ^[286] Display ruleset) ganz oben platziert. Somit kann an dieser Stelle auch Code vor dem eigentlichen „Mail Processing“ platziert werden.
 Key server	Über Key Server wird das zusätzliche Abfragen öffentlicher Schlüssel von Kommunikationspartnern ermöglicht. Somit kann gegebenenfalls auch dann verschlüsselt werden, wenn auf der SEPPmail Appliance noch kein Schlüsselmaterial des Empfängers bekannt, jedoch auf dem eingetragenen Key Server vorhanden ist. Die Key Server Abfrage findet jeweils noch vor der Abfrage des eigenen Schlüsselspeichers (siehe X.509 Certificates ^[477], beziehungsweise OpenPGP Public Keys ^[467]) statt. Die Abfrage wird immer vom E-Mail verarbeitenden System ausgeführt. Sofern dies ein Frontend-Server ist, übergibt dieser das so bezogene Schlüsselmaterial zum Speichern an das Backend-System. Nach dem Speichern eines Key Server Eintrags wird jeweils ein weiteres Eingabefeld eingeblendet.  Hinweis: Öffentliche Key Server und sogenannte Schlüsselsammler beherbergen häufig „totes“ Schlüsselmaterial. Das heißt, für die über den Key Server bereitgestellten öffentlichen Schlüssel besitzen die Empfänger oft nicht mehr den privaten Schlüssel. Somit sind diese nicht in der Lage die verschlüsselten E-Mails zu lesen. Aus diesem Grund wird dringend von der Abfrage solcher Server abgeraten.
 Type ☒	Auswahl des abzufragenden Schlüsselmaterials. Die Suchfilter für eine Schlüsselserver-Abfrage sind für die Standard-Technologien S/MIME und OpenPGP genormt. Sollte dennoch ein anderer Suchfilter erforderlich sein, so besteht die Möglichkeit eine benutzerdefinierte Abfrage über Custom commands ^[308], mittels der Befehle <code>ldap_getpgpkeys()</code> ^[627], beziehungsweise <code>ldap_getcerts()</code> ^[628] zu erstellen.
 S/MIME	Standardeinstellung. Auswahl für S/MIME Schlüsselsuche. (Standardsuchfilter (mail=<E-Mail Adresse des Empfängers>))

Parameter	Beschreibung
	Hinweis: Wird auf dem Key Server ein neueres Zertifikat als im Zertifikatsspeicher (X.509 Certificates^[47]) gefunden, so wird dieses neuere Zertifikat im Zertifikatsspeicher abgelegt und somit für das Verschlüsseln verwendet. Zertifikate, welche über den Key Server bezogen werden, werden auch dann für das Verschlüsseln verwendet, wenn die ausstellende Stammzertifizierungsstelle unbekannt ist.
OpenPGP	Auswahl für OpenPGP Schlüsselsuche. (Standardsuchfilter (pgpUserID=<E-Mail Adresse des Empfängers>)) Hinweis: Wird bei der Abfrage eines öffentlichen OpenPGP Schlüssels ein Schlüssel gefunden, dessen Key ID identisch mit einem bereits vorhandenen Eintrag im Schlüsselspeicher (OpenPGP Public Keys^[46]) ist, so wird dieser Schlüssel auf der Appliance durch das Ergebnis der LDAP-Abfrage überschrieben.
Recipient mask (regex)	Regulärer Ausdruck, welcher die Ziel-E-Mail-Domänen für die Abfrage bestimmt. Soll die Abfrage beispielsweise für nur eine E-Mail-Domäne gelten, so könnte der Ausdruck wie folgt lauten: @mein-kommunikationspartner.tld\.
URI	Gibt den Pfad zum Schlüsselserver an. Beispiele hierfür wären ldap://mein-kommunikationspartner.tld\. ldaps://mein-kommunikationspartner.tld\. ldaps://mein-kommunikationspartner.tld\.:1636
Bind DN (optional)	Zur Abfrage berechtigter Benutzer, zum Beispiel cn=meinefirma,ou=keys,o=mein-kommunikationspartner.tld,c=de
Bind PW (optional)	Zum Benutzer zugehöriges Passwort Hinweis: Semikolons „;“ und Backslashes „\“ müssen jeweils mit einem Backslash als Sonderzeichen gekennzeichnet werden, also „\;“, beziehungsweise „\\“. Somit müsste beispielsweise das Passwort p4ss\w0rd; wie folgt eingegeben werden: p4ss\\w0rd\;
Base DN	LDAP-Suchpfad, in welchem die zu suchenden Schlüssel abliegen.
Ignore failure	Diese Option ist im Standard inaktiv. Verhindert das Ablehnen (bounce) der E-Mail im Falle der Nichterreichbarkeit des LDAP-Servers.
Advanced options	
Completely disable GINA technology	Diese Option ist im Standard inaktiv. Deaktiviert komplett die GINA-Technologie. Als Folge würden als „zu verschlüsselnd“ gekennzeichnete E-Mails abgewiesen werden, wenn keine andere Verschlüsselungsmethoden (S/MIME, OpenPGP, Domain) verfügbar sind.

	 Hinweis: Wird die GINA-Technologie über diese Option abgeschaltet, so ist darauf zu achten, dass alle Optionen aus „Encryption/Decryption“, welche diese Technologie ansteuern, deaktiviert sind. Ebenso darf kein Ansteuern dieser Technologie über Custom commands [308] erfolgen.
 ☐ Completely disable user-based S/MIME and OpenPGP	Diese Option ist im Standard inaktiv. Deaktiviert sowohl die benutzerbezogene S/MIME- als auch OpenPGP-Technologie. Diese Option wird verwendet, wenn ausschließlich Domänen- und/oder GINA-Verschlüsselung verwendet werden soll.  Hinweis: Wird diese Option gewählt, so ist darauf zu achten, dass alle Optionen aus „Encryption/Decryption“, welche diese Technologien ansteuern deaktiviert sind. Ebenso darf kein Ansteuern dieser Technologien über Custom commands [308] erfolgen.
 ☐ Use remote GINA server, reachable under the following e-mail address:	Diese Option ist im Standard inaktiv. Muss aus revisionstechnischen Gründen der GINA-Teil in einer anderen Demilitarisierten Zone (DMZ) als der SMTP verarbeitende Teil stehen, so ist über diese Option ein entsprechendes Auftrennen der Lösung möglich. Die einzelnen Funktionsteile können dabei sogar auf unterschiedliche Standorte verteilt werden. Alle GINA zu verschlüsselnden E-Mails werden dann über die hier angegebene Pseudo-E-Mail Adresse (zum Beispiel GINA@GINApseudodomain.local) S/MIME verschlüsselt per SMTP an den GINA-Satelliten geleitet.
 ☐ This is a remote GINA server	Diese Option ist im Standard inaktiv. Definiert den Gegenpart zur Option Use remote GINA server, reachable under the following e-mail address:, also den GINA-Satelliten. An der Satelliten Appliance muss die Pseudo-Mail-Domäne (im Beispiel oben „ginapseudodomain.local“) als zusätzliche Managed domain [247] eingetragen werden (siehe Mail System [247] Managed domains [247]). Ebenso müssen die Managed domains [247] des Basis-Systems erfasst werden. Die GINA-Konfiguration und deren Zuordnung zu den Managed domains [247] erfolgt auf dem Satelliten-System (siehe GINA Domains [416] Domains [416]).
 Relay for domain:	Hier sind die Managed domains [247] des Basis-Systems als Regulärer Ausdruck einzutragen (siehe Mail System [247] Managed domains [247]). Das Trennen der Domains erfolgt durch ein Pipe-Zeichen „ “, also domain1\.tld domain2\.tld domainn\.tld .  Hinweis: Theoretisch kann somit auch ein GINA-Satellit, für mehrere Appliances, welche unterschiedliche Managed domains [247] beherbergen, konfiguriert werden.
 Relay e-mail address:	Hier ist die gleiche Pseudo-E-Mail Adresse einzutragen wie auf dem „Basis“-System unter Use remote GINA server, reachable under the following e-mail address:.
 Relay domain key fingerprint:	Hier sind die Fingerprints der Domänen Zertifikate der unter „Relay for domain“ angegebenen Managed domains [247], jeweils durch ein Pipe-Zeichen „ “ getrennt als Regulärer Ausdruck, also fingerprint1 fingerprint2 fingerprintn, anzugeben. (siehe ADD/EDIT MANAGED DOMAIN [274] S/MIME domain encryption [274]).

 Use Incamail instead of local GINA interface	Diese Option ist im Standard inaktiv. Aktiviert den Schweizer Dienst Incamail anstelle der GINA Technologie.
 Use custom delivery method:	Im Standard ist diese Option leer. Ist ein Eintrag vorhanden, wird die Option rot dargestellt! Legt die Art und Weise des E-Mail Flusses fest. Beispielsweise kann die vor Version 11.1.11 verfügbare Option Re-inject mails to sending mailserver durch den Eintrag von „loop“ (siehe auch Konfig: Re-inject mails to sending mailserver ^[757]), beziehungsweise die Option Run in queueless mode durch den Eintrag von „queueless“ (siehe auch Konfig: Queueless Mode ^[754]) hervorgerufen werden. Weiterhin kann über diese Option quasi ein „Custom commands for outgoing e-mails AFTER encryption“ abgebildet werden (siehe auch Konfig: Custom commands for outgoing e-mails AFTER encryption ^[753]).

Die vorgenommenen Änderungen werden über die Schaltfläche **Save and create ruleset** gespeichert. Das Ruleset wird mit den vorgenommen Einstellungen generiert.

7.7.1 Encryption Policy

Dieses Sub-Menü wird aus **Mail Processing** ^[286] über **Edit policy table...** aufgerufen.

Spalte	Beschreibung
 Position	Über die Eingabe einer entsprechenden Zahl, kann die Reihenfolge der ENCRYPTION POLICIES beeinflusst werden.
 Name	Zeigt den individuellen, beim Erstellen selbst vergebenen Namen der Regel an. Durch Klicken auf den Namen öffnet das Sub-Menü EDIT ENCRYPTION POLICY ^[314] , über welches die Regel bearbeitet werden kann
 State	Zeigt, ob die Regel aktiv ist oder nicht (Status active / inactive)
 Domains	Zeigt die Managed domain ^[247] an, für welche diese Regel gültig ist.
 Flag	Zeigt gegebenenfalls das Trigger-Flag für die Policy an (siehe ADD/EDIT ENCRYPTION POLICY ^[314] Policy flag).
 Encryption	Zeigt ob und wenn die Art der Verschlüsselung an, mit welcher an die Zieldomäne(n) dieser Regel verschlüsselt werden soll.
 Signing	Zeigt ob und wenn mit welchem hash-Verfahren die S/MIME Signatur erstellt wird.
 Bounce	Zeigt das für diese Policy verwendete Bounce Template an (siehe ADD/EDIT ENCRYPTION POLICY ^[314] Bounce behaviour).
 GINA domain	Zeigt die für diese Policy verwendete GINA Domain ^[416] an (siehe ADD/EDIT ENCRYPTION POLICY ^[314] GINA options ^[317]).

Mit **Create new encryption policy...** wird das Submenü **ADD ENCRYPTION POLICY** ^[314] geöffnet, über welches eine neue Regel erstellt werden kann.

In mandantenfähigen Systemen erscheint pro Mandant ein entsprechend benannter Abschnitt mit dem oben genannten Inhalt.



Achtung:

Encryption Policies sind generell höherwertig als die Einstellungen des globalen Rulesets (siehe **Mail Processing** ^[286] **Ruleset generator** ^[287]). Ausnahmen bilden die Custom commands ^[308], welche noch vor den Encryption Policies verarbeitet werden.

Wurde eine der Regeln aufgrund der konfigurierten Auslöser aktiv, so wird **keine** weitere Regel verarbeitet.

7.7.1.1 Add/Edit Encryption Policy

Dieses Sub-Menü wird aus dem Sub-Menü **ENCRYPTION POLICY** ^[313] aufgerufen.

Sektion **Settings**

Parameter	Beschreibung
 State	
 ☐ Inactive	Diese Option ist im Standard inaktiv. Durch Aktivieren der Option bleibt die Regel inaktiv. Somit kann zum Beispiel eine Regel für das spätere Verwenden vorbereitet werden.
 Polycyname	Individueller Name der Regel, welcher beim Erstellen vergeben wird.
 Policy Domains 	Hier werden die für die Regel verfügbaren Managed domains ^[247] aufgelistet, welche als Quelle ausgewählt werden können. Mehrfachmarkierungen sind durch Klicken mit gedrückter „STRG“ Taste möglich. Verfügbar sind generell nur Managed domains ^[247] , welche noch keiner Regel zugeordnet sind. In mandantenfähigen Systemen sind zudem nur die Managed domains ^[247] sichtbar, welche auch dem Mandanten zugeordnet sind, aus welchem dieses Menü aufgerufen wurde.
 Policy flag	Wird mittels Custom commands ^[308] ein flag() ^[553] - zum Beispiel durch eine LDAP-Abfrage mittels ldap_compare() ^[620] - gesetzt, so kann dieses hier zusätzlich als einschränkendes Kriterium für das Auslösen dieser Policy verwendet werden.
 Encryption mode 	Im Auswahlménü dieser Option wird die gewünschte Art der Verschlüsselung angegeben:
 Do not encrypt	Unterdrückt das Verschlüsseln (vergleiche Mail Processing ^[286] Ruleset Generator ^[287] General settings ^[288] Do not touch mails with the following text in subject: ^[288]).
 S/MIME-only	Erzwingt die benutzerbezogene S/MIME Verschlüsselung ^[287] .
 OpenPGP-only	Erzwingt die benutzerbezogene OpenPGP Verschlüsselung ^[307] .
 GINA-only	Erzwingt die GINA Verschlüsselung ^[327] (vergleiche Mail Processing ^[286] Ruleset Generator ^[287] Encryption ^[292] Outgoing e-mails ^[293] Always use GINA technology for mails with the following text in subject: ^[294]).
 Incmail	Verwendet Incmail (siehe auch Mail Processing ^[286] Ruleset Generator ^[287] Advanced options ^[310] Use Incmail instead of local GINA interface ^[312]) anstatt GINA, sofern kein höherwertiges Verfahren (siehe Verschlüsselungshierarchie ^[667]) zur Verfügung steht.
 Any	Standardeinstellung. Erzwingt das Verschlüsseln gemäß Verschlüsselungshierarchie ^[667] (vergleiche Mail Processing ^[286] Ruleset Generator ^[287] Encryption ^[292] Outgoing e-mails ^[293] Always encrypt mails with the following text in subject: ^[293]).

Parameter	Beschreibung
 S/MIME options	Ermöglicht das Einstellen der zu verwendenden Verschlüsselungsalgorithmen und Signatur Hash-Verfahren für S/MIME
 ☐ S/MIME sign outgoing mails	Diese Option ist im Standard inaktiv. Durch Aktivieren dieser Option wird das S/MIME Signieren ausgehender E-Mails erzwungen.
 ☐ Use opaque signature	Diese Option ist im Standard inaktiv. siehe Mail Processing ^[286] Ruleset Generator ^[287] Signing ^[298] Outgoing e-mails ^[300] Use opaque signature ^[302]
 ☐ Use triple wrapping <i>(neu in 12.1)</i>	Diese Option ist im Standard inaktiv. siehe Mail Processing ^[286] Ruleset Generator ^[287] Signing ^[298] Outgoing e-mails ^[300] Use triple wrapping ^[302]
 ☐ Use default digest for S/MIME signing: 	siehe Mail Processing ^[286] Ruleset Generator ^[287] Signing ^[298] Outgoing e-mails ^[300] Use default digest for S/MIME signing ^[302]
 SHA-1	
 SHA-256	
 SHA-512	
 ☐ Prefer RSA-PSS for S/MIME signatures	siehe Mail Processing ^[286] Ruleset Generator ^[287] Signing ^[298] Outgoing e-mails ^[300] Prefer RSA-PSS for S/MIME signatures ^[303]
 ☐ Prefer RSA-OAEP for S/MIME encryption	siehe Mail Processing ^[286] Ruleset Generator ^[287] Encryption ^[292] Outgoing e-mails ^[293] Prefer RSA-OAEP for S/MIME encryption ^[296]
 ☐ Use default cipher for S/MIME	siehe Mail Processing ^[286] Ruleset Generator ^[287] Encryption ^[292] Outgoing e-mails ^[293] Use default cipher for S/MIME encryption ^[296]

Parameter	Beschreibung
 Inline PGP	
 GINA options	Nur relevant, wenn unter Encryption mode „GINA-only“ oder „Any“ gewählt, wurde.
 [GINA Domain Auswahl]	Auswahl der in dieser Regel zu verwendenden GINA Domain ^[416]. Hinweis: In mandantenfähigen Systemen ist darauf zu achten, dass diese GINA Domain ^[416] demselben Mandanten (Customers ^[494]) zugeordnet ist wie diese Policy 
 Bounce behaviour	Im Standard ist bounce_policy ausgewählt. Bestimmt, wie mit einer E-Mail verfahren wird, sofern das Ausführen der Regel scheitert.
 [E-Mail-Template Auswahl]	Im Standard lautet die Auswahl „bounce_policy“. Auswahlmöglichkeit einer speziellen, zuvor via Mail System ^[247] Edit mail templates... ^[263] erzeugten Vorlage. Damit kann dem Absender gegebenenfalls kenntlich gemacht werden, dass der Versand seiner E-Mail aufgrund dieser speziellen Regel / Policy gescheitert ist.
 Allow default mail processing instead of bouncing if encryption was not immediately successful	Diese Option ist im Standard inaktiv. Über diese Option wird entschieden, ob eine E-Mail, für welche diese Regel / Policy nicht ausgeführt werden konnte, vor einem eventuellen Ablehnen (bounce) zunächst noch einmal das globale Ruleset (siehe Ruleset generator ^[287]) durchlaufen soll. Hinweis: Diese Option hat keinen Einfluss auf das Ablehnen (bounce) aufgrund fehlender Benutzerberechtigungen (User not authenticated) oder fehlendem Schlüsselpaar (No secret key available). Dadurch wird vermieden, dass das zu erzwingende Verschlüsseln / Signieren gegebenenfalls nicht ausgeführt würde. Ist das automatische Generieren von Users ^[396] (siehe Mail Processing ^[288] Ruleset generator ^[287] User creation ^[289]) aktiviert, so wird bei Bedarf für das Umsetzen der Regel ein neuer User generiert. 
 Disclaimer	Individuelle Disclaimer Einstellung für diese Regel.
 [Disclaimer-Template Auswahl]	Auswahlmöglichkeit eines Disclaimers aus LIST DISCLAIMER ^[259]. Wird keine Auswahl getroffen, beziehungsweise „[default]“ gewählt, so wird der in der Managed domains ^[247] des Absenders definierte Disclaimer verwendet. Mit der Auswahl „-NONE-“ wird das Einfügen eines Disclaimers unterdrückt.

 Bounce behaviour	Im Standard ist bounce_policy ausgewählt. Bestimmt, wie mit einer E-Mail verfahren wird, sofern das Ausführen der Regel scheitert.	
 Customer (nur in mandantenfähigen Systemen)	Mandant, für welchen die Policy erstellt ist.  Hinweis: Eine Policy ist immer an eine E-Mail Domäne (Managed domains ^[247]) gebunden. Die Liste der auswählbaren Domänen (Policy Domains ^[314]) hängt dabei vom Mandanten (Customers ^[494]) ab.	
 [Mandanten Auswahl] ☐	Ermöglicht das Zuordnen der Regel zu einem Mandanten.  Hinweis: Das Zuordnen von Regeln zu den jeweiligen Mandanten erfolgt bereits durch den Aufruf aus dem Quell-Menü. Von Änderungen ist im Normalfall dringend abzuweichen, da ein nachträgliches Zuordnen zum Beschädigen der Mandantentrennung und zum fehlerhaften Verarbeiten von E-Mails führen kann.	
 Senders	An dieser Stelle können jeweils unter New Domain / Mailaddress E-Mail Adressen oder auch E-Mail Domänen beziehungsweise Wildcard Domänen als Zeichenkette (String), in der Form max.mustermann@meinefirma.tld, meinefirma.tld oder .meinefirma.tld, eingetragen werden. Die Regel wird dann ausschließlich für diese Einträge greifen. Optional kann im Feld Comment : ein benutzerdefinierter Kommentar für jeden Eintrag hinzugefügt werden. Nach Eingabe einer Adresse wird jeweils nach Klicken von Add entry ein weiteres Eingabefeld eingeblendet.	Eventuelle Einträge in diesem Feld müssen eine Teilmenge der unter Policy Domains ^[314] ausgewählten Managed domains ^[247] sein.
 Recipients		

Mit **Save** wird die Regel gespeichert. **Cancel** bricht den Vorgang ohne Speichern ab. Wurde eine bereits bestehende Regel durch Klicken auf deren Namen geöffnet, so ist auch eine Schaltfläche **Delete** vorhanden, über welche diese bereits bestehende Regel gelöscht werden kann.


Achtung:

Nach dem Anlegen von Policies muss abschließend nach dem Speichern der einzelnen Policies mittels **Save** das Ruleset neu generiert werden (**Mail Processing** ^[286] **SMTP ruleset** ^[286] **Generate ruleset**).

Dies wird auch in der Statusleiste angezeigt:

The ruleset was modified. Please generate a new ruleset to activate it.

7.8 SSL

Im Menüpunkt **SSL**^[319] wird das Zertifikat angezeigt, welches für den SSL Zugang auf das GINA- beziehungsweise auf die Administrations-Oberfläche verwendet wird. Dieses Zertifikat wird auch für die TLS-Verschlüsselung zu anderen Systemen verwendet.



Hinweis:

Bei **SSL**^[319] handelt es sich um eine maschinenbezogene Einstellung. Das heißt, das hier verwendete Zertifikat wird nicht im **Cluster**^[383] synchronisiert. Gegebenenfalls muss - je nach Bedarf und Infrastruktur (siehe insbesondere **ADD TLS DOMAIN**^[282] **TLS settings**^[282] TLS-Einstellung „secure“) - auf jedem Cluster Partner ein eigenes Zertifikat verwendet oder dasselbe Zertifikat importiert werden.

Eine Ausnahme besteht bei Verwenden der Option **Use virtual hosting**^[417] aus der **Sektion Settings**^[416] des Menüs **GINA Domains**^[416], da hier für jede GINA-Domain ein eigenes Zertifikat einzubinden ist.

Ist bereits ein Zertifikat eingebunden, so wird dieses wie unten folgt angezeigt.

Andernfalls kann über die Schaltfläche **Request or create a certificate...**^[322] ein self-signed (gegebenenfalls auch lokal signiertes) SSL Zertifikat oder ein Certificate Signing Request (CSR) erzeugt werden.

Über **Import existing certificate...**^[320] kann ein bereits vorhandenes SSL Zertifikat importiert werden.

Wird oben in der Statusleiste des Menüs die gelb hinterlegte Information **Remember to import the signed certificate** angezeigt, so erscheint lediglich die Schaltfläche **Continue certificate signing request...**^[324]. Damit wird der mittels **Request or create a certificate...**^[322] gestartete Zertifikatsbezug via CSR fortgeführt, beziehungsweise abgeschlossen.



Hinweis:

SSL-Server-Zertifikate müssen als Schlüsselverwendung sowohl digitale Signatur als auch Schlüsselverschlüsselung, sowie unter erweiterte Verwendung die Serverauthentifizierung eingetragen haben.

Erlaubt sind auch Wildcard Zertifikate, also zum Beispiel „*.firma.tld“. Hier gilt jedoch zu beachten, dass mit dieser Art von Zertifikaten die TLS-Einstellung „secure“ (siehe **ADD TLS DOMAIN**^[282]) nicht möglich ist!

Wird kein TLS-secure benötigt, so kann auch im **Cluster**^[383] jeweils dasselbe Zertifikat verwendet werden.

Auch Subject Alternative Name (SAN) Zertifikate (auch Multi Domain Zertifikate genannt) werden unterstützt



Achtung:

Im Fehlerfall ist das Maschinen Zertifikat nicht zu nutzen.

Dies kann zu Problemen beim Zugriff auf die Konfigurationsoberfläche führen. Aus diesem Grund sollte vor Änderungen in diesem Menü sicherheitshalber der HTTP Port über **System**^[224]

Advanced view Admin GUI^[230] **HTTP port**^[230] für den Zugriff auf die Administrationsoberfläche (<http://<Appliance>:8080>) temporär freigegeben werden.



Sektion Issued to

Diese Sektion zeigt Informationen über den Inhaber des SSL Zertifikates.

Abhängig vom Zertifikat müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
 Name (CN)	In der Regel beinhaltet dieses Feld den Domännennamen, über welchen das GINA-Portal zu erreichen ist, zum Beispiel „securemail.meinefirma.tld“. Wird ein sogenanntes Wildcard-Zertifikat verwendet, so würde der Domännename „*.meinefirma.tld“ lauten. Bei self-signed Zertifikaten kann hier zum Beispiel auch „meinefirma.local“ stehen. IP-Adressen, wie zum Beispiel „10.0.0.10“ sollten an dieser Stelle generell vermieden werden.

Parameter	Beschreibung
 E-mail address	In der Regel der wird die E-Mail Adresse des Antragstellers, beziehungsweise des Verwalters des Zertifikates oder dessen Abteilung eingetragen.
 Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Buchhaltung“
 Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel „Firma“
 Locality (L)	Standort zum Beispiel eine Stadt wie „Neuenhof“ oder auch ein Teilgebäude wie „Werk2“
 State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel „AG“ für „Aargau“
 Country (C)	Land, zum Beispiel „CH“ für „Schweiz“
 Serial no.	Seriennummer des Zertifikats
 Subject Alternative Name	Handelt es sich bei dem Zertifikat um ein sogenanntes SAN- oder Multi-Domain-Zertifikat, so sind hier die Alternativen Antragsteller Namen zu sehen.

Sektion Issued by

Diese Sektion zeigt Informationen über den Aussteller des SSL Zertifikates (Wurzel-Zertifikat). Abhängig vom Aussteller müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
 Name (CN)	Name der ausstellenden Zertifizierungsstelle
 E-mail address	In der Regel eine E-Mail Adresse für Support-Anfragen an den Aussteller
 Org. unit (OU)	Gibt eine Organisationseinheit des Ausstellers an
 Organization (O)	Gibt die ausstellende Organisation an
 Locality (L)	Gibt den Standort des Ausstellers an
 State (ST)	Gibt ein Bundesland, Kanton, Provinz oder Ähnliches des Ausstellers an
 Country (C)	Gibt das Land des Ausstellers an
 Serial no.	Seriennummer des Zertifikats

Sektion Validity

Zeigt die Gültigkeit des Zertifikates.

Parameter	Beschreibung
 Issued on	Ausstelldatum des SSL Zertifikates
 Expires on	Ablaufdatum des SSL Zertifikates

Sektion **Fingerprint**

Der Fingerprint ist die Prüfsumme (eben auch hash oder fingerprint) und dient dem Überprüfen eines Zertifikats. An dieser Stelle wird der Hash-Algorithmus (zum Beispiel MD5 SHA1 oder SHA256), mit welchem die Prüfsumme gebildet wurde, sowie der berechnete Wert angezeigt. Sind mehrere fingerprints unterschiedlicher Algorithmen vorhanden, so wird jeder in einer separaten Zeile ausgegeben.

Parameter	Beschreibung
 Hash-Algorithmus des Zertifikates	Beispiel eines SHA1 Fingerprints: 48:2D:99:B1:64:C1:14:9C:B3:F2:C0:8D:FA:7F:40:9F:22:F5:11:F5

Sektion **Backup**

Mittels **Download certificate** kann das SSL-Zertifikat (also ausschließlich der öffentliche Schlüssel) im PEM-Format heruntergeladen werden.

Soll im **Cluster** ³⁸³ dasselbe Zertifikat für alle Cluster Mitglieder verwendet werden, so kann dieses über die Schaltfläche **Transfer to cluster members** an die Mitglieder verteilt werden.

Dieser Transfer funktioniert nur unter Backends (siehe **Cluster** ³⁸³ **Cluster members** ³⁸⁴) oder vom Frontend (siehe **Cluster** ³⁸³ **Remote LDAP server** ³⁸⁶) zum Backend, nicht jedoch vom Backend zum Frontend.

7.8.1 Request Or Create New Certificate (Authority)

Dieses Sub-Menü wird aus **SSL**  beziehungsweise **CA**  aufgerufen.

An dieser Stelle kann ein self-signed Zertifikat (in der Regel nur für Testzwecke) oder ein sogenannter Certificate Signing Request (CSR) erstellt werden.

Wird ein CSR erstellt, so wird das Schlüsselpaar auf der Appliance generiert, und nur der öffentliche Schlüssel in eine csr-Datei geschrieben, welche bei einer Zertifizierungsstelle eingereicht, signiert und als Zertifikat zurückgegeben wird.



Hinweis:

Falls oben in der Statusleiste des Menüs die gelb hinterlegte Information **Remember to import the signed certificate** angezeigt wird, so wurde zuvor bereits ein Zertifikatsantrag erstellt.

Das neu erstellte Zertifikat sollte zusammen mit den gegebenenfalls zusätzlich benötigten Zwischen- oder auch Intermediate-Zertifikate(n) zur Stammzertifizierungsstelle oder auch Root-CA in der Reihenfolge

1. Public key des eigenen Zertifikats
2. Public key des oder der Zwischen-Zertifikate

eingefügt werden. Das Wurzel-Zertifikat der Stammzertifizierungsstelle darf nicht mit eingefügt werden.



Sektion Issued to

In dieser Sektion gibt der Zertifikats-Anforderer seine entsprechenden Informationen an. Die mit * versehenen Parameter sind dabei verpflichtend.

Parameter	Beschreibung
 Name or IP (CN)	In der Regel beinhaltet dieses Feld den Domännennamen, über welchen das GINA-Portal zu erreichen ist, zum Beispiel „meinefirma.tld.tld“. Wird ein sogenanntes Wildcard-Zertifikat angefordert werden, so würde der Domännename „*.meinefirma.tld“ lauten. Bei self-signed Zertifikaten kann hier zum Beispiel auch „meinefirma.local“ stehen. IP-Adressen, wie zum Beispiel „10.0.0.10“ sollten an dieser Stelle generell vermieden werden.
 E-mail address	In der Regel der wird die E-Mail Adresse des Antragstellers, beziehungsweise des Verwalters des Zertifikates oder dessen Abteilung eingetragen.
 Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Buchhaltung“
 Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel „Firma“
 Locality (L)	Standort zum Beispiel eine Stadt wie „Neuenhof“ oder auch ein Teilgebäude wie „Werk2“
 State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel „AG“ für „Aargau“
 Country (C) 	Auswahl des Landes über das Auswahl-Menü
 Subject Alternative Names (Names or IPs separated by whitespaces) (nur bei Aufruf aus SSL verfügbar)	An dieser Stelle können weitere Namen (siehe auch Name or IP (CN)) eingetragen werden um für sogenannte Multi-Domain, beziehungsweise SAN (Subject Alternative Names) Zertifikate generieren zu können.

 Sektion **Attributes**

Parameter	Beschreibung
 Signature v	Über das Auswahl-Menü kann eingestellt werden, was generiert werden soll. Hinweis: Das Verwenden eines self-signed Zertifikat empfiehlt sich jedoch nur auf Test Systemen, da hierdurch • im Falle von SSL-Zertifikaten die Zertifikatsprüfung des Internetbrowsers eines GINA-E-Mail-Empfangers beim Verbinden auf die Appliance fehlschlagen würde. • im Falle einer lokalen CA in der Regel die S/MIME Zertifikatsprüfung fehlschlägt (siehe Hinweis in CA ³²⁸). 
 Certificate signing request	Standardeinstellung. Über diese Option wird ein Schlüsselpaar auf der Appliance generiert. Im Folgemenü CERTIFICATE SIGNING REQUEST (CSR) ³²⁴ wird dann der öffentliche Schlüssel als CSR zur Weitergabe an die CA dargestellt. Der sensible private Schlüssel verlässt die Appliance nicht!
 Self-signed certificate	Durch diese Option wird ein self-signed Zertifikat erzeugt, welches umgehend implementiert wird.
 Signed by local CA (nur bei Aufruf aus SSL verfügbar)	Ist die lokale CA ³²⁸ eingerichtet, so kann über diese Option ein von dieser CA signiertes SSL Zertifikat ausgestellt werden.
 Key size (bits) v	Über das Auswahl-Menü lässt sich die gewünschte Schlüssellänge für das angeforderte Zertifikat einstellen.
 1024	Schlüssellängen von 1024 bit entsprechen nicht mehr dem Sicherheitsstandard und sollten aus dem Grund nicht mehr verwendet werden.
 2048	Standardeinstellung. Derzeitiger Standard.
 4096	Um gegebenenfalls bei einer Erhöhung des allgemeingültigen Standards keine Aufwände zu generieren und den bereits jetzt allgemein maximal unterstützten Sicherheitsstandard zu entsprechen empfiehlt sich die Einstellung der Schlüssellänge auf 4096 bit.
 Validity (days)	Im Standard mit 398 vorgelegt. Gewünschte Gültigkeit des zu erstellenden Zertifikates in Tagen. Dieser Wert wird gegebenenfalls von der signierenden CA ignoriert und durch den CA-Standard ersetzt.

Über die Schaltfläche **Create** - ganz unten im Menü - wird die unter **Signature** gewählte Aktion gestartet.

7.8.1.1 Certificate Signing Request (CSR)

Dieses Sub-Menü ist zu sehen, wenn im Sub-Menü **REQUEST OR CREATE NEW CERTIFICATE (AUTHORITY)** ³²² **Create** mit der Einstellung **Attributes** ³²³ **Signature** *Certificate signing Request* aufgerufen wurde oder aus einem der beiden Hauptmenüs **SSL** ³¹⁹ beziehungsweise **CA** ³²⁸ der Vorgang über **Continue** *certificate signing request...* fortgesetzt wird.

Sektion Details

In dieser Sektion werden die zuvor unter **REQUEST OR CREATE NEW CERTIFICATE (AUTHORITY)** ³²² **Issued to** ³²¹ eingegebenen Parameter nochmals angezeigt. Somit stellt die folgende Tabelle die Maximalkonfiguration dar.

Parameter	Beschreibung
 Name or IP (CN)	In der Regel beinhaltet dieses Feld den Domännennamen, über welchen das GINA-Portal zu erreichen ist, zum Beispiel „securemail.meinefirma.tld“. Wird ein sogenanntes Wildcard-Zertifikat angefordert werden, so würde der Domännennamen „*.meinefirma.tld“ lauten. Bei self-signed Zertifikaten kann hier zum Beispiel auch „meinefirma.local“ stehen. IP-Adressen, wie zum Beispiel „10.0.0.10“ sollten an dieser Stelle generell vermieden werden.
 E-mail address	In der Regel der wird die E-Mail Adresse des Antragstellers, beziehungsweise des Verwalters des Zertifikates oder dessen Abteilung eingetragen.
 Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Buchhaltung“
 Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel „Firma“
 Locality (L)	Standort zum Beispiel eine Stadt wie „Neuenhof“ oder auch ein Teilgebäude wie „Werk2“
 State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel „AG“ für „Aargau“
 Country (C) 	Auswahl des Landes über das Drop-Down-Menü

Sektion Request

Das Eingabefeld enthält den CSR wie er an die Zertifizierungsstelle übermittelt werden muss. Die geschieht häufig über ein Texteingabefeld auf der Webseite der CA.

Sektion Import

Wird nach dem Hochladen des CSR zur Zertifizierungsstelle von dieser das Zertifikat zurückgeliefert, so ist der Inhalt dieses Zertifikats in dieses Eingabefeld einzugeben.

Diese Zertifikat beginnt mit -----BEGIN CERTIFICATE----- und endet mit -----END CERTIFICATE-----.

Unter Umständen werden von der Zertifizierungsstelle weitere Zertifikate bereit gestellt. Dabei handelt es sich um Zwischenzertifikate, welche unterhalb des Öffentlichen Schlüssels in dieses Feld kopiert werden müssen.

Die Eingabe muss unbedingt mit einer Leerzeile abgeschlossen werden!

**Hinweis:**

In dieses Eingabefeld sollten alle notwendigen Zwischenzertifikate für eine vollständige Zertifikatskette eingefügt werden. Eine unvollständige Zertifikatskette führt bei der Zertifikatsprüfung immer dann zu Problemen, wenn der Gegenstelle diese nicht bereits bekannt ist. Im Falle eines SSL-Zertifikates mit fehlender Kette zeigen dann Internet-Tools - wie zum Beispiel CheckTLS - einen falschen TLS-Status an.

Nicht jede Zertifizierungsstelle liefert automatisch die komplette Zertifikatskette. In diesem Fall müssen die benötigten Zwischenzertifikate gegebenenfalls anderweitig besorgt werden.

Über die Schaltfläche **Import certificate** wird der Vorgang abgeschlossen.

Die Schaltfläche **Cancel this certificate enrollment process** bricht den Vorgang ab.

**Achtung:**

Nach dem Abbruch via **Cancel this certificate enrollment process** besteht keine Möglichkeit mehr das zum CSR passende Zertifikat einzubinden, da hiermit der zum CSR passende private key gelöscht wird!

Die Appliance kann durch schlichten Wechsel in ein anderes Menü weiter konfiguriert werden, ohne den Vorgang abzubrechen.

7.8.2 Import An Existing Certificate (Authority)

Dieses Sub-Menü wird aus **SSL**  beziehungsweise **CA**  aufgerufen.

An dieser Stelle kann ein bereits vorhandenes Zertifikat importiert werden.

Sektion Upload existing certificate

Ist bereits ein passendes Zertifikat/Schlüsselpaar vorhanden, so kann dieses auf unterschiedliche Arten - abhängig vom vorliegenden Zertifikats-Format (PEM oder PKCS#12) - hochgeladen werden.

Parameter	Beschreibung
 PKCS12 file	Über die Internet-Browser Schaltfläche „Datei auswählen“ wird die PKCS#12-Datei (diese hat die Endung .p12 oder .pfx) ausgewählt.
 PKCS12 password	Nachdem eine PKCS#12-Datei den Privaten Schlüssel enthält, ist diese Passwort geschützt. Das Passwort muss vor dem Import der oben ausgewählten PKCS#12-Datei in dieses Eingabefeld eingegeben werden.
	 Hinweis: Einige CAs bieten die Möglichkeit, ein neues Zertifikat bei gleichbleibendem Privatem Schlüssel - also ohne CSR - auszustellen. Über einen Import im PEM-Format besteht die Möglichkeit, das Zertifikat bei gleichbleibenden Privatem Schlüssel zu erneuern. Weiterhin ergibt sich daraus die Möglichkeit, bei bislang fehlenden Intermediate Zertifikaten einen erneuten Zertifikatsimport inklusive der fehlenden Intermediate Zertifikate bei unverändertem Privaten Schlüssel durchzuführen.
 PEM file	Über die Internet-Browser Schaltfläche „Datei auswählen“ wird die PEM-Datei (diese hat auch die Endung .pem) ausgewählt.  Achtung: Bei Import einer PEM Datei ist, sofern diese einen Privaten Schlüssel beinhaltet, darauf zu achten, dass dieser nicht in verschlüsselter Form vorliegt! Andernfalls würde dieser abgewiesen.
 PEM text	In dieses Feld wird sowohl der Private (optional), als auch der Öffentliche Schlüssel und gegebenenfalls die Intermediate Zertifikate als Text eingefügt. Falls ein Privater Schlüssel mit importiert wird ist darauf zu achten, dass dieser nicht Kennwort geschützt ist (siehe Warnung unter PEM file). Die Eingabe sollte demnach in etwa so aussehen: <pre> -----BEGIN PRIVATE KEY----- # Privater Schlüssel -----END PRIVATE KEY----- -----BEGIN CERTIFICATE----- # Öffentlicher Schlüssel -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- # Eventuell benötigtes Zwischenzertifikat -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- # Eventuell weitere benötigte Zwischenzertifikate -----END CERTIFICATE----- </pre>

**Hinweis:**

Egal welche Methode für den Import zum Einsatz kommt, ist immer darauf zu achten, dass beim Upload alle notwendigen Zwischenzertifikate für eine vollständige Zertifikatskette beinhaltet sind. Eine unvollständige Zertifikatskette führt bei der Zertifikatsprüfung immer dann zu Problemen, wenn diese der Gegenstelle nicht bereits bekannt ist.

Nicht jede PKCS12- beziehungsweise PEM-Datei enthält die komplette Zertifikatskette. In diesem Fall müssen die benötigten Zwischenzertifikate gegebenenfalls anderweitig besorgt und in das zu importierende Zertifikat eingebettet werden.

Das Wurzel-Zertifikat der Stammzertifizierungsstelle darf nicht mit hinzugefügt werden, da die Gegenstelle diesem ohnehin vertrauen muss!

Im Falle von SSL Zertifikaten würden dann Internet-Tools - wie zum Beispiel CheckTLS - zeigen, dass die Zertifikatskette nicht vollständig ist und melden somit ein unbekanntes Zertifikat.

Wurde das Wurzel-Zertifikat der Stammzertifizierungsstelle fälschlicherweise mit hinzugefügt, melden einige Prüfwerkzeuge Fehler wie etwa „Chain issues - Contains anchor“.

Über die Schaltfläche **Import** wird das Zertifikat in die Appliance hochgeladen.

7.9 CA

Die SEPPmail Appliance beinhaltet eine vollständige Zertifizierungsstelle. Diese kann als sogenannte self-signed CA aber auch als Sub-CA konfiguriert werden.

Alternativ können trusted-CA Zertifikate automatisiert über die Managed Public Key Infrastructure (MPKI^[339]) Konnektoren bezogen werden.



Hinweis:

Das CA Zertifikat dieses Menüpunktes ist maschinenbezogen und wird somit nicht im **Cluster**^[383] synchronisiert. Gegebenenfalls muss - je nach Bedarf - auf jedem Cluster Partner ein eigenes Zertifikat verwendet oder dasselbe Zertifikat importiert werden.
Die **Settings**^[330] hingegen werden synchronisiert.



Hinweis:

Das Verwenden einer self-signed CA ist für das Signieren von E-Mails meist nicht zu empfehlen, da die Signaturen von den Empfängern in der Regel nicht automatisiert geprüft werden können. Dennoch kann das Einrichten der internen Zertifizierungsstelle sinnvoll sein, da die angegebenen Attribute auch für das Erstellen der Domänenzertifikate (siehe **Mail System**^[247] **Managed domain**^[247] **ADD/EDIT MANAGED DOMAINS**^[266] **S/MIME domain encryption**^[274]) verwendet werden.

Ist bereits ein CA-Zertifikat eingebunden, so wird dieses wie unten folgt angezeigt.

Andernfalls kann über **Request or create a certificate authority...**^[322] ein Certificate Signing Request (CSR), für ein CA oder Sub-CA Zertifikat beziehungsweise ein self-signed CA Zertifikat erzeugt werden. Das Verwenden eines self-signed CA Zertifikats empfiehlt sich aus oben genannten Gründen jedoch nur auf Test Systemen.



Achtung:

Beim Signieren des CSR ist auf der signierenden CA darauf zu achten, dass die Attribute

- ist SubCA
- kann Serverzertifikate ausstellen
- kann Clientzertifikate ausstellen

mit angegeben werden.

Über **Import existing certificate authority...**^[322] kann ein vorhandenes CA- oder Sub-CA Zertifikat importiert werden. Das daraufhin erscheinende Sub-Menü **IMPORT AN EXISTING CERTIFICATE AUTHORITY** ist vom Aufbau identisch zu dem aus **SSL IMPORT AN EXISTING CERTIFICATE**^[324].

Wird oben in der Statusleiste des Menüs die gelb hinterlegte Information **Remember to import the signed certificate** angezeigt, so erscheint lediglich die Schaltfläche **Continue certificate signing request...**^[324]. Damit wird der mittels **Request or create a certificate...**^[322] gestartete Zertifikatsbezug via CSR fortgeführt, beziehungsweise abgeschlossen.

Mit **Sign certificate request...** besteht die Möglichkeit, extern generierte CSRs mit der internen CA zu signieren. Bei Anklicken der Schaltfläche öffnet das Sub-Menü **SIGN CERTIFICATE REQUEST**^[338], in welchem der eigentliche Signatur-Prozess durchgeführt werden kann.



Sektion Issued to

Diese Sektion zeigt Informationen über den Inhaber des CA-Zertifikates.

Abhängig vom Zertifikat müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
 Common Name	Gibt den Namen der eigenen Zertifizierungsstelle an

Parameter	Beschreibung
 E-mail address	In der Regel der wird die E-Mail Adresse des Verwalters der eigenen Zertifizierungsstelle oder dessen Abteilung eingetragen.
 Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Sicherheit“
 Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel „Firma“
 Locality (L)	Standort zum Beispiel eine Stadt wie „Neuenhof“
 State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel „AR“ für „Appenzell Ausserrhoden“
 Country (C)	Land, zum Beispiel „CH“ für „Schweiz“
 Serial No.	Seriennummer des Zertifikats

Diese Parameter werden bei von der internen CA ausgestellten Zertifikate als „Issuer“ angezeigt.

Sektion **Issued by**

Diese Sektion zeigt Informationen über den Aussteller des CA-Zertifikates (Wurzel-Zertifikat).
Abhängig vom Aussteller müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
 Name (CN)	Gibt den Namen der eigenen Zertifizierungsstelle an
 E-mail address	In der Regel der wird die E-Mail Adresse des Verwalters der eigenen Zertifizierungsstelle oder dessen Abteilung eingetragen.
 Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Sicherheit“
 Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel „Firma“
 Locality (L)	Standort zum Beispiel eine Stadt wie „Neuenhof“
 State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel „AR“ für „Appenzell Ausserrhoden“
 Country (C)	Land, zum Beispiel „CH“ für „Schweiz“

Sektion **Validity**

Gibt die Gültigkeit des eigenen CA-Zertifikates an.

Parameter	Beschreibung
 Issued on	Ausstelldatum des Zertifikates
 Expires on	Ablaufdatum des Zertifikates

Sektion **Fingerprint**

Der fingerprint ist die Prüfsumme (eben auch hash oder fingerprint) und dient dem Überprüfen eines Zertifikats. An dieser Stelle wird der Hash-Algorithmus (zum Beispiel MD5 SHA1 oder SHA256), mit welchem die Prüfsumme gebildet wurde, sowie der berechnete Wert angezeigt. Sind mehrere fingerprints unterschiedlicher Algorithmen vorhanden, so wird jeder in einer separaten Zeile ausgegeben.

Parameter	Beschreibung
 Hash-Algorithmus des Zertifikates	Beispiel eines SHA1 Fingerprints: 48:2D:99:B1:64:C1:14:9C:B3:F2:C0:8D:FA:7F:40:9F:22:F5:11:F5

Sektion **Certificate Revocation List**

kurz CRL. Wurde die interne Zertifizierungsstelle konfiguriert, so hält diese eine Revokationsliste für die von ihr ausgestellten Zertifikate vor. Sollte ein Privater Schlüssel kompromittiert worden sein, so kann dieser in der Benutzerkonfiguration (siehe **Users** ^[396] **USER 'USER@DOMAIN.TLD'** ^[398] **S/MIME** ^[401]) als ungültig erklärt (revoziert) werden und taucht dann in der Revokationsliste auf. Diese kann über die Schaltfläche **Create and download CRL** heruntergeladen und somit abgefragt werden.

Sektion **Settings**

In dieser Sektion werden die Einstellungen für die self-signed, beziehungsweise Sub-CA eingegeben. Die genannten extension settings sind die Standard Einstellung beim Einrichten einer self-signed CA. Soll eine Sub-CA eingerichtet werden, gibt in der Regel der Betreiber der Haupt-CA entsprechende Werte vor.

Parameter	Beschreibung
 Static subject part	Als static subject part tauchen im Standard die beim Erstellen der Zertifizierungsstelle eingegebenen Parameter für Land (hier ist die zweistellige ISO Länderkennung zu verwenden), Organisationseinheit und Organisation auf, also zum Beispiel /C=CH/OU=Sicherheit/O=Firma
 CA validity in days	Im Standard ist der Wert 3650 vorbelegt. Gibt die Gültigkeit der ausgestellten Zertifikate in Tagen an.  Hinweis: Diese Einstellung gilt auch für die von der Appliance generierten OpenPGP Schlüsselpaare. Der Maximalwert darf 31342 Tage nicht überschreiten.
 CRL validity in days	Im Standard ist der Wert 30 vorbelegt. Gibt die Gültigkeit der Certificate Revocation List ^[330] in Tagen an.

Parameter	Beschreibung
 Automatic renewal  Hinweis: Die Auswahl, für welche Managed domains ^[247] das automatische Erneuern der Zertifikate aktiv sein soll, wird aus der Einstellung MPKI ^[339] Connector ^[339] MPKI managed domains ^[340] übernommen.	
 ☐ Automatically renew expiring certificates if validity days left less than	Diese Option ist im Standard inaktiv und mit dem Wert 90 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (Users^[396]), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wir vermeiden, dass für „Leichen“ im Menü Users^[396] Zertifikate bezogen werden. Der so initiierte Prozess wird <u>über Nacht (!)</u> abgearbeitet. <u>Revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt.</u>  Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.  Hinweis: Diese Einstellung gilt auch für die von der Appliance generierten OpenPGP Schlüsselpaare.  Hinweis: Die Laufzeit der Zertifikate der einzelnen Benutzer kann gegebenenfalls der Datei user-stats.csv, welche mit dem Daily Report^[96] (siehe auch Groups^[413] statisticsadmin^[415]) mitkommt, entnommen werden. Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.  Hinweis: Domänen-Zertifikate (explizit nicht IME !) und -PGP-Schlüssel die auslaufen, werden nach den gleichen Kriterien wie Benutzer Schlüssel erneuert.
 ☐ Automatically create certificates for active users without certificates	Diese Option ist im Standard inaktiv. Bezieht für alle existenten, aktiven Users^[396] automatisiert <u>über Nacht (!)</u> sowohl S/MIME-, wie auch OpenPGP-Schlüssel, sofern nicht bereits entsprechend <u>gültiges (!)</u> Schlüsselmaterial vorhanden ist. Als aktive Users^[396] werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den State^[396] inactive haben,

Parameter		Beschreibung	
		 Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than	
 Extension setting	name:	authorityKeyIdentifier	value: k e y i d , i s s u e r : a l w a y s
	Fügt den durch diese Zertifizierungsstelle ausgestellten Zertifikaten die über den Wert (value:) angegebenen Informationen über die ausstellende Zertifizierungsstelle hinzu		keyid: subjectKeyIdentifier (siehe nächste Option) issuer: IssuerName, Seriennummer always: Gibt eine Fehlermeldung aus, wenn das Kopieren der angegebenen Optionen fehlschlägt
	name:	subjectKeyIdentifier	value: h a s h
	Gibt die Art des Fingerprints des ausgestellten Zertifikats an		hash: bildet einen Hash-Wert gemäß RFC 3280

Parameter	Beschreibung		
			hex: Ein vordefinierter Hex-Wert wird dem Zertifikat angehängt (nicht empfohlen!)
	name:	subjectAltName	value: email : copy
	Ermöglicht das Einbinden weiterer Alternativnamen in das ausgestellte Zertifikat.		email: E-Mail Adresse copy: <i>fügt automatisch eine Kopie der E-Mail Adresse aus dem „SubjectName“ hinzu</i> URI: uniform resource indicator DNS: DNS domain name RID: registered ID: OBJECT IDENTIFIER IP: IP-Adresse im v4 oder v6 Format dirName: sollte auf einen distinguished name (DN) zeigen. Mehrfacheingabe

Parameter	Beschreibung		
			durch + möglich.
	name:	basicConstraints	value: CA:FALSE
	Zeigt auf, ob es sich bei dem Ausgestellten Zertifikat um ein Zertifizierungsstellen-Zertifikat handelt.		CA: mögliche Werte sind TRUE oder FALSE pathlen: optional bei CA:TRUE: gibt die maximale Anzahl von CAs an, welche
	name:	nsComment	value: OpenSSL Generated Certificate
	Kommentareintrag für das Zertifikat		Frei wählbarer Kommentar

Parameter	Beschreibung			
	name:	nsCertType	value:	client, email
	Gibt den Zertifikatstyp an (Netscape)		client, server, email, objsign, reserved, sslCA, emailCA, objCA	
	name:	keyUsage	value:	nonRepudiation, digitalSignature, keyEncipherment

Parameter	Beschreibung			
				h e r m e n t
	Gibt den/die erlaubten Verwendungszweck(e) für das Zertifikat an.		digitalSignature: Digitale Signatur nonRepudiation: Nachweisbarkeit keyEncipherment: Schlüssel Verschlüsselung dataEncipherment: Datenverschlüsselung keyAgreement: Schlüsselaustausch keyCertSign: Zertifikatssignatur cRLSign: Revocation List Signatur encipherOnly: nur Verschlüsselung decipherOnly: nur Entschlüsselung	
(Extension setting) (muss bei Bedarf manuell hinzugefügt werden)	name:	crDistributionPoints	value:	U R L : h t t p s : /

 [Sektion Backup](#)

Dieser Transfer funktioniert nur unter Backends (siehe [Cluster](#)^[383] [Cluster members](#)^[384])

7.9.1 Sign Certificate Request

Dieses Sub-Menü wird aus **CA**  aufgerufen.

An dieser Stelle kann ein extern generierter CSR durch die lokale CA signiert werden.

Sektion **Read CSR**

Parameter	Beschreibung
 PEM file	Über die Internet-Browser Schaltfläche „Datei auswählen“ wird die PEM-Datei (diese hat auch die Endung .pem) ausgewählt, welche den CSR enthält. Alternativ kann der CSR als Text in PEM text kopiert werden.
 PEM text	In dieses Feld kann der extern generierte CSR als Text eingefügt werden. Dieser sollte folgender Form entsprechen: -----BEGIN CSR----- # Privater Schlüssel -----END CSR----- Alternativ kann der CSR als PEM file hochgeladen werden.
 Validity	Im Standard mit 3650 vorgelegt. Gewünschte Gültigkeit des zu erstellenden Zertifikates in Tagen. Dieser Wert überschreibt die, gegebenenfalls im CSR enthaltene, gewünschte Laufzeit.
 Type v	Gibt den gewünschten Verwendungszweck des Zertifikats an.
 Client	Dient dem Authentifizieren eines Client, zum Beispiel beim Anmelden an einen Server.
 Mail	Standardeinstellung. Dient dem Absichern von E-Mails (S/MIME-Zertifikat)
 Server	Dient dem Authentifizieren eines Servers, zum Beispiel bei SSL Verbindungen (SSL-Zertifikat)

Über **Read CSR** werden zunächst die Inhalte des CSR in einem Folgemenü angezeigt, in welchem dann auch über **Sign CSR** das eigentliche Signieren erfolgt. Danach steht das Zertifikat **temporär (!)** zum Download bereit.

7.10 MPKI

Mit der MPKI können diverse akkreditierte Zertifizierungsstellen für den (teil-)automatischen Bezug von trusted CA-Zertifikaten eingebunden werden.



Hinweise zur generellen Funktion aller MPKIs:

Wird die MPKI erst nachträglich aktiviert, so werden für den optional konfigurierbaren automatischen Erneuerungsprozess (Option **Automatically renew expiring certificates if validity days left less than**) bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern (beziehungsweise neu Ausstellen) via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit. Zertifikate der internen Zertifizierungsstelle sowie revozierte Zertifikate werden nicht berücksichtigt.



Achtung:

Die Informationen für den Zertifikatsbezug (Antragsteller) werden dem jeweiligen **Users** ^[396] entnommen. Das heißt bereits bei der User-Anlage muss auf das akkurate Einfügen der relevanten Informationen geachtet werden.



Achtung:

Für die Funktionsfähigkeit der MPKI Schnittstelle muss die Konnektivität zur CA gewährleistet sein (siehe auch **Firewall / Router einrichten** ^[135], beziehungsweise **MPKI proxy settings** ^[238]).



Sektion Connectors

Parameter	Beschreibung
 MPKI type ☐	Je nach Auswahl erscheinen weitere Sektionen unterhalb dieser Sektion, mit den CA spezifischen Parametern für das Anbinden. Über die Schaltfläche Save wird die Auswahl gesichert.
 none	Schaltet die MPKI Schnittstelle ab. Keine weiteren Sektionen werden angezeigt.
 Deutsches Forschungsnetz ^[341]	CA des Deutschen Forschungsnetz (universitärer Bereich)
 DigiCert ^[344]	akkreditierte CA mit Sitz in Lehi, Utah, USA
 Bundesdruckerei D-Trust ^[346]	D-Trust ist die akkreditierte CA der Bundesdruckerei GmbH mit Sitz in Berlin, Deutschland.
 GlobalSign ^[349]	akkreditierte CA mit Sitz in Maidstone, Vereinigtes Königreich
 GlobalTrust ^[352]	akkreditierte CA mit Sitz in Wien, Österreich
 QUOVADIS Trustlink ^[355]	akkreditierte CA mit Sitz in St. Gallen, Schweiz
 Simple Certificate Enrolment Protocol ^[358]	Protokoll für das Anbinden zahlreicher namhafter Zertifizierungsstellenprodukte (zum Beispiel MS-PKI)

Parameter	Beschreibung
 Sectigo  360	akkreditierte US amerikanische Zertifizierungsstelle mit Sitz in Roseland / New Jersey
 SwissSign  364	CA der Schweizerischen Post
 MPKI managed domains 	Im Auswahlfeld sind alle Managed domains  aufgelistet. Das Beziehen von Zertifikaten über die MPKI erfolgt nur für die ausgewählten Managed domains . Somit wird ein eventuelles Abweisen von E-Mails aus Managed domains  für welche keine Zertifikate über die MPKI bezogen werden dürfen, verhindert. Mehrfachmarkierungen sind durch Klicken mit gedrückter „STRG“ Taste möglich. Die Auswahl wird mittels Save gespeichert.  Achtung: Bei bereits aktiver MPKI sind nach einem Update zunächst alle Managed domains  aktiv. Das heißt, Managed domains  welche keine Zertifikate via MPKI beziehen sollen, müssen einmalig deaktiviert werden. Sollen neu angelegte Managed domains  ebenfalls Zertifikate via MPKI beziehen, so sind diese nach Anlage in der Auswahl manuell zu aktivieren,

Gegebenenfalls weitere Sektionen werden gemäß der Auswahl unter **Connectors**  angezeigt.

Parameter	Beschreibung
	 Achtung: Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese unter Umständen beim Kopieren falsch interpretiert oder bei manueller Eingabe falsch angegeben werden (zum Beispiel unterschiedliche Hochkommata: `;`, `;`, `;`) Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mit kopiert wird.

Sektion **Certificate**

Dient dem Authentifizieren gegenüber dem Zertifizierungsstelle Anbieter (Deutsches Forschungsnetz)

Parameter	Beschreibung
 PKCS12 identity file	Zertifikat für das Authentisieren gegenüber der der Zertifizierungsstelle (Deutsches Forschungsnetz). Diese Datei wird vom Deutschen Forschungsnetz bereit gestellt und ist mit einem Passwort versehen (siehe Parameter PKCS12 password) Ist der Zugang zur Zertifizierungsstelle erfolgreich, so erscheint an dieser Stelle die Meldung an operator certificate with valid password has been found.  Hinweis: Ab 30 Tage vor Ablauf des Operator Zertifikats wird eine Meldung im Daily Report ^[96] (siehe auch Groups ^[413] admin ^[413] und statisticsadmin ^[413]) eingefügt, und der Status des Daily Report ^[96] wird zu IMPORTANT geändert..
 PKCS12 password	Passwort um die im PKCS12 identity file enthaltenen „private keys“ freizuschalten. Auch dieses wird vom Deutschen Forschungsnetz bereit gestellt.

Sektion **Settings**

Einstellungen für das automatische Erneuern von Zertifikaten.



Hinweis:

Die Laufzeit der Zertifikate der einzelnen Benutzer kann gegebenenfalls der Datei user-stats.csv, welche mit dem **Daily Report** ^[96] (siehe auch **Groups** ^[413] **statisticsadmin** ^[413]) mitkommt, entnommen werden.
Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
 ☐ Automatically renew expiring certificates if	Diese Option ist im Standard inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (Users ^[396]), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail

Parameter	Beschreibung
validity days left less than	sendet. Damit wird vermieden, dass für „Leichen“ im Menü Users^[396] gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird <u>über Nacht (!)</u> abgearbeitet.  Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). <u>Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt.</u>  Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
 Automatically create certificates for active users without certificates	Diese Option ist im Standard inaktiv. Bezieht für alle existenten, aktiven Users^[396], welche nicht im Besitz eines <u>gültigen (!)</u> Zertifikates sind, automatisiert <u>über Nacht (!)</u> ein Zertifikat. Als aktive Users^[396] werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den State^[396] inactive haben.  Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than
 Chain certificates (needed to sign e-mails)	Durch Klicken von Add or update... werden unter X.509 Root Certificates^[480] die Zwischen-(Intermediate-)Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden.  Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

7.10.2 DigiCert

DigiCert spezifische Sektionen in **MPKI** ^[339]

Sektion **Default parameters**

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden in der Regel mit dem Vertragsschluss zwischen dem E-Mail Domänen Inhaber und DigiCert von DigiCert bereit gestellt.

Parameter	Beschreibung
 Default organization ID	Wird von DigiCert bereit gestellt
 API key	Wird von DigiCert bereit gestellt

Sektion **Domain specific parameters** (optional)

Werden auf der SEPPmail Appliance mehrere E-Mail Domänen (**Managed domains** ^[247]) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden. Nach dem Speichern der Domänen spezifischen Option via **Save entries** erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
 New organization ID:	
 ID	Wird von DigiCert bereit gestellt
 Domains:	Wird von DigiCert bereit gestellt  Achtung: Die hier eingetragene Domäne muss unter Connectors ^[339] MPKI managed domains ^[340] ausgewählt sein, damit Zertifikate bezogen werden.

Sektion **Settings**

Einstellungen für das automatische Erneuern von Zertifikaten.



Hinweis:

Die Laufzeit der Zertifikate der einzelnen Benutzer kann gegebenenfalls der Datei user-stats.csv, welche mit dem **Daily Report** ^[98] (siehe auch **Groups** ^[413] **statisticsadmin** ^[413]) mitkommt, entnommen werden.
Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
 ☐ Automatically	Diese Option ist im Standard inaktiv und mit dem Wert 30 vorbelegt.

Parameter	Beschreibung
renew expiring certificates if validity days left less than	Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (Users³⁹⁶), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü Users³⁹⁶ gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird <u>über Nacht (!)</u> abgearbeitet.  Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). <u>Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt.</u>  Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
 Automatically create certificates for active users without certificates	Diese Option ist im Standard inaktiv. Bezieht für alle existenten, aktiven Users³⁹⁶, welche nicht im Besitz eines <u>gültigen (!)</u> Zertifikates sind, automatisiert <u>über Nacht (!)</u> ein Zertifikat. Als aktive Users³⁹⁶ werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den State³⁹⁶ inactive haben.  Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than
 Chain certificates (needed to sign e-mails)	Durch Klicken von Add or update... werden unter X.509 Root Certificates⁴⁸⁰ die Zwischen-(Intermediate-)Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden.  Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

7.10.3 Bundesdruckerei D-Trust

Bundesdruckerei D-Trust spezifische Sektionen in MPKI 

Informationen zur Managed PKI der Bundesdruckerei D-Trust erhalten Sie bei Bedarf auf der Webseite (www.bundesdruckerei.de)

An dieser Stelle wird die Verbindung zur Bundesdruckerei D-Trust CA, für den automatisierten Bezug von Benutzer-Zertifikaten konfiguriert.



Hinweis:

Bei erfolgreichem Erstellen eines Zertifikats via MPKI werden auch alle notwendigen CA Zertifikate von D-Trust übermittelt und importiert.



Sektion Default parameters

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden in der Regel mit dem Vertragsschluss zwischen dem E-Mail Domänen Inhaber und der Bundesdruckerei von der Bundesdruckerei bereit gestellt.

Parameter	Beschreibung
 Service URL	Angabe der URL, auf welche über die MPKI zugegriffen werden soll. In der Regel lautet die URL https://csm.d-trust.net/httpcmp/request
 Product	Angabe des gebuchten Produktes. In der Regel sind das ➤ BASIC_ENTERPRISE_ID ➤ ADVANCED_ENTERPRISE_ID Weiterhin werden TEAM_ID Produkte angeboten, welche für Organisationen/Gruppenpostfächer, jedoch nicht für Einzelpersonen gedacht sind. Den oben genannten Produktnamen kann alternativ _1, _2, ... bis _5 angehängt werden. Dadurch wird die Laufzeit der via MPKI angeforderten Zertifikate auf die entsprechende Anzahl in Jahren festgelegt. Diese Funktion muss bei Bedarf jedoch im D-Trust Webportal aktiviert werden.
 Static subject part	Dieser Teil taucht im Zertifikat des jeweiligen Benutzers zusätzlich zur E-Mail Adresse E als Erweiterung des Feldes „Antragsteller“ auf. Dabei ist der Eintrag O = [Organisation] verpflichtend und muss mit dem Eintrag, wie er im D-Trust Webportal festgelegt wurde, übereinstimmen.  Achtung: Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese unter Umständen beim Kopieren falsch interpretiert oder bei manueller Eingabe falsch angegeben werden (zum Beispiel unterschiedliche Hochkommata: `;`, `;`) Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mit kopiert wird.



Sektion Domain specific parameters (optional)

Werden auf der SEPPmail Appliance mehrere E-Mail Domänen (**Managed domains** ^[247]) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden. Nach dem Speichern der Domänen spezifischen Option via **Save entries** erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
 Domain	Angabe der E-Mail Domäne, für welche die beiden folgenden Parameter gültig sein sollen.  Achtung: Die hier eingetragene Domäne muss unter Connectors ^[339] MPKI managed domains ^[340] ausgewählt sein, damit Zertifikate bezogen werden.
 Product	Angabe des gegebenenfalls vom Default parameters ^[346] abweichenden Product ^[346] .
 Static subject part	Angabe des gegebenenfalls vom Default parameters ^[346] Static subject part ^[346] .  Achtung: Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese unter Umständen beim Kopieren falsch interpretiert oder bei manueller Eingabe falsch angegeben werden (zum Beispiel unterschiedliche Hochkommata: `;`, `;`, `;`) Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mit kopiert wird.

Sektion **Certificate**

Dient dem Authentifizieren gegenüber dem Zertifizierungsstellen Anbieter (Bundesdruckerei D-Trust).

Parameter	Beschreibung
 PKCS12 identity file	Zertifikat für das Authentisieren gegenüber der der Zertifizierungsstelle (Bundesdruckerei D-Trust). Diese Datei wird von der Bundesdruckerei D-Trust bereit gestellt und ist mit einem Passwort versehen (siehe Parameter PKCS12 password) Ist der Zugang zur Zertifizierungsstelle erfolgreich, so erscheint an dieser Stelle die Meldung an operator certificate with valid password has been found.  Hinweis: Ab 30 Tage vor Ablauf des Operator Zertifikats wird eine Meldung im Daily Report ^[96] (siehe auch Groups ^[413] admin ^[413] und statisticsadmin ^[415]) eingefügt, und der Status des Daily Report ^[96] s wird zu IMPORTANT geändert..
 PKCS12 password	Passwort um die im PKCS12 identity file enthaltenen „private keys“ freizuschalten. Auch dieses wird von der Bundesdruckerei D-Trust bereit gestellt.

Sektion **Settings**

Einstellungen für das automatische Erneuern von Zertifikaten.



Hinweis:

Die Laufzeit der Zertifikate der einzelnen Benutzer kann gegebenenfalls der Datei user-stats.csv, welche mit dem **Daily Report** ^[96] (siehe auch **Groups** ^[413] **statisticsadmin** ^[415]) mitkommt, entnommen werden.

Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
 ☐ Automatic ally renew expiring certificates if validity days left less than	Diese Option ist im Standard inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (Users ^[396]), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü Users ^[396] gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird <u>über Nacht (!)</u> abgearbeitet. Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). <u>Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt.</u> Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
 ☐ Automatically create certificates for active users without certificates	Diese Option ist im Standard inaktiv. Bezieht für alle existenten, aktiven Users ^[396], welche nicht im Besitz eines <u>gültigen (!)</u> Zertifikates sind, automatisiert <u>über Nacht (!)</u> ein Zertifikat. Als aktive Users ^[396] werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den State ^[396] inactive haben. Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than
 Chain certificates (needed to sign e- mails)	Durch Klicken von Add or update... werden unter X.509 Root Certificates ^[486] die Zwischen- (Intermediate-)Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden. Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

7.10.4 GlobalSign

GlobalSign spezifische Sektionen in MPKI ^[339]

Sektion **Default parameters**

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden von GlobalSign bereit gestellt.

Parameter	Beschreibung
 Service URL	Im Standard mit https://system.globalsign.com/services/cr/ws/GasOrderService vorbelegt. Angabe der URL, auf welche über die MPKI zugegriffen werden soll. Wird von GlobalSign vorgegeben.
 Product code	Im Standard mit EPKIPSPersonal vorbelegt Wird von GlobalSign vorgegeben.
 Default profile ID	Wird von GlobalSign vorgegeben.
 Certificate Period	Laufzeit der auszustellenden Zertifikate (ein bis drei Jahre). Wird von GlobalSign vorgegeben.
 Account	Benutzername des Kunden bei GlobalSign. Dieser Benutzer muss im GlobalSign Kunden-Portal Administrator-Rechte besitzen. Wird von GlobalSign vorgegeben.
 Password	Zugehöriges Passwort zu Account



Hinweis:

Zusätzlich zu den oben genannten Eingaben, muss im GlobalSign Kunden-Portal die IP Adresse der SEPPmail Appliance für den automatischen Bezug der Zertifikate freigeschaltet werden!

Sektion **Domain specific parameters** (optional)

Werden auf der SEPPmail Appliance mehrere E-Mail Domänen (**Managed domains** ^[247]) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden. Nach dem Speichern der Domänen spezifischen Option via **Save entries**, erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
 New domain entry	
 Profile ID	Wird von GlobalSign vorgegeben.
 Domains	Angabe der E-Mail Domänen, für welche die beiden folgenden Parameter gültig sein sollen. Nur Domänen, welche beim Stellen des Antrags bei der Zertifizierungsstelle auch benannt, beziehungsweise später separat validiert wurden, dürfen eingetragen werden.

Parameter	Beschreibung
	 Achtung: Die hier eingetragene Domäne muss unter Connectors ^[339] MPKI managed domains ^[340] ausgewählt sein, damit Zertifikate bezogen werden.
 Product code	Angabe des gegebenenfalls vom Default parameters ^[349] abweichenden Product code ^[349] . Wird von GlobalSign vorgegeben.
 Certificate Period	Laufzeit der auszustellenden Zertifikate (ein bis drei Jahre). Wird von GlobalSign vorgegeben. Wird hier nichts eingetragen, gilt der Wert aus den Default parameters ^[349] .
 Account	Angabe des gegebenenfalls vom Default parameters ^[349] abweichenden Account ^[349] s. Wird von GlobalSign vorgegeben.
 Password	Nur erforderlich, wenn der Account vom Default parameters ^[349] abweicht. Wird gegebenenfalls von GlobalSign vorgegeben.

Sektion Settings

Einstellungen für das automatische Erneuern von Zertifikaten.



Hinweis:

Die Laufzeit der Zertifikate der einzelnen Benutzer kann gegebenenfalls der Datei user-stats.csv, welche mit dem **Daily Report** ^[96] (siehe auch **Groups** ^[413] **statisticsadmin** ^[415]) mitkommt, entnommen werden.
Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
 ☐ Automatically renew expiring certificates if validity days left less than	Diese Option ist im Standard inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (Users ^[396]), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü Users ^[396] gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird <u>über Nacht (!)</u> abgearbeitet. Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). <u>Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt.</u> Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.

Parameter	Beschreibung
 Automatically create certificates for active users without certificates	Diese Option ist im Standard inaktiv. Bezieht für alle existenten, aktiven Users ^[396], welche nicht im Besitz eines <u>gültigen (!)</u> Zertifikates sind, automatisiert <u>über Nacht (!)</u> ein Zertifikat. Als aktive Users ^[396] werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den State ^[396] inactive haben.  Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than
 Chain certificates (needed to sign e-mails)	Durch Klicken von Add or update... werden unter X.509 Root Certificates ^[480] die Zwischen-(Intermediate-)Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden.  Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

7.10.5 GlobalTrust

GlobalTrust spezifische Sektionen in **MPKI** ^[339]
(neu in 12.0)

Sektion **Default parameters**

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden in der Regel mit dem Vertragsschluss zwischen dem E-Mail Domänen Inhaber und GlobalTrust von GlobalTrust bereit gestellt.

Parameter	Beschreibung
 Default UID	Wird von GlobalTrust bereit gestellt
 Certificate period	Wird von GlobalTrust mitgeteilt

Sektion **Domain specific parameters** (optional)

Werden auf der SEPPmail Appliance mehrere E-Mail Domänen (**Managed domains** ^[247]) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden. Nach dem Speichern der Domänen spezifischen Option via **Save entries** erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
 New domain entry:	
 UID	Wird von GlobalTrust bereit gestellt
 Domains:	 Achtung: Die hier eingetragene Domäne muss unter Connectors ^[339] MPKI managed domains ^[340] ausgewählt sein, damit Zertifikate bezogen werden.
 Certificate period (empty if default)	Wird bei Bedarf von GlobalTrust mitgeteilt

Sektion **Certificate**

Dient dem Authentifizieren gegenüber dem Zertifizierungsstellen Anbieter (GlobalTrust)

Parameter	Beschreibung
 PKCS12 identity file	Zertifikat für das Authentisieren gegenüber der der Zertifizierungsstelle (GlobalTrust). Diese Datei wird von GlobalTrust bereit gestellt und ist mit einem Passwort versehen (siehe Parameter PKCS12 password) Ist der Zugang zur Zertifizierungsstelle erfolgreich, so erscheint an dieser Stelle die Meldung

Parameter	Beschreibung
	an operator certificate with valid password has been found.  Hinweis: Ab 30 Tage vor Ablauf des Operator Zertifikats wird eine Meldung im Daily Report ^[96] (siehe auch Groups ^[413] admin ^[413] und statisticsadmin ^[413]) eingefügt, und der Status des Daily Report ^[96] s wird zu IMPORTANT geändert..
 PKCS12 password	Passwort um die im PKCS12 identity file enthaltenen „private keys“ freizuschalten. Auch dieses wird von GlobalTrust bereit gestellt.

Sektion Settings

Einstellungen für das automatische Erneuern von Zertifikaten.



Hinweis:

Die Laufzeit der Zertifikate der einzelnen Benutzer kann gegebenenfalls der Datei user-stats.csv, welche mit dem **Daily Report** ^[96] (siehe auch **Groups** ^[413] **statisticsadmin** ^[413]) mitkommt, entnommen werden.

Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
 ☐ Automatically renew expiring certificates if validity days left less than	Diese Option ist im Standard inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (Users ^[396]), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü Users ^[396] gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird <u>über Nacht (!)</u> abgearbeitet.  Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). <u>Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt.</u>  Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
 ☐ Automatically create certificates for active users without certificates	Diese Option ist im Standard inaktiv. Bezieht für alle existenten, aktiven Users ^[396], welche nicht im Besitz eines <u>gültigen (!)</u> Zertifikates sind, automatisiert <u>über Nacht (!)</u> ein Zertifikat. Als aktive Users ^[396] werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den State ^[396] inactive haben.

Parameter	Beschreibung
	 Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than
 Chain certificates (needed to sign e-mails)	Durch Klicken von Add or update... werden unter X.509 Root Certificates ⁴⁸⁰ die Zwischen-(Intermediate-)Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden.  Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

7.10.6 QuoVadis Trustlink

QuoVadis Trustlink spezifische Sektionen in **MPKI** ^[339]

Informationen zur QuoVadis Trustlink MPKI erhalten Sie unter
www.quovadisglobal.ch/Dienstleistungen/ZertifikatsServices.aspx

Sektion **Default parameters**

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden in der Regel mit dem Vertragsschluss zwischen dem E-Mail Domänen Inhaber und QuoVadis Trustlink von QuoVadis Trustlink bereit gestellt

Parameter	Beschreibung
 Service URL	Angabe der URL, über welche der Zugriff auf die MPKI erfolgt. QuoVadis Trustlink teilt die URL mit den Zugangsdaten mit. In der Regel lautet sie „ <a href="https://tlconnector.quovadisglobal.com/<IhreFirma>/<IhreOrganisation>">https://tlconnector.quovadisglobal.com/<IhreFirma>/<IhreOrganisation> “.
 Static subject part	Dieser Teil taucht im Zertifikat des jeweiligen Benutzers als Erweiterung des Feldes „Antragsteller“ auf und kann im Rahmen eines Distinguished Names frei - zum Beispiel /C=[Zweistelliger Ländercode]/OU=[Organisationsdetail]/O=[Organisation] - definiert werden, wobei die Angabe des Ländercodes zwingend ist.  Achtung: Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese unter Umständen beim Kopieren falsch interpretiert oder bei manueller Eingabe falsch angegeben werden (zum Beispiel unterschiedliche Hochkommata: ‘, ’, ’) Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mit kopiert wird.

Sektion **Domain specific parameters** (optional)

Werden auf der SEPPmail Appliance mehrere E-Mail Domänen (**Managed domains** ^[247]) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden. Nach dem Speichern der Domänen spezifischen Option via **Save entries**, erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
 Domain:	Angabe der E-Mail Domäne, für welche die beiden folgenden Parameter gültig sein sollen. Nur Domänen, welche beim Stellen des Antrags bei der Zertifizierungsstelle auch benannt, beziehungsweise später separat validiert wurden, dürfen eingetragen werden. Abweichende Domännennamen können dazu führen, dass Zertifikate nicht ausgestellt werden.  Achtung: Die hier eingetragene Domäne muss unter Connectors ^[339] MPKI managed domains ^[340] ausgewählt sein, damit Zertifikate bezogen werden.

Parameter	Beschreibung
 URL:	Eine gegebenenfalls vom Default parameters ^[355] abweichende Service URL wird von QuoVadis Trustlink mit den Zugangsdaten bereitgestellt.
 Static subject part:	Siehe Sektion Default parameters ^[355] Static subject part  Achtung: Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese unter Umständen beim Kopieren falsch interpretiert oder bei manueller Eingabe falsch angegeben werden (zum Beispiel unterschiedliche Hochkommata: ‘ ’, ‘ ’, ‘ ’) Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mit kopiert wird.

Sektion **Certificate**

Dient dem Authentifizieren gegenüber dem Zertifizierungsstellen Anbieter (QuoVadis Trustlink)

Parameter	Beschreibung
 PKCS12 identity file	Zertifikat für das Authentisieren gegenüber der der Zertifizierungsstelle (QuoVadis Trustlink). Diese Datei wird von QuoVadis bereit gestellt und ist mit einem Passwort versehen (siehe Parameter PKCS12 password) Ist der Zugang zur Zertifizierungsstelle erfolgreich, so erscheint an dieser Stelle die Meldung an operator certificate with valid password has been found.  Hinweis: Ab 30 Tage vor Ablauf des Operator Zertifikats wird eine Meldung im Daily Report ^[96] (siehe auch Groups ^[413] admin ^[413] und statisticsadmin ^[415]) eingefügt, und der Status des Daily Report ^[96] s wird zu IMPORTANT geändert..
 PKCS12 password	Passwort um die im PKCS12 identity file enthaltenen „private keys“ freizuschalten. Auch dieses wird von QuoVadis Trustlink bereit gestellt.
 SSL chain certificates	Damit die SEPPmail Appliance beim Signieren von E-Mails die Zertifikatskette hin zur Stammzertifizierungsstelle (QuoVadis Trustlink) ergänzen kann, muss diese bekannt gemacht werden. Hierfür muss die Zertifikatskette über eine entsprechende Zertifikatsdatei hochgeladen werden. Im darunterliegenden Anzeigefeld werden die hochgeladenen Zwischenzertifikate im Textformat angezeigt. QuoVadis Trustlink stellt die Zertifikatskette in der Regel über eine PEM-Datei mit dem Namen „SSL_tlconnector_quovadisglobal_com_<jjjjmmdd>.pem“ zur Verfügung.

Sektion **Settings**

Einstellungen für das automatische Erneuern von Zertifikaten.

**Hinweis:**

Die Laufzeit der Zertifikate der einzelnen Benutzer kann gegebenenfalls der Datei user-stats.csv, welche mit dem **Daily Report** ^[96] (siehe auch **Groups** ^[413] **statisticsadmin** ^[415]) mitkommt, entnommen werden.

Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
 ☐ Automatically renew expiring certificates if validity days left less than	Diese Option ist im Standard inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (Users ^[396]), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü Users ^[396] gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird <u>über Nacht (!)</u> abgearbeitet.  Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). <u>Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt.</u>  Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
 ☐ Automatically create certificates for active users without certificates	Diese Option ist im Standard inaktiv. Bezieht für alle existenten, aktiven Users ^[396], welche nicht im Besitz eines <u>gültigen (!)</u> Zertifikates sind, automatisiert <u>über Nacht (!)</u> ein Zertifikat. Als aktive Users ^[396] werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den State ^[396] inactive haben.  Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than
 Chain certificates (needed to sign e-mails)	Durch Klicken von Add or update... werden unter X.509 Root Certificates ^[480] die Zwischen-(Intermediate)-Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden.  Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

7.10.7 Simple Certificate Enrollment Protocol

Simple Certificate Enrollment Protocol (SCEP) spezifische Sektionen in **MPKI** ^[339]

Sektion **Parameter**

Dieser Sektion beinhaltet die Verbindungsdaten zur externen CA.

Parameter	Beschreibung
 Service URL	URL unter welchem die Verbindung zur Zertifizierungsstelle hergestellt wird. Voreingestellt ist die URL mit dem Network Device Enrollment (NDES) Namen der SEPPmail Appliance für Microsoft Enterprise CA: http://localhost:10000/certsrv/mscep/mscep.dll

Sektion **Certificate**

In dieser Sektion werden die Parameter für das Authentifizieren an der externen Zertifizierungsstelle angegeben.

Parameter	Beschreibung
 Challenge password	Kennwort für das Übermitteln einer Anforderung an die externe CA.  Hinweis: Das Passwort wird bei der Eingabe im Klartext dargestellt, damit dieses verifiziert werden kann. Beim Speichern wird das Eingabefeld dann geleert.
 Signature certificate	Über diese Funktion wird das Zertifikat zum Signieren der Anforderungen an die externe Zertifizierungsstelle (RA-Zertifikat) eingebunden. Dieses RA-Zertifikat wird von der externen Zertifizierungsstelle in der Regel explizit für das Anbinden der SEPPmail Appliance MPKI ausgestellt.
 CA certificate	An dieser Stelle wird das Wurzel-Zertifikat der extern anzubindenden Zertifizierungsstelle bekannt gemacht.

Sektion **Settings**

Einstellungen für das automatische Erneuern von Zertifikaten.



Hinweis:

Die Laufzeit der Zertifikate der einzelnen Benutzer kann gegebenenfalls der Datei user-stats.csv, welche mit dem **Daily Report** ^[96] (siehe auch **Groups** ^[413] **statisticsadmin** ^[413]) mitkommt, entnommen werden.

Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
 ☐ Automatically renew expiring	Diese Option ist im Standard inaktiv und mit dem Wert 30 vorgelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (Users ^[396]), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail

Parameter	Beschreibung
certificates if validity days left less than	sendet. Damit wird vermieden, dass für „Leichen“ im Menü Users³⁹⁶ gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird <u>über Nacht (!)</u> abgearbeitet.  Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). <u>Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt.</u>  Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
 Automatically create certificates for active users without certificates	Diese Option ist im Standard inaktiv. Bezieht für alle existenten, aktiven Users³⁹⁶, welche nicht im Besitz eines <u>gültigen (!)</u> Zertifikates sind, automatisiert <u>über Nacht (!)</u> ein Zertifikat. Als aktive Users³⁹⁶ werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den State³⁹⁶ inactive haben.  Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

7.10.8 Sectigo

Sectigo spezifische Sektionen in **MPKI** ^[399]

Sektion **Default parameters**

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden von Sectigo bereit gestellt.

Parameter	Beschreibung
 Customer URI	Angabe der URI, auf welche über die MPKI zugegriffen werden soll. Wird von Sectigo vorgegeben.
 Login	Wird von Sectigo vorgegeben.
 Password	Wird von Sectigo vorgegeben.
 Organization ID	Wird von Sectigo bezogen, sofern die Verbindung etabliert ist und valide Login Daten angegeben wurden. Die Anzahl der angezeigten Organisationen und Zertifikatstypen ist von den Einstellungen in der Sectigo WebGUI abhängig.
 Certificate type	Wird von Sectigo bezogen, sofern die Verbindung etabliert ist und valide Login Daten angegeben wurden. Bei den wie folgt angezeigten möglichen Typen kann zusätzlich jeweils die Zertifikatslaufzeit angegeben werden.  Hinweis: Bezugnehmend auf die aktuelle technische Richtlinie des BSI, empfehlen wir generell keine Laufzeiten von mehr als zwei Jahren einzustellen.
GEANT Personal Certificate GEANT IGTF-MICS Personal GEANT IGTF-MICS-Robot Personal GEANT IGTF-Classic-Robot Email	Dies sind Beispiel Zertifikatstypen für allgemeinnützige Organisationen. Weitere Informationen zu den Unterschieden der Zertifikatstypen sind beim Anbieter Sectigo zu erfragen.
 Full name regex	Bedingt durch die Art und Weise, wie Users ^[396] angelegt werden, können beim Beziehen von Zertifikaten Probleme auftauchen, sofern im Feld Name ^[396] des Users ^[396] eine E-Mail Adresse enthalten ist (siehe auch Warnung in der Beschreibung des Feldes Name ^[396]) oder der angegebene Name nicht den Konventionen der CA für den erfolgreichen Bezug eines Zertifikates entspricht. Für diesen Fall besteht die Möglichkeit über Reguläre Ausdrücke den Eintrag im Feld Name ^[396] des Users ^[396] so zu zerlegen, dass ein CA konformes Format entsteht. Der Standard Eintrag (?<GN>.+)(?<SN>.+)

Parameter	Beschreibung
	zerlegt den Eintrag aus dem Feld Name ^[396] des Users ^[396] in Given Name (GN) also dem Vornamen und Surname (SN) also dem Nachnamen. Ausgehend von einem Eintrag Max Mustermann würde dieser in GN=Max SN=Mustermann zerlegt. Bei mehreren Vornamen im Feld Name ^[396] 1.Vorname 2.Vorname Nachname würde der zerlegte Ausdruck wie folgt aussehen GN=1.Vorname 2.Vorname SN=Nachname Sollten im Feld Name ^[396] der Users ^[396] E-Mail-Adressen stehen, so könnten auch diese zerlegt werden. Sofern das übliche E-Mail Format vorname.nachname@firma.tld verwendet wird, müsste der Reguläre Ausdruck wie folgt lauten (?<GN>.*).\.(?<SN>.*)*@.* Am Beispiel max.mustermann@meinefirma.tld würde dieser ebenfalls in GN=Max SN=Mustermann zerlegt.

**Hinweis:**

Zusätzlich zu den oben genannten Eingaben, muss im Sectigo Kunden-Portal die IP Adresse der SEPPmail Appliance für den automatischen Bezug der Zertifikate freigeschaltet werden!

**Sektion Domain specific parameters** (optional)

Diese Parameter sind für wenigstens eine **Organization ID** ^[360] zu setzen. Existieren zum Customer aus den **Default parameters** ^[360] mehrere **Organization ID** ^[360]s, so erscheint pro **Organization ID** ^[360] ein **Domain entry** ^[361].

Nach dem Speichern der Domänen spezifischen Option via **Save entries**, erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
New domain entry	
Organization ID	Wird, beziehungsweise werden jeweils von Sectigo bezogen, sofern das Login (siehe Default parameters ^[360]) erfolgreich war.
Domains	Angabe der E-Mail Domänen, für welche die folgenden Parameter gültig sein sollen. Nur Domänen, welche beim Stellen des Antrags bei der Zertifizierungsstelle auch benannt, beziehungsweise später separat validiert wurden, dürfen eingetragen werden.

Parameter	Beschreibung
	 Achtung: Die hier eingetragene(n) Domäne(n) muss unter Connectors ^[339] MPKI managed domains ^[340] ausgewählt sein, damit Zertifikate bezogen werden.
 Certificate type	siehe Default parameters ^[360] .

Sektion **Settings**

Einstellungen für das automatische Erneuern von Zertifikaten.



Hinweis:

Die Laufzeit der Zertifikate der einzelnen Benutzer kann gegebenenfalls der Datei user-stats.csv, welche mit dem **Daily Report** ^[98] (siehe auch **Groups** ^[413] **statisticsadmin** ^[415]) mitkommt, entnommen werden.

Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
 ☐ Automatically renew expiring certificates if validity days left less than	Diese Option ist im Standard inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (Users ^[396]), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü Users ^[396] gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird <u>über Nacht (!)</u> abgearbeitet.  Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). <u>Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt.</u>  Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
 ☐ Automatically create certificates for active users without certificates	Diese Option ist im Standard inaktiv. Bezieht für alle existenten, aktiven Users ^[396], welche nicht im Besitz eines <u>gültigen (!)</u> Zertifikates sind, automatisiert <u>über Nacht (!)</u> ein Zertifikat. Als aktive Users ^[396] werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den State ^[396] inactive haben.

Parameter	Beschreibung
	 Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than
 Chain certificates (needed to sign e-mails)	Durch Klicken von Add or update... werden unter X.509 Root Certificates die Zwischen-(Intermediate-)Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden.  Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

7.10.9 SwissSign

SwissSign spezifische Sektionen in MPKI ^[339]

Informationen zur Bestellung und zu den Modalitäten für das Einrichten einer SwissSign MPKI erhalten Sie unter www.swisssign.com/managed-pki/managed-pki-service.html

Die Webseite für das SwissSign seitige Verwalten der Zertifikate ist unter <https://swisssign.net> zu erreichen. Das Anmelden an dieser Seite erfolgt mit den jeweiligen Kontodaten oder mit dem aktuellen Operator Zertifikat (siehe auch **Certificate** ^[366]). Hierüber kann auch bei Ablauf des Operatorenzertifikates selbstständig ein neues bezogen werden.



Hinweis:

Insbesondere bei Managed Service Providern (MSP) sind Unterschiede beim Zertifikatsbezug zu beachten:

- **OHNE** Organisationseintrag
Hierbeikann der MSP eine Kunden-E-Mail Domäne einfach per „Self-Validation“ für den Zertifikatsbezug hinzufügen. Die in dieser Variante bezogenen Zertifikate beinhalten jeweils die im Attribut „Antragsteller“ die Daten des Abschnitts **Static subject part** ^[364] der Sektion **Default parameters** ^[364].
- **MIT** Organisationseintrag oder höherwertig
erhält der Kunde einen eigenen Organisationseintrag, welcher jeweils die im Attribut „Antragsteller“ auftaucht. Diesen Eintrag nimmt der MSP für die entsprechende(n) E-Mail Domäne(n) des Kunden in der Sektion **Domain specific parameters** ^[365] vor. Dafür muss der Kunde eine Annahmeerklärung zur Organisationsprüfung an SwissSign senden. Nach erfolgter Prüfung werden von SwissSign die entsprechenden Konfigurationsdaten (**Domain specific parameters** ^[365]) mitgeteilt und der Bezug von Zertifikaten entsprechend freigegeben.
Für diesen Prozess muss ein sogenannter Change-Auftrag bei SwissSign abgesetzt werden (welchen in der Regel SEPPmail auslöst). Dieser Prozess ist kostenpflichtig, sofern ein gewisser Mindestbestellwert an Zertifikaten nicht erreicht wird.



An dieser Stelle wird die Verbindung zur SwissSign CA, für den automatisierten Bezug von Benutzer-Zertifikaten konfiguriert.



Sektion **Default parameters**

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden von SwissSign in der Regel mittels einer „Willkommens-E-Mail“ bereit gestellt.

Parameter	Beschreibung
 Service URL	Angabe der URL, auf welche über die MPKI zugegriffen werden soll. In der Regel lautet die URL https://ra.swisssign.net/ws/cmc
 Static subject part	Dieser Teil taucht im Zertifikat des jeweiligen Benutzers zusätzlich zur E-Mail Adresse E als Erweiterung des Feldes „Antragsteller“ auf. Je nach gewählttem Zertifikatstyp ist der hier einzutragende Wert statisch durch SwissSign vorgegeben ➤ SwissSign Silver ID Zertifikate /CN=Secure Mail: SEPPmail Certificate/O=[Organisation]/C=[Land] Im Feld Antragsteller des Zertifikates würde somit folgendes eingetragen: E = [E-Mail Adresse] CN = Secure Mail: SEPPmail Certificate O = [Organisation] (optional) ST = [Bundesland/Kanton] (optional - nur möglich, wenn O gesetzt) C= [Land] (optional - nur möglich, wenn O gesetzt) beziehungsweise für das Attribut „OU=“ durch den Kunden konfigurierbar. Weiterhin taucht als CN der Anzeigename „Name“ (siehe Users ^[396]) auf

Parameter	Beschreibung
	➤ SwissSign Gold ID Zertifikate /OU=[Organisationsdetail]/O=[Organisation]/C=[Land] wird durch SwissSign vorgegeben und entspricht in der Regel dem Organisationsnamen, wie er im Handelsregister und somit im SwissSign-Antrag vorzufinden ist. Für den Ländernamen ist die zweistellige ISO Länderkennung zu verwenden. Im Feld Antragsteller des Zertifikates würde somit folgendes eingetragen: E = [E-Mail Adresse] CN = [Name des Zertifikatsinhabers] OU = [Organisationsdetail] O = [Organisation] ST = [Bundesland/Kanton] (optional) C= [Land] Achtung: Geringe Abweichungen führen bereits dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese beim Kopieren aus der Willkommens-E-Mail gegebenenfalls falsch interpretiert werden (zum Beispiel unterschiedliche Hochkommata: ` , ` , ` ') Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mit kopiert wird. 
 Static subject override	
 ☐ Suppress "Unconsumed SDN" error	Diese Option ist im Standard inaktiv Bei individueller Konfiguration seitens SwissSign kann der Fall eintreten, dass beim Versuch ein Zertifikat zu beziehen im Static subject part Parameter mitgegeben werden, welche bereits durch SwissSign statisch vorgegeben sind. Daraus resultiert in der Regel folgende Fehlermeldung beim Zertifikatsbezug: Unconsumed SDN (i.e.: SDN attributes not needed and not utilized; please remove them and resubmit your request): o=... Durch Aktivieren dieser Option werden die beim Bezug mitgegebenen, obsoleten Parameter ignoriert und stattdessen die vorgegebenen, statischen Einträge der SwissSign verwendet. Somit kann der Zertifikatsbezug dennoch ungehindert stattfinden.
 Account name	Angabe des Benutzernamens.
 Product name	Angabe des gebuchten Produktes.

Sektion Domain specific parameters (optional)

Werden auf der SEPPmail Appliance mehrere E-Mail Domänen (**Managed domains** ^[24]) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden. Nach dem Speichern der Domänen spezifischen Option via **Save entries**, erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
 Domain	Angabe der E-Mail Domäne, für welche die beiden folgenden Parameter gültig sein sollen. Nur Domänen, welche beim Stellen des Antrags bei der Zertifizierungsstelle auch benannt, beziehungsweise später separat validiert wurden, dürfen eingetragen werden.

Parameter	Beschreibung										
	 Achtung: Die hier eingetragene Domäne muss unter Connectors ^[339] MPKI managed domains ^[340] ausgewählt sein, damit Zertifikate bezogen werden.										
 Product name	Angabe des gegebenenfalls vom Default parameters ^[364] abweichenden Product name. Dieser wird von SwissSign mit den Zugangsdaten bereitgestellt. Hinweis: Über die abweichenden Product names können pro Managed Domain ^[247] somit auch unterschiedliche Qualitätsgüten bezogen werden. Diese unterscheiden sich im Wesentlichen durch die Möglichkeiten beim Individualisieren des Static subject part und somit des im Zertifikat angezeigten Antragstellers: <table border="1"> <thead> <tr> <th>Zertifikat</th><th>möglicher Static subject part</th></tr> </thead> <tbody> <tr> <td>Personal</td><td></td></tr> <tr> <td>Gold-ID</td><td>E-Mail, Vor-/Nachname, Organisation, Land/Bundesland, (eventuell weitere Parameter)</td></tr> <tr> <td>Silber-ID (via MPKI)</td><td>E-Mail, Organisation</td></tr> <tr> <td>Silber-ID</td><td>E-Mail</td></tr> </tbody> </table>	Zertifikat	möglicher Static subject part	Personal		Gold-ID	E-Mail, Vor-/Nachname, Organisation, Land/Bundesland, (eventuell weitere Parameter)	Silber-ID (via MPKI)	E-Mail, Organisation	Silber-ID	E-Mail
Zertifikat	möglicher Static subject part										
Personal											
Gold-ID	E-Mail, Vor-/Nachname, Organisation, Land/Bundesland, (eventuell weitere Parameter)										
Silber-ID (via MPKI)	E-Mail, Organisation										
Silber-ID	E-Mail										
 Static subject part	Siehe Sektion Default parameters ^[364] Static subject part Achtung: Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese unter Umständen beim Kopieren falsch interpretiert oder bei manueller Eingabe falsch angegeben werden (zum Beispiel unterschiedliche Hochkommata: ‘, ’, ’) Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mit kopiert wird. 										

Sektion **Certificate**

Dient dem Authentifizieren gegenüber dem Zertifizierungsstellen Anbieter (SwissSign)

Parameter	Beschreibung
 PKCS12 identity file	Zertifikat für das Authentifizieren gegenüber der der Zertifizierungsstelle (SwissSign). Diese Datei wird von SwissSign bereit gestellt und ist mit einem Passwort versehen (siehe Parameter PKCS12 password) Ist der Zugang zur Zertifizierungsstelle erfolgreich, so erscheint an dieser Stelle die Meldung an operator certificate with valid password has been found.

Parameter	Beschreibung
	 Hinweis: Ab 30 Tage vor Ablauf des Operator Zertifikats wird eine Meldung im Daily Report ^[96] (siehe auch Groups ^[413] admin ^[413] und statisticsadmin ^[415]) eingefügt, und der Status des Daily Report ^[96] wird zu IMPORTANT geändert..
 PKCS12 password	Passwort um die im PKCS12 identity file enthaltenen „private keys“ freizuschalten. Auch dieses wird von SwissSign bereit gestellt.

Sektion Settings

Einstellungen für das automatische Erneuern von Zertifikaten.



Hinweis:

Die Laufzeit der Zertifikate der einzelnen Benutzers kann gegebenenfalls der Datei user-stats.csv, welche mit dem **Daily Report** ^[96] (siehe auch **Groups** ^[413] **statisticsadmin** ^[415]) mitkommt, entnommen werden.

Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
☐ Automatically renew expiring certificates if validity days left less than	Diese Option ist im Standard inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (Users ^[396]), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü Users ^[396] gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird <u>über Nacht (!)</u> abgearbeitet.  Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). <u>Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt.</u>  Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
 ☐ Automatically create certificates for active users without certificates	Diese Option ist im Standard inaktiv. Bezieht für alle existenten, aktiven Users ^[396], welche nicht im Besitz eines <u>gültigen (!)</u> Zertifikates sind, automatisiert <u>über Nacht (!)</u> ein Zertifikat. Als aktive Users ^[396] werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den State ^[396] inactive haben.

Parameter	Beschreibung
	 Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than
 Chain certificates (needed to sign e-mails)	Durch Klicken von Add or update... werden unter X.509 Root Certificates  die Zwischen-(Intermediate-)Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden.  Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

7.11 Administration

Dieses Menü beinhaltet Funktionen für das Verwalten des Systems.

Sektion License and registration

Ist eine gültige Lizenz vorhanden, so wird in diesem Abschnitt die Meldung „Valid License detected“ ausgegeben. Andernfalls die Appliance registriert werden. Im Normalfall geschieht das über die Schaltfläche **Register this device...**, welche das Untermenü **REGISTER THIS DEVICE** ^[376] öffnet.

Ist der Zugang zum SEPPmail Lizenzserver (update.seppmail.ch beziehungsweise support.seppmail.ch) über TCP Port 22 (siehe **Firewall / Router einrichten** ^[135] sowie **Sektion Proxy settings** ^[236] des Menüpunktes **System** ^[224]) nicht möglich, da es sich zum Beispiel um ein PCI gehärtetes oder ein DMZ abgeschottetes System handelt, so kann das Registrieren über **Import license file...** vorgenommen werden.

Sektion Update

View release notes zeigt das Untermenü **REVISION INFORMATION**, welches die komplette Versions-Historie sowie Inhalte verfügbarer und geplanter Updates der SEPPmail Appliance beinhaltet.

Weiterhin kann durch Klicken dieser Schaltfläche ein Abgleich mit dem SEPPmail Lizenzserver erzwungen werden, wodurch zum Beispiel kurzfristig angeforderte Lizenzänderungen sofort übernommen werden.



Achtung:

Nachdem in der **REVISION INFORMATION** auch zwingend vom Administrator zu beachtende Informationen (siehe **rote Schrift**) enthalten sein können, empfehlen wir dringend, diese Informationen vor jedem Update zu lesen.

Perform update (reboot automatically) startet bei verfügbarem Update den Download der Firmware vom SEPPmail Update Server und startet das System im Anschluss mit der neuen Firmware. Nach Klicken dieser Schaltfläche wechselt die Anzeige in das Menü **Home** ^[220]. Dort ist der Fortschritt des Downloads im Abschnitt **Firmware version** der **Sektion System** ^[220] zu verfolgen. Nach Abschluss des Downloads und erfolgreichem Reboot erscheint automatisch wieder das Login.



Hinweis:

Sollte der Zugriff auf die Administrationsoberfläche im Fehlerfall nicht mehr möglich sein, so kann ein Update auch über die Console (siehe auch **Rudimentäre Systembefehle** ^[189]).

Prefetch update (reboot manually) startet bei verfügbarem Update den Download der Firmware vom SEPPmail Update Server. Nach Klicken dieser Schaltfläche wechselt die Anzeige in das Menü **Home** ^[220]. Dort ist der Fortschritt des Downloads im Abschnitt **Firmware version** der **Sektion System** ^[220] zu verfolgen. Nach Abschluss des Downloads wird die neue Firmware mit dem nächsten (manuellen) Reboot übernommen.

Ist der Zugang zum SEPPmail Lizenzserver (update.seppmail.ch beziehungsweise support.seppmail.ch) über TCP Port 22 (siehe **Firewall / Router einrichten** ^[135] sowie **Sektion Proxy settings** ^[236] des Menüpunktes **System** ^[224]) nicht möglich, da es sich zum Beispiel um ein PCI gehärtetes oder ein DMZ abgeschottetes System handelt, so kann eine Update Datei über den Support angefordert werden. Diese Datei wird über **Upload** hochgeladen. Durch einem Neustart der SEPPmail Appliance wird die neue Firmware aktiv.



Hinweise:

In der Regel wird immer die aktuellste Firmware eingespielt. In seltenen Fällen ist jedoch das Update in mehreren Schritten notwendig, zum Beispiel wenn Abhängigkeiten bei den Konfigurationsdateien bestehen. In diesen Fällen muss die Appliance so oft aktualisiert werden, bis Sie auf dem aktuellen Stand ist (Meldung **You already have the latest version installed**).

Beim Update im Cluster ist folgendes zu beachten:

- Alle Maschinen sollten zeitnah aktualisiert werden, so dass lange Laufzeiten mit unterschiedlichen Versionsständen vermieden werden.
- Ist ein Update in mehreren Stufen notwendig (siehe oben), so ist immer auf allen Cluster-Partnern der gleiche Versionsstand herzustellen, bevor auf die nächst höhere Version aktualisiert wird.

Ein Beispiel für die oben genannte Situation wäre das Update von Version 7.0.4 auf 7.2. Hier wird zunächst nur die Version 7.1 zum Update angeboten. Erst wenn alle Maschinen diesen Stand haben darf auf die dann angebotene Version 7.2 aktualisiert werden.

- Ist nach einem Update ein erneutes generieren des Rulesets notwendig (dies wird mittels Klick auf **View release notes** angezeigt), so sind zunächst alle Maschinen auf einen einheitlichen Stand zu bringen. Danach muss das Ruleset an einer beliebigen Maschine aktualisiert werden (siehe **Mail Processing** [286] **Ruleset generator** [287] **Save and create ruleset**).
- Handelt es sich um einen **Frontend-/Backend-Cluster** [180], so sind zunächst die Frontend und erst dann die Backend-Maschinen zu aktualisieren, um zum Beispiel bei Sicherheitserweiterungen den Zugriff innerhalb des Clusters nicht zu gefährden.



Achtung:

Wird die Appliance nach dem Update auf eine Major-Version mit einem Ruleset einer Vorgängerversion betrieben, so erscheint unter **Home** [220] **System status** [220], sowie im **Daily Report** [96] (siehe **Groups** [413] **admin** [413] beziehungsweise **statisticsadmin** [415]) zusätzlich die Meldung **The current ruleset was created for another version. Please generate a new ruleset or update your special ruleset.**

Das heißt, nach dem Update auf eine Major-Version ist grundsätzlich das Ruleset neu zu generieren (siehe **Mail Processing** [286] **Ruleset generator** [287] **Save and create ruleset**).

Werden bei Custom Rulesets noch Befehle verwendet, welche nicht mehr unterstützt werden, wird beim Generieren des Rulesets ein entsprechender Fehler ausgegeben.



Sektion Maintenance



Achtung:

Zu Beachten gilt, dass alle hier aufgeführten Aktionen Wartungsoperationen sind und somit mit einem Neustart der Appliance verbunden sein können beziehungsweise sind.



Parameter	Beschreibung
 Support connection	Sollten auf der SEPPmail Appliance unerwartet Probleme auftauchen, so kann im Rahmen einer Störungsmeldung mittels Connect eine Support Verbindung zum Hersteller aufgebaut werden. Hierdurch wird eine SSH Verbindung (TCP Port 22) zum SEPPmail Support Server aufgebaut. Für das Etablieren einer Support Connection ist zwingend die Eingabe der Ticket Nummer erforderlich, welche beim Öffnen einer Störungsmeldung über die entsprechenden Support-Kanäle mitgeteilt wurde.  Hinweis: Solange die Support Connection aufgebaut ist, wird dies - unabhängig vom Menü - in der Kopfleiste der Administrationsoberfläche durch folgenden Text angezeigt: Support connection is established: Please disconnect under 'Administration' if not needed anymore

Parameter	Beschreibung
	 Hinweis: Sollte der Zugriff auf die Administrationsoberfläche nicht mehr möglich sein, so kann die Support Connection auch über die Console gestartet werden (siehe auch Rudimentäre Systembefehle ^[189]).
 Mail processing	Mit Klicken von Preempt wird der E-Mail Verkehr auf der Appliance angehalten. Eingehende E-Mails werden mit dem SMTP Code 422 temporär abgewiesen. Während Preempt aktiv ist wird folgende Meldung Mail processing is preempted. Please restore it under 'Administration' if not needed anymore. in der Statusleiste angezeigt. Die Einstellung bleibt auch nach einem Neustart der SEPPmail Appliance erhalten. Über Restore wird die normale Funktion der SEPPmail Appliance wiederhergestellt.  Hinweis: Mit dieser Funktion wird die E-Mail Queue angehalten, zum Beispiel während eines Updates im Cluster ^[383] - auch wenn dies nicht erforderlich ist. Kommen im Cluster ^[383] virtuelle IPs zum Einsatz (siehe auch System ^[224] IP ALIAS Addresses ^[226]), kann der E-Mail Verkehr vor einem Update gegebenenfalls bereits auf Netzwerkebene umgeleitet werden. Hierfür kann die „Priority“ temporär auf „Backup“, herabgestuft werden.
 Clone device	Erstellt einen Klon einer anderen SEPPmail Appliance. Hierfür ist die Cluster-ID (siehe Cluster ^[383] Prepare for cluster ^[383] Download cluster identifier) der zu klonenden SEPPmail Appliance - also der Quellmaschine - herunterzuladen und über die „Datei-Auswahl-Schaltfläche“ unter Cluster ID of original device: der Zielmaschine bereitzustellen. Unter IP Address: ist dann die IP- Adresse der Quellmaschine einzugeben. Der Klonprozess wird im Anschluss durch Klicken von Start cloning... gestartet.  Hinweis: Vor dem Klonen haben idealerweise Quell-, als auch Zielmaschine denselben Firmware-Stand. Sind unterschiedliche Firmwarestände nicht zu vermeiden, da zum Beispiel das Update auf der Quellmaschine aufgrund zu geringer Partitionsgrößen verweigert wird, ist das Klonen von einem niedrigeren Versionsstand auf einen höheren zulässig. Dabei ist jedoch das Delta der Versionsstände möglichst gering zu halten. Das heißt, die Quellmaschine ist auf den höchstmöglichen Firmware-Stand zu bringen. Für die Zielmaschine kann immer das unter https://downloads.seppmail.com/index.php/images/ verfügbare Image verwendet werden. Keinesfalls darf eine Quellmaschine mit einem höheren Versionsstand auf ein Ziel mit niedrigeren Versionsstand geklont werden!  Achtung: Handelt es sich bei der Quellmaschine um Hardware, so kann die Device ID ^[220] nicht übernommen werden! Aus diesem Grund ist vor dem Klonen ein Ticket an support@seppmail.de unter Nennung der bestehenden License ID ^[220] zu erstellen. Der Support überträgt dann die Lizenzdaten auf eine neue License ID und teilt diese im Ticket mit. Nach dem Aufsetzen der virtuellen Appliance ist diese zu registrieren (Administration ^[369] License and registration ^[369] REGISTER THIS DEVICE ^[376]) und die über den Support erhaltene neue License ID ^[220] unter Activation Code ^[376] einzugeben.

Parameter	Beschreibung
	Da sich das Ändern der License ID [220] insbesondere im Cluster [383] auswirkt, ist in einer Cluster-Konfiguration die Quellmaschine ZWINGEND vor dem Klonen aus dem Cluster [383] zu entfernen (siehe Remove from cluster [385] remove this device from cluster!). Der Klon kann nach Abschluss des Prozesses dem Cluster [383] wieder hinzugefügt werden (siehe Add this device to existing cluster [383]).  Achtung: Ist auf der Quellmaschine Large File Transfer (LFT) [107] aktiv, so ist vor dem Klonen darauf zu achten, dass der Ziemaschine ebenfalls LFT Speicher von mindestens derselben Größe wie der Quellmaschine (wenigstens aber so groß wie unter Sizing [78] gefordert) zugeordnet ist.  Achtung: Beim Klonen • werden alle Daten auf derjenigen SEPPmail Appliance gelöscht, auf welcher dieser Prozess gestartet wird (Zielmaschine). • werden alle Daten der Quellmaschine - also auch IP addresses [225], Device ID [220] (Ausnahme Hardware, siehe oben), SSL [319] Zertifikate, License [220]-daten und so weiter - auf die Ziemaschine übernommen. • wird die Quellmaschine nach Abschluss des Klon-Prozesses automatisiert heruntergefahren, unter anderem um doppelte IP-Adressen im Netzwerk zu vermeiden.
 Reboot	Reboot... startet das System neu. Es erscheint ein Dialog zur Eingabe eines Sicherheitscodes, wodurch ein versehentlicher Neustart verhindert wird.  Hinweis: Sollte der Zugriff auf die Administrationsoberfläche nicht mehr möglich sein, so kann ein Neustart auch über die Console gestartet werden (siehe auch Rudimentäre Systembefehle [189]).
 Shutdown	Shut down... fährt das System herunter. Es erscheint ein Dialog zur Eingabe eines Sicherheitscodes, wodurch ein versehentliches Herunterfahren verhindert wird.
 Resize large file storage	Durch Resize... wird ein Ändern der LFT Partitionsgröße eingeleitet. Im Folgemenü erscheint ein Dialog, in welchem zur Eingabe eines Sicherheitscodes aufgefordert wird. Nach Eingabe des Codes fährt die Appliance herunter. Bei virtuellen Systemen ist nun die virtuelle Festplatte zu erweitern und das System erneut zu starten, um den Vorgang abzuschließen. Bei Hardware müssten vor dem Durchführen des Resizings die einzelnen Raid-Platten nach und nach durch Größere ersetzt und wiederhergestellt werden. Sind alle Platten ersetzt, kann der eigentliche Prozess durchgeführt werden.  Achtung: Generell sollte vor dieser Aktion unbedingt ein Backup erstellt werden.

Parameter	Beschreibung
 Factory reset	Perform factory reset... setzt das System auf Werkzustand zurück. Es erscheint ein Dialog zur Eingabe eines Sicherheitscodes in umgekehrter Schreibweise um ein ungewolltes Zurücksetzen zu verhindern.  Hinweis: Der Zugriff auf die GUI sollte bereits unmittelbar nach Start des Resets nicht mehr möglich sein. Im Konsolenfenster der Appliance bleibt - sofern diese Option gewählt wurde - während des zehnmöglichen Überschreibens der Login-Prompt erhalten. Nach Abschluss des Resets fährt die Appliance herunter. Wird die Maschine danach neu gestartet, so ist im Konsolenfenster wieder der Hinweis zu sehen, wie in Kapitel Consolen Login ^[14] genannt.

Sektion Backup



Hinweis:

Das Backup ist maschinenbezogen und beinhaltet somit die komplette Konfiguration.

Parameter	Beschreibung
 Backup	Download startet das Herunterladen, Send Backup den E-Mail Versand (siehe Groups ^[413] backup (Backup Operator) ^[413] der Backup-Datei. Diese Datei beinhaltet ausschließlich Konfiguration und Schlüsselmaterial der SEPPmail Appliance. Voraussetzung für ein Backup ist ein gesetztes Backup Passwort, welches via Change password gesetzt beziehungsweise geändert werden kann.
 Restore	Der Restore wird über Import backup file... ^[379] initiiert.  Hinweis: In einem Cluster ^[383] darf kein Restore auf einem einzelnen Cluster-Partner auf diese Art durchgeführt werden. Bei Bedarf ist eine ausgefallene Maschine wie unter Cluster ^[383] Cluster members Device ID beschrieben auf der verbleibenden, intakten Maschine zunächst aus dem Cluster ^[383] zu entfernen. Im Anschluss kann eine neue, virtuelle Maschine aufgesetzt und dem Cluster ^[383] wieder hinzugefügt werden (siehe Add this device to existing cluster ^[383]).
 Backup using scp	Soll das Backup per SCP abgeholt werden, so kann über das Eingabefeld ein entsprechender public key (dieser beginnt mit „ssh-rsa “ und endet mit „=<Beschreibung>“) eingegeben werden, welcher über die Schaltfläche Save public key importiert wird. Damit wird der Zugriff auf das System über den Betriebssystem eigenen Benutzer „backup“ für das Abholen des täglich um Mitternacht bereitgestellten Backups (backup.tgz) gewährleistet. Durch Eingabe eines weiteren Schlüssels, wird der bestehende Schlüssel jeweils gelöscht. Das heißt, wird Save public key ohne die Eingabe eines Schlüssels gedrückt, so wird der Schlüssel gelöscht.

**Hinweis:**

Mitglieder der Gruppe **backup** ^[413] (siehe **Groups** ^[413]) erhalten täglich um Mitternacht die Sicherungsdatei per E-Mail zugesandt. Voraussetzung ist natürlich ein gesetztes Backup Passwort.

Zu beachten gilt, dass Backups des jeweils vorherigen Firmware Standes in den aktuelle Firmware Stand eingespielt werden können. Dabei sollte im Anschluss unbedingt das Ruleset neu generiert werden (siehe **Mail Processing** ^[286] **Ruleset generator** ^[287] **Save and create ruleset**). Backups neuerer Firmware Stände dürfen keinesfalls auf Maschinen mit älterem Firmwarestand eingespielt werden.

**Sektion Bulk import**

In dieser Sektion werden zahlreiche (Massen-)Importfunktionen bereit gestellt.

Auf mandantenfähigen Systemen können die importierten User, beziehungsweise privaten Schlüssel wahlweise automatisch anhand der E-Mail-Domänen oder manuell zugeordnet werden.

GINA-User müssen immer manuell zugeordnet werden.

Parameter	Beschreibung
 Import users (CSV)	Über die Schaltfläche Import können Encryption/Signature-Benutzer mittels csv-Datei mit dem Aufbau „USERID;NAME;EMAIL;PASSWORD“ importiert werden. Dabei ist die Vergabe eines Passwortes optional (siehe Users ^[395]). Bei Benutzern, welche durch die SEPPmail Appliance automatisch generiert wurden entsprechen USERID und EMAIL jeweils der E-Mail Adresse des Benutzers, was die Einmaligkeit garantiert.
 Import GINA users (CSV)	Über die Schaltfläche Import können GINA-Benutzer mittels csv-Datei mit dem Aufbau „EMAIL;PASSWORD;NAME;MOBILE“ importiert werden. Die Angabe einer Mobilfunk-Nummer ist dabei optional. Denkbar wäre zum Beispiel die Eingabe einer Kundenliste, bei welcher die Postleitzahl des Kunden als Initialpasswort dient.
 Import OpenPGP key pairs	Über die Schaltfläche Import ist das Importieren von OpenPGP Schlüsselpaaren möglich. Sollte für die im Schlüsselpaar vorhandene E-Mail Adresse noch kein Benutzer auf der SEPPmail Appliance vorhanden sein, so wird dieser automatisch durch diese Aktion angelegt. Der Import ist sowohl über eine Datei, als auch durch Einfügen als Text, jeweils unter Angabe der passenden Passphrase möglich. Durch das Aneinanderreihen von Schlüsselpaaren - egal ob als Datei oder als Text - ist auch ein Massenimport möglich. Ebenso können einzelne Schlüsseldateien aus einer unverschlüsselten ZIP-Datei ohne Ordnerstruktur importiert werden. Bei einem Massenimport ist darauf zu achten, dass alle Schlüssel dieselbe Passphrase haben!
 Import X.509 keys and certificates	Die Schaltfläche Import ruft das Untermenü BULK IMPORT PKCS#12 CERTIFICATE STRUCTURE ^[380] auf, über welches der Massen-Import von PKCS#12 Dateien ermöglicht wird.

**Sektion Bulk export**

Dient dem Exportieren von öffentlichen Schlüsseln interner Benutzer (**Users** ^[395]).

Somit können diese bei Bedarf zum Beispiel gesammelt an einen Kommunikationspartner weitergegeben werden.

Parameter	Beschreibung
 Export OpenPGP public keys	Über Export werden sämtliche gültigen „OpenPGP public keys“ der internen Benutzer (Users) in eine Datei namens public_openpgp_keys.zip heruntergeladen.
 Export X.509 certificates	Über Export werden sämtliche gültigen S/MIME Zertifikate der internen Benutzer (Users) in eine Datei namens public_smime_cert.zip heruntergeladen.

7.11.1 Register This Device

Dieses Sub-Menü wird aus **Administration** ^[369] **License and Registration** ^[369] aufgerufen.

Die Registrierungsdaten sollten sorgfältig ausgefüllt werden, da unter anderen bei CERT-Meldungen, von welchen die SEPPmail Appliance betroffen ist, die hier genannten Kontakte bei Bedarf informiert werden. Werden mehrere Appliances für den selben Kunden registriert, so ist darauf zu achten, dass die Eingaben identisch gemacht werden.

Sektion **Activation code**



Hinweis:

Diese Sektion erscheint nur bei virtuellen Appliances!
Bei Hardware Appliances ist die License ID immer statisch an die Hardware gebunden. Eine Eingabe ist deshalb nicht erforderlich.

Parameter	Beschreibung
 Enter the device ID of this virtual appliance from your license document. Leave empty to get a test license	Ist bereits das „SEPPmail License Certificate“ der Kauflizenz vorhanden, so ist die darauf befindliche „Device-ID“ in dieses Feld in der Form XXXX-XXXX-XXXX einzutragen. Somit werden die erworbenen Lizenzen auf die Appliance übertragen. Wird dieses Feld leer gelassen, so zieht die Appliance automatisch eine 30-tägige Testlizenz.  Hinweis: Wurde eine Testlizenz bezogen und soll diese im Anschluss in die Produktion übernommen werden, so ist beim Bestellen unbedingt die Device ID ^[220] aus der Sektion System ^[220] des Menüs Home ^[220] mit anzugeben.  Hinweis: Wurde die „Device-ID“ eines „SEPPmail License Certificate“ bereits einmal verwendet, so lässt sich dieses - zum Beispiel nach einer Neuinstallation - kein zweites mal Verwenden. In diesem Fall ist der Support zu kontaktieren.

Sektion **Customer information**

Eingabefeld für die Kundendaten.

Parameter	Beschreibung
 Company	Pflichtfeld. Firmenname des Kunden.
 Address 1	Pflichtfeld. Adresse des Kunden.
 Address 2	Optional. Zusätzliches Adressfeld.
 City	Pflichtfeld. Stadt des Kunden.

Parameter	Beschreibung
 Postal code	Pflichtfeld. Postleitzahl des Kunden.
 Country	Pflichtfeld. Land des Kunden.
 First name	Pflichtfeld. Vorname des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Kunden.
 Last name	Pflichtfeld. Nachname des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Kunden.
 E-mail address	Pflichtfeld. E-Mail Adresse des Ansprechpartners beziehungsweise idealerweise der zuständigen Abteilung beim Kunden.
 Phone number	Pflichtfeld. Telefonnummer in der Form „+<Ländercode> <Vorwahl ohne null„0“> <Rufnummer inklusive Durchwahl>“ des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Kunden.
 Mobile phone number	Optional. Mobilfunknummer in der Form „+<Ländercode> <Vorwahl ohne null„0“> <Rufnummer inklusive Durchwahl>“ des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Kunden.

Sektion Reseller information

Eingabefeld für die Daten des SEPPmail Partners

Parameter	Beschreibung
 Company	Pflichtfeld. Firmenname des Partners.
 Address 1	Pflichtfeld. Adresse des Partners.
 Address 2	Optional. Zusätzliches Adressfeld.
 City	Pflichtfeld. Stadt des Partners.
 Postal code	Pflichtfeld. Postleitzahl des Partners.
 Country	Pflichtfeld. Land des Partners.
 First name	Pflichtfeld. Vorname des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Partners.
 Last name	Pflichtfeld. Nachname des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Partners.
 E-mail address	Pflichtfeld. E-Mail Adresse des Ansprechpartners beziehungsweise idealerweise der zuständigen Abteilung beim Partners.
 Phone number	Pflichtfeld. Telefonnummer in der Form „+<Ländercode> <Vorwahl ohne null„0“> <Rufnummer inklusive Durchwahl>“ des Ansprechpartners beziehungsweise der zuständigen Abteilung Partners.

Parameter	Beschreibung
 Mobile phone number	Optional. Mobilfunknummer in der Form „+<Ländercode> <Vorwahl ohne null„0“> <Rufnummer inklusive Durchwahl>“ des Ansprechpartners beziehungsweise der zuständigen Abteilung Partners.

Über das Klicken der Schaltfläche **Send** wird der Registrierungsprozess abgeschlossen.

7.11.2 Restore

Dieses Sub-Menü wird aus **Administration**  **Backup**  **Restore** mittels **Import backup file...** aufgerufen.

Sektion **Restore**

Parameter	Beschreibung
 Backup File	Über die Browser-Schaltfläche „Datei auswählen“ wird die wiederherzustellende Backup-Datei ausgewählt. Hinweis: Generell sollten nur Backups eingespielt werden, welche mit dem selben oder vorherigen Firmwarestand erzeugt wurden. Hinweis: Wird der Restore nicht auf derselben Maschine durchgeführt, auf welcher die Backup-Datei erstellt wurde, sollte bei virtuellen Maschinen die MAC-Adresse der ersten virtuellen Netzwerkkarte noch <u>vor dem initialen Start</u> auf den Wert der ausgefallenen Maschine angepasst werden!
 Options	
 ☐ Keep current network setting instead of restoring them from the backup	Diese Option ist im Standard inaktiv. Das Einspielen eines Backups stellt die Maschine zu 100% in dem Zustand wieder her, wie er - mit Ausnahme der Log-Dateien - zum Zeitpunkt des Erstellens des Backups war. Durch Aktivieren dieser Option bleiben die Netzwerk-Einstellungen aus dem Menü System  (Advanced view) vom Restore unberührt.
 Password	Backup-Passwort, welches zum Zeitpunkt des Erstellens des Backups gültig war (siehe auch Administration  Backup  Change Password).

7.11.3 Bulk Import OpenPGP Keys

Dieses Sub-Menü wird aus **Administration**  **Bulk import**  **Import OpenPGP key pairs** aufgerufen.

Sektion **Key data**

Parameter	Beschreibung
 Passphrase	Angabe des Passworts, mit welchem der jeweils der private Schlüssel der zu importierenden OpenPGP Schlüsseldateien gesichert ist. Somit wird für den Massen-Import vorausgesetzt, dass die zu importierenden Dateien bereits beim Bezug oder Export von einem anderen System, alle <u>mit derselben Passphrase geschützt</u> wurden!
 Key file	Über die Browser-Schaltfläche „Datei auswählen“ wird die unverschlüsselte ZIP-Datei ohne Ordnerstruktur ausgewählt, welche die Schlüsseldateien (Dateiendung meist ASC) mit <u>jeweils identischer</u> 

Parameter	Beschreibung	
	Passphrase für den privaten Schlüssel enthält. Hinweis: Enthält die ZIP-Datei weitere Dateien, mit anderen als den erwarteten Dateiformaten, beziehungsweise Inhalten, so werden diese ignoriert. 	Hinweis: Sollte für die im Schlüssel vorhandene E-Mail Adresse noch kein Benutzer auf der SEPPmail Appliance vorhanden sein, so wird dieser automatisch durch diese Aktion angelegt. Bei diesen automatisch generierten Benutzern wird als User ID, sowie User Name die E-Mail Adresse verwendet. Soll User ID, beziehungsweise User Name individuell angegeben werden, so müssen die Benutzer vor dem Import der OpenPGP Schlüssel angelegt werden. Hierzu bietet sich im Vorfeld das Verwenden der Funktion Import Users (CSV) an.
 or key as string	Eingabefeld für OpenPGP Schlüsselpaare als Text. Dieser sollte in etwa so aussehen: <pre>-----BEGIN PGP PRIVATE KEY BLOCK----- # Privater Schlüssel -----END PGP PRIVATE KEY BLOCK----- -----BEGIN PGP PUBLIC KEY BLOCK----- # Öffentlicher Schlüssel -----END PGP PUBLIC KEY BLOCK-----</pre>	

Sektion **Advanced options**

Parameter	Beschreibung
 Customer (optional)	Nur in mandantenfähigen Systemen vorhanden.
	Auswahl des Mandanten, welchem die gegebenenfalls durch den Massen-Import neu hinzugefügten Users ^[369] zugeordnet werden sollen
 Let system determine customer automatically	Diese ist die Standard-Auswahl. Durch Aktivieren dieser Option werden User ^[396] jeweils dem Mandanten (Customers ^[494]) zugeordnet, welchem auch die E-Mail Domäne der E-Mail-Adresse aus dem Schlüsselmaterial zugeordnet ist.

Über **Import** wird das angegebene Schlüsselmaterial auf die Appliance hochgeladen.

7.11.4 Bulk Import PKCS#12 Certificate Structure

Dieses Sub-Menü wird aus **Administration** ^[369] **Bulk import** ^[374] **Import X.509 keys and certificates** aufgerufen.

Sektion **Certificate data**

Parameter	Beschreibung
 Passphrase	Angabe des Passworts, welches für den Import der PKCS#12 Schlüsseldateien erforderlich ist. Somit wird für den Massen-Import vorausgesetzt, dass die zu importierenden Dateien bereits beim Bezug oder Export von einem anderen System, alle <u>mit derselben Passphrase geschützt</u> wurden!
 PKCS#12 Files (unprotected ZIP File without directory structure)	Über die Browser-Schaltfläche „Datei auswählen“ wird die unverschlüsselte ZIP-Datei ohne Ordnerstruktur ausgewählt, welche die Zertifikatsdateien (Dateiendung P12 oder PFX) mit <u>jeweils identischer Passphrase</u> für den privaten Schlüssel enthält.  Hinweis: Enthält die ZIP-Datei weitere Dateien, mit anderen als den erwarteten Dateiformaten (P12 oder PFX), so werden diese ignoriert. Sollte für die im Schlüssel vorhandene E-Mail Adresse noch kein Benutzer auf der SEPPmail Appliance vorhanden sein, so wird dieser automatisch durch diese Aktion angelegt. Bei diesen automatisch generierten Benutzern wird als User ID die E-Mail Adresse verwendet. Je nach Güte des Zertifikats wird als User Name der im Zertifikat eingetragene Name verwendet. Enthält das Zertifikat keinen entsprechenden Namen, so wird auch hier die E-Mail Adresse eingetragen. Ist dies nicht gewünscht, so müssen die Benutzer vor dem Import der S/MIME Keys angelegt werden. Hierzu bietet sich im Vorfeld das Verwenden der Funktion Import Users (CSV) an.

Sektion Advanced options

Gibt den Verwendungszweck der zu importierenden PKCS#12 Dateien an.

Parameter	Beschreibung
 ☒ Allow decryption	Im Standard ist diese Option aktiv. Zeigt an, ob die zu importierenden PKCS#12 Schlüssel für das Entschlüsseln von eingehenden E-Mails an den jeweiligen Antragsteller (siehe auch USER 'USER@DOMAIN.TLD' ^[398] X.509 CERTIFICATE 'details' ^[404] Issued to ^[404]) verwendet werden sollen.
 ☒ Allow signing	Im Standard ist diese Option aktiv. Zeigt an, ob die zu importierenden PKCS#12 Schlüssel für das Signieren von ausgehenden E-Mails an des jeweiligen Antragstellers (siehe auch USER 'USER@DOMAIN.TLD' ^[398] X.509 CERTIFICATE 'details' ^[404] Issued to ^[404]) verwendet werden sollen.
 Customer (optional)	Nur in mandantenfähigen Systemen vorhanden.
 ☐	Auswahl des Mandanten, welchem die gegebenenfalls durch den Massen-Import neu hinzugefügten Users ^[398] zugeordnet werden sollen
 Let system determine customer automatically	Dies ist die Standard-Auswahl. Durch Aktivieren dieser Option werden User ^[398] jeweils dem Mandanten (Customers ^[494]) zugeordnet, welchem auch die E-Mail Domäne der E-Mail-Adresse im Antragsteller des jeweiligen Zertifikats zugeordnet ist.

Über **Import** wird das angegebene Schlüsselmaterial auf die Appliance hochgeladen.

**Hinweis:**

Welche Zertifikate Importiert werden können ist von der Auswahl unter **ADVANCED SETTINGS** ⁴⁷⁸ **Advanced settings** ⁴⁷⁸ **Policies** ⁴⁷⁹ **Refuse import of certificates with a signature algorithm using SHA-1 or lower** ⁴⁷⁹ abhängig.

7.12 Cluster

Dieses Menü bietet die Möglichkeit mehrere Appliances zu einem Cluster zusammen zu fügen.

Das Verhalten des Clusters (zum Beispiel aktiv/aktiv, Aktiv/passiv und so weiter) ist dabei stark von den vorgenommenen Systemeinstellungen (siehe unter Anderem [System](#)^[224], [IP ALIAS addresses](#)^[226] und [SMTP loadbalancer](#)^[227]) abhängig.

Maschinen, welche dem Cluster hinzugefügt werden übernehmen die Einstellungen der Basis-Maschine. Das heißt alle eventuell bereits vorgenommenen Einstellungen werden überschrieben.

Ausgenommen vom Synchronisieren im Cluster bleiben die Menüpunkte, welche maschinenbezogene Daten enthalten, wie [System](#)^[224], [EXTENDED POSTFIX MTA SETTINGS](#)^[287], [SSL](#)^[319], das Root-Zertifikat aus [CA](#)^[328], [Logs](#)^[388] und [Statistics](#)^[394].



Hinweis:

Wird [LFT](#)^[107] (siehe auch [Home](#)^[220], [License](#)^[220], [Large File Transfer \(LFT\) licenses](#)^[227], sowie [GINA Domains](#)^[416], [Domains](#)^[416], [CHANGE GINA SETTINGS FOR](#)^[423], [Large File Transfer](#)^[439]) verwendet, so muss der zusätzliche LFT Speicher auf allen Cluster-Partnern (auch Frontend-Systemen) bereit gestellt werden.



Achtung:

Für das Bilden eines Clusters ist zwingend darauf zu achten, dass die Maschinen

- den gleichen Firmware Stand haben (siehe [Home](#)^[220], [System](#)^[220], [Firmware version](#)^[220])
- NTP aktiviert haben und den selben NTP-Server(pool) verwenden (siehe [System](#)^[224], [Advanced view](#), [Time and Date](#)^[240], [Set remote NTP Server](#)^[240])



Sektion [Prepare for cluster](#)

Spalte	Beschreibung
 Cluster password (neu in 12.1)	Eingabe des Passworts zum Schutz des privaten Schlüssels.
Download cluster identifier lädt das Zertifikat, beziehungsweise Schlüsselpaar für das Herstellen der SSH Verbindung vom zukünftigen Cluster-Partner zur Basis-Maschine herunter. In der Regel heißt diese Datei „clusterid.txt“. Das heißt diese Aktion wird an der Maschine vorgenommen, von welcher die Einstellungen übernommen werden sollen.	



Achtung:

Sollen mehrere Maschinen einem Cluster hinzugefügt werden, so muss dies unbedingt nacheinander passieren.
Werden mehrere Maschinen parallel hinzugefügt, kann dies zum Verlust der Konfiguration führen!



Sektion [Add this device to existing cluster](#)

Diese Sektion erscheint nur dann, wenn die SEPPmail Appliance nicht bereits in einem Cluster-Verbund integriert ist und dient dem Hinzufügen zu einem Cluster.

**Achtung:**

Alle Einstellungen, welche nicht maschinenbezogen sind (siehe **Sektion Prepare for cluster** ³⁸³), werden durch diese Aktion mit den Einstellungen der Basis-Maschine überschrieben. Sollten Unsicherheiten bezüglich der Aktion bestehen, empfiehlt sich dringend zuvor ein manuelles Backup zu erstellen (siehe **Administration** ³⁶⁹ **Backup** ³⁷³).

Parameter	Beschreibung	
 Cluster identifier	Über die Browser-Schaltfläche „Datei auswählen“ wird das für die SSH Verbindung benötigte Zertifikat der Basis-Maschine „clusterid.txt“ (siehe Sektion Prepare for cluster ³⁸³) ausgewählt.	
 Cluster member IP	An dieser Stelle wird die physikalische IP-Adresse (kein Alias!, also virtuelle Adresse) der Basis-Maschine über welche die Cluster Kommunikation stattfinden soll sowie der zu verwendende Port (im Standard Port 22 für das SSH-Protokoll) angegeben.	 Achtung: Das Angeben eines Port: ist ausschließlich dann erforderlich, wenn an einer zwischengelagerten Komponente (zum Beispiel Firewall) ein Port-Mapping erfolgt. Die Cluster member IP horcht immer auf Port 22 SSH (Standardeintrag).
 IP address of this device	An dieser Stelle wird die physikalische IP-Adresse (kein Alias!, also virtuelle Adresse, siehe System ²²⁴ IP ALIAS addresses ²²⁶) dieser Maschine über welche die Cluster Kommunikation stattfinden soll sowie der zu verwendende Port (muss identisch mit dem unter Cluster member IP eingegebenen sein) angegeben.	
 Connect	Über die Schaltfläche Start wird die Maschine dem Cluster hinzugefügt.	

**Sektion Cluster members**

Diese Sektion erscheint nur dann, wenn die SEPPmail Appliance bereits Bestandteil eines Cluster ist. In diesem Fall werden alle Cluster-Partner mit den folgenden Daten gelistet:

Spalte	Beschreibung
Device ID	Zeigt die „Device ID“ des jeweiligen Cluster-Partners an. Das Entfernen eines entfernten Cluster-Partners kann durch Klicken auf die „Device ID“ erfolgen. Hierdurch öffnet ein weiteres Menü, in welchem dann der Server über die Schaltfläche Remove device from cluster entfernt werden kann. Die Datenbank bleibt mit dem zuletzt synchronisierten Stand auf dem entfernten System erhalten. Das Entfernen der lokalen Maschine aus dem Cluster-Verbund erfolgt wie in Sektion Remove from cluster ³⁸⁵ beschrieben.
IP address	Zeigt die „IP-Adresse“ des jeweiligen Cluster-Partners an, welche für die Cluster Kommunikation konfiguriert wurde.

Spalte	Beschreibung
 Port	Zeigt den Kommunikations-Port an (im Standard Port 22 für das SSH-Protokoll)
 Status	Arbeitet der Cluster korrekt, so steht hier "OK (XXXX entries in remote database, XXXX entries in local Database)" wobei die Anzahl „XXXX“ identisch sein sollte.
 Comment	Zeigt den für den Cluster-Partner definierten Kommentar an (siehe System Comment ^[224])
 Location	Zeigt den für den Cluster-Partner definierten Standort an (siehe System Comment ^[224])

Sektion Remove from cluster

Durch Klicken der Schaltfläche **remove this device from cluster** wird die Maschine aus dem Cluster herausgenommen. Die lokale Datenbank bleibt dabei erhalten und hat den Stand des letzten Synchronisierens im Cluster.

Sektion Add this device as frontend server (no local database)

Diese Sektion erscheint nur dann, wenn die SEPPmail Appliance nicht bereits in einem Cluster-Verbund integriert ist. Sie dient dem Hinzufügen der Maschine als Frontend-Server zu einer anderen Maschine oder einem Cluster. Als Frontend-Server wird ein Cluster-Partner ohne lokale Datenbank bezeichnet.

Sollte aufgrund von Revisionsvorgaben die SEPPmail Appliance in einer DMZ platziert werden müssen, in welcher keine Datenhaltung - in diesem Fall in erster Linie Schlüsselmateriale - erlaubt ist, so kann über diese Funktion ein Auftrennen zwischen dem Datenbanksystem (backend) und dem E-Mail verarbeitenden System (frontend) vollzogen werden. Häufig wird diese Variante auch zum Abtrennen des GINA verarbeitenden Teils verwendet.

Der Frontend-Server erhält in diesem Fall jeweils nur die diejenigen Daten vom Backend-Server, welche aktuell zum Verarbeiten einer E-Mail benötigt werden. Der Backend-Server steht außerhalb der DMZ und hält die Daten in seiner Datenbank.

Frontend-Server werden nicht in der **Sektion Cluster members** der Backend-Systeme angezeigt.

Parameter	Beschreibung
 Cluster identifier	Über die Browser-Schaltfläche „Datei auswählen“ wird das für die SSH Verbindung benötigte Zertifikat der Basis-Maschine „clusterid.txt“ (siehe Sektion Prepare for cluster ^[383]) ausgewählt.
 Existing appliance IP	An dieser Stelle wird IP-Adresse der Backend-Maschine über welche die Cluster Kommunikation stattfinden soll sowie der zu verwendende Port (im Standard Port 22 für das SSH-Protokoll) angegeben. Existiert ein „Backend-Cluster“, so kann an dieser Stelle eine virtuelle IP-Adresse (siehe System IP ALIAS addresses ^[224]) verwendet werden. Es besteht aber auch die Möglichkeit, der Frontend-Maschine weitere Backend-Server im Nachhinein hinzu zu fügen (siehe Sektion Add additional backend ^[384]) falls keine virtuelle IP-Adresse verfügbar ist.
 Connect	Über die Schaltfläche Start wird die Maschine dem Cluster hinzugefügt.

**Hinweis:**

Vom Frontend wird ausschließlich die Kommunikation zum Backend via Port 22 SSH und zur jeweiligen Server IP Address (siehe **Mail System** ^[247] **Managed domains** ^[247]) via Port 25 SMTP benötigt.

**Achtung:**

(geändert in 12.0)

Nach Änderungen in den Menüs **GINA Domains** ^[416] beziehungsweise **Mail Processing** ^[286] müssen diese auf jedem Frontend separat erneut angewendet (**Save** / **Generate ruleset**) werden. Änderungen der Konfiguration des Backend Systems werden am Frontend System bis zu zehn Minuten später aktiv.

**Sektion Remote LDAP server**

Diese Sektion erscheint nur dann, wenn die SEPPmail Appliance als Frontend-Server bereits Bestandteil eines Clusters ist. In diesem Fall werden alle Backend-Server mit den folgenden Daten gelistet:

Spalte	Beschreibung
 IP address	Zeigt die „IP-Adresse“ der jeweiligen LDAP-(Backend-)Maschine an. Das Entfernen eines LDAP-(Backend-)Servers erfolgt durch klicken auf die IP-Adresse. Hierdurch öffnet ein weiteres Menü, in welchem dann der Server über die Schaltfläche Remove device from cluster entfernt werden kann. Das Entfernen der lokalen Maschine als Frontend-Server erfolgt wie in Sektion Detach from LDAP server ^[386] beschrieben.
 Port	Zeigt den Kommunikations-Port an (im Standard Port 22 für das SSH-Protokoll)
 Status	Arbeitet der Cluster korrekt, so steht hier "OK (XXXX entries in remote database)"

**Sektion Detach from LDAP server**

Über die Schaltfläche **Detach** wird die SEPPmail Appliance als Frontend-Server entfernt. Dabei wird eine leere Lokale Datenbank auf dem System angelegt.

**Hinweis:**

Das Abkoppeln eines Frontend-Servers wird durch einen automatischen Neustart der Appliance abgeschlossen.

**Sektion Add additional backend**

Sollen mehrere Backend-Server aus einem Backend-Cluster für LDAP-Anfragen herangezogen werden, ohne dass eine virtuelle IP-Adresse zu diesem Zweck bereit gestellt wurde, so kann über diese Option jeder Backend-Server separat eingebunden werden.

Parameter	Beschreibung
 Existing appliance IP	An dieser Stelle wird die physikalische IP-Adresse einer weiteren Backend-Maschine sowie der zu verwendende Port (im Standard Port 22 für das SSH-Protokoll) angegeben. Hierdurch kann ein Backend-Cluster ohne Verwenden von virtuellen IP-Adressen ausfallsicher angebunden werden.
 Connect	Über die Schaltfläche Start wird die zusätzliche Backend-Maschine hinzugefügt.

7.13 Logs

Dieses Menü bietet die Möglichkeit die für den E-Mail Betrieb relevanten Logs einzusehen.

Über die Schaltfläche **Show queued mails...** öffnet das Untermenü **MAILS CURRENTLY IN QUEUE**^[391], über welches die E-Mail Warteschlange eingesehen und entsprechende Aktionen vorgenommen werden können. Via **Show other logs...** wird das Untermenü **OTHER LOGS**^[392] geöffnet, welches die Möglichkeit zur Einsicht weiterer Log-Dateien, sowie für das Verwalten des mail logs bietet.

Sektion Filter

Über das Eingabefeld kann ein Suchbegriff als Zeichenfolge (string) eingegeben werden, nach welchem durch Klicken der Schaltfläche **Filter** im aktuellen maillog gesucht wird. Über die beiden darunter liegenden Auswahl-Menüs **Search logs from:** **until:** kann die Suche auf einen bestimmten Zeitraum festgelegt werden. *(entfällt mit 12.1.x) Die jeweils auszuwählenden Zeiträume sind von den Inhalten der E-Mail Archiv Dateien (siehe Mail log archive*^[392]*) abhängig. (neu mit 12.1.x) Wird keine Zeitangabe gemacht, so wird innerhalb der letzten 24 Stunden gesucht.*

Zusätzlich besteht die Möglichkeit nach den Status aus der folgenden Tabelle zu Filtern.

Parameter	Beschreibung
 ☒ Do not show message ID column in table	Im Standard ist diese Option aktiv. Unterdrückt das Anzeigen der Spalte Message-ID .
 ☒ Limit the number of search results	Im Standard ist diese Option aktiv und mit 500 vorbelegt. Limitiert die Anzeige unter Mail log auf die angegebenen Anzahl von Einträgen. Hinweis: Ist der Haken gesetzt, wird im Standard die angegebene Anzahl der laufenden Nr. ^[389] seit dem letzten Eintrag unter Mail log angezeigt. Bei der Suche über Filter wird die angegebene Anzahl der Funde seit dem letzten Eintrag ausgegeben. Die zusätzlichen Filter aus dieser Tabelle beziehen sich jeweils auf die Anzeige in Mail log . Ist der Haken also gesetzt, so wird beim Verwenden der zusätzlichen Filter eine Teilmenge aus der ursprünglich angegebenen Anzahl von Einträgen angezeigt.
 ☒ Mail delivery successful (green)	Im Standard ist diese Option aktiv. Aktiviert den Filter für erfolgreich an die nächste Instanz übergebenen/ausgelieferte E-Mails. Nächste Instanz meldet dsn=2.0.0, status=sent (250 ok, ...)
 ☒ Mail delivery delayed (orange)	Im Standard ist diese Option aktiv. Aktiviert den Filter für temporär nicht ausgelieferte E-Mails, welche in der Warteschlange (siehe auch MAILS CURRENTLY IN QUEUE ^[391]) bis zum nächsten Auslieferungsversuch abgelegt bleiben. Ursache kann das temporäre Abweisen durch die nächste Instanz (dsn=4.x.x, status=deferred (...)) sein.
 ☒ Mail delivery rejected (red)	Im Standard ist diese Option aktiv. Aktiviert den Filter für E-Mails, welche nicht ausgeliefert werden konnten, beziehungsweise von abgewiesen wurden. Eine Benachrichtigungs-E-Mail über diesen Vorgang geht an den Absender.

Parameter	Beschreibung
	Ursache kann das Ablehnen durch die nächste Instanz (dsn=5.x.x, status=bounced (host <mailserver> [<IP>] said: 5xx 5.x.x ...)) sein.
 ☒ Mail not processed (black)	Im Standard ist diese Option aktiv. Aktiviert den Filter für E-Mails, welche aktuell noch vom Ruleset verarbeitet werden oder deren Verarbeitung abgebrochen wurde.  Hinweis: Die Status green, orange und red werden jeweils durch das Nachfolgesystem zurückgeliefert. Das setzt voraus, dass die Ruleset-Verarbeitung erfolgreich abgeschlossen werden konnte. Während des Abarbeitens des Rulesets bleibt der Status black. Kann die Ruleset-Verarbeitung aufgrund eines SPAM- oder Viren-Fundes (siehe Mail Processing ^[286] Ruleset generator ^[287] Protection Pack (AntiVirus / AntiSpam) ^[303]) nicht abgeschlossen werden (E-Mail würde <u>von der Appliance</u> mit einem dsn=5.x.x abgelehnt), so verbleibt der Status dauerhaft black.
Die Felder oberhalb und unterhalb dieser Zeile sind logisch UND verknüpft. Die Felder innerhalb der Blöcke sind logisch ODER verknüpft.	
 ☒ Mail is encrypted ()	Im Standard ist diese Option aktiv. Aktiviert den Filter für E-Mails, welche ver- oder entschlüsselt wurden.
 ☒ Mail is signed ()	Im Standard ist diese Option aktiv. Aktiviert den Filter für E-Mails, welche signiert, oder deren Signatur geprüft wurde.
 ☒ Large file mail ()	Im Standard ist diese Option aktiv. Aktiviert den Filter für E-Mails, welche via LF ^[107] versendet/empfangen wurden.
 ☒ Unsecured mail	Im Standard ist diese Option aktiv. Aktiviert den Filter für E-Mails, welche kryptographisch unbehandelt blieben.

Das Suchergebnis wird in der **Sektion Mail Log** ^[389] angezeigt.

Sektion Mail log

Zeigt die maillog Einträge, beziehungsweise die Filterergebnisse aus **Filter** ^[388] an.



Hinweis:

In der **Sektion Mail log** tauchen E-Mails erst dann auf, wenn die Ruleset-Verarbeitung beginnt. Wird eine E-Mail bereits vor der Ruleset-Verarbeitung - zum Beispiel aufgrund von Black-/Greylisting oder RBLs - abgewiesen, so ist diese über **OTHER LOGS** ^[392] **Show blocked mails log...** zu finden.

Spalte	Beschreibung
 Nr.	Laufende Nummer der Log-Einträge. Durch Klicken auf die Nummer werden Details zum Log-Eintrag angezeigt.

Spalte	Beschreibung
	 Hinweis: In den Details wird bei den Einträgen zwischen „Mail“ und „Message“ unterschieden. Bei Einträgen mit „Mail“ (wie zum Beispiel „Mail from“) ist jeweils der Envelope, bei „Message“ (wie zum Beispiel „Message from“) der Header-Eintrag der E-Mail gemeint.
 <u>Source IP</u>	Quell-IP-Adresse von welcher die E-Mail eingeliefert wurde.
 <u>Date</u>	Datum und Uhrzeit des Vorgangs.
 <u>From</u>	Absender E-Mail Adresse
 <u>To</u>	Empfänger E-Mail Adresse(n). Diese werden je nach Status farbig und je nach ausgeführter kryptographischer Aktion mit einem entsprechenden Symbol angezeigt (siehe auch Tabelle aus Filter ³⁸⁸). Weiterhin wird bei einem Mouse-Over über die Symbole im Tooltip jeweils das verwendete kryptographische Verfahren angezeigt.
 <u>Message-ID</u>	Eindeutige Kennnummer der E-Mail. Mittels dieser ID kann auch auf anderen Komponenten - zum Beispiel Groupware-Server oder AntiSpam Komponente - die E-Mail nachverfolgt werden.
 <u>Subject</u>	Betreff der E-Mail. Dieser wird nur angezeigt, wenn die Anzeige nicht ausgeblendet wurde (siehe Mail Processing ²⁸⁶ , Ruleset generator ²⁸⁷ , General settings ²⁸⁸ , Log message metadata ²⁸⁹).
 <u>Size</u>	Größe der E-Mail.

7.13.1 Mails Currently In Queue

Dieses Sub-Menü wird aus **Logs** ^[388] über **Show queued mails...** aufgerufen.

Sofern die E-Mail Queue nicht deaktiviert wurde (siehe **Mail Processing** ^[286] **Ruleset generator** ^[287] **Advanced options** ^[310] **Use custom delivery method** ^[312] mit Eingabe „loop“) werden durch SEPPmail Appliance verarbeitete E-Mails bei Bedarf - wenn zum Beispiel das Zielsystem temporär nicht erreichbar ist oder aufgrund eines Greylisting Filters beim Kommunikationspartner die E-Mail beim ersten Sendeversuch abgelehnt wird - in einer Warteschlange zwischengespeichert. Die SEPPmail Appliance wird in regelmäßigen Abständen versuchen die E-Mails der Warteschlange auszuliefern. Kann eine E-Mail trotz mehrmaliger Auslieferungsversuche nicht zugestellt werden, so wird der Absender darüber benachrichtigt und die E-Mail verworfen.

Der Inhalt dieser Warteschlange wird unter **Queued e-mails** ^[391] angezeigt. Ein sofortiger, erneuter Auslieferungsversuch der zwischengespeicherten E-Mails kann über die Schaltfläche **Retry to deliver queued mails...** forciert werden.

Über **Filter...** kann zunächst - mittels String - nach E-Mails anhand der E-Mail Adresse (Spalten From und To) gesucht werden. In diesem Fall wird unter **Queued e-mails** ^[391] das Suchergebnis gelistet.

Sektion Queued e-mails

Zeigt die E-Mails in der Warteschlange, beziehungsweise das Suchergebnis des eingegebenen **Filters** an.

Über **Delete** können die unter **Queued e-mails** ^[391] aufgelisteten E-Mails aus der Warteschlange gelöscht werden. **Back** wechselt in das übergeordnete Menü **Logs** ^[388] zurück.

7.13.2 Other Logs

Dieses Sub-Menü wird aus **Logs** über **Show other logs...** aufgerufen.

Dieses Menü stellt Logs für unterschiedliche weitere Funktionskomponenten zur Verfügung.

Sektion Other logs

Sofern die GINA-Technologie nicht deaktiviert wurde (siehe **Mail Processing** ^[286] **Ruleset generator** ^[287] **Advanced options** ^[310] **Completely disable GINA technology** ^[310]) wird eine entsprechende Log-Datei geführt, welche über die Schaltfläche **Show GINA log...** einzusehen ist.

Über **Show blocked mails log...** kann das Log über die von der SEPPmail Appliance abgelehnten E-Mails eingesehen werden. Hier werden neben den üblichen Ablehnungsszenarien (SMTP Codes 4xx und 5xx) bei lizenziertem Protection Pack und aktiviertem Black- Greylisting (siehe **Mail System** ^[247] **Antispam** ^[255] **Blacklists** ^[258] und **Manual blacklisting / whitelisting** ^[258]) insbesondere auch die daraus resultieren Ablehnungen gelistet.

Über **Show audit log...** können Zugriffe auf die Administrationsoberfläche nachvollzogen werden.

Mit **Show system log...** werden systemrelevante Log-Einträge (zum Beispiel Viren-Signatur-Updates, MPKI Zertifikatsbezüge und so weiter) angezeigt.



Hinweis:

Nachdem **AUDIT LOG** und **SYSTEM LOG** jeweils die Einträge eines ganzen Jahres beinhalten, kann der Aufruf mitunter relativ lange dauern.

Sektion Mail log archive

In dieser Sektion stehen diverse Download-Optionen für das maillog zur Verfügung.

Da für eine Log-Analyse meist die letzten 30 Tage ausreichend sind, kann über die Schaltfläche **Download log (last 30 days)** dieser Teilbereich gezielt heruntergeladen werden und steht im Anschluss als maillog-latest.txt zur Verfügung.

Die SEPPmail Appliance lagert in der Regel ab Erreichen einer maillog-Größe von 30 MB jeweils in eine Archiv-Datei aus. Über die Schaltfläche **Download log (complete)** wird die aktuelle Log-Datei sowie alle vorhandenen Archiv-Dateien in einem Stream in eine Datei (maillog.txt) heruntergeladen.

Über die Schaltfläche **Download log archive** werden lediglich alle Archive (maillog-archive.txt) heruntergeladen.

Sektion GINA archive

In dieser Sektion stehen diverse Download-Optionen für das GINA-Log zur Verfügung.

Da für eine Log-Analyse meist die letzten 30 Tage ausreichend sind, kann über die Schaltfläche **Download log (last 30 days)** dieser Teilbereich gezielt heruntergeladen werden und steht im Anschluss als GINAllog-latest.txt zur Verfügung.

Die SEPPmail Appliance lagert in der Regel ab Erreichen einer GINAllog-Größe von 10 MB jeweils in eine Archiv-Datei aus. Über die Schaltfläche **Download log (complete)** wird die aktuelle Log-Datei sowie alle vorhandenen Archiv-Dateien in einem Stream in eine Datei (log.txt) heruntergeladen.

Über die Schaltfläche **Download log archive** werden lediglich alle Archive (GINAllog-archive.txt) heruntergeladen.

Sektion Maintenance

Mittels **Delete log archive index** kann der Suchindex der Log-Archiv Dateien gelöscht werden, um eventuelle Anzeigeprobleme zu beheben. Diese können in seltenen Fällen zum Beispiel durch das Rotieren der Logs entstehen. Der Index wird über Nacht neu aufgebaut. Somit kann eine Suche unmittelbar nach dem Löschen des Index länger als gewöhnlich dauern.

Über **Delete mail log archive** werden alle Log-Archiv-Dateien des E-Mail Logs gelöscht. Dies ist dann erforderlich, wenn der Speicherplatz der Log-Partition knapp wird (siehe **Home** ^[220] **Disk statistics** ^[223] **Log** ^[223]).

Bei Bedarf können die Archive zuvor über **Mail log archive** ^[392] **Download log archive** auf ein anderes System gesichert werden.

Delete GINA log archive ist das Pendant zu **Delete mail log archive** und löscht alle Log-Archiv-Dateien des GINA Logs

Sofern gewünscht kann das Löschen von Log-Einträgen auch über **System** ^[224] **Log cleanup** ^[236] **Automatically delete log archives older than** ^[236] ^[236] **days** ^[236] automatisiert werden.

Über **Back** wird in das übergeordnete Menü **Logs** zurück gewechselt.

7.14 Statistics

In diesem Menü werden diverse Messgrößen grafisch dargestellt. Dabei wird für jede Sektion jeweils

- die letzten 24 Stunden (Today)
- die letzte Woche (Last Week)
- der letzte Monat (Last Month)
- das letzte Jahr (Last Year)
- die letzten drei Jahre (Last 3 Years)

dargestellt.

Sektion **Throughput visualisation**

Die Grafiken dieser Sektion stellen den E-Mail Durchsatz dar.

Graph Farbe	Beschreibung
 grün	Zeigt die Gesamtzahl der empfangenen E-Mails an.
 blau	Zeigt die Gesamtzahl der gesendeten E-Mails an.
 rot	Zeigt die Gesamtzahl der verschlüsselten E-Mails an.
 lila	Zeigt die Gesamtzahl der entschlüsselten E-Mails an.

Sektion **Technology visualisation**

Die Grafiken dieser Sektion stellen die Häufigkeit der verwendeten Verschlüsselungstechnologien dar.

Graph Farbe	Beschreibung
 blau	Zeigt die Gesamtzahl der mittels GINA-Technologie verschlüsselten E-Mails an.
 grün	Zeigt die Gesamtzahl der mittels S/MIME Technologie verschlüsselten E-Mails an. S/MIME signierte E.Mails werden nicht dargestellt.
 rot	Zeigt die Gesamtzahl der mittels OpenPGP Technologie verschlüsselten E-Mails an.
 lila	Zeigt die Gesamtzahl der mittels <u>Domänenverschlüsselung</u> ³¹ verschlüsselten E-Mails an.

Sektion **Spam visualisation**

Wird nur bei vorhandener Protection Pack (PP) Lizenz angezeigt (siehe [Home](#) ²²⁰ [License](#) ²²⁰ **Protection Pack (AntiSpam / AntiVirus)**)

Die Grafiken dieser Sektion stellen die Aktionen der SPAM Abwehrmaßnahmen dar.

Graph Farbe	Beschreibung
 rot	Zeigt die Gesamtzahl aller aufgrund des Greylistings abgewiesenen E-Mails an.

Graph Farbe	Beschreibung
 blau	Zeigt die Gesamtzahl der aufgrund der <u>Realtime Blackhole List</u> (RBL) Funktion abgewiesenen E-Mails an.
 lila	Zeigt die Gesamtzahl der aufgrund der SPAM Erkennung abgewiesenen E-Mails an.
 grün	Zeigt die Gesamtzahl der empfangenen E-Mails an.

Sektion CPU usage visualisation

Die Grafiken dieser Sektion stellen die Prozessorauslastung der Appliance dar.

Graph Farbe	Beschreibung
 grün	Zeigt die vom System verursachte Prozessor Auslastung in Prozent an.
 rot	Zeigt die benutzerbezogene Prozessor Auslastung in Prozent an.
 blau	Zeigt die freien Prozessor Ressourcen in Prozent an.

Sektion Memory usage visualisation

Die Grafiken dieser Sektion stellen die Speicherauslastung der Appliance in Megabyte (MB) dar.

Graph Farbe	Beschreibung
 grün	Zeigt den aktiv benutzten Speicher an.
 rot	Zeigt den belegten Speicher an.
 hellblau	Zeigt den belegten Auslagerungsspeicher an.
 dunkelblau	Zeigt die Größe des zur Verfügung stehenden Auslagerungsspeichers an.
 schwarz	Zeigt die freien Speicher Ressourcen an.

Über **Reset RRD statistics database** können die kompletten Statistiken gelöscht werden. Dies kann zum Beispiel bei Darstellungsproblemen erforderlich sein.

7.15 Users

In diesem Menü werden die auf der SEPPmail Appliance vorhandenen Benutzer angezeigt.

Die Anlage von Benutzern kann automatisch oder manuell (siehe **Mail Processing** [288] **Ruleset generator** [287] **User creation** [289]) erfolgen.

Sollen Benutzer manuell eingerichtet werden, so erfolgt dies über die Schaltfläche **Create new user account...** (siehe Untermenü **CREATE USER ACCOUNT** [410]).

Über die Schaltfläche **Password policy...** werden die Passwort Regeln für SEPPmail Appliance Benutzer definiert (siehe Untermenü **CHANGE PASSWORD POLICY** [411]).

(neu in 12.1)

Die Schaltfläche **Advanced settings...** stellt erweiterte Funktionen bereit, welche auf alle SEPPmail Appliance Benutzer angewendet werden (siehe Untermenü **ADVANCED SETTINGS** [411]).

Da in großen Umgebungen mitunter der Aufbau der Seite sehr lange dauern kann, kann über die Option

Limit the number of returned accounts

die Anzeige auf 1000 User Accounts begrenzt werden. Die Suche nach einem Benutzer muss dann gegebenenfalls zwingend über die Schaltfläche **Filter...** vorgenommen werden. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Bei mandantenfähigen Systemen ist die Anzeige der Benutzer nach Mandanten gruppiert

Spalte	Beschreibung
 User ID	Zeigt die "User ID" des jeweiligen Benutzers an. Diese entspricht bei automatisch generierten Benutzern immer der E-Mail Adresse.
 Name	Zeigt den Namen des jeweiligen Benutzers an. Diese entspricht bei automatisch generierten Benutzern dem Anzeigenamen des Absenders aus dem From-Header, sofern vorhanden. Andernfalls wird auch hier die E-Mail Adresse angezeigt.  Achtung: Ist für das Beziehen von Zertifikate die MPKI [339] Schnittstelle aktiv, so taucht dieser Name - je nach konfigurierter Zertifikats-Güte - unter Umständen als Antragsteller (CN) des Zertifikates auf. Für diesen Fall sollte darauf geachtet werden, dass für jeden Benutzer bei der Anlage der korrekte Name eingetragen wird.
 E-mail	Zeigt die E-Mail Adresse des Benutzers an.
 OpenPGP	Zeigt die Anzahl der für den Benutzer vorhandenen OpenPGP Schlüssel an.
 S/MIME	Zeigt die Anzahl der für den Benutzer vorhandenen S/MIME Schlüssel an.
 State	Zeigt den Status des Benutzers an. Im Regelfall ist dieses Feld leer. Bei technischen Benutzern kann der Status auf "inaktiv" gesetzt werden (siehe Untermenü USER 'USER@DOMAIN.TLD' [398] User data [398] Encryption settings [398] May not encrypt mails [399] und May not sign mails [399]). Inaktive Benutzer sind nicht in der Lage zu verschlüsseln oder signieren und benötigen somit auch keine Benutzerlizenz. Bei Benutzern mit Passwort werden gegebenenfalls auch • Bad Password count: x • Locked temporarily abhängig von den Passwort Richtlinien (siehe Untermenü CHANGE PASSWORD POLICY [411]) und der Anzahl der fehlgeschlagenen Anmeldeversuche angezeigt.

Spalte	Beschreibung
 Last mail sent	Zeigt das Datum der zuletzt durch den jeweiligen Benutzer versendeten E-Mail.

Durch Klicken auf die **User ID** wird das Untermenü mit den Benutzerdetails (**USER 'USER@DOMAIN.TLD'** ) geöffnet.



Hinweis:

Bei Einrichten des Systems ist der Benutzer „admin“ bereits vorhanden. Dieser Benutzer benötigt keine Benutzerlizenz (Encryption/Signature License).
Es wird empfohlen, diesen Benutzer auch im weiteren Verlauf der Konfiguration nicht zu löschen, um gegebenenfalls ein „Aussperren“ aus dem System zu vermeiden.

7.15.1 User 'user@domain.tld'

Dieses Sub-Menü wird aus **Users** ^[396] aufgerufen.

Sektion **User data**

Parameter	Beschreibung
 User ID	Zeigt die eindeutige „User ID“ des jeweiligen Benutzers an. Diese entspricht bei automatisch generierten Benutzern im Standard der E-Mail Adresse. Die „User ID“ kann bei bestehenden Usern nicht geändert werden, da sie ein Alleinstellungsmerkmal für den User darstellt. Hinweis: Wurden bereits vor dem Update auf Version 11.1 User mit identischer User ID angelegt, so ist das Anmelden an der Administrationsoberfläche über die User ID nicht mehr möglich. Alternativ kann das Anmelden dann unter Eingabe der E-mail anstatt der User ID im Login ^[219] erfolgen. Für das Bereinigen von doppelten User IDs sollte der Support kontaktiert werden (siehe Unterstützung ^[22]). 
 Full name	Zeigt den Namen des jeweiligen Benutzers an. Diese entspricht bei automatisch generierten Benutzern dem Anzeigenamen des Absenders aus dem From-Header, sofern vorhanden. Andernfalls wird auch hier die E-Mail Adresse eingesetzt. Hinweis: Werden Zertifikate automatisiert via MPKI ^[339] bezogen, in welchem nicht nur die E-Mail Adresse, sondern auch der Benutzername bestätigt wird, so ist hier zwingend ein Name einzutragen (keine E-Mail Adresse). 
 E-mail	Zeigt die E-Mail Adresse des Benutzers an. Diese kann bei bestehenden Usern nicht geändert werden, da sie ein Alleinstellungsmerkmal für den User darstellt.
 Password	Optional kann hier einem Benutzer ein Passwort vergeben werden. Das Passwort muss den Passwort Regeln entsprechen (siehe Untermenü CHANGE PASSWORD POLICY ^[417]). Hinweis: Die Vergabe eines Passwortes ist für das Nutzen der Appliance nicht notwendig. Durch die Vergabe eines Passwortes wird es einem Benutzer ermöglicht, sich interaktiv an der Appliance - also der Administrationsoberfläche - anzumelden. Hierfür muss der jeweilige Benutzer zusätzlich den entsprechenden Gruppen (siehe Groups ^[413]) zugeordnet werden. 
 Encryption settings	Gibt die Berechtigungen für kryptographische Aktionen des jeweiligen Benutzers an. Hinweis: Sind beide Optionen gewählt, so wird für den Benutzer keine User-Licence in Anspruch genommen. Dies bietet sich zum Beispiel bei technischen Benutzern an, welche keine E-Mails in das Internet versenden (zum Beispiel Backup-Benutzer). Weiterhin müssen inaktive Benutzer somit nicht gelöscht werden. Das hat den Vorteil, dass deren Schlüsselmaterial auf der Appliance erhalten bleibt. Zudem werden empfangene E-Mails gegebenenfalls weiterhin entschlüsselt. Allerdings ist darauf zu achten, dass die 

Parameter	Beschreibung
	empfohlene User-Anzahl (siehe Sizing ^[78]) nicht maßgeblich überschritten wird.
 ☐ May not encrypt mails	Diese Option ist im Standard inaktiv. Untersagt dem Benutzer E-Mails zu verschlüsseln. Wird dennoch „Verschlüsseln“ aufgrund der Ruleset Einstellungen - egal ob automatisch oder per Trigger (siehe auch Mail Processing ^[286] , Ruleset generator ^[287] , Encryption ^[292] , Outgoing e-mails ^[293] beziehungsweise ENCRYPTION POLICY ^[313]) - angefordert, so würde die E-Mail abgewiesen (bounced) werden.
 ☐ May not sign mails	Diese Option ist im Standard inaktiv. Untersagt dem Benutzer E-Mails zu signieren. Wird dennoch „Signieren“ aufgrund der Ruleset Einstellungen - egal ob automatisch oder per Trigger (siehe auch Mail Processing ^[286] , Ruleset generator ^[287] , Signing ^[298] , Outgoing e-mails ^[300] beziehungsweise ENCRYPTION POLICY ^[313]) - angefordert, so würde die E-Mail abgewiesen (bounced) werden.
 MPKI subject part	Dieses Feld hat die gleiche Syntax wie gegebenenfalls in den MPKI ^[339] Einstellungen der jeweils ausgewählten CA. Weicht ein optionaler Eintrag von den Einstellungen der MPKI ^[339] ab, so wird der Eintrag in den MPKI ^[339] Einstellungen beim Generieren eines Zertifikates mit diesem überschrieben.  Achtung: Nicht jede CA, beziehungsweise MPKI ^[339] Einstellung lässt Änderungen am Static Subject Part zu. Werden hier dennoch Änderungen vorgenommen, würden für den jeweiligen Benutzer keine Zertifikate über die MPKI ^[339] ausgestellt. Sind Änderungen zulässig, so wird gegebenenfalls dennoch von der CA ein vorgegebener (Teil-)Ausdruck im Static Subject Part beim Ausstellen eines Zertifikates erwartet. Fehlt dieser Teil in den individuellen Einstellungen, so wird ebenfalls kein Zertifikat über die MPKI ^[339] ausgestellt.
 Notifications 	Individuelle Einstellung für das Ausstellen von GINA-Lesebestätigungen.
Send a notification when recipient reads GINA mail:   Hinweis: Wurde im E-Mail Client eine Lesebestätigung (Disposition-Notification-To Header) angefordert, so wird in jedem Fall die <u>verlässliche</u> GINA-Lesebestätigung ausgestellt, unabhängig von den vorgenommenen Einstellungen.	
 domain default	Standardeinstellung. Die Einstellung aus GINA Domains ^[416] , Domains ^[416] , CHANGE GINA SETTINGS FOR ^[423] , Extended settings ^[431] , Sender receives notification when recipient reads GINA mails ^[432] wird verwendet.
 always	Erzwingt das Ausstellen einer Lesebestätigung bei jeder GINA-Mail.
 never	Unterdrückt das Ausstellen einer Lesebestätigung bei GINA-Mails.
 Account status	Wird ein Account über dieses Menü explizit gesperrt, so muss diese Sperre gegebenenfalls auch wieder manuell aufgehoben werden. Automatische Sperren werden gemäß Einstellung (CHANGE PASSWORD POLICY ^[411]) aufgehoben.

Parameter	Beschreibung	
 locked	Zeigt an ob der Benutzer gesperrt ist (zum Beispiel nach mehrfacher Falscheingabe des Passwortes) beziehungsweise kann der Administrator den Benutzer durch Aktivieren des Buttons sperren.  Hinweis: Gesperrte Benutzer können sich auch nicht per SMTP-Auth, POP oder IMAP authentisieren (siehe Remote POP3 402 402).	
 enabled	Zeigt an ob der Benutzer aktiv ist beziehungsweise kann der Administrator den Benutzer durch Aktivieren des Buttons wieder in den Staus „Aktiv“ versetzen.	
 Creation data <i>(neu in 12.0.9)</i>	Zeigt Informationen, wie ein Benutzer generiert wurde.	
 Created by whom	Zeigt von wem der Benutzer generiert wurde.	
 Created by what	Zeigt welcher Prozess den Benutzer generiert hat.	
 Created at	Zeigt den Zeitpunkt des Generierens des Benutzers	
 Usage statistics	Zeigt die Nutzungsstatistik des Benutzers an.	
 Last outgoing e-mail	Zeitpunkt der letzten ausgehenden E-Mail	
 S/MIME encrypted e-mails sent	Anzahl der versendeten E-Mails, welche mittels S/MIME-Technologie verschlüsselt wurden	
 S/MIME encrypted e-mails received	Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie verschlüsselt waren	
 OpenPGP encrypted e-mails sent	Anzahl der versendeten E-Mails, welche mittels OpenPGP-Technologie verschlüsselt wurden	
 OpenPGP encrypted e-mails received	Anzahl der empfangenen E-Mails, welche mittels -Technologie verschlüsselt waren	
 S/MIME Domain encrypted mails sent	Anzahl der versendeten E-Mails, welche mittels S/MIME-Technologie domänenverschlüsselt wurden	
 S/MIME Domain encrypted mails received	Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie domänenverschlüsselt waren	
 OpenPGP Domain encrypted mails sent	Anzahl der versendeten E-Mails, welche mittels OpenPGP-Technologie domänenverschlüsselt wurden	

Parameter	Beschreibung	
	 OpenPGP Domain encrypted mails received	Anzahl der empfangenen E-Mails, welche mittels OpenPGP-Technologie domänenverschlüsselt waren
	 S/MIME signed e-mails sent	Anzahl der versendeten , welche mittels S/MIME-Technologie signiert wurden
	 S/MIME signed e-mails received	Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie signiert waren
	 GINA encrypted e-mails sent	Anzahl der E-Mails, welche mittels GINA-Technologie verschlüsselt wurden

Sektion Group membership

In dieser Sektion werden die Gruppenzugehörigkeiten des Benutzers angezeigt (siehe auch **Groups** ^[413])

Sektion S/MIME

Serial	Certificate authority	Issued on	Expires on
Zeigt die Seriennummern der Zertifikate an.	Zeigt die ausstellende Zertifizierungsstelle an	Ausstelldatum des Keys JJJJ-MM-TT	Ablaufdatum des Keys JJJJ-MM-TT

Durch Klicken der **Seriennummers** wird das Untermenü **X.509 CERTIFICATE 'details'** ^[474] geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel (Zertifikat) herunterzuladen beziehungsweise das Schlüsselpaar zu revozieren beziehungsweise zu löschen.

Über die Schaltfläche **Import S/MIME key and certificate...** kann ein bereits vorhandenes Zertifikat - zum Beispiel ein gekauftes einer trusted CA - importiert werden (siehe **Mail System** ^[247] **ADD/EDIT MANAGED DOMAIN** ^[266] **S/MIME domain encryption** ^[274] **IMPORT PKCS#12 CERTIFICATE STRUCTURE** ^[280]).

Über die Schaltfläche **Generate S/MIME key and certificate...** wird durch die integrierte Zertifizierungsstelle ein neues Schlüsselpaar auf der Appliance generiert.

Ist eine **MPKI** ^[339] eingerichtet und die **Managed Domain** ^[247], welcher der User angehört für den Bezug von Zertifikaten zugelassen (siehe **MPKI** ^[339] **Connectors** ^[339] **MPKI managed domains**), so erscheint entsprechend der verfügbaren Zertifizierungsstelle die Schaltfläche **Generate key and <MPKI> certificate...**. Durch Klicken dieser Schaltfläche wird ein Schlüsselpaar generiert. Der öffentliche Schlüssel wird dabei durch die MPKI signiert und steht somit als trusted Zertifikat zur Verfügung.

Wird diese Option aktiviert, so werden gegebenenfalls ablaufende Benutzer-Zertifikate auch automatisiert erneuert, sobald die Gültigkeit die angegebene Anzahl an Tagen unterschreitet



Hinweis:

Die Laufzeit des Zertifikates mit der längsten Gültigkeit kann der Datei user-stats.csv, welche mit dem **Daily Report** ^[96] (siehe auch **Groups** ^[413] **statisticsadmin** ^[415]) mitkommt, entnommen werden.

Dies ist insbesondere dann hilfreich, wenn keine **MPKI** ^[339] für das automatische Erneuern von Zertifikaten eingerichtet ist.

Sektion OpenPGP

In dieser Sektion werden die OpenPGP Schlüssel des Benutzers angezeigt, sofern vorhanden.

Key ID	Subkey ID(s) <i>(neu in 12.1)</i>	User ID	Issued on	Expires on
Zeigt die Key IDs der vorhandenen OpenPGP-Keys an	Zeigt die Key IDs aller vorhandenen Subkeys an.	Zeigt die zur Key ID zugehörige User ID an. Diese entspricht der E-Mail Adresse des Benutzers.	Ausstelldatum des Keys JJJJ-MM-TT	Ablaufdatum des Keys JJJJ-MM-TT

Durch Klicken der **Key ID** wird ein Untermenü mit Details zum Key geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

Über die Schaltfläche **Import OpenPGP key pair...** kann ein bereits vorhandenes Schlüsselpaar importiert werden (siehe **Mail System** ^[247] **ADD/EDIT MANAGED DOMAIN** ^[266] **OpenPGP domain encryption** ^[274] **IMPORT OPENPGP KEY** ^[280]).

Über die Schaltfläche **Generate new OpenPGP key pair...** wird ein neues Schlüsselpaar auf der Appliance generiert. Die Laufzeit sowie das automatische Aktualisieren der so erzeugten Schlüssels entspricht der unter **CA** ^[328] **Settings** ^[330] **Validity in days** eingegebenen.

Durch Klicken der **Key ID** wird ein Untermenü mit Details zum Key geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

Sektion Remote POP3

Wurde unter **Mail System** ^[247] **Managed domains** ^[247] die Option **Fetch e-mail from remote POP3 server** gewählt, so können die POP3 beziehungsweise IMAP Zugangsdaten für den jeweiligen Benutzer an dieser Stelle eingegeben werden. Die SEPPmail Appliance wird gemäß des eingestellten Zeitintervalls (siehe oben) E-Mails abholen. Dabei wird IMAPS beziehungsweise STLS (POP3S) präferiert.

Parameter	Beschreibung
 User ID	Eingabe der User ID für das Anmelden am POP3/IMAP Konto beziehungsweise für SMTP-Auth. In der Regel entspricht die User ID der E-Mail Adresse.
 Password	Zur User ID gehöriges Passwort.
 Mail server	POP3 beziehungsweise IMAP-Server von welchem E-Mails abgeholt werden sollen.
 Options	
 ☐ Use SSL instead of STARTTLS	Diese Option ist im Standard inaktiv. Soll für den Aufbau einer sicheren Verbindung (IMAPS / STLS) anstatt STARTTLS SSL verwendet werden, so ist diese Option zu aktivieren.

Sektion Customer

Diese Sektion erscheint nur bei mandantenfähigen Systemen (siehe Menüpunkt **Customers** ^[494]). Sie ermöglicht das Zuordnen des Benutzers zu einem Mandanten.

**Hinweis:**

Das Zuordnen von Benutzern zu den jeweiligen Mandanten erfolgt normalerweise automatisch anhand des Dömantenteils der E-Mail Adresse. Von einem manuellen Anpassen ist deshalb im Normalfall abzusehen.

Alle vorgenommenen Änderungen werden über die Schaltfläche **Save changes** gespeichert.

Das Löschen eines Users erfolgt über **Delete user**.

**Hinweis:**

Ist einem Benutzer gültiges Schlüsselmaterial zugeordnet, so muss dieses vor dem Löschen des Benutzer gelöscht werden. Andernfalls erscheint zunächst eine entsprechende Warnmeldung.

7.15.1.1 X.509 Certificate 'details'

Dieses Sub-Menü wird aus **USER 'USER@DOMAIN.TLD'**  aufgerufen.

Sektion **Issued to**

Diese Sektion zeigt Informationen über den Inhaber des SSL Zertifikates.
Abhängig vom Zertifikat müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
 Name (CN)	Dieses Feld beinhaltet den Antragstellernamen, wie er beim Beantragen des Zertifikates an die CA übermittelt wurde. Dies kann gelegentlich auch die E-Mail Adresse in der Form Email: max.mustermann@meinefirma.tld sein. In der Regel werden aber E-Mail Adressen als „CN“ nicht mehr anerkannt.
 E-mail address	E-Mail Adresse des Antragstellers. Dies kann auch eine Sammeladresse (shared mailbox) sein.
 Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Buchhaltung“
 Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel Meine Firma AG
 Locality (L)	Standort zum Beispiel eine Stadt wie „Neuenhof“ oder auch ein Teilgebäude wie Werk 2
 State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel Musterbundesland
 Country (C)	Land, zum Beispiel de für „Deutschland“
 Serial no.	Seriennummer des Zertifikats

Sektion **Issued by**

Diese Sektion zeigt Informationen über den Aussteller des SSL Zertifikates (Wurzel-Zertifikat).
Abhängig vom Aussteller müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
 Name (CN)	Name der ausstellenden Zertifizierungsstelle
 E-mail address	In der Regel eine E-Mail Adresse für Support-Anfragen an den Aussteller
 Org. unit (OU)	Gibt eine Organisationseinheit des Ausstellers an
 Organization (O)	Gibt die ausstellende Organisation an
 Locality (L)	Gibt den Standort des Ausstellers an

Parameter	Beschreibung
 State (ST)	Gibt ein Bundesland, Kanton, Provinz oder Ähnliches des Ausstellers an
 Country (C)	Gibt das Land des Ausstellers an
 Serial no.	Seriennummer des Zertifikats

Sektion **Validity**

Zeigt die Gültigkeit des Zertifikates.

Parameter	Beschreibung
 Issued on	Ausstelldatum des Zertifikates
 Expires on	Ablaufdatum des Zertifikates

Sektion **Fingerprint**

Der Fingerprint ist die Prüfsumme (auch hash) und dient dem Überprüfen eines Zertifikats. An dieser Stelle wird der Hash-Algorithmus (zum Beispiel MD5 SHA1 oder SHA256), mit welchem die Prüfsumme gebildet wurde, sowie der berechnete Wert angezeigt. Sind mehrere Fingerprints unterschiedlicher Algorithmen vorhanden, so wird jeder in einer separaten Zeile ausgegeben.

Parameter	Beschreibung
 SHA1	SHA1 Fingerprint des Zertifikates Beispiel: D8:CF:CC:47:84:92:A9:F0:7E:2A:15:E8:2E:4F:CA:26:5C:60:10:E9
 SHA256	SHA256 Fingerprint des Zertifikates Beispiel: 83:06:F6:84:34:C2:E7:79:50:47:7B:EC:32:B7:22:13:FD:1F:9C:41:B4:B4:F9:C3:AB:85:12:AA:6B:1E:D2:BE

Sektion **Key usage**

Zeigt den Verwendungszweck des Zertifikates an, wobei nur die aus der folgenden Tabelle berücksichtigt werden.

Parameter	Beschreibung
 S/MIME signing	digitalSignature / Digitale Signatur
 S/MIME encryption	keyEncipherment / Schlüssel Verschlüsselung
 CA certificate	keyCertSign / Zertifikatssignatur

Parameter	Beschreibung
  Allow decryption	Im Standard ist diese Option aktiv. Zeigt an, ob dieses Zertifikat für das Entschlüsseln von E-Mails an den Antragsteller (Issued to ) verwendet wird. Im Standard werden alle für den User vorhandenen Zertifikate für das Entschlüsseln verwendet.
  Allow signing	Im Standard ist diese Option aktiv. Zeigt an, ob dieses Zertifikat für das Signieren verwendet werden darf. Generell wird für das Signieren von E-Mails der Schlüssel mit der längsten Laufzeit verwendet (siehe auch Mail Processing ) Ruleset generator ) Signing ) Outgoing e-mails ) dritter Hinweis). Sollen jedoch Zertifikate hiervon explizit ausgenommen werden, kann dies an dieser Stelle jeweils bewerkstelligt werden.

Über **Save usage** werden Änderungen jeweils übernommen.

Sektion **Key info**

Zeigt erweiterte Informationen zum Zertifikat an.

Parameter	Beschreibung
 Signature algorithm	Zeigt den Signatur-Algorithmus des Zertifikates an, zum Beispiel • md5WithRSAEncryption • sha1WithRSAEncryption • sha256WithRSAEncryption
 Key type	Zeigt das Kryptosystem an, mit welchem der Schlüssel erzeugt wurde. In der Regel ist das RSA.
 Key size	Zeigt die Schlüssellänge an. In der Regel kommen nur noch Schlüssellängen von 2048 bit und mehr vor.
 Last certificate check	Zeigt den Zeitpunkt der letzten Zertifikatsprüfung (via CRL beziehungsweise OCSP) an. Über Check now... kann ein sofortiges Prüfen der Revokations-Informationen erzwungen werden.
 Last successful certificate check	Zeigt das Datum des letzten erfolgreichen OCSP, beziehungsweise CRL Checks an.
 Last check result	Zeigt das Ergebnis der letzten Zertifikatsprüfung an.
 OCSP URI	Gibt die authorityInformationAccess (kurz AIA, Zugriff auf Stelleninformationen) - also den OCSP Pfad - aus. Dieser Punkt ist nur dann sichtbar, wenn im Zertifikat die extension authority information access gesetzt ist.
 CRL URI	Gibt den crlDistributionPoint (Sperrlisten Verteilungspunkt) - also die Lokation, unter welchem die CRL bereit gestellt wird - aus. Dieser Punkt ist nur dann sichtbar, wenn im Zertifikat die extension crlDistributionPoint gesetzt ist.
 Public / private key	Gibt an, welche Schlüssel enthalten sind, private, public oder beide.
 Key origin	Zeigt an, welche CA den öffentlichen Schlüssel signiert hat.

 Sektion Comment

An dieser Stelle kann ein persönlicher Kommentar zum Zertifikat eingegeben werden, zum Beispiel weshalb die entsprechende Vertrauensstellung gewählt wurde.

Mit **Save comment** wird dieser Kommentar gespeichert.

Über die Schaltfläche **Download certificate** besteht die Möglichkeit das Zertifikat im CRT-Format zu speichern.

Über **Revoke / Delete** wird das Zertifikat von der SEPPmail Appliance zunächst revoziert und über einen zweiten Klick gegebenenfalls gelöscht.

7.15.1.2 OpenPGP Key 'details'

Dieses Sub-Menü wird aus `USER 'USER@DOMAIN.TLD'` ³⁹⁸ aufgerufen.

Sektion **Identification**

Diese Sektion zeigt Informationen über den Inhaber des OpenPGP Keys.

Parameter	Beschreibung
 ID	Zeigt die eindeutige ID des OpenPGP Keys an.
 User ID	In der Regel wird der Name sowie die E-Mail Adresse des Schlüsselinhabers angezeigt.
 Key ID	Zeigt die eindeutige Key ID des OpenPGP Keys an
 Subkey ID(s) <i>(neu in 12.1)</i>	Zeigt die Key Ids aller vorhandenen Subkeys an.
 Fingerprint	Hash des Keys. Dieser dient dem Abgleich mit dem Kommunikationspartner, um festzustellen, dass der Key auf dem Weg vom Besitzer zum Kommunikationspartner nicht - zum Beispiel durch eine Man-In-The-Middle-Attacke - ausgetauscht wurde.

Sektion **Validity**

Zeigt die Gültigkeit des Zertifikates.

Parameter	Beschreibung
 Issued on	Ausstelldatum des Zertifikates
 Expires on	Ablaufdatum des Zertifikates

Sektion **Type**

Parameter	Beschreibung
 PK Algorithm	Gibt den Schlüsselalgorithmus an, zum Beispiel RSA oder DSS/SH.
 Key size	Gibt die Schlüssellänge an

Sektion **Valid e-mail addresses**

Parameter	Beschreibung
 Address	Im Standard vorbelegt mit der E-Mail Adresse des jeweiligen Benutzers. Gibt die Adresse(n) an, für welche dieses Schlüsselpaar von der SEPPmail Appliance zusätzlich verwendet werden soll. Werden über New Address(es) weitere Adressen

Parameter	Beschreibung
	hinzugefügt, so wird dieses Feld mehrmals - auch für jede hinzugefügte Adresse - angezeigt.
 New Address(es)	Zur Eingabe weiterer E-Mail Adresse(n) (Mehrfacheingabe ist durch Trennen mit Leerzeichen möglich), für welche das Schlüsselpaar zusätzlich verwendet werden soll. Die Eingabe wird nach Speichern über Save addresses jeweils als Address übernommen.  Hinweis: Diese Einstellung funktioniert nur mit Schlüsselmateriale welches mit 7.4.6 oder höher hochgeladen wurde.

Sektion Usage

Zeigt den Verwendungszweck des Zertifikates an, wobei nur die aus der folgenden Tabelle berücksichtigt werden.

Parameter	Beschreibung
 Allow decryption	Zeigt an, ob dieses Zertifikat für das Entschlüsseln von E-Mails an die unter User ID (Identification) ^[408] beziehungsweise an die unter Valid e-mail addresses ^[408] eingetragene(n) E-Mail-Adresse(n) verwendet wird. Im Standard werden alle für den User vorhandenen OpenPGP Keys für das Entschlüsseln verwendet.
 Allow signing	Zeigt an, ob dieser OpenPGP Key für das Signieren verwendet werden darf. Generell wird für das Signieren von E-Mails der Schlüssel mit der längsten Laufzeit verwendet (siehe auch Mail Processing ^[286] , Ruleset generator ^[287] , Signing ^[298] , Outgoing e-mails ^[300] dritter Hinweis). Sollen jedoch OpenPGP Keys hiervon explizit ausgenommen werden, kann dies an dieser Stelle jeweils bewerkstelligt werden.

Über **Save usage** werden Änderungen jeweils übernommen.

Sektion Comment

An dieser Stelle kann ein persönlicher Kommentar zum OpenPGP Key eingegeben werden, zum Beispiel weshalb die entsprechende Vertrauensstellung gewährt wurde.

Mit **Save comment** wird dieser Kommentar gespeichert.

Über die Schaltfläche **Download public key** besteht die Möglichkeit den öffentlichen Schlüssel im Text-Format als asc-Datei zu speichern. Mit **Send public key by email** wird der öffentlichen Schlüssel im Text-Format als asc-Datei an die in **User ID (Identification)**^[408] genannte E-Mail Adresse gesendet.

Über **Delete** wird das OpenPGP Schlüsselpaar, also privater (!) und öffentlicher Schlüssel aus der Appliance entfernt.

7.15.2 Create User Account

Dieses Sub-Menü wird aus **Users** ^[396] aufgerufen.

Sektion **User data**

Parameter	Beschreibung
 User ID	Eingabe einer Eindeutigen „User ID“ für den neuen Benutzer. Es empfiehlt sich - wie bei automatisch generierten Benutzern - auch an dieser Stelle die E-Mail Adresse zu verwenden, da hierdurch die Eindeutigkeit gewährleistet wird. Hinweis: Diese Eingabe kann in den Benutzerdetails (USER 'USER@DOMAIN.TLD' ^[398] User data ^[398]) nicht mehr geändert werden. 
 Full name	Zeigt den Namen des jeweiligen Benutzers an. Diese entspricht bei automatisch generierten Benutzern immer der E-Mail Adresse.
 E-mail	Zeigt die E-Mail Adresse des Benutzers an. Hinweis: Diese Eingabe kann in den Benutzerdetails (USER 'USER@DOMAIN.TLD' ^[398] User data ^[398]) nicht mehr geändert werden. 
 Password	Optional kann hier einem Benutzer ein Passwort vergeben werden. Das Passwort muss den Passwort Regeln entsprechen (siehe Untermenü CHANGE PASSWORD POLICY ^[411]). Hinweis: Die Vergabe eines Passwortes ist für das Nutzen der Appliance nicht notwendig. Durch die Vergabe eines Passwortes wird dem Benutzer ermöglicht, sich interaktiv an der Appliance - also der Administrationsoberfläche - anzumelden. Hierfür muss der jeweilige Benutzer zusätzlich den entsprechenden Gruppen (siehe Groups ^[413]) zugeordnet werden. 

Über die Schaltfläche **Create account** wird der Benutzer angelegt und kann im Anschluss weiter bearbeitet werden (siehe Untermenü **USER** 'USER@DOMAIN.TLD' ^[398]).

Cancel bricht den Vorgang ab.

7.15.3 Change Password Policy

Dieses Sub-Menü wird aus **Users**  aufgerufen.

Sektion Password settings for system (not GINA) accounts

Die Vergabe eines Passwortes ist ausschließlich für das Anmelden an der Administrationsoberfläche notwendig. Die Berechtigungen für Benutzer mit Passwort wird über die Gruppenzugehörigkeit geregelt (siehe **Groups** ). Das heißt die hier definierten Passwort Regeln sind für das interaktive Anmelden an der Administrationsoberfläche gültig.

Parameter	Beschreibung
 Minimum password length: ☒	Auswahl der minimalen Passwort Länge (4 bis 16 Zeichen, Standard ist 8).
 ☐ Must contain at least one lower case letter	Definiert, ob ein Kleinbuchstabe im Passwort enthalten sein muss.
 ☐ Must contain at least one upper case letter	Definiert, ob ein Großbuchstabe im Passwort enthalten sein muss.
 ☐ Must contain at least one number	Definiert, ob eine Ziffer im Passwort enthalten sein muss.
 ☐ Must contain at least one special character	Definiert, ob ein Sonderzeichen im Passwort enthalten sein muss.
 ☐ Must not contain own name, user name or e-mail address	Definiert, ob das Passwort den eigenen Namen oder E-Mail Adresse enthalten darf.
 ☐ Must be different from previous ☐ password(s)	Definiert, mit wie vielen vorangegangenen Passwörtern bei einem Passwortwechsel keine Übereinstimmung bestehen darf (1 bis 28, Standard ist 4).
 ☐ Must be changed at least every ☐ days	Definiert, ob und nach wie vielen Tagen das Passwort geändert werden muss (Standard ist 90).
 Accounts are locked for ☐ minutes after ☐ failed login attempts.	Definiert, nach wie vielen fehlgeschlagenen Anmeldeversuchen durch falsche Passworteingabe (Standard ist 5) für wie lange (in Minuten, Standard ist 30) der Zugang gesperrt wird.

Über die Schaltfläche **Save** werden die angezeigten Einstellungen gesichert.

Mittels **Back** wird das Menü ohne Speichern eventuell getätigter Eingaben verlassen.

7.15.4 Advanced Settings

(neu in 12.1)

Dieses Sub-Menü wird aus **Users**  aufgerufen.

Die hier vorgenommenen Einstellungen werden für alle SEPPmail Appliance Benutzer, welche im Menü **Users**  gelistet sind angewendet.

Sektion Advanced settings

Parameter	Beschreibung
 Revocation	Über die Schaltfläche Check OCSP/CRL status now werden Zertifikate der in Users  gelisteten SEPPmail Appliance Benutzer sofort via OCSP (Online Certificate Status Protocol), beziehungsweise CRL (Certificate Revocation List) geprüft.
 ☐ Automatically check revocation status every day	Im Standard ist diese Einstellung inaktiv. Durch Aktivieren dieser Option werden Zertifikate der in Users  gelisteten SEPPmail Appliance Benutzer einmal täglich automatisiert einer Gültigkeitsprüfung unterzogen.

Die vorgenommenen Änderungen beider Sektionen werden über die Schaltfläche **Save** gespeichert.

7.16 Groups

In diesem Menü sind bereits administrative Benutzergruppen vorgegeben (siehe Tabelle). Diese dienen der Wirkungsmöglichkeiten einzelner Benutzer bei interaktivem Anmelden an der Administrationsoberfläche. Weiterhin besteht über die Schaltfläche **Create new user group...** die Möglichkeit, weitere Gruppen zur Verwendung im Ruleset (siehe **Mail Processing** ^[286] **Ruleset generator** ^[287] **Custom commands** ^[308]) zu erzeugen.

Über die Schaltfläche **Edit...** kann die jeweilige Gruppe editiert (Gruppen Name und Beschreibung), sowie Benutzer zugeordnet werden. Im Normalfall können nur diejenigen Benutzer einer Gruppe zugeordnet werden, welchen auch ein Passwort zugewiesen wurde (siehe auch **Users** ^[396] **USER 'USER@DOMAIN.TLD'** ^[398] **User data** ^[398]

Password ^[398]). Wird vor dem Klicken der Schaltfläche **Edit...** der Haken des Auswahlkästchens ☐ **Edit for all users** gesetzt, so stehen auch **Users** ^[396] ohne Passwort zur Auswahl. Dies ist insbesondere für Gruppen interessant, an welche ein E-Mail Versand gekoppelt ist (**admin** ^[413], **backup** ^[413], **statisticsadmin** ^[415], **x509rootcertificatesadmin** ^[415]) oder unter Umständen für selbst erstellte Gruppen.

Gruppe	Beschreibung
 admin (Administrator)	Alle Mitglieder dieser Gruppe sind dem Standardbenutzer admin gleichgestellt und haben uneingeschränkten administrativen Zugang zur Konfigurationsoberfläche mit allen Berechtigungen. Weiterhin erhalten Mitglieder dieser Gruppe die mit "IMPORTANT" gekennzeichneten Daily Report ^[96]s (siehe auch statisticsadmin ^[415]) zugesandt. Hinweis: Sollten administrative Aufgaben anfallen, so werden die Mitglieder dieser Gruppe darüber informiert. Somit sollte der Administrator der SEPPmail Appliance unbedingt Mitglied dieser Gruppe sein. Achtung: Um bei Vergessen des Passwortes für den Built-In admin Account handlungsfähig zu bleiben, wird dringend empfohlen, dieser Gruppe wenigstens einen weiteren Account hinzuzufügen. Hinweis: Sollen Administratoren eingerichtet werden, welche sich zwar auf der Appliance anmelden können, jedoch keine Reports erhalten sollen, so sollte beim Anlegen des entsprechenden Users ^[396] als E-Mail Adresse eine Pseudo-Adresse mit @local verwendet werden.
 administrationadmin (GUI access to Administration section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü Administration ^[369] in der Konfigurationsoberfläche.
 backup (Backup operator)	Dieser Gruppe ist eine Sonderbedeutung zugeordnet, da durch die Mitgliedschaft kein Zugriff auf die Konfigurationsoberfläche gewährt wird. Alle Mitglieder dieser Gruppe erhalten das Systembackup des jeweiligen Systems einmal täglich um 0:00 Uhr per E-Mail.

Gruppe	Beschreibung
	 Hinweis: Frontend Server (siehe Cluster ³⁸³) Add this device as frontend server ³⁸⁵) versenden kein Backup, da diese Maschinen über keine eigene Datenbank verfügen.
 caadmin (GUI access to CA section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü CA ³²⁸ der Konfigurationsoberfläche. Weiterhin erhalten die Mitglieder dieser Gruppe jeweils beim Einsammeln eines neuen X.509 Root Certificates ⁴⁸⁰ aus einer E-Mail Signatur eine E-Mail Nachricht mit dem Betreff „New CA added“.
 clusteradmin (GUI access to Cluster section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü Cluster ³⁸³ der Konfigurationsoberfläche.
 domainkeysadmin (GUI access to Domain Keys section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü Domain Certificates ⁴⁸⁹ der Konfigurationsoberfläche.
 groupsadmin (GUI access to Groups section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü Groups ⁴¹³ der Konfigurationsoberfläche.
 homeadmin (GUI access to Home section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü Home ²²⁰ der Konfigurationsoberfläche.
 legacyappadmin (API access to legacy.app REST interface)	*unsupported* Dieser Gruppe ist eine Sonderbedeutung zugeordnet, da durch die Mitgliedschaft kein Zugriff auf die Konfigurationsoberfläche gewährt wird. Nahere Informationen sind bei Bedarf unter https://github.com/seppmail/SEPPmailLegacy zu finden.
 logsadmin (GUI access to Logs section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü Logs ³⁸⁸ der Konfigurationsoberfläche.
 mailprocessingadmin (GUI access to Mail Processing section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü Mail Processing ²⁸⁸ der Konfigurationsoberfläche.
 mailsystemadmin (GUI access to Mail System section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü Mail System ²⁴⁷ der Konfigurationsoberfläche.
 mpkiadmin (GUI access to MPKI section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü MPKI ³³⁹ der Konfigurationsoberfläche.
 multiplecustomersadmin (Admin access to Customer settings in multitenant deployments)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü Customers ⁴⁹⁴ der Konfigurationsoberfläche.
 pgpkeysadmin (GUI access to OpenPGP Keys section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü OpenPGP Public Keys ⁴⁶⁷ der Konfigurationsoberfläche.
 readonlyadmin (Read-only GUI access to all sections)	Alle Mitglieder dieser Gruppe haben ausschließlich lesenden Zugriff auf alle Menüs der Konfigurationsoberfläche.
 readonlyuser	Mitglieder dieser Gruppe haben ausschließlich lesenden Zugriff auf die Menüs, in deren Gruppen sie zusätzlich Mitglied sind.

Gruppe	Beschreibung
(Read-only GUI access to restricted sections)	
 ssladmin (GUI access to SSL section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü SSL ^[319] der Konfigurationsoberfläche.
 statisticsadmin (GUI access to Statistics section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü Statistics ^[394] der Konfigurationsoberfläche. Zusätzlich wird der tägliche System-Report (Daily Report ^[96]) des jeweiligen Systems täglich um 0.00 Uhr via E-Mail an alle Mitglieder dieser Gruppe gesendet.
 systemadmin (GUI access to System section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü System ^[224] der Konfigurationsoberfläche.
 usersadmin (GUI access to Users section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü Users ^[396] der Konfigurationsoberfläche.
 webmailaccountsadmin (GUI access to GINA Accounts section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü GINA Accounts ^[462] der Konfigurationsoberfläche.  Hinweis: Somit ist der Eintrag einer HelpDesk-, beziehungsweise der Admin e-mail ^[424] Adresse(n) sinnvoll, wie sie jeweils unter CHANGE GINA SETTINGS FOR ^[423] Admin ^[424] eingetragen ist. In mandantenfähigen Systemen haben die Customer Administrators ^[496] generell Zugriff auf ihre GINA accounts ^[462]. Somit ist das Angleichen der oben genannten Admin e-mail ^[424] sinnvoll.
 webmaildomainsadmin (GUI access to GINA Domains ^[416] section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü GINA Domains ^[416] der Konfigurationsoberfläche.
 x509certificatesadmin (GUI access to X.509 Certificates section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü X.509 Certificates ^[471] der Konfigurationsoberfläche.
 x509rootcertificatesadmin (GUI access to X.509 Root Certificates section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü X.509 Root Certificates ^[480] der Konfigurationsoberfläche. Zusätzlich wird den Mitgliedern dieser Gruppe eine E-Mail Nachricht mit dem Betreff "IMPORTANT: SEPPmail new CA certificates added on ..." gesendet, sofern aus signierten E-Mails Root- oder Zwischenzertifikate eingesammelt werden, welche noch nicht bekannt sind (siehe X.509 Root Certificates ^[480]).

7.17 GINA Domains

Im Menüpunkt **Mail Processing** [285] wird das Regelwerk der SEPPmail Appliance konfiguriert. Dieses Regelwerk ist mit einem Workflow System vergleichbar und stellt das zentrale Element der SEPPmail Appliance dar.

Sektion Domains

Liste der GINA-Domains.

Über den **Filter...** steht eine Suchfunktion innerhalb der Spalte **GINA name** der folgenden Tabelle bereit. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Spalte	Beschreibung
 GINA name	Liste aller auf der SEPPmail Appliance angelegten GINA-Domains. Im Standard ist an dieser Stelle ausschließlich die „[default]“ GINA-Domain vorhanden.
 Hostname	Zeigt den Hostnamen der jeweiligen GINA-Domain, wie er im Untermenü CHANGE GINA SETTINGS FOR [423] Secure GINA host [423] eingetragen ist.
 Admin	Zeigt die Admin-E-Mail Adresse der jeweiligen GINA-Domain, wie sie im Untermenü CHANGE GINA SETTINGS FOR [423] Admin [424] eingetragen ist.

Sollte nur ein GINA-Webinterface benötigt werden, so ist es ausreichend die „[default]“ Einstellungen individuell anzupassen.

Sollten mehrere **Managed domains** [247] auf dem System eingerichtet sein, so können über **Create new GINA domain** jeweils weitere GINA-Webinterfaces eingerichtet werden (siehe Untermenü **CREATE NEW GINA DOMAIN** [422]).



Achtung:

Bei einer mandantenfähigen Installation ist es zwingend erforderlich, für jeden Kunden wenigstens eine GINA-Domain zu erstellen.

Das Einrichten erfolgt jeweils durch Anklicken der zu konfigurierenden GINA-Domain in der Spalte **GINA name**. (siehe Untermenü **CHANGE GINA SETTINGS FOR** [423]).

Das Zuordnen der jeweiligen GINA-Domain zur jeweiligen **Managed domain** [247] erfolgt in der **Sektion Bounce templates** [270] des Untermenüs **ADD/EDIT MANAGED DOMAIN** [270] aus **Mail System** [247] **Managed domains** [247].



Achtung:

Die „[default]“ GINA-Domain muss in jedem Fall konfiguriert werden, da Sie als Basis für gegebenenfalls weitere GINA-Domains dient. Unterbleibt dies, so ist mit sporadischen Fehlern der Appliance zu rechnen!

Sektion Settings

Allgemeine Einstellungen der GINA-Domains.

Parameter	Beschreibung
 Grace period (in days) after which unregistered GINA accounts are automatically removed	Im Standard ist diese Option mit „0“ vorbelegt und somit deaktiviert. Mit dieser Option werden GINA-Benutzer, für welche zwar ein Account generiert wurde, welche sich jedoch noch nicht registriert haben, automatisch gelöscht. Für die Eingabe der Anzahl von Tagen, nach welcher nicht registrierte Accounts gelöscht werden sollen, steht das Eingabefeld zur Verfügung. Über Trigger now wird die Aktion unter Beachtung des eingestellten Zeitraumes sofort ausgeführt.  Achtung: Mit dem Löschen eines Account, kann der Benutzer sich nicht mehr registrieren und somit die initiale (sowie gegebenenfalls darauf folgende) GINA-Mail nicht mehr lesen.  Hinweis: Diese Option wird in mandantenfähigen Systemen durch die Einstellung Customers^[494] CUSTOMER MANAGEMENT^[496] Retention settings^[498] umgesetzt. Deshalb ist die Einstellung in diesen Systemen ausgegraut.
 Grace period (in days) after which old GINA message metadata is automatically removed. Mails can still be decrypted by recipient if metadata is missing. (set to 0 to disable)	Im Standard ist diese Option mit „0“ vorbelegt und somit deaktiviert. Mit dieser Option werden GINA Meta Daten (Information über die Empfänger und deren Lesestatus), automatisch gelöscht. Für die Eingabe der Anzahl von Tagen, nach welcher diese Informationen gelöscht werden sollen, steht das Eingabefeld zur Verfügung. Über Trigger now wird die Aktion unter Beachtung des eingestellten Zeitraumes sofort ausgeführt. Die Funktion der Accounts wird dadurch nicht beeinflusst!  Hinweis: Diese Option wird in mandantenfähigen Systemen durch die Einstellung Customers^[494] CUSTOMER MANAGEMENT^[496] Retention settings^[498] umgesetzt. Deshalb ist die Einstellung in diesen Systemen ausgegraut.
 Use virtual hosting	Werden mehrere GINA-Domains verwendet, so...
 On for all domains	...muss für jede GINA-Domain ein eigener FQDN verwendet werden. Dies hat zur Folge, dass auch für jede GINA-Domain ein eigenes Zertifikat benötigt wird. Das entsprechende Eingabefeld für das individuelle Zertifikat wird in diesem Fall im Untermenü CREATE NEW GINA DOMAIN ^[422] , beziehungsweise CHANGE GINA SETTINGS FOR ^[423] angezeigt.
 Off for all domains	Standardeinstellung. ...wird generell nur ein FQDN für den Zugriff verwendet. Für jede weitere GINA-Domain wird ein eigener Ordner unterhalb dieses FQDNs angelegt. Dadurch wird auch bei Verwenden von mehreren GINA-Domains nur ein SSL Zertifikat (siehe Menüpunkt SSL ^[319]) für den Zugriff aus dem Internet benötigt.
 Use domain settings	...kann pro GINA Domain (siehe CREATE NEW GINA DOMAIN ^[422] , beziehungsweise CHANGE GINA SETTINGS FOR ^[423]) entschieden werden, welche Variante gewünscht wird.

Parameter	Beschreibung
	 Achtung: Wird ein bestehendes System mit mehreren GINA-Domains im Nachgang auf virtual hosting [423] umgestellt, so ist dies ebenfalls möglich, erfordert jedoch Änderungen unter CHANGE GINA SETTINGS FOR [423] Secure GINA host [423] hostname [423] beziehungsweise Additional hostnames [423].
 Secure track access	Im Standard ist diese Option mit leer und somit deaktiviert. Mit dieser Option werden über den eingetragenen Link erweiterte Informationen in einer GINA-Lesebestätigung bereitgestellt, zum Beispiel, welcher GINA-Empfänger die E-Mail bereits wann gelesen hat. Aktiviert wird diese Funktion durch Eintragen der URL für den Zugriff auf die Administrationsoberfläche der Appliance (siehe auch System [224] Admin GUI [230]).  Hinweis: Für die korrekte Funktion dieser Option muss sichergestellt werden, dass der Absender der GINA-E-Mail auf diese URL zugreifen kann. Aus Sicherheitsgründen sollte ein Zugriff von externen Netzen (insbesondere dem Internet) jedoch nicht zugelassen werden.
 ☐ Disallow insecure ciphers	Diese Option ist im Standard inaktiv. Ermöglicht den Zugriff auf GINA-Domains auch mit älteren Clients / Browsern (RC4 aktiv). Um das Sicherheitspotential der Appliance auszuschöpfen, sollte die Aktion aktiviert werden (siehe Ciphers [103]).
 ☐ Disable strict SNI check when virtual hosting is enabled <i>(neu in 12.0)</i>	Diese Option ist im Standard inaktiv. Durch Aktivieren der Option kann der Schutz gegen das falsche Ansteuern einer GINA Domain, welcher mit der Version 11.1.7 eingeführt wurde, ausgehebelt werden (Fehlermeldung „403 Forbidden You don't have permission to access this resource. Reason: The client software did not provide a hostname using Server Name Indication (SNI), which is required to access this server.“). Das Verwenden der Option stellt das Verhalten wie unter 11.1.6 und kleiner wieder her und sollte nur im Fehlerfall zur temporären Wiederherstellung verwendet werden.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

Sektion **SMS passwords**

Einstellungen für den automatisierten Passwort-Versand via SMS.



Hinweis:

Für das Generieren der SMS kann sowohl ein interner Dienst im Netz des Kunden über ein entsprechendes Gateway, als auch ein externer Dienst im Internet genutzt werden. Der Zugang zu diesem Dienst ist zu gewährleisten (siehe **Firewall / Router einrichten** [\[135\]](#)).

Parameter	Beschreibung
  Disable	Standardeinstellung. Der GINA-Passwort-Versand via SMS ist deaktiviert
  Use cell phone / GSM	Ist eine Hardware Appliance im Einsatz, so kann an einen USB-Anschluss der Appliance ein Mobiltelefon oder GSM-Modem angeschlossen werden, über welches SMS versendet

Parameter	Beschreibung								
modem attached to appliance	werden können. Auf ausreichenden Empfang des Mobiltelefons / GSM-Modems ist zu achten.								
 Use Mail to SMS service (configuration below)	An dieser Stelle werden die Zugangsdaten für den SMS Versand über einen Mail to SMS Dienst eingetragen. <table><tr><td colspan="2">Mail to SMS settings</td></tr><tr><td>Mail from:</td><td>Je nach Anbieter muss hier die beim Anbieter für diesen Service registrierte E-Mail Absenderadresse oder aber auch ein frei wählbarer Absendername eingetragen werden.</td></tr><tr><td>Mail address prefix: <PREFIX XMobile #>@</td><td>Je nach Anbieter wird außer der Empfängernummer ein weiterer Zusatz benötigt, welcher an dieser Stelle bei Bedarf eingegeben werden kann. Diese Daten stellt der Betreiber des Dienstes zur Verfügung. Bei der deutschen Telekom wäre das zum Beispiel 017187654321</td></tr><tr><td>Gateway domain: <mobile #>@</td><td>Gateway-Domäne für den SMS-Versand. Diese Daten stellt der Betreiber des Dienstes zur Verfügung. Bei der deutschen Telekom wäre das zum Beispiel t-d1.sms.de</td></tr></table> Zusammengesetzt würde somit eine Email von von <Mail from:> an <Mail address prefix:><Mobilfunknummer des jeweiligen Passwortempfängers>@<Gateway domain> erstellt.  Achtung: „Mail to SMS“ wird aus Sicherheitsgründen nicht empfohlen, da die E-Mail zum SMS Provider unverschlüsselt übertragen werden muss!	Mail to SMS settings		Mail from:	Je nach Anbieter muss hier die beim Anbieter für diesen Service registrierte E-Mail Absenderadresse oder aber auch ein frei wählbarer Absendername eingetragen werden.	Mail address prefix: <PREFIX XMobile #>@	Je nach Anbieter wird außer der Empfängernummer ein weiterer Zusatz benötigt, welcher an dieser Stelle bei Bedarf eingegeben werden kann. Diese Daten stellt der Betreiber des Dienstes zur Verfügung. Bei der deutschen Telekom wäre das zum Beispiel 017187654321	Gateway domain: <mobile #>@	Gateway-Domäne für den SMS-Versand. Diese Daten stellt der Betreiber des Dienstes zur Verfügung. Bei der deutschen Telekom wäre das zum Beispiel t-d1.sms.de
Mail to SMS settings									
Mail from:	Je nach Anbieter muss hier die beim Anbieter für diesen Service registrierte E-Mail Absenderadresse oder aber auch ein frei wählbarer Absendername eingetragen werden.								
Mail address prefix: <PREFIX XMobile #>@	Je nach Anbieter wird außer der Empfängernummer ein weiterer Zusatz benötigt, welcher an dieser Stelle bei Bedarf eingegeben werden kann. Diese Daten stellt der Betreiber des Dienstes zur Verfügung. Bei der deutschen Telekom wäre das zum Beispiel 017187654321								
Gateway domain: <mobile #>@	Gateway-Domäne für den SMS-Versand. Diese Daten stellt der Betreiber des Dienstes zur Verfügung. Bei der deutschen Telekom wäre das zum Beispiel t-d1.sms.de								
 Use xml service (configuration below)	An dieser Stelle werden die Zugangsdaten für den SMS Versand über einen XML Dienst eingetragen. <table><tr><td>Server address:</td><td>Server Adresse des Dienstanbieters. Diese Daten stellt der Betreiber des Dienstes zur Verfügung.</td></tr><tr><td>xml template</td><td>Diese Daten stellt der Betreiber des Dienstes zur Verfügung. Ein Beispiel hierfür findet sich unten in diesem Abschnitt</td></tr></table> Weiterhin werden die bereitstehenden Variablen angezeigt <table><tr><td>Placeholders:</td></tr></table>	Server address:	Server Adresse des Dienstanbieters. Diese Daten stellt der Betreiber des Dienstes zur Verfügung.	xml template	Diese Daten stellt der Betreiber des Dienstes zur Verfügung. Ein Beispiel hierfür findet sich unten in diesem Abschnitt	Placeholders:			
Server address:	Server Adresse des Dienstanbieters. Diese Daten stellt der Betreiber des Dienstes zur Verfügung.								
xml template	Diese Daten stellt der Betreiber des Dienstes zur Verfügung. Ein Beispiel hierfür findet sich unten in diesem Abschnitt								
Placeholders:									

Parameter	Beschreibung														
	<table> <tr> <td>\$sms: text message</td><td>zu übermittelnder Nachrichtentext.</td></tr> <tr> <td>\$number: cell number including country code (+xx...)</td><td> Mobilfunkrufnummer inklusive Landesvorwahl (+xx...)  Hinweis: Wird die Nummer statt mit +xx... im Format 00xx... benötigt, so kann dies gegebenenfalls mittels 00\$countrycode\$localnumber zusammengesetzt werden. </td></tr> <tr> <td>\$countrycode: country code, e.g. „49“</td><td>Landesvorwahl, zum Beispiel „49“ für Deutschland</td></tr> <tr> <td>\$localnumber: cell number without country code</td><td>Mobilfunkrufnummer OHNE Landesvorwahl</td></tr> </table> sowie eine Beispielkonfiguration: <table> <tr> <td colspan="2">XML Example:</td></tr> <tr> <td>Server:</td><td>https://xml1.aspsms.com</td></tr> <tr> <td>String:</td><td> <pre><?xml version="1.0" encoding="UTF-8"?> <aspsms> <Userkey>xyz</Userkey> <Password>xyz</Password> <Originator>Secmail</Originator> <FlashingSMS>0</FlashingSMS> <Recipient> <PhoneNumber>00\$countrycode\$localnumber</PhoneNumber> </Recipient> <MessageData><![CDATA[\$sms]]></MessageData> <Action>SendTextSMS</Action> </aspsms></pre>  Hinweis: Flashing SMS Mittels der Funktion „Flashing SMS“ wird eine Text-Meldung direkt auf dem Display des Empfängers angezeigt. Der Empfänger braucht nicht durch die Menüs des Handys zu blättern. Jedoch wird die Meldung dann nicht gespeichert und ist somit nach dem Schließen weg. </td></tr> </table>	\$sms: text message	zu übermittelnder Nachrichtentext.	\$number: cell number including country code (+xx...)	Mobilfunkrufnummer inklusive Landesvorwahl (+xx...)  Hinweis: Wird die Nummer statt mit +xx... im Format 00xx... benötigt, so kann dies gegebenenfalls mittels 00\$countrycode\$localnumber zusammengesetzt werden.	\$countrycode: country code, e.g. „49“	Landesvorwahl, zum Beispiel „49“ für Deutschland	\$localnumber: cell number without country code	Mobilfunkrufnummer OHNE Landesvorwahl	XML Example:		Server:	https://xml1.aspsms.com	String:	<pre><?xml version="1.0" encoding="UTF-8"?> <aspsms> <Userkey>xyz</Userkey> <Password>xyz</Password> <Originator>Secmail</Originator> <FlashingSMS>0</FlashingSMS> <Recipient> <PhoneNumber>00\$countrycode\$localnumber</PhoneNumber> </Recipient> <MessageData><![CDATA[\$sms]]></MessageData> <Action>SendTextSMS</Action> </aspsms></pre>  Hinweis: Flashing SMS Mittels der Funktion „Flashing SMS“ wird eine Text-Meldung direkt auf dem Display des Empfängers angezeigt. Der Empfänger braucht nicht durch die Menüs des Handys zu blättern. Jedoch wird die Meldung dann nicht gespeichert und ist somit nach dem Schließen weg.
\$sms: text message	zu übermittelnder Nachrichtentext.														
\$number: cell number including country code (+xx...)	Mobilfunkrufnummer inklusive Landesvorwahl (+xx...)  Hinweis: Wird die Nummer statt mit +xx... im Format 00xx... benötigt, so kann dies gegebenenfalls mittels 00\$countrycode\$localnumber zusammengesetzt werden.														
\$countrycode: country code, e.g. „49“	Landesvorwahl, zum Beispiel „49“ für Deutschland														
\$localnumber: cell number without country code	Mobilfunkrufnummer OHNE Landesvorwahl														
XML Example:															
Server:	https://xml1.aspsms.com														
String:	<pre><?xml version="1.0" encoding="UTF-8"?> <aspsms> <Userkey>xyz</Userkey> <Password>xyz</Password> <Originator>Secmail</Originator> <FlashingSMS>0</FlashingSMS> <Recipient> <PhoneNumber>00\$countrycode\$localnumber</PhoneNumber> </Recipient> <MessageData><![CDATA[\$sms]]></MessageData> <Action>SendTextSMS</Action> </aspsms></pre>  Hinweis: Flashing SMS Mittels der Funktion „Flashing SMS“ wird eine Text-Meldung direkt auf dem Display des Empfängers angezeigt. Der Empfänger braucht nicht durch die Menüs des Handys zu blättern. Jedoch wird die Meldung dann nicht gespeichert und ist somit nach dem Schließen weg.														
 Use HTTP GET service (configuration below)	An dieser Stelle werden die Zugangsdaten für den SMS Versand Dienst per HTTP Get eingetragen. <table> <tr> <td>Server address:</td><td>Den Server für den Zugang zum HTTP Get Service stellt SMS-Provider zur Verfügung.</td></tr> <tr> <td>HTTP Get String</td><td>Den String für den Zugang zum HTTP Get Service stellt SMS-Provider zur Verfügung.</td></tr> </table>	Server address:	Den Server für den Zugang zum HTTP Get Service stellt SMS-Provider zur Verfügung.	HTTP Get String	Den String für den Zugang zum HTTP Get Service stellt SMS-Provider zur Verfügung.										
Server address:	Den Server für den Zugang zum HTTP Get Service stellt SMS-Provider zur Verfügung.														
HTTP Get String	Den String für den Zugang zum HTTP Get Service stellt SMS-Provider zur Verfügung.														

Parameter	Beschreibung						
	Es stehen die aus der XML-Konfiguration bekannten Variablen zur Verfügung. Weiterhin wird die Beispielkonfiguration für den Schweizer Dienst „chrus“ angezeigt. <table border="1"> <tr> <td colspan="2">HTTP GET Example:</td></tr> <tr> <td>Server:</td><td>https://www.chrus.ch</td></tr> <tr> <td>String:</td><td>/mysms/http/send.php? user=xyz&pwd=xyz&from=Secmail&to=\$number&msg=\$sms</td></tr> </table>	HTTP GET Example:		Server:	https://www.chrus.ch	String:	/mysms/http/send.php? user=xyz&pwd=xyz&from=Secmail&to=\$number&msg=\$sms
HTTP GET Example:							
Server:	https://www.chrus.ch						
String:	/mysms/http/send.php? user=xyz&pwd=xyz&from=Secmail&to=\$number&msg=\$sms						
 Access to GINA send password form:	Über diese Option wird der Zugriff auf den Passwort-Versand-Link der Appliance gesteuert.						
  Disabled	Standardeinstellung. Damit wird der Passwort-Versand-Link deaktiviert. Somit erscheint dieser auch nicht in der Passwort-E-Mail, welche beim initialen Versand einer GINA-E-Mail an den Absender der E-Mail gesendet wird.						
  Available via public GINA GUI	Aktiviert das Einfügen des Links für den SMS-Passwort-Versand in der GINA-Passwort-Benachrichtigungs-E-Mail an den Absender.						

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

7.17.1 Create New GINA Domain

Dieses Sub-Menü wird aus **GINA Domains**^[416] **Domains**^[416] aufgerufen.

Sektion **Create new GINA domain**

Parameter	Beschreibung
 Description	Hier ist der Name einzugeben, welcher im Auswahllistenmenü GINA Domains ^[416] Domains ^[416] angezeigt werden soll.
 Hostname	Ist unter GINA Domains^[416] Domains^[416] die Option Use virtual hosting^[417] aktiviert, so ist hier der FQDN anzugeben, unter welchem das Interface erreichbar sein wird (zum Beispiel <code>securemail.meinkunde1.tld</code>). Andernfalls ist hier der Name des Unterverzeichnisses anzugeben, in welchem das GINA-Domain erzeugt werden soll, (zum Beispiel <code>mandant1</code>). Das neue GINA-Domain wird dann im Unterverzeichnis des unter dem FQDN des [default]-GINA-Eintrages erreichbar sein (zum Beispiel <code>https://securemail.meinefirma.tld/mandant1/web.app</code>)  Achtung: An dieser Stelle wird Groß-/Kleinschreibung unterschieden. Das heißt, wird statt <code>mandant1</code> <code>Mandant1</code> als Name verwendet, so würde sich auch die URL dementsprechend ändern, also <code>https://securemail.meinefirma.tld/Mandant1/web.app</code>
 Master template	Durch Auswahl eines Master templates werden bereits beim Anlegen einer neuen GINA-Domain alle Einstellungen aus der hier gewählten GINA-Domain übernommen. Diese Einstellungen können bei Bedarf im Nachgang über CHANGE GINA SETTINGS FOR ^[423] für diese neue GINA-Domain angepasst werden.
 Settings	
 ☐ Use virtual hosting	Nur sichtbar, wenn im übergeordneten Menü GINA Domains ^[416] Settings ^[416] Use virtual hosting ^[417] : Use domain settings ^[417] ausgewählt wurde. Diese Option ist im Standard inaktiv.

Über die Schaltfläche **Create** wird der Vorgang abgeschlossen.

7.17.2 Change GINA Settings For

Dieses Sub-Menü wird aus **GINA Domains** ^[416] **Domains** ^[416] aufgerufen.

In diesem Menü können die Einstellungen für die gewählte GINA-Domain individuell vorgenommen werden. Zusätzlich zu den technischen Einstellungen kann über die Schaltfläche **Edit GINA Layout** jeweils das Design an die Firmenidentität angepasst werden (siehe **LAYOUT** ^[453]).



(entfällt in 12.0)

Achtung:

Beim Einsatz von Frontend-Servern (siehe Cluster ^[383] **Add this device as frontend server** ^[385]) muss jede Änderung in diesen Menüs durch erneutes Speichern am Frontend-Server (Save) bekannt gemacht werden.

Sektion **Secure GINA host** ^[422]

Parameter	Beschreibung
 Hostname	Sofern nicht die [default] GINA-Domain zum Editieren ausgewählt wurde, so ist der Hostname bereits mit dem Wert, welcher beim Erzeugen eingetragen wurde (siehe CREATE NEW GINA DOMAIN ^[422] Create new GINA domain ^[422]) vorausgefüllt.  Achtung: Der hier eingetragene Hostname sollte im produktiven Betrieb keinesfalls geändert werden! Dies würde dazu führen, dass bereits versendete GINA-Mails vom Empfänger nicht mehr entschlüsselt werden können.
 ☐ Use virtual hosting	Nur sichtbar, wenn im übergeordneten Menü GINA Domains ^[416] Settings ^[416] Use virtual hosting ^[417] „Use domain settings“ ausgewählt wurde. Diese Option ist im Standard inaktiv.
 Additional hostnames	Diese Option erscheint nur dann aktiv, wenn Use virtual hosting in diesem oder im übergeordneten Menü GINA Domains ^[416] Settings ^[416] NACHTRÄGLICH aktiviert wurde. Wurde die Einstellung Use virtual hosting bereits bei der initialen Installation gewählt, so ist dieses Feld zwar zu sehen, bleibt aber inaktiv (grau). Wird eine bereits produktive SEPPmail Appliance im Nachgang auf Use virtual hosting umgestellt, so ist bei jedem einzelnen GINA-Interface (außer [default]) der vorhandene Hostname in Additional hostnames zu übertragen. Damit wird gewährleistet, dass bereits versendete GINA-Mails nach wie vor durch den GINA-Empfänger gelesen werden können. Somit bleibt das jeweilige GINA-Interface unter der URL erreichbar, wie sie vor dem Umstellen lautete, zum Beispiel https://securemail.msp.tld/mandant1/web.app wie auch unter neuen URL mit dem unter Hostname eingetragenen FQDN, zum Beispiel https://securemail.mandant1.de/web.app
 Port	Diese Option erscheint nur dann aktiv, wenn Use virtual hosting in diesem oder im übergeordneten Menü GINA Domains ^[416] Settings ^[416] aktiviert wurde. In diesem Fall kann für jede GINA-Domain ein spezieller Port gewählt werden.
 SSL-Certificate	Diese Option erscheint nur dann aktiv, wenn Use virtual hosting in diesem oder im übergeordneten Menü GINA Domains ^[416] Settings ^[416] aktiviert wurde. Da mit dieser Einstellung für jede GINA-Domain ein eigener FQDN verwendet wird, ist auch für jeden FQDN ein passendes SSL Schlüsselpaar zu verwenden, welches über Edit - analog zu SSL ^[319] - zu generieren, beziehungsweise importieren ist.

Parameter	Beschreibung
	Wird hier kein Eintrag vorgenommen, wird das Schlüsselpaar aus SSL ^[319] verwendet.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

Sektion **Master template**

Diese Sektion erscheint nur, falls eine andere als die [default] GINA-Domain editiert wird.

Parameter	Beschreibung
 Master template	Durch Auswahl eines Master templates können in den folgenden Sektionen wahlweise die Einstellungen einer anderen GINA-Domain übernommen werden. Wird diese Auswahl in einer Sektion getroffen, so werden nach dem Klicken der Schaltfläche Save die Eingabefelder dieser Sektion ausgegraut und die Einstellungen des ausgewählten Master templates angezeigt.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

Sektion **Admin**

Einstellungen für den Versand von GINA-Systemmeldungen.

Parameter	Beschreibung
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template ^[424] gewählten Vorlage übernommen.
 Admin e-mail	Die hier eingegebene E-Mail Adresse wird als Absender für GINA-Passwort- und Aktivierungs-E-Mails verwendet. Bleibt das Feld leer, so wird jeweils der interne Absender der GINA-E-Mail auch als Absender für die entsprechenden GINA-Passwort- und Aktivierungs-E-Mails verwendet. Weiterhin kann für die jeweils unterschiedlichen Situationen der Folgeoption Password recipient festgelegt werden, dass im Bedarfsfall anstatt des Absenders einer GINA-Mail (Send to original sender) die hier eingegebene E-Mail Adresse (Send to admin address) benachrichtigt wird.  Hinweis: Empfohlen wird eine Hotline Adresse zu verwenden, welche unter Users ^[396] mit Passwort eingerichtet und in Groups ^[413] mindestens den webmailaccountsadmin ^[415] zugeordnet sein sollte, um GINA-Accounts ^[462] bearbeiten zu können. In mandantenfähigen Systemen haben die Customer Administrators ^[496] generell Zugriff auf ihre GINA accounts ^[462]. Somit sollte hier die Admin e-mail gegebenenfalls auch in die jeweiligen Customer Administrators ^[496] aufgenommen werden. Weiterhin kann das Leerlassen dieses Feldes zu Problemen mit SPF Filtern führen, wenn zum Beispiel die SEPPmail Appliance zentral bei einem Managed Service Provider (MSP), der E-Mail Server der

Parameter	Beschreibung
	Managed domain ^[247] (siehe Spalte Server IP address ^[247]) eines Kunden/Mandanten jedoch on premises steht.
 Password recipient	Bestimmt den jeweiligen Adressaten für GINA-Passwort- und Aktivierungs-E-Mails für
 For initial GINA password delivery:	die initiale GINA-Passwort E-Mail, welche beim erstmaligen GINA-Mail Versand an einen noch unbekannten Empfänger generiert wird.
 ☐ Send to admin address	Das Initial-Passwort wird an die eingetragene Admin e-mail gesendet.
 ☒ Send to original sender	Standardeinstellung. Das Initial-Passwort wird an den ursprünglichen Versender der GINA-E-Mail gesendet.
 For registered GINA account reset:	eine Passwort Rücksetzungsanfrage von Benutzern, welche den Registrierungsprozess nach Erhalt der initialen GINA-Mail bereits durchlaufen haben.
 ☐ Send to admin address	Die Passwort Anfrage wird an die eingetragene Admin e-mail gesendet.
 ☒ Send to original sender	Standardeinstellung. Die Passwort Anfrage wird an den ursprünglichen Versender der GINA-E-Mail gesendet.  Achtung: Der ursprüngliche Versender der E-Mail wird - sofern das GINA-Portal durch Aufruf der Datei secure-email.html aus der Träger-E-Mail aufgerufen wurde - aus der Original E-Mail extrahiert. Wird das GINA-Portal direkt - also beispielsweise https://securemail.meinefirma.tld/web.app - aufgerufen, so wird als ursprünglicher Versender der Creator aus GINA accounts ^[462] verwendet. Da bei selbstregistrierten GINA-Benutzern (siehe Extended settings ^[437] Allow account self-registration in GINA portal without initial mail ^[432]) systembedingt kein interner Creator existiert, wird ein Passwort Reset ohne Self-Service Password Management (SSPM) ^[53] in dieser Konstellation fehlschlagen. Aus diesem Grund ist diese Option in oben genannter Kombination nur bedingt zu empfehlen!
 For unregistered GINA account reset:	eine Passwort Rücksetzungsanfrage von Benutzern, welche nach Erhalt der initialen GINA-Mail den Registrierungsprozess noch nicht durchlaufen haben.  Hinweis: Wird kein Initialpasswort verwendet (Initial password ^[430] Password length wurde auf „0“ gesetzt oder die Option Mail Processing ^[286] Ruleset generator ^[287] Encryption ^[292] Outgoing e-mails „Create GINA users with empty password if the following text is in the subject:“ ^[294] ist aktiv und der entsprechende Trigger wurde in der initialen GINA-Mail gesetzt) so würde beim Versuch des Passwort-Resets eine Kombination der Meldungen aus msgid „no_reset“ und „secmal_or_gosupport“ (siehe EDIT TRANSLATIONS

Parameter	Beschreibung
	FOR LANGUAGE ^[459] Edit translations file ^[460] ausgegeben werden.
 ☐ Send to admin address	Die Passwort-Reset-E-Mail wird an die eingetragene Admin e-mail gesendet.
 ☐ Send to original sender	Standardeinstellung. Die Passwort-Reset-E-Mail wird an den ursprünglichen Versender der initialen GINA-E-Mail gesendet.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

Sektion IDP Settings (neu in 12.1)

Definiert die Einstellungen für externe Identitätsanbieter (ISPs) für das Authentisieren an der GINA-Oberfläche.

Parameter	Beschreibung
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template ^[424] gewählten Vorlage übernommen.

 SAML authentication	
 New SAML authentication	Für das Anlegen neuer Verbindungen zu SAML IDPs steht der der Abschnitt New SAML authentication zur Verfügung.
<Name> SAML authentication	Für eventuell bereits angelegte Konfigurationen erscheint jeweils ein Abschnit mit dem bei der Anlage vergebenen Namen, also <Name> SAML authentication .
 ☐ Authenticate GINA users from this domain with SAML	Diese Option ist im Standard inaktiv. Aktiviert die „externe SAML Authentisierung“ für GINA-Benutzer.
 ☐ Automatically create GINA account if user can authenticate with SAML	Diese Option ist im Standard inaktiv. Wird diese Option aktiviert, so wird - sofern nicht bereits vorhanden - automatisiert ein GINA Account ^[462] bei erfolgreichem Authentisieren via SAML angelegt. Der Registrierungsprozess beim initialen Anmelden entfällt somit für den GINA-Benutzer. Auf mandantenfähigen Systemen sind zwingend die Hinweise in Customers Notes ^[495] bezüglich des Zuordnens von GINA Domains ^[416] zu beachten. Wird die Option im Nachhinein deaktiviert, so werden die bereits vorhandenen GINA-Benutzer beim nächsten Anmelden aufgefordert sich zu registrieren.

SAML authentication	
	 Hinweis: Wird über dieses Verfahren ein GINA Account für einen internen Benutzer, also ein Benutzer aus einer Managed Domain angelegt, so wird - sofern nicht bereits vorhanden - auch automatisiert ein User angelegt. Hierfür wird wiederum eine freie Signatur und Verschlüsselung Lizenz (siehe Encryption/Signature licenses) benötigt. Ist diese Option nicht aktiviert, so müssen die GINA Accounts weiterhin auf der SEPPmail Appliance registriert werden. Dabei muss ein lokales Passwort gesetzt werden. Dieses Passwort wird jedoch nicht für das Authentisieren verwendet, solange das Authentisieren via IDP aktiv ist. Während des initialen Registrierens des Accounts wird ein entsprechender Hinweis angezeigt. Wird beim Anmelden am GINA-Portal das lokale statt dem IDP Passwort verwendet, dann - und nur dann! - erhält der Benutzer einen entsprechenden Hinweis (siehe GINA Domains Domain GINA Edit CHANGE GINA SETTINGS FOR Language settings Edit translations Edit translation file Advanced view Edit translation file msgid „ext_auth_enabled“).
 Used by managed domains ▼	Auswahl-Menü, über welches diejenigen Managed Domains zugeordnet werden können, für welche die jeweils eingerichtete Authentisierung verwendet werden soll. Dabei...
 Search	steht über das Eingabefeld eine Suchfunktion für die eingerichteten Managed Domains zur Verfügung.
 (un)select all	können mittels select all , beziehungsweise unselect all alle Managed Domains gleichzeitig hinzugefügt oder entfernt werden.
 ☐ / ☒	sind die die einzelnen Managed Domains an, beziehungsweise abzuwählen.
 IDP service name	Frei wählbarer Name des hier eingerichteten Dienstes.
IDP metadata XML file	Angabe des Pfads zur XML-Konfigurationsdatei des SAML Identity Providers.
 SP Entity ID	Angabe der eindeutigen ID des Betreibers der SEPPmail Appliance. Diese ID wird in der Regel vom IDP bereit gestellt
 Email attribute	Angabe des Attributs, welches IDP seitig die E-Mail Adresse des GINA Accounts (siehe auch User Data E-Mail) enthält.
 Name attribute	Angabe des Attributs, welches IDP seitig den Klarnamen des GINA Accounts enthält. Bleibt das Eingabefeld leer, so wird bei der Anlage (siehe auch Automatically create GINA account if user can authenticate with SAML dieses Abschnitts) eines neuen GINA Accounts als Klarname (User Data Name) ebenfalls die E-Mail Adresse aus Email attribute eingetragen.
 Mobile attribute	Angabe des Attributs, welches IDP seitig die Mobilfunknummer des GINA Accounts enthält. Bleibt das Eingabefeld leer, so bleibt bei der Anlage des GINA Accounts auch das Feld User Data Mobile number leer.
 PKCS12 identity file	Zertifikat für das Authentisieren von Abfragen beim IDP. Diese Datei wird in der Regel vom IDP bereit gestellt und ist mit einem Passwort versehen (siehe Parameter PKCS12 password) Ist der Zugang zum IDP erfolgreich, so erscheint an dieser Stelle die Meldung an operator certificate with valid password has been found.

SAML authentication		
		 Hinweis: Ab 30 Tage vor Ablauf des Operator Zertifikats wird eine Meldung im Daily Report ^[96] (siehe auch Groups ^[413] admin ^[413] und statisticsadmin ^[415]) eingefügt, und der Status des Daily Report ^[96] wird zu IMPORTANT geändert..
	PKCS12 Password	Passwort für das Freischalten des im PKCS12 identity file enthaltenen „private keys“. Auch dieses wird vom IDP bereit gestellt.
	Login button CSS class(es)	Im Standard vorbelegt mit „btn-default idp-btn“. Gibt die CSS Klasse der Anmelde-Schaltfläche für das weitere Verwenden in der GINA-Oberfläche (siehe auch LAYOUT ^[453] GINA CSS ^[455]) an.
	Login button icon	Ermöglicht das Einfügen einer Bild-Datei, welche mit der Anmelde-Schaltfläche als Icon angezeigt wird.
	Icon css class	Im Standard vorbelegt mit „idp-icon“. Gibt die CSS Klasse des Anmelde-Schaltflächen-Icons für das weitere Verwenden in der GINA-Oberfläche (siehe auch LAYOUT ^[453] GINA CSS ^[455]) an.
	Add	Add erscheint ausschließlich beim Abschnitt New SAML authentication .
	Save Delete	Die Schaltflächen Save und Delete erscheinen ausschließlich beim bereits vorhandenen Konfigurationen, also <Name> SAML authentication .

OAUTH authentication		
	New OAUTH authentication	Für das Anlegen neuer Verbindungen zu OAUTH IDPs steht der der Abschnitt New OAUTH authentication zur Verfügung.
	<Name> OAUTH authentication	Für eventuell bereits angelegte Konfigurationen erscheint jeweils ein Abschnitt mit dem bei der Anlage vergebenen Namen, also <Name> OAUTH authentication .
	Authenticate GINA users from this domain with OAUTH	Diese Option ist im Standard inaktiv. Aktiviert die „externe OAUTH Authentisierung“ für GINA-Benutzer.
	Automatically create GINA account if user can authenticate with OAUTH	Diese Option ist im Standard inaktiv. Wird diese Option aktiviert, so wird - sofern nicht bereits vorhanden - automatisiert ein GINA Account ^[462] bei erfolgreichem Authentisieren via OAUTH angelegt. Der Registrierungsprozess beim initialen Anmelden entfällt somit für den GINA-Benutzer. Auf mandantenfähigen Systemen sind zwingend die Hinweise in Customers Notes ^[495] bezüglich des Zuordnens von GINA Domains ^[416] zu beachten. Wird die Option im Nachhinein deaktiviert, so werden die bereits vorhandenen GINA-Benutzer beim nächsten Anmelden aufgefordert sich zu registrieren.

 OAuth authentication	
 Used by managed domains 	 Hinweis: Wird über dieses Verfahren ein GINA Account ^[462] für einen internen Benutzer, also ein Benutzer aus einer Managed Domain ^[247] angelegt, so wird - sofern nicht bereits vorhanden - auch automatisiert ein User ^[396] angelegt. Hierfür wird wiederum eine freie Signatur und Verschlüsselung ^[127] Lizenz (siehe Encryption/Signature licenses ^[221]) benötigt. Ist diese Option nicht aktiviert, so müssen die GINA Accounts ^[462] weiterhin auf der SEPPmail Appliance registriert werden. Dabei muss ein lokales Passwort gesetzt werden. Dieses Passwort wird jedoch nicht für das Authentisieren verwendet, solange das Authentisieren via IDP aktiv ist. Während des initialen Registrierens des Accounts wird ein entsprechender Hinweis angezeigt. Wird beim Anmelden am GINA-Portal das lokale statt dem IDP Passwort verwendet, dann - und nur dann! - erhält der Benutzer einen entsprechenden Hinweis (siehe GINA Domains ^[416] Domain ^[416] GINA Edit CHANGE GINA SETTINGS FOR ^[423] Language settings ^[446] Edit translations Edit translation file ^[460] Advanced view Edit translation file ^[460] msgid „ext_auth_enabled“).
	Auswahl-Menü, über welches diejenigen Managed Domains ^[247] zugeordnet werden können, für welche die jeweils eingerichtete Authentisierung verwendet werden soll. Dabei...
	 Search steht über das Eingabefeld eine Suchfunktion für die eingerichteten Managed Domains ^[247] zur Verfügung.
	 (un)select all können mittels select all , beziehungsweise unselect all alle Managed Domains ^[247] gleichzeitig hinzugefügt oder entfernt werden.
	 ☐ / ☒ sind die die einzelnen Managed Domains ^[247] an, beziehungsweise abzuwählen.
 IDP service name	Frei wählbarer Name des hier eingerichteten Dienstes.
 Service provider 	Über dieses Auswahlménü wird der anzubindende OAuth ISP gewählt
 Facebook  Google  LinkedIn  M365	In der Regel muss beim jeweiligen ISP ein Konto angelegt werden. Daraus resultieren dann auch die Inhalte der Folgefelder ID und Secret.  Hinweis: Die voreingestellten CSS Klassen des Standard GINA-LAYOUT ^[453] können unter GINA CSS ^[453] über Download LESS template mit heruntergeladen werden. Somit können diese bei Bedarf auch bei bereits vorhanden, angepassten GINA-Oberflächen manuell mit eingebunden werden.  Achtung: Wird ein IDP gewählt, welcher zugleich E-Mail Provider ist Beispielsweise Google oder Microsoft), so besteht die Gefahr, dass durch ein eventuelles Kompromittieren des E-Mail Postfachs auch der Zugang zu dessen GINA-Nachrichten möglich wird.
 ID	Angabe der ID für das Authentisieren von Abfragen beim IDP. Diese wird in der Regel beim Registrieren beim jeweiligen IDP generiert, ebenso wie das zugehörige Secret .

🔗 OAUTH authentication		
	🔗 Secret	Zur ID zugehöriges Passwort.
	🔗 Login button CSS class(es)	Im Standard vorbelegt mit „btn-default idp-btn“. Gibt die CSS Klasse der Anmelde-Schaltfläche für das weitere Verwenden in der GINA-Oberfläche (siehe auch LAYOUT ^[453] GINA CSS ^[455]) an.
	🔗 Login button icon	Ermöglicht das Einfügen einer Bild-Datei, welche mit der Anmelde-Schaltfläche als Icon angezeigt wird.
	🔗 Icon css class	Im Standard vorbelegt mit „idp-icon“. Gibt die CSS Klasse des Anmelde-Schaltflächen-Icons für das weitere Verwenden in der GINA-Oberfläche (siehe auch LAYOUT ^[453] GINA CSS ^[455]) an.
Add		Add erscheint ausschließlich beim Abschnitt New OAUTH authentication .
Save Delete		Die Schaltflächen Save und Delete erscheinen ausschließlich beim bereits vorhandenen Konfigurationen, also <Name> OAUTH authentication .

🔗 **Sektion Mandatory registration fields** (neu in 12.1)

Diese Sektion bietet die Möglichkeit, im Standard optionale Registrierungsfelder zwingend zu machen.

Parameter	Beschreibung
🔗 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template ^[424] gewählten Vorlage übernommen.
🔗 Fields:	
🔗 ☐ Full name	Diese Option ist im Standard inaktiv. Wird die Option aktiviert, so wird das Feld "Voller Name" des Registrierungsprozesses (siehe auch Standard Prozess: Schritt 3 ^[37] Abbildung 3b) zum Pflichtfeld.
🔗 ☐ Mobile number	Diese Option ist im Standard inaktiv. Wird die Option aktiviert, so wird das Feld "Handynummer" des Registrierungsprozesses (siehe auch Standard Prozess: Schritt 3 ^[37] Abbildung 3b) zum Pflichtfeld.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

🔗 **Sektion Initial password**

Parameter	Beschreibung
🔗 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template ^[424] gewählten Vorlage übernommen.

Parameter	Beschreibung
 Password length	Im Standard ist 0 vorausgewählt. Die hier angegebene Passwort-Länge bezieht sich auf das Initial-GINA-Passwort, welches von der Appliance generiert wird. Mit der Passwort-Länge null „0“ ist für das initiale GINA-Anmelden kein Passwort erforderlich. Dadurch wird generell die GINA-Variante 2a (siehe Unterschiedliche Registrierungsarten ^[41]) aktiviert.  Hinweis: Zwar ist die Einstellung null „0“ die komfortabelste, aus Sicherheitsgründen wird jedoch ein Wert größergleich acht „8“ empfohlen. Mögliche Werte sind 0 und zwischen 4 und 16.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

Sektion **Extended settings**

Grundlegende Einstellungen für die über das GINA-Webinterface bereit gestellten Funktionen.

Parameter	Beschreibung
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template ^[42] gewählten Vorlage übernommen.
 Default forward page	Sollte die URL der GINA-Seite ohne den Zusatz „/web.app“ aufgerufen werden, kann an dieser Stelle auf eine andere Seite - zum Beispiel die Homepage des Unternehmens - weitergeleitet werden. Soll dennoch auf das GINA-Portal weitergeleitet werden, so ist die URL einzugeben, wie sie oberhalb der Eingabezeile angezeigt wird. Bleibt man beim Beispiel aus der Sektion Secure GINA host ^[43] würde dort folgendes stehen: Note: If you want to show the GINA login page by default, enter „https://securemail.meinefirma.tld/mandant1/web.app“ (without the quotes)  Hinweis: Bleibt der Eintrag leer, so wird gegebenenfalls auf die Hersteller Homepage weitergeleitet.  Achtung: Wurde unter System ^[22] Advanced view... GINA GUI ^[23] bereits eine Weiterleitung eingerichtet, so ist die Einstellung hier obsolet.
 ☐ Always zip HTML attachments	Diese Option ist im Standard inaktiv.

Parameter	Beschreibung
when encrypting e-mail with GINA technology	Der verschlüsselte HTML Anhang (siehe gegebenenfalls auch Customize the secure attachment file name:) der GINA-Mail wird in eine ZIP Datei gepackt.  Hinweis: Dies wird für die Kompatibilität zu älteren OWA Versionen benötigt. Für einzelne E-Mails kann diese Funktion auch durch das Betreffzeilen Schlüsselwort [164] [zip] gesteuert werden.  Achtung: Durch Aktivieren dieser Option geht die Unabhängigkeit von der eingesetzten Software des Empfängers bei GINA-Mails zum Teil verloren, da für das Entpacken der HTML-Datei aus der ZIP-Datei entsprechende Software vorhanden sein muss.
 ☐ "Send copy to myself" checked by default when writing GINA mails	Diese Option ist im Standard inaktiv. Setzt den Haken für das Senden einer Kopie an den Absender bei über die GINA-Oberfläche verfassten E-Mails als Standard. Dadurch erhält der GINA-Benutzer beim Versenden einer E-Mail diese ebenfalls als GINA-Mail in Kopie und hat somit einen entsprechenden Nachweis über den Versand.
 ☐ Sender receives notification when recipient reads GINA mails	Diese Option ist im Standard inaktiv. Die Lesebestätigung beim Versand von GINA-Mails wird als Standard definiert, kann jedoch für jeden Benutzer unter Users [396] USER 'USER@DOMAIN.TLD' [398] User data [398] Notifications [399] individuell überschrieben werden.  Hinweis: Wurde im E-Mail Client eine Lesebestätigung (Disposition-Notification-To Header) angefordert, so wird in jedem Fall die verlässliche GINA-Lesebestätigung angefordert.
 ☒ Allow account self-registration in GINA portal without initial mail	Im Standard ist diese Option aktiv. Erlaubt Personen, welche sich mit dem GINA-Portal (im Beispiel aus der Sektion Secure GINA host [423], „https://securemail.meinefirma.tld/mandant1/web.app“) verbinden sich ohne initialer GINA-E-Mail zu registrieren. Somit wird einem externen Kommunikationspartner ermöglicht, eine sichere E-Mail Kommunikation über das GINA-Portal auch initial zu starten. Voraussetzung hierfür ist, dass ihm auch eine gültige E-Mail Adresse innerhalb der E-Mail Domäne des SEPPmail Appliance Betreibers bekannt ist beziehungsweise eine entsprechende Auswahl von Empfängern unter Default recipients [438] eingetragen wurde. Dies bedingt auch das Aktivieren der Option Allow GINA users to write new mails.  Hinweis: Durch Erweitern der GINA-URL <a href="https://[default]Hostname[423]/<Hostname[423]/web.app">https://[default]Hostname[423]/<Hostname[423]/web.app also zum Beispiel https://securemail.msp.tld/mandant1/web.app um den Parameter <code>?op=register</code> kann die Selbstregistrierungsseite direkt aufgerufen werden.

Parameter	Beschreibung
	Hinweis: Bei der Selbstregistrierung wird noch kein GINA Account angelegt! Stattdessen wird zunächst eine E-Mail an die neu zu registrierende E-Mail Adresse gesendet, um diese zu verifizieren. Der in dieser E-Mail befindliche Bestätigungs-Link wird mit einem - pro Gateway einmaligen - Schlüssel verschlüsselt. Dadurch wird ein missbräuchliches manuelles Erstellen eines solchen Links unmöglich. Durch Anklicken des Links werden die darin enthaltenen Daten an die SEPPmail Appliance übermittelt. Diese Daten werden erst nach Eingabe des beim Registrieren vergebenen Passwortes entschlüsselt. Das heißt der GINA Account wird erst nach korrekter Eingabe des Passwortes angelegt und der in der E-Mail befindliche Link somit ungültig. Achtung: Diese Option kann nicht in Verbindung mit einem Event login ⁴⁵⁰ verwendet werden!
☐ Prevent associated managed domain accounts from registering in GINA portal	Diese Option ist im Standard inaktiv. Wird die Option aktiviert, so kann sich kein Benutzer mit einer E-Mail Adresse aus einer Managed domain ²⁴⁷ durch self-registration einen GINA-Account erstellen. Das Erstellen von GINA-Accounts durch das Versenden von E-Mails bleibt davon unberührt.
☐ Allow account self-deletion in GINA portal:	Diese Option ist im Standard inaktiv. Erlaubt GINA-Benutzern das Löschen Ihres eigenen Accounts über Ihre „Profil Einstellungen“ der GINA-Oberfläche. Achtung: Durch das Löschen des eigenen Profils wird der GINA-Account sowie alle, vom GINA-Benutzer verwaltbaren Schlüssel/Zertifikate, welche ihm zugeordnet sind, entfernt. Das Lesen noch im Besitz des GINA-Benutzers befindlicher GINA-Mails ist im Anschluss nicht mehr möglich!
☐ Certificate search and management in GINA: 	Hierdurch wird dem angemeldeten GINA-Benutzer • das Suchen von Schlüsselmaterial interner SEPPmail Appliance-Benutzer ermöglicht. • das Hochladen von eigenem Schlüsselmaterial über die GINA-Oberfläche gestattet, um zukünftig S/MIME- beziehungsweise OpenPGP- anstatt GINA-verschlüsselte E-Mails zu erhalten. Hinweis: Welche S/MIME Zertifikate gegebenenfalls Importiert werden können ist von der Auswahl unter ADVANCED SETTINGS ⁴⁷⁸ Advanced settings ⁴⁷⁸ Policies Refuse import of certificates with a signature algorithm using SHA-1 or lower ⁴⁷⁹ abhängig.

Parameter	Beschreibung	
	 Achtung: Ist die Option Allow account self-registration in GINA portal without initial mail aktiv, sollte das Zertifikatsmanagement an dieser Stelle aus Sicherheitsgründen deaktiviert werden.	
	 Disabled	Deaktiviert die Schlüsselverwaltung und Schlüsselsuche über die GINA-Oberfläche komplett.
	 Enabled	Standardeinstellung. Aktiviert die Schlüsselverwaltung und Schlüsselsuche über die GINA-Oberfläche, sowohl für S/MIME als auch OpenPGP.
	 S/MIME only	Aktiviert die Schlüsselverwaltung und Schlüsselsuche über die GINA-Oberfläche ausschließlich für S/MIME.
	 OpenPGP only	Aktiviert die Schlüsselverwaltung und Schlüsselsuche über die GINA-Oberfläche ausschließlich für OpenPGP.
 ☒ Allow download of public domain keys/domain certificates	Im Standard ist diese Option aktiv. Ermöglicht zusätzlich die Suche von öffentlichen Domänen Schlüsseln, von den Managed Domains ^[247], welchen diese GINA zugeordnet ist.  Hinweis: Sofern gewünscht, kann die Anzeige einzelner Domänen Schlüssel - wie im Hinweis ^[275] unter EDIT MANAGED DOMAIN ^[268] S/MIME domain encryption ^[274] beschrieben - unterdrückt werden.	 Hinweis: Die Funktion dieser Optionen setzt eine andere Einstellung als Disabled in der Option Certificate search and management in GINA: voraus.
 ☒ Allow unregistered users to search public keys/certificates of internal users	Im Standard ist diese Option aktiv. Ermöglicht jedem - ohne vorheriges Anmelden - die Schlüsselsuche über die GINA-Oberfläche.  Hinweis: Da für eine Schlüssel Suche über die GINA-Oberfläche immer die E-Mail Adresse des Empfängers eingegeben werden muss, ist ein Address-Harvesting nicht möglich.	
 ☐ Publish local CA certificate on the search page to allow recipients to perform S/MIME signature verification	Diese Option ist im Standard inaktiv. Durch Aktivieren dieser Option taucht auf der GINA-Suchseite ein Link zum Downloads des CA Zertifikates zwischen dem Eingabefeld für die E-Mail Adresse und der Such-Schaltfläche auf, sofern die lokale CA ^[328] eingerichtet ist.	
 ☐ Allow GINA users to write new mails	Diese Option ist im Standard inaktiv. Erlaubt GINA-Benutzern initial E-Mails an Empfänger innerhalb der Managed Domains ^[247] zu senden, welchen diese GINA zugeordnet ist. Diese Einstellung ist in der Regel zwingend, sofern Allow account self-registration in GINA portal without initial mail aktiv ist.	

Parameter	Beschreibung		
 ☐ Do not allow GINA users to edit recipient when replying to e-mails	Diese Option ist im Standard inaktiv. Erlaubt beim Antworten auf GINA-Mails den oder die Empfänger zu editieren. Die angegebenen Empfänger müssen sich jedoch alle innerhalb der Managed Domains ^[247] befinden, welchen diese GINA zugeordnet ist.		
 ☐ Only allow GINA users to write new e-mails to default recipients	Diese Option ist im Standard inaktiv. Erlaubt das Adressieren initialer GINA-Nachrichten (nicht Antworten!) ausschließlich an Default recipients ^[438] .		
 ☐ Allow GINA users to reply to external recipients of GINA messages	Diese Option ist im Standard inaktiv. Erlaubt GINA-Benutzern an alle Empfängern einer GINA-Mail - auch externen, also denen, die nicht der Managed Domains ^[247] angehören, welchen diese GINA zugeordnet ist - zu antworten. Hinweis: Wurde diese Option gewählt, so können bei gleichzeitig deaktivierter Option Do not allow GINA users to edit recipient when replying to e-mails ^[435] nur bereits vorhandene Empfänger durch den GINA-Benutzer entfernt, jedoch keine weiteren hinzugefügt werden.		
 SMTP sender address for sending to external recipients:	Da der Versand der E-Mails an externe Empfänger mit einer existenten E-Mail Adresse innerhalb der Managed Domain ^[247] des ursprünglichen Absenders erfolgen muss (Stichwort SPF Prüfung), ist die Versender-Adresse für die oben genannten Antwort-E-Mails hier einzutragen. Hinweis: Die hier angegebene E-Mail Adresse erhält gegebenenfalls Systembenachrichtigungen wie Bounce- oder Non Delivery Report (NDR) E-Mails.		
 ☐ Allow messages to be downloaded as Outlook message (.msg) files	Diese Option ist im Standard inaktiv. Blendet dem Empfänger einer GINA-E-Mail in der GINA-Oberfläche eine Schaltfläche zum Download der E-Mail im msg-Format - also Outlook - ein. Somit wird der Empfänger in die Lage versetzt die ursprünglich GINA verschlüsselte E-Mail in Outlook im Klartext abzuspeichern.	 Hinweis: Wird nach Abspeichern der Nachricht im Klartext über die „Antworten“ Schaltfläche im E-Mail Client geantwortet, so geschieht dies unverschlüsselt! Daher ist bei Aktivieren dieser Option Vorsicht geboten.	 Hinweis: Bei  ^[107] Mails ist zwar ebenfalls der Download möglich, jedoch wird dann ausschließlich die E-Mail, also ohne Anhänge abgespeichert, um die Funktion des E-Mail-Clients nicht durch zu große Anhänge zu gefährden. In der heruntergeladenen Datei ist dann jeweils ein Hinweis auf die

Parameter	Beschreibung		
 Allow messages to be downloaded as MIME (.eml) files	Diese Option ist im Standard inaktiv. Blendet dem Empfänger einer GINA-E-Mail in der GINA-Oberfläche eine Schaltfläche zum Download der E-Mail im eml-Format für den Import in einen E-Mail Client ein. Somit wird der Empfänger in die Lage versetzt die ursprünglich GINA verschlüsselte E-Mail in seinem E-Mail Client im Klartext abzuspeichern.		
 Allow messages to be downloaded as PDF (.pdf) files	Diese Option ist im Standard inaktiv. Blendet dem Empfänger einer GINA-E-Mail in der GINA-Oberfläche jeweils eine Schaltfläche zur Vorschau, beziehungsweise zum Download der E-Mail im pdf-Format zu Archivierungszwecken ein. Bei -Mails ist zwar ebenfalls der Download möglich, jedoch wird dann ausschließlich der E-Mail-Inhalt, also ohne Anhänge als PDF abgespeichert. Hinweis: Aus sicherheitstechnischen Gründen können beim Generieren der PDF-Datei eingebettete Daten - wie zum Beispiel Bilder - nur als Anhang angefügt werden. Die Fähigkeit die Anhänge separat darzustellen ist vom jeweiligen PDF-Reader abhängig. 		anhängenden Dateien zu finden.
 When encrypting e-mail with GINA technology, use text-only mails	Diese Option ist im Standard inaktiv. Versendet die GINA-Träger-E-Mail im Text- statt im HTML-Format. Dies kann gegebenenfalls notwendig sein, wenn ein Empfänger den Empfang von HTML-Mails nicht zulässt.		
 Extract user IP from proxy request header (use with care)	Diese Option ist im Standard inaktiv. Beim Zugriff auf das GINA-Portal werden die Header X-Original-Remote-Addr und X-Forwarded-For in dieser Reihenfolge abgefragt. Der Inhalt des ersten gefundenen Headers wird dann als IP-Adresse des zugreifenden Nutzers angenommen und im GINA-Log eingetragen. Im Falle von X-Forwarded-For kann dies eine Liste sein. Hinweis: Diese Funktion kann genutzt werden, damit zum Beispiel bei einem  mit vorgeschaltetem Loadbalancer im GINA-Log nicht ausschließlich die IP Adresse des Loadbalancers als Quell-IP für GINA-Zugriffe angezeigt wird. Achtung: Diese Einstellung ist sicherheitstechnisch nicht zu empfehlen, da bereits die Richtigkeit des ursprünglichen Header-Inhalts nicht gewährleistet werden kann. Bei aktiver Option könnte ein Nutzer die genannten Header manuell setzen und somit  		

Parameter	Beschreibung
	die Log Einträge und gegebenenfalls deren Auswertung manipulieren. Um dem vorzubeugen würde ein zusätzliches Proxy-System in der eigenen Infrastruktur benötigt, welches die falschen Header vorher löschen kann und danach auf den korrekten Wert setzt. Weiterhin müsste sichergestellt sein, dass das GINA-Portal nur über diesen Proxy erreicht werden kann.
 Do not add the clients user agent to the session protector originator (neu in 12.1)	Diese Option ist im Standard inaktiv. Durch Aktivieren der Option wird das Anfügen des "User Agent" des Clients für den Identifikator der jeweiligen GINA-Session unterdrückt.  Hinweis: Auf mobilen Endgeräten, insbesondere iOS wechselt mitunter der "User Agent". Dadurch können Anfragen des Clients - also indirekt des GINA-Benutzers - nicht mehr korrekt zugeordnet werden und die Kommunikation bricht ab.
 Force sending of GINA e-mails from this address:	Wird an dieser Stelle eine E-Mail Adresse eingetragen, so wird diese stets als Absender Adresse für GINA-Träger-, Passwort- und Lesebestätigungs-E-Mail verwendet. Im E-Mail Text der Träger-E-Mail wird dann der eigentliche Absender genannt: Sie haben eine verschlüsselte E-Mail von <Eigentlicher Absender> erhalten. Betreff: <Betreff der eigentlichen Nachricht> Ist die hier eingetragene E-Mail Adresse als Benutzer (siehe Users^[396]) mit gültigem S/MIME Schlüsselmaterial vorhanden, so werden die GINA-Träger-, Passwort- und Lesebestätigungs-E-Mail zusätzlich signiert.  Hinweis: Die hier angegebene Absender Adresse muss aus einer Managed domain^[247] stammen, welcher die jeweilige GINA-Domain zugeordnet ist (siehe Mail System^[247] Managed domains^[247]). Weiterhin sollte die Adresse als User auf der Appliance existieren, idealerweise mit gültigem S/MIME Zertifikat (siehe Users^[396] Benutzerdetails^[398] S/MIME^[407]), um die GINA-Träger-, Passwort- und Lesebestätigungs-E-Mail signieren zu können. Auch am Groupware-Server sollte die Adresse existent sein, damit eventuell direkte Antworten - welche irrtümlich nicht über das GINA-Portal erstellt wurden - gegebenenfalls angenommen werden. Beim Einsatz von GINA-Only Lizenzen muss bei Bedarf das Freischalten einer Signatur Lizenz pro GINA-Domain über den Support (support@seppmail.de) beantragt werden.
 Customize the secure attachment file name:	Im Standard lautet der Name des HTML-Containers - welcher die eigentliche E-Mail beinhaltet - in einer GINA-Träger-E-Mail secure-email.html. Soll stattdessen ein alternativer Name (zum Beispiel sichere-E-Mail.html) verwendet werden, so ist dieser in das Eingabefeld dieser Option ohne Dateiendung (also .html) einzutragen, für das genannte Beispiel also sichere-E-Mail.  Hinweis: Aufgrund des unterschiedlichen Umgangs der diversen E-Mail Clients mit Sonderzeichen, kann es zu Abweichungen vom hier eingetragenen Dateinamen kommen. So könnten zum Beispiel Umlaute durch die äquivalenten Vokale ersetzt werden. Im ungünstigsten Falle könnte auch ein neuer, abstrakter, dynamischer Name vom E-Mail Client erzeugt werden!

Parameter	Beschreibung	
 Confirmation password usage: <i>(neu in 12.0)</i>	Mit dem „Bestätigungspasswort“ ist ein weiterer Faktor für das Authentisieren an der GINA-Oberfläche verfügbar.  Achtung: Durch Aktivieren dieser Option darf mittels GINA nur noch ein Empfänger adressiert werden. Wurde mehr als ein Empfänger adressiert und GINA kommt gemäß Verschlüsselungshierarchie bei mehr als einem diese Empfänger zum Einsatz, so würde die E-Mail abgelehnt.  Hinweis: Das durch den Absender der E-Mail im Betreff mittels „[password:xxx]“, „[init:xxx]“ gesetzte Passwort wird beim Versenden aus dem Betreff entfernt und in der E-Mail als Hash hinterlegt. Nach dem Login kann dieses Passwort zusätzlich abgefragt werden.	
 Never ask for password	Standardeinstellung. Mit dieser Einstellung sind die beiden Faktoren „Besitz (die GINA-Nachricht selbst)“ und „Wissen (das GINA-Passwort)“ für das Öffnen einer GINA-Nachricht erforderlich.	
 Always ask for password	Um eine GINA-Nachricht lesen zu können, ist durch den Empfänger jeweils das zusätzliche Passwort bei jedem Lesevorgang zusätzlich einzugeben.	Das Passwort ist an die E-Mail gebunden.
 Ask only once per message	Nur beim initialen Lesevorgang einer GINA-Nachricht ist das zusätzliche Passwort einzugeben. Für weitere Lesevorgänge derselben E-Mail wird das zusätzliche Passwort nicht mehr benötigt.	
 Ask only once per account	Das zusätzliche Passwort ist nur einmalig pro GINA-Empfänger einzugeben.	

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

Sektion Default recipients

Dient dem Vorbelegen des „AN“ Feldes über ein Auswahlmü bei aktivierter Option **Extended settings** ^[43] **Allow GINA users to write new mails** ^[43].

Parameter	Beschreibung	
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template ^[42] gewählten Vorlage übernommen.	
Displayed name	E-mail	☐ Remove
Name wie er dem GINA-User zur Auswahl angeboten wird.	E-Mail Adresse des auszuwählenden Benutzers. Diese ist für den GINA-User in der Auswahl nicht sichtbar!	Durch Setzen des Hakens und anschließendem Speichern, wird der jeweilige Eintrag entfernt.

Displayed name	E-mail	☐ Remove
	Die hier angegebenen E-Mail Adresse muss aus einer Managed domain ^[247] stammen, welcher diese GINA-Domain zugeordnet ist.	

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert. Nach dem Speichern eines Eintrags wird jeweils ein weiteres Eingabefeld eingeblendet.



Hinweis:

Soll zum Beispiel auf einer Internetseite ein Link mit einem oder mehreren fest vordefinierten Empfängern platziert werden, so kann dies durch Erweitern der GINA-URL

[https://\[default\]Hostname^{\[423\]}/<<Hostname^{\[423\]}>/web.app](https://[default]Hostname^[423]/<<Hostname^[423]>/web.app)

also zum Beispiel

<https://securemail.msp.tld/mandant1/web.app>

um den Parameter

?rcpt=

erfolgen. Dabei müssen die Empfänger zunächst mit Semikolon „;“ getrennt und dann Base64 codiert (siehe auch www.base64encode.org) angegeben werden.

Das Eintragen von **Default recipients**^[438] wäre hierfür nicht erforderlich.

Diese Methode ist nur für bereits registrierte GINA-Benutzer möglich.

Beispiel:

Gewünschte, fest definierte Empfänger

info@mandant1.de;sales@mandant1.de

codiert via www.base64encode.org

aW5mb0BjdXN0b21lcjEudGxkO3NhbGVzQGN1c3RvbWVyMS50bGQ=

resultierender Link am oben genannten Beispiel:

[https://securemail.msp.tld/mandant1/web.app?](https://securemail.msp.tld/mandant1/web.app?rcpt=aW5mb0BjdXN0b21lcjEudGxkO3NhbGVzQGN1c3RvbWVyMS50bGQ=)

[rcpt=aW5mb0BjdXN0b21lcjEudGxkO3NhbGVzQGN1c3RvbWVyMS50bGQ=](https://securemail.msp.tld/mandant1/web.app?rcpt=aW5mb0BjdXN0b21lcjEudGxkO3NhbGVzQGN1c3RvbWVyMS50bGQ=)



Ebenso kann der Betreff in gleicher Art und Weise über den Parameter

?subject=

vordefiniert werden.

Auch die **Sprache**^[446] der GINA-Oberfläche kann für den Aufruf vorab definiert werden mit

?lang=

wobei jeweils das Kürzel der **Sprache**^[446] - also zum Beispiel „e“ für **English**^[447] - hinter dem = einzugeben ist.

Sollen mehrere Argumente angegeben werden, so sind diese durch „&“ zu verbinden.

Erweitertes Beispiel:

Vorzugebender Betreff

Bewerbung

codiert via www.base64encode.org

QmV0cmVmZg==

resultierender Gesamt-Link aus beiden Beispielen in Verbindung mit der Vorgabesprache Englisch

[https://securemail.msp.tld/mandant1/web.app?](https://securemail.msp.tld/mandant1/web.app?lang=e&rcpt=aW5mb0BjdXN0b21lcjEudGxkO3NhbGVzQGN1c3RvbWVyMS50bGQ=&subject=QmV0cmVmZg==)

[lang=e&rcpt=aW5mb0BjdXN0b21lcjEudGxkO3NhbGVzQGN1c3RvbWVyMS50bGQ=&subject=QmV0cmVmZg==](https://securemail.msp.tld/mandant1/web.app?lang=e&rcpt=aW5mb0BjdXN0b21lcjEudGxkO3NhbGVzQGN1c3RvbWVyMS50bGQ=&subject=QmV0cmVmZg==)



Sektion Large File Transfer

Einstellungen für das Übertragen großer Dateien. Diese Option steht nur zur Verfügung, wenn **Large File Transfer** **(LFT)**^[107] lizenziert und aktiviert wurde.

**Hinweis:**

Ist eines der Kriterien für den Versand als LFT-Nachricht gegeben, jedoch keine entsprechende Lizenz frei, so wird die Nachricht als „normale“ E-Mail versendet.

**Achtung:**

Nach dem Aktivieren von [LFT](#) ^[107] ist das Ruleset neu zu generieren (siehe [Mail Processing](#) ^[286] [Ruleset generator](#) ^[287] [Save and create ruleset](#)).

Parameter	Beschreibung
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template ^[424] gewählten Vorlage übernommen.
 Outgoing policy	
 The mode used for outgoing messages v	Auswahl des Standard LFT ^[107]-Verfahrens für ausgehende Nachrichten (Richtung Internet).
 Off	Standardeinstellung. Deaktiviert die Funktion
 Plain	 Hinweis: Plain LFT ^[107]s können nicht beantwortet werden, da in diesem Fall kein „echtes“ GINA-Empfängerkonto generiert wird. Ebenso wird in diesem Modus keine GINA-Lesebestätigung ausgestellt.  Hinweis: Das hier ausgewählte Standard Verfahren kann jederzeit durch die im Ruleset generator ^[287] aktiven Trigger • Do not touch mails with the following text in subject • Always encrypt mails with the following text in subject • Always encrypt mails with Outlook "confidential" flag set • Always use GINA technology for mails with the following text in subject • Always use GINA technology for mails with Outlook "private" flag set • Do not encrypt outgoing mails with the following text in subject beziehungsweise der analogen X-Header (siehe Steuern der Appliance ^[164]) übersteuert werden.
 Secure	Bei Auswahl dieser Option muss der Empfänger einer LFT-Mail den GINA-Anmeldeprozess durchlaufen, um die LFT ^[107]-Mail lesen zu können.
 Size (in KiB) above which outgoing	Im Standard ist 10000 voreingestellt.

Parameter	Beschreibung						
messages are treated as large files	Gibt die Grenze - in KiB - an, ab wann eine E-Mail, welche in das Internet gesendet werden soll, als LFT ^[107]-Mail behandelt wird. Dabei gilt zu beachten, dass Anhänge in E-Mails aufgrund der BASE-64 Codierung auf circa $\frac{4}{3}$ der ursprünglichen Größe anwachsen.  Hinweis: Das Übersteuern ist über die in Mail Processing ^[286] Ruleset generator ^[287] Large files ^[303] vorhandenen Optionen möglich. Soll LFT ^[107] ausschließlich per Trigger (siehe oben, beziehungsweise auch Steuern der Appliance ^[164]) gesteuert werden, so ist der jeweilige Schwellwert so hoch (zum Beispiel 9999999999) zu wählen, dass er niemals erreicht werden kann.						
 Maximum size (in KiB) for large files of outgoing messages (set to 0 for no limit, but will not exceed xxxxxx KiB)	Im Standard ist 0 voreingestellt. Gibt eine Maximalgröße für LFT ^[107] Dateien an. Wird hier „0“ (null) eingegeben, so wird kein Limit vorgegeben. Ein Limit ergibt sich jedoch in jedem Fall durch die Größe der LFT ^[107] Partition. Maximal kann dabei ein viertel der Plattengröße pro LFT ^[107]-Mail verwendet werden. Dieses Limit würde dann auch in der GINA-Oberfläche als „Maximalgröße der Anhänge“ angezeigt. Wird beim Einliefern einer übergroßen E-Mail per SMTP das Limit überschritten, so wird die Nachricht mit der Meldung „523 5.3.4 - Message too large (LFT)“ abgewiesen. In der GINA-Oberfläche wird ebenfalls eine Meldung ausgegeben: „Maximalgröße der Nachricht überschritten (xxxx.x MiB)“ Ob und wie (MiB oder MB) die Maximalgröße in der jeweiligen GINA-Oberfläche angezeigt wird, kann in der Übersetzungsdatei (siehe Language settings ^[446] Edit translations EDIT TRANSLATIONS FOR LANGUAGE ^[459] Advanced view Edit Translations files ^[460]) durch Ändern folgender Werte erreicht werden: <table><tr><th>Typ</th><th>Standard Wert (deutsch)</th><th>Beschreibung</th></tr><tr><td>msgid msgstr</td><td>"webmail_size_unit" "MiB"</td><td>Bei Bedarf kann an dieser Stelle die Einheit für die Maximalgröße der Anhänge von MiB (Mebibyte) auf MB (Megabyte) umgestellt werden.</td></tr></table>  Hinweis: Dieser Wert muss größer als der unter Size (in KiB) above which outgoing messages are treated as large files sein!	Typ	Standard Wert (deutsch)	Beschreibung	msgid msgstr	"webmail_size_unit" "MiB"	Bei Bedarf kann an dieser Stelle die Einheit für die Maximalgröße der Anhänge von MiB (Mebibyte) auf MB (Megabyte) umgestellt werden.
Typ	Standard Wert (deutsch)	Beschreibung					
msgid msgstr	"webmail_size_unit" "MiB"	Bei Bedarf kann an dieser Stelle die Einheit für die Maximalgröße der Anhänge von MiB (Mebibyte) auf MB (Megabyte) umgestellt werden.					
 Incoming policy	Hinweis: Generell sind GINA Accounts in der Lage große Datenmengen an interne Empfänger via Large File Transfer zu übertragen. Dem internen Empfänger wird dabei eine Large File Transfer (LFT) ^[128] Lizenz zugewiesen.  Aus diesem Grund sollte gegebenenfalls auf einige Einstellungen besonderes Augenmerk gelegt werden. So sollte Maximum size (in KiB) for large files of incoming messages (set to 0 for no limit, but will not exceed xxxxxx KiB) gegebenenfalls restriktiver gehandhabt werden als in der Outgoing policy. Wird an dieser Stelle kein Limit definiert, kann von einem GINA Account mit nur vier Nachrichten der gesamte LFT-Speicher für den in der Retention policy eingestellte Zeitraum belegt werden.						

Parameter	Beschreibung
	Ebenso sind die Einstellungen der Extended settings ⁴³¹ in diesem Zusammenhang zu betrachten, um gegebenenfalls zu Verhindern, dass ein GINA Account durch das Adressieren einer LFT-Nachricht mit sehr vielen Empfängern im ungünstigsten Fall alle LFT-Lizenzen für 30 Tage bindet. - Ist Allow account selfregistration in GINA portal without initial mail ⁴³² aktiv, versetzt dies jeden potentiellen Kommunikationspartner in die Lage sich zu registrieren und somit im Anschluss große Dateien an einen beliebigen internen Empfänger zu senden. - Ist die oben genannte Option nicht aktiv, kann durch zusätzliches Deaktivieren von Allow GINA users to write new e-mails (not reply) verhindert werden, dass ein GINA Account initial große Nachrichten verfasst. - Die internen Adressaten einer große Nachricht können weiterhin durch Aktivieren von Do not allow GINA users to edit recipient when replying to e-mails, beziehungsweise Only allow GINA users to write new e-mails to default recipients eingeschränkt werden. - Das Deaktivieren von Allow GINA users to reply to external recipients of GINA messages ("Reply All") ist an dieser Stelle eine weitere Möglichkeit des Einschränkens.
 The mode used for incoming messages 	Auswahl des Standard LFT ¹⁰⁷-Verfahrens für eingehende Nachrichten. Hinweis: LFT für eingehende Nachrichten funktioniert ausschließlich über die GINA-Technologie. Eingehende SMTP-Mails bleiben hiervon unberührt.  Achtung: Ist für den internen Empfänger einer eingehenden LFT-Nachricht keine LFT-Lizenz frei oder vorhanden, so kann, bedingt durch den Umstand, dass diese Nachricht dann als „normale“ E-Mail gesendet wird, unter Umständen das interne E-Mail System diese Nachricht aufgrund einer Größenbeschränkung ablehnen. Für diesen Fall muss dafür Sorge getragen werden, dass eine daraufhin vom internen System generierte Bounce-E-Mail den Absender erreicht. Dies ist insbesondere dann relevant, wenn die SEPPmail Appliance als Standalone-Lösung für LFT betrieben wird. 
 Off	Standardeinstellung. Deaktiviert die Funktion
 Plain	Stellt die LFT ¹⁰⁷-Mail sofort und ohne Eingabe eines Passwortes, alleine durch Öffnen des HTML-Anhangs, im GINA-Portal dar. Hinweis: Da der interne E-Mail-Weg von der SEPPmail Appliance bis zum E-Mail-Client bereits abgesichert sein muss und Antworten auf LFT ¹⁰⁷-Mails in der Regel von internen Empfängern nicht erforderlich sind, ist diese Einstellung im Normalfall ausreichend. 

Parameter	Beschreibung						
	 Hinweis: Wird eine LFT ^[107]-Nachricht von einem internen Absender (also aus einer Managed domains ^[247]) an einen internen Empfänger direkt über die GINA-Oberfläche gesendet und überschreitet diese Nachricht nicht den unter Size (in KiB) above which incoming messages are treated as large files ^[443] eingestellten Schwellwert, so würde diese Nachricht als GINA-Nachricht ankommen. Das heißt auch, dass eine Passwort-Eingabe seitens des Empfängers trotz der Einstellung „Plain“ notwendig wäre						
 Secure	Bei Auswahl dieser Option muss der Empfänger einer LFT-Mail den GINA-Anmeldeprozess durchlaufen, um die LFT ^[107]-Mail lesen zu können.  Hinweis: Der Anmeldeprozess für interne Benutzer kann gegebenenfalls durch die Option EDIT MANAGED DOMAIN ^[268] External authentication ^[271] wesentlich zu erleichtern.						
 Size (in KiB) above which incoming messages are treated as large files	Im Standard ist 10000 voreingestellt. Gibt die Grenze - in KiB - an, ab wann eine eingehende GINA-Nachricht als LFT ^[107]-Mail behandelt wird.						
 Maximum size (in KiB) for large files of incoming messages (set to 0 for no limit, but will not exceed xxxxxx KiB)	Im Standard ist 0 voreingestellt. Gibt eine Maximalgröße für LFT ^[107] Dateien an. Wird hier „0“ (null) eingegeben, so wird kein Limit vorgegeben. Ein Limit ergibt sich jedoch in jedem Fall durch die Größe der LFT ^[107] Partition. Maximal kann dabei ein viertel der Plattengröße pro LFT ^[107]-Mail verwendet werden. Dieses Limit würde dann auch in der GINA-Oberfläche als „Maximalgröße der Anhänge“ angezeigt. Wird beim Einliefern einer übergroßen das Limit überschritten, so wird die Nachricht mit der Meldung „Maximalgröße der Nachricht überschritten (xxxx.x MiB)“ in der GINA-Oberfläche abgewiesen. Ob und wie (MiB oder MB) die Maximalgröße in der jeweiligen GINA-Oberfläche angezeigt wird, kann in der Übersetzungsdatei (siehe Language settings ^[446] Edit translations EDIT TRANSLATIONS FOR LANGUAGE ^[459] Advanced view Edit Translations files ^[460]) durch Ändern folgender Werte erreicht werden: <table><tr><th>Typ</th><th>Standard Wert (deutsch)</th><th>Beschreibung</th></tr><tr><td>msgid msgstr</td><td>"webmail_size_unit" "MiB"</td><td>Bei Bedarf kann an dieser Stelle die Einheit für die Maximalgröße der Anhänge von MiB (Mebibyte) auf MB (Megabyte) umgestellt werden.</td></tr></table>  Hinweis: Dieser Wert muss größer als der unter Size (in KiB) above which incoming messages are treated as large files sein!	Typ	Standard Wert (deutsch)	Beschreibung	msgid msgstr	"webmail_size_unit" "MiB"	Bei Bedarf kann an dieser Stelle die Einheit für die Maximalgröße der Anhänge von MiB (Mebibyte) auf MB (Megabyte) umgestellt werden.
Typ	Standard Wert (deutsch)	Beschreibung					
msgid msgstr	"webmail_size_unit" "MiB"	Bei Bedarf kann an dieser Stelle die Einheit für die Maximalgröße der Anhänge von MiB (Mebibyte) auf MB (Megabyte) umgestellt werden.					
 Retention policy							

Parameter	Beschreibung	
 How long (in days) to store large files (set to 0 for no limit. Make sure you have enough storage space, else messages will be dropped)	Im Standard ist 7 voreingestellt. Verweildauer - in Tagen - von LFT 107-Mails auf der SEPPmail Appliance. Der Empfänger bekommt das Verfallsdatum im Betreff der GINA-Benachrichtigungs-E-Mail mitgeteilt. Die Einstellung „0“ null bedeutet, dass LFT 107-Mails nie gelöscht werden. Steht auf dem System nicht genügend Speicher zur Verfügung würden LFT 107-Mails abgewiesen (bounced).  Hinweis: Sofern die LFT 107-Mail vom Empfänger nicht gelesen wird, wird der Absender mindestens 24 (und höchstens 48) Stunden vor dem Ablauf benachrichtigt.	
 Archive Large File Messages on external server	Diese Option ist im Standard inaktiv. Archiviert alle LFT 107-Mails - egal ob ein- oder ausgehend - einmal pro Stunde. Dabei wird im angegebenen Verzeichnis (siehe Path on server) pro Nachricht ein eigenes Verzeichnis, dessen Name unter anderem die Message-ID der Nachricht, sowie die Device-ID der Appliance, von welcher die LFT 107-Mail gesendet wurde, angelegt. In diesem Verzeichnis werden die Anhänge mit ihrem originalen Dateinamen, sowie der Mail-Text (Body) als Datei „messagebody.eml“ abgelegt. Dateien, welche nicht auf das angegeben Ziel übertragen werden können, verbleiben zunächst in einem gesonderten Export-Bereich auf der Appliance. Benötigt das Übertragen einer Datei länger als sechs Stunden, so wird eine Watchdog-Meldung an den Postmaster (siehe Mail System 247 SMTP settings 252) gesendet und alle sechs Stunden wiederholt. Könnte die betroffene Datei innerhalb von 24 Stunden nicht übertragen werden, so wird sie gelöscht. Die Log-Einträge der Archivierung sind im „maillog“ (siehe Logs 388 Show other logs... OTHER LOGS 392 Mail log archive 392 Download complete log) zu finden.	
 Server/Port	Angabe der IP-Adresse oder des Namens, unter welchem der Archiv-Server erreichbar ist.	Angabe des zu verwendenden Kommunikations-Ports für die Verbindung zum Archiv-Server. Der Standard SCP /SFTP Port lautet 22.
 Protocol 	Über das Auswahlménü kann das gewünschte Netzwerk Protokoll für das Übertragen ausgewählt werden.	
 SCP	Standardeinstellung.	
 SFTP		
 User name	Eingabe eines entsprechend berechtigten Benutzers, für das Schreiben der Archive auf den Archiv-Server	
 Key	Über die Download gateway public key kann der Öffentliche Schlüssel der Appliance für die verschlüsselte Kommunikation zum Archiv-Server heruntergeladen werden. Dieser Schlüssel ist auf dem Archiv-Server der Liste der berechtigten Öffentlichen Schlüsseln hinzuzufügen. Auf Unix basierten Systemen ist diese Liste typischerweise im home-Verzeichnis des entsprechenden Benutzers (siehe SCP user name) unter ~/ .ssh/authorized_keys zu finden.	
 Path on server	An dieser Stelle wird der Pfad auf dem Archiv-Server angegeben, unter welchem die LFT-Archivierung Dateien ablegen soll. Wird der Pfad mit einem führenden Schrägstrich „/“ angegeben, so wird ein Absoluter Pfad verwendet. Wird kein führender Schrägstrich angegeben, so wird der Pfad relativ im home-Verzeichnis des entsprechenden Benutzers (siehe SCP user name) angelegt.	

Parameter	Beschreibung
	Für die Angabe des Pfades stehen folgende Variablen zur Verfügung:
%e	E-Mail Adresse des Absenders der LFT-Mail
%y	aktuelles Jahr
%m	aktueller Monat
%d	aktueller Tag
%i	Device ID der Appliance, über welche die LFT-Mail verarbeitet wurde

**Achtung:**

Alle Größenangaben erfolgen in Kibibyte (siehe auch <http://de.wikipedia.org/wiki/Byte>)!

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

**Sektion SOAP**

Alternativ können E-Mails aus Drittanbietersystemen auf der SEPPmail Appliance via SOAP Schnittstelle zur Verschlüsselung eingeliefert werden.

Parameter	Beschreibung
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template ^[424] gewählten Vorlage übernommen.
 ☐ Enable SOAP Handler	Diese Option ist im Standard inaktiv. Über den SOAP-Accesspoint /WebCrypt.Core/services/Service empfangene XML-Daten werden durch das Script webcrypt.app als MIME-Nachricht aufbereitet und ohne Umwege von der Rule Engine verarbeitet. Das Resultat wird als XML-Daten via HTTP zurück an den SOAP-Consumer geleitet. Es findet kein Mail-Versand statt, mit Ausnahme von eventuell generierten Passwort-Mails oder Bounces.
 ☐ Deliver messages received via SOAP directly via SMTP	Diese Option ist im Standard inaktiv. Verändert das oben beschriebene Verhalten der Rule Engine. Die per XML übergebene E-Mail wird nach dem Verschlüsseln direkt mittels SMTP zugestellt. Der Status der Zustellung wird als XML-Nachricht via HTTP zurück an den SOAP-Consumer geleitet.  Hinweis: Da bei mehreren Empfängern nicht mehr unterschieden werden kann, welche Zustellung erfolgreich war und welche nicht, stellt die Schnittstelle sicher, dass pro SOAP-Nachricht nur ein Empfänger angegeben wurde.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

**Sektion Terms of use**

Einstellungen bezüglich Allgemeiner Geschäftsbedingungen.

Parameter	Beschreibung
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template ^[424] gewählten Vorlage übernommen.
 ☐ Require new users to accept terms of use	Diese Option ist im Standard inaktiv. Blendet im GINA-Registrierungsmenü eine zusätzliche Checkbox für das Akzeptieren der Allgemeinen Geschäftsbedingungen ein.
 Terms of use URL	Eingabe der URL zu den Allgemeinen Geschäftsbedingungen zur Nutzung von GINA, zum Beispiel https://www.ihrefirma.tld/agb/GINA .

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

Sektion Language settings

Spracheinstellungen der GINA-Domain und deren Benachrichtigungen.

Parameter		Beschreibung			
 ☒ Use settings from master template		Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template ^[424] gewählten Vorlage übernommen.			
 Default language:		Im Standard ist English vorausgewählt. Über das Auswahlménü wird die Standard-Sprache für die jeweilige GINA-Oberfläche gewählt. Ist bei Available Languages keine Sprache als Enabled markiert, so erscheint in der GINA-Oberfläche (Anmelde-, Willkommen- und Profil-Seite sowie im lokalen Secure Attachment (secure-email.html)) kein Drop-Down-Ménü zur Auswahl der Sprache. In diesem Fall steht ausschließlich die hier gewählte Sprache zur Verfügung. Sofern eine oder mehrere Sprachen unter Available Languages als Enabled markiert wurden, so muss die Default language einer dieser gewählten Sprachen entsprechen.			
 Available languages:		Bei der Auswahl der Sprachen gilt zu beachten, dass mit jeder weiteren Sprache die Länge der <u>initialen(!)</u> GINA-Träger-E-Mail sowie der Passwort-E-Mails zunimmt.			
	Language	Enabled			
	 German (d)	☐ Im Standard sind die ersten fünf Sprachen aktiv. Aktiviert oder deaktiviert	Über die Schaltfläche  öffnet das Untermenü EDIT TRANSLATIONS FOR LANGUAGE ^[459] der jeweiligen Sprache, über welches die Texte aller GINA-Komponenten individuell angepasst werden können.	Über die Schaltfläche  können eventuell vorgenommene Änderungen der Sprachdatei zurückgesetzt werden. Diese Schaltfläche ist nur dann aktiv, wenn die Spracheinstellungen via Edit translations geändert wurden.	Über die Schaltfläche  kann die jeweilige Sprachdatei heruntergeladen werden. Wird diese im Anschluss angepasst, so kann Sie über die [default] GINA-Einstellungen wieder hochgeladen werden.

Parameter		Beschreibung		
 English (e)	die jeweilige Sprache			
 French (f)				
 Italian (i)				
 Spanish (s)				
 Czech (c)				
 Dutch (n)				
 Polish (p)				
 Russian (r)				

Wird die [default] GINA-Domain editiert, so können über die Schaltfläche **Add new** weitere Sprachen hinzugefügt werden. Für das Erstellen einer neuen Sprachdatei ist der einfachste Weg, eine bereits vorhandene über die Schaltfläche **Download** (siehe Tabelle oben) herunter zu laden, zu übersetzen und über die Schaltfläche **Add new** wieder hochzuladen.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.



Hinweis:

Nur die initiale GINA-Benachrichtigungs-E-Mail ist - sofern konfiguriert - mehrsprachig. Jede weitere GINA-Benachrichtigungs-E-Mail wird nur noch in der beim Registrierungsprozess gewählten Sprache versandt.

Je mehr Sprachen aktiviert werden, desto länger werden jedoch die initialen GINA-Benachrichtigungs- und Passwort- E-Mails.

Deshalb sollte der Grundsatz gelten:

Soviel wie nötig, so wenig wie möglich.



Hinweis:

Durch Erweitern der GINA-URL

[https://\[default\]Hostname\[423\]/<Hostname\[423\]/web.app](https://[default]Hostname[423]/<Hostname[423]/web.app)

also zum Beispiel

<https://securemail.msp.tld/mandant1/web.app>

um den Parameter

?lang=e

wird GINA in der definierten Sprache (im Beispiel also **English**[447]) aufgerufen.



Sektion Account login

In dieser Sektion werden die Passwort-Kriterien sowie die Möglichkeiten für das Zurücksetzen von GINA-Passwörtern angegeben.

Parameter	Beschreibung
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template [424] gewählten Vorlage übernommen.

Parameter	Beschreibung
 Choose how the user can retrieve lost passwords	Auswahl der Passwort-Rücksetzungs-Möglichkeiten des GINA-Benutzers.
 default	Standard Einstellung. Diese entspricht der Option „Reset by hotline“.
 Reset by e-mail verification	• Der GINA-Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können. • Daraufhin wird der Benutzer aufgefordert ein neues Passwort einzugeben und dieses zu verifizieren. • Der Benutzer erhält daraufhin eine E-Mail mit einem Link zugesendet. Erst durch Aufruf dieses Links erhält das neu vergebene Passwort seine Gültigkeit.  Achtung: Da diese Variante allein auf dem Medium E-Mail basiert, bedeutet dies einen gewissen Einschnitt in die Sicherheit. Aus diesem Grund ist diese Variante von SEPPmail nicht empfohlen.
 Reset by E-mail verification, no reminder question / answer	• Der GINA-Benutzer wird ohne Sicherheitsfrage aufgefordert ein neues Passwort einzugeben und dieses zu verifizieren. • Der Benutzer erhält daraufhin eine E-Mail mit einem Link zugesendet. Erst durch Aufruf dieses Links erhält das neu vergebene Passwort seine Gültigkeit. • Dies funktioniert jedoch nur, wenn das GINA-Portal über eine GINA-E-Mail aufgerufen wurde, also nicht durch die bloße Anmeldung.  Achtung: Bereits das alleinige Basieren dieser Variante auf dem Medium E-Mail bedeutet einen gewissen Einschnitt in die Sicherheit (siehe oben). Weiterhin ist jedoch in dieser Einstellung bereits der Zugriff eines Angreifers auf das Postfach des GINA-Benutzers ausreichend, um das Passwort zurücksetzen zu können. Ein zweiter Faktor Wissen, also die Antwort auf eine Sicherheitsabfrage ist nicht erforderlich. Dies bedeutet einen weiteren Einschnitt in die Sicherheit. Aus diesem Grund ist diese Variante von SEPPmail absolut nicht empfohlen.
 Reset by hotline	Dies ist die Standardeinstellung. • Der GINA-Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können. • Der Benutzer wird aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben. • Die Hotline beziehungsweise der Original Absender (siehe Admin ⁴²⁴) erhält eine E-Mail mit dem neuen Passwort und der Rückrufnummer des GINA-Benutzers. • Der GINA-Benutzer bekommt sein neues Passwort vom Empfänger der Passwort-Mail mitgeteilt.
 Reset by hotline, no reminder question / answer	• Der GINA-Benutzer wird ohne Sicherheitsfrage zur Eingabe einer Telefonnummer für den Rückruf durch die Hotline aufgefordert. • Dies funktioniert jedoch nur, wenn das GINA-Portal über eine GINA-E-Mail aufgerufen wurde, also nicht durch die bloße Anmeldung. • Die Hotline beziehungsweise der Original Absender (siehe Admin ⁴²⁴) erhält eine E-Mail mit dem neuen Passwort und der Rückrufnummer des GINA-Benutzers. • Der GINA-Benutzer bekommt sein neues Passwort vom Empfänger der Passwort-Mail (Hotline / Original Absender) mitgeteilt.

Parameter	Beschreibung	
	 Hinweis: Bei dieser Einstellung besteht die Schwierigkeit, dass der Rücksetzende (Hotline / Original Absender) die tatsächliche Identität des anzurufenden GINA-Benutzers theoretisch noch einmal verifizieren müsste, da andernfalls ein Angreifer alleine durch den Besitz einer GINA-Mail ein Passwort anfordern könnte.	
 Reset by SMS	Diese Einstellung setzt das Einbinden eines SMS-Dienstes (siehe GINA Domains ^[416] SMS passwords ^[418]) voraus. • Der Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können. • Der GINA-Benutzer bekommt bei einer Passwort Reset Anfrage seine von ihm beim Registrieren eingegebene Mobilfunk-Nummer angezeigt, an welche durch Klicken der Schaltfläche „Senden“ sein neues Passwort gesendet wird. • Wurde bei der Registrierung keine Mobilfunk-Nummer angegeben, so greift Reset by hotline.	
 Reset by SMS, no reminder question / answer	Diese Einstellung setzt das Einbinden eines SMS-Dienstes (siehe GINA Domains ^[416] SMS passwords ^[418]) voraus. • Beim Registrieren muss der GINA-Benutzer zwingend eine Handynummer für den SMS Reset eingegeben. • Der GINA-Benutzer bekommt bei einer Passwort Reset Anfrage ohne Sicherheitsfrage seine beim Registrieren eingegebene Handy-Nummer angezeigt, an welche durch Klicken der Schaltfläche „Senden“ sein neues Passwort gesendet wird. • Dies funktioniert jedoch nur, wenn das GINA-Portal über eine GINA-E-Mail aufgerufen wurde, also nicht durch die bloße Anmeldung. • Wurde beim Registrieren keine Handy-Nummer angegeben, so greift Reset by hotline.	
 Let user choose between hotline and SMS	• Der Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können. • Wurde beim Registrieren eine Handynummer für den SMS Reset eingegeben, so erscheint eine Auswahl, in welcher der Benutzer zwischen seiner Mobilfunk-Nummer (für SMS Reset) und einer einzugebenden Telefonnummer (voreingetragen ist die Mobilfunk-Nummer) für den HelpDesk Rückruf wählen kann. • Steht keine Mobilfunk-Nummer zur Verfügung, so wird der Benutzer aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben.	
 Let user choose between hotline and SMS, no reminder question/ answer (neu in 12.0)	• Wurde beim Registrieren eine Mobilfunk-Nummer für den SMS Reset eingegeben, so erscheint eine Auswahl, in welcher der Benutzer zwischen seiner Mobilfunk-Nummer (für SMS Reset) und einer einzugebenden Telefonnummer (voreingetragen ist die Mobilfunk-Nummer) für den HelpDesk Rückruf wählen kann. • Dies funktioniert jedoch nur, wenn das GINA-Portal über eine GINA-E-Mail aufgerufen wurde, also nicht durch die bloße Anmeldung. • Steht keine Mobilfunk-Nummer zur Verfügung, so wird der Benutzer aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben.	
 Disable user profile and password management	Diese Einstellung unterbindet das Anlegen eines Profils. Ein Passwort Reset ist nicht möglich. Das Anmelden an der GINA-Oberfläche ist nur durch den Aufruf eines GINA-Anhangs (secure-email.html) möglich. In der Regel kommt diese Einstellung nur bei maschinell generierten GINA Accounts zum Einsatz.	
 Minimum password length:	Im Standard ist „min. 8 characters“ vorausgewählt. Gibt die minimale Passwort Länge an. Mögliche Werte liegen zwischen 4 und 16.	

Parameter	Beschreibung	
 ☐ Must contain at least one lower case letter	Diese Option ist im Standard inaktiv. Passwort muss mindestens einen Kleinbuchstaben enthalten.	Hinweis: Bei den hier angegebenen Passwort-Kriterien handelt es sich um das geforderte Sicherheitsminimum. Somit müssen diese Kriterien nicht zwangsläufig eine gute Entropie garantieren. Aus diesem Grund orientiert sich die Anzeige der Passwort-Qualität in der GINA-Oberfläche frei an den verwendeten Zeichen und stellt eine Sicherheitsempfehlung über die Kriterien hinaus dar.
 ☐ Must contain at least one upper case letter	Diese Option ist im Standard inaktiv. Passwort muss mindestens einen Großbuchstaben enthalten.	
 ☐ Must contain at least one number	Diese Option ist im Standard inaktiv. Passwort muss mindestens eine Ziffer enthalten.	
 ☐ Must contain at least one special character	Diese Option ist im Standard inaktiv. Passwort muss mindestens eine Sonderzeichen enthalten.	
 ☐ Must not contain own name or e-mail address	Diese Option ist im Standard inaktiv. Passwort darf nicht die eigene E-Mail Adresse enthalten.	
 ☐ Must be different from previous password(s)	Diese Option ist im Standard inaktiv und der Wert 4 vorausgewählt. Passwort muss sich von den letzten n Passwörtern unterscheiden. Mögliche Werte liegen zwischen 1 und 28.	
 ☐ Must be changed at least every days	Diese Option ist im Standard inaktiv und der Wert 90 vorausgewählt. Passwort muss nach n Tagen geändert werden. Mögliche Werte sind 30, 60, 90, 120.	
 Accounts are locked for minutes after failed login attempts	Im Standard ist die Sperrzeit mit 60 Minuten und die Anzahl der Fehlversuche mit 5 vorgelegt. Gibt die Dauer in Minuten an, für welche ein GINA-Benutzer gesperrt ist, wenn er die angegebene Anzahl von Anmelde-Fehlversuchen erreicht hat.	

**Hinweis:**

Vordefinierte Sicherheitsfragen zur Auswahl können in den jeweiligen Sprachdateien definiert werden (siehe auch [Edit translations file](#) ^[460]), zum Beispiel

```
msgid "question_preset1"
msgstr "Wie lauten die letzten 5 Stellen Ihrer Ausweisnummer?"
```



Generell gilt für Sicherheitsfragen (auch die gegebenenfalls vom Anwender selbst erstellten):

- Die Frage darf die Antwort nicht enthalten.
- Die Antwort darf die E-Mail oder den Namen nicht beinhalten.
- Die Antwort darf alle Teile des Namens oder der E-Mail nicht beinhalten, die größer als zwei Zeichen sind, also im Namen z.B. den Vor- oder Nachnamen, beziehungsweise aus der E-Mail Adresse den Domain-Name oder Teile der lokalen Komponente.

Das gewählte Passwort-Rücksetzverfahren beeinflusst den Detailgrad des Registrierungsprozess (siehe auch [Empfänger – Anmelden und einmaliges Registrieren](#) ^[37]).

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

**Sektion Event login**

In dieser Sektion können vom Standard **Account login** ^[447] abweichende Anmeldeverfahren und Registrierungsprozesse eingestellt werden.



Hinweis:

Alle „Event“ Verfahren beruhen darauf, dass initial eine E-Mail erhalten wurde. Nur so kann ein passendes, gültiges Passwort generiert werden.

Die Einstellung **Extended settings** ^[437] **Allow account self registration in GINA portal without initial mail** ^[432] kann somit **nicht** in Verbindung mit den „Event“ Verfahren angewendet werden.

Parameter	Beschreibung
 Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template ^[424] gewählten Vorlage übernommen.
 Password event:	 Achtung: Das Umstellen des Passwort event bei einer bereits bestehenden GINA-Domain, kann bei bestehenden GINA-Accounts zu unerwünschten Folgeerscheinungen führen. Somit sollte diese Einstellung nach dem initialen Erstellen der GINA-Domain möglichst nicht mehr geändert werden. In • nicht mandantenfähigen Systemen mit mehreren GINA Domains • mandantenfähigen Systemen, bei einem Mandanten mit mehreren GINA-Domains können unterschiedlich eingestellte Verfahren ebenfalls zu unerwünschten Verhaltensweisen führen.
 No password event	Dies ist die Standard Einstellung. Mit dieser Einstellung ist das Account login ^[447] aktiv. Alle anderen Einstellungen setzen das Account login ^[447] außer Kraft.
 Unique e-mail password	Durch Aktivieren dieser Option wird generell die GINA-Variante 4 (siehe GINA-Webmail Unterschiedliche Registrierungsarten ^[417]) aktiviert. Für jede GINA-E-Mail wird ein eigenes E-Mail Passwort generiert, welches auch nur für diese eine GINA-Mail gültig ist. Dieses wird dem Absender über die bekannte Passwort-E-Mail mitgeteilt, welche jedoch zusätzlich Datum und Betreff der ursprünglich an den Empfänger gesendeten E-Mail beinhaltet. Damit ist für den Absender ein problemloses Zuordnen der Passwort-E-Mail zur gesendeten GINA-Mail gewährleistet.  Hinweis: Der Registrierungsprozess entfällt bei dieser Variante vollständig. Aus technischen Gründen wird für den Empfänger dennoch ein GINA Account ^[462] angelegt. Das Passwort-Verhalten bleibt davon aber unbeeinträchtigt.
 One-time password via SMS only	Durch Aktivieren dieser Option wird generell die GINA-Variante 3 (siehe GINA-Webmail Unterschiedliche Registrierungsarten ^[417]) aktiviert. Dabei ist eine Rufnummer des Empfängers, welche SMS empfangen kann, zwingend. Das Registrieren des GINA-Benutzers ist weiterhin notwendig, da die SMS-Rufnummer noch bestätigt werden muss. Das Initial-Passwort unterliegt ebenfalls den Einstellungen unter Initial password ^[430] Password length ^[437] . Sofern der GINA-Benutzer nicht bereits ein Initial-Passwort vom Ansender per SMS erhalten hat, trägt er seine Mobilfunk-Nummer während des Registrierungsprozesses ein.

Parameter	Beschreibung
 One-time password via SMS (account password available)	Wie One-time password via SMS only , allerdings wird hier zusätzlich ein Account angelegt. Der GINA-Benutzer kann somit sowohl das via SMS gesendete Kennwort, wie auch sein Account login ^[44] Passwort verwenden. Somit kann er auch zum Beispiel selbstständig seine Mobilfunk-Nummer für den SMS-Empfang ändern.
 Password strength:	Im Standard ist der Wert 8 vorausgewählt. Die hier angegebene Passwort-Länge bezieht sich auf das von der Appliance für den jeweils eingestellten Password event generierte Passwort. Mögliche Werte liegen zwischen 5 und 16.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

Sektion Certificate login

Ermöglicht das Anmelden an das GINA-Portal mittels Client-Zertifikat. Hierfür muss das Wurzel-Zertifikat der CA, welche die Login Zertifikate ausstellt in das Eingabefeld eingefügt werden.

Parameter	Beschreibung
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template ^[42] gewählten Vorlage übernommen.

Der zugreifende Benutzer muss sein entsprechendes Benutzer-Zertifikat in seinem Browser installiert haben.
Sollte mehr als eine GINA-Domain konfiguriert werden, so ist für diese Art des Logins die Option **Use virtual hosting** ^[41] (siehe **GINA Domains** ^[416] **Settings** ^[416]) zu verwenden.
Weiterhin ist diese Option nicht mit der Einstellung **System** ^[22] **GINA GUI** ^[230] **Enable local https proxy** ^[231] kompatibel.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

Soll eine GINA-Domain über die Schaltfläche **Delete** gelöscht werden, so ist vorher unbedingt zu überprüfen, dass dieses keiner **Managed domain** ^[24] zugeordnet ist. Weiterhin können dadurch eventuell noch bei den Empfängern befindliche GINA-E-Mails dieser GINA-Domain nicht mehr entschlüsselt werden!

7.17.2.1 Layout

Dieses Sub-Menü wird aus **CHANGE GINA SETTINGS FOR** ^[423] aufgerufen.



Hinweis:

Cluster ^[383] Frontend Maschinen übernehmen im Backend vorgenommene Layout-Änderungen zum Teil erst nach einem Neustart.



Sektion **Company logo**

Parameter	Beschreibung
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE GINA SETTINGS FOR ^[423] Master template ^[424]) verwendet.
	Ist bereits ein Logo importiert, so wird dieses hier angezeigt. Über die Browser-Schaltfläche Datei auswählen kann ein Logo im gif-Format zum Upload ausgewählt werden. Das Firmen-Logo erscheint in der Menüleiste oben links in der GINA-Oberfläche. Wird das Firmen-Logo für die Anzeige in der GINA-Träger-E-Mail aktiviert (siehe Extended settings ^[457] Mail messages ^[458] Enable company logo ^[458]), so wird es oberhalb des Beschreibungstextes angezeigt. Die Größe des „Company Logo“ kann bei Bedarf über das GINA CSS ^[455] angepasst werden (siehe „To increase the company logo size in the navigation bar“).  Hinweis: Sollen sehr große Logos zum Einsatz kommen, so wird das Verwenden eines Header logo ^[453] für die GINA-Oberfläche empfohlen, da andernfalls das Logo aufgrund der erforderlichen Verkleinerung eventuell unkenntlich wird. In der GINA-Träger-E-Mail werden große Logos E-Mail Client abhängig gegebenenfalls nicht korrekt skaliert.

Über die Schaltfläche **Delete** wird das Logo-Bild gelöscht. Über die Schaltfläche **Save** wird das ausgewählte Bild gespeichert. Ist bereits ein Bild vorhanden, so wird dieses überschrieben.



Sektion **Header logo (optional)**

Parameter	Beschreibung
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE GINA SETTINGS FOR ^[423] Master template ^[424]) verwendet.
	Ist bereits ein Kopfzeilen-Logo importiert, so wird dieses hier angezeigt. Über die Browser-Schaltfläche Datei auswählen kann ein Logo im gif-Format zum Upload ausgewählt werden. Das Kopfzeilen-Logo kann ausschließlich für die Anzeige auf der Login-Seite der GINA-Oberfläche (siehe Extended settings ^[457] Login page ^[457] Enable header logo ^[457]) oder auch für alle anderen Seiten der GINA-Oberfläche (siehe Extended

Parameter	Beschreibung
	settings ^[457] Other pages ^[457] Enable header logo ^[457] aktiviert werden. Ist das Kopfzeilen-Logo aktiviert, so erscheint dieses ganz oben, unterhalb der Menüleiste. Die maximale Größe des Logos ist vom verwendeten Cascaded Style Sheet (CSS) abhängig. Im Standard beträgt diese 120x80 Pixel.  Hinweis: Generell wird vom Verwenden sehr großer Logos abgeraten, da dies insbesondere bei Mobiltelefonen dazu führen kann, dass zunächst gescrollt werden muss, um an die relevanten Informationen zu kommen.

Über die Schaltfläche **Delete** wird das Logo-Bild gelöscht. Über die Schaltfläche **Save** wird das ausgewählte Bild gespeichert. Ist bereits ein Bild vorhanden, so wird dieses überschrieben.

Sektion Favourites icon (optional)

Parameter	Beschreibung
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE GINA SETTINGS FOR ^[423] Master template ^[424]) verwendet.
	Ist bereits ein Favoriten-Icon importiert, so wird dieses hier angezeigt. Über die Browser-Schaltfläche Datei auswählen kann ein Icon in den Formaten gif, png, jpeg und ico zum Upload ausgewählt werden. Das Favoriten-Icon wird im Register-Reiter der GINA-Oberfläche im Web-Browser angezeigt. Die maximale Größe des Icons sollte 16x16 Pixel nicht überschreiten.

Über die Schaltfläche **Delete** wird das Logo-Bild gelöscht. Über die Schaltfläche **Save** wird das ausgewählte Bild gespeichert. Ist bereits ein Bild vorhanden, so wird dieses überschrieben.

Sektion Footer logo (optional)

Parameter	Beschreibung
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE GINA SETTINGS FOR ^[423] Master template ^[424]) verwendet.
	Ist bereits ein Fußzeilen-Logo importiert, so wird dieses hier angezeigt. Über die Browser-Schaltfläche Datei auswählen kann ein Logo im gif-Format zum Upload ausgewählt werden. Die maximale Größe des Logos ist vom verwendeten Cascading Style Sheet (CSS) abhängig (siehe auch GINA CSS ^[455] und E-mail CSS ^[456]). Das Fußzeilen-Logo kann ausschließlich für die Anzeige auf der Login-Seite der GINA-Oberfläche (siehe Extended settings ^[457] Login page ^[457] Enable footer logo ^[457]) oder für alle Seiten der GINA-Oberfläche (siehe Extended settings ^[457])

Parameter	Beschreibung
	Other pages ^[457] Enable footer logo ^[457] aktiviert werden. Ist das Fußzeilen-Logo aktiviert, so erscheint dieses ganz unten - oberhalb des Footer Textes, sofern konfiguriert (siehe Footer text ^[460]) - angezeigt. Ist das Fußzeilen-Logo für die Anzeige in der GINA-Träger-E-Mail aktiviert (siehe Extended settings ^[457] Mail messages ^[458] Enable footer logo ^[458]), so wird es unterhalb des Beschreibungstextes angezeigt.

Über die Schaltfläche **Delete** wird das Logo-Bild gelöscht. Über die Schaltfläche **Save** wird das ausgewählte Bild gespeichert. Ist bereits ein Bild vorhanden, so wird dieses überschrieben.

Sektion Background image (optional)

Parameter	Beschreibung
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE GINA SETTINGS FOR ^[423] Master template ^[424]) verwendet.
	Ist bereits ein Hintergrundbild importiert, so wird dieses hier angezeigt. Über die Browser-Schaltfläche Datei auswählen kann ein Bild im gif-Format zum Upload ausgewählt werden. Im Standard Cascading Style Sheet (CSS) wird kein Hintergrundbild verwendet. Soll dieses eingebettet werden, so ist das CSS in der Sektion GINA CSS ^[455] (siehe „Background image example usage“) entsprechend anzupassen: <pre>body { background: url('img/secmailBackgroundLogo.gif'); background-attachment: fixed; background-position: center; background-repeat: no-repeat; background-size: contain; }</pre>

Über die Schaltfläche **Delete** wird das Logo-Bild gelöscht. Über die Schaltfläche **Save** wird das ausgewählte Bild gespeichert. Ist bereits ein Bild vorhanden, so wird dieses überschrieben.

Sektion GINA CSS

Parameter	Beschreibung
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE GINA SETTINGS FOR ^[423] Master template ^[424]) verwendet.
 GINA CSS:	Im Eingabefeld kann das Aussehen der GINA-Seiten per Cascading Style Sheet (CSS) an das jeweilige Firmen Design angepasst werden.

Parameter	Beschreibung
	 Hinweis: Individuell angepasste CSS werden anstatt der Standard Einstellungen geladen.  Hinweis: Am Ende der Standardvorlage ist die Möglichkeit gegeben, • das Eingabefeld „Name“ im Registrierungsprozess (siehe „hide the input field „Full name“ in the registration“) • das Eingabefeld „Handynummer“ (wenn zum Beispiel kein Passwort Reset per SMS in der Account login ⁴⁴⁷ genutzt wird) im Registrierungsprozess („hide the input field „Mobile number“ in the registration“) • die Schaltfläche „Abmelden“ (siehe „hide the „Logout“ button when logged in“) • die Schaltfläche „Schlüssel/Zertifikate suchen“ (siehe „hide the „Search“ button in the profile under key“) • die Sprachauswahl nach dem Registrieren auf die GINA-Profil-Einstellungen zu beschränken (siehe „hide the language selection from anywhere but the“) auszublenden, sowie • die Einstellungen für die Barrierefreiheit zu aktivieren beziehungsweise anzupassen. (siehe „Accessibility contrast enhancement for focused inputs“) Weiterhin kann das „Company Logo“ bei Bedarf größer dargestellt werden (siehe „To increase the company logo size in the navigation bar“). Wird ein sehr großes Logo gewünscht, empfehlen wir das Einbinden als Header Logo ⁴⁵³.

Über die Schaltfläche **Preview GINA** wird ein Beispiel der GINA-Anmeldeseite unter Verwendung der vorgenommenen Konfiguration angezeigt.

Durch Klicken der Schaltfläche **Download LESS template** kann selbiges als Vorlage für eine eigene, angepasste CSS-Vorlage herunter geladen werden.

Sollen die Standard SEPPmail Cascading Style Sheet (CSS) wieder hergestellt werden, so ist die Schaltfläche **Restore default CSS** zu klicken.

Mittels **Save** werden die Änderungen am CSS gespeichert.

Sektion E-mail CSS

Parameter	Beschreibung
  Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE GINA SETTINGS FOR ⁴²³ Master template ⁴²⁴) verwendet.
 E-Mail CSS:	Im Eingabefeld kann das Aussehen der GINA-Träger-E-Mail per Cascading Style Sheet (CSS) an das jeweilige Firmen Design angepasst beziehungsweise ersetzt werden. Bei Verwenden eines individuell angepassten CSS wird nur dieses geladen. Somit werden hier keine Elemente aus dem Standard CSS verwendet.

Die Schaltfläche **Preview secure e-mail** generiert ein Beispiel für das Aussehen einer GINA-E-Mail unter Verwendung der vorgenommenen Konfiguration.

Sollen die Standard SEPPmail Cascading Style Sheet (CSS) wieder hergestellt werden, so ist die Schaltfläche **Restore default CSS** zu klicken.

Mittels **Save** werden die Änderungen am CSS gespeichert.

Sektion **Extended settings**

Parameter	Beschreibung
 ☒ Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] GINA-Domain editiert wird und ist im Standard aktiv. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE GINA SETTINGS FOR  Master template ) verwendet.
 Login page	
 ☐ Enable header logo	Diese Option ist im Standard inaktiv. Aktiviert das unter Header logo  hochgeladene Logo auf der GINA-Anmeldeseite.
 ☐ Enable footer logo	Diese Option ist im Standard inaktiv. Aktiviert das unter Footer logo  hochgeladene Logo auf der GINA-Anmeldeseite.
 ☐ Enable footer text	Diese Option ist im Standard inaktiv. Aktiviert den Footer text  aus der der Sprachdatei (siehe Language settings  Edit translations EDIT TRANSLATIONS FOR LANGUAGE ) auf der GINA-Anmeldeseite.
 Other pages	
 ☐ Enable header logo	Diese Option ist im Standard inaktiv. Aktiviert das unter Header logo  hochgeladene Logo auf allen weiteren GINA-Seiten.
 ☐ Enable footer logo	Diese Option ist im Standard inaktiv. Aktiviert das unter Footer logo  hochgeladene Logo auf allen weiteren GINA-Seiten.
 ☐ Enable footer text	Diese Option ist im Standard inaktiv. Aktiviert den Footer text  aus der der Sprachdatei (siehe Language settings  Edit translations EDIT TRANSLATIONS FOR LANGUAGE ) auf allen weiteren GINA-Seiten.
 All pages	
 ☐ Disable "Powered by"	Diese Option ist im Standard inaktiv. Deaktiviert den Text „Powered by SEPPmail“ ganz unten auf der GINA-Seite.

Parameter	Beschreibung
footer text	
 Mail messages	
 ☒ Enable company logo	Im Standard ist diese Option aktiv. Aktiviert das unter Company logo ⁴⁵³ hochgeladene Logo in der GINA-Träger-E-Mail.
 ☒ Enable footer logo	Im Standard ist diese Option aktiv. Aktiviert das unter Footer logo ⁴⁵⁴ hochgeladene Logo in der GINA-Träger-E-Mail.

Über die Schaltfläche **Save** werden die Einstellungen gespeichert.

7.17.2.2 Edit Translations For Language

Dieses Sub-Menü wird aus **CHANGE GINA SETTINGS FOR** ^[423] **Language settings** ^[446] aufgerufen.

In den folgenden Sektionen sind in den Eingabefeldern jeweils bereits die Standardtexte der gewählten Sprache enthalten.

Diese Texte können nach Bedarf angepasst oder ersetzt werden.

Sektion **Customization**

Diese Sektion beinhaltet Syntax-Hinweise für das Bearbeiten der Sprachdatei.

Sektion **Text in GINA**

In dieser Sektion wird der Textkörper der GINA-Träger-E-Mail an den Empfänger definiert.

Folgende Variablen sind an dieser Stelle zulässig:

@send Absender der GINA-E-Mail
 er@
 @subject ursprünglicher Betreff der zu versendenden E-Mail
 ct@

Textfeld	Beschreibung	
 Greeting Mail Text:	Definiert die Überschrift des Textkörpers. Diese ist für alle drei Folgetexte identisch. Die Überschrift wird im Standard fett dargestellt.	
 Standard Mail Text:	Text einer „Standard“-GINA-Träger-E-Mail, wie sie an bereits registrierte GINA Accounts ^[462] gesendet wird.	Die jeweiligen Texte stellen eine Anleitung dar, wie der jeweilige GINA-Nachrichten Empfänger vorzugehen hat, um die Originalnachricht lesen zu können.
 Initial Mail Text:	Text einer „Initial“-GINA-Träger-E-Mail, wie sie an initial erstellte GINA Accounts ^[462] gesendet wird.	
 Insecure Mail Text:	Text für „ungesicherte“ GINA-Nachrichten. Diese resultieren zum Beispiel aus dem Initialversand und Verwenden der Einstellung Initial password ^[430] Password length: ^[431] „0“ oder Verwenden des Betreffzeilen Schlüsselwortes ^[99] der Option Always use GINA technology for mails with the following text in subject ^[294] oder durch Large File Transfer ^[107] (LFT) ^[107] im Plain ^[440] Modus.	

Mittels **Save** werden Änderungen gespeichert. Über **Restore default** wird der Standard-Inhalt der Sektion in der Sprachdatei wieder hergestellt.

Sektion **Open hint in GINA**

Das hier zur Verfügung stehende Textfeld definiert die Beschreibung, welche nach dem Öffnen des HTML-Anhangs (im Standard secure-email.html) unterhalb der Schaltfläche „OK“ angezeigt wird.

Die Beschreibung sollte aufzeigen, welche Aktion(en) durch das Klicken von „OK“ ausgelöst werden.

Mittels **Save** werden Änderungen gespeichert. Über **Restore default** wird der Standard-Inhalt der Sektion in der Sprachdatei wieder hergestellt.

Sektion **Greeting on login page**

Beschreibung
Das erste Eingabefeld definiert eine Überschrift für den im zweiten Eingabefeld folgenden Text. Die Überschrift wird im Standard fett dargestellt.
Im zweiten Eingabefeld folgt die Beschreibung, wie der Empfänger vorzugehen hat, um die anhängende Originalnachricht entschlüsseln zu können.

Mittels **Save** werden Änderungen gespeichert. Über **Restore default** wird der Standard-Inhalt der Sektion in der Sprachdatei wieder hergestellt.

Sektion **Footer text**

Die Eingabe eines Fußnotentextes ist optional. Das Aktivieren der Anzeige des Fußnotentextes muss unter **LAYOUT** ⁴⁵⁷ in der **Sektion Extended settings** ⁴⁵⁷ erfolgen.

Mittels **Save** werden Änderungen gespeichert. Über **Restore default** wird der Standard-Inhalt der Sektion in der Sprachdatei wieder hergestellt.

Sektion **GINA password notification e-mail**

Folgende Variablen sind an dieser Stelle zulässig:

@email E-Mail Adresse des Empfängers der GINA-E-Mail
 @
 @send Absender der GINA-E-Mail
 er@
 @subje ursprünglicher Betreff der zu versendenden E-Mail
 ct@

Beschreibung
Die erste Zeile beinhaltet den Text, welcher in der Betreffzeile der Passwort Benachrichtigungs-E-Mail enthalten sein soll. Am Ende dieses Textes wird beim Versand der Passwort Benachrichtigungs-E-Mail ein Leerzeichen und die E-Mail Adresse des Empfängers der GINA-E-Mail automatisch eingefügt.
Die zweite Zeile beinhaltet den E-Mail Text der Passwort Benachrichtigungs-E-Mail. Dieser Text beginnt mit dem Wiederholen der Betreffzeile. Im Anschluss wird der Text aus dem Textfeld eingefügt und am Schluss eine Zeile mit dem Passwort in der Form „Passwort: <Initialpasswort>“ angefügt.

Mittels **Save** werden Änderungen gespeichert. Über **Restore default** wird der Standard-Inhalt der Sektion in der Sprachdatei wieder hergestellt.

Sektion **Edit translation file**

Über die Schaltfläche **Advanced view** öffnet ein Submenü, in welchem in der **Sektion Edit translation file** über einen integrierten Editor die Sprachdatei direkt angepasst werden kann. Weiterhin wird der Umgang mit dem Editor sowie die Syntax-erklärt.

Das Eingabefeld des Editors beinhaltet bereits den Text der Standard-Sprachdatei für die gewählte Sprache. Dort kann gegebenenfalls über die Browser Suchfunktion nach Ausdrücken gesucht werden, welche dann an die individuellen Bedürfnisse angepasst werden können.

Mittels **Save** werden Änderungen gespeichert.

Über die Schaltfläche **Normal view** wird zur vorherigen Ansicht zurück gewechselt.

7.18 GINA Accounts

In diesem Menü werden die auf der SEPPmail Appliance vorhandenen GINA-Benutzer angezeigt. Handelt es sich um ein mandantenfähiges System, so sind die Benutzer entsprechend der Mandanten aufgeteilt.

Sektion **Filter**

Über das Eingabefeld kann ein Suchbegriff als Zeichenfolge (string) eingegeben werden, nach welchem durch Klicken der Schaltfläche **Filter** in den gesamten GINA-Benutzern gesucht wird.

Parameter	Beschreibung
 ☒ Limit the number of returned entries	Im Standard ist diese Option aktiv. Da in großen Umgebungen mitunter der Aufbau der Seite sehr lange dauern kann, kann über die Option Limit the number of returned accounts die Anzeige auf 1000 User Accounts begrenzt werden. Die Suche nach einem GINA-Benutzer muss dann gegebenenfalls zwingend über die Schaltfläche Filter... vorgenommen werden. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).
Spalte	Beschreibung
 E-mail	Die E-Mail Adresse gewährleistet bei GINA Benutzern die Eindeutigkeit.
 Account status	Zeigt den Status des jeweiligen Benutzers an. Mögliche Status sind: • enabled Soll-Zustand • enabled (unregistered user) Benutzer welcher nach Erhalt der initialen GINA-E-Mail den Registrierungsprozess noch nicht abgeschlossen hat. • locked temporarily Bis zum nächsten erfolgreichen Login gesperrter Benutzer. Nähere Details hierzu zeigt der Last message status. • locked temporarily (unregistered user) Benutzer welcher nach Erhalt der initialen GINA-E-Mail, noch vor dem erfolgreichen Abschließen des Registrierungsprozesses bis zum ersten erfolgreichen Login gesperrt wurde. Nähere Details hierzu zeigt der Last message status.  Hinweis: Ist ein Account locked temporarily so wird der Status erst nach dem nächsten erfolgreichen Anmelden zurückgesetzt, auch wenn die Zeitspanne aus Accounts are locked for minutes after failed login attempts (siehe CHANGE GINA SETTINGS FOR Account login bereits verstrichen ist.  Hinweis: GINA-Benutzersperrungen werden jeweils im Daily Report (siehe auch Groups statisticsadmin) aufgeführt.
 Last message status	Zeigt Informationen zur letzten Aktion des Benutzers an. Mögliche Status sind: • Last succesful login MMM TT, JJJJ hh:mm:ss Gibt Datum und Uhrzeit des letzten erfolgreichen Anmeldens an.

Spalte	Beschreibung
	• X unsuccessful login attempts Gibt die Anzahl der fehlgeschlagenen Anmeldeversuche an.
 Mobile number	Zeigt die für den GINA-Benutzer hinterlegte Mobilfunknummer.
 Creator	In dieser Spalte ist der interne User ³⁹⁶ gelistet, welcher durch den Versand der initialen GINA-E-Mail den GINA-Account generiert hat. Bei selbstregistrierten Accounts wird die E-Mail Adresse des Registrierenden Kommunikationspartners angezeigt, das heißt diese ist identisch mit der unter E-mail (siehe oben) angezeigten Adresse.

Durch Klicken auf die E-mail-Adresse wird ein Untermenü mit Details zum jeweiligen GINA-Benutzer geöffnet (siehe Untermenü **ACCOUNT DETAILS** ⁴⁶⁴).

7.18.1 Account Details

Dieses Sub-Menü wird aus **GINA Accounts** ^[462] aufgerufen.

Sektion **User data**

In diesem Untermenü werden Detailinformationen zum GINA-Benutzer angezeigt. Weiterhin dient diese Menü manuellen Passwort Rücksetzungen, zum Beispiel durch den Support (siehe **GINA Domains** ^[416] **Domains** ^[416] **CHANGE GINA SETTINGS FOR** ^[423] **Admin** ^[424]).

Parameter	Beschreibung
 Creation info	Zeigt - wer gegebenenfalls die initiale GINA-E-Mail gesendet und somit den Benutzer generiert hat (Anzeige der E-Mail Adresse bei unregistrierten, beziehungsweise „Created by...“ bei bereits registrierten Benutzern) - ob es sich um einen selbstregistrierten Benutzer handelt (Account...)
 Name	Hat sich der Benutzer registriert, so wird hier der von ihm beim Registrieren eingetragene Name angezeigt.
 E-mail	Zeigt die E-Mail Adresse des Benutzers an.
 Password reminder	es sind zwei Status möglich: (Hidden) bei registrierten Benutzern - Not set bei unregistrierten Benutzern (Account Status „... (unregistered user)“)
 Answer	es sind zwei Status möglich: (Hidden) bei registrierten Benutzern - Not set bei unregistrierten Benutzern (Account Status „... (unregistered user)“)
 Password	Eingabefelder für das manuelle Rücksetzen des Passwortes durch einen Administrator. Danach muss der GINA-User das Passwort beim nächsten Anmelden ändern.
 ☐ Must change password	Zwingt den GINA-User beim nächsten Anmelden das Passwort zu ändern.
 ☐ Zip attachment	Legt individuell für den Benutzer fest, ob dieser den Anhang des GINA-Mails statt im HTML- im ZIP-Format erhält (vergleiche auch Always zip HTML attachments when encrypting e-mail with GINA technology ^[437]).
 Account status	Wird ein Account über dieses Menü explizit gesperrt, so muss diese Sperre gegebenenfalls auch wieder manuell aufgehoben werden. Automatische Sperren werden gemäß Einstellung (siehe GINA Domains ^[416] Domains ^[416] CHANGE GINA SETTINGS FOR ^[423] Account login ^[447]) aufgehoben.
 ☐ locked	Zeigt an ob der Benutzer gesperrt ist (zum Beispiel nach mehrfacher Falscheingabe des Passwortes) beziehungsweise kann der Administrator den Benutzer durch Aktivieren des Buttons sperren.
 ☒ enabled	Zeigt an ob der Benutzer aktiv ist beziehungsweise kann der Administrator den Benutzer durch Aktivieren des Buttons wieder in den Staus „Aktiv“ versetzen.
 External authentication	☐ Exclude this account from external authentication Ist eine externe Authentisierung aktiviert (siehe auch Mail System ^[247] Managed domains ^[247] ADD/EDIT MANAGED DOMAIN ^[277] External authentication ^[277] , beziehungsweise Change GINA Settings For ^[423] IDP

Parameter	Beschreibung
	Settings [426], so kann diese durch Anhaken dieser Option für einzelne Accounts ausgehebelt werden. Diese Option ist nur GINA accounts [462] zu sehen, welche einer Managed domain [247], beziehungsweise GINA Domain [416] zugeordnet sind, bei welcher Externe Authentisierung aktiv ist.
 Password security level 	Benutzer individuelle Einstellung für das Rücksetzverfahren des Passwortes. Diese Einstellung überschreibt die globale Einstellung unter GINA Domains [416] Domains [416] CHANGE GINA SETTINGS FOR [423] Account login [447].
 Mobile number	Mobilfunknummer für das Zurücksetzen des Passwortes via SMS.

Sektion **User logs**

Durch Klicken der Schaltfläche **Show user logs** wird ein detailliertes Log bezüglich der Aktivitäten des jeweiligen GINA-Benutzers angezeigt.

Alle vorgenommenen Änderungen werden über die Schaltfläche **Save changes** gespeichert.
Das Löschen eines GINA-Benutzers erfolgt über **Delete account**.



Achtung:

Durch das Löschen eines GINA-Benutzers wird auch dessen Schlüssel unwiderruflich gelöscht. Somit kann er eventuell noch in seinem Postfach befindliche GINA-Mails nicht mehr lesen. Der Inhalt dieser E-Mails ist somit verloren!

7.19 LFT Accounts

In diesem Menü werden die auf der SEPPmail Appliance vorhandenen LFT-Benutzer angezeigt.
Handelt es sich um ein mandantenfähiges System, so sind die Benutzer entsprechend der Mandanten aufgeteilt.

Spalte	Beschreibung
 E-mail	E-Mail Adresse des LFT-Benutzers.
 Account last used	Zeigt an, wann der LFT Benutzer zuletzt eine große Datei versendet hat. Bei aktiven Benutzern lässt sich daraus schließen, wann dieser auf inaktiv gesetzt wird und somit die Lizenz frei gibt, sofern in der Zwischenzeit nicht eine weitere große Datei durch ihn versendet/empfangen wird.  Hinweis: Inaktive LFT Accounts werden nach weiteren 30 Tagen gelöscht und bei Bedarf automatisch neu angelegt.

7.20 OpenPGP Public Keys

In diesem Menü werden die für die OpenPGP Verschlüsselung bereitstehenden öffentlichen Schlüssel der Kommunikationspartner wie folgt angezeigt.

Sektion **Local OpenPGP keys**

In dieser Sektion werden die der Appliance bekannten öffentlichen OpenPGP Schlüssel von Kommunikationspartnern angezeigt.

Spalte	Beschreibung
 Key ID	Zeigt die eindeutige Key ID des Schlüssels an.
 Subkey ID(s) (neu in 12.1)	Zeigt die Key Ids aller vorhandenen Subkeys an.
 E-mail addresses	Zeigt E-Mail Adresse(n) an, für welche der Schlüssel ausgestellt wurde.
 User name	Zeigt den Namen des Schlüsselinhabers an.
 Validity	Gibt die Gültigkeit des Schlüssels an. Mögliche Status sind • „keiner“, was mit „OK“ gleichzusetzen ist • EXPIRED • DISABLED (wenn in OPENPGP KEY 'details'  Usage  der Haken unter Allow encryption entfernt wurde und der Status nicht bereits EXPIRED ist)
 Issued on	Ausstelldatum des Schlüssels in der Form JJJJ-MM-TT
 Expires on	Ablaufdatum des Schlüssels in der Form JJJJ-MM-TT

Durch Klicken der **Key ID** wird ein Untermenü mit Details zum Key geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

Das Eingabefeld mit der Schaltfläche **Filter...** dient der Suche nach entsprechenden Schlüsseln anhand einer der in der Tabelle aufgeführten Merkmale. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Über die Schaltfläche **Import OpenPGP key...** öffnet das Sub-Menü **IMPORT OPENPGP KEY**  für den Import einzelner oder mehrerer (Bulk) öffentlicher OpenPGP Schlüssel von Kommunikationspartnern.

(neu in 12.0)

Über **Download all OpenPGP public keys** werden alle in diesem Menü gelisteten öffentlichen OpenPGP Schlüssel - also die der externen Kommunikationspartner - in eine Datei namens `pgp_keys.zip` heruntergeladen.



Hinweis:

Weiterhin werden hier auch per GINA-Portal, sowie via **Key Server**  bereit gestellte OpenPGP Schlüssel angezeigt und verwaltet.

7.20.1 Import OpenPGP Key(s)

Dieses Sub-Menü wird aus **OpenPGP Public Keys**  aufgerufen.

Sektion **Key data**

Parameter	Beschreibung
 Key file	Über die Browser-Schaltfläche „Datei auswählen“ wird entweder die Schlüsseldatei (Dateiendung ASC) für den Einzel-, beziehungsweise eine unverschlüsselte ZIP-Datei ohne Ordnerstruktur, welche die Schlüsseldateien enthält, für den Bulk-Import erwartet.
 or key as string	Liegt ein Schlüssel im Textformat vor, so kann dieser über das Eingabefeld angegeben werden. Auch das Einfügen mehrerer Schlüssel ist durch einfaches Aneinanderreihen möglich: <pre> -----BEGIN PGP PUBLIC KEY BLOCK----- # Schlüssel 1 -----END PGP PRIVATE KEY BLOCK----- -----BEGIN PGP PUBLIC KEY BLOCK----- # Schlüssel 2 -----END PGP PRIVATE KEY BLOCK----- -----BEGIN PGP PUBLIC KEY BLOCK----- # Schlüssel n -----END PGP PRIVATE KEY BLOCK----- </pre>

Über **Import** wird das angegebene Schlüsselmaterial auf die Appliance hochgeladen. Importierte Schlüssel werden ab Import für das Verschlüsseln herangezogen.

7.20.2 OpenPGP Key 'details'

Dieses Sub-Menü wird aus [OpenPGP Public Keys](#) ⁴⁶⁷ aufgerufen.

Sektion **Identification**

Diese Sektion zeigt Informationen über den Inhaber des OpenPGP Keys.

Parameter	Beschreibung
 ID	Zeigt die eindeutige ID des OpenPGP Keys an.
 User ID	In der Regel wird der Name sowie die E-Mail Adresse des Schlüsselinhabers angezeigt.
 Key ID	Zeigt die eindeutige Key ID des OpenPGP Keys an.
 Subkey ID	Zeigt die eindeutige Key ID des Subkeys an.
 Fingerprint	Hash des Keys. Dieser dient dem Abgleich mit dem Besitzer, um festzustellen, dass der Key auf dem Weg vom Besitzer zum Kommunikationspartner nicht - zum Beispiel durch eine Man-In-The-Middle-Attacke - ausgetauscht wurde.

Sektion **Validity**

Zeigt die Gültigkeit des Zertifikates.

Parameter	Beschreibung
 Issued on	Ausstellungsdatum des Zertifikates
 Expires on	Ablaufdatum des Zertifikates

Sektion **Type**

Parameter	Beschreibung
 PK Algorithm	Gibt den Schlüsselalgorithmus an, zum Beispiel RSA oder DSS/SH.
 Key size	Gibt die Schlüssellänge an
 Key capabilities	Zeigt die Schlüsseleigenschaften an (zum Beispiel encrypt, sign, certify).

Sektion **Valid e-mail addresses**

In dieser Sektion können alternative E-Mail Adressen angegeben werden, für welche der Schlüssel dann ebenfalls zur Verfügung steht.

Somit könnte der Schlüssel, welcher primär für
max.mustermann@meinefirma.tld

erstellt wurde ebenso für die alternativen E-Mail Adressen
 m.mustermann@meinefirma.tld
 mustermann@meinefirma.tld

Nach dem Speichern über **Save addresses** wird jeweils ein weiteres Eingabefeld eingeblendet.



Hinweis:

Diese Einstellung funktioniert nur mit Schlüsselmaterial welches mit 7.4.6 oder höher hochgeladen wurde



Sektion **Key usage**

Zeigt den Verwendungszweck des Zertifikates an, wobei nur die aus der folgenden Tabelle berücksichtigt werden.

Parameter	Beschreibung
 ☐ Allow encryption	Gibt an, ob dieser Schlüssel für das Verschlüsseln an die E-Mail Adresse aus der User ID (Identification) beziehungsweise an die unter Valid e-mail addresses eingetragene(n) E-Mail-Adresse(n) verwendet wird. Hinweis: Für Administratoren besteht über diese Option die Möglichkeit, den jeweiligen Schlüssel für das Verwenden zur Verschlüsselung auszuschließen.  Aber auch GINA-User sind in der Lage, Ihre Schlüssel - egal auf welchem Wege diese in X.509 Certificates aufgenommen wurden - auszunehmen. Aus diesem Grund sollte von einem generellen (re-)aktivieren dieser Option durch einen Administrator abgesehen werden.

Über **Save usage** werden Änderungen jeweils übernommen.



Sektion **Comment**

An dieser Stelle kann ein persönlicher Kommentar zum OpenPGP Key eingegeben werden, zum Beispiel weshalb die entsprechende Vertrauensstellung gewährt wurde.

Mit **Save comment** wird dieser Kommentar gespeichert.

Über die Schaltfläche **Download public key** besteht die Möglichkeit den Schlüssel im Text-Format als asc-Datei zu speichern.

Über **Delete** wird der OpenPGP Public Key aus der Appliance entfernt.

7.21 X.509 Certificates

In diesem Menü werden die für die S/MIME Verschlüsselung bereitstehenden Zertifikate wie folgt angezeigt.

Spalte	Beschreibung
 E-mail address	Zeigt E-Mail Adresse (RFC822 Name) des Schlüsselinhabers an.
 Certificate subject	Zeigt das X.509 Subject an.
 Serial number	Seriennummer des Zertifikats.
 Fingerprint	Zeigt den Fingerprint (Hash) des Zertifikates an.
 Validity	Gibt die Gültigkeit des Zertifikates an. Mögliche Status sind • „keiner“, was mit „OK“ gleichzusetzen ist • REVOKED • EXPIRED • DISABLED (wenn in X.509 CERTIFICATE 'details'  Key usage  der Haken unter Allow encryption entfernt wurde und keiner der beiden anderen Status zutrifft)
 OCSP/CRL check	Ergebnis der OCSP/CRL Prüfung. Mögliche Status sind • OK • ? • uncheckable • uncheckable (no supported CRL / OCSP mechanism) • revoked
 Issued on	Ausstelldatum des Zertifikats in der Form JJJJ-MM-TT
 Expires on	Ablaufdatum des Zertifikats in der Form JJJJ-MM-TT

Durch Klicken auf die E-Mail Adresse wird in das Sub-Menü **X.509 CERTIFICATE 'details'**  mit Details zum Zertifikat gewechselt.

Das Eingabefeld mit der Schaltfläche **Filter...** dient der Suche nach entsprechenden Zertifikaten anhand einer der in der Tabelle aufgeführten Merkmale. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Über die Schaltfläche **Import S/MIME certificate...** öffnet das Sub-Menü **IMPORT X.509 CERTIFICATE**  für den Import einzelner oder mehrerer (Bulk) Zertifikate von Kommunikationspartnern.

Die Schaltfläche **Advanced settings...**  führt zum gleichnamigen Untermenü, in welchem das - gegebenenfalls automatisierte - Bereinigen von Zertifikaten vorgenommen wird.



Hinweis:

Stehen für einen Empfänger mehrere, gültige Zertifikate zur Verfügung, so wird der Session Key mit jedem dieser Zertifikate verschlüsselt.

Verwendet der Empfänger zum Beispiel mehrere Hardware Clients, auf welchen jeweils unterschiedliche (private) Schlüssel bereit stehen, so wird hierdurch gewährleistet, dass die E-Mail auf allen Clients gelesen werden kann, sofern natürlich deren zugehörige öffentliche Schlüssel auf der Appliance bekannt sind.

**Hinweis:**

S/MIME Zertifikate werden automatisch aus eingehenden, signierten E-Mails eingesammelt, sofern diese Zertifikate von einer unter **X.509 Root Certificates**^[480] mit dem Status „trusted“ gelisteten Zertifizierungsstelle stammen.

Weiterhin werden hier auch per GINA-Portal, sowie via **Key Server**^[309] bereit gestellte Zertifikate eingesammelt. Generell gilt jedoch, dass keine unsicheren Zertifikate (SHA-1 und MD5, MD4, MD2) importiert werden.

Somit wächst die Anzahl der zur Verfügung stehenden Verschlüsselungszertifikate - und somit die Möglichkeit zur S/MIME verschlüsselten Kommunikation mit Dritten - stetig und automatisch.

7.21.1 Import X.509 Certificate(s)

Dieses Sub-Menü wird aus **X.509 Certificates** ^[47] aufgerufen.

Sektion **Certificate data**

Parameter	Beschreibung
 X.509 certificate	Über die Browser-Schaltfläche „Datei auswählen“ wird entweder die Zertifikatsdatei (Dateiendung CRT, CER oder P7B) für den Einzel-, beziehungsweise eine unverschlüsselte ZIP-Datei ohne Ordnerstruktur, welche die Zertifikatsdateien enthält, für den Bulk-Import erwartet.  Hinweis: Werden versehentlich andere als S/MIME Zertifikate ausgewählt, so werden diese nicht, beziehungsweise bei ZIP-Dateien nur die enthaltenen S/MIME Zertifikate importiert.
 or X.509 certificate as string	Liegt ein Zertifikat im Textformat vor, so kann dieses über das Eingabefeld angegeben werden. Auch das Einfügen mehrerer Zertifikate ist durch einfaches Aneinanderreihen möglich: <pre>-----BEGIN CERTIFICATE----- # Zertifikat 1 -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- # Zertifikat 2 -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- # Zertifikat n -----END CERTIFICATE-----</pre>

Über **Import** wird das angegebene Schlüsselmaterial auf die Appliance hochgeladen. Importierte Zertifikate werden ab Import für das Verschlüsseln herangezogen.



Hinweis:

Welche Zertifikate Importiert werden können ist von der Auswahl unter **ADVANCED SETTINGS** ^[47] **Advanced settings** ^[47] **Policies Refuse import of certificates with a signature algorithm using SHA-1 or lower** ^[47] abhängig.



Achtung:

Für das Importieren muss ein Zertifikat die korrekte X.509 Zertifikatserweiterung „Schlüsselverwendung (Key Usage)“ mit dem Wert „Schlüsselverschlüsselung: (key encipherment)“ aufweisen.
In der Regel haben diese Zertifikate weiterhin die Werte „Datenverschlüsselung: (data encipherment)“ und „Digitale Signatur: (digital signature)“.

7.21.2 X.509 Certificate 'details'

Dieses Sub-Menü wird aus **X.509 Certificates**  aufgerufen.

Sektion **Issued to**

Diese Sektion zeigt Informationen über den Inhaber des SSL Zertifikates.
Abhängig vom Zertifikat müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
 Name (CN)	Dieses Feld beinhaltet den Antragstellernamen, wie er beim Beantragen des Zertifikates an die CA übermittelt wurde. Dies kann gelegentlich auch die E-Mail Adresse in der Form Email: max.mustermann@meinefirma.tld sein. In der Regel werden aber E-Mail Adressen als „CN“ nicht mehr anerkannt.
 E-mail address	In der Regel wird die E-Mail Adresse des Antragstellers angezeigt. Dies kann auch eine Sammeladresse sein.
 Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Buchhaltung“
 Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel Meine Firma AG
 Locality (L)	Standort zum Beispiel eine Stadt wie „Neuenhof“ oder auch ein Teilgebäude wie Werk2
 State (ST)	Bundesland, Kanton, Provinz oder ähnliches, zum Beispiel Musterbundesland
 Country (C)	Land, zum Beispiel de für „Deutschland“
 Serial no.	Seriennummer des Zertifikats
 Subject Alternative Name	Zeigt die E-mail address sowie gegebenenfalls vorhandene Alternativ-Namen an.

Sektion **Issued by**

Diese Sektion zeigt Informationen über den Aussteller des SSL Zertifikates (Wurzel-Zertifikat).
Abhängig vom Aussteller müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
 Name (CN)	Name der ausstellenden Zertifizierungsstelle
 E-mail address	In der Regel eine E-Mail Adresse für Support-Anfragen an den Aussteller
 Org. unit (OU)	Gibt eine Organisationseinheit des Ausstellers an
 Organization (O)	Gibt die ausstellende Organisation an

Parameter	Beschreibung
 Locality (L)	Gibt den Standort des Ausstellers an
 State (ST)	Gibt ein Bundesland, Kanton, Provinz oder ähnliches des Ausstellers an
 Country (C)	Gibt das Land des Ausstellers an
 Serial no.	Seriennummer des Zertifikats

Sektion **Validity**

Zeigt die Gültigkeit des Zertifikates.

Parameter	Beschreibung
 Issued on	Ausstelldatum des Zertifikates
 Expires on	Ablaufdatum des Zertifikates

Sektion **Fingerprint**

Der Fingerprint ist die Prüfsumme (auch hash) und dient dem Überprüfen eines Zertifikats. An dieser Stelle wird der Hash-Algorithmus (zum Beispiel MD5 SHA1 oder SHA256), mit welchem die Prüfsumme gebildet wurde, sowie der berechnete Wert angezeigt. Sind mehrere Fingerprints unterschiedlicher Algorithmen vorhanden, so wird jeder in einer separaten Zeile ausgegeben.

Parameter	Beschreibung
 SHA1	SHA1 Fingerprint des Zertifikates Beispiel: D8:CF:CC:47:84:92:A9:F0:7E:2A:15:E8:2E:4F:CA:26:5C:60:10:E9
 SHA256	SHA256 Fingerprint des Zertifikates Beispiel: 83:06:F6:84:34:C2:E7:79:50:47:7B:EC:32:B7:22:13:FD:1F:9C:41:B4:B4:F9:C3:AB:85:12:AA:6B:1E:D2:BE

Sektion **Valid e-mail addresses**

In dieser Sektion können alternative E-Mail Adressen angegeben werden, für welche die Schlüssel dann ebenfalls zur Verfügung stehen. Somit könnte ein Zertifikat welches primär für

Associated Email Address: max.mustermann@meinefirma.tld

ausgestellt wurde und somit als Antragsteller etwas wie

E = max.mustermann@meinefirma.tld

CN = Max Mustermann

O = Meine Firma AG

C = de

stehen hätte, ebenso für die alternativen E-Mail Adressen m.mustermann@meinefirma.tld und mustermann@meinefirma.tld für das Verschlüsseln verwendet werden, wenn diese Adressen eingetragen würden.

Dies könnte zum Beispiel bei einem Umstellen der Top-Level-Domain einer E-Mail Domäne von .ch auf .com hilfreich sein.

Nach dem Speichern über **Save addresses** wird jeweils ein weiteres Eingabefeld eingeblendet.



Hinweis:

Diese Einstellung funktioniert nur mit Schlüsselmateriale welches mit 7.4.6 oder höher hochgeladen wurde



Sektion **Key usage**

Zeigt den Verwendungszweck des Zertifikates an, wobei nur die aus der folgenden Tabelle berücksichtigt werden.

Parameter	Beschreibung
 S/MIME signing	digitalSignature / Digitale Signatur
 S/MIME encryption	keyEncipherment / Schlüssel Verschlüsselung
 CA certificate	keyCertSign / Zertifikatssignatur
 Allow encryption	Gibt an, ob dieses Zertifikat für das Verschlüsseln an den Antragsteller (Issued to ⁴⁷⁴) beziehungsweise an die unter Valid e-mail addresses ⁴⁷⁵ eingetragene(n) E-Mail-Adresse(n) verwendet wird. Hinweis: Generell ist diese Option bei aus Signaturen eingesammelten, sowie durch den Administrator importierten Zertifikaten aktiv.  Für Administratoren besteht über diese Option die Möglichkeit, den jeweiligen Schlüssel für das Verwenden zur Verschlüsselung auszuschließen. Aber auch GINA-User sind in der Lage, Ihre Zertifikate - egal auf welchem Wege diese in X.509 Certificates ⁴⁷⁶ aufgenommen wurden - auszunehmen. Aus diesem Grund sollte von einem generellen (re-)aktivieren dieser Option durch einen Administrator abgesehen werden.

Über **Save usage** werden Änderungen jeweils übernommen.



Sektion **Key info**

Zeigt erweiterte Informationen zum Zertifikat an.

Parameter	Beschreibung
 Signature algorithm	Zeigt den Signatur-Algorithmus des Zertifikates an, zum Beispiel • md5WithRSAEncryption • sha1WithRSAEncryption • sha256WithRSAEncryption

Parameter	Beschreibung
 Key type	Zeigt das Kryptosystem an, mit welchem der Schlüssel erzeugt wurde. In der Regel ist das RSA.
 Key size	Zeigt die Schlüssellänge an. In der Regel kommen nur noch Schlüssellängen von 2048 bit und mehr vor.
 Last certificate check	Zeigt den Zeitpunkt der letzten Zertifikatsprüfung (via CRL beziehungsweise OCSP) an. Über Check now... kann ein sofortiges Prüfen der Revokations-Informationen erzwungen werden.
 Last successful certificate check	Zeigt das Datum des letzten erfolgreichen OCSP, beziehungsweise CRL Checks an.
 Last check result	Zeigt das Ergebnis der letzten Zertifikatsprüfung an.
 OCSP URI	Gibt die authorityInformationAccess (kurz AIA, Zugriff auf Stelleninformationen) - also den OCSP Pfad - aus. Dieser Punkt ist nur dann sichtbar, wenn im Zertifikat die extension authority information access gesetzt ist.
 CRL URI	Gibt den crlDistributionPoint (Sperrlisten Verteilungspunkt) - also die Lokation, unter welchem die CRL bereit gestellt wird - aus. Dieser Punkt ist nur dann sichtbar, wenn im Zertifikat die extension crlDistributionPoint gesetzt ist.
 Public / private key	Gibt an, welche Schlüssel enthalten sind, private, public/

Sektion Comment

An dieser Stelle kann ein persönlicher Kommentar zum Zertifikat eingegeben werden, zum Beispiel weshalb die entsprechende Vertrauensstellung gewählt wurde.

Mit **Save comment** wird dieser Kommentar gespeichert.

Über die Schaltfläche **Download certificate** besteht die Möglichkeit das Zertifikat im CRT-Format zu speichern.

Über **Delete certificate** wird das Zertifikat von der SEPPmail Appliance zunächst revoziert und über einen zweiten Klick gegebenenfalls gelöscht.

7.21.3 Advanced Settings

Dieses Sub-Menü wird aus **X.509 Certificates** ^[47] aufgerufen.

Sektion **Advanced settings**

Parameter	Beschreibung
 Deduplication	Über die Schaltfläche Delete duplicated certificates now werden eventuell mehrfach vorhandene Zertifikate einmalig sofort gelöscht. Beibehalten wird jeweils das Zertifikat mit der längsten Gültigkeit. Hinweis:  Durch das Entfernen von Duplikaten kann ein Empfänger unter Umständen eine verschlüsselte E-Mail nicht mehr auf all seinen Endgeräten lesen. Verwendet der Empfänger beispielsweise auf seinem Notebook und seinem Mobil-Telefon unterschiedliche Schlüssel, so kann er durch das Löschen von Duplikaten nur noch auf dem Endgerät die verschlüsselte E-Mail lesen, auf welchem sein Zertifikat mit der längsten Laufzeit installiert ist.
 Delete duplicated certificates automatically	Im Standard ist diese Einstellung inaktiv. Durch Aktivieren dieser Option wird der oben genannte Bereinigungsprozess einmal täglich automatisiert ausgeführt.
 Expiration	Über die Schaltfläche Delete expired certificates now werden abgelaufene Zertifikate einmalig sofort entfernt. Hinweis:  Im Standard verwendet die SEPPmail Appliance auch abgelaufene Zertifikate für das Verschlüsseln (siehe auch Policies ^[47] Refuse usage of expired certificates for encryption ^[47]), sofern kein aktuelles Zertifikat zur Verfügung steht. Durch das Löschen abgelaufener Zertifikate wird dieses Verhalten ebenso unterbunden wie durch die zuvor genannte Option.
 Delete expired certificates automatically	Im Standard ist diese Einstellung inaktiv. Durch Aktivieren dieser Option wird der oben genannte Bereinigungsprozess einmal täglich automatisiert ausgeführt.
 Revocation	Über die Schaltfläche Check OCSP/CRL status now wird für alle Zertifikate des Menüs X.509 Certificates ^[47] die Gültigkeit via OCSP (Online Certificate Status Protocol) beziehungsweise CRL (Certificate Revocation List) sofort geprüft.
 Number of days after which unverifiable certificates are ignored:	Im Standard lautet der Eintrag „never“. Zertifikate, deren Gültigkeit innerhalb der hier eingegebenen Anzahl von Tagen nicht geprüft werden kann, werden nicht für das Verschlüsseln herangezogen. Achtung:  Eine andere Einstellung als „never“ kann zu sporadischen Problemen beim Verschlüsseln führen. Wären beispielsweise 7 Tage eingestellt, die ausstellende CA stellt jedoch nur alle 10 Tage neue Revokationsinformationen zur Verfügung, so wäre ein Zertifikat dieser CA immer für sieben Tage für das Verschlüsseln verfügbar und für die restlichen drei Tage nicht.
 Automatically check revocation	Im Standard ist diese Einstellung inaktiv.

Parameter	Beschreibung
status every day (neu in 12.1)	Durch Aktivieren dieser Option werden alle in X.509 Certificates ^[47] enthaltenen Zertifikate einmal täglich automatisiert einer Gültigkeitsprüfung unterzogen.
 Policies	
 Refuse import of certificates with a signature algorithm using SHA-1 or lower	Im Standard ist diese Einstellung inaktiv. Verhindert den Import von Zertifikaten mit einem unsicheren Hash Algorithmus, also SHA-1 und älter (siehe auch X.509 Certificates ^[47] Import S/MIME certificate... CHANGE GINA SETTINGS FOR ^[423] Extended settings ^[43] Certificate search and management in GINA:).
 Refuse usage of expired certificates for encryption	Im Standard ist diese Einstellung inaktiv. SEPPmail Appliance kann auch abgelaufene Zertifikate für das Verschlüsseln verwenden, sofern kein aktuelles Zertifikat zur Verfügung steht. Durch Aktivieren dieser Option wird dieses Verhalten unterbunden, auch ohne abgelaufene Zertifikate zu löschen (siehe Expiration ^[478] Delete expired certificates automatically ^[478]).
 Bulk export (neu in 12.0)	Über Download all X.509 certificates werden alle im übergeordneten Menü X.509 Certificates ^[47] aufgelisteten Zertifikate - also die der externen Kommunikationspartner - in eine Datei namens smime_certificates.zip heruntergeladen.

Die vorgenommenen Änderungen beider Sektionen werden über die Schaltfläche **Save** gespeichert.

7.22 X.509 Root Certificates

In diesem Menü wird die Vertrauensstellung zu den einzelnen Zertifizierungsstellen (CA) verwaltet.

Bei der Installation sind bereits die Root CA Zertifikate der üblichen, akkreditierten CAs vorausgenommen (siehe auch **Trust state set by** [481] [481]), ähnlich wie zum Beispiel bei Internet Browsern. Gegebenenfalls kann diese vorhandene Liste mit eventuell bestehenden Revisionsvorgaben abgeglichen und unter Umständen unerwünschten CAs das Vertrauen entzogen werden. Das heißt, SEPPmail nimmt hier keine weiteren Änderungen vor, auch nicht zum Beispiel bei Updates. Somit sind unerwünschte Eingriffe in das Sicherheitskonzept des jeweiligen Betreibers ausgeschlossen.

Ab der Installation wächst das System an dieser Stelle dynamisch. Gehen auf der SEPPmail Appliance signierte E-Mails ein, deren Signaturzertifikate von unbekannten Zertifizierungsstellen stammen, so werden gegebenenfalls Root- und Zwischenzertifikate aus diesen Signaturen eingesammelt und mit dem Status „?“ (unbekannt) gespeichert. Dabei wird den Mitgliedern der **Groups** [413] **x509rootcertificatesadmin** [413] eine E-Mail Nachricht mit dem Betreff „IMPORTANT: SEPPmail new CA certificates added on ...“ gesendet. Ebenso enthalten ist diese Information im **Daily Report** [98], welcher dadurch den Status „IMPORTANT“ erhält und somit auch an die Mitglieder der **Groups** [413] **admins** [413] und die **Postmaster address** [253] gesendet wird.

Im Anschluss sollte das Einstufen dieser Zertifikate bezüglich deren Vertrauenswürdigkeit durch einen Administrator erfolgen.

Über die Schaltfläche **Import S/MIME root certificate...** öffnet das Sub-Menü **IMPORT X.509 ROOT CERTIFICATE(S)** [483] für den Import einzelner oder mehrerer (Bulk) Root-Zertifikate von Kommunikationspartnern

Über die Schaltfläche **Advanced settings...** öffnet das Sub-Menü **ADVANCED SETTINGS** [478]. In diesem kann eingestellt werden, wie mit X.509 Root Zertifikaten umzugehen ist.

Sektion **Filter**

Das Eingabefeld mit der Schaltfläche **Filter...** dient der Suche nach entsprechenden Zertifikaten anhand einer der in der Tabelle aufgeführten Merkmale. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Sektion **Root certificate**

Angezeigt werden die Root- und Zwischenzertifikate wie folgt.

Spalte	Beschreibung
 Trust state	Zeigt die Vertrauensstellung an. Mögliche Status sind • trusted → vertrauenswürdig • UNTRUSTED → nicht vertrauenswürdig • ? → unbekannt • implicit → Zwischenzertifikat, welches aus einer gültigen E-Mail Signatur extrahiert und importiert wurde. Zwischenzertifikaten mit dem Status „implicit“ wird ohne manuellen Eingriff vertraut, solange dem zugehörigen Root Zertifikat nicht das Vertrauen entzogen wird. • ORPHANED → Zwischenzertifikat, dessen zugehöriges Wurzel-Zertifikat fehlt. Aufgrund des fehlenden Wurzel-Zertifikats kann diesen Zertifikaten selbst dann nicht vertraut werden, wenn der Status auf „trusted“ (siehe CERTIFICATE DETAILS [486]) gesetzt wird. In diesem Fall würde der angezeigte Status

Spalte	Beschreibung
	sofort nach dem Importieren und trusten des zugehörigen Wurzel-Zertifikates von ORPHANED zu „trusted“ wechseln. Bei unbekanntem Status („?“) ist ein Eingreifen des Administrators erforderlich. Dieser muss entscheiden, ob der Zertifizierungsstelle vertraut werden soll oder nicht. Sind Zertifikate mit dem Status „?“ vorhanden, so werden diese bei Auftauchen an die CA-Administratoren (siehe Groups ^[413] caadmin ^[414]) und im Rahmen des Daily Report ^[96], welcher dann den Status „IMPORTANT“ erhält, den Maschinen-Administratoren (siehe Groups ^[413] admin ^[413]) gemeldet. Durch Klicken auf den Vertrauensstatus des Zertifikates können Details eingesehen und die Vertrauensstellung angepasst werden (siehe Untermenü CERTIFICATE DETAILS ^[486]).  Hinweis: Zertifikate aus Signaturen, deren ausstellenden Zertifizierungsstelle vertraut (trusted) wird, werden automatisiert eingesammelt (siehe X.509 Certificates ^[471]) und stehen somit für das Verschlüsseln bereit.  Hinweis: <i>(geändert in 12.1)</i> Wird der Status eines Zertifikates auf „trusted“ geändert, so vererbt sich dieser Status in der Baumstruktur nach unten auf alle zugehörigen Zwischen-(Intermediate-)Zertifikate bis zum ersten, welches gegebenenfalls den Status „untrusted“ aufweist. Bei Ändern des Status auf „untrusted“ ändern sich alle in der Baumstruktur darunterliegenden Zertifikate hin zu „untrusted“, egal welchen Status diese vorher hatten. Ein Zertifikat, welches in der Baumstruktur unterhalb eines anderen Zertifikates mit dem Status „untrusted“ liegt, kann niemals in den Status „trusted“ versetzt werden.
 Subject	Gibt den Namen (CN) des Antragstellers an
 Trust state set by <i>(neu in 12.1)</i>	Zeigt an, von wem das Zertifikat ausgestellt wurde. • Factory (tusted by SEPPmail factory default settings) → Im Auslieferungszustand der SEPPmail Appliance mitgeliefert Zertifikate. • Automatic (auto-trusted by RuleEngine) → Zertifikate, welchen durch die Option Automatically trust new root certificates ^[485] das Vertrauen ausgesprochen wurde. • Manual (Administrator through Admin-GUI) → Zertifikate, welchen das Vertrauen manuell über die Administrationsoberfläche ausgesprochen oder entzogen wurde. • none → Zertifikate mit undefiniertem

Spalte	Beschreibung
	Vertrauensstatus (Trust state ⁴⁸⁰ "?")
 Issued on	Ausstelldatum des Zertifikats in der Form JJJJ-MM-TT
 Expires on	Ablaufdatum des Zertifikats in der Form JJJJ-MM-TT
 Fingerprint	Zeigt den Fingerprint (Hash) des Zertifikates an.
 Type	Gibt den Hash des Zertifikates an. Zum Beispiel RSA-MD5, RSA-SHA1, RSA-SHA256,...
 Validity	Gibt die Gültigkeit des Zertifikates an. Mögliche Status sind • „keiner“, was mit „OK“ gleichzusetzen ist • REVOKED • EXPIRED
 OCSP/CRL check	Ergebnis der OCSP/CRL Prüfung. Mögliche Status sind • OK • ? • uncheckable • uncheckable (no supported CRL / OCSP mechanism) • revoked

 Sektion Root certificate with verification errors
(neu in 12.1)

Angezeigt werden die Root- und Zwischenzertifikate wie folgt.

Spalte	Beschreibung
 Trust state	siehe Root certificate ⁴⁸⁰ Trust state ⁴⁸⁰
 Subject	siehe Root certificate ⁴⁸⁰ Subject ⁴⁸¹
 Trust state set by	siehe Root certificate ⁴⁸⁰ Trust state set by ⁴⁸¹
 Issued on	siehe Root certificate ⁴⁸⁰ Issued on ⁴⁸²
 Expires on	siehe Root certificate ⁴⁸⁰ Expires on ⁴⁸²
 Fingerprint	siehe Root certificate ⁴⁸⁰ Fingerprint ⁴⁸²
 Type	siehe Root certificate ⁴⁸⁰ Type ⁴⁸²
 Validity	Gibt den Ursache aus, weshalb ein Zertifikat ungültig ist. ▼ mögliche Status Unspecified certificate verification errorUnable to get issuer certificateUnable to get certificate CRLUnable to decrypt

Spalte	Beschreibung
	certificate's signatureUnable to decrypt CRL's signatureUnable to decode issuer public keyCertificate signature failureCRL signature failureCertificate is not yet validCertificate has expiredCRL is not yet validCRL has expiredFormat error in certificate's notBefore fieldFormat error in certificate's notAfter fieldFormat error in CRL's lastUpdate fieldFormat error in CRL's nextUpdate fieldOut of memorySelf signed certificateSelf signed certificate in certificate chainUnable to get local issuer certificateUnable to verify the first certificateCertificate chain too longCertificate revokedInvalid CA certificatePath length constraint exceededUnsupported certificate purposeCertificate not trustedCertificate rejectedSubject issuer mismatchAuthority and subject key identifier mismatchAuthority and issuer serial number mismatchKey usage does not include certificate signingUnable to get CRL issuer certificateUnhandlled critical extensionKey usage does not include CRL signingUnhandlled critical CRL extensionInvalid non-CA certificate (has CA markings)Proxy path length constraint exceededKey usage does not include digital signatureProxy certificates not allowed, please set the appropriate flagInvalid or inconsistent certificate extensionInvalid or inconsistent certificate policy extensionNo explicit policyDifferent CRL scopeUnsupported extension featureRFC 3779 resource not subset of parent's resourcesPermitted subtree violationExcluded subtree violationName constraints minimum and maximum not supportedApplication verification failureUnsupported name constraint typeUnsupported or invalid name constraint syntaxUnsupported or invalid name syntaxCRL path validation errorPath LoopSuite B: certificate version invalidSuite B: invalid public key algorithmSuite B: invalid ECC curveSuite B: invalid signature algorithmSuite B: curve not allowed for this LOSuite B: cannot sign P-384 with P-256Hostname mismatchEmail address mismatchIP address mismatchNo matching DANE TLSA recordsEE certificate key too weakCA certificate key too weakCA signature digest algorithm too weakInvalid certificate verification contextIssuer certificate lookup errorCertificate Transparency required, but no valid SCTs foundProxy subject name violationOCSP verification neededOCSP verification failedOCSP unknown certCertificate public key has explicit ECC parameters
 OCSP/CRL check	siehe Root certificate ⁴⁸⁰ OCSP/CRL check ⁴⁸²

7.22.1 Import X.509 Root Certificate(s)

Dieses Sub-Menü wird aus [X.509 Root Certificates](#) ⁴⁸⁰ aufgerufen.

Sektion Certificate data

Parameter	Beschreibung
 X.509 certificate	Über die Browser-Schaltfläche „Datei auswählen“ wird entweder die Zertifikatsdatei (Dateiendung CRT, CER oder P7B) für den Einzel-, beziehungsweise eine unverschlüsselte ZIP-Datei ohne Ordnerstruktur, welche die Zertifikatsdateien enthält, für den Bulk-Import erwartet.

Parameter	Beschreibung
	 Hinweis: Werden versehentlich andere als CA Zertifikate ausgewählt, so werden diese nicht, beziehungsweise bei ZIP-Dateien nur die enthaltenen CA Zertifikate importiert.
 or X.509 certificate as string	Liegt ein Zertifikat im Textformat vor, so kann dieses über das Eingabefeld angegeben werden. Auch das Einfügen mehrerer Zertifikate ist durch einfaches Aneinanderreihen möglich: <pre> -----BEGIN CERTIFICATE----- # Zertifikat 1 -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- # Zertifikat 2 -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- # Zertifikat n -----END CERTIFICATE----- </pre>
 Options	
 ☒ Automatically trust the imported X.509 root certificates	Im Standard ist diese Option aktiv. Durch die aktive Option wird den zu importierenden CAs sofort vertraut (siehe X.509 Root Certificates ⁴⁸⁰ , Tabelle Spalte Trust state Status „trusted“). Bei inaktiver Option werden die CAs mit unbekannten Trust state (Status „?“) importiert.

Über **Import** wird das angegebene Schlüsselmaterial auf die Appliance hochgeladen.



Hinweis:

Generell ist ein Upload von unsicherem Schlüsselmaterial (SHA-1 und MD5, MD4, MD2) nicht möglich.

7.22.2 Advanced Settings

Dieses Sub-Menü wird aus **X.509 Root Certificates** ^[480] aufgerufen.

Sektion **Advanced settings**

Parameter	Beschreibung
 Trust (neu in 12.0)	
 Automatically trust new root certificates	Im Standard ist diese Einstellung aktiv. Durch Aktivieren dieser Option wird Zertifikaten, welche via IMPORT X.509 ROOT CERTIFICATE(S) ^[483] importiert wurden, sofort das Vertrauen ausgesprochen. Somit tauchen diese Zertifikate in der Tabelle des Hauptmenüs X.509 Root Certificates ^[480] in der Spalte Trust state sofort als trusted auf.  Achtung: Das Verwenden dieser Option erfordert das - in regelmäßigen und kurzen Abständen - Überwachen der Nachrichten mit dem Betreff „New CA added“ (siehe auch caadmin ^[414]). Nur so kann eingesammelten, fragwürdigen Stammzertifizierungsstellen das Vertrauen zeitnah wieder manuell entzogen werden.
 Expiration	Über die Schaltfläche Delete expired certificates now werden abgelaufene Root Zertifikate einmalig sofort entfernt.
 Delete expired certificates automatically	Im Standard ist diese Einstellung aktiv. Durch Aktivieren dieser Option wird der oben genannte Bereinigungsprozess einmal täglich automatisiert ausgeführt.
 Revocation	Über die Schaltfläche Check OCSP/CRL status now wird für alle Zertifikate des Menüs X.509 Root Certificates ^[480] die Gültigkeit via OCSP (Online Certificate Status Protocol) beziehungsweise CRL (Certificate Revocation List) sofort geprüft.
 Automatically check revocation status every day (neu in 12.1)	Im Standard ist diese Einstellung inaktiv. Durch Aktivieren dieser Option werden alle in X.509 Root Certificates ^[480] enthaltenen Zertifikate einmal täglich automatisiert einer Gültigkeitsprüfung unterzogen.
 Bulk export (neu in 12.0)	Über Download all X.509 root certificates werden alle im übergeordneten Menü X.509 Root Certificates ^[480] aufgelisteten Zertifikate in eine Datei namens smime_root_certificates.zip heruntergeladen.

Die vorgenommenen Änderungen beider Sektionen werden über die Schaltfläche **Save** gespeichert.

7.22.3 Certificate Details

Dieses Sub-Menü wird aus **X.509 Root Certificates**  aufgerufen.

Sektion Issued to

Diese Sektion zeigt Informationen über den Inhaber des CA-Zertifikates.
Abhängig vom Zertifikat müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
 Name (CN)	Gibt den Namen der eigenen Zertifizierungsstelle an
 E-mail address	In der Regel der wird die E-Mail Adresse des Verwalters der eigenen Zertifizierungsstelle oder dessen Abteilung eingetragen.
 Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Sicherheit“
 Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel „Firma“
 Locality (L)	Standort zum Beispiel eine Stadt wie „Neuenhof“
 State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel „AR“ für „Appenzell Ausser rhoden“
 Country (C)	Land, zum Beispiel „CH“ für „Schweiz“
 Serial no.	Seriennummer des Zertifikats

Sektion Issued by

Diese Sektion zeigt Informationen über den Aussteller des CA-Zertifikates (Wurzel-Zertifikat).
Abhängig vom Aussteller müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
 Name (CN)	Name der ausstellenden CA
 E-mail address	In der Regel eine E-Mail Adresse für Support-Anfragen an den Aussteller
 Org. unit (OU)	Gibt eine Organisationseinheit des Ausstellers an
 Organization (O)	Gibt die ausstellende Organisation an
 Locality (L)	Gibt den Standort des Ausstellers an
 State (ST)	Gibt ein Bundesland, Kanton, Provinz oder Ähnliches des Ausstellers an
 Country (C)	Gibt das Land des Ausstellers an

Sektion **Validity**

Gibt die Gültigkeit des eigenen CA-Zertifikates an.

Parameter	Beschreibung
 Issued on	Ausstelldatum des Zertifikates
 Expires on	Ablaufdatum des Zertifikates

Sektion **Fingerprint**

Der Fingerprint ist die Prüfsumme (auch hash) und dient dem Überprüfen eines Zertifikats. An dieser Stelle wird der Hash-Algorithmus (zum Beispiel MD5 SHA1 oder SHA256), mit welchem die Prüfsumme gebildet wurde, sowie der berechnete Wert angezeigt. Sind mehrere Fingerprints unterschiedlicher Algorithmen vorhanden, so wird jeder in einer separaten Zeile ausgegeben.

Parameter	Beschreibung
 SHA1	SHA1 Fingerprint des Zertifikates Beispiel: D8:CF:CC:47:84:92:A9:F0:7E:2A:15:E8:2E:4F:CA:26:5C:60:10:E9
 SHA256	SHA265 Fingerprint des Zertifikates Beispiel: 83:06:F6:84:34:C2:E7:79:50:47:7B:EC:32:B7:22:13:FD:1F:9C:41:B4:B4:F9:C3:AB:85:12:AA:6B:1E:D2:BE

Sektion **Key usage**

Zeigt den Verwendungszweck des Zertifikates an, wobei nur die aus der folgenden Tabelle berücksichtigt werden. Mögliche Status sind jeweils „Yes“ oder „No“.

Parameter	Beschreibung
 S/MIME signing	digitalSignature / Digitale Signatur
 S/MIME encryption	keyEncipherment / Schlüssel Verschlüsselung
 S/MIME CA certificate	keyCertSign / Zertifikatssignatur
 SSL server CA certificate	keyCertSign / Zertifikatssignatur
 SSL client CA certificate	keyCertSign / Zertifikatssignatur

Sektion **Key info**

Zeigt erweiterte Informationen zum Zertifikat an.

Parameter	Beschreibung
 Signature algorithm	Zeigt den Signatur-Algorithmus des Zertifikates an, zum Beispiel • md5WithRSAEncryption • sha1WithRSAEncryption • sha256WithRSAEncryption
 Last certificate check	Zeigt den Zeitpunkt der letzten Zertifikatsprüfung (via CRL beziehungsweise OCSP) an. Über Check now... kann ein sofortiges Prüfen der Revokations-Informationen erzwungen werden.
 Last check result	Zeigt das Ergebnis der letzten Zertifikatsprüfung an.
 OCSP URI	Gibt die authorityInformationAccess (kurz AIA, Zugriff auf Stelleninformationen) - also den OCSP Pfad - aus. Dieser Punkt ist nur dann sichtbar, wenn im Zertifikat die extension authority information access gesetzt ist.
 CRL URI	Gibt den crlDistributionPoint (Sperrlisten Verteilungspunkt) - also die Lokation, unter welchem die CRL bereit gestellt wird - aus. Dieser Punkt ist nur dann sichtbar, wenn im Zertifikat die extension crlDistributionPoint gesetzt ist.

Sektion **Comment**

An dieser Stelle kann ein persönlicher Kommentar zum Zertifikat eingegeben werden, zum Beispiel weshalb die entsprechende Vertrauensstellung gewählt wurde.

Mit **Save comment** wird dieser Kommentar gespeichert.

Über die Schaltfläche **Download certificate** besteht die Möglichkeit das Zertifikat im CRT-Format zu speichern. Je nach Vertrauensstellung wird die Schaltfläche **Trust this certificate**, über welche dem Zertifikat das Vertrauen bestätigt wird oder **Untrust this certificate**, durch welche das Vertrauen abgelehnt wird, vorhanden.

Über **Delete certificate** wird das Zertifikat von der SEPPmail Appliance gelöscht. Wird im Anschluss eine E-Mail empfangen, welche mit einem Schlüssel dieser Zertifizierungsstelle signiert wurde, so wird das Zertifikat wieder mit dem **Trust-Status** „?“ in der Appliance gespeichert.

7.23 Domain Certificates

Durch Klicken von **S/MIME domain certificates...** öffnet das Sub-Menü für das Verwalten manuell importierter **S/MIME Domain Certificates** von Kommunikationspartnern.

Durch Klicken von **OpenPGP domain keys...** öffnet das Sub-Menü für das Verwalten importierter **OpenPGP domain keys** von Kommunikationspartnern.

Sektion Domain encryption usage

Hinweis zur Arbeitsweise der **Domänenverschlüsselung** über den **Managed Domain Service**.

Sektion Search for managed S/MIME certificate

Mit **Display managed domain certificate...** wird geprüft, ob die eingegebene E-Mail Domäne ebenfalls am **SEPPmail Managed Domain Service** teilnimmt.

Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Ob die eigene(n) Domäne(n) ebenfalls für den **Managed Domain Service** freigeschaltet sind, kann der Spalte **SEPPmail Managed Domain Encryption** der Tabelle unter **Mail System** **Managed domains** entnommen werden.

Sektion Managed SEPPmail domain certificates

Da alle SEPPmail Appliances im Standard (siehe **Mail System** **Managed domains** **ADD/EDIT MANAGED DOMAIN** **Settings** **S/MIME domain keys**) am sogenannten **Managed Domain Service** teilnehmen, findet zwischen SEPPmail Appliances mindestens eine **Domänenverschlüsselung** statt, ohne explizit Schlüsselmateriale austauschen zu müssen.

Der Austausch der **Managed Domain Service** Zertifikate erfolgt alle *(geändert in Version 12.0.11) sechs Stunden* stündlich automatisch über den SEPPmail Key Server, sofern die Option  **Auto-update S/MIME domain certificates** aktiv ist. Im Bedarfsfall (zum Beispiel bei Hinzukommen eines neuen, bekannten Kommunikationspartners) kann ein sofortiges Herunterladen neu hinzugekommener Schlüssel über die Schaltfläche **Update domain certificates...** forciert werden.

Die Anzahl der über diesen Dienst verfügenden E-Mail Domänen wird im Text direkt unter der Sektionsüberschrift angegeben.

Die Domänen, zu welchen in den letzten drei Monaten über den **Managed Domain Service** verschlüsselt kommuniziert wurde, werden in der Tabelle dieser Sektion nach Top-Level-Domain sortiert aufgeführt.



Hinweis:

Beim **Managed Domain Service** wird der S/MIME Verschlüsselungsalgorithmus AES256 verwendet.

7.23.1 S/MIME domain certificates

Dieses Sub-Menü wird aus **Domain Certificates** ^[489] aufgerufen.

Sektion Domain encryption usage

Hinweis zur Arbeitsweise der **Domänenverschlüsselung** ^[31].

Sektion Filter manual S/MIME domains

Mit **Filter...** wird geprüft, ob für die eingegebene E-Mail Domäne ein manueller Eintrag für die Domänenverschlüsselung via S/MIME vorliegt.

Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Sektion Manual S/MIME domain certificates

Zeigt die Zertifikate aller E-Mail Domänen an, zu denen hin mittels S/MIME domänenverschlüsselt wird. Diesen Domänen sollte im Gegenzug das S/MIME Zertifikat der durch diese SEPPmail Appliance verwalteten E-Mail Domäne(n) bekannt sein. Diese Schlüssel zu den intern in der SEPPmail Appliance verwalteten E-Mail Domänen sind unter **Mail System** ^[247] **Managed domains** ^[247] **ADD/EDIT MANAGED DOMAIN** ^[274] in der **Sektion S/MIME domain encryption** ^[274] zu finden. Die öffentlichen Schlüssel für diese Domänen können je nach GINA-Konfiguration vom Kommunikationspartner auch über das GINA-Portal auf sicherem Wege heruntergeladen werden (siehe **GINA Domains** ^[416] **Domains** ^[416] **CHANGE GINA SETTINGS FOR** ^[423] **Extended settings** ^[431] **Certificate search and management in GINA** ^[433]).



Hinweis:

Der verwendete S/MIME Verschlüsselungsalgorithmus (AESxxx/3DES) ist von der Einstellung **Mail Processing** ^[286] **Ruleset Generator** ^[287] **Encryption / Decryption** ^[292] **Outgoing e-mails** ^[293] **Use default cipher for S/MIME encryption:** ^[296] abhängig.

Spalte	Beschreibung
 Mail domain	Zeigt E-Mail Adresse (RFC822 Name) des Schlüsselinhabers an.
 E-mail address	(Pseudo-)E-Mail Adresse für die Domänenverschlüsselung ^[31] .
 Serial number	Seriennummer des Zertifikats.
 Issued on	Ausstelldatum des Zertifikats in der Form JJJJ-MM-TT
 Expires on	Ablaufdatum des Zertifikats in der Form JJJJ-MM-TT
 Active	Gibt an, ob die Domänenverschlüsselung zum angegebenen Ziel aktiv ist.

Über die Schaltfläche **Import S/MIME certificate...** besteht die Möglichkeit, Zertifikate weiterer Kommunikationspartner (E-Mail Domänen) aufzunehmen. Da die Zertifikate in der Regel direkt durch die Administratoren ausgetauscht werden, reichen an dieser Stelle im Normalfall Self-Signed-Zertifikate aus. Um Fehlerquellen auszuschließen, sollte jedoch darauf geachtet werden, dass die Domänenzertifikate dem Standard RFC 3183 (<https://tools.ietf.org/html/rfc3183>) entsprechen.

**Achtung:**

Die Domänenverschlüsselung zu einer Zieldomäne kann nur über ein Verfahren, S/MIME oder OpenPGP, eingerichtet werden!

Sollte dennoch versucht werden für dieselbe Zieldomäne einen weiteren Schlüssel zu importieren, würde das mit einem Fehler

OpenPGP key already exists for domain ...

quittiert werden.

**Hinweis:**

Sind, beziehungsweise werden für die Domänenverschlüsselung ³¹⁾ vorgesehene E-Mail Domänen beim Import mit einem führenden Punkt „.“ angegeben, so gilt die Verschlüsselung auch für alle zugehörigen Sub Domänen.

Das heißt, ein für „meinefirma.tld“ eingetragener Schlüssel würde zum Beispiel auch für „ch.meinefirma.tld“, „de.meinefirma.tld“ und so weiter gelten.

7.23.2 OpenPGP domain keys

Dieses Sub-Menü wird aus **Domain Certificates** ^[489] aufgerufen.

Sektion Domain encryption usage note

Hinweis zur Arbeitsweise der **Domänenverschlüsselung** ^[31].

Sektion Filter

Mit **Filter...** wird geprüft, ob für die eingegebene E-Mail Domäne ein Eintrag für die Domänenverschlüsselung via OpenPGP vorliegt.

Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Sektion Manual OpenPGP domain keys

Zeigt die Schlüssel aller E-Mail Domänen an, zu denen hin mittels OpenPGP domänenverschlüsselt wird. Diesen Domänen sollte im Gegenzug der öffentliche OpenPGP Key der durch diese SEPPmail Appliance verwalteten E-Mail Domäne(n) bekannt sein. Die Schlüssel zu den intern in der SEPPmail Appliance verwalteten E-Mail Domänen sind unter **Mail System** ^[247] **Managed domains** ^[247] **ADD/EDIT MANAGED DOMAIN** ^[274] in der **Sektion OpenPGP domain encryption** ^[274] zu finden. Die öffentlichen Schlüssel für diese Domänen können je nach GINA-Konfiguration vom Kommunikationspartner auch über das GINA-Portal auf sicherem Wege heruntergeladen werden (siehe **GINA Domains** ^[416] **Domains** ^[416] **CHANGE GINA SETTINGS FOR** ^[423] **Extended settings** ^[431] **Certificate search and management in GINA** ^[433]).

Spalte	Beschreibung
 Mail domain	Gibt die E-Mail Domäne an, für welche der Schlüssel gültig ist. Durch Klicken auf die Domäne werden Details zum Schlüssel angezeigt. Ebenso wird die hierdurch die Möglichkeit geboten, den key im ASC-Format zu speichern oder zu löschen.
 Key ID	Zeigt die Key Ids der vorhandenen OpenPGP keys an.
 Subkey ID(s) <i>(neu in 12.1)</i>	Zeigt die Key Ids aller vorhandenen Subkeys an.
 Issued on	Ausstelldatum des Zertifikats in der Form JJJJ-MM-TT
 Expires on	Ablaufdatum des Zertifikats in der Form JJJJ-MM-TT
 Active	Gibt an, ob die Domänenverschlüsselung zum angegebenen Ziel aktiv ist.

Über die Schaltfläche Import **Import OpenPGP key...** besteht die Möglichkeit, Schlüssel weiterer Kommunikationspartner (E-Mail Domänen) aufzunehmen.



Achtung:

Die Domänenverschlüsselung zu einer Zieldomäne kann nur über ein Verfahren, S/MIME oder OpenPGP, eingerichtet werden!

Sollte dennoch versucht werden für dieselbe Zieldomäne einen weiteren Schlüssel zu importieren, würde das mit einem Fehler

S/MIME certificate already exists for domain ... quittiert werden.

**Hinweis:**

Sind, beziehungsweise werden für die **Domänenverschlüsselung** ³¹⁾ vorgesehene E-Mail Domänen beim Import mit einem führenden Punkt „.“ angegeben, so gilt die Verschlüsselung auch für alle zugehörigen Sub Domänen.

Das heißt, ein für „meinefirma.tld“ eingetragener Schlüssel würde zum Beispiel auch für „ch.meinefirma.tld“, „de.meinefirma.tld“ und so weiter gelten.

7.24 Customers

Ist eine Multitenancy Lizenz vorhanden, so lässt sich in diesem Menü die Mandantenfähigkeit des Systems aktivieren, beziehungsweise die Mandanten verwalten.

Sektion **Multiple customers**

Nach Anwahl von **Enable multiple customer handling** lässt sich über **Enable** die Mandantenfähigkeit aktivieren. Voraussetzung hierfür ist natürlich das Vorhandensein der entsprechenden Lizenz (siehe **Home** ^[220] **License** ^[220] **Multitenancy** ^[221]).



 **Achtung:**
Dieser Prozess ist irreversibel!

*(geändert in 12.0.9) Sollte diese bereits aktiv sein, so bietet sich die Möglichkeit über das DropDown-Menü einen Mandanten auszuwählen und über **Delete...** zu löschen oder über **Edit...** zu bearbeiten. Weiter bietet*

Create new customer... bietet die Möglichkeit einen neuen Mandanten anzulegen.

Nach Anschalten der Mandantenfähigkeit existieren bereits zwei Standard Customers, („No Customer“ und „Default Customer“), welche für die interne Verwaltung benötigt werden und nicht gelöscht werden können.

Wird bei einer bereits bestehenden Installation mit bereits vorhandenen GINA Accounts nachträglich die Mandantenfähigkeit aktiviert, so werden diese Accounts zunächst dem „Default Customer“ zugeordnet. Um das nachträgliche zuordnen der Accounts zum richtigen Mandanten zu erleichtern, wird angezeigt, aus welcher **Managed domain** ^[247] der Account erzeugt wurde.

Der „No Customer“ bietet die Möglichkeit, einzelne Accounts - gegebenenfalls temporär - komplett aus der Mandantenfähigkeit auszuschließen.

Ist bei einem nachträglichen Anschalten der Mandantenfähigkeit das sofortige zuordnen zu einem Mandanten aus dem „Default Customer“ heraus nicht erwünscht - wenn der Account zum Beispiel einem später noch einzurichtenden Mandanten zugeordnet werden soll - so kann dieser im „No Customer“ quasi „zwischengeparkt“ werden.

(neu in 12.1)

Spalte	Beschreibung
 Customer	Liste aller auf der SEPPmail Appliance angelegten Mandanten.
 Description	Zeigt die bei der Anlage des jeweiligen Mandanten eingegebene Beschreibung an.
 Domains	Zeigt die dem jeweiligen Mandanten zugeordnete(n) Managed domain ^[247] (s) an.
 Users	Zeigt die Anzahl der Postfächer aus allen Managed domain ^[247] des jeweiligen Mandanten an, welche bereits über die SEPPmail Appliance E-Mails in das Internet gesendet haben.
 GINA users	Zeigt die Anzahl der GINA-Accounts ^[462] an, welche dem jeweiligen Mandanten zugeordnet sind (siehe auch Edit settings for customer "x" ^[496] Assigned GINA accounts ^[496]).
 Valid S/MIME certificates	Zeigt die Anzahl der aktuell vorhandenen, gültigen S/MIME Zertifikate des jeweiligen Mandanten an.
 Encryption licenses (used /	Zeigt die für den jeweiligen Mandanten insgesamt verfügbaren (limit) Signatur und Verschlüsselung ^[127] lizenzen an und wieviele davon aktuell genutzt werden (used)

Spalte	Beschreibung
limit)	
 LFT Licenses (used / limit)	Zeigt die für den jeweiligen Mandanten insgesamt verfügbaren (limit) Large File Transfer (LFT) [128] Lizenzen an und wieviele davon aktuell genutzt werden (used)
 Action	 Lädt eine CSV-Datei (Statistik) mit den Lizenz technisch relevanten Informationen herunter  Lädt ein Backup (Export) des Mandanten herunter (vergleiche Backup/Restore [498]).  Löscht den Mandanten

Sektion Notes

Für einen Mandanten **muss** immer (mindestens) eine eigene GINA-Domain angelegt werden (siehe gegebenenfalls **GINA Domains** [416] **Domains** [416] **Create new GINA domain** **CREATE NEW GINA DOMAIN** [422]). Sollte der Mandant mehrere **Managed domains** [247] inne haben, so kann all diesen die gleiche GINA-Domain zugeordnet (siehe **Mail System** [247] **Managed domains** [247] **ADD/EDIT MANAGED DOMAIN** [266] **Settings** [266] **GINA domain** [270]) werden.



Achtung:

Keinesfalls darf eine GINA-Domain für mehrere Mandanten verwendet werden!
Das Verwenden einer GINA-Domain für mehrere E-Mail (Managed) Domänen eines einzigen Mandanten ist hingegen problemlos möglich.

Externe Empfänger welche mit mehreren Mandanten mittels GINA kommunizieren, erhalten für jeden Mandanten einen eigenen GINA Account, mit den daraus resultierenden Einschränkungen (siehe **GINA Domains** [416] **Domains** [416] **CHANGE GINA SETTINGS FOR** [437] **Extended settings** [437]).

Öffentliche Schlüssel (siehe **OpenPGP Public Keys** [467] und **X.509 Certificates** [471]) stehen grundsätzlich allen Mandanten für die Verschlüsselung zur Verfügung.

7.24.1 Create New / Edit Settings For Customer

Dieses Sub-Menü wird aus **Customers** ^[494] **Multiple Customers** ^[494] aufgerufen.

Dieses Menü dient der Anlage neuer beziehungsweise dem Verwalten bereits vorhandener Mandanten auf der SEPPmail Appliance.

Die Anlage neuer Mandanten kann manuell, oder durch den Import eines bereits bestehenden Mandanten Backup (zum Beispiel für den Umzug eines Mandanten auf eine andere Maschine) erfolgen.

Sektion **Customer details**

Diese Sektion enthält Informationen zum Mandanten und verhält sich je nach Modus - „Create“ oder „Edit“ - unterschiedlich.

Parameter	Beschreibung
 Customer	Eingabe des System-Namens für einen neuen Mandanten. Die Eingabe ist nur bei der Neuanlage möglich. Im Editier-Modus wird der Name lediglich angezeigt.
 Customer name	Anzeige-Name des Mandanten.
 Customer admin e-mail	E-Mail Adresse des Mandanten-Administrators, welcher die Mandanten spezifischen Systemmeldungen erhalten soll.
 Comment	Optional, frei wählbarer Kommentar.
 Creation info	Systeminformationen zur Erzeugung des Mandanten. Dieses Feld ist erst nach dem Erzeugen des Mandanten, also im Editier-Modus zu sehen.

Im „Create“-Modus wird der Benutzer mittels Schaltfläche **Create** mit den angegebenen Daten angelegt. Das System wechselt sodann in den Editier-Modus.

Im Editier-Modus werden vorgenommene Änderungen über die Schaltfläche **Change** übernommen.

Sektion **Import backup**

Diese Sektion erscheint nur im „Create“-Modus und dient der Anlage neuer Mandanten durch den Import eines bereits bestehenden Mandanten Backups (zum Beispiel für den Umzug eines Mandanten auf eine andere Maschine).

Die vorhandene Backup Datei wird über die Schaltfläche **Import backup file ...** eingespielt.

Alle folgenden Menüs sind nur vom System-Administrator im **Editier-Modus** zu sehen:

Sektion **Customer administrators**

Dient dem Verwalten von Mandanten Admins. Mandanten Admins sind in der Lage sich interaktiv am System anzumelden und sehen die für sie relevanten Menüs **Login/Logout** ^[219], **Logs** ^[388], **Users**, **GINA Domains** ^[416], **GINA Accounts** ^[462], **Customers** ^[494] und optional bei aktivierter Option **LFT accounts** ^[466]. Dabei beschränkt sich die Anzeige in den Menüs ausschließlich auf die Daten des jeweiligen Mandanten.

Bereits zugeordnete Mandanten Admins sind in der folgenden Tabelle zu sehen und können dort verwaltet werden.

Spalte	Beschreibung
 User ID	Zeigt die Benutzer ID des jeweiligen Administrators, wie sie unter Users ^[396] angezeigt wird.

Spalte	Beschreibung
 E-mail	Zeigt die E-Mail Adresse des jeweiligen Administrators, wie sie unter Users ^[396] angezeigt wird.
 Remove from this customer	Beinhaltet die Schaltfläche Remove zum Entfernen des jeweiligen Mandanten Admins.

Die weitere Tabelle der Sektion dient dem Zuordnen weiterer Mandanten Admins.

Spalte	Beschreibung
 Name	Beherbergt das DropDown Menü ☐ zur Auswahl des Benutzers, der als Mandanten-Admin zugeordnet werden soll.
 Assign to this customer	Über die Schaltfläche Assign wird der unter Name ausgewählte Benutzer als Mandanten-Admin hinzugefügt.



Hinweis:

Mandanten Admins müssen über ein Passwort verfügen (siehe **Users** ^[396] **USER** 'USER@DOMAIN.TLD' ^[398] **User data** ^[398] **Password**), damit das Anmelden am System möglich ist!



Hinweis:

Wird ein Mandanten-Admin vom Maschinen-Admin (siehe **Groups** ^[413] **admin (Administrator)** ^[413] in **Groups** ^[413] **readonlyuser (Read-only GUI access to restricted sections)** ^[414] aufgenommen, so hat dieser Mandanten-Admin ausschließlich Leserechte.



Sektion **License limiter**

An dieser Stelle können die für den jeweiligen Mandanten zur bereitstehenden Lizenzen limitiert werden. Wird ein Feld leer gelassen, wird nicht limitiert. Das heißt der Mandant kann beliebig viele Lizenzen aus dem Gesamtkontingent der Maschine beziehen.

Parameter	Beschreibung
 Maximum encryption licenses	Limit der Signatur und Verschlüsselung ^[127] lizenzen.
 Maximum large file licenses	Limit der Large File Transfer (LFT) ^[128] Lizenzen.

Änderungen werden durch **Change** übernommen.



Sektion **Assigned managed domains**

In dieser Sektion werden die dem Mandanten zugeordneten **Managed domains** ^[247] angezeigt. Das Zuordnen von **Managed domains** ^[247] zum Mandanten erfolgt in der Regel bereits bei der Anlage über das Menü **Mail System** ^[247] **Managed domains** ^[247] **ADD/EDIT MANAGED DOMAIN** ^[268] **Bounce templates** ^[270].

Spalte	Beschreibung
 Domain name	Zeigt die zugeordnete(n) Managed domain(s) ^[247]
 Remove from this customer and reassign to Default Customer	Beinhaltet die Schaltfläche Remove zum Entfernen der jeweiligen Managed domain ^[247] .

Die folgende Tabelle wird nur dann angezeigt, wenn nicht zugeordnete **Managed domains** ^[247] vorhanden sind..

Spalte	Beschreibung
 Domain name	Beherbergt das DropDown Menü ☐ zur Auswahl der Managed domain ^[247] , welche dem Mandanten zugeordnet werden soll.
 Assign to this customer	Über die Schaltfläche Assign wird der unter <i>Domain name</i> ausgewählte Benutzer als Mandanten-Admin hinzugefügt.

Sektion **Assigned GINA accounts**

In dieser Sektion wird die Anzahl der dem Mandanten zugeordneten GINA-Benutzer angezeigt.

Über die Schaltfläche **Manage accounts** können die GINA-Benutzer des Mandanten verwaltet sowie gegebenenfalls nicht zugeordnete Accounts zugeordnet werden (siehe **MANAGE ASSIGNED GINA ACCOUNTS** ^[500]).

Sektion **Backup/Restore**

Parameter	Beschreibung
 Backup	Der System- oder Mandanten- Administrator über Schaltfläche Download das Herunterladen der Mandanten-Backup-Datei starten. Diese Datei beinhaltet ausschließlich die mandantenrelevante Konfiguration und dessen Schlüsselmateriale. Voraussetzung für den Download des Backups ist die Vergabe eines Backup Passwortes, welches via Change password gesetzt beziehungsweise geändert werden kann.
 ☐ Automatically send backup to Customer Admin E-mail	Durch Aktivieren dieser Option erhält der eingetragene Mandanten Administrator täglich per E-Mail sein Mandanten Backup. Ein Ändern dieser Option muss durch klicken der Schaltfläche Change bestätigt werden.
 Restore	Durch klicken von Import backup File... kann das Mandanten Backup durch den System- oder Mandanten- Administrator zurück gespielt werden. Hierfür wird das zum Zeitpunkt des Erstellens des Backups gültige Backup-Passwort benötigt. Das Einspielen des Backups stellt die mandantenspezifischen Teile der Appliance - mit Ausnahme der Log-Dateien - zu 100% wieder her.

Sektion **Retention settings**

Die hier aufgeführten Optionen ersetzen in mandantenfähigen Systemen die gleichlautenden Einstellungen unter **GINA Domains** ^[416] **Settings** ^[416].

Änderungen werden via **Change** gespeichert.

7.24.1.1 Manage Assigned GINA Accounts

Dieses Sub-Menü wird aus **Customer Management** ^[496] **Assigned** ^[496] **GINA accounts** ^[498] aufgerufen.

Sektion **Assigned GINA accounts**

Zeigt die dem Mandanten bereits zugeordneten GINA-Benutzer an und bietet die Möglichkeit einzelne GINA-Benutzer von diesem Mandanten zu entfernen, um diesen zum Beispiel einem anderen zuzuordnen. Somit bleibt das Schlüsselmaterial des GINA-Benutzers trotz des Wechsels zu einem anderen Mandanten identisch.

Über die Schaltfläche **Remove all accounts** kann die Zuordnung für alle GINA-Benutzer entfernt werden.

Spalte	Beschreibung
 Name	Zeigt den Namen des jeweiligen GINA-Benutzers, den er beim Registrieren eingetragen hat.
 E-mail	Zeigt die E-Mail Adresse des jeweiligen GINA-Benutzers.
 Creation info	Zeigt • wer gegebenenfalls die initiale GINA-E-Mail gesendet und somit den Benutzer generiert hat (Anzeige der E-Mail Adresse bei unregistrierten, beziehungsweise „Created by...“ bei bereits registrierten Benutzern) • ob es sich um einen selbstregistrierten Benutzer handelt (Account...)
 Remove from this customer	Beinhaltet die Schaltfläche Remove zum Entfernen GINA-Benutzers.

Sektion **Assign other GINA accounts**

GINA-Benutzer, welche aktuell keinem Benutzer zugeordnet sind werden hier in zwei Tabellen angezeigt.

Dabei zeigt die erste Tabelle diejenigen GINA-Benutzer, welche dem Mandanten zwar nicht zugeordnet sind, jedoch von einem internen Benutzer der SEPPmail Appliance erzeugt wurden, dessen E-Mail Domäne (**Managed domain** ^[247]) dem Mandanten zugeordnet ist.

In der Regel sollten solche GINA-Benutzer dem Mandanten mittels Schaltfläche **Assign** zugeordnet werden.

Über die Schaltfläche **Assign all proposed accounts** kann die Zuordnung für alle aufgelisteten GINA-Benutzer gleichzeitig hinzugefügt werden.

Spalte	Beschreibung
 Name	Zeigt den Namen des jeweiligen GINA-Benutzers, den er beim Registrieren eingetragen hat.
 E-mail	Zeigt die E-Mail Adresse des jeweiligen GINA-Benutzers.
 Creation info	Zeigt wer die initiale GINA-E-Mail gesendet und somit den Benutzer generiert hat. Dies ist immer ein interner Benutzer einer Managed domain ^[247] des Mandanten.
 Assign to this customer	Beinhaltet die Schaltfläche Assign mit welcher der GINA-Benutzer dem Mandanten zugeordnet werden kann.

Die zweite Tabelle der Sektion zeigt diejenigen GINA-Benutzer, welche keinem Mandanten zugeordnet sind und

- von einem internen Benutzer der SEPPmail Appliance erzeugt wurden, dessen E-Mail Domäne (**Managed domain** ^[247]) nicht dem Mandanten zugeordnet ist

- b) mittels Selbstregistrierung (siehe **GINA Domains** ⁴¹⁶ **Domains** ⁴¹⁶ **Edit** **CHANGE GINA SETTINGS FOR** ⁴²³ **Extended settings** ⁴³¹ **Allow account self-registration in GINA portal without initial mail** ⁴³²) generiert wurden.

In der Regel sollten GINA-Benutzer, welche von einem internen Benutzer der SEPPmail Appliance einer **Managed domain** ²⁴⁷ eines anderen Mandanten erzeugt wurden, nicht zugeordnet werden.

Über die Schaltfläche **Assign all unassigned accounts** kann die Zuordnung für alle aufgelisteten GINA-Benutzer gleichzeitig hinzugefügt werden.

Spalte	Beschreibung
 Name	Zeigt den Namen des jeweiligen GINA-Benutzers, den er beim Registrieren eingetragen hat.
 E-mail	Zeigt die E-Mail Adresse des jeweiligen GINA-Benutzers.
 Creation info	Zeigt, ob es sich um einen selbst registrierten GINA-Benutzer handelt, beziehungsweise wer die initiale GINA-E-Mail gesendet und somit den Benutzer generiert hat. Dies ist <u>kein</u> Benutzer einer Managed domain ²⁴⁷ des Mandanten.
 Assign to this customer	Beinhaltet die Schaltfläche Assign mit welcher der GINA-Benutzer dem Mandanten zugeordnet werden kann.

7.24.2 Delete Customer

Dieses Sub-Menü wird aus **Customers** ⁴⁹⁴ **Multiple Customers** ⁴⁹⁴ über  aus der Spalte **Action** ⁴⁹⁵ aufgerufen.

Das Menü dient dem Löschen einzelner Mandanten-Teile bis hin zum Löschen des kompletten Mandanten.

Sektion **Delete options** (neu in 12.1)

In dieser Sektion wird festgelegt, welche Mandanten-Teile gelöscht werden sollen.

Parameter	Beschreibung
 ☒ delete everything related to this customer (implies all other delete-options)	Diese Option ist im Standard aktiv. Wir mit aktiver Option gelöscht, so wird der komplette Mandant entfernt. Das heißt, diese Option beinhaltet alle weiteren Löschoptionen.
 ☐ delete all implicate and explicite assigned users	Diese Option ist im Standard inaktiv. Löscht alle dem jeweiligen Mandanten zugeordneten Users ³⁹⁶ . Dabei ist unerheblich, ob die jeweiligen Users ³⁹⁶ dem Mandanten ursprünglich durch die Zugehörigkeit einer ihm zugeordneten Managed Domain ²⁴⁷ automatisch (implizit) oder manuell durch den Administrator (explizit) vorgenommen wurden.
 ☐ delete all assigned GINA users	Diese Option ist im Standard inaktiv. Löscht alle dem Mandanten zugeordneten Assigned GINA accounts ⁴⁹⁶ aus GINA-Accounts ⁴⁶² .
 ☐ delete all assigned admin users	Diese Option ist im Standard inaktiv. Löscht alle dem jeweiligen Mandanten zugeordneten Customer administrators ⁴⁹⁶ aus Users ³⁹⁶ .
 ☐ delete all assigned managed	Diese Option ist im Standard inaktiv.

Parameter	Beschreibung
domains	Löscht alle dem jeweiligen Mandanten zugeordneten Assigned managed domains ^[497] aus Managed Domains ^[247] .
 ☐ delete all assigned GINA domains	Diese Option ist im Standard inaktiv. Löscht alle den jeweiligen Managed Domains ^[247] des jeweiligen Mandanten zugeordneten GINA Domains ^[416] .
 ☐ delete all assigned encryption policies	Diese Option ist im Standard inaktiv. Löscht jede dem jeweiligen Mandanten zugeordnete Encryption Policy ^[313] .
 ☐ delete all disclaimers only used by this customer	Diese Option ist im Standard inaktiv. Löscht alle Disclaimer ^[259] , welche ausschließlich Managed Domains ^[247] des jeweiligen Mandanten zugeordnet sind.

Parameter	Beschreibung
 delete all smarthost credentials only used by this customer	Diese Option ist im Standard inaktiv. Löscht alle Additional credentials for managed domains ^[25] (Smarthost ^[25]-Einträge ^[25]), welche ausschließlich von Managed Domains ^[24] des jeweiligen Mandanten verwendet werden.

Über **Delete** wird das Löschen mit den eingestellten Löschoptionen ausgeführt.

8 Referenz der Regelwerk-Anweisungen

Generell werden die Anforderungen an die Funktion, beziehungsweise den Ablauf des Verarbeitens von E-Mail, mittels des unter **Mail Processing** bereitgestellten **Ruleset generator** umgesetzt.

Sollten Anforderungen über diese Standard Optionen hinaus gehen, so wird ebenfalls im **Ruleset generator** mit dem Abschnitt **Custom commands** die Möglichkeit geschaffen, das Regelwerk programmatisch zu erweitern und die jeweils kundenspezifischen Teile entsprechend im Ablauf zu platzieren. In speziellen Fällen kann auch ein komplettes Regelwerk - ohne die Zuhilfenahme der Möglichkeiten des **Ruleset generator** erstellt und über die Schaltfläche **Upload** der **Sektion SMTP ruleset** eingespielt werden.

In diesem Kapitel werden die möglichen Befehle aufgelistet und die jeweilige Funktion beschrieben.

8.1 Allgemeine Informationen

Grundsätzliche Vorgehensweisen

Bei Einsatz von **Custom commands** wird das Durchführen weitläufiger Tests empfohlen, um die korrekte Funktion zu gewährleisten, aber auch eventuelle Wechselwirkungen festzustellen und noch vor dem produktiven Einsatz zu erkennen.



Achtung:

Für das Ausführen der eigentlichen kryptographischen Aktion sollte innerhalb einer Bedingung - soweit dies möglich ist - immer das entsprechende **Betreffzeilen Schlüsselwörter** gesetzt werden. Damit ist sichergestellt, dass bei Bedarf auch die Standard-Fehlerbehandlungsroutinen zum Tragen kommen.

8.1.1 Syntax

Abschluss von Befehlen

Befehle müssen grundsätzlich mit einem Semicolon (;) abgeschlossen werden.

Parameter

Parameter werden immer durch einfache Anführungszeichen ' ' begrenzt.

Parameter ohne eckige Klammern werden zwingend benötigt und müssen somit angegeben werden.

Parameter in eckigen Klammern, wie zum Beispiel [oldrecipient] sind optional und müssen nicht angegeben werden.

Wird ein optionaler Parameter nicht angegeben, so wird ein vordefinierter Standardwert bzw. das Standardverhalten angewendet.

Sind mehrere optionale Parameter möglich, wobei zum Beispiel nur der zweite Parameter benötigt wird, so muss auch für den ersten Parameter ein gültiger Wert eingesetzt werden.

Eingabe Beispiele:

```
command(required,[optional], [optional]);
```

Richtig:

```
command('required');
```

```
oder      command('required','optional');
```

```
oder      command('required','optional','optional');
```

```
oder      command('required','', 'optional');
```

FALSCH:

```
command('required',, 'optional');
```

Verwenden von Anführungszeichen in Strings

Werden doppelte Anführungszeichen innerhalb eines Strings verwendet, so sind diese innerhalb der einfachen Anführungszeichen zu schreiben, also ' " " '.

Sind einfache Anführungszeichen innerhalb eines Strings zu schreiben, so sind diese durch doppelte Anführungszeichen zu begrenzen, also " ' ' "

Zeilenumbrüche

Zeilenumbrüche in String-Parametern - egal ob innerhalb einfacher (' ') oder doppelter (" ") Anführungszeichen werden auch als solche verarbeitet.

Beispiel:

Der wie folgt in einer angenommenen Test Funktion angegebene String

```
test_funktion('dies ist ein  
Zeilenumbbruch')
```

würde in

```
'dies ist ein\nZeilenumbruch'
```

umgesetzt werden.

Um an dieser Stelle ungewollte Verhaltensweisen zu unterbinden, sind Zeilenumbrüche in Strings zu unterlassen.

Kommentare

Kommentare werden durch Voranstellen von „# “ markiert.

Syntaxprüfung

Wird ein Ruleset mit **Custom commands** ^[308] via **Save and create ruleset** neu generiert beziehungsweise ein komplettes **SMTP ruleset** ^[286] via **Upload** hochgeladen, so erfolgt zunächst eine Syntaxprüfung. Somit wird vermieden, dass syntaktisch falsche Rulesets aktiviert werden.

Bei auftretenden Fehlern wird in der Fehlermeldung in der Statusleiste oben in der Administrationsoberfläche jeweils die Zeilennummer des **SMTP ruleset** ²⁸⁶ ausgegeben, wie es durch Klicken von **Display Ruleset** angezeigt wird.

8.1.2 Variablen

Für Befehle, welche den Hinweis „Variablen verfügbar“ enthalten, stehen sowohl die Variablen aus der folgenden Tabelle, sowie die gegebenenfalls über die Befehle `setvar()` ^[522] und `ldap_read()` ^[617] erzeugten Variablen zur Verfügung.

Variablen sind jeweils an eine E-Mail gebunden.

Variable	Inhalt
\$from	Absender aus dem Envelope der E-Mail
\$header_from	Absender aus dem FROM-Header der E-Mail
\$user_mail	E-Mail Adresse, des authentisierten Benutzers (siehe auch <code>authenticated()</code> ^[537])
\$user_name	Eingetragene CN / Full Display Name des Nutzers (siehe auch <code>Name</code> ^[396])
\$to	Empfänger aus dem Envelope der E-Mail
\$header_to	Empfänger aus dem TO-Header der E-Mail
\$header_cc	Empfänger aus dem CC-Header der E-Mail
\$head	Kompletter E-Mail Header
\$admin	wird nur übersetzt in die „Postmaster“ ^[252] Adresse
\$mailid	Message ID der E-Mail
\$subject	Betreff der E-Mail
\$date	Datum der E-Mail
\$vscanresult	Sofern der Viren-Scan aktiv ist Ergebnis des selbigen der E-Mail



Achtung:

Bei Befehlen, welche gleichnamige Variablen mit anderem als in der Tabelle genannten Inhalt verwenden, ist dies in den jeweiligen Beschreibungen hinterlegt.

8.1.3 Kontrollstrukturen - if/else Anweisungen

Die `if/else` Anweisungen sind Kontrollstrukturen und dienen innerhalb des Rulesets der Ablaufsteuerung. Sie sind ein elementarer Bestandteil des Regelwerks. Ist eine Bedingung erfüllt, wird eine Aktionen ausgeführt, sonst wird eine alternative Aktion ausgeführt. Die auszuführende Aktion kann immer nur ein Befehl sein. Wenn als Aktion mehrere Befehle ausgeführt werden sollen, so können diese einzelnen Befehle in einem Anweisungsblock zusammengefasst werden. Ein Anweisungsblock wird innerhalb geschweifter Klammern geschrieben.

Mit `if` wird festgelegt, welche Voraussetzung für das Ausführen einer Aktion erfüllt sein muss. Mit `else` wird eine alternative Aktion eingeleitet, sollte die durch `if` geforderte Bedingung nicht erfüllt sein. Eine `if/else` Anweisung muss nicht durch ein Semikolon abgeschlossen werden. `if/else` Anweisungen können geschachtelt werden.

Ein führendes Ausrufezeichen „!“ bei einem Befehl innerhalb der Abfrage invertiert die Funktion des Befehls.

Aufbau einer if/else Anweisung

```
if (Bedingung) {  
    Anweisungsblock 1;  
}
```

oder

```
if (!Bedingung) {  
    Anweisungsblock 1;  
}
```

oder

```
if (Bedingung) {  
    Anweisungsblock 1;  
} else {  
    Anweisungsblock 2;  
}
```

oder

```
if (Bedingung) {  
    Anweisungsblock 1;  
} else if (Bedingung) {  
    Anweisungsblock 2;  
} else {  
    Anweisungsblock 3;  
}
```

Die `if`-Anweisung bestimmt aufgrund des Rückgabewertes der `Bedingung` den weiteren Verlauf im Programmablauf. Die Bedingung besteht aus einem einzelnen Befehl, welcher mindestens einen Rückgabewert hat.

`Anweisungsblock 1` wird nur dann ausgeführt, wenn der Rückgabewert **positiv** ist. Andernfalls wird ausschließlich `Anweisungsblock 2` ausgeführt.

Beispiel

a)

Zeile	Code
01	<code>if (authenticated()) {</code>
02	<code>} else {</code>
03	<code>createaccount();</code>
04	<code>log(1, 'user account generated');</code>
05	<code>}</code>

b)

Zeile	Code
01	<code>if (!authenticated()) {</code>
03	<code>createaccount();</code>
04	<code>log(1, 'user account generated');</code>
05	<code>}</code>

Erklärung

Das Beispiel a) wertet den Rückgabewert des Befehls `authenticated()` aus. Konnte der interne Absender der E-Mail erfolgreich authentifiziert werden, so ist der Rückgabewert **true**. Nachdem für diesen Fall keine weitere Anweisung definiert wurde, wird ohne weitere Aktion im Programmablauf fortgefahren. Schlug das Authentifizieren fehl, das heißt der Rückgabewert ist **false**, so kommt der unter `else` angeführte Anweisungsblock zum Tragen. Im Beispiel würde somit ein Benutzerkonto für den Absender angelegt und ein OpenPGP Schlüsselpaar erzeugt.

In Beispiel b) wird die Funktion des Befehls `authenticated()` durch das vorangestellte `!` in `!authenticated()` invertiert, wodurch der nachfolgende Anweisungsblock der `else` Bedingung aus Beispiel a) entspricht.

Das Programmiererergebnis beider Varianten wird also das gleiche sein.

8.1.4 Makros

Makros sind Codeblöcke, welche einmalig definiert (siehe auch [Mail Processing](#) ^[286] [Ruleset generator](#) ^[287] **Custom commands** ^[308] [Custom macros and commands for all e-mails BEFORE processing:](#) ^[309]) und im Anschluss beliebig oft in den Custom Commands verwendet werden können.

Makros

- können jederzeit definiert werden und sind global gültig.
- können erst verwendet werden, nachdem sie deklariert wurden.
- können nicht redefiniert werden, das heißt ist bereits ein Makro mit gleichem Namen vorhanden, wird dieses nicht überschrieben.
- enthalten komplette Codeblöcke, das heißt sie können nicht als Variablen in Funktionen verwendet werden.
- können ineinander verschachtelt werden.
- können beliebig oft aufgerufen werden.
- werden zur Compile-Time - also beim Generieren eines neuen Rulesets (siehe auch [Mail Processing](#) ^[286] [Ruleset generator](#) ^[287] [Save and Create ruleset](#)) - gelesen und expandiert.
- mit falscher Syntax verhindern das Generieren eines Rulesets.
- mit korrekter Syntax, welche jedoch nicht verwendet werden, erzeugen beim Generieren des Rulesets keinen Code.
- dürfen keine [Vordefinierte Funktionen](#) ^[629] enthalten.

Aufbau eines Makros

```
<Name_des_Makros> = {
  Codeblock
};
```

Abruf eines Makros

```
$<Name_des_Makros>;
```

Beispiel

Zeile	Code
01	my encryption = {
02	if (smime keys avail()) {
03	log(1, 'S/MIME certificate available for recipient(s) \$to');
04	if (encrypt smime()) {
05	log(1, 'e-mail successfully S/MIME encrypted');
06	} else {
07	log(1, 'e-mail could not be S/MIME encrypted');
08	}
09	} else {
10	log(1, 'no S/MIME certificate available for recipient(s) \$to');
12	}
13	};

Abruf des Makros (in jedem beliebigen **Custom commands** ^[308], gegebenenfalls auch verschachtelt in weiteren Makros):

Zeile	Code
01	\$my_encryption;
02	deliver();

8.1.5 Reguläre Ausdrücke

Innerhalb von Befehlen werden zum Teil Reguläre Ausdrücke (regular expressions) verwendet, welche der Perl Syntax entsprechen müssen. Meist werden Reguläre Ausdrücke als Such-Zeichenketten (search strings) verwendet. Jedoch ist auch das Ersetzen von Ausdrücken möglich.

Zahlreiche Erklärungen und Beispiele hierzu sind im Internet zu finden, beispielsweise unter

http://de.wikipedia.org/wiki/Regul%C3%A4rer_Ausdruck

http://wiki.selfhtml.org/wiki/Perl/Regul%C3%A4re_Ausdr%C3%BCcke



Hinweis:

Folgende Zeichen haben bei Regulären Ausdrücken eine Sonderfunktion:

. ^ \$ * + ? () [] { } < > \ |

Sollen diese als „normale“ Zeichen verwendet werden, so müssen sie durch Voranstellen eines \ markiert (escaped) werden (siehe folgende Tabelle).

Auflistung von Zeichen mit Sonderfunktion und ihre Wirkung

Zeichen	Wirkung / Einsatz
beliebig	steht für das Zeichen, falls nicht anders angegeben.
.	steht für ein beliebiges einzelnes Zeichen außer einem Zeilen- oder einem Absatzumbruch. Beispielsweise liefert der Suchbegriff „Schmi.t“ liefert sowohl „Schmitt“ als auch „Schmidt“.
^	findet den Suchbegriff nur, wenn er am Absatzanfang steht. Sonderinhalte wie zum Beispiel Leerfelder und an Zeichen verankerte Rahmen am Absatzanfang werden ignoriert. Beispiel „^Peter“.
^.	findet das erste Zeichen eines Absatzes.
\$	findet den Suchbegriff nur, wenn er am Absatzende steht. Sonderinhalte wie zum Beispiel Leerfelder und an Zeichen verankerte Rahmen am Absatzende werden ignoriert. Beispiel „Peter\$“.
	allein stimmt mit dem Ende eines Absatzes überein. So ist es möglich, Absatzumbrüche zu suchen und zu ersetzen.
^\$	findet einen leeren Absatz.
*	findet keines oder mehr der Zeichen vor dem „*“. So liefert etwa der Suchbegriff „Ab*c“ die Einträge „Ac“, „Abc“, „Abbc“, „Abbbc“ und so weiter.
+	findet ein oder mehr der Zeichen vor dem „+“. Beispielsweise findet „AX.+4“ zwar „AXx4“, jedoch nicht „AX4“. Es wird immer die längstmögliche Zeichenfolge gefunden, die dem Suchmuster in einem Absatz entspricht. Wenn der Absatz die Zeichenfolge „AX 4 AX4“ enthält, wird der gesamte Ausdruck hervorgehoben.
?	findet keines oder eines der Zeichen vor dem „?“. Beispielsweise findet „Texts?“ „Text“ und „Texts“ und „x(ab c)?y“ findet „xy“, „xaby“ oder „xcy“.
\	die Suchfunktion interpretiert das Sonderzeichen nach dem „\“ als ein normales Zeichen und nicht als einen regulären Ausdruck (außer bei den Kombinationen \n, \t, \> und \<). Beispielsweise wird bei der Suche nach „kein.\" zwar „kein.“ gefunden, jedoch nicht „keine“ oder „keins“.
\n	steht im Feld „Suchen nach“ für einen mit Umschalt+Eingabetaste eingefügten Zeilenumbruch. Im Feld „Ersetzen durch“ steht \n für einen Absatzumbruch. So werden Zeilenumbrüche jeweils gegen Absatzumbrüche ausgetauscht, indem \n jeweils in die Felder „Suchen nach“ und „Ersetzen durch“ eingegeben wird.
\s	steht für ein Leerzeichen. Dieser Ausdruck kann auch im Feld „Ersetzen durch“ verwendet werden.
\t	steht für ein Tabulatorzeichen. Dieser Ausdruck kann auch im Feld „Ersetzen durch“ verwendet werden.
\b	findet eine Wortgrenze. Zum Beispiel findet „\bbuch“ das Wort „Buchstabe“ aber nicht „Textbuch“, wohingegen „buch\b“ das Wort „Textbuch“ findet aber nicht „Buchstabe“.
& oder \$0	fügt die Zeichenfolge, die durch die Suchkriterien im Feld „Suchen nach“ gefunden wurde, zu dem Begriff im Feld „Ersetzen durch“ hinzu. Wird in „Suchen nach“ beispielsweise „Fenster“ und in „Ersetzen durch“ „&rahmen“ eingegeben, so wird das Wort „Fenster“ durch „Fensterrahmen“ ersetzt. Weiterhin können mit dem Ausdruck „&“ im Feld „Ersetzen durch“ die Attribute oder das Format des durch die Suchkriterien gefundenen Suchbegriffs geändert werden.
[abc123]	steht für eines der Zeichen in der Klammer.
[a-e]	steht für irgendein Zeichen zwischen a und e, einschließlich beider Start- und Endzeichen. Die Zeichen werden anhand ihrer Kennziffer angeordnet.
[a-eh-x]	steht für ein beliebiges Zeichen im Buchstabenbereich a-e und h-x.

Zeichen	Wirkung / Einsatz	
[^a-s]	repräsentiert alles, was nicht zwischen a und s ist.	
\uXXXX	steht für ein Zeichen auf Grundlage seines vierstelligen Hexadezimal-Unicode (XXXX).	Der Code einiger Zeichen hängt von der jeweiligen Schrift ab
\UXXXXXX XX	für unbedeutende Zeichen mit achtstelligem Hexadezimal-Unicode (XXXXXXXX).	
	findet sowohl Begriffe, welche vor dem „ “ vorkommen, als auch die, die nach dem „ “ auftauchen. „dies das“ findet „dies“ und „das“.	
{2}	gibt an, wie oft das Zeichen vor der öffnenden Klammer vorkommen muss. Zum Beispiel liefert der Suchbegriff „Man{2}“ das Wort „Mann“.	
{1,2}	gibt sowohl die minimale als auch maximale Anzahl an, die das Zeichen in vor der sich öffnenden Klammer vorkommen kann. „Man{1,2}“ findet und wählt sowohl „Man“, als auch „Mann“.	
{1,}	gibt an, wie oft das Zeichen vor der öffnenden Klammer im Wort mindestens vorkommen muss. Beispiel: Der Suchbegriff „Man{2,}“ findet „Mann“, „Mannn“ und „Mannnn“.	
()	<u>im Feld „Suchen nach“:</u> Die in der Klammer enthaltenen Zeichen gelten als Referenz. Auf die erste Referenz im aktuellen Ausdruck kann dann mit „\1“, auf die zweite mit „\2“ und so weiter. Bezug genommen werden. Enthält ein Text zum Beispiel die Zahl 134 87 889, so würde eine Suche mit dem Ausdruck (8)7\1\1 , „ 8788 “ finden. Ebenso kann durch () Suchtext gruppiert werden. Der Suchtext „a(bc)?d“ findet somit „ad“ oder „abcd“.	
	<u>Im Feld „Ersetzen durch“:</u> Um Referenzen zu ersetzen, wird statt \ (umgekehrter Schrägstrich) \$ (Dollar) verwendet. Um die gesamte gefundene Zeichenkette zu ersetzen, wird \$0 verwendet.	
	[alpha:]?	Steht für ein alphabetisches Zeichen. Verwenden Sie [alpha:]+, um eines zu finden.
	[digit:]?	Steht für eine Dezimalziffer. Verwenden Sie [digit:]+, um eine Ziffer zu finden.
	[alnum:]?	Steht für ein alphanumerisches Zeichen ([alpha:] und [digit:]).
	[space:]?	Steht für ein Leerzeichen (aber kein anderes Platzhalter-Zeichen).
	[print:]?	Steht für ein druckbares Zeichen.
	[cntrl:]?	Steht für ein nicht-druckbares Zeichen.
	[lower:]?	Steht für einen Kleinbuchstaben, wenn Groß-/Kleinschreibung in den Optionen ausgewählt ist.
	[upper:]?	Steht für einen Großbuchstaben, wenn Groß-/Kleinschreibung in den Optionen ausgewählt ist.

Beispiele

max\.mustermann@test\.tld
steht für die E-Mail Adresse max.mustermann@test.tld

@test\.tld
steht für alle E-Mail Adressen aus der Domäne test.tld

@test\...+
steht für alle E-Mail Adressen aus den Domäne test.*, also zum Beispiel test.ch, test.com, test.local aber auch test.local.de und so weiter.

@test\...{3,4}\$
steht für alle E-Mail Adressen aus den Domäne test.* mit zwei oder dreistelliger Länderdomäne, also zum Beispiel test.ch, test.com, nicht aber test.a oder test.abcd und so weiter.

@.*\.test\.tld
steht für alle E-Mail Adressen aus der Domäne test.tld und deren Sub-Domänen, also auch ch.test.tld, de.test.tld local.test.tld und so weiter.

(@.*)(\waste\.tld\$)

In diesem komplexeren Beispiel wird jede E-Mail Adresse gefunden, welche auf **.waste.tld** endet. Das **\$** Zeichen am Ende des Ausdrucks bedeutet, dass in der untersuchten E-Mail Adresse nach **.waste.tld** keine weiteren Zeichen folgen dürfen. Der komplette Teil der E-Mail Adresse, welcher sich vor der Endung **.waste.tld** befindet, wird durch den Ausdruck **@.*** definiert.

Durch den Einschluss in Klammern werden die einzelnen Ausdrücke abgegrenzt. Somit können die eingeklammerten Teile durch Variablen abgerufen werden. Im Beispiel könnte somit als alles was in **(@.*)** steht, mit der Variable **\$1** wieder abgerufen werden.

Im konkreten Beispiel würde durch Verwenden von **\$1** von allen E-Mail Adressen, welche auf **.waste.tld** enden, eben dieses abgeschnitten.

Somit würde stünde dann in Variable **\$1** beispielsweise bei der ursprünglich eingelesenen Adresse „test@customer.tld.waste.tld“ „**test@customer.tld**“.

\[confidential\]\<crypt>

reagiert sowohl auf den Ausdruck [confidential] als auch <crypt> (ODER-Verknüpfung). Damit wird zum Beispiel das Verwenden mehrerer Schlüsselwörter für das Verschlüsseln ermöglicht.

(?i)max\.mustermann

durch (?i) wird im Ausdruck max\.mustermann nicht zwischen Groß- und Kleinschreibung unterschieden.

8.1.6 X-Header

Die SEPPmail Appliance verwendet beim Verarbeiten von E-Mails stellenweise intern X-Header.

Die X-Header für das Steuern der Appliance, welche in der Regel vom **SEPPmail Microsoft Outlook Add-In** ^[190] gesetzt werden, sind der Tabelle des Kapitels „Steuern der Appliance / **Betreffzeilen Schlüsselwörter** ^[164] / **X-Header**“ zu entnehmen. Die dort aufgeführten X-Header werden zu Beginn des Verarbeitens zunächst in das jeweilige Betreffzeilen Schlüsselwort ^[164] umgesetzt. Im weiteren Verlauf des Rulesets wird also ausschließlich mit den entsprechenden Schlüsselwörtern gearbeitet.

Die Bedeutung der X-Header wird in folgender Tabelle aufgezeigt:

X-Header / Wert	Bedeutung
X-SM-incoming	Bezeichnet eine E-Mail, welche an eine Managed domain ^[247] gesendet wurde.
X-SM-internal	Bezeichnet eine E-Mail, welche von einer Managed domain ^[247] an eine Managed domain ^[247] gesendet wurde.
X-SM-outgoing	Bezeichnet eine E-Mail, welche von einer Managed domain ^[247] in das Internet gesendet wurde.
X-SM-encrypted	Bezeichnet eine E-Mail, welche verschlüsselt wurde.
X-SM-decrypted	Bezeichnet eine E-Mail, welche entschlüsselt wurde.
X-ESWmail-Plain / yes	Bezeichnet eine über die GINA-Oberfläche erzeugte E-Mail, welche direkt - also ohne weitere Verschlüsselung - an den internen Empfänger ausgeliefert werden soll.
X-ESWmail-Reply / yes	Bezeichnet eine GINA-Antwort-Mail.
X-ESWmail-Copy / yes <i>(neu in 12.0.5)</i>	Bezeichnet eine GINA-Antwort-Mail Kopie (siehe auch Send copy to myself ^[432]).
X-ESWmail-Noreply / yes	Ist dieser X-Header gesetzt und kommt GINA-Verschlüsselung zum Einsatz, so kann vom Empfänger der GINA-Mail auf diese - unabhängig von den Einstellungen der jeweiligen GINA Domains ^[416] (siehe Domains ^[416] GINA name ^[416]) - nicht geantwortet werden.
X-ESWmail-LFM / yes	Bezeichnet eine LFM ^[107] -Mail.
X-ESWmail-InternalEncrypt / yes	Bezeichnet eine - per GINA-Technologie - intern verschlüsselte E-Mail.
X-SM-ORIGTO	siehe SEPPmail IIME 1.0 ^[119]
X-SM-ORIGCC	
X-SM-ORIGBCC	
X-SM-smarthost	Im X-Header kann ein vom Standard abweichender Smarthost (siehe Outgoing server ^[250] , beziehungsweise Smarthost ^[247]) für das Weiterleiten der E-Mail angegeben werden.
x-smplain / yes	siehe Betreffzeilen Schlüsselwörter ^[164] / X-Header
x-smenc / yes	
x-smnoenc / yes	
x-smwebmail / yes	
x-smsign / yes	
x-smnosign / yes	
x-smdomainsign / yes	Anfordern der S/MIME Domänensignierung (nicht mehr unterstützt)

X-Header / Wert	Bedeutung
x-smemptypw / yes	Unterdrückt die Notwendigkeit der Eingabe eines Initialpasswortes bei initialen GINA-Mails (sicherheitstechnisch bedenklich).
x-smlfm / yes	Erzwingt das Verwenden der  -Technologie, unabhängig vom eingestellten Schwellwert.
x-smnolfm / yes	Unterdrückt das Verwenden der  -Technologie selbst dann, wenn der eingestellte Größen-Schwellwert überschritten wird.

Tabelle 1

8.2 Allgemeine Befehle

8.2.1 incoming()

Der Befehl `incoming()` bestimmt das Auslieferungsziel (intern/extern) einer E-Mail.

Dieser Befehl prüft, ob eine E-Mail lokal ausgeliefert wird. Sind nicht alle Empfänger der E-Mail ausschließlich lokal oder ausschließlich extern, so werden zwei Gruppen gebildet.

Als „lokal“ werden Empfänger bezeichnet, welche einer **Managed domains** ^[247] (siehe **Mail System** ^[247] **Managed domains** ^[247]) zugehörig sind.

Aufbau des Befehls

```
incoming();
```

Rückgabewert

positiv für die Gruppe der lokalen Empfänger
negativ für die Gruppe der externen Empfänger



Hinweis:

Als lokale Empfänger werden diejenigen bezeichnet, deren E-Mail Domänen auf der Appliance als **Managed domains** ^[247] definiert sind.
 Alle anderen Empfänger werden als extern bezeichnet.

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (incoming()) {</code>
02	<code># Ruleset-Anweisungen für alle E-Mails die lokal zugestellt werden können</code>
03	<code># Anweisungsblock 1 - Rückgabewert: positiv</code>
04	<code>} else {</code>
05	<code># Ruleset-Anweisungen für alle E-Mails die extern zugestellt werden müssen</code>
06	<code>#Anweisungsblock 2 - Rückgabewert: negativ</code>
07	<code>}</code>

Erklärung

In diesem Beispiel wird für eine eingehende E-Mail der **Anweisungsblock 1 (Zeile 02, 03)** ausgeführt. Für eine ausgehende E-Mail wird der **Anweisungsblock 2 (Zeile 05, 06)** ausgeführt.

8.2.2 internal()

Der Befehl `internal()` bezieht sich auf E-Mails von **Managed domains** ^[247] an **Managed domains** ^[247].

Dieser Befehl prüft, ob eine von einer **Managed domain** ^[247] stammende E-Mail an eine **Managed domain** ^[247] adressiert ist. Sind nicht alle Empfänger der E-Mail ausschließlich aus **Managed domain** ^[247] so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
internal();
```

Rückgabewert

positiv für E-Mails eines Absenders aus einer **Managed domain** ^[247], an Empfänger in **Managed domains** ^[247].

negativ für die Gruppe Empfänger, bei der keine reine interne Kommunikation vorhanden ist, also (Sender oder Empfänger) oder (Sender und Empfänger) aus keiner **Managed domain** ^[247] stammen.

Parameter
keine

Beispiel 1

Zeile	Code
01	<code>if (internal()) {</code>
02	<code># Ruleset-Anweisungen für E-Mails welche aus einer Managed domain ^[247] stammen und an eine Managed domain ^[247] zugestellt werden sollen.</code>
03	<code># Anweisungsblock 1 - Rückgabewert: positiv</code>
04	<code>} else {</code>
05	<code># Ruleset-Anweisungen für alle E-Mails die aus keiner Managed domain ^[247] und/oder an keine Managed domain ^[247] zugestellt werden sollen.</code>
06	<code>#Anweisungsblock 2 - Rückgabewert: negativ</code>
07	<code>}</code>

Erklärung

In diesem Beispiel wird für eine, aus einer **Managed domain** ^[247] stammende E-Mail, an die Adressaten einer **Managed domain** ^[247] der Anweisungsblock 1 (Zeile 02, 03) ausgeführt. Für Adressaten einer Fremddomäne, beziehungsweise wenn der Absender aus einer Fremddomäne stammt, wird der Anweisungsblock 2 (Zeile 05, 06) ausgeführt.

8.2.3 external()

Der Befehl `external()` bezieht sich auf E-Mails, welche weder von einer **Managed domain** ^[247] kommen, noch an eine **Managed domain** ^[247] gehen.

Dieser Befehl prüft, ob sowohl der Absender, als auch die Empfänger einer E-Mail aus einer Fremddomäne, also **keiner Managed domain** ^[247], stammen. Stammt eine E-Mail von einem Absender einer Fremddomäne und ist sowohl an Empfänger einer Fremddomäne, als auch an Empfänger einer **Managed domain** ^[247] gerichtet, so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
external();
```

Rückgabewert

positiv für E-Mails eines Absenders einer Fremddomäne, an Empfänger einer Fremddomäne

negativ für E-Mails, bei welchen keine reine externe Kommunikation vorhanden ist, also Sender oder Empfänger, oder Sender und Empfänger, aus einer **Managed domain** ^[247] stammen.

Parameter
keine

Beispiel 1

Zeile	Code
01	<code>if (external()) {</code>
02	<code># Ruleset-Anweisungen für E-Mails welche aus einer Fremddomäne stammen und an keine Managed domain ^[247] zugestellt werden sollen.</code>
03	<code># Anweisungsblock 1 - Rückgabewert: positiv</code>
04	<code>} else {</code>
05	<code># Ruleset-Anweisungen für alle E-Mails die aus einer Managed domain ^[247] stammen und/oder an eine Managed domain ^[247] zugestellt werden sollen.</code>
06	<code>#Anweisungsblock 2 - Rückgabewert: negativ</code>
07	<code>}</code>

Erklärung

In diesem Beispiel wird für eine, aus einer Fremddomäne stammende E-Mail, an die Adressaten einer Fremddomäne, der Anweisungsblock 1 (Zeile 02, 03) ausgeführt. Für die Adressaten einer **Managed domain**^[247], beziehungsweise wenn die E-Mail von einem Absender einer **Managed domain**^[247] stammt, wird der Anweisungsblock 2 (Zeile 05, 06) ausgeführt.

8.2.4 getheader()

Der Befehl `getheader()` speichert Informationen aus einem Header in eine Variable.

Dieser Befehl liest den Wert eines anzugebenden Headers aus und schreibt diesen in eine anzugebende Variable.

Aufbau des Befehls

```
getheader('header', 'variable');
```

Rückgabewert

positiv wenn die Variable erfolgreich gesetzt wurde.

negativ wenn der angegebene Header nicht vorhanden ist oder die Variable nicht geschrieben werden kann.



Hinweis:

Ist der angegebene Header in der E-Mail nicht vorhanden, so wird die Variable dennoch erzeugt, bleibt jedoch leer.

Somit kann später noch geprüft werden, ob ein Wert enthalten ist oder nicht. Eine Abfrage mittels `empty($variable)` wäre also positiv, da die Variable vorhanden und leer ist.

Ebenso würde die Ausgabe im Log mittels `log(1, 'Meine $variable')` die Ausgabe „Meine “ erzeugen. Würde die Variable nicht erzeugt, so würde die Ausgabe „Meine \$variable“ lauten.

Parameter

header

Gibt den Header an, welcher ausgelesen werden soll.

variable

Gibt den Namen der Variablen an, in welche der Wert des unter **header** angegebenen Headers geschrieben werden soll.



Hinweis:

Die angegebene **variable** steht jeweils zweimal zur Verfügung. Einmal dekodiert unter **\$variable** und bei Bedarf unter **\$variable_raw** im Roh-Format, also noch mime-kodiert.

Beispiel 1

Zeile	Code
01	<code>if (getheader('x-additional-information', 'additional information') {</code>
02	<code>log(1, 'raw (mime-coded) content of header x-additional-information is \$additional information raw');</code>
03	<code>log(1, 'decoded content of header x-additional-information is \$additional information');</code>
04	<code>} else {</code>
05	<code>log(1, 'header x-additional-information doesn't exist or variable additional information could not be written');</code>
06	<code>}</code>

Erklärung

In diesem Beispiel wird versucht, den Wert des **headers** „x-additional-information“ in die **variable** „\$additional_information“ zu schreiben (**Zeile 01**). Ist der **header** „x-additional-information“ vorhanden und wurde dessen Wert erfolgreich in die **variable** „\$additional_information“ geschrieben, so wird der Wert des Headers zunächst im Roh-Format (mime-kodiert) in das Log geschrieben (**Zeile 02**) und anschließend im dekodierten Format (**Zeile 03**).

Konnte die **variable** nicht erstellt werden, so wird dies ebenfalls im Log dokumentiert (**Zeile 05**).

8.2.5 notify()

Der Befehl `notify()` sendet eine E-Mail Nachricht an einen zu definierenden Empfänger während des Verarbeitens einer anderen E-Mail.

Dieser Befehl erzeugt eine E-Mail Nachricht an einen zu definierenden Empfänger (`recipient`) unter Verwendung der Vorlage (`template`). Optional können `header` beziehungsweise `x-header` in diese Benachrichtigungs-E-Mail geschrieben werden.

Aufbau des Befehls

```
notify('recipient','template', ['header:value[;header:value]']);
```

Rückgabewert

positiv immer

Parameter

recipient

Angabe der Empfänger-E-Mail Adresse der Benachrichtigungs-E-Mail.

Mögliche Werte

- E-Mail Adresse Sendet eine Nachricht an die angegebene SMTP E-Mail Adresse
- sender Benachrichtigt den ursprünglichen Absender der E-Mail
- admin Benachrichtigt den lokalen SEPPmail Appliance Administrator
Dieser wird in **Mail System** ^[247] **SMTP settings** ^[252] unter **Postmaster address** definiert.

template

Dieser Parameter definiert die zu verwendende Vorlage für diese Benachrichtigungs-E-Mail.

Die Vorlage kann über **Mail System** ^[247] **Edit mail templates...** ^[263] erstellt und verwaltet werden.

header (optional)

Angabe des zu schreibenden Headers inklusive des zugehörigen Wertes `value`.

Mögliche Werte für header

- return-path:
- date:
- from: Standard Absender ist die **Postmaster address** (siehe **Mail System** **SMTP settings** ^[252] beziehungsweise **ADD/EDIT MANAGED DOMAIN** ^[266] **Settings** ^[266])
- sender:
- reply-to:
- to:
- cc:
- subject: Standard Betreff lautet „Notification“
- beliebiger X-Header



Hinweis:

Das Setzen mehrerer `header` beziehungsweise `x-header` ist durch trennen mittels Semicolon möglich.

Beispiel 1

Zeile	Code
01	<code>notify('sender','bounce_noenc','from: "System Admin"<admin@meinefirma.tld>;subject: Benachrichtigung; x-MyOwnHeader: Test');</code>

Erklärung

In diesem Beispiel wird eine Benachrichtigungs-E-Mail an den ursprünglichen Absender - welcher über die Variable `sender` bereit gestellt wird - generiert. Als Vorlage für die E-Mail wird die Standard-Vorlage `bounce_noenc` verwendet. Im `header` der Benachrichtigungs-E-Mail wird als Absender „System Admin“ `<admin@meinefirma.tld>` und als Betreff „Benachrichtigung“ gesetzt. Weiterhin wird ein X-Header mit der Bezeichnung „x-MyOwnHeader“ und dem Wert „Test“ geschrieben.

8.2.6 setvar()

Der Befehl `setvar()` schreibt einen beliebigen, anzugebenden Wert in eine zu definierende Variable.

Aufbau des Befehls

```
setvar('var', 'value');
```

Rückgabewert

positiv wenn die Variable korrekt angelegt wird, beziehungsweise deren Wert korrekt übernommen wurde
negativ wenn die Variable nicht angelegt werden kann (siehe Warnung unter `var`)

Parameter

var

Name der Variablen, in welcher der Wert `'value'` abgelegt werden soll. Der Name der Variable muss eindeutig sein.



Achtung:

Der Name der Variable **var** darf keinesfalls mit einer Zahl beginnen.
 Bei Nichtbeachten wird die Variable nicht gespeichert

value

Inhalt, welcher bei Abfrage der Variablen `'var'` ausgegeben werden soll.

Beispiel 1

Der Wert des Attributs „Name“ soll aus einem LDAP-Verzeichnis ausgelesen werden. Dieser soll in der Variable „name_from_ldap“ abgespeichert werden.
 Die Anweisung sieht wie folgt aus:

Zeile	Code
01	<code>if (rmatchsplit('@mandant1\.de')) {</code>
02	<code> setvar('customer', 'c1');</code>
03	<code>}</code>
04	<code>if (rmatchsplit('@mandant2\.de')) {</code>
05	<code> setvar('customer', 'c2');</code>
06	<code>}</code>

Erklärung

In diesem Beispiel wird die E-Mail auf das Vorhandensein des Ausdrucks `@mandant1.de` in den Envelope Empfängern geprüft (**Zeile 01**). Für diejenigen Empfänger, deren E-Mail Adresse den Ausdruck beinhaltet, wird die Variable `$customer` mit dem Inhalt `c1` gesetzt.

8.3 Vergleichende Befehle

8.3.1 check_sender()

Über den Befehl `check_sender()` wird geprüft, ob eine Spoofing Situation vorliegt. Das bedeutet, bei einer aus einem externen Netz (Internet) stammende E-Mail soll der Eindruck vermittelt werden, dass diese von einer internen E-Mail Domäne/Adresse (siehe [Mail System](#) ^[247] [Managed domains](#) ^[247]) stammt.



Achtung:

Das Prüfen mittels `check_sender()` wird durch einen Whitelist Eintrag (siehe [Mail System](#) ^[247] [Manual blacklisting/whitelisting](#) ^[258]) unterbunden.

Aufbau des Befehls

```
check_sender('managed_domain','valid_from','allowed_IP');
```

Rückgabewert

positiv wenn einer der aktivierten Tests fehlschlug
negativ wenn alle Tests erfolgreich durchgeführt wurden

Parameter

managed_domain

Ist dieser Parameter gesetzt ('1'), so wird geprüft, dass sowohl der im Envelope der E-Mail, wie auch im FROM-Header (als auch SENDER-Header, sofern vorhanden) eingetragene Absender aus keiner [Managed domain](#) ^[247] stammt.



Achtung:

Mit dieser Option wird sämtlicher interner E-Mail Verkehr, also von [Managed domains](#) ^[247] an [Managed domains](#) ^[247], unterbunden. Dies spielt im Normalfall keine Rolle, da interne E-Mails vom E-Mail Server direkt zugestellt werden und nicht bis zur SEPPmail Appliance gelangen. Insbesondere in MSP Umgebung werden jedoch E-Mails von den [Managed domains](#) ^[247] eines Kunden an [Managed domains](#) ^[247] anderer Kunden gesendet, sodass diese Option hier keinesfalls aktiviert werden sollte.

Mögliche Werte:

- true, yes oder 1
 - false, no oder 0
- Standardeinstellung ist 0

valid_from

Ist dieser Parameter gesetzt ('1') wird geprüft, ob im FROM- (und, falls vorhanden SENDER-) Header eine gültige E-Mail Adresse enthalten ist (siehe auch [Mail Processing](#) ^[286] [Ruleset generator](#) ^[287] [Protection Pack](#) ^[303] **Reject mails if from header does not contain a valid e-mail address** ^[306]).



Achtung:

Dies kann dazu führen, dass System-E-Mails ebenfalls abgewiesen werden, da diese häufig ohne Absender gesendet werden.

Mögliche Werte:

- true, yes oder 1
 - false, no oder 0
- Standardeinstellung ist 0

allowed_IP

Ist dieser Parameter gesetzt ('1') werden die zusätzlichen Sicherheitsangaben aus den **Settings** der jeweiligen **Managed domain** geprüft (siehe auch **Mail System** **Managed domains** **ADD/EDIT MANAGED DOMAIN** **Settings**), das heißt

Header check

Exchange Online Integration

Password and certificate authentication

Allowed sending servers for this domain (leave empty to allow all relaying networks).

Schlägt in einer Exchange Online Umgebung das Verifizieren des Absenders über **Exchange Online Integration** fehl, so werden die unter **Allowed sending servers for this domain** aufgelisteten Relay-Server als Fallback herangezogen. In diesem Fall ist davon auszugehen, dass eine entsprechende E-Mail offensichtlich nicht aus Exchange Online kommt, obwohl diese für den abschließenden Versand dorthin übergeben werden soll. Ein denkbare Szenario hierfür wären von einem Web-Server generierte E-Mails eines Kontaktformulars.

Mögliche Werte:

- true, yes oder 1
 - false, no oder 0
- Standardeinstellung ist 0



Hinweis:

Wäre im FROM-Header die E-Mail Adresse einer anderen **Managed domain** als im SENDER-Header eingetragen, so müsste die sendende IP-Adresse für beide **Managed domains** berechtigt sein.

Beispiel 1

Zeile	Code
01	<code>if (check_sender('1','1','1')) {</code>
02	<code>log(1,'E-mail seems to be spoofed. Dropping e-mail');</code>
03	<code>drop('554'. '5.7.1 Relay access denied');</code>
04	<code>}</code>

Erklärung

Dieses Beispiel prüft, dass die E-Mail von keiner unter **Managed domains** eingetragenen E-Mail Domäne stammt, gültige E-Mail Adressen in den entsprechenden Headern enthält und von einem Server stammt, welcher im **Managed domain** spezifischen Relaying (**Allowed outgoing sending servers (leave empty to allow all relaying networks)**) eingetragen ist (**Zeile 01**). Schlägt einer dieser Tests fehl, so wird der Log-Eintrag 'E-mail seems to be spoofed. Dropping e-mail' erzeugt (**Zeile 02**) und die E-Mail abgewiesen (**Zeile 03**).

8.3.2 compare()

Der Befehl `compare()` prüft Werte in Header-Feldern auf einen zu definierenden Vergleichswert.

Dieser Befehl vergleicht den Inhalt eines Headers (**header-field**) mit Hilfe eines Vergleichsoperators (**operator**) mit einem angegebenen Wert (**value**).

Aufbau des Befehls

```
compare('header-field', 'operator', 'value');
```

Rückgabewert

- positiv** bei zutreffender Bedingung
negativ bei nicht zutreffender Bedingung (siehe auch Hinweis zu **value**!)

Parameter

header-field

Gibt das Kopfzeilen-Feld an, dessen Inhalt gegen den Inhalt des Parameters `value` verglichen werden soll. Als Kopfzeilen-Felder können alle Header in einer E-Mail verwendet werden.

Mögliche Werte:

- return-path
- date
- from
- sender
- reply-to
- to
- cc
- bcc
- subject
- beliebiger X-Header



Hinweis:

Header sind laut RFC case-insensitive. Dennoch wird das zu vergleichende `'header-field'` in der eingetragenen Schreibweise ersetzt. Dies kann von Vorteil sein, wenn ein nachfolgendes System - entgegen des RFC - Groß- und/oder Kleinschreibung erwartet.

operator

Mögliche Werte:

- equal vergleicht auf Gleichheit (case sensitive)
- match prüft auf das Zutreffen eines regulären Ausdrucks (case insensitive!)
- substitute ist gleich wie `match`, entfernt aber den zutreffenden Teil von `value` aus `header-field`



Hinweis:

Codierte Felder werden vor dem Vergleich decodiert. Die Sonderzeichen Tabulator, Wagenrücklauf, Zeilenvorschub und Seitenende werden vor einem Vergleich mit dem Operator `equal` entfernt.

value

Gibt den Wert an, gegen den Vergleichen werden soll. Dieser Wert kann auch ein regulärer Ausdruck sein.

**Hinweis:**

Wird als value `' '` angegeben, so wird auch dann „true“ zurückgegeben, wenn der unter header-field angegebene Header gar nicht vorhanden ist!

Folgender Log-Eintrag wird generiert:

Compare with empty string - skip and return true

Beispiel 1

Zeile	Code
01	<code>if (compare('x-smenc', 'equal', 'yes')) {</code>
02	<code> tagsubject('[confidential]');</code>
03	<code>}</code>

Erklärung

Dieses Beispiel prüft, ob der Header `x-smenc` vorhanden ist und exakt den Wert `yes` beinhaltet (**Zeile 01**). Dies bedeutet nicht, dass der Wert `yes` lediglich vorhanden ist, sondern, dass der Wert ausschließlich `yes` beinhaltet. Ist die abgefragte Kondition gegeben, wird die E-Mail für das Verschlüsseln markiert (**Zeile 02**).

Beispiel 2

Zeile	Code
01	<code>if (compare('to', 'match', '@customer.de')) {</code>
02	<code> tagsubject('[nosign]');</code>
03	<code>}</code>

Erklärung

Dieses Beispiel prüft bei einer ausgehenden E-Mail im header `to` mit dem Operator `match` auf das Vorhandensein der Domain `@customer.de` innerhalb der Empfänger E-Mail Adresse (**Zeile 01**). Wenn die E-Mail Adresse des Empfängers die Zeichenkette `@customer.de` enthält, dann ist der Rückgabewert von `compare()` **true**. Im Betreff wird das Schlüsselwort (tag) `[nosign]` hinzugefügt (**Zeile 02**). Je nach Basiskonfiguration des Rulesets wird dadurch das Signieren der E-Mail unterdrückt.

Beispiel 3

Zeile	Code
01	<code>compare('subject', 'substitute', '(\s)*\[secure\]');</code>

Erklärung

Dieses Beispiel prüft den Betreff (Header `subject`) einer E-Mail auf das Vorhandensein der Zeichenkette `[secure]` (als regulärer Ausdruck `(\s)*\[secure\]`). Wird diese Zeichenkette innerhalb des Betreff gefunden, so wird diese entfernt.

8.3.3 compareattr()

Der Befehl `compareattr()` prüft Attribute/Systemvariablen auf einen zu definierenden Vergleichswert.

Dieser Befehl vergleicht den Inhalt einer Variablen (**attribute**) mit Hilfe eines Vergleichsoperators (**operator**) mit einem angegebenen Wert (**value**).

Aufbau des Befehls

```
compareattr('attribute','operator','value');
```

Rückgabewert

- positiv** bei zutreffender Bedingung
negativ bei nicht zutreffender Bedingung

Parameter

attribute

Mögliche Werte:

- `connect_from` gibt die IP-Adresse des Systems aus, von welcher eine E-Mail an die Appliance übergeben wurde.
- `SENDER` gibt den Envelope Sender einer E-Mail aus.



Hinweis:

Die E-Mail Adresse wird immer in spitzen Klammern <> ausgegeben. Das heißt, selbst wenn nach einem leeren Envelope Sender gesucht wird, so muss der **value** <> lauten.

- `use_lfm` erkennt das Verwenden von LFT, auch wenn keine Header/Subject Tags verwendet werden und die Schwellwerte greifen
- `unsafe_lfm` erkennt das Verwenden des LFT-Plain-Modus
- **Variablen** ⁵⁰⁶ Beim Vergleich von Variablen ist darauf zu achten, dass diese ohne dem üblicherweise vorangestellten „\$“ eingegeben werden muss.

operator

Mögliche Werte:

- `equal` vergleicht auf Gleichheit eines Ausdrucks (String)
- `match` prüft auf das Zutreffen eines regulären Ausdrucks (case insensitive!)

value

Wert gegen den verglichen werden soll.

Beispiel 1

Zeile	Code
01	<code>if (compareattr('connect from','equal','172.16.161.1')) {</code>
02	<code>log(1,'Message comes from 172.16.161.1');</code>
03	<code>}</code>

Erklärung

Dieses Beispiel prüft, ob die zu verarbeitende E-Mail von einem bestimmten E-Mail Server (mit der IP-Adresse 172.16.161.1) kommt. Dabei wird die Systemvariable `connect_from` ausgewertet (**Zeile 01**). Kommt die E-Mail von besagtem Server, so wird ein entsprechender Log-Eintrag erzeugt (**Zeile 02**).

Beispiel 2

Zeile	Code
01	<code>if (compareattr('connect from','match','172\.\16\.\161\.[1-2])) {</code>
02	<code>log(1,'Message comes from 172.16.161.1/2');</code>
03	<code>}</code>

Erklärung

Dieses Beispiel prüft, ob die zu verarbeitende E-Mail von einem der beiden E-Mail Server mit der IP-Adresse 172.16.161.1 oder 172.16.161.2 kommt. Dabei wird die Systemvariable `connect_from` ausgewertet (**Zeile 01**).

Kommt die E-Mail von besagtem Server, so wird ein entsprechender Log-Eintrag erzeugt (**Zeile 02**).

Beispiel 3

Zeile	Code
01	<code>if (compareattr('SENDER','equal','<>')) {</code>
02	<code>log(1,'Message has empty envelope sender');</code>
03	<code>}</code>

Erklärung

Dieses Beispiel prüft, ob bei der zu verarbeitenden E-Mail der Absender im Envelope leer ist. Dabei wird die Systemvariable `SENDER` ausgewertet (**Zeile 01**).

Ist der Absender im Envelope leer, so wird ein entsprechender Log-Eintrag erzeugt (**Zeile 02**).

Beispiel 4

Zeile	Code
01	<code>if (compareattr('use lfm','equal','1')) {</code>
02	<code>log(1,'Message is LFT');</code>
03	<code>if (compareattr('unsafe lfm','equal','1')) {</code>
04	<code>log(1,'LFT Plain mode is used');</code>
05	<code>} else {</code>
06	<code>log(1,'LFT Secure mode is used');</code>
07	<code>}</code>
08	<code>} else {</code>
09	<code>log(1,'No LFT message');</code>
10	<code>}</code>

Erklärung

Dieses Beispiel prüft, ob die zu verarbeitende E-Mail eine LFT Nachricht ist (**Zeile 01**). Falls nicht, wird eine entsprechende Nachricht ausgegeben (**Zeile 09**), andernfalls wird zunächst eine entsprechende Log Nachricht ausgegeben (**Zeile 02**) und weiterhin geprüft, ob der LFT Plain Modus verwendet wird (**Zeile 03**). Wenn dem so ist, wird ein entsprechender Log Eintrag erzeugt (**Zeile 04**), andernfalls wird die Log Meldung ausgegeben, dass der Secure Modus verwendet wird (**Zeile 06**).

8.3.4 comparebody()

Der Befehl `comparebody()` prüft den Nachrichtentext der E-Mail auf Vorhandensein einer Zeichenkette.

Dieser Befehl durchsucht den Nachrichtentext einer E-Mail nach dem angegebenen Wert (`value`).



Achtung:

Aufgrund der Vielzahl von Möglichkeiten bei den Content-Types und Content-Transfer-Encodings ist ein eindeutiges Erkennen im Nachrichtentext (Mail-Body) nicht immer 100%ig zu gewährleisten. Aus diesem Grund ist diese Funktion nur sehr bedingt - insbesondere als Entscheidungskriterium für das Triggern der Verschlüsselung - zu empfehlen und ist im Einzelfall immer zu prüfen.

Aufbau des Befehls

```
comparebody('value');
```

Rückgabewert

positiv sofern der Wert aus `value` wenigstens einmal im Nachrichtentext vorkommt
negativ sofern der Wert aus `value` nicht im Nachrichtentext vorkommt

Parameter

value

Der Parameter `value` definiert den Suchbegriff, nach dem innerhalb der E-Mail gesucht wird. `value` hat das Format eines regulären Ausdrucks.

Beispiel 1

Zeile	Code
01	<code>if (comparebody('(?:?:25[0-5] 2[0-4][0-9] [01]?[0-9][0-9]?\\.){3}(?:25[0-5] 2[0-4][0-9] [01]?[0-9][0-9]?')) {</code>
02	<code>log(1, 'Mail contains an IP address');</code>
03	<code>}</code>

Erklärung

In diesem Beispiel wird innerhalb des Nachrichtentextes einer E-Mail auf das Vorhandensein einer IP-Adresse geprüft (**Zeile 01**). Wird mindestens eine IP-Adresse gefunden, so wird der Log-Eintrag 'Mail contains an IP address' erzeugt (**Zeile 02**).

8.3.5 empty()

Der Befehl `empty()` prüft, ob ein übergebener Parameter leer oder 0 ist.

Dieser Befehl prüft, ob ein Übergabe-Parameter (zum Beispiel ein **Betreffzeilen Schlüsselwort** ¹⁶⁴) vorhanden ist.

Aufbau des Befehls

```
empty('value');
```

Rückgabewert

positiv sofern der übergebene Parameter leer oder 0 ist.
negativ sofern der übergebene Parameter einen Wert hat.

Parameter

value

Der Parameter `value` definiert den Übergabe-Parameter

Beispiel 1

Zeile	Code
01	# BEGIN removelfmtags
02	if (!empty('@LARGEFILETEXT@')) {
03	compare('subject', 'substitute', '@LARGEFILETEXT@');
04	}
08	# END removelfmtags

Erklärung

In diesem Beispiel wird auf das Vorhandensein des **Betreffzeilen Schlüsselwortes** ¹⁶⁴ für **Large File Transfer** **LFT** ¹⁰⁷ geprüft (**Zeile 02**). Ist das Schlüsselwort vorhanden, so wird dieses entfernt (**Zeile 03**).

8.3.6 from_managed_domain()

Der Befehl `from_managed_domain()` prüft, ob eine E-Mail von einem Absender einer **Managed domain** stammt.

Aufbau des Befehls

```
from_managed_domain();
```

Rückgabewert

- positiv** sofern die E-Mail von einem Absender einer **Managed domain** (siehe **Mail System**) **Managed domains** stammt
- negativ** falls die E-Mail von einer anderen E-Mail Domäne stammt.

Parameter

keine

Beispiel 1

Zeile	Code
01	if (from managed domain()) {
02	log(1, 'E-Mail is from managed domain');
03	}

Erklärung

Dieses Beispiel prüft, ob eine E-Mail von einer, unter **Managed domains** eingetragenen, Absender E-Mail Adresse gesendet wurde (**Zeile 01**). Ist dies der Fall, so wird der Log-Eintrag „E-Mail is from managed domain“ erzeugt (**Zeile 02**).

8.3.7 member_of()

siehe `member_of()` [\[54\]](#)

8.3.8 rmatch()

Der Befehl `rmatch()` prüft, ob ein regulärer Ausdruck auf mindestens einen Empfänger im Envelope zutrifft.

Aufbau des Befehls

```
rmatch('regexp');
```

Rückgabewert

positiv wenn der reguläre Ausdruck (`regexp`) auf mindestens einen Empfänger zutrifft
negativ wenn der reguläre Ausdruck (`regexp`) auf keinen Empfänger zutrifft

Parameter

regexp

Definiert den regulären Ausdruck der verglichen werden soll (case insensitive!).

Beispiel 1

Zeile	Code
01	<code>if (rmatch('@customer\.de')) {</code>
02	<code> notify ('sender', 'info send mail');</code>
03	<code>}</code>

Erklärung

Dieses Beispiel prüft, ob die E-Mail Adresse mindestens eines Empfängers einer E-Mail den Domain-Bestandteil '@customer.de' hat (**Zeile 01**). Ist dies der Fall, so wird eine E-Mail Benachrichtigung an den Absender dieser E-Mail gesendet (**Zeile 02**).

8.3.9 rmatchsplit()

Der Befehl `rmatchsplit()` prüft, ob ein regulärer Ausdruck auf mindestens einen Empfänger im Envelope zutrifft und teilt die E-Mail in zwei Gruppen

Über diesem Befehl wird im Envelope einer E-Mail auf das Vorhandensein eines regulären Ausdrucks (`regexp`) geprüft. Eine E-Mail wird bei Bedarf in zwei Gruppen aufgeteilt: Eine Gruppe, mit Empfängern, welche dem regulären Ausdruck entsprechen und eine weitere Gruppe dessen Empfänger den regulären Ausdruck nicht enthalten. Somit wird der Befehl `rmatchsplit()` klassisch innerhalb der `if/else` Kontrollstruktur verwendet.

Aufbau des Befehls

```
rmatchsplit('regexp');
```

Rückgabewert

- positiv** für die Gruppe, deren Empfänger den regulären Ausdruck `regexp` enthalten
negativ für die Gruppe, deren Empfänger den regulären Ausdruck `regexp` nicht enthalten

Parameter

regexp

Dieser Parameter definiert den regulären Ausdruck auf dessen Vorhandensein innerhalb der E-Mail (case insensitive!) geprüft wird.

Beispiel 1

Zeile	Code
01	<code>if (rmatchsplit('sales@customer\.de invoice')) {</code>
02	<code> # Anweisungsblock 1</code>
03	<code>} else {</code>
04	<code> # Anweisungsblock 2</code>
05	<code>}</code>

Erklärung

In diesem Beispiel wird die E-Mail auf das Vorhandensein des Ausdrucks `sales@customer.de` oder `invoice` in den Envelope Empfängern geprüft (**Zeile 01**). Für diejenigen Empfänger, deren E-Mail Adresse wenigstens einen der beiden Ausdrücke beinhaltet, wird der `# Anweisungsblock 1` (**Zeile 02**), für alle anderen Empfänger wird `# Anweisungsblock 2` (**Zeile 04**) ausgeführt.

8.4 Logging

8.4.1 log()

Der Befehl `log()` erzeugt einen Eintrag im Mail-Log.

Der Eintrag im Mail-Log zeigt einen frei definierbaren Text (`description`) sowie eine Gewichtung (`severity`) des Eintrags. Zudem wird dem Log-Eintrag in Spitzklammern die Message-ID des E-Mail Headers hinzugefügt. Die Aufgezeichneten Meldungen können im Menü **Logs** eingesehen werden.

Aufbau des Befehls

```
log(severity, 'description');
```

Rückgabewert

positiv immer

Parameter

severity

Dieser Parameter gibt die Gewichtung des Log-Eintrags an.

severity	Bedeutung
0	debug
1	info
2	notice
3	warning
4	error
5	critical
6	alert
7	emergency

description

Beschreibung wie Sie im Mail-Log aufgezeichnet werden soll.

Variable verfügbar!

Beispiel 1

Zeile	Code
01	<code>log(1, 'Hello World');</code>

Header der E-Mail:

```
Date: Fri, 05 Aug 2013 11:40:00 +0200
From: sender@vendor.de
To: recipient@customer.de
Subject: Some Topic
Content-Type: text/plain;
Message-Id: <E0D4DE42-DCB5-11D7>
```

Aufzeichnung im Log:

```
Aug 05 11:40:04 test gateway: <E0D4DE42-DCB5-11D7> Hello World
```

Erklärung

Der Text `Hello World` wird mit der Gewichtung `info` im Mail- Log aufgezeichnet.

8.4.2 logheader()

Der Befehl `logheader()` schreibt den Inhalt des genannten Headers oder X-Headers in das System-Log.

Dieser Befehl dient im Regelfall dem Debuggen beim Verarbeiten von E-Mails durch die Rule Engine. Die Aufgezeichneten Log-Meldungen können im Menü **Logs** eingesehen werden.

Aufbau des Befehls

```
logheader('header');
```

Rückgabewert

positiv immer

Parameter

header

Angabe des zu protokollierenden Headers oder X-Headers.

Mögliche Werte

- return-path
- date
- from
- sender
- reply-to
- to
- cc
- bcc
- subject
- beliebiger X-Header

Beispiel 1

Zeile	Code
01	<code>logheader('Message-ID');</code>

Header der E-Mail:

```
Date: Fri, 05 Aug 2013 11:40:00 +0200
From: sender@vendor.de
To: recipient@customer.de
Subject: Some Topic
Content-Type: text/plain;
Message-Id: <E0D4DE42-DCB5-11D7>
```

Aufzeichnung im Log:

```
Aug 05 11:40:04 Message-Id: <E0D4DE42-DCB5-11D7>
```

Erklärung

Die Zeichenkette aus dem Header „Message-ID:“ wird wie aufgezeigt im System Log aufgezeichnet.

8.4.3 logsubject()

Der Befehl `logsubject()` protokolliert den Inhalt der Betreffzeile einer E-Mail im System-Log. Weiterhin wird bei RTF-formatierten E-Mails die Meldung „*Message Content contains RTF-formatted MIME parts*“ ausgegeben.

Die aufgezeichneten Log-Meldungen können im Menü **Logs**  eingesehen werden.

Aufbau des Befehls

```
logsubject();
```

Rückgabewert

positiv immer

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>logsubject();</code>

Header der E-Mail:

```
Date: Fri, 05 Aug 2013 11:40:00 +0200
Message From: sender@vendor.de
Message To: recipient@customer.de
Subject: Some Topic
Content-Type: text/plain;
Message-Id: <E0D4DE42-DCB5-11D7>
```

Aufzeichnung im Log:

```
Aug 05 11:40:04 Message Subject is Some Topic
```

Erklärung

Die Zeichenkette aus dem Header „Subject:“ wird wie aufgezeigt im E-Mail Log aufgezeichnet.

8.5 Verwalten von Benutzern

8.5.1 authenticated()

Der Befehl `authenticated()` überprüft den Identifikationsstatus des Absenders.

Der Identifikationsstatus des Absenders beinhaltet die Identität und die Authentifizierung.

Für das Authentifizieren wird zunächst geprüft, ob der Sender-Header vorhanden ist und dessen Inhalt gegebenenfalls zwischengespeichert. Ist kein Sender-Header vorhanden, wird der Inhalt des Envelope-From (Envelope MAIL) stattdessen zwischengespeichert. Gehört die zwischengespeicherte Adresse einer **Managed Domain**^[247] an, so wird diese für das Authentifizieren genutzt, sofern der From-Header keine Adresse einer **Managed Domain**^[247] enthält.

Für das erfolgreiche Authentifizieren eines Absenders muss die - wie oben beschrieben ermittelte - SMTP-Adresse als „Named User“ (siehe **Users**^[396]) bereits auf der Appliance vorhanden sein.

Aufbau des Befehls

```
authenticated(['from-header']);
```

Rückgabewert

positiv sofern der Absender erfolgreich authentifiziert werden konnte
negativ bei Fehlschlagen der Authentifizierung des Absenders

Parameter

from-header (optional)

Erzwingt das Authentifizieren anhand der SMTP-Adresse des From-Headers.

Mögliche Werte

- true, yes oder 1
 - false, no oder 0
- Standardeinstellung ist 0



Hinweis:

Der für eine E-Mail Signatur benötigte Schlüssel wird immer anhand der E-Mail Adresse des authentifizierten Benutzers herangezogen.

Das heißt, sofern der Parameter `from-header` den Wert „1“ erhält, wird das Signieren mit dem Schlüssel des Absenders aus dem From-Header erzwungen.

Beispiel 1

Zeile	Code
01	<code>if (!authenticated()) {</code>
02	<code> createaccount();</code>
03	<code> log(1, 'user account generated');</code>
04	<code>}</code>

Erklärung

Das Beispiel wertet den negierten Rückgabewert des Befehls `authenticated()` aus (**Zeile 01**). Konnte der interne Absender der E-Mail erfolgreich authentifiziert werden, so ist der Rückgabewert aufgrund der Negierung **false**. Schlug das Authentifizieren fehl, so ist der Rückgabewert aufgrund der Negierung **true** und der angeführte Anweisungsblock kommt zum Tragen. Im Beispiel würde somit ein Benutzerkonto für den - wie eingehend beschrieben ermittelten Absender angelegt (**Zeile 02**) und ein entsprechender Log-Eintrag erzeugt (**Zeile 03**).

Beispiel 2

Zeile	Code
01	<code>if (!authenticated('1')) {</code>
02	<code> createaccount();</code>
03	<code> log(1, 'user account generated');</code>

Zeile	Code
04	}

Erklärung

Im Gegensatz zu **Beispiel 1** wird aufgrund des gesetzten Parameters `'from-header'` das Verwenden des Absenders aus dem FROM-Header erzwungen.

8.5.2 createaccount()

Der Befehl `createaccount()` erstellt neue Benutzerkonten.

Als Benutzerkonto wird ein lokales SEPPmail Appliance Benutzerkonto bezeichnet. Dieses Benutzerkonto kann im Menü **Users** eingesehen werden.



Achtung:

Wird `createaccount()` in **Custom macros and commands for all e-mails BEFORE processing** aufgerufen, so muss durch `incoming()` zunächst die Richtung einer E-Mail (eingehend / ausgehend) bestimmt werden, da an dieser Stelle noch keine Entscheidung über die Gültigkeit und Richtung der Mail getätigt wurde.

Empfohlen wird Macros lediglich für ein Flagging (zum Beispiel über `ldap_compare()` zu verwenden um dann in **Custom commands for outgoing e-mails BEFORE encryption** eine entsprechende Aktion auszuführen.

Aufbau des Befehls

```
createaccount([0], ['userID'], ['name']);
```

Rückgabewert

positiv immer

Parameter

keys

Dieser Parameter wurde außer Kraft gesetzt. Für das Generieren von Schlüsselmaterial ist ausschließlich der Befehl `createkeys()` zu verwenden.

Sollen weitere Parameter verwendet werden, so muss `keys` zwingend mit `null (0)` angegeben werden, sofern weitere Parameter verwendet werden sollen.

userID (optional)

Dieser Parameter gibt die eindeutige ID des Benutzers an.

Wird dieser Parameter nicht angegeben, so wird für das Generieren des Benutzers seine E-Mail Adresse als `userID` verwendet. Sonderzeichen werden automatisch ersetzt.

Variablen verfügbar!

name (optional)

Dieser Parameter gibt des Namen des Benutzers an.

Wird dieser Parameter nicht angegeben, so wird für das Generieren des Benutzers der Anzeigenname, beziehungsweise wenn dieser nicht vorhanden ist seine E-Mail Adresse als `name` verwendet. Sonderzeichen werden automatisch ersetzt.

Variablen verfügbar!

Beispiel 1

Zeile	Code
01	<code>if (!authenticated()) {</code>
03	<code>createaccount();</code>
04	<code>log(1, 'user account generated');</code>
05	<code>}</code>

Erklärung

Das Beispiel wertet den negierten Rückgabewert des Befehls `authenticated()` aus (**Zeile 01**). Konnte der interne Absender der E-Mail erfolgreich authentifiziert werden, so ist der Rückgabewert aufgrund der Negierung **false**. Schlug das Authentifizieren fehl, so ist der Rückgabewert aufgrund der Negierung **true** und der angeführte Anweisungsblock kommt zum Tragen. Im Beispiel würde somit ein Benutzerkonto für den Absender angelegt (**Zeile 02**) und ein entsprechender Log-Eintrag erzeugt (**Zeile 03**).

8.5.3 createkeys()

Der Befehl `createkeys()` erstellt neue Schlüssel für einen authentisierten Benutzer.

Dieser Befehl stellt sicher, dass für einen authentisierten Benutzer das gewünschte Schlüsselmaterial zur Verfügung steht. Das heißt, sofern der entsprechende Benutzer kein, nur abgelaufenes oder revoziertes Schlüsselmaterial zur Verfügung hat, würde neues Schlüsselmaterial gemäß Einstellung (siehe Parameter **keys**) generiert. Dies entspricht den Einstellungen, wie Sie im [Ruleset generator](#)^[287] unter **Key generation**^[291] vorgenommen werden können.

Aufbau des Befehls

```
createkeys('keys', ['continue']);
```

Rückgabewert

positiv immer

Parameter

keys (optional)

Dieser Parameter gibt an, welches Schlüsselmaterial generiert werden soll. Das Format entspricht einer Bitmaske in Oktalnotation.

Die folgenden Werte stehen zur Verfügung:

- Bit 0 : OpenPGP-Schlüsselpaar generieren
- Bit 1 : S/MIME-Zertifikat mit der eigenen Zertifizierungsstelle generieren
- Bit 2 : S/MIME-Zertifikat via CA-Connector generieren

	Mask				
Bit 0: OpenPGP	x		x		x
Bit 1: S/MIME mit eigener CA		x	x		
Bit 2: S/MIME via CA-Connector				x	x
Wert für keys	1	2	3	4	5

continue (optional)

Über diesen Parameter wird entschieden, ob eine E-Mail während des Generierens des Schlüsselmaterials temporär mit (420 An encryption key for your account will be available shortly) abgelehnt (false) oder in der Warteschlange der SEPPmail Appliance gehalten wird.

Mögliche Werte

- true, yes oder 1
 - false, no oder 0
- Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	<code>if (authenticated()) {</code>
02	<code> createkeys('3');</code>
03	<code> log(1, 'OpenPGP Key generated');</code>
04	<code>}</code>

Erklärung

Das Beispiel wertet den Rückgabewert des Befehls `authenticated()` aus (**Zeile 01**). Konnte der interne Absender der E-Mail erfolgreich authentifiziert werden, so ist der Rückgabewert **true**. Somit wird mit `createkeys()` (**Zeile 02**), fortgefahren und ein OpenPGP Schlüsselpaar erzeugt, sofern nicht bereits gültiges vorhanden ist (**Zeile 02**). Weiterhin wird ein Log-Eintrag erzeugt (**Zeile 03**).

8.5.4 member_of()

Der Befehl `member_of()` prüft die Zugehörigkeit eines Absenders zu einer Gruppe.

Als Gruppe wird eine lokale SEPPmail Appliance Gruppe bezeichnet. Diese Gruppen werden im Menü **Groups** ⁴¹³ verwaltet.

Aufbau des Befehls

```
member_of('group');
```

Rückgabewert

positiv wenn der Absender der angegebenen Gruppe zugeordnet ist
negativ wenn der Absender nicht der angegebenen Gruppe zugeordnet ist

Parameter

group

Definiert den Namen der Gruppe auf dessen Mitgliedschaft die E-Mail Adresse des Absenders geprüft werden soll.

Beispiel 1

Zeile	Code
01	<code>if (member_of('support')) {</code>
02	<code>setheader('x-smenc', 'yes');</code>
03	<code>}</code>

Erklärung

In diesem Beispiel wird geprüft, ob der Absender Mitglied der Gruppe „support“ ist (**Zeile 01**). Falls ja, dann wird als Rückgabewert true geliefert, und der Befehl `setheader()` wird ausgeführt (**Zeile 02**). Andernfalls wird als Rückgabewert false geliefert.

8.5.5 setuserattr()

Der Befehl `setuserattr()` fügt einem Benutzerkonto Attribute hinzu oder ändert diese.

Das Benutzerkonto kann im Menü **Users** eingesehen werden.

Aufbau des Befehls

```
setuserattr('attr','value');
```

Rückgabewert

positiv immer

Parameter

ATTR und VALUE

Folgende Systemattribute (**attr**) stehen mit den jeweiligen Werten (**value**) gemäß folgender Tabelle zur Verfügung:

ATTR	VALUE																				
accountOptions	Bit 0: User darf nicht verschlüsseln Bit 1: nicht belegt Bit 2: User darf nicht signieren <table><tr><th></th><th colspan="3">Mask</th></tr><tr><td>Bit 0: User darf nicht verschlüsseln</td><td>x</td><td></td><td>x</td></tr><tr><td>Bit 1: nicht belegt</td><td>-</td><td>-</td><td>-</td></tr><tr><td>Bit 2: User darf nicht signieren</td><td></td><td>x</td><td>x</td></tr><tr><td>Wert für value</td><td>1</td><td>4</td><td>5</td></tr></table> Standardwert ist '0' (darf alles)		Mask			Bit 0: User darf nicht verschlüsseln	x		x	Bit 1: nicht belegt	-	-	-	Bit 2: User darf nicht signieren		x	x	Wert für value	1	4	5
	Mask																				
Bit 0: User darf nicht verschlüsseln	x		x																		
Bit 1: nicht belegt	-	-	-																		
Bit 2: User darf nicht signieren		x	x																		
Wert für value	1	4	5																		
mpkiSubjectPart	Benutzerspezifischer Subject Part (siehe USER 'USER@DOMAIN.TLD' User data MPKI subject part)																				
SN	Name des Benutzers (siehe USER 'USER@DOMAIN.TLD' User data Full name Variablen verfügbar!																				
UID	User ID des Benutzers (siehe USER 'USER@DOMAIN.TLD' User data User ID Variablen verfügbar!																				



Hinweis:

- Alle Attribute können von InetOrgPerson benutzt werden.
- Die Attribute können in der Administrationsoberfläche angezeigt werden.

Das Alleinstellungsmerkmal eines SEPPmail Appliance Benutzerkontos ist die E-Mail Adresse, weshalb diese auch nicht geändert werden kann.

Beispiel 1

Zeile	Code
01	if(ldap_compare('192.168.10.10,192.168.10.11;CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local;mypassword;OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local;(mail=\$sender)','memberOf','SecureMail')) {
02	if(authenticated()) {
03	setuserattr('accountOptions','0');
04	}

Zeile	Code
05	}

Erklärung

In diesem Beispiel wird geprüft, ob der Absender Mitglied der Gruppe „support“ ist (**Zeile 01**). Falls ja, wird mittels `(authenticated())` geprüft, ob der Absender bereits als Benutzer in der Appliance definiert ist (**Zeile 02**).

Treffen beide Bedingungen zu, so wird diesem Benutzer über den Befehl `setuserattr()` das Recht für „Verschlüsseln und Signieren“ zugewiesen (**Zeile 03**).

Beispiel 2

Zeile	Code
01	<code>ldap_read('172.16.161.5;CN=ldapquery,OU=ServiceAccounts,OU=BenutzerDC=mandant1,DC=local;Kennwort;OU=Benutzer,DC=mandant1,DC=local;(mail=\$from)','StaticSubjectPart','StaticSubjectPart');</code>
02	<code>ldap_read('172.16.161.5;CN=ldapquery,OU=ServiceAccounts,OU=Benutzer,DC=mandant1,DC=local;Kennwort;OU=Benutzer,DC=mandant1,DC=local;(mail=\$from)','displayName','displayName');</code>
03	<code>ldap_read('172.16.161.5;CN=ldapquery,OU=ServiceAccounts,OU=Benutzer,DC=mandant1,DC=local;Kennwort;OU=Benutzer,DC=mandant1,DC=local;(mail=\$from)','sAMAccountName','sAMAccountName');</code>
04	<code>setuserattr('UID','\$sAMAccountName');</code>
05	<code>setuserattr('SN','\$displayName');</code>
06	<code>setuserattr('mpkiSubjectPart','\$StaticSubjectPart');</code>

Erklärung

In diesem Beispiel werden in **Zeile 01 - 03** die Werte für „Static Subject Part“, „Anzeigenname“ und „UserID“ aus einem LDAP ausgelesen und jeweils in gleichnamige Variablen geschrieben. In **Zeile 04 - 06** werden diese Werte für den SEPPmail User übernommen.

8.6 Handhaben von Nachrichten

8.6.1 archive()

Der Befehl `archive()` kopiert die E-Mail und stellt sie einen zusätzlichen Empfänger zu.

Die E-Mail wird innerhalb der Verarbeitung kopiert und in einem neuen Envelope der zusätzlich angegebenen E-Mail Adresse (`e-mail-address`) zugestellt (vergleiche [Mail Processing](#) ^[287], [Ruleset generator](#) ^[287], [Archiving](#) ^[308]).



Hinweis:

Diese Aktion wird nicht in Verbindung mit den Befehlen `bounce()` ^[548] oder `drop()` ^[552] ausgeführt

Aufbau des Befehls

```
archive('e-mail_address');
```

Rückgabewert

positiv immer

Parameter

e-mail_address (optional)

E-Mail Adresse des zusätzlichen Empfängers.

Beispiel 1

Zeile	Code
01	<code>archive('archive@customer.de');</code>

Erklärung

In diesem Beispiel wird die gerade verarbeitete E-Mail als Kopie zusätzlich an den Empfänger „archive@customer.“ gesendet.

8.6.2 autoreply()

Der Befehl `autoreply()` generiert eine neue E-Mail an den ursprünglichen Absender unter Verwendung einer angegebenen E-Mail Vorlage.

Dieser Befehl erzeugt automatisch eine E-Mail Antwort an den ursprünglichen Absender unter Verwendung der Vorlage (`template`).

Absender der automatisierten Antwort ist der ursprüngliche Empfänger, Betreff ist der ursprüngliche Betreff mit dem vorangestellten Kennzeichen einer Antwort, also „AW:“, „Re:“ und so weiter.

Enthält die E-Mail des ursprünglichen Absenders mehrere Empfänger, so wird pro Empfänger eine Rück-E-Mail generiert.



Achtung:

Dieser Befehl ist in erster Linie für Tests von externen Kommunikationspartnern gedacht und ersetzt in keinem Fall etwa die Autoreply-Funktion eines E-Mail Clients wie MS-Outlook.

Aufbau des Befehls

```
autoreply('template', ['header:value[;header:value]']);
```

Rückgabewert

positiv für die neu generierte Antwort-Mail

Parameter

template

Dieser Parameter definiert die zu verwendende Vorlage für die automatisierte E-Mail Antwort.

Die Vorlage kann über **Mail System** ²⁴⁷ **Edit mail templates...** ²⁶³ erstellt und verwaltet werden.

header (optional)

Angabe des zu schreibenden `Headers` inklusive des zugehörigen Wertes `value`.

Mögliche Werte für header

- return-path:
- date:
- from: Standard Absender ist die ursprüngliche Empfängeradresse
- sender:
- reply-to:
- to:
- cc:
- subject: ursprünglicher Betreff mit dem vorangestellten Kennzeichen einer Antwort, also „AW:“, „Re:“ und so weiter.
- beliebiger X-Header



Hinweis:

Das Setzen mehrerer `header` beziehungsweise `x-header` ist durch trennen mittels Semicolon möglich.

Beispiel 1

Zeile	Code
01	<code>log(1,'Start custom commands for incoming e-mails BEFORE decryption');</code>
02	<code>if (compare('subject','match','\[get\scertificate\])) {</code>
03	<code>log(1,'certificate requested by subject');</code>
04	<code>if (autoreply('send certificate')) {</code>
05	<code>if (authenticated(1)) {</code>

Zeile	Code
06	if (sign smime()) {
07	log(1,'sent certificate for \$to to \$from');
08	} else {
09	log(1,'signing not possible for \$to, no key found');
10	}
11	} else {
12	log(1,'signing not possible for \$to, no user found');
13	}
14	}
15	deliver();
16	}

Erklärung

Zunächst muss das **e-mail template** ²⁶³ „send_certificate“ definiert werden.

Beim Empfang einer E-Mail wird zunächst geprüft, ob über einen vordefinierten Betreff (dieser muss laut Beispiel [get certificate] lauten) eine signierte Rück-Mail für das Erlangen des öffentlichen Schlüssels des Empfängers angefordert wurde (**Zeile 02**). Ist dies der Fall, so wird für von jedem der Empfänger eine automatisierte Rück-Mail an den ursprünglichen Absender unter Verwendung des **e-mail templates** ²⁶³ „send_certificate“ generiert (**Zeile 05**). Anschließend wird für jeden ursprünglichen Empfänger geprüft, ob für ihn ein Benutzer auf der SEPPmail Appliance angelegt ist (**Zeile 06**). Ist dies der Fall, so wird im Anschluss versucht, die jeweilige Rück-Mail zu signieren (**Zeile 07**). und abschließend versendet (**Zeile 15**).

Über diese Funktion kann ein externer Kommunikationspartner per E-Mail an den öffentlichen S/MIME Schlüssel eines lokal vorhandenen Benutzers kommen.

Beispiel 2

Zeile	Code
01	log(1,'Start custom commands for incoming e-mails BEFORE decryption');
02	if (compare('to','match','auto-reply@company.tld')) {
03	log(1,'Recipient is auto-reply@company.tld, create reply');
04	if (autoreply('test autoreply')) {
05	if (domain smime keys avail()) {
06	log(1,'found S/MIME domain certificate for recipient(s) \$to - trying to encrypt mail');
07	compare('subject','substitute','(\s)*\[secure\]');
08	compare('subject','substitute','\[empty\]');
09	compare('subject','substitute','(?i)<im>.*<c> (\[confidential\])');
10	if (encrypt domain smime('aes256')) {
11	log(1,'smime domain encryption successful');
12	} else {
13	log(1,'smime domain encryption FAILED - Mail will be bounced');
14	bounce('bounce noenc');
15	}
16	}
17	deliver();
18	}
19	}

Erklärung

Zunächst muss das **e-mail template** ²⁶³ definiert werden.

Beim Empfang einer E-Mail an den Empfänger „autoreply@company.tld“ (**Zeile 02**) wird eine automatisierte Rück-Mail unter Verwendung des **e-mail templates** ²⁶³ SEPPmail „test autoreply“ generiert (**Zeile 04**). Im nächsten Schritt wird geprüft, ob für die Domäne des Empfängers der Rück-Mail - also dem ursprünglichen Absender der E-Mail - ein Domänenzertifikat vorliegt (**Zeile 05**). Um zu vermeiden, dass eventuell bereits in der ursprünglichen E-Mail vorhandene Betreff Kennzeichen in der Rück-Mail auftauchen, werden diese entfernt (**Zeile 07-09**). Nun wird

die Rück-Mail Domänenverschlüsselt (**Zeile 10**). Schlägt dies fehl, so wird die Rück-Mail abgewiesen (**Zeile 14**).
Andernfalls wird sie ausgeliefert (**Zeile 17**).

Über diese Funktion kann die Domänenverschlüsselung³¹ von externen Kommunikationspartnern zu Ihrer eigenen Domäne getestet werden.

8.6.3 bounce()

Der Befehl `bounce()` erstellt eine Nichtzustellbarkeits-Nachricht an den Absender der E-Mail.

Dieser Befehl erzeugt eine Bounce-E-Mail (wird auch Non Delivery Notification (NDN) oder Non-Delivery Report/Receipt (NDR) bezeichnet) und löscht die ursprüngliche E-Mail. Das Aussehen der Bounce-E-Mail wird durch eine Vorlage definiert. Der Absender dieser Bounce-E-Mail ist der Postmaster (siehe [Mail System](#) [252] [SMTP settings](#) [252]

Postmaster address [253]). Optional wird der Header der ursprünglichen E-Mail der Bounce-E-Mail als Dateianlage angehängt.



Hinweis:

- Die E-Mail wird zunächst vom E-Mail System angenommen und erst mit dem Erstellen der Bounce-E-Mail verworfen (siehe Unterschied zu [drop\(\)](#) [552])
- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt [Kontrollstrukturen - if/else Anweisungen](#) [507]).

Aufbau des Befehls

```
bounce('template', ['attach_header']);
```

Rückgabewert

kein

Parameter

template

Definiert die zu verwendende Vorlage.

Vorlagen werden über die Administrationsoberfläche (siehe [Mail System](#) [247] [Edit mail templates...](#) [263]) definiert und verwaltet.

attach_header

Dieser Parameter gibt an, ob der Header der ursprünglichen E-Mail der Bounce-E-Mail als Dateianlage angehängt werden soll (`true`) oder nicht (`false`).

Mögliche Werte

- true, yes oder 1
 - false, no oder 0
- Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	<code>bounce('bounce', 'yes');</code>

Erklärung

Die Auslieferung der E-Mail soll verhindert werden. Zugleich sollen dem Absender über eine Rück-(Bounce-)E-Mail Informationen bereit gestellt werden. Der Inhalt dieser Rück-E-Mail ist in der Vorlage `bounce` definiert. Weiterhin wird der Header der nicht ausgelieferten E-Mail als Anlage angehängt (Wert `yes` des Parameters `attach_header`).

8.6.4 deliver()

Der Befehl `deliver()` ermöglicht es, eine E-Mail unmittelbar auszuliefern.



Hinweis:

- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt [Kontrollstrukturen - if/else Anweisungen](#) ^[507]).

Aufbau des Befehls

```
deliver(['mailserver[:port]' | 'loop' | 'queueless']);
```

Rückgabewert

positiv immer

Parameter

Wird kein Parameter angegeben, so wird die E-Mail dem lokalen Mail-Transport-Agent (MTA) übergeben.

mailserver (optional)

Gibt den E-Mail Server an, über welchen die E-Mail ausgeliefert werden soll.

Wird kein Parameter angegeben, so wird die E-Mail dem lokalen Mail-Transport-Agent (MTA) übergeben.

:port (optional)

Gibt den Port an, auf welchem der angegebene E-Mail Server E-Mails empfängt.

Standard ist Port 25 SMTP

loop (optional)

Die E-Mail wird an den E-Mail Server zurückgegeben, von welchem sie angenommen wurde.

queueless (optional)

Diese Einstellung bewirkt, dass E-Mails an einzelne Empfänger während der Verarbeitung nicht zwischengelagert werden. Stattdessen wird die eingehende Verbindung erst quittiert, wenn die abgehende Verbindung quittiert wurde. Wenn beim Versand an mehrere Empfänger die Annahme für einige Empfänger nicht quittiert wird, befinden sich diese E-Mails kurzzeitig bis zum Quittieren durch die empfangenden E-Mail Server auf der Appliance.



Hinweis:

Die Parameter

- `mailserver[:port]`
- `loop`
- `queueless`

schließen sich gegenseitig aus.

Beispiel 1

Zeile	Code
01	<code>deliver('relay.customer.de:587');</code>

Erklärung

In diesem Beispiel wird die E-Mail an den angegebenen E-Mail Server mit dem Ziel Port TCP/587 gesendet.

Beispiel 2

Zeile	Code
01	<code>deliver();</code>

Erklärung

In diesem Beispiel wird die E-Mail direkt über den eigenen lokalen E-Mail Transport Agent (MTA) ausgeliefert.

8.6.5 disclaimer()

Der Befehl `disclaimer()` fügt einer E-Mail eine Fußnote einer bestehenden E-Mail hinzu.

Dieser Befehl fügt einer E-Mail einen vordefinierten Text- beziehungsweise HTML-Baustein (**template**) hinzu. Wird keine Vorlage angegeben, so wird versucht, anhand der Einstellungen der **Managed domains** den richtigen Baustein zu wählen. Dazu werden die den jeweiligen E-Mail Domänen zugeordneten Disclaimer ausgewertet.

Aufbau des Befehls

```
disclaimer(['template'], ['position'], ['force']);
```

Dieser Befehl fügt einen Textanhang aus dem angeführten **template** einer bestehenden E-Mail hinzu. Wenn eine leere Zeichenfolge als **template** angegeben ist, wird versucht, anhand der Einstellungen der **Managed domains** den richtigen Baustein zu wählen. Dazu werden die den jeweiligen E-Mail Domänen zugeordneten **Disclaimer** ausgewertet.

Rückgabewert

positiv wenn der Disclaimer erfolgreich angehängt wurde

negativ wenn kein **template** gefunden/zugeordnet (beispielsweise wegen einer nicht definierten Variable) oder der Disclaimer nicht angehängt werden kann.

Parameter

template (optional)

Definiert den Namen der Vorlage (**template**), welche als Textanhang verwendet werden soll. Fußnoten- (Disclaimer-)Vorlagen werden über die Administrationsoberfläche (siehe **Mail System**) konfiguriert und verwaltet.

Wird keine Vorlage angegeben, so wird das Standard disclaimer template der jeweiligen **Managed domain** verwendet.

Variablen verfügbar!

position (optional)

Mögliche Werte

- top oberhalb des E-Mail Body
- bottom unterhalb des E-Mail Body

Standardeinstellung ist **bottom**

Das Positionieren eines Disclaimers kann alternativ auch manuell in einer E-Mail selbst erfolgen.

Hierzu ist einer E-Mail an der Stelle, an welcher der Disclaimer positioniert werden soll, eine Zeile mit dem Text

##MAILDISCLAIMER##

hinzuzufügen.

(erweitert in 12.0)

Durch Angabe von

##MAILDISCLAIMER_<disclaimer>##

(wobei **<disclaimer>** dem gewünschten Disclaimer aus **LIST DISCLAIMER** entspricht), kann nicht nur die Position, sondern auch explizit der zu verwendende Disclaimer ausgewählt werden.

force (optional)

Ist der Parameter gesetzt ('1'), wird das Hinzufügen eines Textanhangs an eine ausgehende E-Mail erzwungen. Das heißt der Textanhang wird auch an Antwort-E-Mails angehängt.

Mögliche Werte

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Beispiel 1

Zelle	Code
01	<code>disclaimer('','bottom','yes');</code>

Erklärung

In diesem Beispiel wird der Standard Textanhang anhand der Einstellungen innerhalb der **Managed domains** ausgewählt und am Ende jeder versendeten E-Mail angehängt. Dabei ist unerheblich, ob es sich um eine Antwort-E-Mail handelt oder nicht.

Beispiel 2

Zeile	Code
01	<code>encrypt webmail();</code>
02	<code>disclaimer('GINAdisclaimer','bottom');</code>
03	<code>deliver();</code>

Erklärung

Die Disclaimer Funktion kann über die **Custom commands** auch innerhalb der GINA-Träger-E-Mails verwendet werden.

Im vorliegenden Beispiel wurde hierfür zunächst ein eigenes **Disclaimer template** mit dem Namen „GINAdisclaimer“ angelegt.

In **Zeile 01** wird die GINA-Verschlüsselung ausgeführt. Im direkten Anschluss (**Zeile 02**) muss nun das Anhängen des Disclaimers für die GINA-Träger-E-Mail erfolgen. Dabei wird das zuvor erstellte **Disclaimer template** mit dem Namen „GINAdisclaimer“ verwendet. Aufgrund des Parameters `'bottom'` wird dieser Disclaimer jeweils an das Ende des Hinweistextes jeder ausgewählten Sprache der GINA-Träger-E-Mail angehängen. Danach wird die GINA-Mail versendet (**Zeile 03**).

8.6.6 drop()

Der Befehl `drop()` verweigert das Annehmen einer E-Mail und gibt an das absendende System den angegebenen SMTP-Code mit einem frei definierbarem Informationstext zurück.



Hinweis:

- Die eingehende E-Mail wird nicht angenommen (siehe Unterschied zu `bounce()` ⁵⁴⁸).
- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt [Kontrollstrukturen - if/else Anweisungen](#) ⁵⁰⁷).

Aufbau des Befehls

```
drop(['smtp_code'], ['text']);
```

Rückgabewert

positiv immer

Parameter

smtp_code (optional)

Der `smtp_code` gibt den Grund für das Zurückweisen einer E-Mail an.
Die Bedeutung der Codes gliedert sich wie folgt:

1XX	Mailserver hat die Anforderung akzeptiert, ist aber selbst noch nicht tätig geworden. Eine Bestätigungsmeldung ist erforderlich.
2XX	Mailserver hat die Anforderung erfolgreich ohne Fehler ausgeführt.
3XX	Mailserver hat die Anforderung verstanden, benötigt aber zur Verarbeitung weitere Informationen.
4XX	Mailserver hat einen temporären Fehler festgestellt. Wenn die Anforderung ohne jegliche Änderung wiederholt wird, kann die Verarbeitung möglicherweise abgeschlossen werden.
5XX	Mailserver hat einen fatalen Fehler festgestellt. Die Anforderung kann nicht verarbeitet werden.

Quelle: Wikipedia

Detaillierte Auflistungen der Fehlercodes sind zum Beispiel unter www.supermailer.de/smtp_reply_codes.htm zu finden.

Default: Wird dieser Parameter nicht angegeben, so wird der Code „555“ verwendet.

text (optional)

Der Informationstext spezifiziert den Grund des Abweisens näher.

Default: Wird dieser Parameter nicht angegeben, so wird der Text „mail NOT accepted“ ausgegeben.

Beispiel 1

Zeile	Code
01	<code>drop('451', 'Die Nachricht konnte nicht entschlüsselt werden');</code>

Erklärung

In diesem Beispiel wird eine E-Mail mit dem Fehlercode „451 - Die Nachricht konnte nicht entschlüsselt werden“ abgewiesen. Im System-Log wird für diese Aktion folgender Eintrag generiert: „Message Rejected. (451 - Die Nachricht konnte nicht entschlüsselt werden)“.

8.6.7 flag()

Der Befehl `flag()` dient dem Markieren einer E-Mail ermöglicht die spätere Abfrage dieser Markierung. Damit können X-Header und Subject-Tags für das Triggern bestimmter Aktionen abgelöst werden.

Aufbau des Befehls

```
flag('name'[, 'boolean']);
```

Rückgabewert

positiv falls gesetzt
negativ falls nicht vorhanden

Parameter

name

Gibt den Namen der Markierung an. Dieser muss eindeutig sein.

boolean (optional)

Wird der Parameter nicht angegeben, so wird der Wert der Markierung für eine if-Anweisung ausgelesen

Mögliche Werte

- true, yes oder 1 Setzt die Markierung
 - false, no oder 0 Entfernt die Markierung
- Standardeinstellung ist 1

Beispiel 1

Zeile	Code
01	<code>if (!flag('webmail')) {</code>
02	<code> log(1, 'Webmail ist nicht vorhanden/aktiviert');</code>
03	<code>}</code>
04	<code>flag('webmail', 1);</code>
05	<code>if (flag('webmail')) {</code>
06	<code> log(1, 'Webmail ist aktiviert');</code>
07	<code>}</code>
08	<code>if (flag('webmail', 0)) {</code>
09	<code> log(1, 'Webmail war aktiv und wurde deaktiviert');</code>
10	<code>}</code>

Erklärung

In diesem Beispiel wird in **Zeile 01** abgefragt, ob die Markierung `webmail` noch nicht vorhanden ist. Da diese zuvor nicht gesetzt wurde, ist der Rückgabewert aufgrund der Negierung (!) positiv und **Zeile 02** wird ausgeführt. Der Text `Webmail ist nicht vorhanden/aktiviert` wird in das Log geschrieben.

In **Zeile 04** wird nun die Markierung `webmail` gesetzt. In **Zeile 05** wird die Markierung `webmail` erneut abgefragt. Der Rückgabewert ist aufgrund des Setzen des Flags in **Zeile 04** positiv, so dass der Text `Webmail ist aktiviert` aus **Zeile 06** in das Log geschrieben wird.

In **Zeile 08** wird die Markierung erneut abgefragt und gleichzeitig deaktiviert. Da der Wert zum Zeitpunkt der Abfrage noch positiv war und erst mit der Abfrage negativ wurde, wird der Text aus **Zeile 09** `Webmail wurde deaktiviert` noch in das Log geschrieben, auch wenn der Wert danach negativ ist.

Das heißt mit dem Befehl ist ein gleichzeitiges Abfragen und Setzen möglich!

8.6.8 reject()

Der Befehl `reject()` wurde durch `drop()`^[552] ersetzt und ist nicht länger gültig.

8.6.9 reprocess()

Der Befehl `reprocess()` ermöglicht es, eine oder mehrere E-Mail(s) erneut zu verarbeiten.

Alle an eine E-Mail angehängten E-Mails - oder auch OpenPGP verschlüsselten Dateien - werden erneut verarbeitet und an den Absender zurückgesendet. Dies kann dann erforderlich sein, wenn sich im Posteingang eines Benutzers noch verschlüsselte E-Mails befinden. Diese E-Mails können als Anhang einer neuen E-Mail des betroffenen Benutzers zur erneuten Verarbeitung - also zum Entschlüsseln - an die Appliance gesendet werden. Der Befehl hat keinen Rückgabewert. Dieser Befehl hat keinen Parameter.



Hinweis:

- Die ursprüngliche Message-ID wird aus den neu entschlüsselten E-Mails entfernt.
- Es wird keine Bounce E-Mail an den Absender erzeugt.
- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt [Kontrollstrukturen - if/else Anweisungen](#)^[507]).

Aufbau des Befehls

```
reprocess(attached_message_only);
```

Rückgabewert (bei aktivem Parameter `attached_message_only`)

positiv sofern in einer Nachricht eine weitere Nachricht für das „reprocessing“ gefunden wurde
negativ falls kein „reprocessing“ stattgefunden hat

Parameter

attached_message_only (optional)

Mit dem Setzen (1) des Parameters kann der Rückgabewert kann abgefragt werden.

Wurde in einer E-Mail eine Nachricht für das „reprocessing“ gefunden (Rückgabewert positiv) kann somit entschieden werden, ob die E-Mail in welcher sich die Nachricht befand verworfen werden soll. Fand kein reprocessing statt (Rückgabewert negativ) kann die E-Mail unbeeinflusst weiterverarbeitet werden (siehe Beispiel 2).

Mögliche Werte

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	<code>if (compare('to','match','reprocess@decrypt\reprocess')) {</code>
02	<code>log(1,'reprocess recipient found - re-injecting attached messages');</code>
03	<code>reprocess();</code>
04	<code>drop('220','message reprocessed');</code>
05	<code>}</code>

Erklärung

Sendet ein interner Benutzer (eine) verschlüsselte E-Mail(s) als Anhang in einer neuen, nicht verschlüsselten E-Mail an die systemspezifische E-Mail Adresse `reprocess@decrypt.reprocess` (**Zeile 01**), so werden die E-Mails aus dem Anhang erneut verarbeitet (**Zeile 03**). Somit wird versucht diese anhängenden E-Mails zu entschlüsseln. Für den Vorgang werden entsprechende Log-Einträge erzeugt. Nach dem Ausführen von `reprocess()` wird die ursprüngliche, neue E-Mail mit `drop()` gelöscht (**Zeile 04**).

Beispiel 2

Zeile	Code
01	<code>if (compare('from', 'match', '@sender.tld')) {</code>
02	<code> if (reprocess(true)) {</code>
03	<code> drop('220', 'message reprocessed');</code>
04	<code> }</code>
05	<code>}</code>

Erklärung

Zunächst wird geprüft, ob der Absender einer E-Mail aus der E-Mail Domäne @sender.tld (**Zeile 01**) stammt. Ist dies der Fall und enthält diese E-Mail eine weitere Nachricht, so wird diese verarbeitet und ein positiver Rückgabewert erzeugt (**Zeile 02**). Die E-Mail in welcher die weitere Nachricht enthalten war wird verworfen. Dem abgebenden System wird die Annahme der E-Mail (220) mit dem Kommentar `message reprocessed` signalisiert (**Zeile 03**).

8.6.10 Manipulieren von Envelope und Header

8.6.10.1 add_rcpt()

Der Befehl `add_rcpt()` fügt der E-Mail eine zusätzliche Empfänger E-Mail Adresse im Envelope hinzu.

Aufbau des Befehls

```
add_rcpt('e-Mail_address');
```

Rückgabewert

positiv immer

Parameter

e-mail_address

Dieser Parameter definiert die E-Mail Adresse welche dem Envelope als zusätzlicher Empfänger hinzugefügt werden soll.

Beispiel 1

Zeile	Code
01	<code>add_rcpt('recipient@customer.');</code>

Erklärung

In diesem Beispiel wird der Empfänger `recipient@customer.org` hinzugefügt. Beim Empfänger erscheint die E-Mail im Posteingang so, als ob diese via BCC gesendet wurde. Der ursprüngliche Empfänger wird nicht verändert.

8.6.10.2 normalize_header()

Der Befehl `normalize_header()` ersetzt alle Sonderzeichen in einem (X-)Header durch normale ASCII-Zeichen.

Dieser Befehl ersetzt alle Sonderzeichen des angegebenen Headers (`header`) durch normale ASCII-Zeichen. Sonderzeichen können zum Beispiel deutsche Umlaute wie ä, ö, ü aber auch ? sein.

Aufbau des Befehls

```
normalize_header('header');
```

Rückgabewert

positiv immer

Parameter

header

Angabe des zu bearbeitenden Headers oder X-Headers an.

Mögliche Werte

- return-path
- date
- from
- sender
- reply-to
- to
- cc
- bcc
- subject
- beliebiger X-Header

Beispiel 1

Zeile	Code
01	<code>normalize_header('subject');</code>

Erklärung

In diesem Beispiel wird im Header-Feld `subject` zum Beispiel aus der Zeichenkette „Herr Müller“ die normalisierte Form „Herr Mueller“.

Beispiel 2

Zeile	Code
01	<code>normalize_header('to');</code>

Erklärung

In diesem Beispiel wird im Header TO aus der Zeichenkette
 '<Bernd Hänsel> bernd.haensel@customer.de'
 die normalisierte Form
 '<Bernd Haensel> bernd.haensel@customer.com'.

8.6.10.3 replace_rcpt()

Der Befehl `replace_rcpt()` ersetzt in einer E-Mail den oder die Empfänger durch einen anzugebenden anderen.

Die Empfänger der zu verarbeitenden E-Mail können in Abhängigkeit der verwendeten Parameter verändert werden.

Aufbau des Befehls

```
replace_rcpt(['old_recipient',] 'new_recipient', ['only_envelope']);
```

Rückgabewert

positiv immer

Parameter

new_recipient

Neue E-Mail Adresse (als String), wenn dies der einzige gesetzte Parameter ist. Es wird nur der Envelope der E-Mail behandelt. Mehrere Empfänger können durch Semikolon getrennt eingegeben werden.

Andernfalls können auch Teile ersetzt werden. Dies impliziert jedoch das Verwenden von Regulären Ausdrücken und des Parameters **old_recipient**.

Variablen 506 verfügbar!

old_recipient (optional)

Regulärer Ausdruck der die ursprüngliche E-Mail Adresse oder Teile davon beschreibt.

only_envelope (nur bei Verwenden des Parameters **old_recipient** möglich)

Im Standard wird bei Verwenden des Parameters **old_recipient** zusätzlich zum Envelope auch der TO- sowie CC-Header der E-Mail geändert. Mit dem Setzen (1) dieses Parameters wird das Ändern des TO-Headers unterdrückt

Mögliche Werte

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	<code>replace_rcpt('support@customer.tld');</code>

Erklärung

In diesem Beispiel wird der ursprüngliche Empfänger der E-Mail im Envelope durch den Empfänger „support@customer.tld“ ersetzt.

Wäre beispielsweise der ursprünglich Empfänger der E-Mail „admin@customer.com“, so würde dieser entfernt und durch den neuen Empfänger (**new_recipient**) „support@customer.tld“ ersetzt. Somit wird die E-Mail an den neuen Empfänger „support@customer.tld“ gesendet.

Beispiel 2

Zeile	Code
01	<code>replace_rcpt('@mydomain\.com', '@customer.tld');</code>

Erklärung

In diesem Beispiel wird im Parameter **old_recipient** der Domain-Anteil der ursprünglichen E-Mail Adresse des/der Empfänger/s von '@mydomain.com' in den Wert des Parameters **new_recipient**, '@customer.tld', sowohl im Envelope, als auch gegebenenfalls in den Headern TO sowie CC geändert. Der Bestandteil der E-Mail Adresse vor dem '@' bleibt dabei unverändert. Falls mehrere E-Mail Empfängeradressen vorhanden sind, würden alle Empfängeradressen welche auf '@mydomain.com' enden '@customer.tld' geändert werden.

Beispiel 3

Zeile	Code
01	<code>replace_rcpt('(@.*)(\..waste\.tld\$)', '\$1', 1);</code>

Erklärung

In diesem komplexeren Beispiel wird jede E-Mail Adresse gefunden, welche auf **.waste.tld** endet. Das **\$** Zeichen am Ende des Ausdrucks bedeutet, dass in der untersuchten E-Mail Adresse nach **.waste.tld** keine weiteren Zeichen folgen dürfen. Der komplette Teil der E-Mail Adresse, welcher sich vor der Endung **.waste.tld** befindet wird durch den Ausdruck **@.*** definiert und durch den Einschluss in Klammern **()** abgegrenzt, um ihn als Variable **\$1** im Parameter **new_recipient** zu verwenden.

Das heißt, mit dem genannten Beispiel wird von allen E-Mail Adressen, welche auf **.waste.tld** enden, eben dieses abgeschnitten.

Somit würde beispielsweise die ursprüngliche Empfänger Adresse „test@customer.tld.waste.tld“ durch „test@customer.tld“ ersetzt. Da zusätzlich der Parameter **only_envelope** auf „1“ gesetzt wurde, würde diese Änderung ausschließlich den Envelope der E-Mail, nicht jedoch die Header betreffen.

Beispiel 4

Zeile	Code
01	<code>replace rcpt('(@mail\.)','@');</code>

Erklärung

In diesem Beispiel wird die Sub-Domäne „mail.“ aus der E-Mail Adresse entfernt.

Somit wird beispielsweise aus der ursprünglichen Empfängeradresse „support@mail.customer.tld“ (**old_recipient**) „support@customer.tld“ (**new_recipient**).

8.6.10.4 replace_sender()

Der Befehl `replace_sender()` verändert den Absender einer E-Mail.

Dieser Befehl ersetzt den ursprünglichen Absender einer E-Mail - je nach verwendeten Parametern - im Envelope beziehungsweise Header.

Aufbau des Befehls

```
replace_sender(['old_sender'], 'new_sender', ['only_envelope']);
```

Rückgabewert

positiv immer

Parameter

new_sender

Neue E-Mail Adresse (als String), wenn dies der einzige gesetzte Parameter ist. Es wird nur der Envelope der E-Mail behandelt.

Andernfalls können auch Teile ersetzt werden. Dies impliziert jedoch das Verwenden von Regulären Ausdrücken und des Parameters **old_sender**.

Variablen 500 verfügbar!

old_sender (optional)

Regulärer Ausdruck der die ursprüngliche E-Mail Adresse oder Teile davon beschreibt.

only_envelope (nur bei Verwenden des Parameters **old_sender** möglich)

Im Standard wird bei Verwenden des Parameters **old_sender** zusätzlich zum Envelope auch der FROM-, REPLY-TO- sowie SENDER-Header der E-Mail geändert. Mit dem Setzen (1) dieses Parameters wird das Ändern des FROM-Headers unterdrückt

Mögliche Werte

- true, yes oder 1
 - false, no oder 0
- Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	<code>replace_sender('support@customer.tld');</code>

Erklärung

In diesem Beispiel wird der ursprüngliche Sender der E-Mail im Envelope durch den Sender „support@customer.tld“ ersetzt.

Wäre beispielsweise der ursprüngliche Sender der E-Mail „admin@customer.com“, so würde dieser entfernt und durch den neuen Empfänger (**new_sender**) „support@customer.com“ ersetzt.

Beispiel 2

Zeile	Code
01	<code>replace_sender('@mydomain\.com', '@customer.tld');</code>

Erklärung

In diesem Beispiel wird im Parameter **old_sender** der Domain-Anteil der ursprünglichen E-Mail Adresse des Senders von '@mydomain.com' in den Wert des Parameters **new_sender** '@customer.tld', sowohl im Envelope, als auch in den Headern geändert. Der Bestandteil der E-Mail Adresse vor dem '@' bleibt dabei unverändert.

Beispiel 3

Zeile	Code
01	<code>replace_sender('(@.*) (\.waste\.tld\$)', '\$1', 1);</code>

Erklärung

In diesem komplexeren Beispiel wird der Sender einer E-Mail nur dann geändert, wenn dessen E-Mail Adresse mit **.waste.tld** endet. Das **\$** Zeichen am Ende des Ausdrucks bedeutet, dass in der untersuchten E-Mail Adresse nach **.waste.tld** keine weiteren Zeichen folgen dürfen. Der komplette Teil der E-Mail Adresse, welcher sich vor der

Endung **.waste.tld** befindet wird durch den Ausdruck **@.*** definiert und durch den Einschluss in Klammern () abgegrenzt, um ihn als Variable **\$1** im Parameter **new_recipient** zu verwenden.

Das heißt, mit dem genannten Beispiel wird von E-Mail Adressen, welche auf **.waste.tld** enden, eben dieses abgeschnitten.

Somit würde beispielsweise die ursprüngliche Absender Adresse „test@customer.tld.waste.tld“ durch „test@customer.tld“ ersetzt. Da zusätzlich der Parameter **only_envelope** auf 1 gesetzt wurde, würde diese Änderung ausschließlich den Envelope der E-Mail, nicht jedoch den FROM-Header betreffen.

8.6.10.5 rmheader()

Der Befehl `rmheader()` löscht eine Header oder X-Header Zeile innerhalb einer E-Mail.

Aufbau des Befehls

```
rmheader('header');
```

Rückgabewert

positiv immer

Parameter

header

Angabe des zu löschenden Headers oder X-Headers an.

Mögliche Werte

- return-path
- date
- from
- sender
- reply-to
- to
- cc
- bcc
- subject
- beliebiger X-Header



Hinweis:

Falls mehrere Header mit dem unter `header` angegebenen Namen existieren, werden alle zutreffenden Header gelöscht. Groß-/Kleinschreibung spielt dabei keine Rolle.

Beispiel 1

Zeile	Code
01	<code>rmheader('X-Greylist');</code>

Erklärung

In diesem Beispiel werden alle `X-Greylist` Header entfernt.

8.6.10.6 setheader()

Der Befehl `setheader()` fügt eine Header-Zeile innerhalb einer E-Mail hinzu oder verändert eine vorhandene.

Aufbau des Befehls

```
setheader('header','value');
```

Rückgabewert

positiv immer

Parameter

header

Angabe des Headers oder X-Headers der hinzugefügt oder geändert werden soll.

Mögliche Werte

- return-path
- date
- from
- sender
- reply-to
- to
- cc
- bcc
- subject
- beliebiger X-Header



Hinweis:

Falls mehrere Header mit dem unter `header` angegebenen Namen existieren, wird der jeweils erste gefundene Header angepasst.

value

Angabe des Wertes, den der Header annehmen soll.

Variablen 500 verfügbar!

Beispiel 1

Zeile	Code
01	<code>setheader('x-smenc','yes');</code>

Erklärung

In diesem Beispiel wird einer E-Mail der zusätzliche Header `x-smenc` mit dem Wert „yes“ hinzugefügt.

Beispiel 2

Zeile	Code
01	<code>setheader('from','info@customer.com');</code>

Erklärung

In diesem Beispiel wird in einer E-Mail der FROM-Header auf dem Wert „info@customer.com“ geändert.

Beispiel 3

Zeile	Code
01	<code>if (compare('subject','match','\[priv\]')) {</code>
02	<code>setheader('Disposition-Notification-To','<\$from>');</code>
03	<code>}</code>

Erklärung

In diesem Beispiel wird bei jeder E-Mail mit [priv] im Betreff der Disposition-Notification-To-Header mit der Absender-E-Mail Adresse des FROM-Headers in spitzen Klammern als Wert (entspricht der Lesebestätigungsanforderung des E-Mail Clients) gesetzt.

8.6.10.7 splitrecipients()

Der Befehl `splitrecipients()` erzeugt für jeden Empfänger einer E-Mail eine separate E-Mail.

Aufbau des Befehls

```
splitrecipients(['set_to']);
```

Rückgabewert

positiv immer

Parameter

set_to

Durch Aktivieren dieses Parameters ('1') taucht im TO-Header jeder Einzel-E-Mail nur noch der Empfänger der jeweiligen E-Mail auf.

Dies ist zum Beispiel für den Versand von Newslettern hilfreich.

Mögliche Werte

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0



Hinweis:

Die Funktion ist vor allem für den Newsletter Versand gedacht, bei welchen vor allem aus AntiSpam-Gründen jedoch einzelne Mails mit richtigem TO-Header benötigt werden.

Für Einträge aus dem CC-Header wird ebenfalls je eine separate E-Mail mit entsprechendem TO-Header generiert. Einträge im CC-Header bleiben erhalten.

8.6.10.8 tag_subject()

Der Befehl `tag_subject()` wurde durch `tagsubject` ersetzt und ist nicht länger gültig.

8.6.10.9 tagsubject()

Der Befehl `tagsubject()` fügt dem Betreff einer E-Mail den zu definierenden Text hinzu.

Aufbau des Befehls

```
tagsubject('text', ['position']);
```

Rückgabewert

positiv immer

Parameter

text

Der Parameter gibt den Text (Zeichenkette) an, der in die Betreffzeile eingefügt wird.

Variablen verfügbar!

position

Der Parameter gibt die Position des einzufügenden Textes an.

Mögliche Werte

- true, yes oder 1 zu Beginn des Betreffs
 - false, no oder 0 am Ende des Betreffs
- Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	<code>tagsubject('[priv]', 1);</code>

Erklärung

In diesem Beispiel wird an den Inhalt der Betreffzeile einer E-Mail die Zeichenkette '[priv]' am Anfang angehängt. Dadurch würde bei entsprechendem Platzieren im Ruleset (siehe **Custom commands**) bei Standard-Einstellungen und aktivierter Option „Always use GINA technology for mails with the following text in subject:“ (siehe **Mail Processing** **Ruleset generator** **Encryption / Decryption** **Outgoing e-mails**) das Verschlüsseln einer ausgehenden E-Mail über die GINA-Technologie erzwungen werden.

8.6.11 Kryptographische Behandlung

8.6.11.1 OpenPGP

8.6.11.1.1 attachpgpkey()

Der Befehl `attachpgpkey()` hängt den OpenPGP-Public-Key des Absenders (User) an eine E-Mail an.

Dieser Befehl hängt den OpenPGP-Public-Key des Absenders (interner Benutzer in der Appliance aus dem Menü **Users** ^[402]) an eine E-Mail als Dateianhang an, um diesen dem Empfänger bereit zu stellen.



Hinweis:

Das Verteilen des öffentlichen OpenPGP Schlüssels an Kommunikationspartner impliziert immer, dass die Prüfsumme (Hash) dieses Schlüssels vor dem Verwenden durch den Kommunikationspartner auf einem zweiten Kanal - zum Beispiel per Telefon - im Nachgang geprüft wird. Dies ist erforderlich, um die Integrität des Schlüssels sicherzustellen.

Aus diesem Grund wird empfohlen, das Bereitstellen von OpenPGP Schlüsseln über die GINA-Technologie zu realisieren (siehe **GINA Domains** ^[416], **Domains** ^[416], **CHANGE GINA SETTINGS FOR** ^[423], **Extended settings** ^[431], **Certificate search and management in GINA** ^[423]).

Aufbau des Befehls

```
attachpgpkey();
```

Rückgabewert

positiv immer

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (pgp secret keys avail()) {</code>
02	<code>attachpgpkey();</code>
03	<code>}</code>

Erklärung

In diesem Beispiel wird zunächst geprüft, ob der Absender über ein OpenPGP Schlüsselpaar auf der Appliance verfügt (**Zeile 01**). Ist dies der Fall, so wird der ausgehenden E-Mail der öffentliche OpenPGP Schlüssel angehängt (**Zeile 02**).

8.6.11.1.2 pgp_encrypted()

Der Befehl `pgp_encrypted()` prüft, ob eine E-Mail OpenPGP verschlüsselt ist.

Dieser Befehl prüft, ob eine E-Mail OpenPGP verschlüsselt ist. Dabei spielt die Art der Verschlüsselung (Domänen oder Benutzer basiert) keine Rolle.

Aufbau des Befehls

```
pgp_encrypted();
```

Rückgabewert

positiv wenn die E-Mail OpenPGP verschlüsselt ist
negativ wenn die E-Mail nicht OpenPGP verschlüsselt ist

Parameter

keine

Beispiel 1

Zeile	Code
01	if (pgp encrypted()) {
02	log(1, 'e-mail is OpenPGP encrypted');
03	if (decrypt domain pgp()) {
04	log(1, 'mail successfully OpenPGP domain decrypted');
05	} else {
06	log(1, 'mail could not be OpenPGP domain decrypted');
07	if (decrypt pgp()) {
08	log(1, 'mail successfully OpenPGP decrypted');
09	} else {
10	log(1, 'mail could not be OpenPGP decrypted');
11	}
12	}
13	} else {
14	log(1, 'e-mail is not OpenPGP encrypted');
15	}

Erklärung

In diesem Beispiel wird zunächst geprüft, ob eine E-Mail OpenPGP verschlüsselt ist (**Zeile 01**) und ein entsprechender ein Log Eintrag geschrieben (**Zeile 02 und 14**). Ist die E-Mail OpenPGP verschlüsselt, so wird zunächst versucht die E-Mail mit dem privaten OpenPGP Domänen Schlüssel zu entschlüsseln (**Zeile 03**) und Erfolg beziehungsweise Misserfolg protokolliert wird (**Zeile 04 und 06**).

Konnte nicht mit dem privaten OpenPGP Domänen Schlüssel entschlüsselt werden, so wird nun versucht mit einem Benutzer basierten, privaten OpenPGP Schlüssel zu entschlüsseln (**Zeile 07**). Das Ergebnis dieser Aktion wird ebenfalls protokolliert (**Zeile 08 und 10**).

8.6.11.1.3 Domänen basiert

8.6.11.1.3.1 decrypt_domain_pgp()

Der Befehl `decrypt_domain_pgp()` entschlüsselt OpenPGP Domänen verschlüsselte E-Mails.

Dieser Befehl versucht eingehende OpenPGP Domänen verschlüsselten Texte und Anlagen einer E-Mail zu entschlüsseln, die durch den Absender mittels öffentlichen OpenPGP Domänen Schlüssel (siehe [Mail System](#)^[247] [Managed domains](#)^[247] [ADD/EDIT MANAGED DOMAIN](#)^[274] [OpenPGP Domain Encryption](#)^[274]) verschlüsselt wurden.

Aufbau des Befehls

```
decrypt_domain_pgp();
```

Rückgabewert

positiv wenn mindestens ein Text oder eine Anlage entschlüsselt werden wurde
negativ wenn das Entschlüsseln fehlgeschlagen ist.

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (decrypt domain pgp()) {</code>
02	<code>log(1,'mail successfully OpenPGP domain decrypted');</code>
03	<code>} else {</code>
04	<code>log(1,'mail could not be OpenPGP domain decrypted');</code>
05	<code>}</code>

Erklärung

In diesem Beispiel wird eine OpenPGP Domänen verschlüsselte E-Mail entschlüsselt (**Zeile 01**). Erfolg beziehungsweise Misserfolg des Entschlüsselns wird protokolliert (**Zeile 02 und 04**).

8.6.11.1.3.2 domain_pgp_keys_avail()

Der Befehl `domain_pgp_keys_avail()` prüft die Verfügbarkeit von öffentlichen OpenPGP Domänen Schlüsseln.

Dieser Befehl prüft die Verfügbarkeit öffentlicher OpenPGP Domänen Schlüssel (siehe [OpenPGP domain keys](#) ^[492] [Manual OpenPGP domain keys](#) ^[492]) anhand der Empfänger aus dem Envelope für das [Verschlüsseln](#) ausgehender E-Mails.

Aufbau des Befehls

```
domain_pgp_keys_avail();
```

Rückgabewert

positiv für die Gruppe mit vorhandenem öffentlichen OpenPGP Domänen Schlüssel
negativ für die Gruppe ohne öffentlichen OpenPGP Domänen Schlüssel

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (domain pgp keys avail()) {</code>
02	<code> log(1,'OpenPGP domain key available for recipient(s) \$to');</code>
03	<code> if (encrypt domain pgp()) {</code>
04	<code> log(1,'mail successfully OpenPGP domain encrypted');</code>
05	<code> } else {</code>
06	<code> log(1,'mail could not be OpenPGP domain encrypted');</code>
07	<code> }</code>
08	<code>} else {</code>
09	<code> log(1,'no OpenPGP domain key available for recipient(s) \$to');</code>
10	<code>}</code>

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein passender öffentlicher OpenPGP Domänen Schlüssel für das Verschlüsseln zur Verfügung steht (**Zeile 01**). Das Ergebnis dieser Abfrage wird protokolliert (**Zeile 02 und 09**). Steht ein entsprechender Schlüssel zur Verfügung, wird mit dem Verschlüsseln fortgefahren (**Zeile 03**), dessen Erfolg beziehungsweise Misserfolg ebenfalls protokolliert wird (**Zeile 04 und 06**).

8.6.11.1.3.3 encrypt_domain_pgp_inline()

Der Befehl `encrypt_domain_pgp_inline()` verschlüsselt E-Mails mittels OpenPGP inline Domänenverschlüsselung ^[31].

Dieser Befehl verschlüsselt alle Texte und Anlagen ausgehender E-Mails via OpenPGP inline Domänenverschlüsselung ^[31].

Stehen nicht für alle Empfänger aus dem Envelope der E-Mail öffentliche OpenPGP Domänen Schlüssel (siehe [OpenPGP domain keys](#) ^[492] [Manual OpenPGP domain keys](#) ^[492]) für das Verschlüsseln bereit, so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
encrypt_domain_pgp();
```

Rückgabewert

positiv für die Gruppe der Empfänger, für die verschlüsselt werden konnte
negativ für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (encrypt_domain_pgp()) {</code>
02	<code> log(1, 'mail successfully OpenPGP domain encrypted');</code>
03	<code>} else {</code>
04	<code> log(1, 'mail could not be OpenPGP domain encrypted');</code>
05	<code>}</code>

Erklärung

In diesem Beispiel wird versucht eine E-Mail mittels öffentlichen OpenPGP Domänen Schlüssel des Kommunikationspartners zu Verschlüsseln (**Zeile 01**). Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert (**Zeile 02 und 04**).

8.6.11.1.3.4 encrypt_domain_pgp_mime()

Der Befehl `encrypt_domain_pgp_mime()` verschlüsselt E-Mails mittels OpenPGP MIME

[Domänenverschlüsselung](#) ^[31]

Dieser Befehl verschlüsselt alle Texte und Anlagen ausgehender E-Mails via OpenPGP MIME

[Domänenverschlüsselung](#) ^[31]

Stehen nicht für alle Empfänger aus dem Envelope der E-Mail öffentliche OpenPGP Domänen Schlüssel (siehe [OpenPGP domain keys](#) ^[492] [Manual OpenPGP domain keys](#) ^[492]) für das [Verschlüsseln](#) bereit, so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
encrypt_domain_pgp();
```

Rückgabewert

positiv für die Gruppe der Empfänger, für die verschlüsselt werden konnte

negativ für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (encrypt domain pgp mime()) {</code>
02	<code>log(1, 'mail successfully OpenPGP domain encrypted');</code>
03	<code>} else {</code>
04	<code>log(1, 'mail could not be OpenPGP domain encrypted');</code>
05	<code>}</code>

Erklärung

In diesem Beispiel wird versucht eine E-Mail mittels öffentlichen OpenPGP Domänen Schlüssel des Kommunikationspartners zu Verschlüsseln (**Zeile 01**). Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert (**Zeile 02 und 04**).

8.6.11.1.4 Benutzer basiert

8.6.11.1.4.1 decrypt_pgp()

Der Befehl `decrypt_pgp()` entschlüsselt OpenPGP verschlüsselte E-Mails.

Dieser Befehl versucht alle OpenPGP verschlüsselten Texte und Anlagen einer eingehenden E-Mail zu entschlüsseln, die durch den Absender mittels des persönlichen öffentlichen OpenPGP Schlüssels des Empfängers (siehe **Users** ^[398] **USER 'USER@DOMAIN.TLD'** ^[398] OpenPGP ^[402] verschlüsselt wurden.

Aufbau des Befehls

```
decrypt_pgp();
```

Rückgabewert

positiv wenn mindestens ein Text oder eine Anlage entschlüsselt werden konnte
negativ wenn das Entschlüsseln fehlgeschlagen ist.

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (decrypt_pgp()) {</code>
02	<code> log(1, 'mail successfully OpenPGP decrypted');</code>
03	<code>} else {</code>
04	<code> log(1, 'mail could not be OpenPGP decrypted');</code>
05	<code>}</code>

Erklärung

In diesem Beispiel wird eine Benutzer basiert OpenPGP verschlüsselte E-Mail entschlüsselt (**Zeile 01**). Erfolg beziehungsweise Misserfolg des Entschlüsselns wird protokolliert (**Zeile 02 und 04**).

8.6.11.1.4.2 pgp_keys_avail()

Der Befehl `pgp_keys_avail()` prüft die Verfügbarkeit von öffentlichen OpenPGP Schlüsseln.

Dieser Befehl prüft die Verfügbarkeit personenbezogener öffentlicher OpenPGP Schlüssel der Empfänger (siehe **OpenPGP public keys** ^[467]) für das Verschlüsseln ausgehender E-Mails anhand des Envelopes.

Aufbau des Befehls

```
pgp_keys_avail();
```

Rückgabewert

positiv für die Gruppe mit vorhandenem öffentlichen OpenPGP Schlüssel
negativ für die Gruppe ohne öffentlichen OpenPGP Schlüssel

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (pgp keys avail()) {</code>
02	<code> log(1, 'OpenPGP key available for recipient(s) \$to');</code>
03	<code> if (encrypt pgp()) {</code>
04	<code> log(1, 'mail successfully OpenPGP encrypted');</code>
05	<code> } else {</code>
06	<code> log(1, 'mail could not be OpenPGP encrypted');</code>
07	<code> }</code>
08	<code>} else {</code>
09	<code> log(1, 'no OpenPGP key available for recipient(s) \$to');</code>
10	<code>}</code>

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein passender, Benutzer basierter öffentlicher OpenPGP Schlüssel für das Verschlüsseln zur Verfügung steht (**Zeile 01**). Das Ergebnis dieser Abfrage wird protokolliert (**Zeile 02 und 09**). Steht ein entsprechender Schlüssel zur Verfügung, wird mit dem Verschlüsseln fortgefahren (**Zeile 03**), dessen Erfolg beziehungsweise Misserfolg ebenfalls protokolliert wird (**Zeile 04 und 06**).

8.6.11.1.4.3 pgp_secret_keys_avail()

Der Befehl `pgp_secret_keys_avail()` prüft die Verfügbarkeit von privaten OpenPGP Schlüsseln.

Dieser Befehl prüft, ob ein interner Benutzer der Appliance (siehe **Users** ^[396] `USER 'USER@DOMAIN.TLD'` ^[398] **OpenPGP** ^[402]) einen gültigen privaten OpenPGP-Schlüssel besitzt.

Aufbau des Befehls

```
pgp_secret_keys_avail();
```

Rückgabewert

positiv wenn der zur E-Mail Adresse gehörende persönliche private OpenPGP Schlüssel vorhanden ist
negativ wenn kein zur E-Mail Adresse gehörender persönlicher privater OpenPGP Schlüssel vorhanden ist

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if pgp secret keys avail(){</code>
02	<code>sign pgp mime();</code>
03	<code>}</code>

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein privater OpenPGP Schlüssel verfügbar ist (**Zeile 01**). Ist dies der Fall, so wird die ausgehende E-Mail OpenPGP signiert (**Zeile 02**).

8.6.11.1.4.4 encrypt_pgp()

Ersetzt durch `encrypt_pgp_inline()` ^[576], beziehungsweise `encrypt_pgp_mime()` ^[577].

8.6.11.1.4.5 encrypt_pgp_inline()

Der Befehl `encrypt_pgp_inline()` ermöglicht es, E-Mails via OpenPGP inline zu verschlüsseln und zu signieren.

Dieser Befehl verschlüsselt alle Texte und Anlagen einer ausgehenden E-Mail mit dem öffentlichen OpenPGP Schlüssel des Empfängers (siehe [OpenPGP public keys](#) ^[467]). Dabei wird das OpenPGP inline Verfahren genutzt. Optional kann zusätzlich mit dem privaten OpenPGP Schlüssel des Absenders (siehe [Users](#) ^[396] [User details](#) ^[398] `USER 'USER@DOMAIN.TLD'` [OpenPGP](#) ^[402]) signiert werden.

Stehen nicht für alle Empfänger aus dem Envelope der E-Mail öffentliche OpenPGP Schlüssel bereit, so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
encrypt_pgp_inline(['sign'], ['address']);
```

Rückgabewert

- positiv** für die Gruppe der Empfänger, für die verschlüsselt werden konnte, unabhängig ob das optionale Signieren erfolgreich war
- negativ** für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

Parameter

sign

Dieser Parameter entscheidet, ob die E-Mail mit dem privaten OpenPGP Schlüssel des Absenders signiert werden soll.

Mögliche Werte

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

address

E-Mail Adresse des Empfängers, dessen öffentlicher OpenPGP Schlüssel für das Verschlüsseln verwendet werden soll.

Wird kein Parameter angegeben, so wird der öffentliche OpenPGP Schlüssel des jeweiligen Empfängers verwendet.

Beispiel 1

Zeile	Code
01	<code>encrypt_pgp_inline('yes', 'recipient@customer.org');</code>

Erklärung

In diesem Beispiel wird versucht alle Texte und Anlagen einer E-Mail zu verschlüsseln und zu signieren, da der Parameter `sign` den Wert „yes“ hat. Für das Verschlüsseln wird der öffentliche OpenPGP Schlüssel des durch den Parameter `address` spezifizierten Empfängers verwendet. Im Beispiel „recipient@customer.org“.

8.6.11.1.4.6 encrypt_pgp_mime()

Der Befehl `encrypt_pgp_mime()` ermöglicht es, E-Mails via OpenPGP inline zu verschlüsseln und zu signieren.

Dieser Befehl verschlüsselt ausgehende E-Mails mit dem öffentlichen OpenPGP Schlüssel des Empfängers (siehe [OpenPGP public keys](#) [467]). Dabei wird das OpenPGP MIME Verfahren genutzt. Optional kann zusätzlich mit dem privaten OpenPGP Schlüssel des Absenders (siehe [Users](#) [396] [User details](#) [398] `USER 'USER@DOMAIN.TLD'` [OpenPGP](#) [402]) signiert werden.

Stehen nicht für alle Empfänger aus dem Envelope der E-Mail öffentliche OpenPGP Schlüssel bereit, so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
encrypt_pgp_mime(['sign'], ['address']);
```

Rückgabewert

- positiv** für die Gruppe der Empfänger, für die verschlüsselt werden konnte, unabhängig ob das optionale Signieren erfolgreich war
- negativ** für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

Parameter

sign

Dieser Parameter entscheidet, ob die E-Mail mit dem privaten OpenPGP Schlüssel des Absenders signiert werden soll.

Mögliche Werte

- true, yes oder 1
 - false, no oder 0
- Standardeinstellung ist 0

address

E-Mail Adresse des Empfängers, dessen öffentlicher OpenPGP Schlüssel für das Verschlüsseln verwendet werden soll.

Wird kein Parameter angegeben, so wird der öffentliche OpenPGP Schlüssel des jeweiligen Empfängers verwendet.

Beispiel 1

Zeile	Code
01	<code>encrypt_pgp_mime('yes', 'recipient@customer.org');</code>

Erklärung

In diesem Beispiel wird versucht alle Texte und Anlagen einer E-Mail zu verschlüsseln und zu signieren, da der Parameter `sign` den Wert „yes“ hat. Für das Verschlüsseln wird der öffentliche OpenPGP Schlüssel des durch den Parameter `address` spezifizierten Empfängers verwendet. Im Beispiel „recipient@customer.org“.

8.6.11.1.4.7 pgp_signed()

Der Befehl `pgp_signed()` prüft, ob eine E-Mail OpenPGP MIME signiert ist.

(siehe [Mail Processing](#) ^[286] [Ruleset generator](#) ^[287] [Signing](#) ^[298])

Aufbau des Befehls

```
pgp_signed();
```

Rückgabewert

positiv wenn die E-Mail OpenPGP MIME signiert ist
negativ wenn die E-Mail nicht OpenPGP MIME signiert ist

Parameter

keine

Beispiel 1

Zeile	Code
01	if (pgp signed()) {
02	log(1, 'e-mail is OpenPGP signed');
03	if (validate pgp sig('')) {
04	log(1, 'signature is valid');
05	} else {
06	log(1, 'signature is invalid');
07	}
08	} else {
09	log(1, 'e-mail is not OpenPGP MIME signed');
10	}

Erklärung

In diesem Beispiel wird zunächst geprüft, ob eine E-Mail OpenPGP MIME signiert ist (**Zeile 01**) und ein entsprechender ein Log Eintrag geschrieben (**Zeile 2 und 9**). Ist die E-Mail OpenPGP MIME signiert, so wird die Signatur geprüft (**Zeile 03**) und Erfolg beziehungsweise Misserfolg protokolliert (**Zeile 04 und 06**).

8.6.11.1.4.8 validate_pgp_sig()

Der Befehl `validate_pgp_sig()` prüft die OpenPGP MIME Signatur einer E-Mail auf ihre Gültigkeit.

(siehe Hinweis unter [Mail Processing](#)^[286] Ruleset generator^[287] **Signing**^[298] **Incoming e-mails** Add this text to message subject if OpenPGP signature check succeeds:)

Aufbau des Befehls

```
validate_pgp_sig('');
```

Rückgabewert

positiv bei gültiger Signatur.
negativ bei ungültiger Signatur

Parameter

keine

Beispiel 1

Zeile	Code
01	if (validate pgp sig('')) {
02	log(1,'signature is valid');
03	} else {
04	log(1,'signature is invalid');
05	}

Erklärung

In diesem Beispiel wird die OpenPGP MIME Signatur einer E-Mail geprüft (**Zeile 01**) und Erfolg beziehungsweise Misserfolg protokolliert wird (**Zeile 02 und 04**).

8.6.11.1.4.9 delete_pgp_sig()

Der Befehl `delete_pgp_sig()` ermöglicht die OpenPGP MIME-Signatur einer E-Mail zu löschen.

**Hinweis:**

Die Gültigkeit der S/MIME-Signatur wird nicht geprüft.

Aufbau des Befehls

```
delete_pgp_sig();
```

Rückgabewert

positiv

wenn die OpenPGP Signatur erfolgreich entfernt wurde

negativ

wenn die OpenPGP nicht entfernt werden konnte (weil keine Signatur vorhanden ist oder tatsächlich nicht entfernt werden konnte)

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (validate_pgp_sig('')) {</code>
02	<code> log(1,'signature is valid');</code>
03	<code> delete_pgp_sig();</code>
04	<code>} else {</code>
05	<code> log(1,'signature is invalid');</code>
06	<code>}</code>

Erklärung

In diesem Beispiel wird die OpenPGP MIME Signatur einer E-Mail geprüft (**Zeile 01**) und Erfolg beziehungsweise Misserfolg protokolliert (**Zeile 02 und 05**). Wurde die Signatur als gültig eingestuft, so wird sie gelöscht (**Zeile 03**).

8.6.11.1.4.10 sign_pgp_mime()

Der Befehl `sign_pgp_mime()` signiert eine E-Mail.

Dieser Befehl signiert die ausgehende E-Mail mit dem persönlichen privaten OpenPGP Schlüssel des Absenders (siehe **Users** ³⁹⁶ `USER 'USER@DOMAIN.TLD'` ³⁹⁸ `OpenPGP` ⁴⁰²) aus dem Envelope der E-Mail.

Aufbau des Befehls

```
sign_pgp_mime(['address']);
```

Rückgabewert

positiv wenn die Nachricht erfolgreich signiert wurde
negativ bei Fehlschlägen der Signatur

Parameter

address

E-Mail Adresse des Empfängers, dessen privater OpenPGP Schlüssel für das Signieren verwendet werden soll. Wird kein Parameter angegeben, so wird der private OpenPGP Schlüssel des Absenders verwendet.

Beispiel 1

Zeile	Code
01	<code>if (pgp secret keys avail()){</code>
02	<code> log(1,'OpenPGP private key available, trying to sign');</code>
03	<code> if (sign pgp mime()) {</code>
04	<code> log(1,'signing successful');</code>
05	<code> } else {</code>
06	<code> log(1,'signing failed');</code>
07	<code> }</code>
08	<code>} else {</code>
09	<code> log(1,'no OpenPGP private key available, do not sign');</code>
10	<code>}</code>

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein privater OpenPGP Schlüssel verfügbar ist (**Zeile 01**). Das Ergebnis wird protokolliert (**Zeile 02 und 09**). Ist ein privater OpenPGP Schlüssel vorhanden, so wird versucht die E-Mail zu signieren (**Zeile 03**). Das Ergebnis dieser Aktion wird ebenfalls in das Log geschrieben (**Zeile 04 beziehungsweise 06**).

8.6.11.2 S/MIME

8.6.11.2.1 smime_encrypted()

Der Befehl `smime_encrypted()` prüft, ob eine E-Mail S/MIME verschlüsselt ist.

Aufbau des Befehls

```
smime_encrypted();
```

Rückgabewert

positiv wenn die E-Mail S/MIME verschlüsselt ist
negativ wenn die E-Mail nicht S/MIME verschlüsselt ist

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (smime encrypted()) {</code>
02	<code> log(1, 'e-mail is S/MIME encrypted');</code>
03	<code> if (decrypt domain smime()) {</code>
04	<code> log(1, 'mail successfully S/MIME domain decrypted');</code>
05	<code> } else {</code>
06	<code> log(1, 'mail could not be S/MIME domain decrypted');</code>
07	<code> if (decrypt smime()) {</code>
08	<code> log(1, 'mail successfully S/MIME decrypted');</code>
09	<code> } else {</code>
10	<code> log(1, 'mail could not be S/MIME decrypted');</code>
11	<code> }</code>
12	<code>}</code>
13	<code>} else {</code>
14	<code> log(1, 'mail is not S/MIME encrypted');</code>
15	<code>}</code>

Erklärung

In diesem Beispiel wird zunächst geprüft, ob eine E-Mail S/MIME verschlüsselt ist (**Zeile 01**) und ein entsprechender ein Log Eintrag geschrieben (**Zeile 02 und 14**). Ist die E-Mail S/MIME verschlüsselt, so wird zunächst versucht die E-Mail mit dem privaten S/MIME Domänen Schlüssel zu entschlüsseln (**Zeile 03**) und Erfolg beziehungsweise Misserfolg protokolliert wird (**Zeile 04 und 06**).

Konnte nicht mit dem privaten S/MIME Domänen Schlüssel entschlüsselt werden, so wird nun versucht mit einem Benutzer basierten, privaten S/MIME Schlüssel zu entschlüsseln (**Zeile 07**). Das Ergebnis dieser Aktion wird ebenfalls protokolliert (**Zeile 08 und 10**).

8.6.11.2.2 Domänen basiert

8.6.11.2.2.1 decrypt_domain_smime()

Der Befehl `decrypt_domain_smime()` entschlüsselt S/MIME Domänen verschlüsselte E-Mails.

Dieser Befehl versucht eingehende S/MIME Domänen verschlüsselte E-Mails zu entschlüsseln, die durch den Absender mittels öffentlichen S/MIME Domänen Schlüssel (siehe [Mail System](#) ^[247], [Managed domains](#) ^[247], [ADD/EDIT MANAGED DOMAIN](#) ^[274], [S/MIME Domain Encryption](#) ^[274]) verschlüsselt wurden.

Aufbau des Befehls

```
decrypt_domain_smime([keydomain]);
```

Rückgabewert

positiv wenn die E-Mail entschlüsselt werden konnte
negativ wenn das Entschlüsseln der E-Mail fehlgeschlagen ist.

Parameter

keydomain (optional)

An dieser Stelle kann die [Managed domain](#) ^[247] angegeben werden, deren Domain Keys für das entschlüsseln von E-Mails verwendet werden sollen.

Beispiel 1

Zeile	Code
01	<code>if (decrypt domain smime()) {</code>
02	<code>log(1, 'mail successfully S/MIME domain decrypted');</code>
03	<code>} else {</code>
04	<code>log(1, 'mail could not be S/MIME domain decrypted');</code>
05	<code>}</code>

Erklärung

In diesem Beispiel wird eine S/MIME Domänen verschlüsselte E-Mail entschlüsselt (**Zeile 01**). Erfolg beziehungsweise Misserfolg des Entschlüsselns wird protokolliert (**Zeile 02 und 04**).

8.6.11.2.2.2 domain_smime_keys_avail()

Der Befehl `domain_smime_keys_avail()` prüft die Verfügbarkeit von öffentlichen S/MIME Domänen Schlüsseln (Zertifikaten).

Dieser Befehl prüft die Verfügbarkeit von Domänen Zertifikaten (siehe [S/MIME domain certificates](#) ⁴⁹⁰ [Manual](#) [S/MIME domain certificates](#) ⁴⁹⁰ beziehungsweise [Domain Certificates](#) ⁴⁸⁹ [Managed S/MIME domain certificates](#) ⁴⁸⁹) anhand der Empfänger aus dem Envelope für das Verschlüsseln ausgehender E-Mails.

Aufbau des Befehls

```
domain_smime_keys_avail();
```

Rückgabewert

positiv für die Gruppe mit vorhandenem S/MIME Domänen Zertifikat
negativ für die Gruppe ohne S/MIME Domänen Zertifikat

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (domain smime keys avail()) {</code>
02	<code> log(1,'S/MIME domain certificate available for recipient(s) \$to');</code>
03	<code> if (encrypt domain smime()) {</code>
04	<code> log(1,'mail successfully S/MIME domain encrypted');</code>
05	<code> } else {</code>
06	<code> log(1,'mail could not be S/MIME domain encrypted');</code>
07	<code> }</code>
08	<code>} else {</code>
09	<code> log(1,'S/MIME domain certificate available for recipient(s) \$to');</code>
10	<code>}</code>

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein passendes S/MIME Domänen Zertifikat das Verschlüsseln zur Verfügung steht (**Zeile 01**). Das Ergebnis dieser Abfrage wird protokolliert (**Zeile 02 und 09**). Steht ein entsprechender Schlüssel zur Verfügung, wird mit dem Verschlüsseln fortgefahren (**Zeile 03**), dessen Erfolg beziehungsweise Misserfolg ebenfalls protokolliert wird (**Zeile 04 und 06**).

8.6.11.2.2.3 encrypt_domain_smime()

Der Befehl `encrypt_domain_smime()` verschlüsselt E-Mails mittels S/MIME [Domänenverschlüsselung](#) ^[31].

Dieser Befehl verschlüsselt die komplette ausgehende E-Mail via S/MIME [Domänenverschlüsselung](#) ^[31]. Davon ausgenommen sind lediglich E-Mail Header, da diese unter anderem für den E-Mail Transport benötigt werden. Stehen nicht für alle Empfänger der E-Mail Domäne öffentliche S/MIME Domänen Schlüssel (Zertifikate) für das [Verschlüsseln](#) bereit (siehe [S/MIME domain certificates](#) ^[490] [Manual S/MIME domain certificates](#) ^[490] beziehungsweise [Domain Certificates](#) ^[489] [Managed S/MIME domain certificates](#) ^[489]), so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
encrypt_domain_smime(['cipher[;pAdd-Ing]']);
```

Rückgabewert

positiv für die Gruppe der Empfänger, für die verschlüsselt werden konnte
negativ für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

Parameter

cipher (optional)

Dieser Parameter erzwingt das Verschlüsseln mit dem jeweils angegebenen Verschlüsselungsalgorithmus (siehe auch [Mail Processing](#) ^[286] [Ruleset generator](#) ^[287] [Encryption](#) ^[292] [Outgoing e-mails](#) Use default cipher for S/MIME encryption).

Mögliche Werte

- des3
- aes128
- aes192
- aes256

Standardeinstellung ist des3

pAdd-Ing (optional)

Dieser Parameter erzwingt das gewählte PAdd-Ing-Verfahren (siehe auch [Mail Processing](#) ^[286] [Ruleset generator](#) ^[287] [Encryption](#) ^[292] [Outgoing e-mails](#) ^[293] Prefer RSA-OAEP for S/MIME encryption ^[296]).

Mögliche Werte

- pkcs
- oaep

Standardeinstellung ist pkcs

Beispiel 1

Zeile	Code
01	<code>if (encrypt domain smime()) {</code>
02	<code> log(1,'mail successfully S/MIME domain encrypted');</code>
03	<code>} else {</code>
04	<code> log(1,'mail could not be S/MIME domain encrypted');</code>
05	<code>}</code>

Erklärung

In diesem Beispiel wird versucht eine E-Mail mittels S/MIME Domänen Zertifikat des Kommunikationspartners zu Verschlüsseln (**Zeile 01**). Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert (**Zeile 02 und 04**).

8.6.11.2.3 Benutzer basiert

8.6.11.2.3.1 decrypt_smime()

Der Befehl `decrypt_smime()` entschlüsselt S/MIME verschlüsselte E-Mails.

Dieser Befehl entschlüsselt eingehende E-Mails, welche durch den Absender mittels des persönlichen öffentlichen S/MIME Schlüssel (Zertifikat) des Empfängers (siehe `Users` `USER 'USER@DOMAIN.TLD'` `S/MIME`) verschlüsselt wurden.

Aufbau des Befehls

```
decrypt_smime();
```

Rückgabewert

positiv wenn die E-Mail entschlüsselt wurde
negativ wenn das Entschlüsseln der E-Mail fehlgeschlagen ist.

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (decrypt smime()) {</code>
02	<code>log(1, 'mail successfully S/MIME decrypted');</code>
03	<code>} else {</code>
04	<code>log(1, 'mail could not be S/MIME decrypted');</code>
05	<code>}</code>

Erklärung

In diesem Beispiel wird eine Benutzer basiert S/MIME verschlüsselte E-Mail entschlüsselt (**Zeile 01**). Erfolg beziehungsweise Misserfolg des Entschlüsselns wird protokolliert (**Zeile 02 und 04**).

8.6.11.2.3.2 smime_keys_avail()

Der Befehl `smime_keys_avail()` prüft die Verfügbarkeit von öffentlichen S/MIME Schlüsseln (Zertifikate).

Dieser Befehl prüft die Verfügbarkeit personenbezogener Zertifikate der Empfänger (siehe [X.509 Certificates](#)^[471]) für das Verschlüsseln ausgehender E-Mails anhand des Envelopes.

Aufbau des Befehls

```
smime_keys_avail();
```

Rückgabewert

positiv für die Gruppe mit vorhandenem S/MIME Zertifikat
negativ für die Gruppe ohne S/MIME Zertifikat

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (smime keys avail()) {</code>
02	<code> log(1,'S/MIME certificate available for recipient(s) \$to');</code>
03	<code> if (encrypt smime()) {</code>
04	<code> log(1,'mail successfully S/MIME encrypted');</code>
05	<code> } else {</code>
06	<code> log(1,'mail could not be S/MIME encrypted');</code>
07	<code> }</code>
08	<code>} else {</code>
09	<code> log(1,'no S/MIME certificate available for recipient(s) \$to');</code>
10	<code>}</code>

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein passendes, Benutzer basiertes S/MIME Zertifikat für das Verschlüsseln zur Verfügung steht (**Zeile 01**). Das Ergebnis dieser Abfrage wird protokolliert (**Zeile 02 und 09**). Steht ein entsprechender Schlüssel zur Verfügung, wird mit dem Verschlüsseln fortgefahren (**Zeile 03**), dessen Erfolg beziehungsweise Misserfolg ebenfalls protokolliert wird (**Zeile 04 und 06**).

8.6.11.2.3.3 encrypt_smime()

Der Befehl `encrypt_smime()` verschlüsselt E-Mails mittels S/MIME.

Dieser Befehl verschlüsselt die komplette ausgehende E-Mail via S/MIME. Davon ausgenommen sind lediglich E-Mail Header, da diese unter anderem für den E-Mail Transport benötigt werden.

Stehen nicht für alle Empfänger aus dem Envelope der E-Mail personenbezogene öffentliche S/MIME Schlüssel (Zertifikate) für das Verschlüsseln bereit (siehe [X.509 Certificates](#) ^[47]), so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
encrypt_smime(['internal'], ['host'], ['cipher[:pAdd-Ing]']);
```

Rückgabewert

- positiv** für die Gruppe der Empfänger, für die verschlüsselt werden konnte
negativ für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

Parameter

internal (optional)

Dieser Parameter gibt an, ob die E-Mail nach intern mittels S/MIME verschlüsselt werden soll (siehe auch [Internal Mail Encryption \(IME\)](#) ^[114])

Mögliche Werte:

- true, yes oder 1
 - false, no oder 0
- Standardeinstellung ist 0

host (optional)

Herstellerspezifischer Parameter

cipher (optional)

Dieser Parameter erzwingt das Verschlüsseln mit dem jeweils angegebenen Verschlüsselungsalgorithmus (siehe auch [Mail Processing](#) ^[286], [Ruleset generator](#) ^[287], [Encryption](#) ^[292], [Outgoing e-mails](#) Use default cipher for S/MIME encryption).

Mögliche Werte:

- des3
 - aes128
 - aes192
 - aes256
- Standardeinstellung ist des3

pAdd-Ing (optional)

Dieser Parameter erzwingt das gewählte PAdd-Ing-Verfahren (siehe auch [Mail Processing](#) ^[286], [Ruleset generator](#) ^[287], [Encryption](#) ^[292], [Outgoing e-mails](#) Prefer RSA-OAEP for S/MIME encryption).

Mögliche Werte:

- pkcs
 - oaep
- Standardeinstellung ist pkcs

Beispiel 1

Zeile	Code
01	<code>if (encrypt_smime('false','', 'aes192')) {</code>
02	<code>log(1, 'mail successfully S/MIME encrypted');</code>
03	<code>} else {</code>
04	<code>log(1, 'mail could not be S/MIME encrypted');</code>
05	<code>}</code>

Erklärung

In diesem Beispiel wird versucht eine E-Mail mittels Benutzer basiertem S/MIME Zertifikat des Kommunikationspartners zu AES192 zu Verschlüsseln (**Zeile 01**). Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert (**Zeile 02 und 04**).

8.6.11.2.3.4 smime_signed()

Der Befehl `smime_signed()` prüft, ob eine E-Mail S/MIME signiert ist

(siehe Warnung unter [Mail Processing](#) ^[286] [Ruleset generator](#) ^[287] [Signing](#) ^[298]).

Aufbau des Befehls

```
smime_signed();
```

Rückgabewert

positiv wenn die E-Mail S/MIME signiert ist
negativ wenn die E-Mail nicht S/MIME signiert ist

Parameter

keine

Beispiel 1

Zeile	Code
01	if (smime signed()) {
02	log(1, 'e-mail is S/MIME signed');
03	if (validate smime sig('1')) {
04	log(1, 'signature is valid');
05	} else {
06	log(1, 'signature is invalid');
07	}
08	} else {
09	log(1, 'e-mail is not S/MIME signed');
10	}

Erklärung

In diesem Beispiel wird zunächst geprüft, ob eine E-Mail S/MIME signiert ist (**Zeile 01**) und ein entsprechender ein Log Eintrag geschrieben (Zeile 2 und 9). Ist die E-Mail S/MIME signiert, so wird die Signatur geprüft (**Zeile 03**) und Erfolg beziehungsweise Misserfolg protokolliert (**Zeile 04 und 06**).

8.6.11.2.3.5 validate_smime_sig()

Der Befehl `validate_smime_sig()` prüft die S/MIME Signatur einer E-Mail auf ihre Gültigkeit.

(siehe Hinweis unter [Mail Processing](#)^[286] [Ruleset generator](#)^[287] [Signing](#)^[298] [Incoming e-mails](#) Add this text to message subject if S/MIME signature check succeeds:)

Aufbau des Befehls

```
validate_smime_sig('fetch_certificate');
```

Rückgabewert

positiv bei gültiger Signatur.
negativ bei ungültiger Signatur

Parameter

fetch_certificate (optional)

Ist dieser Parameter gesetzt ('1'), wird der in der Signatur enthaltene öffentliche Schlüssel (Zertifikat) des Absenders gespeichert (siehe [X.509 Certificates](#)^[47]). Voraussetzung hierfür ist, dass die Zertifikatskette vollständig ist und geprüft werden kann (siehe [X.509 Root Certificates](#)^[48]). Dies ist unabhängig davon, ob die E-Mail verändert wurde oder nicht

Mögliche Werte:

- true, yes oder 1
 - false, no oder 0
- Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	<code>if (validate_smime_sig('1')) {</code>
02	<code>log(1, 'signature is valid');</code>
03	<code>} else {</code>
04	<code>log(1, 'signature is invalid');</code>
05	<code>}</code>

Erklärung

In diesem Beispiel wird die S/MIME Signatur einer E-Mail geprüft (**Zeile 01**) und Erfolg beziehungsweise Misserfolg protokolliert wird (**Zeile 02 und 04**).

8.6.11.2.3.6 delete_smime_sig()

Der Befehl `delete_smime_sig()` ermöglicht es, die S/MIME-Signatur einer E-Mail zu löschen.

(siehe Hinweis unter [Mail Processing](#)^[286] [Ruleset generator](#)^[287] [Signing](#)^[298] [Incoming e-mails Remove signature if S/MIME signature check succeeds](#))



Hinweis:

Die Gültigkeit der S/MIME-Signatur wird nicht geprüft.

Aufbau des Befehls

```
delete_smime_sig();
```

Rückgabewert

positiv

wenn die S/MIME Signatur erfolgreich entfernt wurde

negativ

wenn die S/MIME Signatur nicht entfernt werden konnte (weil keine Signatur vorhanden ist oder tatsächlich nicht entfernt werden konnte)

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (validate smime sig('1')) {</code>
02	<code> log(1,'signature is valid');</code>
03	<code> delete smime sig();</code>
04	<code>} else {</code>
05	<code> log(1,'signature is invalid');</code>
06	<code>}</code>

Erklärung

In diesem Beispiel wird die S/MIME Signatur einer E-Mail geprüft (**Zeile 01**) und Erfolg beziehungsweise Misserfolg protokolliert wird (**Zeile 02 und 05**). Wurde die Signatur als gültig eingestuft, so wird sie gelöscht (**Zeile 03**).

8.6.11.2.3.7 has_smime_key()

Der Befehl `has_smime_key()` prüft, ob der Benutzer einen gültigen privaten S/MIME-Schlüssel besitzt.

Dieser Befehl prüft, ob ein interner Benutzer der Appliance (siehe [Users](#) ^[396] `USER 'USER@DOMAIN.TLD'` ^[398] `S/MIME` ^[401]) einen gültigen privaten S/MIME-Schlüssel besitzt.



Hinweis:

Voraussetzung für eine Suche mit `has_smime_key()` ist, dass der Benutzer bereits authentifiziert ist (siehe `authenticated()` ^[537]).

Aufbau des Befehls

```
has_smime_key();
```

Rückgabewert

positiv wenn der Benutzer einen gültigen privaten S/MIME-Schlüssel besitzt

negativ wenn der Benutzer

- keine oder nur abgelaufene S/MIME-Schlüssel besitzt.
- auf den Status **may not encrypt** gesetzt ist.
- auf den Status **may not sign** gesetzt ist.

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (has smime key()){</code>
02	<code> log(1,'S/MIME key available, trying to sign');</code>
03	<code> if (sign smime()) {</code>
04	<code> log(1,'signing successful');</code>
05	<code> } else {</code>
06	<code> log(1,'signing failed');</code>
07	<code> }</code>
08	<code>} else {</code>
09	<code> log(1,'no S/MIME key available, do not sign');</code>
10	<code>}</code>

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein privater S/MIME Schlüssel verfügbar ist (**Zeile 01**). Das Ergebnis wird protokolliert (**Zeile 02 und 09**). Ist ein privater S/MIME Schlüssel vorhanden, so wird versucht die E-Mail zu signieren (**Zeile 03**) und das Ergebnis dieser Aktion wird ebenfalls in das Log geschrieben (**Zeile 04 beziehungsweise 06**).

8.6.11.2.3.8 sign_smime()

Der Befehl `sign_smime()` signiert eine E-Mail.

Dieser Befehl signiert die ausgehende E-Mail mit dem persönlichen privaten S/MIME Schlüssel des authentifizierten (`authenticated()` [\[537\]](#)) Absenders (siehe [Users](#) [\[396\]](#) `USER 'USER@DOMAIN.TLD'` [\[396\]](#) [S/MIME](#) [\[401\]](#)) der E-Mail.

Aufbau des Befehls

```
sign_smime(['hash[:pAdd-Ing][:opaque]']);
```

Rückgabewert

positiv wenn die Nachricht erfolgreich signiert wurde
negativ bei Fehlschlägen der Signatur

Parameter

hash (optional)

Mit diesem Parameters wird der für das Signieren verwendete hash-Algorithmus angegeben (siehe auch [Mail Processing](#) [\[286\]](#) [Ruleset generator](#) [\[287\]](#) [Signing](#) [\[298\]](#) [Outgoing e-mails](#) Use default digest for S/MIME signing).

Mögliche Werte:

- sha1
- sha256
- sha512

Standardeinstellung ist sha256

pAdd-Ing (optional)

Dieser Parameter erzwingt das gewählte `pAdd-Ing`-Verfahren (siehe auch [Mail Processing](#) [\[286\]](#) [Ruleset generator](#) [\[287\]](#) [Signing](#) [\[298\]](#) [Outgoing e-mails](#) Prefer RSA-PSS for S/MIME signatures).

Mögliche Werte:

- pkcs
- pss

Standardeinstellung ist pkcs

opaque (optional)

Mit diesem Parameters wird das Signaturverfahren gewählt, detached (oder auch clear text) oder opaque (siehe auch [ADD/EDIT ENCRYPTION POLICY](#) [\[314\]](#) [Settings](#) [\[314\]](#) [S/MIME options](#) Use opaque signature).

Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	<code>if (has smime key()) {</code>
02	<code> log(1,'S/MIME key available, trying to sign');</code>
03	<code> if (sign smime(';;1')) {</code>
04	<code> log(1,'signing successful');</code>
05	<code> } else {</code>
06	<code> log(1,'signing failed');</code>
07	<code> }</code>
08	<code>} else {</code>
09	<code> log(1,'no S/MIME key available, do not sign');</code>
10	<code>}</code>

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein privater S/MIME Schlüssel verfügbar ist (**Zeile 01**). Das Ergebnis wird protokolliert (**Zeile 02 und 09**). Ist ein privater S/MIME Schlüssel vorhanden, so wird die E-Mail unter

Verwenden des SHA256Algorithmus (Standard) im Opaque Verfahren signiert (**Zeile 03**) und das Ergebnis dieser Aktion wird ebenfalls in das Log geschrieben (**Zeile 04 beziehungsweise 06**).

8.6.11.3 GINA

8.6.11.3.1 encrypt_webmail()

Der Befehl `encrypt_webmail()` verschlüsselt eine E-Mail unter Verwendung der GINA-Technologie.

Dieser Befehl verschlüsselt eine ausgehende Nachricht via GINA-Technologie an die Empfängeradresse. Die Empfänger- sowie die Absenderadresse wird aus der aktuell verarbeiteten Nachricht für die GINA-Träger-E-Mail entnommen.

Nach dem Verschlüsseln einer Nachricht mittels GINA-Technologie sollte diese immer direkt mit `deliver()` versendet werden.

Aufbau des Befehls

```
encrypt_webmail(['template'], ['no_pw_mail_if_sms_sent']);
```

Rückgabewert

positiv bei erfolgreicher GINA-Verschlüsselung
negativ bei fehlgeschlagener GINA-Verschlüsselung

Parameter

template (optional)

Definiert die zu verwendende GINA-Domain.

Wird kein Parameter angegeben, so wird die Vorlage anhand der E-Mail Domäne der Absenderadresse ausgewählt (siehe **Mail System**^[247] **Managed domains**^[247] **ADD/EDIT MANAGED DOMAIN**^[266] **Settings**^[266] **GINA domain**)

no_pw_mail_if_sms_sent (optional)

Unterdrückt ('1') die Passwort-E-Mail an den Absender, bei Verwenden eines 'template' mit der Einstellung **Unique e-mail password**^[451], sofern das Passwort bereits via SMS übermittelt werden konnte (siehe auch Schlüsselwort [SMS:] in Tabelle 1 des Kapitels **Steuern der Appliance**^[164]).

Mögliche Werte:

- true, yes oder 1
 - false, no oder 0
- Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	<code>if (encrypt_webmail()) {</code>
02	<code> log(1,'mail successfully GINA encrypted');</code>
03	<code> deliver();</code>
04	<code>} else {</code>
05	<code> log(1,'mail could not be GINA encrypted');</code>
06	<code> drop('451','Die Nachricht konnte nicht verschlüsselt werden');</code>
07	<code>}</code>

Erklärung

In diesem Beispiel wird versucht eine E-Mail mittels GINA-Technologie zu Verschlüsseln (**Zeile 01**). Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert (**Zeile 02 und 05**). Bei erfolgreichem Verschlüsseln wird die E-Mail - wie empfohlen - direkt ausgeliefert (**Zeile 03**). Andernfalls wird sie mit dem temporären Fehler „451“ und dem Hinweistext „Die Nachricht konnte nicht verschlüsselt werden“ abgewiesen (**Zeile 06**).



Hinweis:

Wird `encrypt_webmail()` mit einem 'template' verwendet, welches in der **Sektion Event login**^[450] die Einstellung **Unique e-mail password**^[451] aktiv hat, so wird durch Verwenden des Befehls dieses **Unique e-mail password**^[451] versendet. Dieses Passwort wird somit auch nicht gespeichert. Ein **GINA Account**^[462] ist dennoch erforderlich, da andernfalls `encrypt_webmail()` fehlschlagen würde.

Die Funktion versendet keine Passwörter bei den 'template' Einstellungen **No password event**^[451] oder **One-time password via SMS only**^[451], da mit diesen Einstellungen der erforderliche **GINA Account**^[462] maßgeblich ist.

Beispiel 2

Zeile	Code
01	if (webmail keys avail()) {
02	log(1, 'GINA account already exists');
03	} else {
04	log(1, 'no GINA account available, creating new account');
05	webmail keys gen(' ', '0');
06	}
07	if (encrypt webmail('<GINA-template with Unique-e-mail-password>')) {
08	log(1, 'mail successfully GINA encrypted');
09	deliver();
11	} else {
12	log(1, 'mail could not be GINA encrypted');
13	drop('451', 'Message could not be encrypted');
14	}

Erklärung

In diesem Beispiel wird zunächst geprüft, ob für den Empfänger bereits ein **GINA Account**^[462] vorhanden ist (**Zeile 1**). Falls nicht, wird ein **GINA Account**^[462] mit der Passwort-Länge „0“ generiert. Durch die eingestellte Passwort-Länge „0“ wird keine Passwort-E-Mail gesendet. Nun wird die E-Mail mittels GINA-Technologie verschlüsselt (**Zeile 07**). Dabei wird der Parameter 'template' verwendet, der auf eine **GINA Domain**^[416] verweist, welche in der **Sektion Event login**^[450] die Einstellung **Unique e-mail password**^[451] aktiv hat. Somit wird für jede E-Mail, welche über diesen Mechanismus gesendet wird ein E-Mail bezogenes Passwort mit der in der **GINA Domain**^[416] aus 'template' unter **Event login**^[450] **Password strength**^[452] angegebenen Passwort-Länge generiert und versendet.

Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert (**Zeile 08 und 12**). Bei erfolgreichem Verschlüsseln wird die E-Mail - wie empfohlen - direkt ausgeliefert (**Zeile 09**). Andernfalls wird sie mit dem temporären Fehler „451“ und dem Hinweistext „Message could not be encrypted“ abgewiesen (**Zeile 13**).

8.6.11.3.2 change_webmail_sender()

Der Befehl `change_webmail_sender()` tauscht den Absender einer GINA-Träger-E-Mail gegen eine vorzugebende Adresse aus.

Durch diesen Befehl kann nach erfolgter GINA-Verschlüsselung die Absender Adresse der GINA-Träger-E-Mail zum Beispiel durch eine zentrale Absender Adresse ersetzt werden (siehe auch **CHANGE GINA SETTINGS FOR** ^[423] Extended settings ^[431] **Force sending of GINA mails from this address**!).

Aufbau des Befehls

```
change_webmail_sender('sender');
```

Rückgabewert

- positiv** bei erfolgreichem Ändern des GINA-Träger-E-Mail Absenders - auch wenn es bereits der selbe Absender war.
- negativ** wenn der Absender nicht geändert werden konnte

Parameter

sender (optional)

Gibt die Absender E-Mail Adresse für die GINA-Träger-E-Mail an.

Die hier angegebene Absender Adresse muss aus einer **Managed domain** ^[247] stammen, welcher die jeweilige GINA-Domain zugeordnet ist (siehe Tabelle **Mail System** ^[247] **Managed domains** ^[247] Spalte **GINA settings**). Weiterhin sollte die Adresse als User auf der Appliance existieren, idealerweise mit gültigem S/MIME Zertifikat (siehe **Users** ^[396] **USER 'USER@DOMAIN.TLD'** ^[398] **S/MIME** ^[401]), um die GINA-Träger-E-Mail signieren zu können. Auch am Groupware-Server sollte die Adresse existent sein, damit eventuell direkte Antworten - welche irrtümlich nicht über die GINA-Oberfläche erstellt wurden - gegebenenfalls angenommen werden.

Beispiel 1

Zeile	Code
01	<code>if (change webmail sender('GINA@meinefirma.tld')) {</code>
02	<code>log(1,'GINA carrier e-mail sender address successfully changed');</code>
03	<code>log(1,'trying to S/MIME sign GINA carrier e-mail');</code>
04	<code>if (has smime key()) {</code>
05	<code>log(1,'S/MIME key available, trying to sign');</code>
06	<code>if (sign smime()) {</code>
07	<code>log(1,'signing successful');</code>
08	<code>} else {</code>
09	<code>log(1,'signing failed');</code>
10	<code>}</code>
11	<code>} else {</code>
12	<code>log(1,'no signing key available');</code>
13	<code>}</code>
14	<code>} else {</code>
15	<code>log(1,'GINA carrier e-mail sender address could not be changed');</code>
16	<code>}</code>

Erklärung

In diesem Beispiel wird der Absender der Träger-E-Mail einer mittels GINA-Technologie verschlüsselten E-Mail zu GINA@meinefirma.tld geändert (**Zeile 01**).

Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert (**Zeile 02 und 15**). Nach erfolgreichem Ändern wird zusätzlich versucht, die GINA-Träger-E-Mail mit dem S/MIME key des neuen Absenders GINA@meinefirma.tld zu signieren (**Zeile 03 - 13**).

Somit können alle GINA-Träger-E-Mails mit nur einem S/MIME Schlüssel signiert werden.

8.6.11.3.3 pack_mail()

Der Befehl `pack_mail()` ermöglicht das Senden von GINA-Mails über ein abgekoppeltes GINA-Relay-System.

Dieser Befehl ermöglicht das Senden von GINA-Mails über ein abgekoppeltes GINA-Relay-System (vergleiche **Mail Processing** ^[288] **Ruleset generator** ^[287] **Advanced options** ^[310] **Use remote GINA server, reachable under the following e-mail address** ^[311]).

Aufbau des Befehls

```
pack_mail('e-mail_address', ['domainsignature']);
```

Rückgabewert

positiv bei erfolgreichem Weiterleiten der GINA-Anforderung an das GINA-Relay-System
negativ bei fehlgeschlagenem Weiterleiten der GINA-Anforderung an das GINA-Relay-System

Parameter

e-mail_address

Definiert die E-Mail Adresse unter welcher das GINA-Relay-System erreichbar ist.

domainsignature (optional)

Durch diesen Parameter wird die an das GINA-Relay-System weitergeleitete E-Mail zusätzlich mit einer Domänensignatur - ohne Prüfen des Absenders!!! - versehen.

Geprüft wird auf Empfängerseite (siehe **unpack_mail()** ^[599]) mittels Fingerabdruck des Domänen Zertifikates.

Mögliche Werte:

- true, yes oder 1
 - false, no oder 0
- Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	<code>if (pack mail('gina-relay@customer.org', 'yes')) {</code>
02	<code>log(1, 'mail successfully sent to remote GINA server');</code>
03	<code>} else {</code>
04	<code>log(1, 'mail could not delivered to remote GINA server');</code>
05	<code>drop('451', 'Die Nachricht konnte nicht verschluesselt werden');</code>
06	<code>}</code>

Erklärung

In diesem Beispiel wird die ausgehende E-Mail zur Weiterleitung an ein GINA-Relay-System gepackt, welches unter der (Pseudo) E-Mail Adresse „gina-relay@customer.org“ erreichbar ist und mit dem Domainzertifikat signiert (**Zeile 01**). Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert (**Zeile 02 und 04**). Bei fehlschlagen der Aktion wird die E-Mail mit dem temporären Fehler „451“ und dem Hinweistext „Die Nachricht konnte nicht verschluesselt werden“ abgewiesen (**Zeile 05**).

8.6.11.3.4 unpack_mail()

Der Befehl `unpack_mail()` entpackt auf einem GINA-Relay-System die vom Basis-System übermittelten GINA-Anforderungen.

Mit diesem Befehl werden die vom Basis-System mittels `pack_mail()` übermittelten GINA-Anforderungen angenommen (vergleiche **Mail Processing**, **Ruleset generator**, **Advanced options**, **This is a remote GINA server**).

Das weitere Verarbeiten der E-Mail findet im Anschluss statt.

Aufbau des Befehls

```
unpack_mail();
```

Rückgabewert

positiv immer

Parameter

keine

8.6.11.3.5 webmail_keys_avail()

Der Befehl `webmail_keys_avail()` prüft, ob für den Empfänger ein GINA Account vorhanden ist.

Aufbau des Befehls

```
webmail_keys_avail();
```

Rückgabewert

positiv für die Gruppe mit vorhandenem GINA Account
negativ für die Gruppe ohne GINA Account

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (webmail keys avail()) {</code>
02	<code>log(1,'GINA account already exists');</code>
03	<code>} else {</code>
04	<code>log(1,'no GINA account available, creating new account');</code>
05	<code>webmail keys gen('','8');</code>
06	<code>}</code>

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein GINA Account vorhanden ist (**Zeile 01**). Das Ergebnis dieser Abfrage wird protokolliert (**Zeile 02 und 04**). Ist kein GINA Account vorhanden, so wird ein neues angelegt (**Zeile 05**).

8.6.11.3.6 webmail_keys_gen()

Der Befehl `webmail_keys_gen()` erstellt einen GINA Account.

Dieser Befehl generiert ein GINA Account und schickt das Initial Kennwort an den Absender der ursprünglichen E-Mail oder alternativ an eine optional anzugebende E-Mail Adresse.

Aufbau des Befehls

```
webmail_keys_gen(['recipient'], ['password_length'], ['no_pw_mail_if_sms_sent']);
```

Rückgabewert

positiv immer

Parameter

recipient (optional)

Definiert die E-Mail Adresse, an welche die E-Mail mit dem Initial Kennwort gesendet werden soll.
Wird keine E-Mail Adresse angegeben, so wird die Absender E-Mail Adresse verwendet.

password_length (optional)

Definiert die Länge des Initial Kennworts. Dabei steht die „0“ (null) für ein leeres Kennwort.
Wird der Parameter nicht angegeben, so wird der Standardwert der Konfigurationsoberfläche (siehe [CHANGE GINA SETTINGS FOR](#) ^[425] [Initial password](#) ^[430] [Password length](#) ^[431]) verwendet.

no_pw_mail_if_sms_sent (optional)

Mit dieser Option ('1') wird die E-Mail mit dem Initial-Passwort an den Absender unterbunden, wenn dieses bereits per SMS übermittelt werden konnte (siehe auch Schlüsselwort [SMS:] in Tabelle 1 des Kapitels [Steuern der Appliance](#) ^[164]).

Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	<code>webmail keys_gen('', '8');</code>

Erklärung:

In diesem Beispiel wird ein GINA Account erzeugt. Der Absender der ursprünglichen E-Mail erhält eine E-Mail Benachrichtigung mit dem Initial Kennwort. Dieses Initial Kennwort hat '8' (acht) Zeichen.

Beispiel 2

Zeile	Code
01	<code>webmail keys_gen('', '', '1');</code>

Erklärung:

In diesem Beispiel wird ein GINA Account erzeugt. Die Passwort-Länge aus den Einstellungen der zum Einsatz kommenden GINA-Domain wird verwendet. Der Absender der ursprünglichen E-Mail erhält nur dann eine E-Mail Benachrichtigung mit dem Initial Kennwort für den Empfänger, sofern dieses nicht bereits per SMS gesendet werden konnte.

8.6.11.4 TLS

8.6.11.4.1 force_tls_domain()

Der Befehl `force_tls_domain()` auf eingerichtete TLS-Verschlüsselungen.

Dieser Befehl prüft, ob zur Ziel-E-Mail-Domäne eine TLS-Verschlüsselung in einer Ausprägung höher „may“ eingerichtet ist (siehe [Mail System](#) ^[247] [TLS settings](#) ^[251]).

Aufbau des Befehls

```
force_tls_domain();
```

Rückgabewert

positiv wenn TLS-Verschlüsselung mit einer höheren Ausprägung als „may“ eingerichtet ist
negativ wenn keine TLS-Verschlüsselung eingerichtet wurde oder die Ausprägung „none“ oder „may“ gewählt wurde.

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (force_tls_domain()) {</code>
02	<code>log(1, 'Mails to recipient(s) \$to are secured by forced TLS);</code>
03	<code>} else {</code>
04	<code>drop('500', 'Mails to recipient(s) \$to are NOT secured by forced TLS);</code>
05	<code>}</code>

Erklärung

In diesem Beispiel werden die Empfänger der zu sendenden E-Mail in zwei Gruppen geteilt (**Zeile 01**). Für die Gruppe der Empfänger, zu welchen TLS-Verschlüsselung höher „may“ eingerichtet ist, wird dies entsprechend in das Log eingetragen (**Zeile 02**). Ist für die Empfänger Domäne keine TLS-Verschlüsselung eingerichtet oder die Ausprägung „none“ oder „may“ gewählt, wird die E-Mail abgewiesen (**Zeile 04**).

8.6.12 Content Management

8.6.12.1 iscalendar()

Der Befehl `iscalendar()` prüft, ob es sich bei einer E-Mail um einen Kalendereintrag handelt.

Der Befehl prüft, unter anderem anhand des Mime-Type **text/calendar**, ob es sich bei einer E-Mail um einen Kalendereintrag - zum Beispiel Einladungen, Termine, Besprechungsanfragen oder die jeweiligen Zu/Absagen - handelt. Diese Abfrage wird typischerweise für das anschließende Unterbinden kryptographischer Aktionen bei Kalendereinträgen verwendet, da viele E-Mail Clients damit nicht umgehen können.

RTF-formatierte E-Mails werden ebenfalls als Kalendereinträge erkannt.

Aufbau des Befehls

```
iscalendar();
```

Rückgabewert

positiv wenn es sich bei der E-Mail um einen Kalendereintrag handelt
negativ wenn es sich bei der E-Mail nicht um einen Kalendereintrag handelt

Parameter

keine

Beispiel 1

Zeile	Code
01	<code>if (iscalendar()) {</code>
02	<code> log(1, 'meeting request, do not sign');</code>
03	<code> tagsubject('@NOSIGNTXT@');</code>
04	<code>}</code>

Erklärung

In diesem Beispiel wird über den Befehl `iscalendar()` (**Zeile 01**) geprüft, ob es sich bei der E-Mail um einen Kalendereintrag handelt. Wenn dem so ist, so wird dies im Log eingetragen (**Zeile 02**) und mittels `tagsubject()` ⁵⁶⁶ als nicht zu signierend (`@NOSIGNTXT@` ⁶³⁷) (**Zeile 03**) markiert.

8.6.12.2 issпам()

Der Befehl `issпам()` prüft, ob es sich bei einer E-Mail um SPAM handelt.

Dieser Befehl ist nur bei aktiviertem Protection Pack verfügbar. Er prüft den SPAM Level einer E-Mail und führt die entsprechend der eingestellten Schwellwerte definierte Aktion aus (Markieren oder Abweisen).

(siehe auch [Mail Processing](#)^[286], [Ruleset generator](#)^[287], [Protection Pack \(Anti-Spam / Anti-Virus\)](#)^[303]).



Achtung:

ist die Option **Use antispam Engine (Note: remember to activate in ruleset)**^[256] aus [Mail System](#)^[247] [Antispam](#)^[255] deaktiviert, so würde keine Spam-Erkennung stattfinden.

E-Mails, welche 5 MB überschreiten werden nicht geprüft um Timeouts zu vermeiden. Ein entsprechender Log Eintrag wird generiert.

Aufbau des Befehls

```
issпам('mark_level','tag','reject_level');
```

Rückgabewert

positiv immer

Parameter

mark_level

Dieser Parameter definiert den Punktwert, ab welchem eine E-Mail als SPAM E-Mail markiert wird.

Wertebereich: 0.5 - 19.5

Schrittweite: 0.5

Markieren heißt dem Betreff einer E-Mail wird ein entsprechendes Merkmal hinzugefügt. Dieses Merkmal wird mittels dem Parameter `tag` definiert

tag

Dieser Parameter definiert einen Wortbestandteil (`tag`) der zur Markierung einer E-Mail als SPAM an den Betreff angehängt wird.

reject_level

Dieser Parameter definiert den Punktwert, ab welchem eine E-Mail als SPAM E-Mail abgewiesen wird.

Wertebereich: 0.5 - 19.5

Schrittweite: 0.5

Beispiel 1

Zeile	Code
01	<code>issпам('2.5','[SPAM]','4.5');</code>

Erklärung

In diesem Beispiel wird eine E-Mail auf SPAM überprüft. Wird der SPAM Schwellwert von „2.5“ erreicht, bleibt jedoch unter „4.5“, so wird die E-Mail im Betreff mit dem Hinweis „[SPAM]“ gekennzeichnet. Ab Erreichen des Schwellwertes 4.5 wird die E-Mail abgewiesen (rejected).

8.6.12.3 partoftype()

Der Befehl `partoftype()` ermittelt den Dateityp von E-Mail Dateianhängen.

Dieser Befehl prüft Dateianlagen anhand des Inhalts der Datei, ob diese einem bestimmten Datei-Typ entsprechen. Ist dies der Fall, so wird eine definierte Aktion ausgeführt. Die Inhalte von Archivdateien können ebenfalls durchsucht werden.

Aufbau des Befehls

```
partoftype('type','action','check_archive');
```

Rückgabewert

positiv wenn der angegebene MIME Type in der/den Anlage(n) der E-Mail gefunden wurde
negativ wenn keine Anlage des genannten MIME Types gefunden wurde

Parameter

type

Weitere Informationen zum Parameter **type** sind im Abschnitt [Liste von MIME Typen](#) ^[60] zu finden. Dabei können Dateitypen ebenso durch Komma getrennt eingefügt werden, wie ganze Typ-Gruppen.

Die Listen [Liste der Dateitypen](#) ^[61] und [Liste von Dateigruppen](#) ^[61], welche vor 7.4.2 zum Einsatz kamen werden aus Kompatibilitätsgründen weiterhin unterstützt, jedoch nicht weiter gepflegt.

Auch das Definieren von Ausnahmen ist durch Voranstellen eines Ausrufungszeichens „!“ möglich. Ausnahmen müssen grundsätzlich am Anfang des Parameters stehen.

action

Mögliche Werte

- info stellt das Resultat für die folgenden Befehle zu Verfügung
 - delete entfernt zusätzlich die entsprechende Dateianlage aus der E-Mail
- Standardeinstellung ist `info`

check_archive

Durch Anschalten dieses Parameter wird der angegebene MIME **type** zusätzlich in Archivdateien gesucht. Bei einem Fund innerhalb eines Archivs bei gleichzeitiger Aktionseinstellung „delete“, wird nur die entsprechende Datei aus dem Archiv entfernt. Das Archiv selbst bleibt erhalten.

Mögliche Werte:

- true, yes oder 1
 - false, no oder 0
- Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	<code>partoftype('!zip,application/msword,application/pdf,video','delete','true');</code>

Erklärung

In diesem Beispiel wird eine E-Mail auf das Vorhandensein von Dateianhängen der Typen 'application/msword' und 'application/pdf', sowie der Gruppe „video“, mit Ausnahme von Dateien mit der Endung „zip“ überprüft. Wird ein Dateianhang eines genannten MIME-Typs beziehungsweise eine MIME-Type Gruppe gefunden, so wird dieser aus der E-Mail entfernt. Enthält die E-Mail als Dateianhang eine Archivdatei, so wird diese ebenfalls durchsucht und betroffene Dateien entfernt.

8.6.12.3.1 Liste von MIME Typen

Folgende MIME-Types werden unterschieden:

Group/Type	Beschreibung
application	Wird „application“ als Gruppe verwendet, so beinhaltet dies alle mit „application/“ beginnenden MIME-Types.
application/dicom	
application/mac-binhex40	
application/msword	
application/octet-stream	
application/ogg	
application/pdf	
application/pgp	
application/pgp-keys	
application/pgp-signature	
application/postscript	
application/vnd.lotus-wordpro	
application/vnd.ms-excel	
application/vnd.ms-tnef	
application/vnd.oasis.opendocument.text	
application/vnd.rn-realmedia	
application/vnd.symbian.install	
application/x-123	
application/x-arc	
application/x-archive	
application/x-arj	
application/x-awk	
application/x-bittorrent	
application/x-bzip2	
application/x-coredump	
application/x-cpio	
application/x-dbm	
application/x-debian-package	
application/x-dosexec	
application/x-dvi	
application/x-eet	
application/x-elc	
application/x-executable	
application/x-gawk	
application/x-gdbm	
application/x-gnucash	
application/x-gnumeric	
application/x-gnupg-keyring	
application/x-gzip	
application/x-hdf	
application/x-hwp	

Group/Type	Beschreibung
application/x-ichitaro4	
application/x-ichitaro5	
application/x-ichitaro6	
application/x-iso9660-image	
application/x-java-applet	
application/x-java-jce-keystore	
application/x-java-keystore	
application/x-java-pack200	
application/x-kdelnk	
application/x-lha	
application/x-lharc	
application/x-mif	
application/x-ms-reader	
application/x-msaccessapplication/x-nawk	
application/x-object	
application/x-perl	
application/x-pgp-keyring	
application/x-quark-xpress-3	
application/x-quicktime-player	
application/x-rar	
application/x-rpm	
application/x-sc	
application/x-sharedlib	
application/x-shellscrip	
application/x-shockwave-flash	
application/x-stuffit	
application/x-svr4-package	
application/x-tar	
application/x-tex-tfm	
application/x-zoo	
application/zip	
audio	Wird „audio“ als Gruppe verwendet, so beinhaltet dies alle mit „audio/“ beginnenden MIME-Types.
audio/basic	
audio/midi	
audio/mp4	
audio/mpeg	
audio/x-adpcm	
audio/x-aiff	
audio/x-dec-basic	
audio/x-flac	
audio/x-hx-aac-adif	
audio/x-hx-aac-adts	
audio/x-mod	
audio/x-mp4a-latm	

Group/Type	Beschreibung
audio/x-pn-realaudio	
audio/x-unknown	
audio/x-wav	
image	Wird „image“ als Gruppe verwendet, so beinhaltet dies alle mit „image/“ beginnenden MIME-Types.
image/gif	
image/jp2	
image/jpeg	
image/png	
image/svg+xml	
image/tiff	
image/vnd.adobe.photoshop	
image/vnd.djvu	
image/x-coreldraw	
image/x-cpi	
image/x-ico	
image/x-ms-bmp	
image/x-niff	
image/x-portable-bitmap	
image/x-portable-greymap	
image/x-portable-pixmap	
image/x-quicktime	
image/x-unknown	
text	Wird „text“ als Gruppe verwendet, so beinhaltet dies alle mit „text/“ beginnenden MIME-Types.
text/PGP	
text/html	
text/rtf	
text/texmacs	
text/troff	
text/x-fortran	
text/x-info	
text/x-tex	
text/x-texinfo	
text/x-vcard	
text/x-xmcd	
video	
video/3gpp	
video/h264	
video/mp2p	
video/mp2t	
video/mp4	
video/mp4v-es	
video/mpeg	
video/mpv	

Group/Type	Beschreibung
video/quicktime	
video/x-flc	
video/x-fli	
video/x-flv	
video/x-jng	
video/x-mng	
video/x-msvideo	
video/x-sgi-movie	
Exoten	Die unter „Exoten“ gelisteten MIME-Types können nicht über eine Gruppe ausgewählt werden
message/news	
message/rfc822	
model/vrml	
x-epoc/x-sisx-app	

Liste der Dateitypen

8.6.12.3.2 Liste der Dateitypen (veraltet)

Folgende Dateitypen wurden bis Version 7.4.1 unterschieden:

ID	Beschreibung
BMP	PC Bitmap
BZIP	BZIP Compressed
CAB	Microsoft CAB file
COM	MSDOS Computable
EMF	Enhanced Windows Metafile
EXE	MSDOS Executable
FAX	G3 Fax
GIF	GIF Image
GZIP	GZIP Compressed
ICO	Windows Icon
ISO9660	ISO 9660 CD-ROM
JPEG	JPEG Image
JPG2000	JPEG 2000 Image
LHA	LHa 2.x? Archive
LHARC	LHarc 1.x Archive
LWF	LuraWave Image
MPEG.L3	MPEG Layer 3
MPEG.SYS	MPEG System Stream
MPEG.VID	MPEG Video
MS.ASF	Microsoft ASF
MS.OFF	MS Office document
MS.XLS	MS Excel 5.0 Worksheet
NIFF	NIFF Image
PBMPLUS	PBMPLUS Bitmap
PCX	Z-Soft Image
PDF	PDF Document
PNG	PNG Image
RAR	RAR Archive
RIFF.ANI	MS RIFF Animated Cursor
RIFF.AVI	MS RIFF Audio Video Interleave
RIFF.DIB	MS RIFF DIB Bitmap
RIFF.MID	MS RIFF MIDI File
RIFF.MMF	MS RIFF Multimedia Movie
RIFF.WAV	MS RIFF Wave Audio
RTF	Rich Text Format
TAR	TAR Archive
TARGA	TARGA Bitmap
TIFF	TIFF Image
ZIP	PKZIP Archive
ZOO	Zoo Archive

Liste der Dateitypen

Mit Versionen ab 7.4.2 werden diese Dateitypen aus Kompatibilitätsgründen zwar weiterhin unterstützt, jedoch nicht mehr weiter gepflegt. Das heißt es werden seitens SEPPmail keine weiteren, neuen Dateitypen hinzugefügt, beziehungsweise obsoleete Dateitypen entfernt.

8.6.12.3.3 Liste von Dateigruppen (veraltet)

Folgende Gruppen von Dateitypen wurde bis Version 7.4.1 unterschieden:

ID	Beschreibung	Beinhaltete Dateitypen
ARCHIVES	Archivdateien	ZIP ZIP.SFX RAR LHARC LHA SQUISH UC2 ZOO TAR CAB BZIP GZIP
EXE	Ausführbare Dateien	EXE.PE EXE.COM
FS	Dateisysteme	ISO9660 HISIERRA
IMAGES	Bilder	JPEG BMP TIFF PNG GIF TARGA PBMPLUS NIFF FAX PCX LWF ICO JPG2000 EMF
MEDIA	Multimedia	RIFF.WAV RIFF.AVI RIFF.ANI RIFF.MID RIFF.MMF RIFF.DIB RIFF.RIFX MPEG.VID MPEG.SYS MPEG.L3 MS.ASF
OFFICE	Office-Dokumente	RTF PDF MS.OFF MS.XLS

Gruppen von Dateitypen

Mit Versionen ab 7.4.2 werden diese Gruppen aus Kompatibilitätsgründen zwar weiterhin unterstützt, jedoch nicht mehr weiter gepflegt. Das heißt es werden seitens SEPPmail keine weiteren, neuen Dateitypen hinzugefügt.

8.6.12.4 vscan()

Der Befehl `vscan()` prüft die gesamte E-Mail auf Viren.

Dieser Befehl ist nur bei aktiviertem Protection Pack verfügbar. Er prüft eine E-Mail (Dateianlagen sowie E-Mail Text und Betreff) auf Viren und sendet eine Benachrichtigung an eine zu definierende E-Mail Adresse.

(siehe auch [Mail Processing](#) ^[266], [Ruleset generator](#) ^[287], [Protection Pack \(Anti-Spam / Anti-Virus\)](#) ^[303]).

Aufbau des Befehls

```
vscan(['notification_e-mail_address'], ['restrictive_[value_1]|[value_2]|[value_n]'], ['exclude_[value_1]|[value_2]|[value_n]']);
```

Rückgabewert

positiv wenn das Ergebnis mindestens einer Prüfung der Dateianlagen einer E-Mail positiv (Virenfund) ist
negativ wenn kein Virus in der E-Mail gefunden wurde.



Achtung:

Ist die Option **Use AntiVirus Engine (Note: remember to activate in ruleset)** ^[256] aus **Mail System** ^[247] **Antispam** ^[255] deaktiviert, so würden E-Mails als „Virus-frei“ weitergeleitet.

Dateien, welche 1 GB überschreiten werden nicht gescannt um Timeouts zu vermeiden. Ein entsprechender Log Eintrag wird generiert.

Rückgabe Variable

\$vscanresult gibt das Ergebnis des Scans aus

Parameter

notification_e-mail_address (optional)

Definiert die E-Mail Adresse an welche bei Virenfund eine Benachrichtigung gesendet wird.

restrictive

Erkennt die angegebenen Inhalte ebenfalls als Malware. Die Eingabe erfolgt als Regulärer Ausdruck.

Mögliche Werte

- (Broken.Executable) schadhafte ausführbare Dateien.
- (Heuristics.Encrypted) verschlüsselte Inhalte (zum Beispiel verschlüsselte ZIP Dateien)
- (Heuristics.Phishing.Email) per Heuristik erkannte Phishing E-Mails
- ... siehe gegebenenfalls www.clamav.net

exclude

Für den Fall, dass ClamAV nach einem Signatur-Update sogenannte false positive Meldungen erzeugt, können an dieser Stelle Ausnahmen vom Virens캔 definiert werden. Dies können

- heuristische Teil-Prüfungen sein (siehe gegebenenfalls www.clamav.net)
- einzelne Viren Namen, wie sie dem Log zu entnehmen sind

sein.

Beispiel 1

Zeile	Code
01	<code>vscan('antivirus-admin@customer.com');</code>

Erklärung

In diesem Beispiel wird eine E-Mail Benachrichtigung an 'antivirus-admin@customer.com' gesendet, wenn ein Virus gefunden wurde.

8.6.12.5 whitelist_recipients()

Der Befehl `whitelist_recipients()` trägt die Empfänger einer E-Mail in die auf dem System geführte Whitelist ein.

Dieser Befehl ist nur bei aktiviertem Protection Pack verfügbar. Durch den Befehl werden die Empfänger einer E-Mail whitelisted und somit als reale Kommunikationspartner gekennzeichnet. Wird im Anschluss eine E-Mail von einer dieser Adressen empfangen, wird aufgrund des whitelisting kein Spam Check vorgenommen. Der Einsatz dieses Befehls empfiehlt sich deshalb vor allem bei ausgehenden E-Mails.

Aufbau des Befehls

```
whitelist_recipients();
```

Rückgabewert

positiv immer

Parameter

keine

Beispiel 1

Zelle	Code
01	if (!incoming()) {
02	whitelist_recipients();
03	}

Erklärung

In **(Zeile 01)** wird geprüft, ob es sich um eine ausgehende E-Mail handelt. Ist dies der Fall, wird die Bedingung aus **(Zeile 02)** `whitelist_recipients();` ausgeführt, wodurch alle (externen) Empfänger der E-Mail whitelisted werden.

8.7 Zugriff auf externe LDAP-Verzeichnisse

Beim Verwenden von LDAP Anfragen wird grundsätzlich nur beim ersten Aufruf die Verbindung zum LDAP hergestellt und dann gehalten (cached). Dadurch wird Performance-Engpässen durch häufigen Verbindungsaufbau zum LDAP-Server vorgebeugt. Unterstützt wird sowohl LDAP als auch LDAPS.

8.7.1 ldap_init()

Der Befehl `ldap_init()` leert den LDAP Cache.

Dieser Befehl leert den LDAP Cache, sofern dieser in Verbindung mit einem der LDAP Befehle `ldap_read()` ^[617] oder `ldap_compare()` ^[620] zu Problemen führt.

Hintergrund:

Die beiden oben genannten Befehle bauen jeweils bei der ersten Abfrage eine Verbindung zum LDAP-Server auf und halten diese Verbindung für weitere Abfragen offen. Dadurch wird die Performance des LDAP-Servers möglichst wenig beeinträchtigt. Ruft dieses Verhalten jedoch Probleme hervor, zum Beispiel bei Einsatz einer zwischengeschalteten Firewall, welche die Verbindung nach einer Zeit x trennt und somit ein sauberes Beenden der Verbindung unterbindet, kann dem mittels `ldap_init()` entgegengewirkt werden.

Dies hat dann jedoch zur Folge, dass mit jeder LDAP Abfrage eine neue Verbindung zum LDAP-Server aufgebaut wird.

Aufbau des Befehls

```
ldap_init();
```

Rückgabewert

positiv immer

Parameter

keine

8.7.2 ldap_read()

Der Befehl `ldap_read()` liest einen Wert aus einem LDAP-Verzeichnis aus und legt diesen in einer Variablen ab.

Dieser Befehl baut eine Verbindung zu einem LDAP-Server auf, liest den Wert eines Attributs aus und legt diesen in einer Variable ab.

Wird keiner der angegebenen LDAP-Server erreicht, so wird die E-Mail mit einem temporären Fehler abgewiesen (420, could not bind to LDAP server).

Aufbau des Befehls

```
ldap_read('ldap', 'attr', 'var');
```

Rückgabewert

positiv wenn das Attribut `'attr'` gefunden und somit der Variablen `'var'` ein Wert zugewiesen werden kann

negativ wenn der Variablen `'var'` kein Wert zugewiesen werden kann

Parameter

Variablen  verfügbar!



Achtung:

Die Inhalte der Variablen im Parameter „Filter“ weichen von den Standard-**Variablen**  ab!

ldap

Der Parameter ist wie folgt aufgebaut:

'URI;BindDN;Password;SearchBase;Filter'

Die Bedeutung der einzelnen Teil Strings ist der folgenden Tabelle beschrieben:

Parameter	Beschreibung
URI	Angabe des LDAP-Servers, der abgefragt werden soll. Als Eingabe wird der Hostname oder die IP-Adresse akzeptiert. Es können auch zwei mit Komma getrennte Werte angegeben werden: In diesem Fall wird automatisch auf den zweiten Server zugegriffen, wenn der erste nicht erreicht werden kann. Hinweis:  ist mehr als ein LDAP Server eingetragen, so wird für jeden einzelnen Server eine Verbindung aufgebaut. Die Verbindungen werden zwischengespeichert. Die eigentliche Abfrage wird dann in der eingegebenen Reihenfolge der Server ausgeführt, bis die Abfrage erfolgreich ist. War eine Abfrage erfolglos, so wird die Verbindung aus dem Zwischenspeicher entfernt. Ist keine verbleibende Verbindung im Zwischenspeicher, so werden die Verbindungen neu aufgebaut.
BindDN	Eingabe des vollständigen Distinguished Name (DN) des (read-only) Accounts, welcher zur Suche des unter „SearchBase“ im LDAP Verzeichnis berechtigt ist.
Password	Das Passwort des unter BindDN angegebenen Benutzers Hinweis:  Semikolons „;“, und Backslashes „\“ im Password müssen jeweils mit einem Backslash als Sonderzeichen gekennzeichnet werden, also „\\“, beziehungsweise „\\“. Somit müsste beispielsweise das Passwort p4ss\\w0rd; wie folgt eingegeben werden: p4ss\\w0rd\;
SearchBase	Suchpfad: Gibt den Zweig des LDAP Verzeichnisses an, in welchem mittels Suchfilter (siehe nächste Zeile) rekursiv nach dem Objekt gesucht werden soll, aus welchem das Attribut 'attr' ausgelesen werden soll.
Filter	Angabe des Such-Attributes /-Wertes, mittels welchem im Zweig der „SearchBase“ nach dem Objekt zu suchen ist. Das Such-Attribut ist in der Regel „(mail=...)“. Für das Auswerten der E-Mail Adresse(n) stehen die im Folgenden genannten Variablen zur Verfügung. Variablen Achtung:  Die Inhalte der hier genannten Variablen weichen von den Standard-Variablen ^[508] ab! Würde der Parameter 'ldap' also zum Beispiel mit einer mittels setvar() ^[522] geschriebenen Variable befüllt, so können Abweichungen beim Verarbeiten auftreten. \$from Diese Variable gibt die E-Mail Adresse des Absenders aus dem FROM-Header der E-Mail aus. Ist der Sender des FROM-Headers nicht intern - also keiner Managed domain ^[247] zuzuordnen - so wird auf das Vorhandensein des SENDER-Headers geprüft. Ist dieser vorhanden und der darin enthaltene Sender intern, so wird dieser anstatt des Senders aus dem FROM-Header ausgegeben. Dadurch werden Probleme, zum Beispiel beim Weiterleiten von Kalendereinladungen, vermieden. <i>Rückgabewert bei Verwenden dieser Variable</i> positiv wenn ein entsprechendes Objekt mit dem angegebenen Attribut 'attr' im, mittels LDAP Suchstring (ldap/Filter) abgegebenen Pfad, gefunden wurde. negativ wenn kein entsprechender Wert gefunden wurde. Achtung:  Vor dem Verwenden von <code>ldap_read()</code> mit den folgenden Variablen, ist zwingend ein <code>splitrecipients()</code> ^[565] erforderlich, um das Schreiben der Variable 'var' pro Empfänger gewährleisten zu können.
© 2021 SEPPmail AG	\$one_recipient Enthält eine E-Mail mehrere Empfänger, so wird für <u>alle Empfänger</u> nach einem Objekt mit dem angegebenen Attribut 'attr' im LDAP Suchstring (ldap/Filter) gesucht. <i>Rückgabewert bei Verwenden dieser Variable</i> positiv wenn <u>mindestens für einen Empfänger</u> ein entsprechendes Objekt mit dem angegebenen Attribut 'attr' im, mittels LDAP Suchstring (ldap/Filter) abgegebenen Pfad, gefunden wurde. negativ wenn für <u>keinem Empfänger</u> ein entsprechendes Objekt/Attribut gefunden

attr

Attribut, dessen Wert nach erfolgreicher Suche (siehe (**ldap**/Filter)) ausgelesen werden soll.

var

Name der Variablen, in welcher der Wert des Attributes '**attr**' abgelegt werden soll

Beispiel 1

Der Wert des Attributs „Name“ soll aus einem LDAP-Verzeichnis ausgelesen werden. Dieser soll in der Variable „name_from_ldap“ abgespeichert werden.

Die Anweisung sieht wie folgt aus:

Zeile	Code
01	<code>ldap_read('ldaps://directory.domain.tld;CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local;mypassword;OU=SBSUsers,OU=Users,OU=MyBusiness,DC=firma,DC=local;(mail=\$sender)', 'name', 'name from ldap');</code>

Erklärung

Der LDAP-Server mit der IP-Adresse 192.168.10.10 (und dem Standardport 389) wird abgefragt.

Der DistinguishedName (DN) des Benutzers (Peter Mueller) unter welchem die Abfrage ausgeführt wird (dieser muss die entsprechenden Berechtigungen besitzen) lautet

CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local

Das Passwort dieses Benutzers lautet

mypassword

Der LDAP Pfad, in welchem nach dem Attribut „**name**“ gesucht werden soll lautet

OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local

Der Benutzer, dessen Gruppenzugehörigkeit festgestellt werden soll, wird anhand der Absender E-Mail Adresse (**ldap**/Filter) definiert.

Existiert das angegebene Attribut '**attr**' oder der gesuchte Eintrag nicht, so wird der Variable '**var**' ein leerer Wert zugewiesen.

Werden mehrere Einträge (Objekte) im Attribut '**attr**' gefunden, so wird nur der erste ausgewertet.

Sollten mehrere Attribute '**attr**' vorhanden sein, so werden alle Attribute ausgewertet (multi value).

Wird keiner der angegebenen LDAP-Server erreicht, so wird die E-Mail mit einem temporären Fehler abgewiesen.

8.7.3 ldap_compare()

Der Befehl `ldap_compare()` vergleicht einen vorgegebenen Wert mit dem Wert eines LDAP-Attributs.

Dieser Befehl baut eine Verbindung zu einem LDAP-Server auf und prüft den Wert eines Attributs.

Wird keiner der angegebenen LDAP-Server erreicht, so wird die E-Mail mit einem temporären Fehler abgewiesen (420, could not bind to LDAP server).

Aufbau des Befehls

```
ldap_compare('ldap','attr','value');
```

Rückgabewert

Der Rückgabewert ist abhängig von der verwendeten Variable im LDAP-Suchstring

Parameter

`Variable`^[506] verfügbar!



Achtung:

Die Inhalte der Variablen im Parameter „Filter“ weichen von den Standard-`Variable`^[506] ab!

ldap

Der Parameter ist wie folgt aufgebaut:

'URI;BindDN;Password;SearchBase;Filter'

Die Bedeutung der einzelnen Teil Strings ist der folgenden Tabelle beschrieben:

Parameter	Beschreibung
URI	Angabe des LDAP(S)-Servers, der abgefragt werden soll. Als Eingabe wird der Hostname oder die IP-Adresse akzeptiert. Es können auch Komma getrennte Werte angegeben werden. In diesem Fall wird automatisch auf den jeweils nächsten Server zugegriffen, wenn der erste nicht erreicht werden kann. Hinweis:  ist mehr als ein LDAP Server eingetragen, so wird für jeden einzelnen Server eine Verbindung aufgebaut. Die Verbindungen werden zwischengespeichert. Die eigentliche Abfrage wird dann in der eingegebenen Reihenfolge der Server ausgeführt, bis die Abfrage erfolgreich ist. War eine Abfrage erfolglos, so wird die Verbindung aus dem Zwischenspeicher entfernt. Ist keine verbleibende Verbindung im Zwischenspeicher, so werden die Verbindungen neu aufgebaut.
BindDN	Eingabe des vollständigen Distinguished Name (DN) des (read-only) Accounts, welcher zur Suche des unter „SearchBase“ angegebenen Pfades der LDAP Verzeichnisstruktur berechtigt ist.
Password	Das Passwort des unter BindDN angegebenen Benutzers Hinweis:  Semikolons „;“, „\“ und Backslashes „\“ im Password müssen jeweils mit einem Backslash als Sonderzeichen gekennzeichnet werden, also „\\“, beziehungsweise „\\\\“. Somit müsste beispielsweise das Passwort p4ss\\w0rd; wie folgt eingegeben werden: p4ss\\\\w0rd\\;
SearchBase	Suchpfad: Gibt den Zweig des LDAP Verzeichnisses an, in welchem mittels Suchfilter (siehe nächste Zeile) rekursiv nach dem Objekt gesucht werden soll, in welchem auf Vorhandensein des Attributs 'attr' mit dem angegebenen Wert 'value' geprüft werden soll.
Filter	Angabe des Such-Attributs /-Wertes, mittels welchem im Zweig der „SearchBase“ nach dem Objekt suchen ist. Das Such-Attribut ist in der Regel „(mail=...)“. Für das Auswerten der E-Mail Adresse(n) stehen die im Folgenden genannten Variablen zur Verfügung. Variablen  Achtung: Die Inhalte der hier genannten Variablen weichen von den Standard-Variablen ⁵⁰⁸ ab! Würde der Parameter 'ldap' also zum Beispiel mit einer mittels setvar() ⁵²² geschriebenen Variable befüllt, so können Abweichungen beim Verarbeiten auftreten. \$sender Diese Variable gibt den Envelope Absender der E-Mail aus. <i>Rückgabewert bei Verwenden dieser Variable</i> positiv wenn der Wert 'value' für das angegebene Attribut 'attr', im mittels LDAP Suchstring (ldap/Filter) gefundenen Objekt, vorhanden ist. negativ wenn kein entsprechender Wert gefunden wurde.  Achtung: Da bei System E-Mails wie zum Beispiel auch Out Of Office (OOO) Meldungen kein Envelope Sender eingetragen ist, würde die Abfrage mit dieser Variable scheitern. Deshalb wird in diesem Fall das Verwenden von \$from empfohlen. \$from Diese Variable gibt die E-Mail Adresse des Absenders aus dem FROM-Header der E-Mail aus. Dies ist insbesondere bei Abwesenheitsmeldungen notwendig, da in diesen kein Envelope-Sender gesetzt ist. Ist der Sender des FROM-Headers nicht intern - also keiner Managed domain ⁷⁴ Mail AG zuzuordnen - so wird auf das Vorhandensein des SENDER-Headers geprüft. Ist dieser vorhanden und der darin enthaltene Sender intern, so wird dieser anstatt des Senders aus dem FROM-Header ausgegeben. Dadurch werden Probleme beim Weiterleiten von Kalendereinladungen vermieden. <i>Rückgabewert bei Verwenden dieser Variable</i> positiv wenn der Wert 'value' für das angegebene Attribut 'attr', im mittels

attr

Attribut nach welchem im LDAP-Verzeichnis gesucht werden soll.

**Hinweis:**

Sollten mehrere Attribute '**attr**' mit dem gesuchten Namen gefunden werden, so werden alle Attribute ausgewertet (multi value).

value

Wert, welcher im abgefragten Attribut '**attr**' vorkommen soll.

**Hinweis:**

Enthält '**value**' mehrere Einträge, so wird die Suche nach der ersten Übereinstimmung beendet.

Der Vergleich findet case-sensitive statt.

Beispiel 1

Die Zugehörigkeit des internen Absenders einer E-Mail „(mail=\$from)“ zur Gruppe „MailCrypt“ soll im LDAP anhand des **im envelope** der E-Mail eingetragenen Absenders geprüft werden, zum Beispiel um festzustellen, ob dieser berechtigt ist, kryptographisch behandelte E-Mails zu senden.

Die Anweisung sieht wie folgt aus:

Zeile	Code
01	<code>if (ldap_compare('192.168.10.10;CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local;mypassword;OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local;(mail=\$from)', 'memberOf', 'MailCrypt')) {</code>
02	<code>log(1, 'Mitglied der AD-Gruppe MailCrypt, markiere E-Mail für Signatur');</code>
03	<code>tagsubject('[sign]');</code>
04	<code>} else {</code>
05	<code>log(1, 'nicht Mitglied der AD-Gruppe Exchange, liefere unbehandelt aus');</code>
06	<code>deliver();</code>
07	<code>}</code>

Erklärung**In (Zeile 01) wird**

- der LDAP-Server mit der IP-Adresse 192.168.10.10 (und dem Standardport 389) wird abgefragt.
- der DistinguishedName (DN) des Benutzers unter welchem die Abfrage ausgeführt wird (dieser muss die entsprechenden Berechtigungen besitzen) lautet
CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local
- das folgende Passwort für diesen Benutzers verwendet
mypassword
- der LDAP Pfad, in welchem der Suchfilter (mail=\$sender) angewendet werden soll lautet
OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local
- der Benutzer, dessen Gruppenzugehörigkeit festgestellt werden soll, anhand der Absender E-Mail Adresse aus dem **FROM-Header** der E-Mail (mail=\$from) festgestellt.

Mindestens ein Wert des Attributes „memberOf“ muss den Wert „MailCrypt“ haben, damit der Rückgabewert **positiv** ist, und somit der Anwendungsblock aus (Zeile 02, 03) ausgeführt wird. Ist der Wert „MailCrypt“ nicht im Attribut, beziehungsweise das Attribut „memberOf“ nicht vorhanden, so ist der Rückgabewert **negativ**, wodurch der Anwendungsblock (Zeile 05, 06) ausgeführt wird.

Beispiel 1a

Die Parameter 'ldap' und 'attr' (Zeile 02) werden aus einer zuvor definierten Variable \$ldap_attr (Zeile 01) ausgelesen.

Zeile	Code
01	if (compare('from','match','@customer1.tld') {
02	setvar('ldap_attr','ldaps://directory.domain.tld;CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local;mypassword;OU=SBSUsers,OU=Users,OU=MyBusiness,DC=firma,DC=local;(mail=\$header from)');
03	}
04	if (ldap compare('\$ldap_attr','memberOf','MailCrypt')) {
05	...
06	}

Erklärung

Dies ist insbesondere in mandantenfähigen Systemen hilfreich. So kann zunächst anhand der Absenderadresse der Zugang zu dem zum Mandanten gehörigen LDAP definiert werden. Die eigentliche LDAP-Verzweigung bleibt dann für alle Mandanten identisch.



Achtung:

Bei diesem Beispiel ist zu beachten, dass für ldap_compare() der FROM-Header (mail=\$from) verwendet werden soll.

Da setvar() jedoch die Standard-Variable `506` verwendet und bereits mit dem Schreiben der Variable auflöst, muss im Befehl setvar() die Variable \$header_from verwendet werden.

Beispiel 2

Die Zugehörigkeit des internen Absenders einer E-Mail „(mail=\$sender)“ zur Gruppe „MailCrypt“ soll im LDAP anhand des im **FROM-Header** der E-Mail eingetragenen Absenders geprüft werden, zum Beispiel um festzustellen, ob dieser berechtigt ist, kryptographisch behandelte E-Mails zu senden.

Die Anweisung sieht wie folgt aus:

Zeile	Code
01	ldap_compare('ldaps://192.168.10.10;CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=firma,DC=local;mypassword;OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local; (mail=\$sender)', 'memberOf', 'MailCrypt');

Erklärung

Prinzipiell macht der Ausdruck in diesem Beispiel das gleiche wie der in Beispiel 1 (Zeile 01), mit dem Unterschied, dass statt im FROM-Header im **Envelope** der E-Mail nach dem Absender gesucht wird.

Beispiel 3

Ausgangspunkt sind zwei unterschiedliche Groupware- (interne E-Mail) Server (zum Beispiel Exchange und Domino), welche parallel eingesetzt werden.

Abgefragt soll werden, ob das Postfach wenigstens eines internen Empfängers einer eingehenden E-Mail - mit gegebenenfalls mehreren Empfängern - ein Exchange Postfach ist.

Die Anweisung sieht wie folgt aus:

Zeile	Code
01	if (ldap_compare('ldap://192.168.10.10,ldap://192.168.10.11;CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=firma,DC=local;mypassword;OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local; (mail=\$rcptaddress)', 'MailServerGruppe', 'Exchange')) {
02	log(1, 'Mitglied der AD-Gruppe Exchange');
03	} else {
04	log(1, 'nicht Mitglied der AD-Gruppe Exchange');
05	}

Erklärung

Im LDAP Suchpfad (SearchBase) wird der Suchfilter (Filter) „(mail=\$recipients)“ angewendet (**Zeile 01**). Für die Empfänger der E-Mail, welche im LDAP--Verzeichnis gefunden wurden, im Besitz des genannten Attributs sind und der Wert dieses Attributs der Vorgabe entspricht, wird der Log-Eintrag „Mitglied der AD-Gruppe Exchange“ generiert (**Zeile 02**). Für alle anderen Empfänger wird der Log-Eintrag „nicht Mitglied der AD-Gruppe Exchange“ generiert (**Zeile 04**).

Beispiel 4

Ausgangspunkt sind wieder zwei unterschiedliche Groupware-Server, welche parallel eingesetzt werden. Es soll abgefragt werden, ob das Postfach wenigstens eines internen Empfängers einer eingehenden E-Mail - mit gegebenenfalls mehreren Empfängern - ein Exchange Postfach ist. Die Anweisung sieht wie folgt aus:

Zeile	Code
01	ldap_compare('ldaps://myldap.local;CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=firma,DC=local;mypassword;OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local;(mail=\$one_recipient)', 'MailServer', 'Exchange');

Erklärung

Im LDAP Suchpfad (SearchBase) wird der Suchfilter (Filter) „(mail=\$one_recipient)“ angewendet. Hat **wenigstens ein Empfänger** der E-Mail „(mail=\$one_recipient)“ den Wert „Exchange“ im Attribut „MailServer“ so ist der Rückgabewert **positiv**.

Beispiel 5

Es soll abgefragt werden, ob das Postfach aller internen Empfänger einer eingehenden E-Mail - mit gegebenenfalls mehreren Empfängern - Domino Postfächer sind. Die Anweisung sieht wie folgt aus:

Zeile	Code
01	ldap_compare('ldaps://myldap.local;CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=firma,DC=local;mypassword;OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local;(mail=\$all_recipients)', 'MailServer', 'Domino');

Erklärung

Im LDAP Suchpfad (SearchBase) wird der Suchfilter (Filter) „(mail=\$all_recipients)“ angewendet. Nur wenn **alle internen Empfänger** der E-Mail „(mail=\$all_recipients)“ den Wert „Domino“ im Attribut „MailServer“ haben, so ist der Rückgabewert **positiv**.

Beispiel 6

Geprüft werden soll, ob der interne Absender einer E-Mail „(proxyaddresses=smtp:\$sender)“ ein User der Domäne firma.local ist. Die Anweisung sieht wie folgt aus:

Zeile	Code
01	ldap_compare('ldaps://192.168.10.10;Administrator@myldap.local;mypassword;DC=firma,DC=local;(proxyaddresses=smtp:\$sender)'; 'objectclass', 'user');

Erklärung

Im LDAP Suchpfad (SearchBase) wird der Suchfilter (Filter) „(proxaddresses=smtp:\$sender)“ angewendet. Wird die Absenderadresse des **Envelope** der E-Mail (smtp:\$sender) in einem User-Object (objectclass=user) gefunden, so ist der Rückgabewert **positiv**. Da in einem AD-User-Object im Attribut **proxaddresses** auch E-Mail-Aliases aufgeführt werden, funktioniert diese Abfrage mit allen E-Mail Adressen des Users und nicht nur mit der Haupt-Adresse (Attribut **mail**).

8.7.4 ldap_getcerts()

Der Befehl `ldap_getcerts()` ruft öffentliche S/MIME Schlüssel (Zertifikate) bei einem LDAP-Verzeichnisdienst ab.

Dieser Befehl ruft für jeden Empfänger einer E-Mail öffentliche S/MIME Schlüssel (Zertifikate) bei einem LDAP-Verzeichnisdienst ab.

Der Suchfilter hierfür lautet (mail=) und ist nicht konfigurierbar.

Aufbau des Befehls

```
ldap_getcerts('ldap', ['filter'], ['optional']);
```

Rückgabewert

positiv immer

Parameter

Variablen ⁵⁰⁶ verfügbar!

ldap

Der Parameter ist wie folgt aufgebaut:

'URI;BindDN;Password;SearchBase'

Die Bedeutung der einzelnen Teil Strings ist der folgenden Tabelle beschrieben:

Parameter	Beschreibung
URI	Angabe des LDAP(s)-Servers, der abgefragt werden soll. Als Eingabe wird der Hostname oder die IP-Adresse akzeptiert. Es können auch zwei mit Komma getrennte Werte angegeben werden: In diesem Fall wird automatisch auf den zweiten Server zugegriffen, wenn der erste nicht erreicht werden kann. Hinweis:  ist mehr als ein LDAP Server eingetragen, so wird für jeden einzelnen Server eine Verbindung aufgebaut. Die Verbindungen werden zwischengespeichert. Die eigentliche Abfrage wird dann in der eingegebenen Reihenfolge der Server ausgeführt, bis die Abfrage erfolgreich ist. War eine Abfrage erfolglos, so wird die Verbindung aus dem Zwischenspeicher entfernt. Ist keine verbleibende Verbindung im Zwischenspeicher, so werden die Verbindungen neu aufgebaut.
BindDN	Eingabe des vollständigen Distinguished Name (DN) des (read-only) Accounts, welcher zur Suche des unter „SearchBase“ im LDAP Verzeichnis berechtigt ist.
Password	Das Passwort des unter BindDN angegebenen Benutzers Hinweis:  Semikolons „;“ und Backslashes „\“ im Password müssen jeweils mit einem Backslash als Sonderzeichen gekennzeichnet werden, also „\\“, beziehungsweise „\\“. Somit müsste beispielsweise das Passwort p4ss\\w0rd; wie folgt eingegeben werden: p4ss\\\\w0rd\\;
SearchBase	Suchpfad: Gibt den Zweig des LDAP Verzeichnis an, in welchem das Attribute aus dem Parameter <code>'attr'</code> zu suchen ist.

filter (optional)

Ist ein vom Standard (mail=<E-Mail Adresse des Empfängers>) abweichender Suchfilter erforderlich, so kann dieser optional mitgegeben werden.

optional (optional)

Bestimmt das Verhalten, sofern der LDAP-Verzeichnisdienst nicht erreichbar ist

Mögliche Werte

- true, yes oder 1 verhindern des Abbruchs
 - false, no oder 0 sofortiger Abbruch
- Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	<code>ldap_getcerts('ldaps://directory.meinefirma.tld;;;ou=pki-participant,dc=pki,dc=meinefirma,dc=tld');</code>

Erklärung

Der LDAP-Server, welcher unter dem Fully Qualified Domain Name (FQDN) „ldap-directory.domain.tld“ (auf dem LDAPS Standardport 636) erreichbar ist, wird abgefragt. Ein Benutzer (BindDN) mit Passwort (Password) zum Autorisieren der Abfrage ist nicht notwendig, da es sich im Beispiel um einen öffentlichen LDAP Verzeichnisdienst handelt. Der LDAP Pfad, in welchem die Zertifikate abliegen lautet ou=pki-participant,dc=pki,dc=domain,dc=tld

8.7.5 ldap_getpgpkeys()

Der Befehl `ldap_getpgpkeys()` ruft öffentliche OpenPGP Schlüssel bei einem LDAP-Verzeichnisdienst ab.

Dieser Befehl ruft für jeden Empfänger einer E-Mail öffentliche OpenPGP Schlüssel bei einem LDAP-Verzeichnisdienst ab.

Der Suchfilter hierfür lautet (pgpUserID=) und ist nicht konfigurierbar.

Aufbau des Befehls

```
ldap_getpgpkeys('ldap', ['filter'], ['optional']);
```

Rückgabewert

positiv immer

Parameter

Variablen ⁵⁰⁶ verfügbar!

ldap

Der Parameter ist wie folgt aufgebaut:

'URI;BindDN;Password;SearchBase'

Die Bedeutung der einzelnen Teil Strings ist der folgenden Tabelle beschrieben:

Parameter	Beschreibung
URI	Angabe des LDAP(s)-Servers, der abgefragt werden soll. Als Eingabe wird der Hostname oder die IP-Adresse akzeptiert. Es können auch zwei mit Komma getrennte Werte angegeben werden: In diesem Fall wird automatisch auf den zweiten Server zugegriffen, wenn der erste nicht erreicht werden kann. Hinweis:  ist mehr als ein LDAP Server eingetragen, so wird für jeden einzelnen Server eine Verbindung aufgebaut. Die Verbindungen werden zwischengespeichert. Die eigentliche Abfrage wird dann in der eingegebenen Reihenfolge der Server ausgeführt, bis die Abfrage erfolgreich ist. War eine Abfrage erfolglos, so wird die Verbindung aus dem Zwischenspeicher entfernt. Ist keine verbleibende Verbindung im Zwischenspeicher, so werden die Verbindungen neu aufgebaut.
BindDN	Eingabe des vollständigen Distinguished Name (DN) des (read-only) Accounts, welcher zur Suche des unter „SearchBase“ im LDAP Verzeichnis berechtigt ist.
Password	Das Passwort des unter BindDN angegebenen Benutzers Hinweis:  Semikolons „;“ und Backslashes „\“ im Password müssen jeweils mit einem Backslash als Sonderzeichen gekennzeichnet werden, also „\\“, beziehungsweise „\\“. Somit müsste beispielsweise das Passwort p4ssw0rd; wie folgt eingegeben werden: p4ss\\w0rd\;
SearchBase	Suchpfad: Gibt den Zweig des LDAP Verzeichnis an, in welchem das Attribute aus dem Parameter <code>'attr'</code> zu suchen ist.

filter (optional)

Ist ein vom Standard (pgpUserID=<E-Mail Adresse des Empfängers>) abweichender Suchfilter erforderlich, so kann dieser optional mitgegeben werden.

optional (optional)

Bestimmt das Verhalten, sofern der LDAP-Verzeichnisdienst nicht erreichbar ist

Mögliche Werte

- true, yes oder 1 verhindern des Abbruchs
 - false, no oder 0 sofortiger Abbruch
- Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	<code>ldap_getpgpkeys('ldaps://directory.domain.tld;;;ou=pki-participant,dc=pki,dc=domain,dc=tld');</code>

Erklärung

Der LDAP-Server, welcher unter dem Fully Qualified Domain Name (FQDN) „ldap-directory.domain.tld“ (auf dem Standardport 389) erreichbar ist, wird abgefragt. Ein Benutzer (BindDN) mit Passwort (Password) zum Autorisieren der Abfrage ist nicht notwendig, da es sich im Beispiel um einen öffentlichen LDAP Verzeichnisdienst handelt. Der LDAP Pfad, in welchem die öffentlichen OpenPGP Schlüssel abliegen lautet ou=pki-participant,dc=pki,dc=domain,dc=tld

8.8 Vordefinierte Platzhalter



Achtung:

Vordefinierte Platzhalter werden - sofern es sich um komplette Ruleset Abschnitte handelt - zunächst noch aus Kompatibilitätsgründen beibehalten, jedoch seit Version 9.0 sukzessive durch **Makros** [509], beziehungsweise **Vordefinierte Makros** [638] ersetzt.

Das heißt vordefinierte Platzhalter sollten - soweit möglich -

- a) beim Erstellen neuer **Custom commands** [308] nicht mehr verwendet werden.
- b) aus vorhandenen **Custom commands** [308] durch die ersetzenden **Vordefinierte Makros** [638] ausgetauscht werden.

um auch weiterhin die Kompatibilität mit neuen Versionen zu erhalten.

Vordefinierte Platzhalter, werden für das Einfügen von Template-Schnipseln verwendet. An jeder Stelle im Ruleset, an welcher dieser Platzhalter auftaucht, wird das entsprechende Schnipsel eingefügt.

Dabei werden vor allem variable Werte aus dem **Ruleset generator** [287] (des Menüs **Mail Processing** [286]) übernommen.

Dadurch kann die Ruleset Programmierung dynamisch auf Änderungen variabler Werte reagieren und wird somit vereinfacht, verkürzt und übersichtlicher gestaltet werden.



Hinweis:

Die hier aufgelisteten Platzhalter werden nur in den **Custom commands** [308] des **Ruleset generator** [287], mit Ausnahme der **Custom macros and commands for all e-mails BEFORE processing**, entsprechend aufgelöst!

Wird ein komplettes Ruleset in einem externen Editor erstellt und über die Schaltfläche **Upload** [286] der **Sektion SMTP Ruleset** [286] hochgeladen, so können diese Platzhalter nicht interpretiert werden.

8.8.1 Allgemein

8.8.1.1 @CUSTOMDELIVER@

Die Funktion @CUSTOMDELIVER@ gibt den unter **Use custom delivery method** [312] eingetragenen Inhalt aus.

Beispiel

Zeile	Code
01	@CUSTOMDELIVER@

8.8.2 Benutzerverwaltung

8.8.2.1 @CREATEGPGKEYS@

Der Platzhalter @CREATEGPGKEYS@ gibt den Wert der Bitmaske (siehe `createkeys()` ⁵⁴⁰) aus, welcher den Einträgen der Administrationsoberfläche (siehe **Mail Processing** ²⁸⁶ **Ruleset generator** ²⁸⁷ **Key generation** ²⁹¹) entspricht.

Beispiel

Zeile	Code
01	<code>createkeys('@CREATEGPGKEYS@');</code>

8.8.3 Signatur

8.8.3.1 @NOSIGNTEXT@

Der Platzhalter @NOSIGNTEXT@ gibt das im Ruleset generator angegebene Betreffzeilen Schlüsselwort für das Unterdrücken des Signierens (siehe Mail Processing Ruleset generator Signing Outgoing e-mails „Do not S/MIME sign outgoing mails with the following text in subject:“) aus.

Beispiel

Zeile	Code
01	if (iscalendar()) {
02	log(1,'meeting request, do not encrypt or sign');
03	compare('subject','substitute','\[sign\]');
04	tagsubject('@NOSIGNTEXT@');
05	}

Erklärung

In diesem Beispiel wird über den Befehl iscalendar() (Zeile 01) geprüft, ob es sich bei der E-Mail um einen Kalendereintrag handelt. Wenn dem so ist, so wird dies im Log eingetragen (Zeile 02). Ein eventuell vorhandenes Schlüsselwort (tag) zum Signieren (hier „[sign]“) der E-Mail wird entfernt (Zeile 03) und - für den Fall, dass die Option für das Signieren aller ausgehenden E-Mails gesetzt ist - als nicht zu signierend (@NOSIGNTEXT@) (Zeile 04) markiert.

8.8.3.2 @TAGSIGNED@

Der Platzhalter @TAGSIGNED@ fügt dem Betreff der E-Mail die zum Kennzeichnen erfolgreich geprüfter Signaturen definierte Markierung hinzu (siehe Mail Processing Ruleset generator Signing Incoming e-mails „Add this text to message subject if S/MIME signature check succeeds:“).

Beispiel

Zeile	Code
01	if (validate smime sig('true')) {
02	log(1,'smime signed valid');
03	@TAGSIGNED@
04	} else {
05	log(1,'smime signed, but signature invalid');
06	}

Erklärung

In diesem Beispiel wird über den Befehl validate_smime_sig() (Zeile 01) die Signatur einer E-Mail überprüft. Ist die Signatur valide, so wird das mittels log() in das Log geschrieben (Zeile 02). Zusätzlich wird über den Platzhalter @TAGSIGNED@ (Zeile 03) dem Betreff der E-Mail das Kennzeichen für erfolgreich geprüfte Signaturen - im Standard [signed OK] angefügt.

Ist die Signatur ungültig, so wird dies ebenfalls über den Befehl log() in das Log geschrieben (Zeile 05).

8.8.3.3 @TAGSIGNEDINVALID@

Der Platzhalter @TAGSIGNEDINVALID@ fügt dem Betreff der E-Mail die zum Kennzeichnen ungültiger Signaturen definierte Markierung hinzu (siehe [Mail Processing Ruleset generator](#) [298] Incoming e-mails Add this text to message subject if S/MIME signature check fails:).

Beispiel

Zeile	Code
01	<code>if (validate smime sig('true')) {</code>
02	<code>log(1,'smime signed valid');</code>
03	<code>} else {</code>
04	<code>log(1,'smime signed, but signature invalid');</code>
05	<code>@TAGSIGNEDINVALID@</code>
06	<code>}</code>

Erklärung

In diesem Beispiel wird über den Befehl `validate_smime_sig()` [590] (Zeile 01) die Signatur einer E-Mail überprüft. Ist die Signatur valide, so wird das mittels `log()` [534] in das Log geschrieben (Zeile 02). Ist die Signatur ungültig, So wird dies ebenfalls über den Befehl `log()` [534] in das Log geschrieben (Zeile 04). Zusätzlich wird über den Platzhalter @TAGSIGNEDINVALID@ [632] (Zeile 05) dem Betreff der E-Mail das Kennzeichen für ungültige Signaturen - im Standard [signed INVALID] - angefügt.

8.8.3.4 @REMOVETAGDECRYPTED@

Der Platzhalter @REMOVETAGDECRYPTED@ entfernt alle von der Appliance verwendeten **Betreffzeilen Schlüsselwörter** ^[164], welche auf eine verschlüsselte E-Mail hindeuten (siehe **Mail Processing** ^[286] **Ruleset generator** ^[287] **Encryption** ^[292] **Incoming e-mails** ^[292] „Add this text to message subject after decryption“ ^[292]), aus einer E-Mail.

Beispiel

Zeile	Code
01	@REMOVETAGDECRYPTED@

8.8.3.5 @REMOVETAGS@

Der Platzhalter @REMOVETAGS@ entfernt alle von der Appliance verwendeten **Betreffzeilen Schlüsselwörter** ^[164], welche auf eine signierte E-Mail hindeuten (siehe **Mail Processing** ^[286] **Ruleset generator** ^[287] **Signing** ^[298] **Incoming e-mails** ^[298]), aus einer E-Mail. Somit erfüllt diese Funktion die Summe aus den Funktionen @REMOVETAGSIGNED@ ^[633] und @REMOVETAGSIGNEDINVALID@ ^[634].

Beispiel

Zeile	Code
01	@REMOVETAGS@

8.8.3.6 @REMOVETAGSIGNED@

Der Platzhalter @REMOVETAGSIGNED@ entfernt das in der Appliance (siehe **Mail Processing** ^[286] **Ruleset generator** ^[287] **Signing** ^[298] **Incoming e-mails** ^[298] „Add this text to message subject if S/MIME signature check succeeds:“ ^[298]) festgelegte Schlüsselwort (tag), welches nach dem erfolgreichen Prüfen einer S/MIME Signatur - im Standard [signed OK] - gesetzt wird, aus dem Betreff einer E-Mail.

Beispiel

Zeile	Code
01	@REMOVETAGSIGNED@

8.8.3.7 @REMOVETAGSIGNEDINVALID@

Der Platzhalter @REMOVETAGSIGNEDINVALID@ entfernt das in der Appliance über den **Ruleset generator** (siehe **Mail Processing** ²⁸⁶ **Ruleset generator** ²⁸⁷ **Signing** ²⁹⁶ **Incoming e-mails** „Add this text to message subject if S/MIME signature check fails: ²⁹⁵“) festgelegte Schlüsselwort (tag), welches nach dem Prüfen einer S/MIME signierten E-Mail mit **ungültiger** Signatur - im Standard ist das [signed INVALID] - gesetzt wird, aus dem Betreff einer E-Mail.

Beispiel

Zeile	Code
01	@REMOVETAGSIGNEDINVALID@

8.8.4 Verschlüsselung

8.8.4.1 @TRIGGERTEXT@

Der Platzhalter @TRIGGERTEXT@ gibt das im **Ruleset generator** angegebene **Betreffzeilen Schlüsselwort** für das Verschlüsseln (siehe **Mail Processing** **Ruleset generator** **Encryption / Decryption** **Outgoing e-mails** „Always encrypt mails with the following text in subject:“ aus.

Beispiel

Zeile	Code
01	if (rmatchsplit('@test\.tld')) {
02	log(1,'e-mail to domain test.tld, force encryption');
03	tagsubject('@TRIGGERTEXT@');
04	}

Erklärung

In diesem Beispiel wird über den Befehl `rmatchsplit()` (Zeile 01) geprüft, ob Empfänger der E-Mail zur E-Mail Domäne „@test.tld“ gehören. Für diese Empfänger wird ein entsprechender Log Eintrag erzeugt (Zeile 02). Anschließend wird durch das Setzen des **Betreffzeilen Schlüsselwort** aus der Administrationsoberfläche mittels `tagsubject()` (Zeile 03), das Verschlüsseln der E-Mail mittels HIN-Verschlüsselung erzwungen.

8.8.4.2 @NOENCTEXT@

(entfernt in 11.0.7)

8.8.4.3 @KEYSERVER@

(abgelöst in 11.1.10) -> \$keyserver

8.8.4.4 @TAGDECRYPTED@

Der Platzhalter @TAGDECRYPTED@ fügt dem Betreff einer E-Mail das im **Ruleset generator** (siehe **Mail Processing** **Ruleset generator** **Encryption / Decryption** **Incoming e-mails** „Add this text to message subject after decryption“) eingetragene Schlüsselwort für entschlüsselte E-Mails an.

Beispiel

Zeile	Code
01	if (decrypt smime()) {
02	log(1,'mail is smime signed encrypted');
03	@TAGDECRYPTED@
04	} else {
05	log(1,'mail could not be smime decrypted');
06	}

Erklärung

In diesem Beispiel wird über den Befehl `decrypt smime()` (Zeile 01) versucht die E-Mail mit einem passenden S/MIME User-Key zu entschlüsseln. Gelingt dies, so wird das mittels `log()` in das Log geschrieben (Zeile 02). Zusätzlich wird über den Platzhalter @TAGDECRYPTED@ dem Betreff der E-Mail das Kennzeichen für das erfolgreiche Entschlüsseln (im Standard [secure]) hinzugefügt. Schlägt das Entschlüsseln fehl, so wird dies ebenfalls über den Befehl `log()` in das Log geschrieben (Zeile 05).

8.8.4.5 @REMOVETAGDECRYPTED@

Der Platzhalter @REMOVETAGDECRYPTED@ entfernt das in der Appliance (siehe **Mail Processing** ²⁸⁵ **Ruleset generator** ²⁸⁷ **Encryption / Decryption** ²⁹² **Incoming e-mails** „Add this text to message subject after decryption“ ²⁹²) festgelegte Schlüsselwort (tag), welches nach erfolgreichem Entschlüsseln gesetzt wird - im Standard [secure] - aus dem Betreff einer E-Mail.

Beispiel

Zeile	Code
01	@REMOVETAGDECRYPTED@

8.8.5 LFT

8.8.5.1 @LARGEFILETEXT@

Der Platzhalter @LARGEFILETEXT@ gibt das im Ruleset generator angegebene **Betreffzeilen Schlüsselwort** für das Erzwingen von **Large File Transfer (LFT)** (siehe **Mail Processing** Ruleset generator **Large files**) **Always use large file processing for mails with the following text in subject:** aus.

Beispiel

Zeile	Code
01	tagsubject ('@LARGEFILETEXT@');

8.8.5.2 @NOLARGEFILETEXT@

Der Platzhalter @NOLARGEFILETEXT@ gibt das im Ruleset generator angegebene **Betreffzeilen Schlüsselwort** für das Unterdrücken von **Large File Transfer (LFT)** (siehe **Mail Processing** Ruleset generator **Large files**) **Do not use large file processing for mails with the following text in subject:** aus.

Beispiel

Zeile	Code
01	tagsubject ('@NOLARGEFILETEXT@');

8.8.5.3 @REMOVELFMTAGS@

(abgelöst in 11.0.7) -> \$removelfmtags

8.8.6 Header Tagging

8.8.6.1 @TAGHEADERENCRYPTED@

Der Platzhalter `@TAGHEADERENCRYPTED@` fügt einer E-Mail den im **Ruleset generator** (siehe **Mail Processing**) **Ruleset generator** **Header Tagging** **Set header** ☐ to value ☐ For all mails that have been encrypted eingetragenen X-Header mit dem entsprechenden Wert an.

Beispiel

Zeile	Code
01	<code>if (encrypt smime()) {</code>
02	<code>log(1,'mail successfully smime encrypted');</code>
03	<code>@TAGHEADERENCRYPTED@</code>
04	<code>} else {</code>
05	<code>log(1,'mail could not be smime decrypted');</code>
06	<code>}</code>

Erklärung

In diesem Beispiel wird über den Befehl `encrypt_smime()` (Zeile 01) versucht die E-Mail mit einem passenden S/MIME Zertifikat zu verschlüsseln. Gelingt dies, so wird das mittels `log()` in das Log geschrieben (Zeile 2). Zusätzlich wird über den Platzhalter `@TAGHEADERENCRYPTED@` der E-Mail der X-Header für erfolgreich verschlüsselte E-Mails angefügt.

Schlägt die Verschlüsselung fehl, so wird dies ebenfalls über den Befehl `log()` in das Log geschrieben (Zeile 05).

8.8.6.2 @TAGHEADERDECRYPTED@

Der Platzhalter `@TAGHEADERDECRYPTED@` fügt einer E-Mail den im **Ruleset generator** (siehe **Mail Processing**) **Ruleset generator** **Header Tagging** **Set header** ☐ to value ☐ For all mails that have been decrypted eingetragenen X-Header mit dem entsprechenden Wert an.

Beispiel

Zeile	Code
01	<code>if (decrypt smime()) {</code>
02	<code>log(1,'mail is smime decrypted');</code>
03	<code>@TAGHEADERDECRYPTED@</code>
04	<code>} else {</code>
05	<code>log(1,'mail could not be smime decrypted');</code>
06	<code>}</code>

Erklärung

In diesem Beispiel wird über den Befehl `decrypt_smime()` (Zeile 01) versucht die E-Mail mit einem passenden S/MIME User-Key zu entschlüsseln. Gelingt dies, so wird das mittels `log()` in das Log geschrieben (Zeile 2). Zusätzlich wird über den Platzhalter `@TAGHEADERDECRYPTED@` der E-Mail der X-Header für erfolgreich entschlüsselte E-Mails angefügt.

Schlägt die Entschlüsselung fehl, so wird dies ebenfalls über den Befehl `log()` in das Log geschrieben (Zeile 05).

8.9 Vordefinierte Makros

Vordefinierte **Makros** werden per Standard in der SEPPmail Appliance bereitgestellt und stehen somit immer für das Verwenden in **Custom commands** zur Verfügung.

8.9.1 Allgemein

8.9.1.1 \$archive

Das Makro `$archive` archiviert E-Mails unter Verwendung der unter **Mail Processing** ²⁸⁶ **Ruleset generator** ²⁸⁷ **Archiving** ³⁰⁸ eingetragenen E-Mail Adresse.

Beispiel

Zeile	Code
01	<code>\$archive;</code>

8.9.2 Verwalten von Benutzern

8.9.2.1 \$createanyuser

Das Makro `$createanyuser` generiert einen neuen Benutzer (siehe **Users** ³⁹⁶), gemäß dem unter **Mail Processing** ²⁸⁶ **Ruleset generator** ²⁸⁷ **User creation** ²⁸⁹ eingestellten Standard für das Generieren von Benutzern.

Somit stellt dieses Makro einen Platzhalter für die unter **Mail Processing** ²⁸⁶ **Ruleset generator** ²⁸⁷ **User creation** ²⁸⁹ vorgenommene Einstellung dar. Somit würde mit

Do not create accounts ²⁸⁹
kein **User** ³⁹⁶ angelegt

Create accounts for new users if user tries to sign / encrypt ²⁸⁹

ein **User** ³⁹⁶ nur dann angelegt, wenn dieser eine kryptographische Aktion auslöst (sign/encrypt) und nicht bereits als **User** ³⁹⁶ vorhanden ist.

Ist die Option **Mail Processing** ²⁸⁶ **Ruleset generator** ²⁸⁷ **Custom commands** ³⁰⁸ **Custom commands for User Creation** ³⁰⁸ aktiv, so würde der entsprechende Code für das Anlegen des Users zum Tragen kommen.

Create accounts for all users ²⁹⁰

generell für die sendende E-Mail Adresse ein **User** ³⁹⁶ angelegt, sofern dieser nicht bereits als **User** ³⁹⁶ vorhanden ist.

Ist die Option **Mail Processing** ²⁸⁶ **Ruleset generator** ²⁸⁷ **Custom commands** ³⁰⁸ **Custom commands for User Creation** ³⁰⁸ aktiv, so würde der entsprechende Code für das Anlegen des Users zum Tragen kommen.

Beispiel

Zeile	Code
01	<code>\$createanyuser;</code>

8.9.2.2 \$createcustomuser

Das Makro `$createcustomuser` generiert einen neuen Benutzer (siehe **Users** ³⁹⁶), sofern dieser nicht bereits vorhanden ist.

Basis für das Generieren sind die unter **Mail Processing** ²⁸⁶ **Ruleset generator** ²⁸⁷ **Custom commands** ³⁰⁸ **Custom commands for User Creation** ³⁰⁸ definierten Einstellungen, sofern diese aktiv sind.

Die Auswahl der Einstellung unter **Mail Processing** ²⁸⁶ **Ruleset generator** ²⁸⁷ **User creation** ²⁸⁹ spielt bei diesem Makro keine Rolle. Das heißt, der Code wird selbst mit der Einstellung **Do not create accounts** ausgeführt.

Beispiel

Zeile	Code
01	<code>\$createcustomuser;</code>

8.9.2.3 \$createwebuser

Das Makro `$createwebuser` generiert einen neuen GINA Account (siehe [GINA accounts](#) ⁴⁶²), sofern dieser nicht bereits vorhanden ist.

Hierfür werden die Einstellungen der Administrationsoberfläche unter [CHANGE GINA SETTINGS FOR](#) ⁴²³ `Initial password` ⁴³⁰ `Password length` ⁴³¹ herangezogen.

Beispiel

Zeile	Code
01	<code>\$createwebuser;</code>

8.9.3 Tagging

8.9.3.1 \$removelfmtags

Das Makro `$removelfmtags` entfernt alle von der Appliance für LFT verwendeten Tags (**Betreffzeilen**, **Schlüsselwörter** ^[164]) aus einer E-Mail, also [lfm] und [nolfm] (siehe auch Tabelle 1 des Kapitels **Steuern der Appliance** ^[164]).

Beispiel

Zeile	Code
01	<code>\$removelfmtags;</code>

8.9.4 Verschlüsselung

8.9.4.1 \$keyserver

Das Makro `$keyserver` sucht auf den unter **Mail Processing** ^[286] **Ruleset generator** ^[287] **Key server** ^[309] eingetragenen Schlüssel-Servern nach öffentlichen Schlüsseln - egal ob OpenPGP oder S/MIME - für das Verschlüsseln an externe Kommunikationspartner.

Beispiel

Zeile	Code
01	<code>\$keyserver;</code>
02	<code>if (pgp keys avail()){</code>
03	<code> log(1,'OpenPGP key available');</code>
04	<code> if (encrypt pgp()) {</code>
05	<code> log(1,'mail successfully OpenPGP encrypted');</code>
06	<code> } else {</code>
07	<code> log(1,'mail could not be OpenPGP encrypted');</code>
08	<code> }</code>
09	<code>} else {</code>
10	<code> log(1,'no OpenPGP key available');</code>
11	<code>}</code>

Erklärung

In diesem Beispiel wird über `$keyserver` definiert, dass öffentliche Schlüssel - egal ob S/MIME oder OpenPGP - nicht nur lokal auf der Appliance, sondern auch auf den in der Administrationsoberfläche angegebenen Schlüssel-Servern (siehe **Mail Processing** ^[286] **Ruleset generator** ^[287] **Key server** ^[309]) gesucht werden soll (**Zeile 01**).

Der Befehl `pgp_keys_avail()` ^[574] prüft somit sowohl lokal auf der Appliance als auch auf den in der Administrationsoberfläche angegebenen Schlüsselservern, ob ein passender, Benutzer basierter öffentlicher - im Beispiel OpenPGP - Schlüssel für das Verschlüsseln zur Verfügung steht (**Zeile 2**). Das Ergebnis dieser Abfrage wird protokolliert (**Zeile 03 und 10**). Steht ein entsprechender Schlüssel zur Verfügung, wird mit dem Verschlüsseln fortgefahren (**Zeile 04**), dessen Erfolg beziehungsweise Misserfolg ebenfalls protokolliert wird (**Zeile 05 und 07**).

9 HowTo / FAQ

Dieses Kapitel enthält Konfigurationsvorschläge, insbesondere für das Anpassen der SEPPmail Appliance an infrastrukturelle Gegebenheiten, beziehungsweise kundenindividuelle Anforderungen, welche den üblichen Standard überschreiten.

Achtung:

Die hier aufgeführten Konfigurationsbeispiele sind als Konfigurationsvorschlag zu verstehen, insbesondere, wenn sich diese auf Systeme von Drittherstellern beziehen. Systembedingt sind hier gegebenenfalls weitere Anpassungen vorzunehmen.

Enthalten Konfigurationsbeispiele individuellen Code (siehe auch [Mail Processing](#)²⁸⁶, [Ruleset generator](#)²⁸⁷, [Custom commands](#)³⁰⁸), so ist in jedem Fall zu prüfen ob

- das jeweilige Beispiel 100%ig auf die Anforderung passt.
- gegebenenfalls ein weiteres, individuelles Anpassen erforderlich ist.
- der entsprechende Code das gewünschte Verhalten ohne Seiteneffekte hervorruft.



Sollten Kombinationen aus diesen Code-Beispielen benötigt werden, so ist unbedingt

- auf die korrekte Reihenfolge beim Platzieren im Regelwerk
- eventuelle Wechselwirkungen mit bereits vorhandenem Code zu achten

In jedem Fall muss die Konfiguration vor dem Produktivschalten eines Systems getestet werden.

9.1 Admin: Admins sollen keine „Daily Reports“ erhalten

Ausgangssituation:

Auf der SEPPmail Appliance sind mehrere Administratoren eingerichtet. Jedoch sollen nicht alle Administratoren die „IMPORTANT: **Daily Report**“s erhalten.

Frage:

Wie kann verhindert werden, dass einzelne Mitglieder der **Groups** **admin** den „IMPORTANT: **Daily Report**“s zugesendet bekommen

Antwort:

Für Administratoren welche sich zwar auf der Appliance anmelden können, jedoch keine Reports erhalten sollen, sollte beim Anlegen des entsprechenden **Users** in **CREATE USER ACCOUNT** **User data** unter **E-mail** eine Pseudo-Adresse mit @local verwendet werden.

9.2 Admin: Anmelden nach Passwort-Wechsel mit Sonderzeichen nicht möglich

Ausgangssituation:

Das Anmelden an der Administrationsoberfläche ist nach einem Passwort-Wechsel unter Verwendung von Sonderzeichen nicht mehr möglich.

Frage:

Unterstützt die SEPPmail Appliance Sonderzeichen im Passwort?

Antwort:

Ja. Sonderzeichen werden natürlich unterstützt.

Ursache:

Wenn dieses Phänomen auftritt, wurde der Passwort-Wechsel erfahrungsgemäß nicht in einem Browser-Fenster auf dem lokalen Client, sondern über eine Remote-Session (RDP, TeamViewer, oder Andere) vollzogen. Hier ist immer wieder festzustellen, dass sich der Zeichensatz während der Remote-Session ändert. Somit werden beim Passwort-Wechsel unter Umständen andere Zeichen eingegeben, als auf der Tastatur angezeigt.

Abhilfe:

Anmelden mit einem anderen Admin User und das Passwort des betroffenen Users über sein User Objekt zurücksetzen (siehe `USER 'USER@DOMAIN.TLD'|398|User data|398|Password|398|`).

9.3 Admin: API Funktionen

Ausgangssituation:

Kundenseitig besteht der Wunsch, Abfragen und Managementprozesse, wie zum Beispiel das On- beziehungsweise Off-Boarding von Benutzern, auf der SEPPmail Appliance über Drittsysteme vorzunehmen.

Frage:

Besteht die Möglichkeit die SEPPmail Appliance von außen zu Administrieren und wie wird das realisiert.

Antwort:

Bislang stehen hierfür zwei APIs auf der SEPPmail Appliance zur Verfügung. Eine Beschreibung der APIs sowie PowerShell Module für den Zugriff auf diese APIs steht jeweils auf GitHub bereit

(<https://github.com/seppmail/SEPPmailAPI>, beziehungsweise <https://github.com/seppmail/SEPPmailLegacy>).

(neu in 12.1.0)

Mit der Version 12.1.0 der SEPPmail Appliance werden die Funktionen beider APIs vereint. Nähere Informationen zu den API Funktionen sind [hier](#) zu finden.

Um den API Zugang zur SEPPmail Appliance zu aktivieren, ist unter **System**^[224] in der Ansicht **Advanced View** unter **RestAPI**^[232] zunächst der Haken **Enabled**^[232] zu setzen und bei Bedarf der **HTTPS Port**^[232] für den API Zugriff an die Infrastruktur vor Ort anzupassen.

Für das Authentisieren der API-Zugriffe ist weiterhin ein entsprechender Token notwendig, welcher im Abschnitt **New API Token**^[232] generiert und für die gewünschten Zugriffe berechtigt werden kann.

9.4 Admin: API Test mit „Postman“

Ausgangssituation:

Kundenseitig besteht der Wunsch, Abfragen und Managementprozesse, wie zum Beispiel das On- beziehungsweise Offboarding von Benutzern, auf der SEPPmail Appliance über Drittsysteme vorzunehmen.

Frage:

Besteht die Möglichkeit den API Zugriff auf die SEPPmail Appliance zu testen?

Antwort:

Ist der API Zugriff auf der SEPPmail Appliance eingerichtet (siehe [Admin: API Funktionen](#)^[646]), beziehungsweise [RestAPI](#)^[232], so kann dieser beispielsweise via „Postman“ getestet werden.

Hierfür muss Postman zunächst lokal installiert werden (siehe auch <https://www.postman.com>).

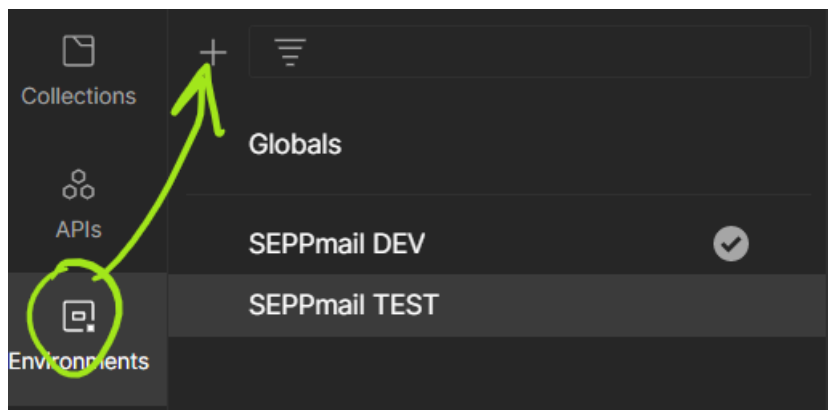
Konfiguration:

Die Konfiguration startet mit dem Einrichten eines

„Environments“.

In diesem werden die Zugangsinformationen zu demjenigen System definiert, auf welches via REST-API zugegriffen werden soll. Im konkreten Fall ist das also die SEPPmail Appliance.

Für das Anlegen ist in der Postman-Oberfläche unter „Environments“ zunächst auf das Plus-Symbol „+“ zu klicken:



Dem neuen Environment sollte ein sprechender Name gegeben werden. Anschließend sind die entsprechenden Parameter zu setzen.

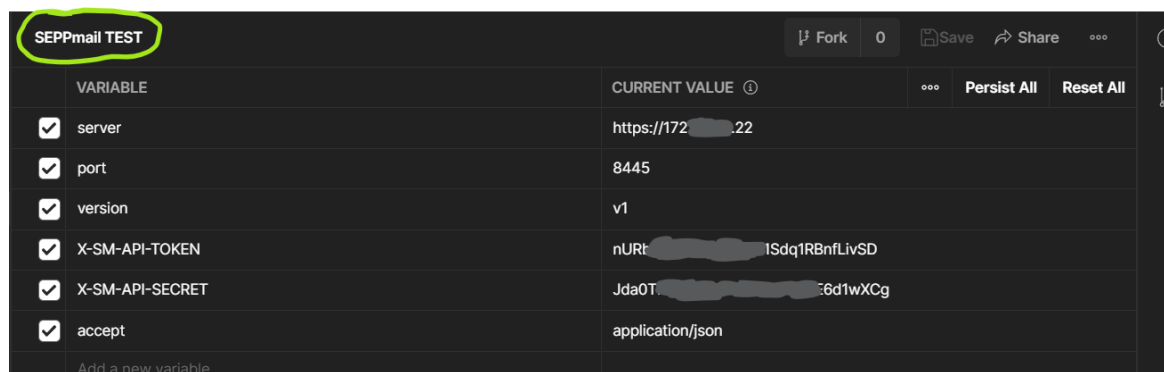
WICHTIG!

Die Parameter Namen müssen exakt mit denen aus der folgenden Tabelle übereinstimmen. Andernfalls funktioniert das Skript für die Verwendung der Werte nicht.

Parameter Name	Wert
server	URL über welche die SEPPmail Appliance erreichbar ist, beispielsweise https://yourseppmail.domain.com Alternativ kann auch eine IP Adresse (beispielsweise https://192.168.0.10) verwendet werden.
port	Port, welcher unter RestAPI ^[232] HTTPS Port ^[232] eingetragen ist, im Standard also 8445
version	v1
X-SM-API-	String aus RestAPI ^[232] RestAPI keys ^[232] API token ^[234] , beispielsweise gAhAMwP2PyDVd3YlxbcnITFWtjFYBAQJ

Parameter Name	Wert
TOKEN	
X-SM-API-SECRET	String aus RestAPI keys , beispielsweise GuvQXNA8B2Zzq0S9G2oFKvECipIUYJhi
accept	application/json

Ein fertig konfiguriertes Environment könnte dann wie folgt aussehen:



SEPPmail TEST		Fork	0	Save	Share	...
	VARIABLE	CURRENT VALUE		Persist All	Reset All	
☒	server	https://172...22				
☒	port	8445				
☒	version	v1				
☒	X-SM-API-TOKEN	nURt...ISdq1RBnfLivSD				
☒	X-SM-API-SECRET	JdaOT...:6d1wXCg				
☒	accept	application/json				
Add a new variable						

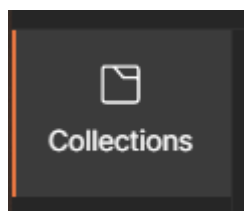
Mit dem Speichern (Save) des Environments ist dieser Punkt abgeschlossen.

Fortgesetzt wird die Konfiguration mit dem Einrichten einer

„Collection“

In dieser werden die für das Steuern der SEPPmail Appliance verfügbaren Befehle definiert.

Hierfür wird zunächst auf „Collections“



geklickt und anschließend auf „File“ -> „Import“ -> „Raw Text“.

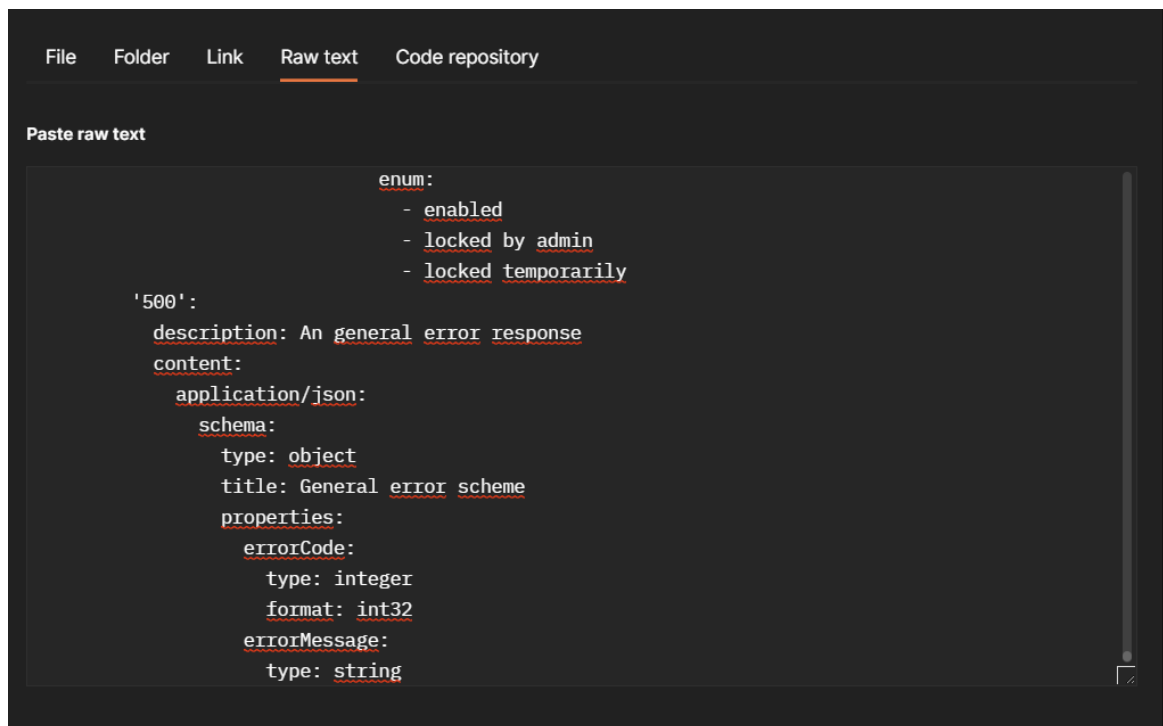
Nun über einen Web-Browser den Pfad https://github.com/seppmail/OpenAPI-YAML/blob/main/seppmail_rest_api.yaml öffnen und den Inhalt der Datei im GitHub Editor anzeigen lassen. Dabei ist für die Anzeige im GitHub Editor das „Raw“ Format auszuwählen. Der angezeigte Text sollte in etwa wie folgt aussehen

```

openapi: 3.0.3
info:
  title: SEPPmail API
  description: Manage your SEPPmail-Appliance with code
  termsOfService: 'https://api.seppmail.com'
  contact:
    name: API Support
    url: 'http://www.seppmail.de/support'
    email: support@seppmail.de
  license:
    name: Apache 2.0
    url: 'https://www.apache.org/licenses/LICENSE-2.0.html'
    x-comment: we have to fix the license
    version: 1.0.2
servers:
  - url: 'https://{server}:{port}/v1'
    description: internal development server
    variables:
      server:
        default: seppmail.domain.com
      port:
        default: '8445'
components:
  securitySchemes:
    apiToken:
      type: apiKey
      in: header
      name: X-SM-API-TOKEN
    apiSecret:
      type: apiKey
      in: header
      name: X-SM-API-SECRET

```

und ist nun in die Zwischenablage zu kopieren. Folgend ist in den eingehend geöffneten Postman Dialog zu wechseln und der zuvor in die Zwischenablage kopierte Text einzufügen.



The screenshot shows the Postman interface with the 'Raw text' tab selected. The text area contains the following JSON snippet:

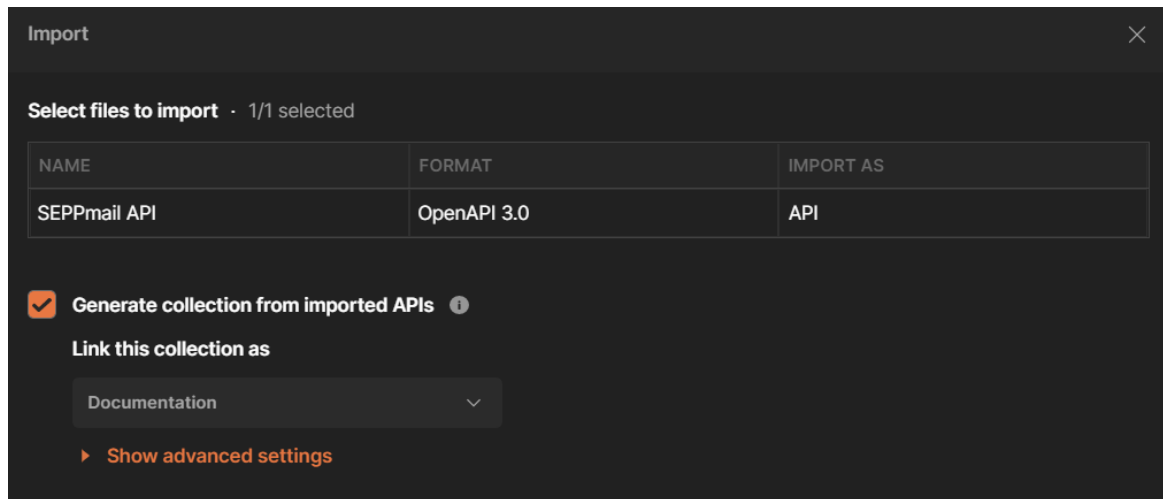
```

enum:
  - enabled
  - locked by admin
  - locked temporarily

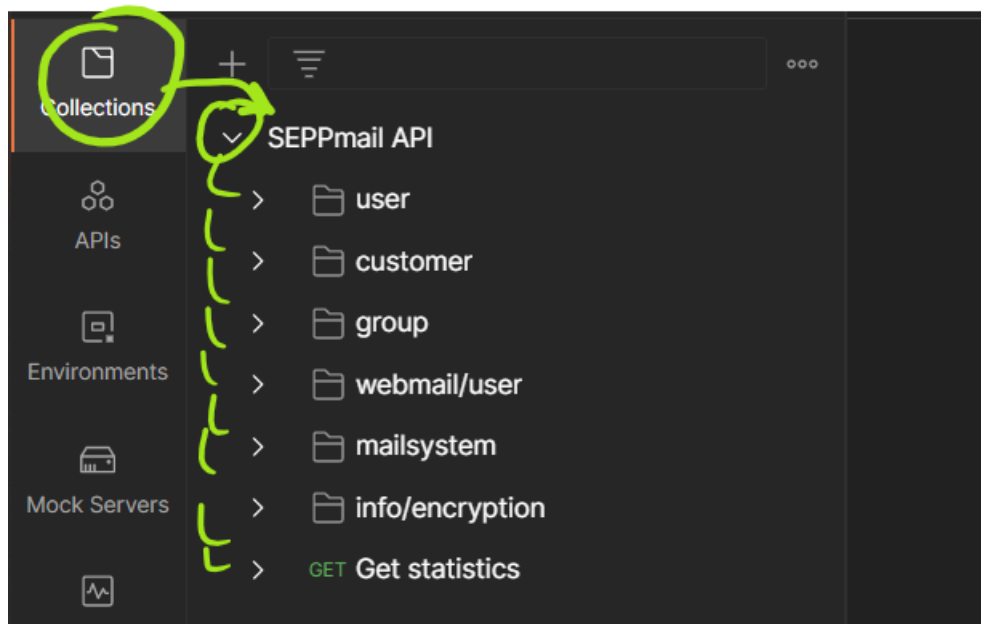
'500':
  description: An general error response
  content:
    application/json:
      schema:
        type: object
        title: General error scheme
        properties:
          errorCode:
            type: integer
            format: int32
          errorMessage:
            type: string

```

Nach einem Klick auf „continue“ sollte in Postman folgender Dialog erscheinen:

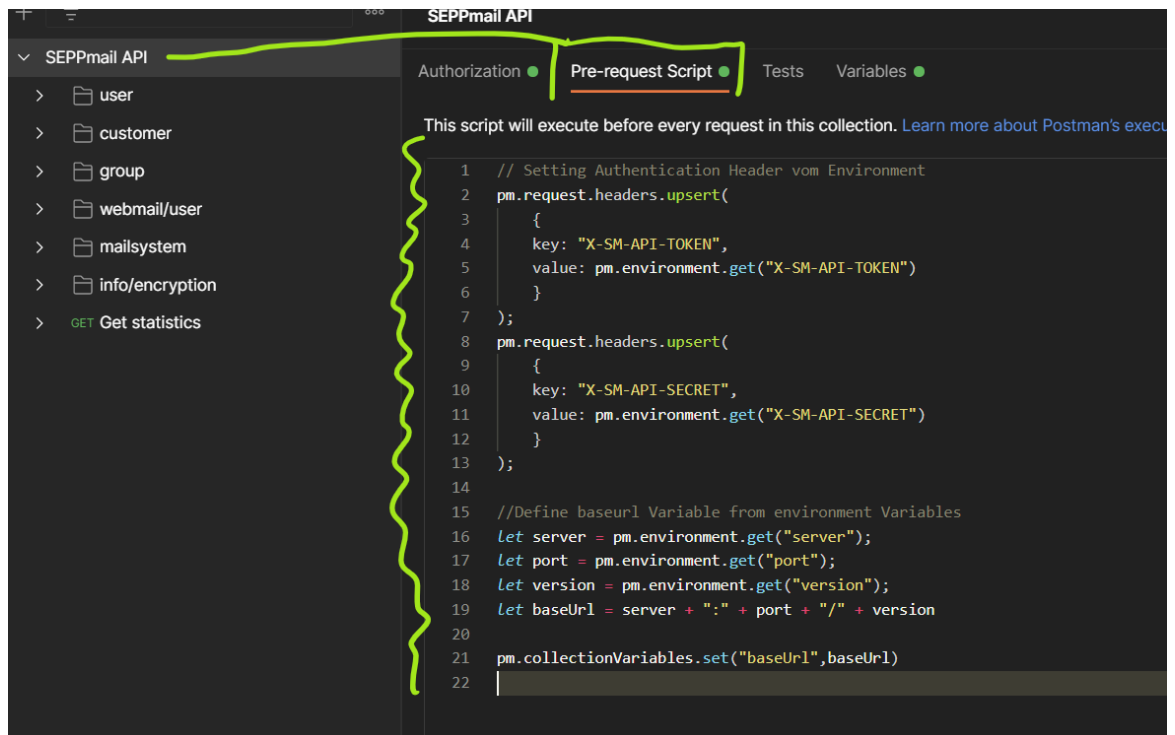


Nun erscheint in den „Collections“ die API mit den Ordnern der einzelnen Bereiche



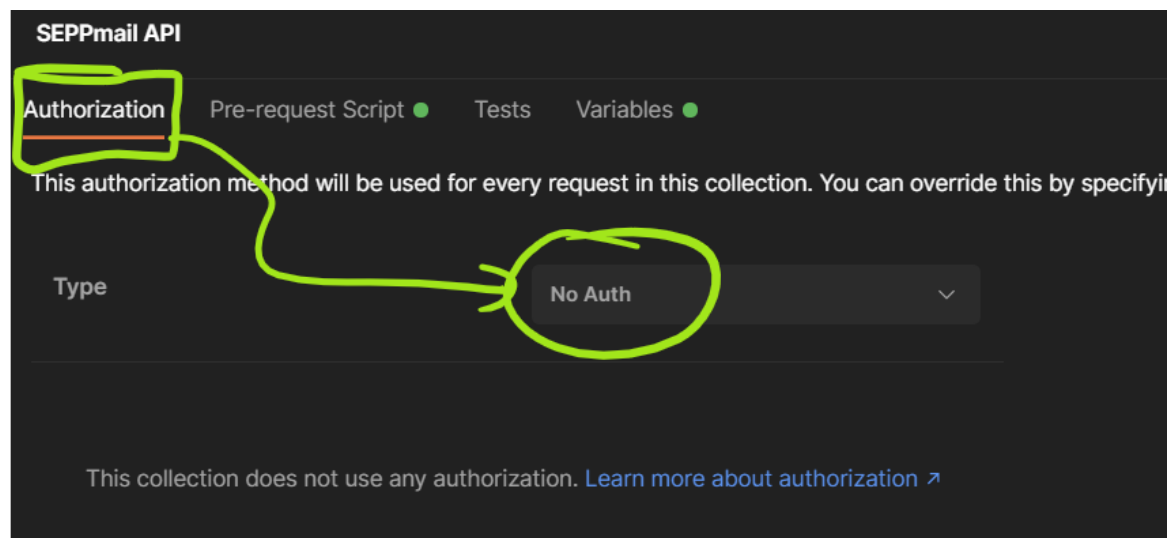
Mit dem „Pre-Request Script“ werden die API-Aufrufe aus den „Collections“ unter Zuhilfenahme des eingehend definierten „Environments“ getestet.

Das Pre-Request Script ist ebenfalls auf dem GitHub Repository unter <https://github.com/seppmail/OpenAPI-YAML/blob/main/postmanConfig.js> zu finden. Der Inhalt dieser Datei wird analog zu den „Collections“ kopiert und ist wie folgt einzufügen:

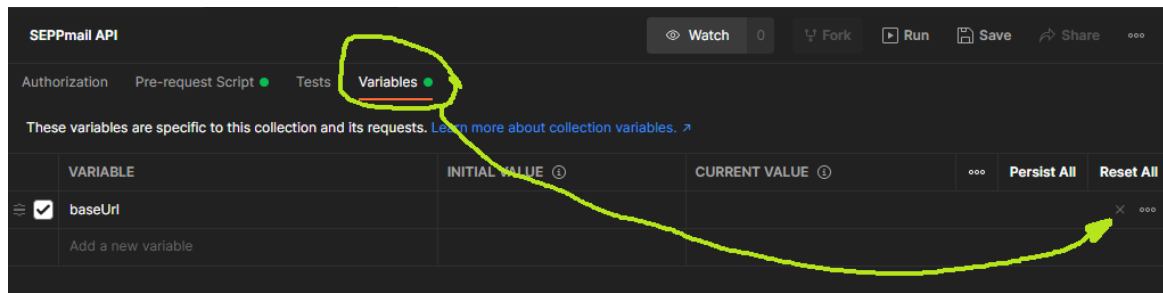


Nun bedarf es noch der „Authorization“ der „Collection“.

Da die Authorization mittels Header in der REST-API durchgeführt wird, muss die Authorization auf „No Auth“ gesetzt werden:

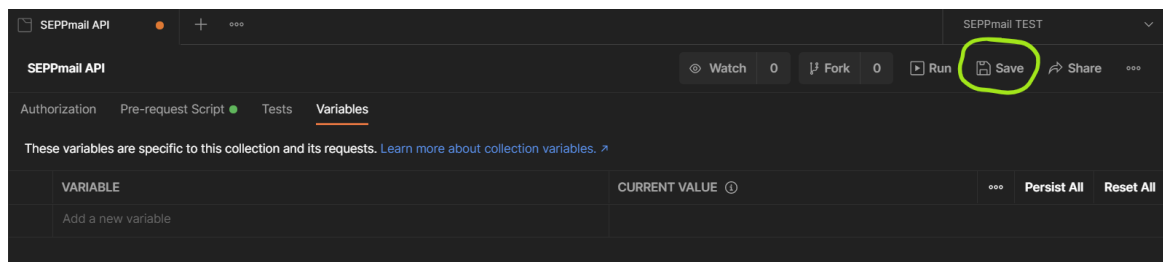


Eventuell vorhandene Collection-„Variables“ müssen nun gelöscht werden.



Für den eigentlichen Zugriff werden die Werte aus dem „Environment“ verwendet.

Abschließend muss die Collection noch abgespeichert werden:



Nun kann ein Zugriffstest erfolgen.

Dieser findet in den Collections statt. Hier ist zunächst zu beachten, dass das zuvor angelegte Environment (im Beispiel „SEPPmail Test“) ausgewählt wurde. Nun wird in der „SEPPmail API“ der Befehl „Get statistics“ ausgewählt und mittels „Send“ abgesetzt.



Hinweis:

Gegebenenfalls sind die Einstellungen in Postman nochmals zu prüfen. Beispielsweise müsste bei Verwenden eines selbst signierten Zertifikates auf der SEPPmail Appliance die Zertifikatsprüfung in Postman abgestellt werden.

9.5 Admin: Erkennen kryptographisch behandelter E-Mails

Ausgangssituation:

Der Kommunikationspartnern erkennt die von der SEPPmail Appliance kryptographisch verarbeiteten E-Mails nicht als solche, beziehungsweise die vom Kommunikationspartner kryptographisch behandelten E-Mails werden von der SEPPmail Appliance nicht als solche erkannt.

Frage:

Weshalb werden die durch die SEPPmail Appliance verschlüsselten beziehungsweise signierten E-Mails vom System meines Kommunikationspartners nicht als solche erkannt?

Antwort:

Bei S/MIME verschlüsselten, beziehungsweise signierten E-Mails sind als „Content-Type“ des Headers jeweils zwei Ausdrücke möglich, nämlich

1. „application/x-pkcs7-mime“ für verschlüsselte E-Mails
 „application/x-pkcs7-signature“ für signierte E-Mails
 Diese Ausdrücke fanden bereits vor Entstehen des Standards weite Verbreitung und sind deshalb weiterhin üblich.
2. „application/pkcs7-mime“ für verschlüsselte E-Mails
 „application/pkcs7-signature“ für signierte E-Mails
 Diese Ausdrücke entsprechen RFC5751 und sind ebenso üblich.

Die SEPPmail-Appliance verarbeitet bei eingehenden E-Mails beide Ausdrücke gleichermassen. Bei ausgehenden E-Mails wird die Variante 1. verwendet (siehe auch **Mail Processing**^[286] **Ruleset generator**^[287] **Encryption**^[292], beziehungsweise **Signing**^[298]).

Bei empfangenden Drittsystemen - also beim Kommunikationspartner - ist darauf zu achten, dass diese ebenfalls beide Varianten gleichermassen verarbeiten, auch um Inkompatibilitäten von anderer Seite zu vermeiden.

9.6 Admin: „Factory reset“ funktioniert nicht

Ausgangssituation:

Eine SEPPmail Appliance soll auf Werkseinstellungen zurückgesetzt werden, beziehungsweise soll Hardware außer Betrieb genommen und verschrottet werden. Damit keine Datenreste auf den Festplatten zurückbleiben, soll ein

Factory reset (siehe [Administration](#) ³⁶⁹ [Maintenance](#) ³⁷⁰) durchgeführt werden.

Frage:

Weshalb funktioniert der **Factory reset** trotz korrekt eingegebenem **Security code** nicht?

Antwort:

Der **Security code** muss aufgrund der folgensweren Auswirkungen eines versehentlich durchgeführten „Factory reset“ **rückwärts** eingegeben werden.

9.7 Admin: Gruppenzuordnung im Menü „Users“

Ausgangssituation:

Das Detail Menü eines SEPPmail Appliance **Users** [396] (siehe **USER 'USER@DOMAIN.TLD'** [398]) ist geöffnet. In der **Sektion Group membership** [401] soll eine weitere Gruppe aus **Groups** [413] hinzugefügt werden.

Frage:

Warum kann dem Benutzer keine Gruppe zugeordnet werden?

Antwort:

Dies funktioniert aufgrund der internen Rechtestruktur nicht. Andernfalls könnte sich ein Benutzer, der nur Mitglied der Gruppe **usersadmin** [415] ist und somit auch nur Zugriff auf das Menü **Users** [396] hat, sich selbst zum Administrator (**admin** [413]) machen.

9.8 Admin: Klonen von SEPPmail Appliances

Ausgangssituation:

Eine SEPPmail Appliance oder auch mehrere Maschinen eines Clusters sollen geklont werden.

Gründe für das Klonen von SEPPmail Appliances können sein:

- Das Update auf die aktuelle SEPPmail Appliance Version kann aufgrund zu geringer Partitionsgrößen nicht ausgeführt werden.
- Der Virtualisierungs-Host soll gewechselt werden (beispielsweise von MS Hyper-V auf ESX oder umgekehrt)
- ...

Frage:

Wie ist beim Klonen vorzugehen?

Antwort:

Generell sollte beim Klonen

- die Quellmaschine auf den aktuellen, beziehungsweise höchst möglichen Softwarestand heben (siehe **Administration** [369] **Update** [369] **Perform update (reboot automatically)**) und mit diesem Stand ein neues Ruleset generieren (siehe **Mail Processing** [286] **SMTP ruleset** [286] **Type** [286] **Generator** [286] **Generate ruleset**). Dabei ist darauf zu achten, dass die Quellmaschine keinesfalls eine höhere Version als die Zielmaschine aufweist.
- von der Download Seite <https://downloads.seppmail.com/> das dem Virtualisierungs-Host entsprechende Image heruntergeladen werden
- das heruntergeladene Image für den zu erstellenden Klon in das entsprechende Host-System eingebunden werden
- der neu erstellten Appliance jeweils eine IP Adresse vergeben werden (siehe **Consolen Login** [141]), welche sich im gleichen Subnetz wie die zugehörige Bestandsmaschine befindet, sodass die neue Maschine per Browser erreichbar ist (diese neue Maschine keinesfalls registrieren!)
- die alte Maschine (Quelle) auf die neue Maschine (Ziel) gemäss **Administration** [369] **Maintenance** [370] **Clone device** [371] klonen
- gegebenenfalls weitere verfügbare Updates wie gewohnt über **Administration** [369] **Update** [369] **Perform update (reboot automatically)** durchführen.

Durch das Klonen wird die Quellmaschine jeweils nach Abschluss des Vorgangs heruntergefahren und die Zielmaschine übernimmt nahtlos deren Betrieb. Somit können auch einzelne Maschinen aus einem Cluster problemlos geklont werden.

Mit dem Klonen sind die Partitionsgrößen automatisch großzügiger ausgelegt.



Achtung:

Ist **Large File Transfer (LFT)** [107] aktiv, so muss die Zielmaschine ebenfalls eine LFT-Platte - von mindestens derselben Größe wie auf den Bestandsmaschine - aufweisen.

9.9 Admin: Mehrere SMTP-Authentifizierungen verwalten

Ausgangssituation:

Zum Beispiel auf einem mandantenfähigen System sollen mehrere SMTP Zugänge mit Authentifizierung - anstatt eines Relaying^[254] Eintrags - für die Abgabe von E-Mails des Kunden Groupware-Servers an die SEPPmail Appliance bereit gestellt werden

Lösung:

1. Erstellen einer (pseudo) Managed domain^[247] - zum Beispiel „pseudo.local“ - mit der IP-Adresse [127.0.0.1] als Forwarding server Eintrag (Mail System^[247] Managed domain^[247] Add domain... Add managed domains^[266] Settings^[266] Forwarding server IP or MX name).
2. Mail System^[247] Antispam^[255] Recommended settings:^[255] PTR check^[257] sowie Optional settings:^[258] Strict PTR check^[258] deaktivieren falls aktiv.
3. Anlage je eines Benutzers pro benötigter SMTP-Authentifizierung (Mandant)
Administrationsoberfläche Users^[396] Create new user account^[410] CREATE USER ACCOUNT^[410] User Data^[410].

Beispiel

Zugriff Mandant A

USERS » CREATE USER ACCOUNT

User Data	
User ID	SMTP_Auth_A
Full Name	SMTP_Auth_A
E-Mail	smtp_auth_a@pseudo.local
Password	***** *****
Note: If the password is set here, the user will be prompted for a new password on first login. The password must be at least 8 characters long.	
Create account	

Zugriff Mandant B

USERS » CREATE USER ACCOUNT

User Data	
User ID	SMTP_Auth_B
Full Name	SMTP_Auth_B
E-Mail	smtp_auth_b@pseudo.local
Password	***** *****
Note: If the password is set here, the user will be prompted for a new password on first login. The password must be at least 8 characters long.	
Create account	

und so weiter.

Am jeweiligen Groupware-System ist nun die SEPPmail Appliance als SMTP-Server, „smtp_auth_a@pseudo.local“ - also die E-Mail Adresse des angelegten Benutzers - mit dem vergebenen Passwort als Benutzer für „Zugriff Mandant A“, beziehungsweise „smtp_auth_b@pseudo.local“ mit dem vergebenen Passwort als Benutzer für „Zugriff Mandant B“ und so weiter, einzutragen.

Damit diese (Pseudo-)User keine User-Lizenz auf der Appliance verbrauchen, empfiehlt es sich diesen (Anmelde-) Benutzern das Recht für das kryptographische Behandeln von E-Mails zu entziehen. Hierfür ist in Administrationsoberfläche unter **Users** jeweils der entsprechende Benutzer (im Beispiel SMTP_Auth_A und SMTP_Auth_B) anzuklicken und im Folgenden **USER 'USER@DOMAIN.TLD'** in der **Sektion User Data** im Abschnitt **Encryption settings** jeweils die Haken bei den Optionen **May not Encrypt mails** und **May not sign mails** zu setzen.

Sollen für die Authentifizierung ausschließlich TLS gesicherte Verbindungen genutzt werden können, so ist zusätzlich unter **Mail System** **SMTP settings** die Option **Require TLS encryption** zu aktivieren.

Weiterhin ist darauf zu achten, dass zwischen Client und SEPPmail Appliance keine Schutzkomponente (zum Beispiel Firewall) durch SMTP - Proxying das Auth login abschneidet.

9.10 Admin: Menü „Administration“ öffnet nicht

Ausgangssituation:

Die Administrationsoberfläche wurde geöffnet und die Anmeldung war erfolgreich. Der Wechsel in andere Menüs funktioniert einwandfrei. Lediglich das Menü **Administration**  öffnet nicht, beziehungsweise nur nach langer Wartezeit.

Ursache:

In **System**  **DNS**  ist die Auswahl **Use the following DNS Servers:** aktiv. Der unter **Primary** eingetragene DNS-Server ist jedoch für die SEPPmail Appliance nicht erreichbar. Das Warten auf einen entsprechenden Timeout verursacht die lange Wartezeit.

Lösung:

Eintragen eines möglichst immer verfügbaren DNS-Server als **Primary**.

9.11 Admin: Unerwartetes Verhalten bei E-Mails mit vielen Empfängern

Ausgangssituation:

Über die SEPPmail Appliance wird eine E-Mail mit sehr vielen Empfängern gesendet, zum Beispiel ein Newsletter.

Verhalten:

Am abgebenden E-Mail Server fällt auf, dass die E-Mail von der SEPPmail Appliance in Tranchen verarbeitet wird. In seltenen Fällen wird die E-Mail auch nur an einen Teil der adressierten Empfänger ausgeliefert.

Hintergrund:

Jeder E-Mail Server hat ein Limit, wie viele Empfängeradressen eine E-Mail haben darf. Wird dieser Wert überschritten, handeln die E-Mail Server automatisch aus, dass die E-Mail in jeweils so viele E-Mails gesplittet wird, dass mit den einzelnen E-Mails das Limit nicht überschritten wird.

Auf der SEPPmail Appliance (siehe auch **Mail System** ^[24] **SMTP settings** ^[25] **Extended settings** ^[25] **Extended Postfix MTA settings...** im Folgenden **Extended postfix MTA settings** **MTA Settings Tag** „smtpd_recipient_limit“) sind per Standard (**Appliance default setting**) „25“ Adressen zulässig. Dieser Wert kann jedoch dynamisch (**Appliance dynamic setting**) von den zur Verfügung stehenden Systemressourcen beeinflusst werden.

Durch diese Einstellung wird gewährleistet, dass die vorhandenen Systemressourcen auch dann nicht überschritten werden, wenn bei einer Verschlüsselungsanforderung der „worst case“ einträte und von keinem der Empfänger Schlüsselmaterial vorhanden wäre. In diesem Fall müsste die E-Mail für jeden Empfänger einmal gesplittet und separat mittels GINA-Technologie verschlüsselt werden.

Beim **Appliance default setting** „25“ und einer eingehenden E-Mail mit 250 Empfängern würde dies bedeuten, dass die SEPPmail Appliance beim Versuch des E-Mail Servers diese abzusetzen signalisiert, dass nur E-Mails mit maximal 25 Empfängern angenommen werden. Der E-Mail Server splittet die E-Mail daraufhin in 10 E-Mails zu je 25 Empfänger, welche dann von der SEPPmail Appliance entgegen genommen werden können.

Arbeitet der abgebende E-Mail Server an dieser Stelle nicht regelkonform, kann dies zu Koplikationen führen.

9.12 Admin: Wiederholte Logouts aus der Administrationsoberfläche

Ausgangssituation:

Die Administrationsoberfläche wurde geöffnet und die Anmeldung war erfolgreich. Jedoch kommt mit dem Wechsel in ein anderes Menü häufig eine erneute Anmeldeaufforderung.

Ursache 1:

Ein weiterer Administrator arbeitet parallel mit denselben Login-Credentials auf der Administrationsoberfläche derselben SEPPmail Appliance.

Lösung:

Generell sollten nicht mehrere Admins dasselbe Login, also denselben **User** für die Administration verwenden! Abhilfe schafft das Anlegen von jeweils benutzerbezogenen **Users** für jeden SEPPmail Appliance Administrator und das Zuordnen dieser **Users** zur Gruppe (**Groups**) **admin (Administrator)**.

Ursache 2:

Der Wert unter **System** **Admin GUI** **Admin GUI Session timeout** wurde zu kurz gewählt.

Lösung:

Wählen eines längeren Zeitraums.

9.13 Admin: Vertrauen für gesammelte Root Zertifikate herstellen

Ausgangssituation:

Die SEPPmail Appliance sammelt X.509 Zertifikate aus E-Mail Signaturen. Taucht dabei ein Zertifikat einer bislang noch unbekannten Zertifizierungsstelle (CA) auf, so wird dieses ebenfalls eingesammelt. Da nicht jeder CA automatisch vertraut werden kann, müssen diese X.509 Root Zertifikate klassifiziert werden. Hierfür wird der Administrator per E-Mail benachrichtigt.

Wird der CA beziehungsweise dessen X.509 Root CA Zertifikat vertraut, so wird auch allen von dieser CA ausgestellten Zertifikaten vertraut.

Frage:

Welchen **X.509 Root Certificates**  kann das Vertrauen (trust) ausgesprochen werden?

Antwort:

Jedes Unternehmen muss gemäß Ihrer eigenen Anforderungen und des eigenen Schutzbedarfs individuell entscheiden, welchen CAs das Vertrauen ausgesprochen werden kann. Viele Unternehmen haben dazu Revisionsvorgaben. Ein HowTo oder Best Practise existiert an dieser Stelle leider nicht, insbesondere, da keine genormte Klassifizierung für die Qualität von CAs existiert. Häufig anzufindenden Einstufungen wie Class 1 -n keinesfalls aussagekräftig.

Die üblichen „Trusted CAs“, wie sie per Standard auch zum Beispiel im Windows-Zertifikats-Store zu finden sind, müssen - um hier aufgenommen zu werden - zahlreiche Zertifizierungen vorweisen können. Dabei geht es in erster Linie darum, dass diese CAs nicht kompromittiert werden können und beim Ausstellen von Zertifikaten den jeweiligen Antragsteller entsprechend durchleuchten.

Bei selbst signierten CAs werden diese Voraussetzungen meist selbst von namhaften Unternehmen nicht zu 100% erfüllt. Hilfreich sind bei diesen selbstsignierten CAs unter Umständen dann Zusammenschlüsse, wie zum Beispiel die European Bridge CA (EBCA www.ebca.de/ebca) der TeleTrust, deren Mitglieder sich freiwillig den Vorgaben dieses Zusammenschlusses unterwerfen.

Bei kleineren Betreibern selbst signierter CAs, könnte gegebenenfalls ein eigens zusammengestellter Anforderungskatalog helfen, dessen Einhaltung der Betreiber bestätigt, um Ihr Vertrauen zu erlangen.

Häufige Entscheidungskriterien im Allgemeinen sind

- akkreditierte oder self-signed CA
- Herkunftsland der CA
- CRL und/oder OCSP von der CA unterstützt, beziehungsweise auch Bereitstellungsintervall der Revokations-Informationen.
- Vertrauen per Standard in den Vertrauenswürdigen Stammzertifizierungsstellen von Windows

9.14 Allgemein: Anzeige der für den Empfänger verfügbaren Verschlüsselungsverfahren

Ausgangssituation:

Die SEPPmail Appliance hält die öffentlichen Schlüssel der externen Kommunikationspartner vor. Die Information, ob für einen Kommunikationspartner Schlüsselmaterial vorhanden ist oder nicht, soll dem Absender bereit gestellt werden.

Frage:

Wie kann dem organisationsinternen Absender die Information bereit gestellt werden, welches Verschlüsselungsverfahren beim Anfordern der Verschlüsselung zum Einsatz kommt?

Antwort:

Generell sollte das Anfordern der Verschlüsselung vom Inhalt (schützenswerte Daten oder nicht) einer E-Mail abhängig sein und nicht von den eventuellen Möglichkeiten der Verschlüsselung.

Mit der **Verschlüsselungshierarchie** [66] in Verbindung mit der **GINA Technologie** [32] wird sichergestellt, dass eine E-Mail, welche aufgrund des schützenswerten Inhalts als zu verschlüsselnd markiert wurde, auch immer verschlüsselt werden kann.

Dabei wäre die Vorabinformation für den Absender, ob ein Standard Verfahren (**S/MIME** [28], **OpenPGP** [30] oder **Domänenverschlüsselung** [31]) für einen Empfänger möglich ist oder nicht, in der Praxis kontraproduktiv, da der Absender dann gegebenenfalls - wider besseres Wissen - trotz vertraulicher Daten nicht verschlüsselt (Haftung der Geschäftsführung!)

9.15 Allgemein: E-Mails werden mit „452.3.1 Insuffizient System Storage abgewiesen“

Ausgangssituation:

Die SEPPmail Appliance ist in den E-Mail Fluss integriert. Ein abgebendes System versucht eine E-Mail an die SEPPmail Appliance zu übertragen. Dabei wird die E-Mail von der SEPPmail Appliance temporär mit der Meldung „452.3.1 Insuffizient System Storage“ abgewiesen, obwohl die Mail-Partition (siehe [Home](#)^[220] [Disk statistics](#)^[223] [Mail queue](#)^[223]) noch mit noch ca. 40% freiem Speicher angezeigt wird.

Ursache:

Dies ist eine Sicherheitsfunktion des zur E-Mail Verarbeitung integrierten Postfix. Dadurch ist gewährleistet, dass selbst dann genügend Speicher zur Verfügung steht, wenn eine neue E-Mail zum Beispiel aufgrund mehrerer Empfänger vervielfacht werden muss.

9.16 Allgemein: Automatisches Einsammeln von OpenPGP Public Keys

Ausgangssituation:

Die SEPPmail Appliance soll auch OpenPGP als Signatur- und Verschlüsselungsverfahren nutzen. Dabei fällt auf, dass öffentliche OpenPGP Schlüssel - im Gegensatz zu S/MIME Zertifikaten - von der SEPPmail Appliance nicht automatisch aus signierten E-Mails eingesammelt werden.

Frage:

Weshalb werden OpenPGP Schlüssel nicht automatisch eingesammelt, beziehungsweise was ist zu konfigurieren, um dies zu realisieren?

Antwort:

Aufgrund der unterschiedlichen Vertrauensmodelle bei den Technologien S/MIME und OpenPGP ist das automatische Einsammeln nur bei S/MIME Zertifikaten sinnvoll, beziehungsweise möglich.

Erklärung:

Ein S/MIME-Zertifikat beinhaltet den von einer Certification Authority (CA) beglaubigten öffentlichen Schlüssel und bestätigt somit die eindeutige Zugehörigkeit des beinhalteten öffentlichen Schlüssels zum Inhaber, sowie dessen Identität.

Somit ist

- das Zertifikat mit einem Pass
- die CA als beglaubigende Stelle mit dem Passamt, welches die Echtheit des Passes bestätigt vergleichbar.

OpenPGP basiert hingegen auf einem anarchistischen Vertrauensmodell (Web of Trust). Das Vertrauen wird dabei durch Vertrauensketten hergestellt, also "Ich vertraue jemanden, dem jemand vertraut, dem ich vertraue".

Um also einem OpenPGP das Vertrauen aussprechen zu können, ist ein „manuelles“ Verifizieren über einen zweiten, unabhängigen Kanal (in der Regel Telefon, SMS) durch Vergleich der Hash-Werte erforderlich.

Alternativen:

Die SEPPmail Appliance bietet folgende Möglichkeiten für den OpenPGP Schlüsselimport:

1. Durch den externen Kommunikationspartner über die GINA-Oberfläche (siehe auch [Change GINA Settings for](#)^[425] [Extended settings](#)^[431] [Certificate search and management in GINA](#)^[433])
Da über eine GINA-Anmeldung eine Person eindeutig identifiziert wird, ist das von ihr hochgeladene Schlüsselmaterial in jedem Fall vertrauenswürdig.
2. Durch den SEPPmail Appliance Administrator (siehe auch [IMPORT OPENPGP KEYS](#)^[468])
Dieser ist dafür verantwortlich, eindeutige Herkunft des Schlüsselmaterials zu prüfen.
3. Automatisiert über Key Server Abfragen (siehe auch [Mail Processing](#)^[310] [Ruleset generator](#)^[310] [Key server](#)^[310] [Type OpenPGP](#)^[310])

9.17 Allgemein: E-Mails als Anhang einer leeren Träger-E-Mail

Ausgangssituation:

Die SEPPmail Appliance ist so konfiguriert, dass sie nach dem Prüfen einer S/MIME Signatur diese nicht abschneidet. Interne E-Mail Empfänger erhalten zum Teil ihre E-Mails als Anhang einer leeren Träger-E-Mail.

Frage:

Weshalb erhalte ich teilweise E-Mails als Anhang einer leeren Träger-E-Mail?

Ursache:

Das beziehungsweise ein nachfolgendes E-Mail System - in der Regel der interne Groupware Server - versucht der E-Mail einen Disclaimer oder Footer anzuhängen, zum Beispiel „Bitte prüfen Sie, ob diese Mail wirklich ausgedruckt werden muss!“.

Dabei stellt das E-Mail-System fest, dass die von der SEPPmail Appliance kommende E-Mail über eine S/MIME Signatur verfügt. Da diese Signatur durch Anhängen des Disclaimers zerstört würde, packt das Dritt-Hersteller-System die komplette E-Mail als Anhang in eine Träger-E-Mail, welcher dann mit dem Disclaimer versehen wird.

Lösung:

1. Abstellen des Anhängens eines Disclaimers bei eingehenden E-Mails.
2. Abschneiden erfolgreich geprüfter Signaturen in der SEPPmail Konfiguration (Remove signature if S/MIME signature check succeeds).

9.18 Allgemein: E-Mails werden mangels TLS vom annehmenden Server abgewiesen

Ausgangssituation:

E-Mails der SEPPmail Appliance werden vom adressierten E-Mail Server nicht angenommen, da dieser eine TLS Verbindung erwartet, die SEPPmail Appliance jedoch keine TLS gesicherte Verbindung aufbaut.

Ursache:

Der annehmende Server erwartet TLS, offeriert jedoch keines (STARTTLS). Somit kann durch die SEPPmail Appliance das zur Verfügung stehende von TLS nicht erkannt werden, wodurch in der TLS Standardeinstellung („may“, siehe **ADD TLS DOMAIN** ²⁸² **TLS settings** ²⁸² zweiter **Hinweis** ²⁸³) auch kein Versuch unternommen wird, die Verbindung mittels TLS abzusichern.

Lösung:

Für das Ziel muss eine TLS Verbindung mit einer Ausprägung höher „may“ eingerichtet werden (siehe ebenfalls **ADD TLS DOMAIN** ²⁸² **TLS settings** ²⁸²).

9.19 Allgemein: E-Mails über ablaufende Zertifikate

Ausgangssituation:

Interne Mitarbeiter bekommen Benachrichtigungen über ablaufende Zertifikate per E-Mail. Dies zieht vermehrt Support Anfragen nach sich.

In der SEPPmail Appliance ist die **MPKI** ^[339] aktiviert und eine automatische Zertifikatserneuerung x Tage vor Ablauf eines Zertifikates eingestellt. Somit sind für die internen Benutzer stets gültige Zertifikate verfügbar.

Ursache:

- Drittssysteme von Kommunikationspartnern versenden Benachrichtigungen, sofern auf diesen Systemen ablaufende Zertifikate interner Mitarbeiter gespeichert sind. Dies obwohl diese Systeme nicht feststellen können, ob der Zertifikatsinhaber - also der interne Mitarbeiter - inzwischen ein neues Zertifikat ausgestellt bekommen hat.

Individuelle Abhilfe:

Zunächst ist ein allgemeingültiges Alleinstellungsmerkmal dieser Benachrichtigungs-E-Mails zu ermitteln. Anhand dieses Merkmals sollten E-Mails via **Custom commands** ^[308] abgewiesen werden. Dieses Abweisen muss in den **Custom commands for incoming emails BEFORE decryption** ^[308] erfolgen. Das heißt diese Option muss aktiviert werden. Der Code für das Abweisen lautet beispielsweise

Zeile	Code
01	# Begin: custom commands for incoming e-mails BEFORE decryption
02	log(1,'Begin: Custom commands for incoming e-mails BEFORE decryption');
03	if (compare('subjectX-Totemo_TrustMail_Notification_Name','equal','Recipient certificate renewal')) {
04	drop('500','Mail rejected, cannot process automatically');
05	}
06	log(1,'End: Custom commands for incoming e-mails BEFORE decryption');
07	# End: custom commands for incoming e-mails BEFORE decryption

Code

- Die CA, welche via **MPKI** ^[339] angebunden ist generiert diese E-Mails. Am Beispiel SwissSign ^[364] lautet die E-mail in etwa wie folgt:

Betreff: SwissSign – Your Certificate xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx Has Expired

Dear customer,

The following SwissSign certificate has expired:

```
/CN=Secure Mail: SEPPmail Certificate
/Email=max.mustermann@meinefirma.tld<mailto:Certificate
/Email=max.mustermann@meinefirma.tld<mailto:Certificate
/Email=max.mustermann@meinefirma.tld%3cmailto:Certificate
/Email=max.mustermann@meinefirma.tld>>
```

The request ID is

```
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

If you bought your certificate in our webshop please visit our SwissSign Webshop<<https://www.swissign.com/en>> again and request a new SwissSign Certificate. If you are a Managed PKI user please request a new certificate via your Managed PKI IT administrator.

If you have already renewed your certificate, you can ignore this message.

This is an automatically generated email. Please do not reply to this email. If you have any questions as direct customer of our SwissSign web shop please feel free to use our contact form<<https://www.swissign.com/contact>>. If you are a Managed PKI customer please contact directly the helpdesk of your organization.

Best regards,

Your SwissSign Team

Individuelle Abhilfe:

Da - wie in der Ausgangslage erwähnt - das automatische Erneuern der Zertifikate aktiv ist, sind diese Benachrichtigungen obsolet und können ignoriert werden. Um die Benachrichtigungen der CA abzustellen sollte Kontakt mit dem CA-Anbieter aufgenommen werden.

9.20 Allgemein: Entfernen von (X-)Header oder den darin enthaltenen Informationen

Ausgangssituation:

In der internen E-Mail Infrastruktur werden Header mit vertraulichen Informationen befüllt, beziehungsweise werden X-Header für diverse Zwecke verwendet.

Die Informationen sollen jedoch nicht nach außen dringen und somit an der SEPPmail Appliance entfernt werden.

Frage:

Wie können Informationen aus (X-)Header entfernt, beziehungsweise die (X-)Header komplett entfernt werden?

Lösung:

Über die entsprechenden **Custom commands** (siehe **Mail Processing Ruleset generator**) können die zu entfernenden Informationen an der gewünschten Stelle entfernt werden. Bei ausgehenden E-Mails ist das in der Regel „Custom commands for outgoing e-mails BEFORE encryption“

1. Entfernen von Informationen aus Headern

wird über den Befehl `compare()` mit dem „operator“ `substitute` realisiert.

Soll beispielsweise der String „servername.firma.local“ aus allen „Received“-Headern entfernt werden, so würde der Befehl wie folgt lauten:

```
compare('Received', 'substitute', ' servername\.firma\.local '))
```

für das Entfernen aller IP-Adressen welche mit 192.168.0. beginnen

```
compare('Received', 'substitute', '192\.168\.0\.(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?) '))
```

2. Entfernen von (X-)Headern

wird über den Befehl `rmheader()` realisiert.

Soll zum Beispiel der Header „x-originating-ip“ entfernt werden, so würde der Befehl wie folgt lauten:

```
rmheader('x-originating-ip');
```

9.21 Allgemein: Kalenderanfragen kommen als HTML-Datei mit PGP im Dateinamen an

Ausgangssituation:

Ein externer Kommunikationspartner sendet eine verschlüsselte Kalenderanfrage. Im Outlook erscheint anstatt des eigentlichen Kaledereintrags (vcs) ein html Anhang mit „PGP“ im Dateinamen.

Ursache:

Die Gegenseite scheint die Kalenderanfrage mit PGP/Inline verschlüsselt zu haben. Nach der Entschlüsselung kann Outlook nichts mehr mit der Anfrage anfangen.

Lösung:

1. Die Gegenseite kann S/MIME statt PGP verwenden.
2. Die Gegenseite kann PGP/MIME statt PGP/Inline verwenden
3. Die Einladungen können unverschlüsselt geschickt werden. Dies impliziert, dass mit Kalendereinträgen keine vertraulichen Daten gesendet werden dürfen!

9.22 Allgemein: Kalenderanfragen kommen zerstört beim Empfänger an

Ausgangssituation:

Kalenderanfragen kommen beim Kommunikationspartner zerstört an.

Ursache:

1. Die Anfrage wurde im Microsoft proprietären RTF-Format gesendet.

Individuelle Abhilfe:

Sowohl im Outlook, als auch am Exchange Server sollte das RTF Format (TNEF) deaktiviert werden. Entsprechende Dokumentationen hierfür sind beim Hersteller (Microsoft) zu finden.



Hinweis:

RTF (TNEF) ist ein Microsoft proprietäres (also kein Standard!) Format. Somit sollte dieses generell deaktiviert werden, da es Ursache für viele weitere E-Mail Probleme sein kann.

2. Die Kalenderanfrage wurde von der SEPPmail Appliance verschlüsselt. Die Gegenstelle entschlüsselt direkt im Outlook Client.

Individuelle Abhilfe:

Generell keine Kalendereinträge nicht als zu verschlüsselnd markieren. Dies impliziert, dass mit Kalendereinträgen keine vertraulichen Daten gesendet werden dürfen!

Ist die Option „Always use S/MIME or OpenPGP if user keys are available“ ist zusätzlich die Option „Exclude calendar entries“ zu verwenden (siehe [Mail Processing](#)^[286] [Ruleset generator](#)^[287] [Encryption](#)^[292] **Outgoing e-mails**^[293]).

3. E-Mail-Virens Scanner außerhalb der SEPPmail Appliance.

Individuelle Abhilfe:

Im Einzelfall zu prüfen.

9.23 Allgemein: Kennzahlen der SEPPmail Appliance

Ausgangssituation:

Für das Dimensionieren der SEPPmail Appliance(s) innerhalb einer E-Mail Infrastruktur sind deren Kennzahlen für das Sizing erforderlich.

Frage:

Wo sind die Kennzahlen - wie zum Beispiel E-Mail-Durchsatz - der SEPPmail Appliance zu entnehmen?

Antwort:

Die Kennzahlen sind unter **Sizing**  zu finden.

9.24 Allgemein: Langsames Verarbeiten von E-Mails

Ausgangssituation:

Die SEPPmail Appliance scheint E-Mails nur sehr langsam zu Verarbeiten.

Frage:

Wo sind gegebenenfalls die Ursachen für das langsame Verarbeiten auf der SEPPmail Appliance zu suchen?

Antwort:

Zunächst muss sichergestellt sein, dass die Randsysteme wie zum Beispiel vorgelagerte Schutzkomponenten (Firewall, Schutz-Relay aber auch DNS, gegebenenfalls LDAP falls angebunden und so weiter) einwandfrei arbeiten und somit nicht ursächlich für die Verzögerungen sind.

Sollten die Verzögerungen tatsächlich durch die SEPPmail Appliance verursacht werden, so liegt das meist an einem nicht erreichbaren DNS Server.

Sind unter **System** **DNS** **Use the following DNS servers** mehrere Server eingetragen, so wird eine DNS Anfrage zunächst immer an den **Primary** gerichtet. Ist dieser nicht erreichbar, wird erst nach Ablauf des Timeouts der **Alternate 1** und nach Ablauf eines weiteren Timeouts der **Alternate 1** angefragt. Aus der Summe dieser Timeouts resultiert die Verzögerung.

Dieses Phänomen potentierte sich insbesondere bei aktiviertem **Protection Pack (PP)** mit zusätzlichen DNS-Prüfverfahren wie **PTR check** / **Strict PTR check**.

Eine weitere Ursache könnte das Scannen nach Malware innerhalb von ZIP-Archiven darstellen (siehe **Search inside unencrypted zip archives**, beziehungsweise **Search inside unencrypted zip archives**).

9.25 Allgemein: Mehrere Aktionen mit einem Schlüsselwort triggern

Ausgangssituation:

Beim Verarbeiten von E-Mails auf der SEPPmail Appliance sollen mehrere Aktionen durch ein einzelnes **Schlüsselwort** [164] getriggert werden.

Frage:

Können mehrere kryptographische Aktionen durch nur ein Schlüsselwort getriggert werden, beispielsweise durch ein **Schlüsselwort** [164] [signcrypt] Verschlüsseln und Signieren gleichzeitig, also

Mail Processing [286] **Ruleset generator** [287]

Encryption [292] **Outgoing e-mails** [293] Always encrypt mails with the following text in subject [293]: [signcrypt]

Signing [298] **Outgoing e-mails** [300] S/MIME sign outgoing mails with the following text in subject [300]: [signcrypt]

Antwort:

Nativ funktioniert das Trigger beider Aktionen in der oben genannten Art und Weise nicht, da das Schlüsselwort bereits bei der zuerst durchgeführten Aktion entfernt wird und somit zum Triggern der zweiten Aktion nicht mehr zur Verfügung steht.

Jedoch ist eine Lösung via **Custom commands** [308] möglich.

Lösung:

Zunächst muss die Option **Mail Processing** [286] **Ruleset generator** [287] **Custom commands** [308] **Custom commands for outgoing e-mails BEFORE encryption** [308] aktiviert werden. Ausgehend von den Standard-**Schlüsselwörtern** [164] [confidential] für Verschlüsseln und [sign] für Signieren, würde folgendes Code-Beispiel zur Lösung führen:

Zeile	Code
01	# Begin: Custom commands for outgoing e-mails BEFORE encryption
02	log(1,'Begin: Custom commands for outgoing e-mails BEFORE encryption');
03	if (compare('subject','substitute','\[signcrypt\]')) {
04	log(1,'Found keyword [signcrypt], splitting into [confidential] and [sign]');
05	tagsubject('[confidential][sign]');
06	}
07	log(1,'End: Custom commands for outgoing e-mails BEFORE encryption');
08	# End: Custom commands for outgoing e-mails BEFORE encryption

[Code](#)

Beschreibung

In **Zeile 03** wird zunächst geprüft, ob das **Schlüsselwort** [164] [signcrypt] im Betreff der zu verarbeitenden E-Mail vorhanden ist. Dabei würde dieses entfernt werden.

Bei vorhandenem **Schlüsselwort** [164] würde nun jeweils das Standard-**Schlüsselwort** [164] für Verschlüsseln [confidential] und für Signieren [sign] in den Betreff geschrieben werden (**Zeile 05**).

Somit würden im weiteren Verlauf des Rulesets beide Aktionen getriggert.

9.26 Allgemein: Mehrere Schlüsselwörter als Trigger für eine Aktion

Ausgangssituation:

Für das Auslösen von einzelnen Aktionen beim Verarbeiten von E-Mails auf der SEPPmail Appliance sollen parallel mehrere **Schlüsselwörter** als Trigger eingesetzt werden.

Frage:

Sind mehrere Schlüsselwörter für eine Funktion, wie zum Beispiel unter **Mail Processing Ruleset generator Encryption Outgoing e-mails** Always encrypt mails with the following text in subject: möglich?

Antwort:

Ja. Aus diesem Grund sind die **Schlüsselwörter** in **Mail Processing Ruleset generator** als **Reguläre Ausdrücke** einzugeben.

Lösung:

Die gewünschten Schlüsselwörter sind als Regulärer Ausdruck, also mittel Pipe, „|“ getrennt, einzugeben. Soll also, um beim Beispiel für **Always encrypt mails with the following text in subject**: zu bleiben, sowohl auf das Schlüsselwort [confidential], als auch <c>, als auch (vertraulich) reagiert werden, so würde der Ausdruck

\[confidential\]|\<c\>|\(vertraulich\)
lauten.

Denkbar wäre dann zum Beispiel auch, auf das via **Mail Processing Ruleset generator Encryption Incoming e-mails** gesetzte Schlüsselwort für eingehend entschlüsselte E-Mails (im Standard [secure] zu reagieren, um Antworten auf ursprünglich verschlüsselte Nachrichten automatisch ebenfalls wieder zu verschlüsseln. In diesem Fall wäre oben genannter Ausdruck wie folgt zu erweitern (rot):

\[confidential\]|\<c\>|\(vertraulich\)|\[secure\]

9.27 Allgemein: Permanentes Synchronisieren mit Zeitserver (NTP)

Ausgangssituation:

In den **System** ^[224] Einstellungen (**Advanced View...**) der SEPPmail Appliance ist unter **Time and date** ^[240] das Synchronisieren mit einem Zeitserver via NTP aktiviert (**Set remote NTP server**).

Die Appliance synchronisiert unerwarteter Weise mehrmals pro Minute mit dem Zeitserver.

Ursache:

Unter optimalen Bedingungen synchronisiert NTP per Standard alle 64 bis 1024 Sekunden.

Ein kürzerer Abstand zwischen den Synchronisierungen kann durch diverse Umstände hervorgerufen werden.

Häufigste Ursachen sind jedoch

1. mangelnde Synchronisationsgüte

Individuelle Abhilfe:

Verwenden anderer Zeitserver

2. nicht zu erreichende – gegebenenfalls einzelne – Zeitserver, zum Beispiel aufgrund von Firewall-Regeln.

Individuelle Abhilfe:

- a. Freischalten des Zugangs zu allen verwendeten Zeitservern
- b. Entfernen der nicht erreichbaren Zeitserver

3. verwenden von verbindungslosen UDP mit entsprechend hoher Paketverlustrate.

Individuelle Abhilfe:

- c. Verbessern der Verbindungsqualität
- d. Verwenden von TCP anstatt UDP

Ausschlaggebend kann auch die Art der Appliance sein (Hardware oder virtuell).

Bei Microsoft Hyper-V kann zum Beispiel durch starken Clock-Drift im Gastsystem vermehrt die in Punkt 1 genannte Ursache auftreten.

9.28 Allgemein: Rückmelden der ausgeführten kryptographischen Aktionen

Ausgangssituation:

Eine SEPPmail Appliance steht im E-Mail-Fluss des Unternehmens. Die internen Absender möchten eine (E-Mail-) Benachrichtigung über die auf der Appliance ausgeführte kryptographische Aktion

Frage:

Kann der interne Absender nach dem Versand einer signierten und/oder verschlüsselten E-Mail eine Art Status-E-Mail erhalten, in welcher der erfolgreiche, signierte/verschlüsselte Versand inklusive des angewandten Verschlüsselungsverfahrens dokumentiert ist?

Antwort:

Natürlich wäre das Generieren solcher Status-E-Mails möglich. Allerdings ist so ein Verhalten weder notwendig noch wünschenswert.

Zum einen hätte die zu vermutende Anzahl dieser Status-E-Mails SPAM-Charakter.

Zum Anderen kann aufgrund der **Verschlüsselungshierarchie** ^[66] und dank der GINA-Technologie eine vom Absender als zu verschlüsselnd markierte E-Mail immer verschlüsselt werden.

Somit beschränkt sich die Rückmeldung der SEPPmail Appliance im Standard auf Fälle, in welchen die E-Mail nicht ausgeliefert werden konnte.

Dies kann im Einzelfall durch

- fehlendes Schlüsselmaterial für den Absender, beim gleichzeitigen Versuch eine E-Mail zu signieren
- eine **ENCRYPTION POLICY** ^[313], welche ein bestimmtes Verschlüsselungsverfahren erzwingt, jedoch das hierfür benötigte Schlüsselmaterial des Empfängers fehlt,

hervorgerufen werden.

9.29 Allgemein: SEPPmail Appliance NDRs werden nicht zugestellt

Ausgangssituation:

Generell werden NDRs, welche von der SEPPmail Appliance generiert werden, mit leerem Envelope Sender erzeugt. Dies ist Standard und auch sinnvoll, damit bei diesen Bounce Nachrichten keine sogenannten Loops entstehen können.

Ursache:

Im eingehenden E-Mail Fluss – also bei E-Mails aus dem Internet – wird auf einem System NACH der SEPPmail Appliance eine Bounce Address Tag Validation durchgeführt.

Lösung:

Eine entsprechende Prüfung muss gegebenenfalls auf eine Instanz vor, beziehungsweise falls die SEPPmail Appliance den Übergang zum Internet bildet auf diese verlagert werden.

Wird diese Prüfung dennoch am nachfolgenden System durchgeführt, so sind dort entsprechende Ausnahmen von der Bounce Address Tag Validation für die SEPPmail Appliance zu definieren.

9.30 Allgemein: Text Codierung (ungleich UTF-8)

Ausgangssituation:

Aufgrund einer Text Codierung ungleich UTF-8 tauchen an einem der E-Mail verarbeitenden Relays Probleme auf.

Auswirkung:

Eingehend:

Aufgrund eines eventuellen Umkodierens an einem vorgelagerten Relay, könnten E-Mails gegebenenfalls an der SEPPmail Appliance nicht mehr entschlüsselt werden, beziehungsweise anhängende Signaturen durch das Verändern zerstört worden sein.

Individuelle Abhilfe:

Möglichst keine Umkodierungen an vorgelagerten Relays vornehmen.

Ausgehend:

Bei ausgehenden E-Mails könnten Formatierungsprobleme bei anzuhängenden Disclaimern auftreten.

Ursache:

Outlook verwendet in der Regel das minimal notwendige Charset. Sind zum Beispiel keine Umlaute (oder sonstige Sonderzeichen) in der E-Mail, so würde das Charset us-ascii genutzt.

Da die SEPPmail Appliance eine E-Mail so wenig wie möglich manipuliert, würden bei Verwenden der Disclaimer-Funktion eventuell im Disclaimer enthaltene Umlaute oder Sonderzeichen in das bereits vorhandene Charset überführt. Dies führt zwangsläufig zur fehlerhaften Darstellung dieser Sonderzeichen.

Individuelle Abhilfe:

1. Für Outlook: Generelles verwenden von UTF-8 einstellen (gegebenenfalls im AD via GPOs).
2. E-Mail-Clients einsetzen, welche generell per Standard an die Landessprache angepasst sind (wie zum Beispiel Thunderbird) oder generell UTF-8 nutzen.
3. „Force UTF-8“ Einstellung der SEPPmail Appliance verwenden (siehe **EDIT DISCLAIMER** ²⁶⁷ **Disclaimer settings** ²⁶⁷ **Advanced** ²⁶⁷).

9.31 AntiSpam: Dienst startet nicht

Ausgangssituation:

Auf der SEPPmail Appliance ist das **Protection Pack (PP)** ¹⁰⁶ aktiv. Der AntiSpam Dienst (siehe **AntiSpam: Funktionen / Engine** ⁶⁸⁰) ist via **Use antisпам engine** ²⁵⁶ eingeschaltet.

Frage:

Weshalb wird in der Statusleiste der Administrationsoberfläche, beziehungsweise per Watchdog gemeldet, dass der AntiSpam Dienst (spamd) nicht gestartet ist.

Antwort:

Häufigste Ursache hierfür ist der fehlende / blockierte Zugriff auf die von SpamAssassin benötigten Ports (siehe auch Tabelle des Kapitels **Firewall / Router einrichten** ¹³⁵ Spalte **Funktion / Feature** "**Protection Pack** ¹²⁶ (optional)").

9.32 AntiSpam: Funktionen / Engine

Ausgangssituation:

Die SEPPmail Appliance bildet den Übergang zum Internet. Aus diesem Grund sollen, beziehungsweise müssen die AntiSpam Funktionen aktiviert werden

Frage:

Welche AntiSpam Funktionen, beziehungsweise Engine beinhaltet das **Protection Pack (PP)**  der SEPPmail Appliance?

Antwort:

In einer ersten Stufe der Spam Abwehr kommen die in Postfix integrierten Filtermöglichkeiten (Header Checks, RBL, Reverse Lookups, etcetera) zum Einsatz.

Als zweite Stufe wird SpamAssassin verwendet.

Weiterhin steht eine eigenentwickelte Anti-Spoofing Funktion zur Verfügung.

Abgewiesen werden E-Mails grundsätzlich per inline rejection. Ein Quarantäne Bereich ist deshalb weder notwendig noch gewünscht.

9.33 AntiVirus: Funktionen / Engine

Ausgangssituation:

Die SEPPmail Appliance soll den E-Mail Verkehr auf Malware überprüfen, zum Beispiel, weil die SEPPmail Appliance den Übergang zum Internet bildet oder ein vorgelagertes Schutz-Relay verschlüsselte E-Mail nicht scannen kann (Zweistufigkeit des Virenskans).

Frage:

Welche AntiVirus Funktionen, beziehungsweise Engine beinhaltet das **Protection Pack (PP)**  der SEPPmail Appliance?

Antwort:

Eingesetzt wird ClamAV, optional mit Zusatzsignaturen von Sanesecurity.

9.34 AntiVirus: Wo erfolgt der Scan

Ausgangssituation:

Das **Protection Pack (PP)** ¹⁰⁰¹ der SEPPmail Appliance ist lizenziert und der Virensan aktiviert.

Frage:

Wo im System wird nach Viren gescannt?

Antwort:

Der Scan erfolgt innerhalb des SMTP-Daemon. Hier findet die zentrale E-Mail-Verarbeitung – auch der GINA-Mails – in der SEPPmail Appliance statt.

9.35 Backup: Kopieren von SEPPmail Appliance Backups

Ausgangssituation:

Die SEPPmail Appliance erstellt täglich um Mitternacht automatisiert ein Backup und sendet dieses per Standard an die Mitglieder der **Group backup (Backup Operator)** ^[413].

Frage:

Können Backups auch im Dateisystem kopiert/abgeholt werden?

Antwort:

Ja, die SEPPmail Appliance bietet die Möglichkeit die erstellten Backups per SCP abzuholen (siehe **Administration** ^[363] **Backup** ^[375] **Backup using scp**).

9.36 Backup: Quiescing

Ausgangssituation:

Die SEPPmail Appliance wurde auf einem Linux basierendem Virtualisierer (ESX, KVM,...) eingebunden. Dort soll die virtuelle Appliance unter Verwendung von „quiescing“ gesichert werden.

Frage:

Unterstützt die SEPPmail Appliance „quiescing“?

Antwort:

Nein.

Normalerweise wird die Quiescing-Funktion von den VMware-Tools bereitgestellte Funktion geprüft.

Da in den VMware-Tools für OpenBSD jedoch genau die Funktion, welche für das „quiescing“ benötigt wird, nicht zur Verfügung steht, schlägt das Backup an dieser Stelle fehl.

Auswirkung:

Beim Sichern der virtuellen SEPPmail Appliance über Drittanbieter Tools wie zum Beispiel „Networker“ oder „Veeam“, zeigt diese Sicherungssoftware unter Umständen eine Meldung wie

An error occurred while quiescing the virtual machine

sofern die VMware Tools auf der SEPPmail Appliance aktiv sind.

Individuelle Abhilfe:

Die bevorzugte Vorgehensweise zur Lösung des Problems ist das „quiescing“ für die Sicherung der virtuellen SEPPmail Appliance in der Sicherungssoftware auszuschalten.

Sollte dies nicht möglich sein, so können alternativ auch die VMware-Tools in der Appliance deaktiviert werden (siehe **System**^[224], Ansicht **Advanced view...**, **Virtualization tools**^[246] **Enable VMware tools**^[246]).

Dabei ist zu beachten, dass mit dem Deaktivieren der VMware-Tools die Optionen zur Steuerung der virtuellen Maschine (zum Beispiel Reboot/Shutdown) über die Konsole des Host-Systems nicht mehr verfügbar sind.



Hinweis:

Quiescing ist in etwa das Pendant bei Linux basierten Systemen zu Microsofts Volume Shadow Copy .

Dabei wird das zu sichernde System im laufenden Betrieb in einen für Backups geeigneten Zustand versetzt.

9.37 Backup: Volume Shadow Copy for Linux

Ausgangssituation:

Die SEPPmail Appliance wurde auf einem Microsoft basierendem Virtualisierer (Hyper-V) eingebunden. Dort soll die virtuelle Appliance unter Verwendung von „Volume Shadow Copy for Linux“ gesichert werden.

Frage:

Unterstützt die SEPPmail Appliance „Volume Shadow Copy for Linux“?

Antwort:

Nein.

Die SEPPmail Appliance basiert aus Sicherheitsgründen nicht auf einem Linux System, sondern auf OpenBSD. Für OpenBSD steht ein entsprechendes Tool nicht zur Verfügung.



Hinweis:

Microsofts Volume Shadow Copy ist in etwa das Pendant zum quiescing bei Linux basierten Systemen.

Volume Shadow Copy for Linux kommt also in Linux basierten Gastsystemen zum Einsatz, welche über einen Microsoft basierten Virtualisierer (Hyper-V) gesichert werden sollen

Dabei wird das zu sichernde System im laufenden Betrieb in einen für Backups geeigneten Zustand versetzt.

9.38 Benutzer: Anlage / Zertifikatsbezug auf Basis des Envelope- oder Sender-Eintrags

Ausgangssituation:

Aufgrund individueller Anforderungen sollen die **Users** ^[396] auf der SEPPmail Appliance nicht anhand des Eintrags im From-Header einer ausgehenden E-Mail sondern aufgrund des Eintrags im Sender-Header oder des Envelope-Senders angelegt werden. Ebenso soll der Zertifikatsbezug angepasst werden.

Frage:

Ist das Anlegen von **Users** ^[396] sowie der Zertifikatsbezug auf Basis des Envelope- oder Sender-Eintrags möglich und wenn ja, wie?

Antwort:

Die Reihenfolge, welcher Absender einer E-Mail für die Anlage des **Users** ^[396] herangezogen wird, kann durch die Variable `createAccountAddressOrder` für die Anlage des und durch `createKeysAddressOrder` für den Zertifikatsbezug gesteuert werden (siehe Tabelle):

Wert	Reihenfolge			Standard
f,s,e	From-Header	Sender-Header	Envelope-Sender	x
s,e,f	Sender-Header	Envelope-Sender	From-Header	
e,f,s	Envelope-Sender	From-Header	Sender-Header	
e,s,f	Envelope-Sender	Sender-Header	From-Header	
s,f,e	Sender-Header	From-Header	Envelope-Sender	
f,e,s	From-Header	Envelope-Sender	Sender-Header	

**Achtung:**

Der Standard basiert darauf, dass ein E-Mail Client beim Prüfen einer E-Mail Signatur den Absender aus dem From-Header zum Vergleich mit dem in Zertifikat eingetragenen CN (Common Name) heranzieht.

Einige E-Mail Clients ziehen alternativ den Eintrag aus dem Sender-Header heran, sofern dieser vorhanden ist und der Vergleich des CN mit dem Eintrag des From-Headers fehlgeschlagen ist. Der Envelope-Sender wird nie zum Vergleich herangezogen (siehe gegebenenfalls auch

[Verwendeter Schlüssel bei Microsoft Vertreterregelung](#) [827] [827].

Beispielcode

- Überprüfen der Einstellung **Mail Processing** [286] **Ruleset generator** [287] **User creation** [289] Create accounts for new users if user tries to sign / encrypt [289]
- Navigieren zu **Mail Processing** [286] **Ruleset generator** [287] **Custom commands** [308] **Custom commands for User Creation** [308]:
- Aktivieren der Option, sowie Einfügen des folgenden Codes in das darunter liegende Eingabefeld:

Zeile	Code
01	# Begin: Custom commands for User Creation
02	log(1,'Begin: Custom commands for User Creation');
03	if (!authenticated()) {
04	setvar('createAccountAddressOrder','f,s,e');
05	setvar('createKeysAddressOrder','f,s,e');
06	if (!empty('\$header from')) {
07	log(1,'creating user, based on from header \$header from');
08	} else if (!empty('\$sender')) {{
09	log(1,'creating user, based on sender header \$sender');
10	} else if (!empty('\$from')) {{
11	log(1,'creating user, based on envelope sender \$from');
12	}
13	createaccount();
14	createkeys('@CREATEGPGKEYS@');
15	}
16	log(1,'End: Custom commands for User Creation');
17	# End: Custom commands for User Creation

Code**Beschreibung**

Der Abschnitt **Custom commands for User Creation:** wird bei aktiver Option **Create accounts for new users if user tries to sign / encrypt** [289] nur dann ausgeführt, wenn vom Absender eine kryptographische Aktion angefordert wurde. Ist diese Voraussetzungen gegeben, wird in diesem Beispiel zunächst geprüft, ob der **User** [396] noch nicht vorhanden ist (**Zeile 03**). In diesem Fall wird zunächst festgelegt, in welcher Reihenfolge in der E-Mail vorhandenen Absenderadressen (Envelope, From- oder Sender-Header) für das Anlegen des neuen **Users** [396] (**Zeile 04**), beziehungsweise für den Bezug des Zertifikates (**Zeile 05**) herangezogen wird. In den **Zeilen 06 bis 12** wird im Log festgehalten, welche der Adressen für die Anlage zum Einsatz kam. Nun wird der **User** [396] angelegt (**Zeile 13**) und das Schlüsselmaterial gemäß der Einstellung unter **Mail Processing** [286] **Ruleset generator** [287] **Key generation** [291] für den neu angelegten **User** [396] bezogen (**Zeile 14**).

Verwendete**Befehle**

bounce() [548]
 createaccount() [539]
 createkeys() [540]
 empty() [530]
 log() [534]
 setvar() [522]

Funktionen

@CREATEGPGKEYS@ [630]

9.39 Benutzer: Anlage mittels LDAP Abfrage

Ausgangssituation:

Das automatische Generieren von Benutzern soll auf einen bestimmten Personenkreis eingeschränkt werden. Das Bestimmen des Personenkreis soll zum Beispiel durch die Abfrage eines LDAP-Verzeichnisdienstes erfolgen.

Konfigurationsvorschlag

- Überprüfen der Einstellung **Mail Processing** ^[286] **Ruleset generator** ^[287] **User creation** ^[289] Create accounts for new users if user tries to sign / encrypt ^[289]
- Navigieren zu **Mail Processing** ^[286] **Ruleset generator** ^[287] **Custom commands** ^[308] **Custom commands for User Creation** ^[308]:
- Aktivieren der Option, sowie Einfügen des folgenden Codes in das darunter liegende Eingabefeld:

Zeile	Code
01	# Begin: Custom commands for User Creation
02	log(1,'Begin: Custom commands for User Creation');
03	if (!authenticated()) {
04	if (ldap_compare('192.168.10.10;CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local;mypassword;OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local;(mail=\$from)', 'memberOf', 'SecureMail')) {
05	log(1,'\$header_from is member of SecureMail, creating user, generating keys');
06	createaccount();
07	createkeys('@CREATEGPGKEYS@');
08	} else {
09	log(1,'\$header from is not member of SecureMail, bouncing e-mail');
10	bounce('bounce_noenc');
11	}
12	} else {
13	createkeys('@CREATEGPGKEYS@');
14	}
15	log(1,'End: Custom commands for User Creation');
16	# End: Custom commands for User Creation

Code

Beschreibung

Der Abschnitt **Custom commands for User Creation:** wird bei aktiver Option Create accounts for new users if user tries to sign / encrypt ^[289] nur dann ausgeführt, wenn vom Absender eine kryptographische Aktion angefordert wurde. Ist diese Voraussetzungen gegeben, wird in diesem Beispiel zunächst über eine LDAP-Anfrage (in diesem Fall AD) die Zugehörigkeit des Absenders zur berechtigten Gruppe geprüft (**Zeile 04**). Ist der Absender berechtigt, so wird dies im Log eingetragen (**Zeile 05**), der Absender als Benutzer in der SEPPmail Appliance angelegt (**Zeile 06**) und mit den unter **Mail Processing** ^[286] **Ruleset generator** ^[287] **Key generation** ^[291] angegebenen Schlüsselmaterial versorgt (**Zeile 07**). Andernfalls wird dies ebenfalls in das Log eingetragen (**Zeile 09**), die E-Mail jedoch abgewiesen (**Zeile 10**). Durch den Befehl in **Zeile 13** wird bei bereits vorhandenen Benutzern sichergestellt, dass diese mit gültigem Schlüsselmaterial versorgt werden, sofern nicht bereits vorhanden.

Verwendete

Befehle

bounce() ^[548]
 createaccount() ^[539]
 createkeys() ^[540]
 ldap_compare() ^[620]
 log() ^[534]

Funktionen

keine

9.40 Benutzer: Berechtigung mittels LDAP Abfrage

Ausgangssituation:

Die Berechtigung für das Durchführen kryptographischer Aktionen soll im Live-Betrieb geprüft werden. Das Abfragen der Berechtigung soll mittels Abfrage eines LDAP-Verzeichnisdienstes realisiert werden.

Konfigurationsvorschlag



Achtung:

Durch diese Art des Implementierens wird beim Versand jeder einzelnen, kryptographisch zu behandelnden E-Mail eine LDAP-Abfrage gestartet. Trotz cachens der Verbindung seitens der SEPPmail Appliance, kann dies unter Umständen zu erheblichen Performance Einbußen, beziehungsweise gegebenenfalls auch zum Überlasten des/r LDAP-Server/s führen.

- Navigieren zu **Mail Processing** ²⁸⁶ **Ruleset generator** ²⁸⁷ **Custom Commands** ³⁰⁸ **Custom commands for outgoing e-mails BEFORE encryption:**
- Aktivieren der Option, sowie Einfügen des folgenden Codes in das darunter liegende Eingabefeld:

Zeile	Code
01	# Begin: Custom commands for outgoing e-mails BEFORE encryption
02	log(1,'Begin: Custom commands for outgoing e-mails BEFORE encryption');
03	# Begin: check if user is allowed to to send cryptographic e-mails
04	log(1,'Begin: check if user is allowed to to send cryptographic e-mails');
05	setvar('ldap_bind','ldaps://myldap1.local,ldaps://myldap2.local;CN=ldapquery,OU=ServiceAccounts,OU=Benutzer,DC=customer1,DC=local;Kennwort;OU=Benutzer,DC=customer1,DC=local;(mail=\$header from)');
06	if (ldap compare('\$ldap_bind','memberOf','Secure E-Mail')) {
07	if(authenticated()) {
08	setuserattr('accountOptions','0');
09	} else {
10	log(1,'\$from is member of SecureMail, creating user, generating keys');
11	ldap read('\$ldap_bind','displayName','displayName');
12	ldap read('\$ldap_bind','sAMAccountName','sAMAccountName');
13	createaccount('0','\$sAMAccountName','\$displayName');
14	createkeys('@CREATEGPGKEYS@');
15	}
16	} else {
17	if(authenticated()) {
18	log(1,'\$from is not longer member of SecureMail, revoking permission to encrypt and/or sign e-mails');
19	setuserattr('accountOptions','5');
20	} else {
21	log(1,'\$from is not member of SecureMail, user does not exist, nothing to do');
22	}
23	## force domain encryption - if available - for unlicensed users
24	## only needed if "Always use S/MIME or OpenPGP if user keys areavailable" is selected
25	## and "User creation" is not set to "Manual user creation: Only process outgoing mails from users with an account"
26	if (domain smime keys avail()) {

Zeile	Code
27	log(1,'found S/MIME domain certificate for recipient(s) \$header_to; \$header_cc - trying to encrypt mail');
28	if (encrypt domain smime()) {
29	log(1,'S/MIME Domain Encryption successful for recipient(s) \$header_to; \$header_cc');
30	deliver();
31	} else {
32	log(1,'S/MIME Domain Encryption FAILED for recipient(s) \$header_to; header cc - trying OpenPGP Domain Encryption');
33	}
34	} else {
35	log(1,'no S/MIME domain certificate found for recipient(s) \$header_to; \$header_cc - trying OpenPGP Domain Encryption');
36	}
37	if (domain pgp keys avail()) {
38	log(1,'found OpenPGP public domain key for recipient(s) \$header_to; \$header_cc - trying to encrypt mail');
39	if (encrypt domain pgp()) {
40	log(1,'OpenPGP Domain Encryption successful for recipient(s) \$header_to; \$header_cc');
41	deliver();
42	} else {
43	log(1,'pgp domain encryption FAILED - going on without any action');
44	}
45	} else {
46	log(1,'Recipient(s) \$header_to; \$header_cc have no valid public OpenPGP key');
47	}
48	log(1,'No domain encryption possible for \$header_to; \$header_cc, sending plain');
49	deliver();
50	## end forcing domain encryption
51	}
52	log(1,'End: check if user is allowed to to send cryptographic e-mails');
53	# End: check if user is allowed to to send cryptographic e-mails
54	log(1,'End: Custom commands for outgoing e-mails BEFORE encryption');
55	# End: Custom commands for outgoing e-mails BEFORE encryption

Code

Beschreibung

In diesem Beispiel wird zunächst die statischen Parameter für die folgende LDAP-Abfrage in die Variable „ldap_bind“ geschrieben (**Zeile 05**). Über eine LDAP-Anfrage (in diesem Fall AD) wird die Zugehörigkeit des Absenders zur berechtigten Gruppe geprüft (**Zeile 06**). Ist der Absender berechtigt, so wird geprüft, ob er bereits ein Konto auf der SEPPmail Appliance hat (**Zeile 07**). Ist ein Konto vorhanden, so werden diesem die Rechte für das Verschlüsseln/Signieren zugewiesen (**Zeile 08**). Andernfalls wird zunächst ein Log Eintrag (**Zeile 10**) erzeugt, der Windows Benutzer- und der Anzeigenname aus dem AD ausgelesen und jeweils als Variable bereit gestellt (**Zeile 11/12**). Nun wird ein neues Benutzerkonto für den Absender erzeugt (**Zeile 13**). Dabei werden für „User ID“ und „Name“ die zuvor aus dem AD ausgelesenen Werte verwendet. Anschließend wird der neu angelegte User mit Schlüsselmaterial gemäß der Vorgabe aus **Mail Processing** ^[286] **Ruleset generator** ^[287] **Key generation** ^[288] bestückt (**Zeile 14**).

Ist der Absender im Besitz eines Kontos auf der SEPPmail Appliance, jedoch nicht mehr Mitglied der entsprechenden AD-Gruppe (**Zeile 17**), so wird dies im Log vermerkt (**Zeile 18**) und dem Benutzer die Rechte für

das Verschlüsseln/Signieren entzogen (**Zeile 19**) (damit das Schlüsselmaterial auf der Appliance erhalten bleibt, wird das Konto lediglich deaktiviert, nicht gelöscht. Durch das Deaktivieren des Benutzerkontos wird die verwendete Benutzerlizenz wieder freigegeben).
Für Absender, welche weder im Besitz eines Benutzerkontos, noch Mitglied der berechtigenden AD-Gruppe sind, ist keine Aktion erforderlich. Dies wird so in das Log eingetragen (**Zeile 21**).

Die durch die Kommentarzeilen `## force domain encryption` und `## end forcing domain encryption` eingegrenzten Befehle sind nur dann notwendig, wenn die Option „Always use S/MIME or OpenPGP if user keys are available“ **des Abschnitts Mail Processing Ruleset generator Encryption/Decryption** aktiviert wurde und **Mail Processing Ruleset generator User creation** nicht auf **Do not create accounts (also disables custom commands for user creation)** steht.

Hierdurch wird für den beschriebenen Konfigurationsfall gewährleistet, dass die **Domänenverschlüsselung** auch dann zum Tragen kommt, wenn vom Empfänger ein öffentlicher Domänenschlüssel vorhanden, der Absender jedoch nicht in der Gruppe der zum Verschlüsseln berechtigten Personen ist.

So wird zunächst geprüft, ob ein öffentlicher S/MIME Domänenschlüssel der Ziel-E-Mail Domäne(n) vorhanden ist (**Zeile 26**). Ist dies der Fall, so wird das protokolliert (**Zeile 27**) und die E-Mail an die Ziel-E-Mail-Domänen mit dem jeweiligen Schlüssel verschlüsselt (**Zeile 28**), im Log dokumentiert (**Zeile 29**) und die E-Mail ausgeliefert (**Zeile 30**). Schlägt das S/MIME-Domänenverschlüsseln fehl, so wird dies ebenso protokolliert (**Zeile 32**), als wenn kein S/MIME Schlüssel des/r Empfänger vorhanden ist (**Zeile 35**). Für diejenigen Empfängerdomänen, für die kein S/MIME Schlüssel bekannt ist, oder die Verschlüsselung fehlschlug, wird nun versucht, mit einem öffentlichen OpenPGP Domänenschlüssel zu verschlüsseln. Auch hier wird zunächst geprüft, ob ein öffentlicher OpenPGP Domänenschlüssel der Ziel-E-Mail Domäne(n) vorhanden ist (**Zeile 37**). Ist dies der Fall, so wird das protokolliert (**Zeile 38**) und die E-Mail an die Ziel-E-Mail Domänen mit dem jeweiligen Schlüssel verschlüsselt (**Zeile 39**), im Log dokumentiert (**Zeile 40**) und die E-Mail ausgeliefert (**Zeile 41**). Schlägt die Verschlüsselung fehl, so wird dies ebenso protokolliert (**Zeile 43**), als wenn kein OpenPGP Schlüssel des/r Empfänger vorhanden ist (**Zeile 46**).

Sofern nicht bereits aufgrund einer erfolgreichen Domänenverschlüsselung ausgeliefert wurde, wird unverschlüsselt versendet (**Zeile 49**), ungeachtet eventuell vorhandener Steuerkennzeichen (siehe **Steuern der Appliance**).

Dieses Verhalten kann natürlich durch entsprechenden Zusatzcode bei Bedarf ebenfalls angepasst werden.

Verwendete

Befehle

```
authenticated()
createaccount()
createkeys()
deliver()
domain_pgp_keys_avail()
domain_smime_keys_avail()
encrypt_domain_pgp()
encrypt_domain_smime()
ldap_compare()
log()
setuserattr()
```

Funktionen

keine

9.41 Benutzer: Einschränken des LFT berechtigten Personenkreises

Ausgangssituation:

LFT [186] soll auf der SEPPmail Appliance genutzt werden. Die Voraussetzungen hierfür (gültige Lizenz / zusätzlicher Plattenspeicher) wurden bereits geschaffen und die Konfiguration vorgenommen (siehe **CHANGE GINA SETTINGS FOR** [423] **Large File Transfer** [439]). Jedoch soll das Nutzen dieses Features aufgrund bestimmter Kriterien (zum Beispiel AD-Gruppenzugehörigkeit, bestimmte E-Mail Adressen, sendende IP-Adresse) eingeschränkt werden.

Lösung:

Die berechtigten Personen sollen in einer Microsoft Active Directory (AD) Gruppe zusammengefasst werden. Die Zugehörigkeit eines Senders kann über eine LDAP-Abfrage im AD geprüft werden. Nur wenn der Absender für den **LFT** [186] Versand berechtigt ist, wird **LFT** [186] ausgeführt. Andernfalls wird eine zu definierende Aktion (Versand als „normale“ E-Mail / Bounce) ausgeführt.

Konfigurationsvorschlag:

Abfrage einer bestimmten AD-Gruppenzugehörigkeit eines Absenders

- Navigieren zu **Mail Processing** [286] **Ruleset generator** [287] **Custom commands** [308] **Custom macros and commands for all e-mails BEFORE processing:** [309]
- Aktivieren der Option, sowie Einfügen des folgenden Codes in das darunter liegende Eingabefeld:

Zeile	Code
01	# Begin: Custom macros and commands for all e-mails BEFORE processing
02	log(1,'Begin: Custom macros and commands for all e-mails BEFORE processing');
03	# Begin: Check if e-mail is LFT and user is allowed to send LFT
04	log(1,'Begin: Check if e-mail is LFT and user is allowed to send LFT');
05	if(!incoming()) {
06	if (!internal()) {
07	if (compareattr('use lfm','equal','1')) {
08	log(1,'Mail is LFT, check if user is allowed to use');
09	if (ldap_compare('192.168.10.10;CN=Peter Mueller,OU=Users,OU=MyBusiness,DC=Firma,DC=local;mypassword;OU=Users,OU=MyBusiness,DC=Firma,DC=local;mail=\$sender','memberOf','LFT-Benutzer')) {
10	log(1,'User is allowed to send large files, proceeding');
11	} else {
12	log(1,'User is not allowed to send large files, e-mail will be dropped');
13	drop('500','User is not allowed to send large files');
14	}
15	}
16	}
17	}
18	log(1,'End: Check if e-mail is LFT and user is allowed to send LFT');
19	# End: Check if e-mail is LFT and user is allowed to send LFT
20	log(1,'End: Custom macros and commands for all e-mails BEFORE processing');
21	# End: Custom macros and commands for all e-mails BEFORE processing

Code

Beschreibung

In diesem Beispiel wird zunächst geprüft, ob es sich um eine ausgehende „LFT“-Mail handelt (**Zeilen 05 - 07**). Ist dies der Fall, wird über eine LDAP-Anfrage (in diesem Fall AD) die Zugehörigkeit des Absenders zur berechtigten Gruppe geprüft (**Zeile 09**). Ist der Absender berechtigt, so wird dies im Log eingetragen und im Ruleset

fortgefahren (**Zeile 10**). Andernfalls wird dies ebenfalls in das Log eingetragen (**Zeile 12**), die E-Mail jedoch verworfen (**Zeile 13**).

Variationen

Anstelle des LDAP-Vergleichs in **Zeile 09** mittels `ldap_compare()` [620], könnte auch `compare()` [525] oder `compareattr()` [527] zum Einsatz kommen:

Zeile	Code
09	<code>if (compare('to','match','mail@address')) {</code>

Zeile	Code
09	<code>if (compareattr('connect from','equal','192.168.139.1')) {</code>

Anstelle des Befehls `drop()` [552] in **Zeile 13**, kann die E-Mail über den Befehl `bounce()` [548], unter Verwendung einer entsprechenden Vorlage (hier `bounce_LFT`), abgewiesen werden.

Zeile	Code
12	<code>log(1,'User is not allowed to send large files, e-mail will be bounced');</code>
13	<code>bounce('bounce_LFT');</code>

Soll das Senden als LFT-Nachricht einfach nur unterdrückt werden, kann anstelle des Befehls `drop()` [552] die mutmaßliche LFT-Nachricht in eine „normale“ SMTP-Mail zurückkonvertiert werden.

Zeile	Code
12	<code>log(1,'User is not allowed to send large files, e-mail will be sent as "normal" SMTP-mail);</code>
13	<code>flag('nolmf', true);</code>
13a	<code>flag('x-smlfm', false);</code>
13b	<code>setheader('X-ESWmail-LFM','NO');</code>

Verwendete

Befehle

`bounce()` [548]
`compare()` [525]
`compareattr()` [527]
`drop()` [552]
`flag()` [553]
`incoming()` [516]
`internal()` [516]
`ldap_compare()` [620]
`log()` [534]
`setheader()` [563]

Funktionen

keine

9.42 CDM: Personalisierte Grußformel automatisiert erstellen

Ausgangssituation:

Für das Erweitern der Disclaimer- zur Footer-Funktion, sollen die persönlichen Daten des Absenders der SEPPmail Appliance zunächst bekannt gemacht werden. Hierfür sollen die benötigten Informationen, wie zum Beispiel Name, Telefonnummer und so weiter, zunächst von einem Drittsystem per LDAP in Erfahrung gebracht werden.

Frage:

Wie können über das **Central Disclaimer Management (CDM)** ^[125] personalisierte Fußnoten für die internen Absender von E-Mails erstellt werden?

Lösung:

Folgend wird eine Beispielabfrage aus Microsoft Active Directory (AD) dargestellt. Dabei werden die Variablen weiterhin so aufbereitet, dass Sie entsprechend für HTML- und TXT-Footer verwertbar sind. Damit wird vermieden, dass bei leeren Variablen zum Beispiel Trennzeichen stehen bleiben.

Die benötigten Werte werden über einen entsprechenden Code in der aktiven Option **Custom commands for outgoing e-mails BEFORE encryption** aus **Mail Processing** ^[286] **Ruleset generator** ^[287] **Custom Commands** ^[308] in Variablen umgesetzt:

Zeile	Code
001	# Begin: Custom commands for outgoing e-mails BEFORE encryption
002	log(1,'Begin: Custom commands for outgoing e-mails BEFORE encryption');
003	# Begin: Getting footer information for disclaimer
004	log(1,'Begin: Getting footer information for disclaimer');
005	# Begin: Setting sender domain based ldap-bind information
006	log(1,'Begin: Setting sender domain based ldap-bind information');
007	if (compare('from','match','@sample-company1.tld')) {
008	log(1,'setting ldap-bind information for sample-company1.tld');
009	setvar('ldap_cust','192.168.1.5;CN=ldapquery,OU=ServiceAccounts,OU=Users,DC=sample-company1,DC=tld;ldapquery_password;OU=Users,DC=sample-company1,DC=tld;mail=\$header from');
010	}
011	if (compare('from','match','@sample-company1.tld')) {
012	log(1,'setting ldap-bind information for sample-company2.tld');
013	setvar('ldap_cust','192.168.1.5;CN=ldapquery,OU=ServiceAccounts,OU=Users,DC=sample-company2,DC=tld;ldapquery_password; OU=Users,DC=sample-company2,DC=tld;mail=\$header from');
014	}
015	# Begin: Set variables to empty
016	setvar('\$displayName','');
017	setvar('\$title','');
018	setvar('\$company','');
019	setvar('\$locality','');
020	setvar('\$telefon','');
021	setvar('\$durchwahl','');
022	setvar('\$mobil','');
023	setvar('\$fax','');
024	setvar('\$e-mail','');
025	setvar('\$internet','');

Zeile	Code
026	setvar('\$telephoneNumber','');
027	setvar('\$physicalDeliveryOfficeName','');
028	setvar('\$mobile','');
029	setvar('\$facsimileTelephoneNumber','');
030	setvar('\$mail','');
031	setvar('\$wWWHomePage','');
032	setvar('\$HTMLdisplayName','');
033	setvar('\$HTMLtitle','');
034	setvar('\$HTMLcompany','');
035	setvar('\$HTMLlocality','');
036	setvar('\$HTMLtelefon','');
037	setvar('\$HTMLdurchwahl','');
038	setvar('\$HTMLmobil','');
039	setvar('\$HTMLfax','');
040	setvar('\$HTMLe-mail','');
041	setvar('\$HTMLinternet','');
042	setvar('\$HTMLtelephoneNumber','');
043	setvar('\$HTMLphysicalDeliveryOfficeName','');
044	setvar('\$HTMLmobile','');
045	setvar('\$HTMLfacsimileTelephoneNumber','');
046	setvar('\$HTMLmail','');
047	setvar('\$HTMLwWWHomePage','');
048	# End: Set variables to empty
049	log(1,'End: Setting sender domain based ldap-bind information');
055	# End: Setting sender domain based ldap-bind information
051	# Begin: Reading footer information from ldap
052	log(1,'Begin: Reading footer information from ldap');
053	ldap read('\$ldap cust','displayName','displayName');
054	if (!empty('\$displayName')) {
055	setvar('HTMLdisplayName','\$displayName ');
056	}
057	ldap read('\$ldap cust','title','title');
058	if (!empty('\$title')) {
059	setvar('HTMLtitle','\$title ');
060	}
061	ldap read('\$ldap cust','company','company');
062	if (!empty('\$company')) {
063	setvar('HTMLcompany','\$company ');
064	}
065	ldap read('\$ldap cust','l','l');
066	if (!empty('\$l')) {
067	setvar('HTMLlocality','\$l ');
068	}
069	ldap read('\$ldap cust','telephoneNumber','telephoneNumber');
070	if (!empty('\$telephoneNumber')) {

Zeile	Code
071	setvar('HTMLtelephoneNumber','\$telephoneNumber ');
072	setvar('HTMLtelefon','Telefon ');
073	}
074	ldap_read('\$ldap_cust','physicalDeliveryOfficeName','physicalDeliveryOfficeName');
075	if (!empty('\$physicalDeliveryOfficeName')) {
076	setvar('HTMLphysicalDeliveryOfficeName','\$physicalDeliveryOfficeName ');
077	setvar('HTMLdurchwahl','Durchwahl ');
078	}
079	ldap_read('\$ldap_cust','facsimileTelephoneNumber','facsimileTelephoneNumber');
080	if (!empty('\$facsimileTelephoneNumber')) {
081	setvar('HTMLfacsimileTelephoneNumber','\$facsimileTelephoneNumber ');
082	setvar('HTMLfax','FAX ');
083	}
084	ldap_read('\$ldap_cust','mobile','mobile');
085	if (!empty('\$mobile')) {
086	setvar('HTMLmobile','\$mobile ');
087	setvar('HTMLmobil','Mobil ');
088	}
089	ldap_read('\$ldap_cust','mail','mail');
090	if (!empty('\$mail')) {
091	setvar('HTMLmail','\$mail ');
092	setvar('HTMLE-mail','E-Mail </br>');
093	}
094	ldap_read('\$ldap_cust1','wWWHomePage','wWWHomePage');
095	if (!empty('\$wWWHomePage')) {
096	setvar('HTMLinternet','Internet');
097	setvar('HTMLwWWHomePage','\$wWWHomePage');
098	}
099	log(1,'End: Reading footer information from ldap');
100	# End: Reading footer information from ldap
101	log(1,'End: Getting footer information for disclaimer');
102	# End: Getting footer information for disclaimer
103	log(1,'End: Custom commands for outgoing e-mails BEFORE encryption');
104	# End: Custom commands for outgoing e-mails BEFORE encryption

Code

Im Beispiel werden die benötigten Attribute aus dem Benutzerobjekt - welches anhand der Absender-E-Mail-Adresse ermittelt wird - unter dem, zum LDAP-Attribut gleichlautenden Variablennamen bereitgestellt, also beispielsweise der „Anzeigenname des Benutzers“ unter dem Variablennamen „displayName“ und - wie oben erwähnt - für die entsprechenden Parts (HTML/TXT) aufbereitet

Die so erzeugten Variablen können nun im Untermenü, welches aus **Mail System**  **Edit mail disclaimer...**  aufgerufen wird, verwendet werden.

Um die im folgenden Beispiel verwendeten Bilder zu Verwenden, sind diese zunächst unter **Disclaimer as HTML** unter **Inlines** hochzuladen, also

Name	Content-Type	Content-ID
facebook.png	image/x-png	facebook.png
LinkedIn.png	image/x-png	LinkedIn.png
RSS.png	image/x-png	RSS.png
sc_logo.png	image/x-png	sc_logo.png
Twitter.png	image/x-png	Twitter.png
veranstaltung.png	image/x-png	veranstaltung.png

Im HTML Eingabefeld folgt der entsprechende Code, der so aussehen könnte:

```
<body>
  <html lang="de">
  <meta charset="UTF-8" />

  <p><span style="font-size: 10.0pt;font-family: Arial , sans-serif;color: rgb(0,0,0);">
    <br/><br/>
    Mit freundlichen Gr&uuml;&szlig;en<br/><br/>
    $HTMLdisplayName
    $HTMLtitle
    <br/>
  </span></p>

  <style>
    div.table1 {
      display: table;
      width: 420;
      font-size: 10.0pt;
      font-family: Arial , sans-serif;
      color: rgb(0,0,0);
    }
    div.spalteA {
      display: table-cell;
      width: 120px;
    }
    div.spalteB {
      display: table-cell;
      width: 300px;
    }
  </style>

  <div class="table1">
    <div class="spalteA"> $HTMLtelefon $HTMLdurchwahl $HTMLmobil $HTMLfax $HTMLe-mail
    $HTMLinternet</div>
    <div class="spalteB"> $HTMLtelephoneNumber $HTMLphysicalDeliveryOfficeName $HTMLmobile
    $HTMLfacsimileTelephoneNumber $HTMLmail $HTMLwWWHomePage</div>
  </div>

  <br/><br/>
```

```

<p><b><span style="font-size: 10.0pt;font-family: Calibri , sans-serif;color: rgb(127,127,127);">
    $HTMLcompany
    
</span></b><br/></p>

<p><span style="font-size: 10.5pt;font-family: Helvetica , sans-serif;color: rgb(155,180,36);border: none
windowtext 1.0pt;pAdd-Ing: 0.0cm;background: white;text-decoration: none;">
    <a href="https://www.sample-company.tld/feed/" target="_blank"></span></a>&nbsp;
    <a href="https://twitter.com/sample-company" target="_blank"></a>&nbsp;
    <a href="https://www.facebook.com/pages/sample-company/567468464688162?sk=wall"
    target="_blank"></span></a>&nbsp;
    <a href="https://www.linkedin.com/company/sample-company" target="_blank"></span></a>&nbsp;
<br/><br/>

<style>
    div.table2 {
        display: table;
        width: 800;
        font-size: 10.0pt;
        font-family: Arial , sans-serif;
        color: rgb(166,166,166);
    }
    div.spalte2 {
        display: table-cell;
        width: 400px;
    }
</style>

<div class="table2">
    <div class="spalte2">Sitz der Gesellschaft: $HTMLlocality</div>IBAN CH98 7654 3210 0000 1234
    56</div>
    <div class="spalte2">Gesch&auml;fts&uuml;hrung: Max Mustermann</div>BIC SPKOEFFXXX</div>
</div>

<!-- optionale Veranstaltungsinformationen -->
<br/><br/>
<p><span style="font-size: 10.0pt;font-family: Arial;color: rgb(0,0,0);"><br/>
    Besuchen Sie uns auf der Messe!
    <br/><br/><br/><br/>
    <a href="https://www.messe.tld" target="_blank">https://www.messe.tld</a>
</span></p>

</html>
</body>

```

Code

Die Eingabe unter **Disclaimer as Text** ²⁶² könnte wie folgt aussehen:

Mit freundlichen Grüßen

\$displayName
\$title

\$telephonNumber
\$physicalDeliveryOfficeName
\$mobile

\$facsimileTelephoneNumber
\$mail
\$wWWHomePage

\$company

Sitz der Gesellschaft: \$locality
IBAN CH98 7654 3210 0000 1234 56

Geschäftsführung: Max Mustermann
BIC SPKOEFFXXX

Code

9.43 Cluster: Doppel-Bezug von Zertifikaten verhindern

Ausgangssituation:

In einem SEPPmail Appliance **Cluster**³⁸³⁾ geht die Verbindung zwischen den Cluster-Partnern verloren. Ein Absender, welcher auf der SEPPmail Appliance bislang über kein oder ein ungültiges Zertifikat verfügt, sendet zwei zu signierende E-Mails. Dabei wird die eine über Cluster-Partner A, die andere über Cluster-Partner B gesendet.

Frage:

Wie wird verhindert, dass bei einer ungünstigen Ausfallsituation ein Benutzer auf zwei Cluster-Partner jeweils ein neues, zweites Zertifikat via **MPKI**³³⁹⁾ bezieht?

Antwort:

Dieses Verhalten kann nicht verhindert werden. Im genannten Fall würden die Zertifikate bei Wiederverfügbarkeit des **Cluster**³⁸³⁾ synchronisiert werden, sodass beide parallel für das Entschlüsseln verfügbar sind. Für das Signieren wird das neuere Zertifikat verwendet.

9.44 Cluster: Failover (CARP) funktioniert nicht

Ausgangssituation:

SEPPmail Appliance ist mit zwei oder mehr Maschinen als **Cluster** konfiguriert. Der **Cluster** wird über eine virtuelle IP-Adresse (siehe **System IP ALIAS addresses**) angesprochen. Trotz Ausfall der Maschine mit der höchsten CARP Priorität „Primary“, übernimmt keine der im **Cluster** verbleibenden Maschinen dessen Aufgabe.

Frage:

Warum übernimmt bei Ausfall eines Cluster-Partners nicht der andere?

Ursache:

Die virtuelle IP-Adresse wird nur dann vom entsprechend konfigurierten Cluster-Partner übernommen, wenn die problembehaftete Maschine auch netzwerktechnisch nicht mehr erreichbar ist.

Tritt zum Beispiel bei einer virtuellen Maschine aufgrund eines nicht mehr, oder nicht mehr zuverlässig verfügbaren Datenspeichers „kernel panic“ auf, so kann die Appliance unter Umständen funktional ihren Dienst einstellen, jedoch IP-technisch noch erreichbar sein.

Somit würde die Partner-Maschine nicht erkennen, dass sie die Funktion übernehmen muss.

9.45 Cluster: GINA-Satellite Konfiguration

Ausgangssituation:

Zum Beispiel aufgrund einer vorhandenen Infrastruktur mit Demilitarisierten Zonen (DMZ), ist das Aufteilen der SEPPmail Appliance in verschiedenen Funktionseinheiten erforderlich. Deshalb soll eine **GINA Satellit** ¹⁸⁷ Konfiguration aufgebaut werden.

Frage:

Was muss für das Einrichten einer **GINA Satellit** ¹⁸⁷ Konfiguration beachtet werden?

Antwort:

Nachdem drei Varianten für eine **GINA Satellit** ¹⁸⁷ Konfiguration existieren, ist auch beim Einrichten dieser Varianten unterschiedlich vorzugehen.

- **Variante 1** ⁷⁰³
Diese entspricht im Wesentlichen dem **Frontend/Backend Cluster** ¹⁸⁰, bei welchem das Frontend-System ausschließlich die GINA-Funktion übernimmt.
- **Variante 2** ⁷⁰⁴
Die Kommunikation zwischen dem Basis-System und dem Satelliten-System erfolgt via SMTP Port 25. Zum Internet hin wird das GINA-Web-Interface - meist getrennt durch eine Web Application Firewall (WAF) - über SSL Port 443 bereit gestellt.
- **Variante 3** ⁷⁰⁹
Soll der GINA-Satellit als reiner Web-Server betrieben werden, das heißt der Zugriff auf die Maschine ist von außen zwar möglich, jedoch darf das System selbst nicht nach außen kommunizieren, so können E-Mails nach dem Verarbeiten auf dem Satelliten-System dort zwischengespeichert werden. Das Backend System würde in diesem Fall die auf dem Satelliten-System zwischengespeicherten E-Mails via POP3s abholen.

9.45.1 Variante 1

Voraussetzung:

Das Frontend-System muss das Backend-System via Port 22 SSH erreichen.

Ist **Large File Transfer (LFT)** aktiv, so muss die Port 22 SSH Kommunikation in beide Richtungen möglich sein. Das Frontend-System muss weiterhin eine LFT-Disk mit identischer Größe wie auf dem Backend-System angebunden haben. Weiterhin muss die GINA-Oberfläche des Frontend-Systems aus dem Internet erreicht werden.

Backend-System

- **Cluster** **Prepare for Cluster** **Download Cluster Identifier** Herunterladen des „Cluster Identifier“ (Datei clusterid.txt).

GINA-Satellite-System

- **Cluster** **Add this device as frontend server**
 - **Cluster Identifier**
Hochladen des zuvor vom Backend-System heruntergeladenen „Cluster Identifier“ (Datei clusterid.txt)
 - **Existing appliance IP**
Eingabe der IP-Adresse des Backend-Systems
 - **Connect** **Start**
Herstellen und Speichern der Verbindung zu Backend-System

9.45.2 Variante 2

Vorgehen:

Generell wird empfohlen einen Relay-Server für den Versand von E-Mails in das Internet zu verwenden. Dieser sollte sowohl vom Backend- als auch vom GINA-Satellite-System verwendet werden (siehe **Mail System** [247] **Outgoing server** [250]).

Weiterhin sind auf beiden Systemen folgende Vorbereitungen zu treffen:

- (nur notwendig, sofern eine direkte Verbindung zwischen dem Backend- und dem GINA-Satellite-System und entgegengesetzt hergestellt werden kann und soll)
 - SSL** [319]
 - Generieren (**Request or create new certificate...**) oder Einbinden eines vorhandenen Zertifikates (**Import existing certificate...**)
 - o **Fingerprint** [321]
 - Notieren des Fingerprints zur späteren Verwendung im entgegengesetzten System für das Einrichten der TLS-Verbindung
 - **CA** [328]
 - o Anlage der CA via **Request or create new certificate authority...**
 - o **Backup** [337]
 - Download des Root Zertifikats mittels **Download certificate** für das spätere Einbinden im entgegengesetzten System unter **X.509 Root Certificates** [480]
 - **X.509 Root Certificates** [480]
 - Import des Root Zertifikates des entgegengesetzten Systems via **Import S/MIME root certificate...**

Backend-System

- **Mail System** [247]
 - o **Managed domains** [247]
 - Öffnen jedes einzelnen **Domain name** durch Klicken auf den jeweiligen **Namen**
 - **EDIT MANAGED DOMAIN**
 - **Settings** [266] **GINA domain** [270]
 - Auswahl auf „[default]“
 - Wird „- disabled -“ gewählt, so wird das GINA Forwarding für die jeweilige **Managed domain** [247] unterbunden.
 - **S/MIME domain encryption** [266]
 - Öffnen des Domänen-Zertifikat-Folgemenüs durch Klicken auf **Fingerprint SHA1:....**
 - o **Fingerprint**
 - Wert aus **SHA256** notieren
 - Diese Fingerprints müssen im Satellite System unter **Relay domain key fingerprint:** [317] eingegeben werden.
 - Sofern der das zu verwendende Domänen-Zertifikat unter **Domain encryption** einen anderen Status als „managed“ hat, beziehungsweise das Satelliten-System die Teilnahme am **Managed Domain Service** [317] nicht prüfen kann, Sind die Zertifikate zum späteren Import auf dem Satellitensystem zu exportieren:
 - o **Download certificate**
 - o (das zusätzliche Absichern der Verbindung zwischen den beiden Systemen via TLS ist nur möglich, sofern eine direkte Verbindung hergestellt werden kann)
 - TLS settings** [257] **Add TLS domain...**, Folgemenü **Add TLS Domain** [282] unter
 - **Domain info** [282]
 - **Domain name (use a leading "." to include all subdomains)** [282]
 - Eintrag „kunde.pseudo“
 - (dies ist die Domäne, welche später für die E-Mail Adresse unter **Use remote GINA server, reachable under the following email address** [317] verwendet wird.

- **Optional forwarding server address**^[282]
bleibt leer, sofern der **Domain name**^[282] per DNS aufgelöst wird, andernfalls muss die IP-Adresse des GINA-Satellite-Systems eingetragen werden
- **TLS settings**^[282]
Auswahl von **Fingerprint: Only send mail if TLS is possible and the fingerprint of the server certificate has the following fingerprint**^[284]
Im darunterliegenden Eingabefeld wird der/die Fingerprint(s) des/r Zertifikate/s aus dem Menü **SSL**^[319] der GINA-Satellite-Systeme eingetragen.
- **Mail Processing**^[286] **Ruleset generator**^[287]
 - **General settings**^[288] **Log message meta data**^[289]
Deaktivieren
 - **Advanced options**^[310] **Use remote GINA server, reachable under the following email address**^[311]
Angabe einer E-Mail-Adresse mit einer keinesfalls erreichbaren E-Mail Domäne (zum Beispiel „GINA@kunde.pseudo“ (siehe auch **Domain name (use a leading "." to include all subdomains)**^[282])
- **Domain Certificates**^[489] **S/MIME domain certificates...**, Folgemenü **Domain certificates**^[490] **Manual S/MIME domain certificates**^[490] **Import S/MIME certificate...**, Folgemenü **Import X.509 certificate**
 - **Domain name**
Laut Beispiel „kunde.pseudo“
 - **Certificate Data**
Import des zuvor vom GINA-Satellite-System für die dort angelegte **Managed domain**^[247] „kunde.pseudo“ erzeugten Domänenzertifikates (siehe auch **EDIT MANAGED DOMAIN**^[268] **S/MIME domain encryption**^[274])
- **GINA Domains**^[416]
Eine **GINA Domain**^[416] muss nicht angelegt werden

GINA-Satellite-System

- **Administration**^[369] **Bulk import**^[374] **Import X.509 keys and certificates**^[374] **Import**^[374]
Damit GINA-Träger-E-Mails signiert werden können, ist das Importieren wenigstens eines PKCS#12 Schlüsselpaares und das daraus resultierende automatische Anlegen eines **Users**^[396] erforderlich.
Sollen unterschiedliche **GINA Domains**^[416] zum Einsatz kommen, ist unter Umständen das Importieren jeweils eines PKCS#12 Schlüsselpaares pro **GINA Domains**^[416] sinnvoll. Dabei sollte im Antragsteller des Zertifikates aus dem PKCS#12 jeweils eine E-Mail Adresse mit einem möglichst allgemeingültigen Namensteil und der, beziehungsweise eine der zugeordneten **Managed domains**^[247], im Domänenteil stehen, wie zum Beispiel „securemail@managed-domain1.tld“, „securemail@managed-domain2.tld“, „securemail@managed-domainn.tld“. Diese E-Mail Adressen kommen dann bei der Konfiguration der jeweiligen **GINA Domain**^[416] zum Einsatz (siehe nächster Punkt)
- **GINA Domains**^[416]
Konfigurieren der der **[default]** GINA, beziehungsweise Einrichten der erforderlichen **GINA Domains**^[416]
 - **Domains**^[416]
 - **GINA name**^[416]
Öffnen der jeweiligen **GINA**
Im Folgemenü **Change GINA Settings for**^[423] die gewünschten Einstellungen vornehmen^[423].
Für das Signieren der GINA-Träger-E-Mails
 - **Extended settings**^[431] **Force sending of GINA mails from this address:**^[437]
Eintragen der zur jeweiligen **GINA Domains**^[416] passenden E-Mail Adresse (siehe Punkt oberhalb)
- **Mail System**^[247]
 - **Managed domains**^[247]
 - **Create S/MIME domain keys for managed domain encryption and send public key to vendor pool**^[248]
Auf „Off for all domains“ setzen

- Anlage der E-Mail Domäne der unter **Use remote GINA server, reachable under the following email address** [31] des Backend-Systems angegebenen E-Mail Adresse via **Add managed domain...**

Im Folgemenü **Add managed domain** [266] **Settings** [266]

- **Domain name** [266]
Eingabe laut Beispiel „kunde.pseudo“
- **Forwarding server** [266]
- Eingabe der IP-Adresse, des Hostname oder des MX-Eintrag des Backend-Systems

Erneutes Öffnen der soeben angelegten **Managed domain** [247]

- **EDIT MANAGED DOMAIN** [266] **S/MIME domain encryption** [274]
 - Klicken von **Generate S/MIME key**
 - Öffnen des neu generierten Zertifikates durch Klicken auf **SHA1:...** unter **Fingerprint**
 - Im sich öffnenden Untermenü das Zertifikat mittels **Download certificate...** herunterladen. Dieses ist auf dem Backend-System unter **Domain Certificates** [489] für die Zieldomäne (laut Beispiel „kunde.pseudo“) einzubinden.

Anlage aller **Managed domains** [247], wie sie auch auf dem Backend-System vorhanden sind mittels **Add managed domain...**

Im Folgemenü **Add managed domain** [266] **Settings** [266]

- **Domain name** [266]
Kommagetrennte Eingabe der Domänen aus dem Backend-System
- **Forwarding server** [266]
Eingabe des der IP Adresse, des Hostnames oder des MX des Backend-Systems
- Gegebenenfalls Zuordnen der jeweils gewünschten **GINA** [247] zur jeweiligen **Managed domains** [247] (siehe **EDIT MANAGED DOMAIN** [266] **Settings** [266] **GINA domain** [270]).
- (nur möglich, sofern eine direkte Verbindung mit dem Backend-System hergestellt werden kann) **TLS settings** [251] **Add TLS domain...**, Folgemenü unter
 - **Domain info** [282]
 - **Domain name (use a leading "." to include all subdomains)** [282]
Eingabe des Names Backend-Systems
 - **Optional forwarding server address** [282]
bleibt leer, sofern der **Domain name** [282] per DNS aufgelöst wird, andernfalls muss die IP-Adresse des Backend-Systems eingetragen werden
 - **TLS settings** [282]
Auswahl von **Fingerprint: Only send mail if TLS is possible and the fingerprint of the server certificate has the following fingerprint** [284]
Im darunterliegenden Eingabefeld wird der/die Fingerprint(s) des/r Zertifikate/s aus dem Menü **SSL** [319] der Backend Maschine(n) eingetragen.
- **SMTP settings** [252] **max. message size (KiB) (Note: cannot exceed xxxxxxxx KiB)** [252]
Begrenzung aus dem Backend-System, beziehungsweise E-Mail Server übernehmen
- **Relaying** [254]
Eingabe der IP Adresse(n) des/r Backend-Systems/e
- **Mail Processing** [286]
 - **Ruleset generator** [287]
 - **General settings** [288]
Entfernen der Haken der Optionen
 - **Do not touch mails with the following text in subject** [288]

- **Reprocess mails sent to reprocess@decrypt.reprocess** [288]
- **User creation** [289]
 - Auswahl von **Create accounts for all users** [290]
- **Encryption** [292]
 - **Incoming e-mails** [292]
 - Einstellungen des Backend-Systems übernehmen
 - **Outgoing e-mails** [293]
 - Einstellungen sind irrelevant, da eine **Encryption Policy** [313] zum Einsatz kommt, in welcher GINA erzwungen wird.
- **Signing** [298]
 - Entfernen aller Haken
- **Advanced options** [310]
 - **This is a remote GINA server** [311]
 - Aktivieren
 - **Relay for domain:** [311]
 - Eingabe aller **Managed domains** [247] des Backend Systems als Regulärer Ausdruck
 - **Relay e-mail address:** [311]
 - Eingabe der Adresse aus der Option **Use remote GINA server, reachable under the following email address** [311] des Backend-Systems, im Beispiel „GINA@kunde.pseudo“
 - **Relay domain key fingerprint:** [311]
 - Eingabe der Fingerprints der zu verwendenden Domänenverschlüsselungszertifikate aus den jeweiligen **Managed domains** [247] des Backend Systems (siehe **EDIT MANAGED DOMAIN** [266] **S/MIME domain encryption** [274]), passen zur Eingabe unter **Relay for domain:** [311]
 - **Use custom delivery method:** [312]
 - Eingabe von `continue'); if (!pack_mail('GINA@kunde.pseudo', true)) { log(1, 'pack_mail() failed'); drop(500, 'pack_mail() failed'); } deliver('`

Über **Edit policy table...** wird im Folgemenü **Encryption Policy** [313] via **Create new encryption policy...** eine neue Policy erzeugt.

Im Folgemenü **Add Encryption Policy** [314] sind in den **Settings** [314] folgende Parameter zu setzen:

- **Policy name** [314]
 - Eingabe eines eindeutigen Namens, zum Beispiel „GINA“.
- **Policy domains** [314]
 - Auswahl aller **Managed domains** [247] mit Ausnahme von „kunde.pseudo“
- **Encryption mode** [314]
 - Auswahl von „GINA-only“
- **GINA options** [317]
 - bleibt leer
- **Domain Certificates** [489]
 - Sofern das Satellite System die Domänenschlüssel der **Managed domains** [247] des Backend-Systems nicht automatisch über den **Managed Domain Service** [311] beziehen kann, müssen diese via **S/MIME domain certificates...** in **S/MIME domain certificates** [490] **Manual S/MIME domain certificates** [490] **Import S/MIME certificate...** jeweils importiert werden.

Einschränkungen

Large File Transfer (LFT) ^[107]

LFT ist nur bedingt möglich.

So ist die in **Large File Transfer (LFT)** ^[107] beschriebene Variante 1 (ausschließlich über den E-Mail Client) nicht möglich. Für Variante 2 (Einliefern per GINA - beziehungsweise für LFT nach intern) müssten gegebenenfalls interne Benutzer via **Administration** ^[369] **Bulk import** ^[374] **Import GINA Users (CSV)** ^[374] oder via Rest Schnittstelle (siehe auch **Groups** ^[413] **legacyappadmin** ^[414]) auf der Maschine als GINA-Accounts angelegt und auch gepflegt werden. Auch für Variante 3 müssen die Voraussetzungen wie bei Variante 2 geschaffen werden.

Protection Pack (PP) ^[106]

Einstellung nach Bedarf. Gegebenenfalls ist das Umleiten auf eine externe Schutz-Instanz via **Custom commands** ^[308] möglich (siehe auch **Sophos UTM: Erneute Virenprüfung nach dem Entschlüsseln** ^[831]). In der Regel ist dies jedoch nicht notwendig, da die Schutzmechanismen des Backend-Systems greifen.

9.45.3 Variante 2a

Vorgehen:

Generell wird empfohlen einen Relay-Server für den Versand von E-Mails in das Internet zu verwenden. Dieser sollte sowohl vom Backend- als auch vom GINA-Satellite-System verwendet werden (siehe **Mail System**^[247] **Outgoing server**^[250]).

Weiterhin sind auf beiden Systemen folgende Vorbereitungen zu treffen:

- **SSL**^[319]
 - Generieren (**Request or create new certificate...**) oder Einbinden eines vorhandenen Zertifikates (**Import existing certificate...**)
 - (nur notwendig, sofern eine direkte Verbindung zwischen dem Backend- und dem GINA-Satellite-System und entgegengesetzt hergestellt werden kann und soll)
 - Fingerprint**^[321]
 - Notieren des Fingerprints zur späteren Verwendung im entgegengesetzten System für das Einrichten der TLS-Verbindung

Backend-System

- **Mail System**^[247]
 - **Managed domains**^[247]
 - Öffnen jedes einzelnen **Domain name** durch Klicken auf den jeweiligen **Namen**
 - **EDIT MANAGED DOMAIN**
 - **Settings**^[269] **GINA domain**^[270]
 - Auswahl auf „[default]“
 - Wird „- disabled -“ gewählt, so wird das GINA Forwarding für die jeweilige **Managed domain**^[247] unterbunden.
 - **Fetch mail from remote POP3 server.Interval in minutes:**^[249] aktivieren^[249] und Wert auf „1“ setzen.
 - (das zusätzliche Absichern der Verbindung zwischen vom Backend- zum GINA-Satellite-System via TLS ist nur möglich, sofern eine direkte Verbindung hergestellt werden kann)
 - TLS settings**^[251] **Add TLS domain...**, Folgemenü **Add TLS Domain**^[282] unter
 - **Domain info**^[282]
 - **Domain name (use a leading "." to include all subdomains)**^[282]
 - Eintrag „kunde.pseudo“
 - (dies ist die Domäne, welche später für die E-Mail Adresse unter **Use remote GINA server, reachable under the following email address**^[311] verwendet wird.
 - **Optional forwarding server address**^[282]
 - bleibt leer, sofern der **Domain name**^[282] per DNS aufgelöst wird, andernfalls muss die IP-Adresse des GINA-Satellite-Systems eingetragen werden
 - **TLS settings**^[282]
 - Auswahl von **Fingerprint: Only send mail if TLS is possible and the fingerprint of the server certificate has the following fingerprint**^[284]
 - Im darunterliegenden Eingabefeld wird der/die Fingerprint(s) des/r Zertifikate/s aus dem Menü **SSL**^[319] der GINA-Satellite-Systeme eingetragen.
 - **Mail Processing**^[286] **Ruleset generator**^[287]
 - **General settings**^[288] **Log message meta data**^[289]
 - Deaktivieren
 - **Custom Commands**^[308] **Custom macros and commands for all e-mails BEFORE processing**^[309]

Zeile	Code
01	# Begin: Custom macros and commands for all e-mails BEFORE processing
02	log(1,'Begin: Custom macros and commands for all e-mails BEFORE processing');
03	if (compare('to', 'match', 'GINA@kunde.pseudo')) {

Zeile	Code
04	<code>log(1, 'unpacking satellite mail');</code>
05	<code>unpack mail();</code>
06	<code>logsubject();</code>
07	<code>log(1, 'deliver satellite mail unchanged');</code>
08	<code>deliver();</code>
09	<code>}</code>
10	<code># metadata setting is disabled in ruleset generator</code>
11	<code>logsubject();</code>
12	<code>log(1, 'End: Custom macros and commands for all e-mails BEFORE processing');</code>
13	<code># End: Custom macros and commands for all e-mails BEFORE processing</code>

- **Advanced options** ^[310] **Use remote GINA server, reachable under the following email address** ^[317]
Angabe einer E-Mail-Adresse mit einer keinesfalls erreichbaren E-Mail Domäne (zum Beispiel „GINA@kunde.pseudo“ (siehe auch **Domain name (use a leading "." to include all subdomains)** ^[282])
- **CA** ^[328]
 - Anlage der CA via **Request or create new certificate authority...**
 - **Backup** ^[337]
Download des Root Zertifikats mittels **Download certificate** für das spätere Einbinden im GINA-Satellite-System unter **X.509 Root Certificates** ^[480]
- **Users** ^[396]
Um auf dem GINA-Satellite-System generierte E-Mails (in der Regel „GINA@-Antworten und -Passwort-E-Mails“) via POP3(s) auf das Backend-System für das weitere Verarbeiten abholen zu können, muss via **Create new user account...** im Folgemenu **CREATE USER ACCOUNT** ^[410] ein Benutzer (im Beispiel „GINA@kunde.pseudo“) mit einem Passwort erstellt werden (siehe **USER 'USER@DOMAIN.TLD'** ^[398]). Im Anschluss erscheint das Detail-Menu **USER 'USER@DOMAIN.TLD'** ^[398] des neu angelegten Users. Dort müssen die Eingabefelder der Sektion **Remote POP3** ^[402] entsprechend befüllt werden, gemäß Beispiel
 - **User ID** ^[402]
Laut Beispiel wäre das „GINA@kunde.pseudo“
 - **Mail server** ^[402]
Eingabe der IP-Adresse, des Hostname oder des MX-Eintrag des GINA-Satellite-System
 - **Options** ^[402] **Use SSL instead of STARTTLS** ^[402]
Aktivieren.
- **Domain Certificates** ^[489] **S/MIME domain certificates...**, Folgemenu **Domain certificates** ^[490] **Manual S/MIME domain certificates** ^[490] **Import S/MIME certificate...**, Folgemenu **Import X.509 certificate**
 - **Domain name**
Angabe des <„kunde.pseudo“
 - **Certificate Data**
Import des zuvor vom GINA-Satellite-System für die dort angelegte **Managed domain** ^[247] „kunde.pseudo“ erzeugten Domänenzertifikates (siehe auch **EDIT MANAGED DOMAIN** ^[266] **S/MIME domain encryption** ^[274])
- **GINA Domains** ^[416]
Eine **GINA Domain** ^[416] muss nicht angelegt werden

GINA-Satellite-System

- **Administration** ^[369] **Bulk import** ^[374] **Import X.509 keys and certificates** ^[374] **Import**
Damit GINA-Träger-E-Mails signiert werden können, ist das Importieren wenigstens eines PKCS#12 Schlüsselpaares und das daraus resultierende automatische Anlegen eines **Users** ^[396] erforderlich.

Sollen unterschiedliche **GINA Domains** zum Einsatz kommen, ist unter Umständen das Importieren jeweils eines PKCS#12 Schlüsselpaars pro **GINA Domains** sinnvoll. Dabei sollte im Antragsteller des Zertifikates aus dem PKCS#12 jeweils eine E-Mail Adresse mit einem möglichst allgemeingültigen Namensteil und der, beziehungsweise eine der zugeordneten **Managed domains**, im Domänenteil stehen, wie zum Beispiel „securemail@managed-domain1.tld“, „securemail@managed-domain2.tld“, „securemail@managed-domainn.tld“.

Diese E-Mail Adressen kommen dann bei der Konfiguration der jeweiligen **GINA Domain** zum Einsatz (siehe nächster Punkt)

- **GINA Domains**
 - Konfigurieren der der **[default]** GINA, beziehungsweise Einrichten der erforderlichen **GINA Domains**
 - **Domains**
 - **GINA name**

Öffnen der jeweiligen **GINA**

Im Folgenden **Change GINA Settings for** die gewünschten Einstellungen vornehmen.

Für das Signieren der GINA-Träger-E-Mails

 - **Extended settings** **Force sending of GINA mails from this address:**

Eintragen der zur jeweiligen **GINA Domains** passenden E-Mail Adresse (siehe Punkt oberhalb)
- **Mail System**
 - **Managed domains**
 - **Create S/MIME domain keys for managed domain encryption and send public key to vendor pool**

Auf „Off for all domains“ setzen
 - **Verify recipient addresses using SMTP lookups**

Deaktivieren
 - Anlage der E-Mail Domäne der unter **Use remote GINA server, reachable under the following email address** des Backend-Systems angegebenen E-Mail Adresse via **Add managed domain...**

Im Folgenden **Add managed domain** **Settings**

 - **Domain name**

Eingabe laut Beispiel „kunde.pseudo“
 - **Forwarding server**

Eingabe „[127.0.0.1]“
 - Erneutes Öffnen der soeben angelegten **Managed domain**
 - **EDIT MANAGED DOMAIN** **S/MIME domain encryption**
 - Klicken von **Generate S/MIME key**
 - Öffnen des neu generierten Zertifikates durch Klicken auf **SHA1:...** unter **Fingerprint**
 - Im sich öffnenden Untermenü das Zertifikat mittels Download certificate... herunterladen. Dieses ist auf dem Backend-System unter **Domain Certificates** für die Zieldomäne (laut Beispiel „kunde.pseudo“) einzubinden.
- Anlage aller **Managed domains**, wie sie auch auf dem Backend-System vorhanden sind mittels **Add managed domain...**

Im Folgenden **Add managed domain** **Settings**

 - **Domain name**

Kommagetrennte Eingabe der Domänen aus dem Backend-System
 - **Forwarding server**

Eingabe „[127.0.0.1]“
- Gegebenenfalls Zuordnen der jeweils gewünschten **GINA** zur jeweiligen **Managed domains** (siehe **EDIT MANAGED DOMAIN** **Settings** **GINA domain**).

- (nur möglich, sofern eine direkte Verbindung mit dem Backend-System hergestellt werden kann)
- **TLS settings** ^[251] **Add TLS domain...**, Folgemenu unter
 - **Domain info** ^[282]
 - **Domain name (use a leading "." to include all subdomains)** ^[282]
 - Eingabe des Names Backend-Systems
 - **Optional forwarding server address** ^[282]
bleibt leer, sofern der **Domain name** ^[282] per DNS aufgelöst wird, andernfalls muss die IP-Adresse des Backend-Systems eingetragen werden
 - **TLS settings** ^[282]
Auswahl von **Fingerprint: Only send mail if TLS is possible and the fingerprint of the server certificate has the following fingerprint** ^[284]
Im darunterliegenden Eingabefeld wird der/die Fingerprint(s) des/r Zertifikate/s aus dem Menü **SSL** ^[319] der Backend Maschine(n) eingetragen.
- **SMTP settings** ^[252] **max. message size (KiB) (Note: cannot exceed xxxxxxxx KiB)** ^[252]
Begrenzung aus dem Backend-System, beziehungsweise E-Mail Server übernehmen
- **Relaying** ^[254]
Eingabe der IP Adresse(n) des/r Backend-Systems/e
- **Mail Processing** ^[286]
 - **Ruleset generator** ^[287]
 - **General settings** ^[288]
Entfernen der Haken der Optionen
 - **Do not touch mails with the following text in subject** ^[288]
 - **Reprocess mails sent to reprocess@decrypt.reprocess** ^[288]
 - **User creation** ^[289]
Auswahl von **Create accounts for all users** ^[290]
 - **Encryption** ^[292]
 - **Incoming e-mails** ^[292]
Einstellungen des Backend-Systems übernehmen
 - **Outgoing e-mails** ^[293]
Einstellungen sind irrelevant, da eine **Encryption Policy** ^[313] zum Einsatz kommt, in welcher GINA erzwungen wird.
 - **Signing** ^[298]
Entfernen aller Haken
 - **Advanced options** ^[310]
 - **This is a remote GINA server** ^[311]
Aktivieren
 - **Relay for domain:** ^[311]
Eingabe aller **Managed domains** ^[247] des Backend Systems als Regulärer Ausdruck
 - **Relay e-mail address:** ^[311]
Eingabe der Adresse aus der Option **Use remote GINA server, reachable under the following email address** ^[311] des Backend-Systems, im Beispiel „GINA@kunde.pseudo“
 - **Relay domain key fingerprint:** ^[311]
bleibt leer.
 - **Use custom delivery method:** ^[312]
Eingabe von `continue'`; `if (!pack_mail('GINA@kunde.pseudo', true)) { log(1,`

```
'pack_mail() failed'); drop(500, 'pack_mail() failed'); } deliver('
```

Über **Edit policy table...** wird im Folgemenü **Encryption Policy** via **Create new encryption policy...** eine neue Policy erzeugt.

Im Folgemenü **Add Encryption Policy** sind in den **Settings** folgende Parameter zu setzen:

- **Policy name**
Eingabe eines eindeutigen Namens, zum Beispiel „GINA“.
- **Policy domains**
Auswahl aller **Managed domains** mit Ausnahme von „kunde.pseudo“
- **Encryption mode**
Auswahl von „GINA-only“
- **GINA options**
bleibt leer
- **SSL**
Generieren (**Request or create new certificate...**) oder Einbinden eines vorhandenen Zertifikates (**Import existing certificate...**)

(nur notwendig, sofern eine direkte Verbindung zwischen dem Backend- und dem GINA-Satellite-System und entgegengesetzt hergestellt werden kann und soll)
 - **Fingerprint**
Notieren des Fingerprints zur späteren Verwendung im Backend-System für das Einrichten der TLS-Verbindung
- **Users**
Um auf dem GINA-Satellite-System generierte E-Mails (in der Regel „GINA@-Antworten und -Passwort-E-Mails“) via POP3(s) auf das Backend-System für das weitere Verarbeiten abholen zu können, muss via **Create new user account...** im Folgemenü **CREATE USER ACCOUNT** ein Benutzer mit einem Passwort erstellt werden (siehe **USER 'USER@DOMAIN.TLD'**).
Laut Beispiel wäre das „GINA@kunde.pseudo“
- **X.509 Root Certificates**
Import des Root Zertifikates des Backend-Systems via **Import S/MIME root certificate...**
- **Domain Certificates**
Sofern das Satellite System die Domänenschlüssel der **Managed domains** des Backend-Systems nicht automatisch über den **Managed Domain Service** beziehen kann, müssen diese via **S/MIME domain certificates...** in **S/MIME domain certificates** **Manual S/MIME domain certificates** **Import S/MIME certificate...** jeweils importiert werden.

Einschränkungen

Large File Transfer (LFT)

LFT ist nur bedingt möglich.

So ist die in **Large File Transfer (LFT)** beschriebene Variante 1 (ausschließlich über den E-Mail Client) nicht möglich. Für Variante 2 (Einliefern per GINA - beziehungsweise für LFT nach intern) müssten gegebenenfalls interne Benutzer via **Administration** **Bulk import** **Import GINA Users (CSV)** oder via Rest Schnittstelle (siehe auch **Groups** **legacyappadmin**) auf der Maschine als GINA-Accounts angelegt und auch gepflegt werden. Auch für Variante 3 müssen die Voraussetzungen wie bei Variante 2 geschaffen werden.

Protection Pack (PP)

Einstellung nach Bedarf. Gegebenenfalls ist das Umleiten auf eine externe Schutz-Instanz via **Custom commands** möglich (siehe auch **Sophos UTM: Erneute Virenprüfung nach dem Entschlüsseln**). In der Regel ist dies jedoch nicht notwendig, da die Schutzmechanismen des Backend-Systems greifen.

[Code](#)

9.46 Cluster: Priorität bei der Replikation

Ausgangssituation:

Die SEPPmail Appliance wird in einem **Cluster**  Verbund betrieben.

Frage:

Mit welcher Priorität werden Änderungen im **Cluster**  repliziert? Zum Beispiel: Schlüsselmaterial – Konfiguration – LFT?

Antwort:

Schlüsselmaterial und Konfiguration wird unabhängig (das heißt gegebenenfalls parallel) von LFT synchronisiert.

9.47 Cluster: Replikation arbeitet nicht wie erwartet

Ausgangssituation:

Die SEPPmail Appliance soll in einem **Cluster** ^[383] Verbund betrieben werden, beziehungsweise wird bereits betrieben.

Frage:

Weshalb treten Probleme beim Synchronisieren des **Cluster** ^[383] s auf?

Antwort:

Für den Cluster-Betrieb muss

- die Kommunikation via Port 22 SSH (siehe auch **Firewall / Router einrichten** ^[135]) gewährleistet sein.
- die korrekte (synchrone) Zeit der Cluster-Partner sichergestellt sein. Zu prüfen ist, dass
 - NTP aktiv ist (siehe **System** ^[224] **Time and date** ^[240]).
 - auf den Cluster-Partnern die selben Zeitserver verwendet werden (siehe **System** ^[224] **Time and date** ^[240]).
 - der NTP Zugriff und somit die Zeitsynchronisation auf allen Cluster-Partnern funktioniert.

9.48 Cluster: Replikations-Intervalle

Ausgangssituation:

Die SEPPmail Appliance wird in einem **Cluster**^[383] Verbund betrieben.

Frage:

Wie häufig, beziehungsweise in welchen Zeitabständen wird im **Cluster**^[383] repliziert?

Antwort:

Ein SEPPmail Appliance **Cluster**^[383] besteht aus gleichberechtigten Cluster-Partnern. Änderungen auf einem Cluster-Partner werden daher sofort, also ohne merkbare Zeitverzögerung auf alle anderen Partner repliziert.

9.49 Cluster: Replizierte Daten

Ausgangssituation:

Die SEPPmail Appliance wird in einem **Cluster** ^[383] Verbund betrieben.

Frage:

Welche Daten werden im **Cluster** ^[383] repliziert?

Antwort:

Im **Cluster** ^[383] wird das gesamte Schlüsselmateriale sowie die Konfiguration repliziert. Ebenso werden **LE** ^[107] Daten repliziert, sofern dieses Feature aktiv ist.

Ausgenommen von der Replikation sind

- Systemeinstellungen (**System** ^[224])
- Lizenzinformationen
- CA Keys aus **CA** ^[328] (die Einstellungen unter **CA** ^[328] **Settings** ^[330] jedoch schon!)
- SSL Zertifikate aus **SSL** ^[319]
- **Logs** ^[388]
- **Statistics** ^[394]

9.50 Cluster: Sendende IP Adresse im Cluster

Ausgangssituation:

In einem SEPPmail Appliance **Cluster**^[383] wird mit virtuellen IP Adressen gearbeitet (siehe **System**^[224] **IP ALIAS addresses**^[226]).

Frage:

Mit welcher IP Adresse sendet die SEPPmail Appliance an die nachfolgenden Relays (siehe **Mail System**^[247] **Outgoing server**^[250], beziehungsweise **Managed domains**^[247] Tabelle, Spalte **Server IP address**^[247] und **Smarthost**^[247])?

Antwort:

Virtuelle IP-Adressen dienen ausschließlich dem E-Mail Empfang.

Gesendet werden E-Mails immer über die physikalische IP Adresse (siehe **System**^[224] **IP addresses**^[225]) der jeweiligen Maschine im **Cluster**^[383]. Somit sollte jeweils die physikalische IP Adresse jeder einzelnen SEPPmail Appliance im **Cluster**^[383] auf dem ausgehenden SMTP-Relay (siehe **Mail System**^[247] **Outgoing server**^[250], beziehungsweise **Managed domains**^[247] Tabelle, Spalte **Smarthost**^[247]) für das Relaying freigegeben werden.

9.51 Cluster: Update Reihenfolge der Cluster Maschinen

Ausgangssituation:

In einem SEPPmail Appliance **Cluster** soll ein Firmware Update der einzelnen Members ausgeführt werden.

Frage:

Ist beim Update der einzelnen Cluster-Partnern eine bestimmte Reihenfolge zu beachten?

Antwort:

Prinzipiell sind alle Partner eines **Cluster** gleichberechtigt. Somit ist die Reihenfolge, in welcher ein Update von staten geht irrelevant.

Wird im SEPPmail Appliance **Cluster** mit virtuellen IP Adressen gearbeitet (siehe **System IP ALIAS addresses**) gearbeitet, so ist gegebenenfalls die hier eingestellte Hierarchie beim Entgegennehmen des SMTP-Verkehrs zu berücksichtigen, um selbst während des Updates einen ungestörten E-Mail-Fluss zu gewährleisten.

Eine Ausnahme sind **Frontend/Backend Cluster**, da in dieser Konfiguration die Frontend-Maschinen über keine Datenbank verfügen. In diesem Fall ist/sind immer zuerst die Frontend Maschine(n) zu aktualisieren.

Nähere Informationen zum **Update** sind in der gleichnamigen Sektion des Menüs **Administration** zu finden.

9.52 Cluster: Verfügbarkeit der GINA-Interfaces prüfen

Ausgangssituation:

Einem SEPPmail Appliance **Cluster** ist ein externer Loadbalancer vorgeschaltet. Dieser soll die Verfügbarkeit der GINA-Oberfläche der Cluster-Partner prüfen.

Frage:

Über welche Mechanismen kann das Prüfen der Verfügbarkeit stattfinden?

Antwort:

Im Standard kann die Verfügbarkeit via OpenSSL wie folgt geprüft werden:

Zunächst die Verbindung zur Appliance über den **Hostname** der unter dem **GINA name** [default] der **Sektion Domains** des Menüs **GINA Domains** angezeigt wird, herstellen, im Beispiel securemail.meinefirma.tld) mittels

```
openssl s_client -connect securemail.meinefirma.tld:443
```

herstellen. Daraufhin wird Zertifikat, Handshake und so weiter angezeigt. Nun

```
GET / HTTP/1.0
```

eingeben und zwei mal (!) Enter drücken. Ist das Interface verfügbar, so wird zunächst die Meldung

```
HTTP/1.1 200 OK
```

sowie einige weitere Informationen ausgegeben.

Werden auf der Appliance mehrere GINA Interfaces (ohne **virtual hosting**) bereitgestellt, so können diese bei Bedarf explizit durch Angabe deren **Hostname** (zum Beispiel „Mandant 1“) geprüft werden (Achtung, Gross-/Kleinschreibung ist zu beachten), also

```
openssl s_client -connect securemail.meinefirma.tld:443/Mandant1
```

Die Abfrage würde nach Herstellen der Verbindung zur Appliance wie folgt lauten:

```
GET /Mandant1/ HTTP/1.0
```

9.53 Cluster: Virtuelle IP-Adressen (CARP) funktionieren nicht.

Ausgangssituation:

In einem SEPPmail Appliance **Cluster** sollen virtuelle IP Adressen verwendet werden. Diese scheinen jedoch nicht zu funktionieren.

Frage:

Wie kann die Funktion der virtuellen IP Adressen mittels CARP gewährleistet werden?

Antwort:

Zunächst ist sicherzustellen, dass die entsprechenden Einstellungen (siehe **System** **IP ALIAS addresses**) korrekt vorgenommen wurden.

Um die Funktion von CARP zu gewährleisten, müssen weiterhin die Netzwerkkomponenten (Switches) virtuelle MAC-Adressen zulassen. Bei Hardware Switches ist dies in der Regel die Standardeinstellung. Bei virtuellen Komponenten muss dies meist konfiguriert werden (siehe **Hinweis**).

9.54 DATEV: Austausch von Domänenschlüsseln mit DATEV-Kunden

Ausgangssituation:

Auf der SEPPmail Appliance soll eine Domänenverschlüsselung zu einem Kommunikationspartner eingerichtet werden der DATEV Kunde ist und die Produkterweiterung DATEV E-Mail-Verschlüsselung (DEMV) nutzt.

Frage:

Wie kann der E-Mailverkehr zwischen den Kommunikationspartnern bidirektional über eine Domänenverschlüsselung abgesichert werden?

Antwort:

DATEV DEMV Kunden stehen die Managed Domain Zertifikate und somit die Möglichkeit zur Domänenverschlüsselung an teilnehmende Managed Domains automatisch zur Verfügung.

Da die DATEV jedoch für DEMV Kunden keine Managed Domain Zertifikate zur Verfügung stellt, muss gegebenenfalls für das Verschlüsseln an die entsprechenden Empfänger das jeweils personenbezogene S/MIME Zertifikat beim DATEV Keyserver abgefragt werden.

Dies kann in der SEPPmail Appliance unter **Mail Processing** ^[286] **Ruleset generator** ^[287] **Key server** ^[309] wie folgt realisiert werden::

Type:

S/MIME

Recipient mask (regexp):

E-Mail Domäne/n des/r DEMV-Kunden als Regulärer Ausdruck

URI:

'ldap://ldap.crl.esecure.de

Bind DN:

<leer>

Bind PW:

<leer>

Base DN:

dc=esecure,dc=de

Ignore failure:

<entsprechend der gewünschten Verarbeitungsweise>

9.55 E-Mail Fluss: „ERROR: Missing mandatory headers Date and From“

Ausgangssituation:

Die SEPPmail Appliance lehnt E-Mails mit dem SMTP-Code „ERROR: Missing mandatory headers Date and From“ ab.

Ursache:

Die SEPPmail Appliance prüft bei E-Mails deren RFC-Konformität. Fehlen die obligatorischen E-Mail Header „from“ und „date“, so wird die E-Mail mit besagtem Fehler abgewiesen.

9.56 E-Mail Fluss: Verarbeiten von E-Mails an Sub-Domänen

Ausgangssituation:

Auf der SEPPmail Appliance soll eine Haupt-Domäne (zum Beispiel main-domain.tld) sowie Sub-Domänen dieser Haupt-Domäne (zum Beispiel sub1.main-domain.tld) verarbeitet werden.

Frage:

Verarbeitet die SEPPmail Appliance E-Mails an Sub-Domänen der unter **Managed domains** ²⁴⁷ eingetragenen **Domain Name** ²⁴⁷ automatisch?

Antwort:

Nein. Sub-Domänen müssen jeweils separat als eigene Managed Domain angelegt werden.
Auch das unter Umständen aus Postfix bekannte varanstellen eines Punktes „.“, um generell alle Sub-Domänen einzuschließen ist nicht zulässig.

9.57 ESX: Netzwerkadapter wird nicht erkannt

Ausgangssituation:

In den ESX Gast-Betriebssystem-Einstellungen der SEPPmail Appliance wird für den Netzwerkadapter die Meldung *Dieser Netzwerkadapter wird von {0} nicht unterstützt. Anderes (64Bit)* oder eine ähnliche angezeigt.

Ursache:

Gewisse ESX – Versionen scheinen hier Probleme zu haben. Im OVF-Image ist kein spezieller Typ angegeben.

Lösung:

Adaptertyp in den Gasteinstellungen ändern oder dort den Netzwerkadapter entfernen und anschließend neu hinzufügen.

9.58 ESX: Abstürzte / Einfrieren der Maschine

Ausgangssituation:

Die SEPPmail Appliance stürzt von Zeit zu Zeit ab, beziehungsweise friert ein.

Ursache:

Mangelnde System-Ressourcen

Lösung:

Hinzufügen von weiteren Systemressourcen (RAM, CPU).

**Hinweis:**

Die der SEPPmail Appliance zugeordneten Ressourcen müssen zuverlässig (statisch) zur Verfügung stehen.

Ist das sogenannte „Thin Provisioning“ aktiv, so stellt der Virtualisierungs-Host die Systemreccourcen nur bei Bedarf (dynamisch) zur Verfügung und auch nur dann, wenn zum Zeitpunkt des Bedarfs auf dem Host-System genügend Ressourcen zur Verfügung stehen!

9.59 GINA: 403 Forbidden / Server Name Indication (SNI)

Ausgangssituation:

Auf der SEPPmail Appliance sind mehrere virtuelle Hosts konfiguriert (siehe **Use virtual hosting**^[417] unter **GINA Domains**^[416] konfiguriert.

Beim Öffnen einer GINA-Nachricht erscheint beim Verbindungsaufbau zur SEPPmail Appliance die Meldung

403 Forbidden You don't have permission to access this resource. Reason: The client software did not provide a hostname using Server Name Indication (SNI), which is required to access this server.

Frage:

Weshalb kann die GINA-Nachricht nicht geöffnet werden, beziehungsweise woraus resultiert diese Meldung?

Antwort:

In der Regel wird dieses Verhalten durch einen vorgelagerten Proxy Server verursacht.

Beim Öffnen der GINA-Nachricht wird der falsche virtuelle Host angesprochen, beziehungsweise fehlt der angesprochene Hostname. Seit der SEPPmail Appliance Version 11.1.7 wird zum Schutz vor Ansteuern einer falschen **GINA Domain**^[416] - vor allem in mandantenfähigen Systemen - der Zugriff verweigert.

Lösung:

Durch die Option **Disable strict SNI check when virtual hosting is enabled**^[418] (siehe **GINA Domains**^[416] **Settings**^[416]) kann das Verhalten wie unter 11.1.6 und kleiner wiederhergestellt werden. Da hiermit jedoch der Schutz gegen falsche Ansteuerung ausgehebelt wird, ist das Verwenden der Option nur im Fehlerfall zur temporären Wiederherstellung gedacht.

9.60 GINA: Anmelden interner Benutzer

Ausgangssituation:

Die GINA Oberfläche soll auch für interne Benutzer bereit gestellt werden, beispielsweise für **Large File Transfer (LFT)** oder **SEPPmail IME** unter ausschließlicher Verwendung der GINA-Technologie.

Frage:

Kann sich ein interner Benutzer automatisch an der GINA Oberfläche anmelden, oder muss er zuvor als **GINA account** angelegt werden?

Antwort:

Wurde für die **Managed domain** unter **EDIT MANAGED DOMAIN** die **External authentication** mit den entsprechenden Optionen **Authenticate GINA users from this domain to external LDAP server** und **Automatically create GINA account if user exists on external LDAP server** aktiviert, so kann sich jeder interne Benutzer dieser E-Mail Domäne mit seiner E-Mail Adresse und seinem Netzwerk (Windows-) Kennwort an der GINA Oberfläche anmelden.

Andernfalls muss der Benutzer schon vorher eine GINA- oder LFT- Mail erhalten haben.

Alternative Möglichkeit für das Erzeugen des **GINA account** ist die Selbstregistrierung. Diese ist jedoch nur möglich, sofern die entsprechende Option in den Detailsinstellungen der jeweiligen **GINA Domain** unter **GINA SETTINGS FOR** **Extended settings** **Allow account self-registration in GINA portal without initial mail** gesetzt wurde.

9.61 GINA: Apple E-Mail App zeigt GINA-Mail unverschlüsselt an

Ausgangssituation:

Auf einem Endgerät mit Betriebssystem iOS wird in der Apple E-Mail App eine vermeintliche GINA-Nachricht im Klartext dargestellt.

In der Apple E-Mail-App ist sowohl das Sender- als auch das Empfänger E-Mail Konto eingerichtet

Frage:

Weshalb die E-Mail, welche als GINA-Nachricht gesendet wurde beim Empfänger im Klartext zu sehen?

Antwort:

Die Apple E-Mail App erkennt intern, dass es sich bei der E-Mail aus den gesendeten E-Mails des Sender-Kontos und dem Posteingang des Empfänger-Kontos um dieselbe handelt und stellt dort anstatt der GINA-verschlüsselten Nachricht des Empfänger-Kontos die Nachricht des Sender-Kontos dar.

Wurden für das Triggern von Verschlüsseln/GINA vom Sender **Betreffzeilen Schlüsselwort** ⁹⁹ verwendet, lässt sich dieser Vorgang auch daran erkennen, dass das entsprechende **Betreffzeilen Schlüsselwort** ⁹⁹ in der im Posteingang des Empfängers dargestellten E-Mail noch zu sehen ist. Wäre die beim Empfänger dargestellte E-Mail durch die SEPPmail Appliance verarbeitet worden, wäre mit dem Verarbeiten das **Betreffzeilen Schlüsselwort** ⁹⁹ entfernt worden.

Wird das Sender Konto auf dem Endgerät deaktiviert, so wird die E-Mail im Posteingang des Empfängers wieder wie erwartet als GINA-Nachricht dargestellt.

9.62 GINA: Einrichten eines Bewerberportals

Ausgangssituation:

Im Unternehmen soll eine Plattform für Bewerber bereit gestellt werden, über welche Unterlagen sicher übermittelt werden können.

Optional soll ein Bewerber selbstständig in der Lage sein, seinen Account wieder zu entfernen.

Frage:

Was ist auf der SEPPmail Appliance einzurichten, um ein Bewerberportal zu realisieren?

Antwort/ Lösung:

Das folgende Konfigurationsbeispiel bezieht sich auf das Einrichten ohne „virtual hosting“.

Zunächst ist unter **GINA Domains** ^[416] **Domains** ^[416] über **Add GINA domain...** eine neue GINA-Domäne einzurichten.

Im Folgenden **CREATE NEW GINA DOMAIN** ^[422] ist in der gleichnamigen **Sektion Create new GINA domain** ^[422] unter **Description** ein aussagekräftiger Name wie beispielsweise **Bewerberportal** und unter **Hostname** zum Beispiel **bewerbung** einzugeben. Ein **Master Template** kann, muss aber nicht gewählt werden. Mit Klicken von **Create** wird der Vorgang abgeschlossen. Die Ansicht wechselt wieder in das Menü **GINA Domains** ^[416].

Hier wird nun durch Klicken auf den **GINA name** der neu erstellten **Domains** ^[416] in das Detail-Menü **CHANGE GINA SETTINGS FOR** ^[423] gewechselt.

Dort wird unter **Extended settings** ^[431] neben den sonst gewünschten Einstellungen die Option **Only allow GINA users to write new e-mails to default recipients** aktiviert.

Unter **Default recipients** ^[438] wird unter

- **E-mail** die Empfängeradresse für Bewerbungen angegeben, beispielsweise **bewerbung@meinefirma.tld**
- **Display** der Anzeigename, wie er später im Adressfeld der GINA-Oberfläche zu sehen sein soll, eingetragen, zum Beispiel **Bewerbung**

Sofern mehrere Bewerbungen ausgeschrieben werden sollen, wäre auch denkbar, mehrere „Default recipients“ einzurichten, beispielsweise

- **E-mail** = **fachabteilung1@meinefirma.tld** / **Display** = **Stellenausschreibung 1234**
- **E-mail** = **fachabteilung2@meinefirma.tld** / **Display** = **Stellenausschreibung 5678**
- und so weiter

Nun kann an geeigneter Stelle, zum Beispiel auf der Homepage der Link zur GINA-Registrierungsseite publiziert werden. Dieser würde im Beispiel so aussehen:

<https://securemail.meinefirma.tld/bewerbung/web.app?op=register>

Ein Bewerber würde sich daraufhin registrieren, den Link aus der Registrierungs-E-Mail öffnen und nach der Passworteingabe auf die GINA-Seite für das Verfassen einer neuen Nachricht gelangen, bei welcher der **Default recipients** ^[438] „Bewerbung“ (siehe oben) fest eingetragen, beziehungsweise ausschließlich die **Default recipients** ^[438] auswählbar sind. Das Adressieren eines anderen Empfängers ist aufgrund der Option **Only allow GINA users to write new e-mails to default recipients** nicht möglich.

9.63 GINA: Lesebestätigung auch bei Schlüsselwort

Ausgangssituation:

Die SEPPmail Appliance soll bei Anfordern von **GINA** über das entsprechende **Betreffzeilen Schlüsselwort** die verlässliche Lesebestätigung ausstellen, so wie beim Triggern durch das **Microsoft Outlook Add-In**.

Lösung:

Das Ausstellen der verlässlichen Lesebestätigung kann

- global pro **GINA Domain** in den Detailsinstellungen **CHANGE GINA SETTINGS FOR Extended settings** **Sender receives notification when recipient reads GINA mails**
- pro **User** in dessen Detailsinstellungen **USER 'USER@DOMAIN.TLD' User data Notifications**

vorgenommen werden.

Unabhängig von den oben genannten Einstellungen wird die verlässliche Lesebestätigung immer erzwungen, wenn mit der gesendeten E-Mail zusätzlich zu GINA eine Lesebestätigung (disposition-notification-to Header) angefordert wurde. Das MS Outlook Add-In fordert bei Betätigen der Schaltfläche „Verschlüsseln mit Lesebestätigung“ beides an. Wird für das Verfassen von E-Mails kein MS Outlook verwendet, oder steht das MS Outlook Add-In nicht zur Verfügung, so muss das entsprechende Schlüsselwort für GINA-Verschlüsselung (im Standard [priv]) in den Betreff der E-Mail eingegeben und über das entsprechende Menü des E-Mail Clients die Lesebestätigung angefordert werden.

Alternativ könnte beim Anfordern der GINA-Verschlüsselung über das **Betreffzeilen Schlüsselwort** generell zentral der disposition-notification-to Header per **Custom commands** gesetzt werden. Der entsprechende Code müsste unter **Custom commands for outgoing e-mails BEFORE encryption** platziert werden und könnte wie folgt aussehen:

Zeile	Code
01	# Begin: Custom commands for outgoing e-mails BEFORE encryption
02	log(1,'Begin: Custom commands for outgoing e-mails BEFORE encryption');
03	# Begin: Requesting read receipt, when GINA is triggered
04	log(1,'Begin: Requesting read receipt, when GINA is triggered');
05	if(compare('subject','match','\[priv\]')) {
06	if (!compare('disposition-notification-to','match','*.')) {
07	setheader('disposition-notification-to','\$header from');
09	}
10	}
11	log(1,'End: Requesting read receipt, when GINA is triggered');
12	# End: Requesting read receipt, when GINA is triggered
13	log(1,'End: Custom commands for outgoing e-mails BEFORE encryption');
14	# End: Custom commands for outgoing e-mails BEFORE encryption

Code

Beschreibung

In diesem Beispiel wird zunächst geprüft, ob das Betreffzeilen Schlüsselwort für GINA-Verschlüsselung gesetzt ist (**Zeilen 05**). Falls ja, wird geprüft, ob die Lesebestätigung bereits angefordert wurde (**Zeilen 06**). Falls nicht, wird der disposition-notification-to Header mit dem Absender aus dem From-Header der E-Mail als Empfänger der Lesebestätigung gesetzt (**Zeilen 07**).

9.64 GINA: Öffnen des HTML-Anhangs einer GINA-Nachricht in iOS schlägt fehl

Ausgangssituation:

Eine GINA-Nachricht soll auf einem iOS baasiertem Gerät gelesen werden. Das Öffnen des GINA-Anhangs funktioniert jedoch weder mit, noch ohne installierter SEPPmail-App nicht. Nach dem Bestätigen der erscheinenden Meldung mit „OK“ beginnt scheinbar der Ladevorgang, jedoch passiert nicht weiter.

Frage:

Wie lässt sich der GINA-Anhang öffnen?

Ursache:

Für die GINA-Webseite ist auf der SEPPmail Appliance kein gültiges Zertifikat vorhanden. Dies kann durch Öffnen der GINA-Webseite – zum Beispiel <https://securemail.meinefirma.tld/web.app> – mit einem normalen Browser auf dem iOS Gerät überprüft werden.

Lösung:

Einbinden eines gültigen Zertifikates unter **SSL** ^[319] beziehungsweise sofern bei Betreiben mehrerer GINA-Webseiten **Use virtual hosting** ^[423] zum Einsatz kommt, jeweils einbinden eines gültigen SSL-Zertifikates pro **GINA domain** ^[416] via **SSL certificate** ^[423].

9.65 GINA: Paralleles Verwenden von „Account login“ und „Unique e-mail password“

Ausgangssituation:

Für E-Mail Empfänger ohne eigenem Schlüsselmaterial, mit welchen jedoch häufiger kommuniziert wird, soll GINA unter Verwendung eines festen Accounts (**Account login**^[447]) verwendet werden.

Für eine einmalige sichere Kommunikation soll jedoch der Registrierungsprozess entfallen, das Passwort also nur für die jeweils gesendete GINA-Mail gültig sein (**Unique e-mail password**^[451]).

Frage:

Ist ein paralleles Verwenden beider Authentifizierungsvarianten möglich?

Antwort / Lösung:

Ja, die Möglichkeit besteht. Hierzu müssen zunächst zwei separate **GINA Domains**^[416] angelegt werden, eine mit aktivem **Account login**^[447], die andere mit aktiver **Unique e-mail password**^[451].

In den Einstellungen der **Managed domain**^[247] (siehe **Mail System**^[247]), beziehungsweise **EDIT MANAGED DOMAIN**^[266] wird unter **Settings**^[266] **GINA domain** die **GINA Domain**^[416] ausgewählt, welche per Standard verwendet werden soll. Im weiteren Verlauf des Beispiel wird angenommen, dass **Account login**^[447] das gewählte Standardverfahren ist.

Im nächsten Schritt wird unter **Mail Processing**^[286] **Ruleset generator**^[287] **Custom commands**^[308] die **Option Custom commands for outgoing e-mails BEFORE encryption**: aktiviert und im darunterliegenden Eingabefeld zum Beispiel folgender Code eingegeben:

Zeile	Code
01	# Begin: Custom commands for outgoing e-mails BEFORE encryption
02	log(1,'Begin: Custom commands for outgoing e-mails BEFORE encryption');
03	if (compare('subject','substitute','\[once\]')) {
04	flag('once',1);
05	}
06	log(1,'Begin: Custom commands for outgoing e-mails BEFORE encryption');
07	# Begin: Custom commands for outgoing e-mails BEFORE encryption

Code

Somit kann durch Markieren einer E-Mail mit dem Schlüsselwort [once] im Betreff über die noch zu erstellende **ENCRYPTION POLICY**^[313] angesteuert werden.

Nun wird in **Mail Processing**^[286] via **Edit policy table...** in das Sub-Menü **ENCRYPTION POLICY**^[313] gewechselt, in welchem über **Create new encryption policy...**^[314] die bereits genannte Regel erstellt wird. Dabei ist darauf zu achten, dass unter **Policy flag** „once“ (ohne Anführungszeichen) eingetragen, unter Encryption mode „GINA-only“ und unter **GINA options** die **GINA Domain**^[416] ausgewählt wird, in welcher die **Unique e-mail password**^[451] verwendet wird.

9.66 GINA: Session / Verbindungs-Abbrüche

Ausgangssituation:

Bei einem GINA-Benutzer kommt es bei Aktionen innerhalb des GINA-Portals immer wieder zu Verbindungsabbrüchen. Dies ist vor allem bei mobilen Endgeräten, insbesondere mit dem Betriebssystem iOS (Apple) zu beobachten.

Ursache:

Auf mobilen Endgeräten, insbesondere mit iOS wechselt mitunter der "User Agent". Dadurch können Anfragen des Clients - also indirekt des GINA-Benutzers - nicht mehr korrekt zugeordnet werden und die Kommunikation bricht ab.

Lösung:

Aktivieren der Option **Do not add the clients user agent to the session protector originator**^[437]
(siehe **Change GINA Settings for**^[423] **Extended Settings**^[437]).

9.67 GINA: Session Timeouts

Ausgangssituation:

Ein GINA-Benutzer, ist an der GINA-Oberfläche angemeldet.

Nach einiger Zeit ohne weiterer Aktion kann durch den GINA-Benutzer auf der GINA-Oberfläche nicht mehr gearbeitet werden, da die Session abgelaufen ist.

Frage:

Ist die Zeit für den Ablauf einer GINA-Session konfigurierbar, beziehungsweise wann läuft diese ab?

Antwort:

Der Ablauf einer GINA-Session ist nicht konfigurierbar.

Bei angemeldetem Benutzer und aktivem „Schreiben“ Fenster wird alle 10 Minuten ein Keep-Alive gesendet. Dies wird jedoch nach 12 Stunden durch einen „Hard-Timeout“ beendet. Ansonsten greift ein Session-Timeout von 30 Minuten.

9.68 GINA: SMS-Anbieter

Ausgangssituation:

Das Mitteilen initialer GINA-Passworte, beziehungsweise das Zurücksetzen von Passwörtern für GINA Accounts soll automatisiert werden. Dabei soll das SMS-Verfahren zum Einsatz kommen. Ein SMS-Gateway ist nicht vorhanden. Stattdessen soll ein SMS-Dienst im Internet verwendet werden.

Frage:

Gibt es eine Empfehlung, beziehungsweise welche SMS-Provider wurden bereits erfolgreich angebunden?

Antwort:

Rückmeldungen bezüglich erfolgreich angebundener liegen uns bislang zu

- aspsms.com der VADIAN.NET AG (www.aspsms.com)
- interactive digital media GmbH (www.i-digital-m.com)
- websms der sms.at mobile internet services gmbh und atms GmbH (www.websms.de)

vor.

Jedoch sollte jeder andere Provider ebenfalls anzubinden sein. Wichtig dabei ist jedoch, dass dieser eine entsprechende Rückmeldung bei erfolgreichem, beziehungsweise fehlgeschlagenem Versand zurückgibt. Ebenso sind gegebenenfalls die erforderlichen Firewall-Freischaltungen im Vorfeld vorzunehmen.

aspsms.com

Eine Beispielkonfiguration zu aspsms.com ist jeweils bei der Auswahl **GINA Domains** ⁴¹⁶ **SMS passwords** ⁴¹⁸

- Use xml service
- Use HTTP GET service

zu sehen.

interactive digital media GmbH

Mit interactive digital media GmbH konnte bisher nur „Use HTTP GET service“ erfolgreich implementiert werden. Ein Konfigurationsbeispiel sieht wie folgt aus:

Server address

<https://api.i-digital-m.com>

http-get string

/v1/sms?

accept=xml&method=POST&username=<USERNAME>&password=<PASSWORD>=latin9&sender=SMail&recipient=\$countrycode\$localnumber&message=\$sms

websms

Mit websms wurde bislang ebenfalls nur die von websms präferierte Variante über die WEB API (HTTP GET) getestet. Ein Konfigurationsbeispiel sieht wie folgt aus:

Server address

<https://api.websms.com>

http-get string

/rest/smsmessaging/text?

access_token=<ACCESS_TOKEN>&messageContent=\$sms&recipientAddressList=\$countrycode\$localnumber
(siehe gegebenenfalls auch https://developer.websms.com/rest-api/smsmessaging_simple_get/)

ProSMS

Auch mit ProSMS wurde bislang nur die von ProSMS präferierte Variante über die WEB API (HTTP GET) getestet. Ein Konfigurationsbeispiel sieht wie folgt aus:

Server address

<https://prosms.dds.a1.net>

http-get string

```
/mssms/rest/sendSms.do?  
username=<USERNAME>&password=<PASSWORD>&recipients=$countrycode$localnumber&encoding=8&split  
msg=true&msgtext=$sms
```

9.69 GINA: „Kopie an mich selbst“: Vertauschter Absender/Empfänger

Ausgangssituation:

Der Empfangende einer GINA-Nachricht hat beim Antworten das Auswahlfeld „Kopie dieser Nachricht anfordern“ aktiviert.

Bei der GINA-Träger-E-Mail der GINA-verschlüsselten Kopie an den Antwortenden sind Absender und Empfänger vertauscht.

Ursache:

Dies ist technisch nicht anders zu lösen, da andernfalls die Kopie der GINA-Antwort nicht an den Antwortenden, sondern an den initial Absendenden der ursprünglichen GINA-Nachricht gesendet würde.

9.70 Hyper-V: Hardware Einstellungen

Ausgangssituation:

Die SEPPmail Appliance soll als virtuelle Maschine unter Microsoft Hyper-V betrieben werden.

Frage:

Wie soll die Gastmaschine konfiguriert werden.

Antwort:

Beim Einrichten der Gastmaschine ist als „Generation der virtuellen Computers“ „Generation 1“ zu wählen.

Die Hardware-Anforderungen sind jeweils dem Kapitel [Sizing](#) ^[78] zu entnehmen.

Sollen virtuelle IP-Adressen zum Einsatz kommen, ist unbedingt der entsprechende [Hinweis](#) ^[226] der **Sektion IP ALIAS addresses** ^[226] zu beachten!

9.71 IBM Notes: Schaltfläche für verschlüsseltes Senden erzeugen

Ausgangssituation:

Auf IBM Notes Clients sollen - ähnlich wie über das Add-In in Microsoft Outlook - Schaltflächen für das Markieren / Triggern von E-Mails angezeigt werden.

Frage:

Gibt es von SEPPmail auch für IBM Notes ein Add-In?

Antwort:

Aufgrund der andersgearteten Struktur von IBM Notes, kann hierfür kein Add-In bereitgestellt werden. Jedoch bietet IBM Notes die Möglichkeit, die E-Mail-Schablone so anzupassen, dass auch hier entsprechende Schaltflächen angezeigt werden können.

Um unter Umständen bereits vorhandene Anpassungen an der Mail-Schablone nicht zu gefährden, liefern wir lediglich ein Beispiel, wie eine Schaltfläche erzeugt werden kann. Die eigentliche Änderung obliegt dem Kunden, beziehungsweise dessen Systembetreuer.

Anbei ein Beispiel-Code für das Einfügen einer Schaltfläche "Senden verschlüsselt":



```
MEMO_SEND:="1024";
FIELD Subject := "[confidential]" : Subject ;
FIELD ActionInProgress:=MEMO_SEND;
@If(@Command([FileSave]);@Command([FileCloseWindow]);@Return(""))
```

Somit würde das **Betreffzeilen Schlüsselwort** [164] [confidential] beim Versenden mittels der rot markierten Schaltfläche in die Betreffzeile eingefügt werden.

Eventuell weitere Schaltflächen für das Signieren, beziehungsweise gleichzeitige Verschlüsseln und Signieren können aus diesem Beispiel abgeleitet werden.

9.72 IME: Interne E-Mails verschlüsseln

Ausgangssituation:

Die SEPPmail Appliance soll neben der E-Mail Kommunikation in das Internet auch den internen E-Mail Verkehr absichern.

Frage:

Wie kann das Absichern interner E-Mails, also innerhalb der eigenen E-Mail-Domäne realisiert werden?

Lösung:

In diesem Zusammenhang sollten zunächst die Hinweise zum Absichern des internen E-Mail Verkehrs im Allgemeinen betrachtet werden (siehe [Internal Mail Encryption \(IME\)](#) ¹¹⁴ ff.).

Entsprechend den individuellen Anforderungen sollte dann die Variante [SEPPmail IME 1.0](#) ¹¹⁹ oder [SEPPmail IME 2.0](#) ¹²¹ gewählt werden.

9.72.1 IME 1.0

Für das Umsetzen der hier genannten [SEPPmail IME 1.0](#) ¹¹⁹ ist lediglich der Erwerb der erforderlichen [Internal Mail Encryption \(IME\) Lizenz](#) ¹²⁹ und das Einrichten des [Microsoft Outlook Add-In](#) ¹⁹⁰ mit den unter [Interne Verschlüsselung](#) ²¹⁰ genannte Einstellungen für [IME 1.0](#) ¹¹⁹ erforderlich.

9.72.2 IME 2.0

Für **SEPPmail IME 2.0** [121] sind neben dem Erwerb der erforderlichen **Internal Mail Encryption (IME) Lizenz** [129] und das Einrichten des **Microsoft Outlook Add-In** [190] mit den unter **Interne Verschlüsselung** [210] genannte Einstellungen für **IME 2.0** [121] noch weitreichendere, infrastrukturelle Maßnahmen zu ergreifen.

Da **IME 2.0** [121] zumeist in Microsoft Windows Umgebungen beziehungsweise Netzwerken betrieben wird, sind in den folgenden Beschreibungen Microsoft Windows typische Bezeichnungen zu finden, welche gegebenenfalls auf andere Drittsystem adaptiert werden müssen.

9.72.2.1 Vorbereitung

Wie bereits in **SEPPmail IME 2.0** [121] beschrieben, sind sowohl infrastrukturelle Vorbereitungen zu treffen, als auch Anpassungen an den Systemen vorzunehmen. Diese Vorbereitenden Maßnahmen sind in den folgenden Punkten beschrieben.

9.72.2.1.1 Infrastruktur

Wie in der Beschreibung des **Microsoft Outlook Add-In** [190] für **Interne Verschlüsselung** [210] **IME 2.0** [121] bereits erwähnt, muss dem Outlook Client Schlüsselmateriale für das Signieren und Verschlüsseln der erzeugten Container-E-Mail bereitgestellt werden.

Im Regelfall werden alle am **Windows- / Outlook-Client** [744] benötigten Zertifikate über die Windows Group Policy Objects (GPOs) ausgerollt.

Für die Signaturschlüssel (S/MIME) der internen Benutzer ist eine interne CA erforderlich. Meist ist das eine Microsoft PKI, welche bereits für die Schlüsselverwaltung zur Absicherung des internen Netzwerkverkehrs vorhanden ist. Über diese PKI werden nun zusätzlich für alle E-Mail Adressen S/MIME Schlüsselpaare (PKCS#12) ausgestellt und für die jeweils zugehörigen Benutzer ausgerollt. Im Windows Zertifikatsspeicher der Clients sollte das Schlüsselpaar somit in
Zertifikate - Aktueller Benutzer / Eigene Zertifikate
abliegen.

Weiterhin sollte diese PKI eine LDAP-Key-Server-Funktion für den automatisierten Bezug der öffentlichen Schlüssel (Zertifikate) der für die internen Benutzer ausgestellten S/MIME Zertifikate bereit stellen. Über diese Funktion bezieht die **SEPPmail Appliance** [743] im produktiven Betrieb die für das Verschlüsseln an interne Empfänger benötigten Zertifikate.

Natürlich muss dem Root CA Zertifikat dieser internen CA am **Windows- / Outlook-Client** [744] vertraut werden, Das heißt, dieses Root Zertifikat muss dort unter
Zertifikate (lokaler Computer) / Vertrauenswürdige Stammzertifizierungsstellen
zu finden sein.

Für das eigentliche Verschlüsseln einer E-Mail vom MS Outlook Client bis zur SEPPmail Appliance muss weiterhin das IME Zertifikat für die jeweils eigene E-Mail Domäne, sowie das Root CA Zertifikat der ausstellenden CA dieses Zertifikates importiert werden. Beide Zertifikate sind hierfür zunächst - wie in **SEPPmail Appliance** [743] beschrieben - zu generieren/importieren und ebenfalls auf die **Windows- / Outlook-Client** [744] auszurollen.

Das Root Zertifikat sollte im Anschluss ebenfalls unter
Zertifikate (lokaler Computer) / Vertrauenswürdige Stammzertifizierungsstellen
das IME Zertifikat je nach Anwendungsfall unter
Zertifikate (lokaler Computer) / Andere Personen
beziehungsweise
Zertifikate - Aktueller Benutzer / Andere Personen
zu finden sein.



Hinweis:

Der Ordner „Andere Personen“ wird im Standard erst dann im Zertifikatsspeicher angelegt, wenn für einen Kontakt im Outlook-Adressbuch ein Zertifikat importiert wurde. Das heißt, für die E-Mail Adresse aus dem IME-Zertifikat sollte in der Global Address List (GAL) ein Eintrag mit dem zugehörigen Zertifikat erstellt werden.

9.72.2.1.1.1 GAL Eintrag erstellen

Zunächst ist im Exchange Control Panel (ECP) einen neuen Kontakt (nicht Benutzer!) anzulegen. Dabei können die Felder

Vorname
Initialen
Nachname

leer bleiben.

Unter

***Anzeigename**
***Name**
***Alias**

sollte jeweils ein identischer Eintrag erfolgen, welcher mit einem Sonderzeichen wie zum Beispiel einem Unterstrich „_“ beginnt (siehe auch [Verzögerter Start von MS Outlook](#) ^[746]) und gegebenenfalls auch auf IME hindeutet, wie zum Beispiel

_IME

oder

#domain-confidentiality-authority

Als

***Externe E-Mail-Adresse**

ist der Eintrag aus dem CN (Common Name) des IME Zertifikates (siehe auch [SEPPmail Appliance](#) ^[743], vierter Absatz) zu verwenden. Dieser lautet in der Regel wie in folgendem Beispiel

domain-confidentiality-authority@ime.meinefirma.tld

wobei meinefirma.tld dem **Domain Name** ^[247] der **Managed Domain** ^[247] entspricht, für welche IME eingerichtet werden soll.

In

Organisationseinheit

ist in der Regel der Pfad auszuwählen, in welchem per Standard „Kontakte“ abgelegt werden. Häufig lautet dieser meinefirma.tld/Benutzer/Kontakte.

Nun ist das IME Zertifikat der jeweiligen **Managed Domain** ^[247] auf den Windows Domaincontroller/Exchange Server abzulegen, zum Beispiel unter

C:\Temp\Domain_certificate_for_ime.meinefirma.tld.crt

In einer Windows Powershell mit entsprechenden Adminrechten wird nun durch Eingabe des Befehls

certutil.exe -dsPublish C:\Temp\Domain_certificate_for_ime.meinefirma.tld.cer

das Zertifikat dem zuvor angelegten Kontakt, aufgrund des Übereinstimmens des „CN“ aus dem Zertifikat und „***Externe E-Mail-Adresse**“ aus dem Kontakt, zugeordnet.

Die Rückmeldung des Befehls (anhand des Beispielnamens **_IME** sollte dann in etwa

CN=_IME,OU=Kontakte,OU=Benutzer,DC=meinefirma,DC=tld?userCertificate

Zertifikat wurde zum Verzeichnisdienstspeicher hinzugefügt.

CertUtil: -dsPublish-Befehl wurde erfolgreich ausgeführt.
lauten

Für das Überprüfen des Erfolgs dieses Vorgangs kann nun der Kontakt im „ADSI Editor“ geöffnet werden. Dazu ist im ADSI Editor der Pfad zu wählen, welcher bei der Anlage des Kontakts unter „**Organisationseinheit**“ gewählt wurde. Dort sind nun die Eigenschaften des Kontaktes -im Beispiel „**CN= _IME**“ (beziehungsweise „**CN=#domain-confidentiality-authority<%OEM-CLOSE-QUOTE%**) durch Klick mit der rechten Maustaste zu wählen.

Im sich öffnenden Fenster ist nun auf den Karteikartenreiter „Attribute Editor“ zu wechseln und bis zum „Attribute“ „userCertificate“ zu scrollen.

Dieses „Attribute“ sollte nur einen „Wert“ aufweisen, welcher in etwa wie folgt aussehen könnte:

\30\82\06\68\30\83\05\50\AD\03\02\01\...

Abschließend sollte in der Exchange-Shell zunächst die Globale Adressliste und im Anschluss die Offline Adressbücher aktualisiert werden.

Dabei kann mit

Get-GlobalAddressList

der Name der Globalen Adressliste herausgefunden werden, in der Regel lautet dieser

Globale Standardadressliste

Diese wird nun mittels

Update-GlobalAddressList -Identity Globale Standardadressliste

aktualisiert.

Nun sollten noch die Offline Adressbücher entsprechend aktualisiert werden. Ausgelesen werden die vorhandenen Offline Adressbücher mittels

Get-OfflineAddressBook

In der Rückgabe werden die Namen der Offline Adressbücher sowie die jeweils zugehörige Adressliste angezeigt, in etwa

<u>Name</u>	<u>Versions</u>	<u>AddressLists</u>
Standard-Offlineadressbuch	{Version 4}	{\Globale Standardadressliste}
OAB-XYZ	{Version 4}	{\Globale Standardadressliste}

Im Beispiel sollten also alle Offline Adressbücher, welche der **AddressList** {\Globale Standardadressliste} angehören mittels

Get-OfflineAddressBook -Identity "Standard-Offlineadressbuch"

Get-OfflineAddressBook -Identity "OAB-XYZ"

aktualisiert werden.

9.72.2.1.2 SEPPmail Appliance

Zunächst muss das Root CA Zertifikat der internen PKI (und optional die Zwischenzertifikate) auf der SEPPmail Appliance unter **X.509 Root Certificates** [480] mittels **Import S/MIME root certificate** importiert werden. Dabei ist darauf zu achten, dass beim Import unter **Options** [484] der Haken bei **Automatically trust the imported X.509 Root Certificates** [484] gesetzt ist.

Weiterhin muss entschieden werden, ob für die IME Verschlüsselung ein auf der SEPPmail Appliance selbst generiertes Zertifikat verwendet werden soll, oder ein importiertes Zertifikat einer anderen (meist der MS-PKI welche auch die S/MIME Zertifikate der internen Benutzer generiert) verwendet werden soll.

Soll ein importiertes Zertifikat verwendet werden, so wird die entsprechende PKCS#12 Datei in den Detailsinstellungen der jeweiligen **Manged domain** [247] (**EDIT MANAGED DOMAIN** [266]) in der **Sektion Internal mail encryption** [276] über die Schaltfläche **Import S/MIME key...** hochgeladen. Sofern der ausstellenden PKI nicht bereits vertraut wird (siehe oben), ist auch das Root CA Zertifikat dieser CA - wie oben beschrieben - unter **X.509 Root Certificates** [480] zu importieren.

Soll ein von der SEPPmail Appliance selbst generiertes Zertifikat verwendet werden, so ist zunächst - sofern nicht bereits geschehen - die interne **CA** [328] einzurichten. Abschließend wird das Root CA Zertifikat der soeben eingerichteten **CA** [328] über die Schaltfläche **Download certificate** der **Sektion Backup** [337] heruntergeladen, damit es zur Verteilung - wie unter **Infrastruktur** [741] beschrieben - bereit steht.

Im Anschluss ist in den Detailsinstellungen der jeweiligen **Manged domain** [247] (**EDIT MANAGED DOMAIN** [266]) in der **Sektion Internal mail encryption** [276] über die Schaltfläche **Generate new S/MIME key** das IME Zertifikat zu generieren. Durch Klicken auf den Fingerprint des soeben generierten Zertifikates öffnet das zugehörige Detailmenü, in welchem das Zertifikat über die Schaltfläche **Download certificate** für das anschließende Verteilen (siehe **Infrastruktur** [741], beziehungsweise **GAL Eintrag erstellen** [742]) heruntergeladen werden kann. Weiterhin sollte die in den Zertifikatsdetails unter **Issued to** angezeigte **E-Mail Address** (beispielsweise domain-confidentiality-authority@ime.meinefirma.tld) zur weiteren Verwendung notiert werden (siehe auch **Windows- / Outlook-Client** [744]).

Damit die SEPPmail Appliance E-Mails, welche an interne E-Mail Empfänger adressiert sind gemäß **Verschlüsselungshierarchie** [66] mittels S/MIME verschlüsselt, müssen die öffentlichen Schlüssel (Zertifikate) der internen Empfänger auf der SEPPmail Appliance bereit gestellt werden. Hierfür wird die interne CA in der Regel unter **Mail Processing** [286] **Ruleset generator** [287] als **Key server** [309] vom **Type** „S/MIME“ eingetragen, in etwa

Type	Recipient mask (regexp)	URI	Bind DN
S/MIME	@meinefirma\.tld	ldaps://directory.meinefirma.local	CN=LDAP,OU=Service,OU=Users,DC=meinefirma,DC=local

Bind PW	Base DN	Ignore failure
mypassword	OU=Users,DC=meinefirma,DC=local	

Sollten nicht alle E-Mail Adressen des Unternehmens mit entsprechendem Schlüsselmateriale versorgt sein, so würden bei angeforderter interne Verschlüsselung an interne Empfänger ohne eigenem Schlüssel GINA-Mails gesendet. In diesem Fall ist dringend das Einrichten der **External authentication** ^[274] (siehe **EDIT MANAGED DOMAIN** ^[268]) zu empfehlen, um das Anmelden an der GINA-Oberfläche mit dem internen Window-Passwort zu ermöglichen.

9.72.2.1.3 Windows- / Outlook-Client

Zunächst müssen die unter **Infrastruktur** ^[741] bereits genannten und zum Teil unter **SEPPmail Appliance** ^[743] erzeugten Zertifikate auf dem Client verfügbar sein:

- internes S/MIME Schlüsselpaar (PKCS#12) für den jeweils angemeldeten Benutzer
Zertifikate - Aktueller Benutzer / Eigene Zertifikate
- IME Zertifikat, passend zum Domänenteil der eigenen E-Mail Adresse, wie es in der SEPPmail Appliance in den Detailsinstellungen der jeweiligen **Managed domain** ^[247] (**EDIT MANAGED DOMAIN** ^[268]) in der **Sektion Internal mail encryption** ^[276] zu finden ist
Zertifikate (lokaler Computer) / Andere Personen
beziehungsweise
Zertifikate - Aktueller Benutzer / Andere Personen
- Root CA Zertifikat(e) der jeweils ausstellenden CAs der beiden oben genannten Zertifikate unter
Zertifikate (lokaler Computer) / Vertrauenswürdige Stammzertifizierungsstellen

Im nächsten Schritt wird das **Microsoft Outlook Add-In** ^[190] installiert/ausgerollt (siehe **Installation** ^[198]). Empfohlen wird die dynamische Konfiguration des Add-Ins ebenfalls via GPOs (siehe **Add-In Verwaltung** ^[212]).

9.72.2.2 Eingehende E-Mails umverschlüsseln

Das Entschlüsseln eingehender E-Mails und anschließende Verschlüsseln mit dem internen Schlüsselmaterial des/der Empfänger(s) ist zum Beispiel durch folgenden Code zu gewährleisten:

Zeile	Code
01	# Begin: Custom commands for incoming e-mails AFTER decryption
02	log(1,'Begin: Custom commands for incoming e-mails AFTER decryption');
03	# Begin: Encrypt decrypted e-mails to internal users
04	log(1,'Begin: Encrypt decrypted e-mails to internal users');
05	if(compare('subject','match','\[secure\])) {
06	\$IME encrypt;
07	}
08	log(1,'End: Encrypt decrypted e-mails to internal users');
09	# End: Encrypt decrypted e-mails to internal users
10	log(1,'End: Custom commands for incoming e-mails AFTER decryption');
11	# End: Custom commands for incoming e-mails AFTER decryption

[Code](#)

Dabei werden zunächst eingehende, durch die SEPPmail Appliance entschlüsselte Nachrichten am entsprechenden Kennzeichen ([secure]) erkannt und über das zu definierende Makro `$IME_encrypt` nach intern verschlüsselt.

Der Code des Makros `$IME_encrypt` könnte dabei wie folgt lauten:

Zeile	Code
01	# Begin: Custom macros and commands for all e-mails BEFORE processing
02	log(1,'Begin: Custom macros and commands for all e-mails BEFORE processing');
03	IME encrypt = {
04	# Begin: IME encrypt
05	ldap_getcerts('ldaps://directory.meinefirma.tld;;;ou=pki-participant,dc=pki,dc=meinefirma,dc=tld');
06	if (smime keys avail()) {
07	log(1,'S/MIME certificate available for recipient \$to');
08	if (encrypt smime('true')) {
09	log(1,'Encryption successful');
10	}
11	} else {
12	if (!webmail keys avail()) {
13	log(1,'no GINA account available, creating new account');
14	webmail keys gen('','0');
15	}
16	if (encrypt webmail()) {
17	log(1,'Encryption successful');
18	}
19	}
20	# End: IME encrypt
21	};
22	log(1,'End: Custom macros and commands for all e-mails BEFORE processing');
23	# End: Custom macros and commands for all e-mails BEFORE processing

[Code](#)

Natürlich sind an dieser Stelle zahlreiche Variationen denkbar. So könnte beispielsweise das Verschlüsseln nach intern von der Zugehörigkeit zu einer AD-Gruppe oder dem bloßen Vorhandensein eines internen Schlüssels abhängig gemacht werden.

Auch der Umgang mit S/MIME Signaturen kann an dieser Stelle gegebenenfalls explizit definiert werden.

Um zu verhindern, dass Outlook beim Antworten auf eine E-Mail verschlüsselt, was an eine externe Adresse mangels im Outlook verfügbarem Zertifikat fehlschlagen würde, muss im AD eine Richtlinie eingerichtet sein, welche das Aktivieren der Verschlüsselung im Outlook unterdrückt.

Da das Add-In programmiertechnisch von dieser Richtlinie nicht betroffen ist, funktioniert dieses dennoch, sodass die Schaltfläche „Auch intern verschlüsseln“ weiterhin funktionsfähig bleibt.

Erhält ein Empfänger im Outlook eine verschlüsselte E-Mail mit gesetztem Vertraulichkeits-Flag (Header sensitivity=companyconfidential), so setzt Outlook selbstständig die Verschlüsselung auf „AN“.

Das Add-In ignoriert jedoch das Outlook Kennzeichen zum Verarbeiten der E-Mail, sofern eine Schaltfläche für Verschlüsseln oder Signieren aktiv ist, und unterdrückt somit das Outlook seitige Verschlüsseln / Signieren.

Wird jedoch ohne aktive Schaltfläche für ein kryptographisches Behandeln der E-Mail geantwortet, so würde Outlook auf eine verschlüsselte E-Mail versuchen verschlüsselt zu antworten.

9.73 IME: Verzögerter Start von MS Outlook

Ausgangssituation:

Auf der SEPPmail Appliance wird im Zusammenspiel mit dem **SEPPmail Microsoft Outlook Add-In** ^[190] **IME 2.0** ^[121] umgesetzt.

Dabei fällt auf, dass nach dem Konfigurieren des **SEPPmail Microsoft Outlook Add-In** ^[190] für **IME 2.0** ^[121] der Start von MS Outlook extrem lange dauert.

Frage:

Weshalb verlangsamt das **SEPPmail Microsoft Outlook Add-In** ^[190] nach dem Konfigurieren für **IME 2.0** ^[121] den Start von MS Outlook?

Antwort:

Der in der Regel in der „Global Address List (GAL)“ des Exchange Servers zu erzeugende Kontakt, welcher als E-Mail Adresse den Eintrag des CN des IME-Zertifikates (siehe **Internal Mail Encryption** ^[276]) und das IME-Zertifikat selbst enthält, ist aufgrund der alphabetischen Sortierung relativ weit am Ende der GAL. Das **SEPPmail Microsoft Outlook Add-In** ^[190] sucht beim Start von MS Outlook automatisch nach diesem Eintrag um an das IME-Zertifikat zu kommen. Ist die GAL entsprechend groß, kann diese Suche mitunter sehr lange dauern. Als Folge verzögert sich der Start von MS Outlook entsprechend.

Eine weitere Folge daraus könnte ein automatisches Deaktivieren des **SEPPmail Microsoft Outlook Add-In** ^[190] sein, sofern dem nicht durch entsprechende Konfigurationsmaßnahmen entgegengewirkt wurde.

Lösung:

Der GAL Kontakt sollte mit einem Sonderzeichen im Namen, zum Beispiel einem Unterstrich „_“ beginnen. Dadurch rückt der Eintrag relativ weit an den Anfang des GAL. Hierdurch kann die Suche entsprechend schnell abgeschlossen werden. In der Folge startet Outlook wieder im normalen Zeitrahmen.

9.74 IronPort: Anbinden der SEPPmail Appliance



Achtung:

Wichtig ist die aktuelle Policy des IronPort Systems zu verstehen, bevor Änderungen durchgeführt werden.

Konfigurationsvorschlag

Alle einkommenden E-Mails werden von IronPort empfangen und auf SPAM und Viren geprüft. Alle soweit geprüften E-Mails werden an die SEPPmail Appliance weitergeleitet, wo diese gegebenenfalls entschlüsselt und zur IronPort zurück gesendet werden. Dort werden alle E-Mails (jetzt auch die entschlüsselten) nochmals Viren und SPAM geprüft und an das interne Groupware-System, zum Beispiel Microsoft Exchange oder IBM Domino, weitergeleitet.

Alternativ kann das IronPort-System veranlasst werden, verschlüsselte und/oder signierte E-Mails zu erkennen und nur diese an die SEPPmail Appliance umleiten. Alle anderen E-Mails werden direkt an das interne Groupware-System weitergeleitet.

Ausgehende E-Mails schickt das interne Groupware-System zu IronPort. Dieses leitet ausgehende E-Mails in jedem Fall zur SEPPmail Appliance weiter. Dort wird das Regelwerk gepflegt, welche E-Mails signiert und verschlüsselt werden sollen. Anschließend werden die ausgehenden E-Mails von der SEPPmail Appliance zurück zum IronPort-System geleitet, welches als einziges System E-Mails in Richtung Internet versendet.

Das Problem bei dieser Konfiguration ist, dass die SEPPmail Appliance in der Relay-Liste des IronPort-Systems stehen muss, da die SEPPmail Appliance ausgehende E-Mails in Richtung Internet versenden will. Für alle Hosts in der Relay-Liste von IronPort gilt automatisch immer die Outgoing Mail Policy. Nach der aktuellen Outgoing Policy findet dort keine Virenprüfung statt, so dass die SEPPmail Appliance Anbindung so keinen Zusatznutzen bringt.

Dazu gibt es zwei Lösungen:

1. Die Outgoing Mail Policy auf dem IronPort System wird so umgebaut, dass sie ähnlich aussieht wie die Incoming Policy. Das ist aber eine unschöne Lösung.
2. Sie konfigurieren einen speziellen Listener, über den die SEPPmail Appliance eingehende E-Mails einliefert. Auf diesem Listener darf die SEPPmail Appliance nicht in der Relay-Liste eingetragen sein. Dieser Listener kann zum Beispiel auf der bestehenden IP-Adresse 192.168.1.11 auf einen speziellen Port (zum Beispiel 10025) gebunden sein, oder auf einer weiteren IP-Adresse im IP-Netzwerk 192.168.1.0/24.

Die Umleitung kann man auf zwei Arten Implementieren:

3. per Content Filter
4. per Message Filter

Der Unterschied zwischen Message Filter und Content Filter ist, dass ein Message Filter immer auf die gesamte E-Mail angewendet wird. Hat eine E-Mail zum Beispiel mehrere Empfänger, so gilt die Aktion für alle Empfänger. Bei einem Content Filter kann man über verschiedene Policy-Einträge die E-Mail aufsplitten. Das sollte in unserem Fall keine Rolle spielen. Ein weiterer Unterschied ist, dass man im Message Filter erkennen kann, ob eine E-Mail verschlüsselt oder signiert ist und somit nur diese E-Mail zur SEPPmail Appliance umleiten kann.

Um die Lösung einfach und übersichtlich zu gestalten empfehlen wir, alle ausgehenden E-Mails zur SEPPmail Appliance weiterzuleiten (nicht nur die zu verschlüsselnden oder signierenden E-Mails) und mit einem Content Filter zu arbeiten.

Konfiguration

IronPort

- Bestehender Listener mit SEPPmail Appliance in der Relay-Liste
- Neuer Listener Incoming SEPPmail Appliance mit SEPPmail Appliance nicht in der Relay-Liste

Incoming Contentfilter : IncomingSEPPmail Appliance

(normalerweise nicht notwendig: Receiving Listener = IncomingMail AND)

Remote IP IS NOT \[IP von SEPPmail Appliance 1\]

AND

Remote IP IS NOT \[IP von SEPPmail Appliance 2\]

(optional, falls Sie nur eine Ihrer Domänen über SEPPmail Appliance betreiben lassen wollen: AND Envelope Recipient ends with [@securemailcustomer.ch](#))

Action: Send to Alternate Destination Host: \[Cluster IP der beiden SEPPmail Appliance\]

SEPPmail Appliance

Die SEPPmail Appliance ist so einzurichten, dass eingehende E-Mails an den **Incoming SEPPmail Appliance Listener** geschickt werden.

Menü **Mail System** ^[247]: Siehe [Zu verwaltende E-Mail Domänen einrichten](#) ^[154].

Domain Name	Server IP Address	Server Port	TLS level	Secure Webmail Settings	Disclaimer Setting
maildomain.ch	[192.168.1.11]	10025	may	[default]	

☐ Automatically create and publish S/MIME domain keys for all domains
☐ Fetch Mail from remote POP3 server
☐ Verify recipient addresses using SMTP-Lookups

Sektion **Managed domains** ^[247]

Das Problem hier ist, dass in der SEPPmail Appliance Konfiguration nur eine einzige IP-Adresse angegeben werden kann, wohin die eingehenden E-Mails weitergeleitet werden, also nicht beide Incoming IP-Adressen Ihrer IronPorts. Hierzu ist es notwendig, einen (fiktiven) DNS-Eintrag zu erzeugen, welcher in beide IP-Adressen der IronPorts aufgelöst werden kann. Dieser fiktive DNS-Name wird als „Server IP address“ der E-Mail Domäne eingetragen.

Ausgehende E-Mail versendet die SEPPmail Appliance an den **bestehenden Listener**:

Siehe [Ausgehenden E-Mail Verkehr steuern](#) ^[155].

☐ Use built-in mail transport agent
☒ Use the following SMTP server:

Server name: 192.168.1.xxx
 User ID:
 Password:

☐ Server requires authentication:

Sektion **Outgoing server** ^[250]

Hier ist die IP-Adresse des Listeners anzugeben, bzw. wie oben ein Hostname, welcher auf beide Listener aufgelöst wird.

Für beide IP-Adressen der IronPort Systeme ist in der SEPPmail Appliance die Relay-Berechtigung einzutragen. Siehe [Mail Relaying](#) ^[156].

Relaying allowed: 192.168.1.11 / 32
 Relaying allowed: 192.168.1.12 / 32
 Add Relaying for: / 32

Sektion **Relaying** ^[254]

Die Konfigurationsbeschreibung für die SEPPmail Appliance - IronPort Anbindung wurde uns mit freundlicher Genehmigung bereit gestellt von:

AVANTEC AG

Badenerstrasse 281

CH-8003 Zürich
www.avantec.ch
info@avantec.ch

9.75 Konfig: Anbinden von LDAP Datenbeständen

Ausgangssituation:

Für die Art des Verarbeitens von E-Mails, das Generieren von SEPPmail Appliance **Users** oder auch für das Anmelden interner Benutzer am GINA-Web-Interface, zum Beispiel für das Nutzen von **External**, ist das Heranziehen externer LDAP Daten, wie zum Beispiel aus dem Microsoft Active Directory (AD), gewünscht.

Frage:

Können externe LDAP Daten für das Verarbeiten in der SEPPmail Appliance genutzt werden?

Antwort:

Ja, Daten aus externen LDAP Quellen können in der SEPPmail Appliance an verschiedenen Stellen genutzt werden. Für die einzelnen Anwendungsfälle existieren jeweils weitere Beschreibungen, beziehungsweise Dokumente:

- Anmelden am GINA-Web-Interface mit externen Zugangsdaten, zum Beispiel einer Microsoft Unternehmensdomäne, also E-Mail-Adresse und Windows-Kennwort.
Hierfür ist unter **Mail System** **Managed domains** in der Tabelle auf die entsprechende E-Mail-Domäne zu klicken. Im folgenden Untermenü **EDIT MANAGED DOMAIN** ist in die **Sektion External authentication** zu navigieren und die entsprechenden Zugangsdaten für die LDAP-Verbindung einzugeben.
- **Einschränken des für kryptographische Aktionen berechtigten Personenkreises mittels LDAP Abfrage**
- **Einschränken des automatischen Generierens von Benutzern auf einen bestimmten Personenkreis via LDAP**
- **Einschränken des LFT berechtigten Personenkreises**
- **Persönliche Fußnoten (footer) automatisiert erstellen**
- ...

9.76 Konfig: Angabe von mehreren E-Mail Servern

Ausgangssituation:

Die SEPPmail Appliance wird in den E-Mail Fluss eingebunden. Nach dem Verarbeiten der E-Mails durch die Appliance sollen diese an einen Cluster abgegeben werden. Für die Server aus dem Cluster existiert weder ein DNS-Eintrag (MX oder Round Robin), noch eine gemeinsame virtuelle IP Adresse.

Die entsprechenden Eingabefelder in der SEPPmail Appliance (**Mail System** ^[247] **Managed domains** ^[247] **EDIT MANAGED DOMAIN** ^[266] **Settings** ^[266] **Forwarding server** und **Mail System** ^[247] **Outgoing server** ^[250] **Server name**) lassen jedoch kein Mehrfacheingabe zu.

Frage:

Wie können alle Systeme aus dem entgegennehmenden Cluster angesprochen werden?

Lösung:

In **System** ^[224] **Advanced view...** **DNS** ^[229] **add local zone** kann zu diesem Zweck ein lokaler, ausschließlich auf der SEPPmail Appliance gültiger MX-Record erzeugt werden.

Hierzu ist unter **Domain name**: ein entsprechender Domänenname einzutragen, der anderweitig niemals vorhanden sein kann, also weder im lokalen Netz noch im Internet.

In den darunterliegenden Feldern **host**: **mx**: **ip**: wird jeweils ein frei wählbare Hostname, die MX-Priorität und die IP-Adresse des jeweiligen für die Cluster-Partner eingegeben.

Dies könnte dann je nach Verwendungszweck zum Beispiel so aussehen:

Domain name:		forwarding.pseudo				
host	mailserver1	mx	10	ip:	10.0.0.11	
host	mailserver2	mx	20	ip:	10.0.0.12	

für den Eintrag **forwarding.pseudo** als **Forwarding server**, beziehungsweise

Domain name:		outgoing.pseudo				
host	relay1	mx	10	ip:	10.0.10.11	
host	relay2	mx	20	ip:	10.0.10.12	

für den Eintrag **outgoing.pseudo** als **Server name** unter **Outgoing server** ^[250].

9.77 Konfig: Bounce von E-Mails nicht authentifzierter Benutzer

Ausgangssituation:

Unter **Mail Processing** ^[286] **Ruleset generator** ^[287] **User creation** ^[289] die Option **Do not create accounts (also disables custom commands for user creation)** ^[289] gewählt. Im Standardverhalten der SEPPmail Appliance werden mit dieser Einstellung E-Mails von Benutzern aus **Managed domains** ^[247], auch trotz angeforderter kryptographischer Aktion unbehandelt durchgeleitet, sofern diese Absender keinen Benutzer Account (siehe **Users** ^[396]) auf der Appliance haben.

Entgegen des Standardverfahrens sollen E-Mails in dieser Konstellation abgewiesen (bounced) werden.

Konfigurationsvorschlag

- Navigieren zu **Mail Processing** ^[286] **Ruleset generator** ^[287] **Custom Commands** ^[308] **Custom commands for User Creation** ^[308]:
- Aktivieren der Option, sowie Einfügen des folgenden Codes in das darunter liegende Eingabefeld:

Zeile	Code
01	# Begin: Custom commands for User Creation
02	log(1,'Begin: Custom commands for User Creation');
03	if (!authenticated()) {
04	log(1,'user account missing, bouncing email');
05	bounce('bounce noauth','true')
06	}
07	log(1,'Begin: Custom commands for User Creation');
08	# Begin: Custom commands for User Creation

Code

- **Umstellen der Option** **Mail Processing** ^[286] **Ruleset generator** ^[287] **User creation** ^[289] von **Do not create accounts (also disables custom commands for user creation)** ^[289] auf **Create accounts for new users if user tries to sign / encrypt** ^[289]

Beschreibung

Die unter **Custom commands for User Creation** ^[308] aufgeführten Befehle werden durch Verwenden der Option **Create accounts for new users if user tries to sign / encrypt** ^[289] immer dann ausgeführt, wenn kryptographische Aktionen angefordert wurden, der anfordernde Absender jedoch nicht als Benutzer auf der Appliance vorhanden ist.

Da nur bereits - manuell - angelegten Benutzern das Ausführen kryptographischer Aktionen gestattet sein soll, wird nun - anstatt einen Benutzer anzulegen - die betreffende E-Mail abgewiesen (gelöscht), eine Bounce-E-Mail unter Verwendung der Vorlage „bounce_no_user“ und mit dem Header der ursprünglichen E-Mail an den Absender gesendet (**Zeile 05**) und der Vorgang in das Log geschrieben (**Zeile 04**).

Damit im Ruleset die entsprechende Stelle erreicht werden kann, muss die **User Creation** ^[289] von **Do not create accounts (also disables custom commands for user creation)** ^[289] auf **Create accounts for new users if user tries to sign / encrypt** ^[289] umgestellt werden.

Variationen

Anstelle des Befehls `bounce()` ^[548] kann die E-Mail auch über den Befehl `drop()` ^[552] abgewiesen werden.

Verwendete

Befehle

```
authenticated() [537]
bounce() [548]
drop() [552]
log() [534]
```

Funktionen

keine

9.78 Konfig: Custom commands for outgoing e-mails AFTER encryption

Ausgangssituation:

Nach dem Verarbeiten ausgehender E-Mails sollen noch weitere Befehle ausgeführt werden, also quasi "Custom commands for outgoing e-mails AFTER encryption"

Lösung:

Dies kann über **Use custom delivery method**³¹² wie folgt realisiert werden:

```
continue'); <Befehl 1>; <Befehl 2>; <Befehl n>; deliver('
```

also beispielsweise

```
continue'); log(1, "Dies ist ein Test"); deliver('
```

Der hier platzierte Eintrag kann in den Custom Commands via **@CUSTOMDELIVER@**⁶²⁹ abgerufen werden.

9.79 Konfig: Queueless Mode

Ausgangssituation:

Die SEPPmail Appliance soll nach dem entgegennehmen einer E-Mail an das Abgebende Relay erst dann den erfolgreichen Empfang („250 ok“) melden, wenn diese E-Mail bereits vom nachfolgenden Relay als erfolgreich empfangen quittiert wurde (ebenfalls „250 ok“).

Grund:

Wird diese Option verwendet, so kann bei einem Austausch der Appliance (zum Beispiel bei einem Hardware-Defekt) annähernd sichergestellt werden, dass keine E-Mails verloren gehen.

Lösung:

Bis zur SEPPmail Appliance Version 11.1.11 stand hierfür die Option **Queueless mode** zur Verfügung. Diese wurde mit der Version 11.1.11 durch die neue Option **Use custom delivery method** ^[312] abgelöst. Durch den Eintrag „queueless“ wird mit dieser Option dasselbe Verhalten erzielt wie vormals durch **Queueless mode**.

Achtung:

Aufgrund dieser Einstellung können - vor allem wenn die E-Mail verarbeitenden Maschinen in unterschiedlichen Netzen stehen - Verzögerungen auftreten. Eine Folge davon können vermehrt auftretende Timeouts sein.

Weiterhin kann das vorläufige Zwischenspeichern einer E-Mail in der E-Mail Warteschlange durch diese Einstellung nicht zu 100% verhindert werden:

- Werden beispielsweise bei ausgehenden E-Mails mehrere E-Mail Domänen adressiert, von denen eine nicht den Empfang mit dem SMTP Code 250 quittiert, so würde die E-Mail an diese eine E-Mail Domäne dennoch in der E-Mail Queue zwischengespeichert werden.
- Bei Komplettausfall des nächsten E-Mail HOPs würde die Appliance ebenfalls die E-Mails in der Warteschlange speichern und somit dem abgebenden System den Empfang quittieren.
- Ebenso werden LFT ^[107] Benachrichtigungs-E-Mails in der Warteschlange zwischengespeichert, wenn der Empfänger temporär nicht erreichbar ist.



Ebenfalls ist zu beachten, dass mit dieser Einstellung ein eventuell in einer **Managed domain** ^[247] eingetragener **Smarthost** ^[247] ignoriert wird. Stattdessen wird immer der global eingetragene **Outgoing Server** ^[250] aus **Use The Following SMTP Server** ^[250] verwendet.

Die Einstellung **Use Built-In Mail Transport Agent** ^[250] ist mit dem **Queueless mode** nicht kompatibel und würde somit beim Versand die Meldung „Could not retrieve default mail routing information - queueless mode disabled“ im Log generieren.

Hinweis zum Update-Verhalten auf die Version 11.1.11

Die Einstellung aus **Queueless mode** wird beim Update in die neue Option **Use custom delivery method** ^[312] automatisch übernommen (Eintrag „queueless“).



9.80 Konfig: Migrieren von „on premises“ zu einem MSP Mandanten

Ausgangssituation:

Kundenseitig besteht der Wunsch, seine on premises Appliance abzubauen und SEPPmail als Service bei einem Provider zu nutzen. Die Konfiguration der on premises Installation soll vom Provider übernommen werden.

Lösung:

Auf der on premises Appliance wird die Mandantenfähigkeit eingeschaltet, ein „Mandanten Backup“ gezogen und dieses beim Provider eingespielt.

Im Detail ist hierfür wie folgt vorzugehen:

auf der „on premises Appliance“

- a) zunächst ist sicherzustellen, dass die Appliance möglichst denselben, jedoch keinen höheren Firmware-Versionsstand als die Ziel Appliance des Providers hat
-> **Home** [220] **System** [220] **Firmware version** [220]
- b) Falls ausschließlich die [default] GINA-Domain eingesetzt wurde, Erzeugen einer neuen GINA-Domain, deren Namen möglichst bereits den Namenskonventionen des MSPs entspricht. Beim Erzeugen muss die [default] GINA-Domain als Master template gewählt werden.
Andernfalls kann mit Punkt c) fortgefahren werden
-> **GINA Domains** [416] **Domains** [416] **Create new GINA domain**



Achtung:

Damit bereits versendete GINA-Nachrichten weiterhin gelesen werden können, muss die bislang verwendete URL später auf die GINA-Domain MSP-Appliance zeigen. Es empfiehlt sich das Verwenden der Option **Use virtual hosting** [423] (**Change GINA settings** for [423] **Secure GINA host** [423] **Virtual hosting** [423]).

- c) Übernehmen der neu erzeugten GINA-Domain für die verwalteten Domänen
-> **Mail System** [247] **Managed domains** [247] die zu bearbeitende verwaltete Domäne anklicken und im Folgemenü unter **Settings** [266] unter **GINA domain** die neu erstellte GINA auswählen. Der Vorgang muss für jede verwaltete Domäne wiederholt werden.
- d) Aktivieren der Mandantenfähigkeit auf der „on premises Appliance“ (dieses Feature schaltet der Support (support@seppmail.de) auf Anfrage für die entsprechende Appliance frei)
-> **Customers** [494] **Multiple Customers** [494] **Enable**
- e) Einrichten eines Mandanten auf der Maschine, wobei die Namensgebung bereits den Konventionen des MSPs entsprechen sollte. Die hier eingetragene Customer Admin E-Mail wird später täglich automatisiert das Mandanten Backup empfangen.
-> **Customers** [494] **Multiple Customers** [494] **Create new customer...**
- f) Öffnen der Eigenschaften für den neu angelegten Mandanten
-> **Customers** [494] **Multiple Customers** [494], Auswahl des zuvor erzeugten Mandanten, **Edit**
- g) Zuordnen des/r Mandanten Administrator(en). Diese können später selbstständig die Log-Einträge ihrer zugeordneten E-Mail Domänen sehen, ihre GINA-Einstellungen vornehmen und ihre GINA Accounts verwalten.
-> **Customer Administrators** [496], Auswahl des/r Administratoren, **Assign**
- h) Zuordnen aller auf der Appliance verwalteten Domänen
-> **Assigned managed domains** [497], Auswahl der Domäne(n), **Add**
- i) Zuordnen aller auf der Appliance vorhandenen GINA Accounts
-> **Assigned GINA accounts** [498] **Manage accounts** im Folgemenü **Assign other GINA accounts** [500] **Assign** für jeden in der Sektion befindlichen GINA Accounts
-> nach Abschluss dieser Aktion zurück in das übergeordnete Menü via **Back**

j) Vergeben des Mandanten Backup Passwortes
-> **Backup/Restore** ^[498], **Backup** **Change password**

k) Download des Backups
-> **Backup/Restore** ^[498], **Backup** **Download**

auf der „MSP Appliance“

l) Erstellen eines neuen Mandanten

-> **Customers** ^[494] **Multiple Customers** ^[494] **Create new customer...**

m) Im darauf hin erscheinenden Sub-Menü für das Erstellen eines neuen Mandanten (**Create new customer** ^[496]) ist das zuvor auf der „on premises Appliance“ erstellte Backup zu importieren

-> **Import backup** ^[498] **Import backup file**

n) Der DNS Eintrag für den FQDN, welcher im **Hostname** ^[423] der durch den Import angelegten **GINA Domains** ^[416] eingetragen ist, muss dahingehend geändert werden, dass die IP Adresse der SEPPmail Appliance des MSPs aufgelöst wird.

In der durch den Import angelegten **GINA Domain** ^[416] ist im Sub-Menü **Change GINA settings for** ^[423] unter **Secure GINA host** ^[423] im Abschnitt **Virtual hosting** ^[423] die Option **Use virtual hosting** ^[423] zu aktivieren und das passende Schlüsselpaar (PKCS#12) zu dem im Abschnitt **SSL certificate** ^[423] mittels **Edit** zu importieren.

o) Abschließend ist im DNS auch der MX Eintrag dahingehend zu ändern, dass dieser auf die Mailserver des MSPs zeigt. Hierbei sind gegebenenfalls auch erforderliche TXT-Einträge für DKIM, SPF und so weiter zu beachten.

9.81 Konfig: Re-Inject mails to sending mailserver

Ausgangssituation:

E-Mails sollen nach dem Verarbeiten durch die SEPPmail Appliance an dieselbe IP Adresse zurückgegeben werden, von welcher sie an die SEPPmail Appliance gesendet wurden.

Grund:

In einer Infrastruktur, in welcher die SEPPmail Appliance parallel zu einem vorgelagerten Relay-Cluster steht (siehe auch **Parallel zur Schutzkomponente** ^[83]), soll gewährleistet sein, dass E-mails an dieselbe Maschine aus diesem Cluster zurückgegeben wird, von welchem sie an die SEPPmail Appliance übergeben wurde. Dadurch kann zum Beispiel in einer Fehlersituation das Nachverfolgen einer E-Mail erleichtert werden.

Lösung:

Bis zur SEPPmail Appliance Version 11.1.11 stand hierfür die Option **Re-inject mails to sending mailserver** zur Verfügung. Diese wurde mit der Version 11.1.11 durch die neue Option **Use custom delivery method** ^[312] abgelöst. Durch den Eintrag „loop“ wird mit dieser Option dasselbe Verhalten erzielt wie vormals durch **Re-inject mails to sending mailserver**.

Hinweis:



Forwarding Server ^[266] und **Outgoing Server** ^[250] werden bei aktivierter Funktion ignoriert beziehungsweise als Fallback Einstellung verwendet.



Achtung:

Durch das Aktivieren dieser Option kann unter Umständen eine E-Mail Schleife (Loop) erzeugt werden, wenn das einliefernde E-Mail System diese Funktion nicht unterstützt oder falsch konfiguriert wurde.



Hinweis zum Update-Verhalten auf die Version 11.1.11

Die Einstellung aus **Re-inject mails to sending mailserver** wird beim Update in die neue Option **Use custom delivery method** ^[312] automatisch übernommen (Eintrag „loop“).

9.82 LFT: Schwellwerte Ungenauigkeiten

Ausgangssituation:

Large File Transfer (LFT)  ist auf der Appliance aktiviert und entsprechende Schwellwerte für das senden als LFT-Nachrichten wurden definiert.

Frage:

Weshalb kann das Auslösen von LFT, trotz der definierten Schwellwerte nicht exakt bestimmt werden?

Antwort:

Das Über-, beziehungsweise Unterschreiten des LFT-Schwellwertes ist von der jeweiligen Kodierung der eingehenden E-Mail abhängig. Durch ein eventuelles Umkodieren einer E-Mail - bereits vor oder auch auf der SEPPmail Appliance - wird auch die Größe der E-Mail beeinflusst. Im Falle des Umkodierens auf Base64 würde eine E-Mail beispielsweise auf 4/3 der ursprünglichen Größe anwachsen.

9.83 LFT: Datenablage im Cluster

Ausgangssituation:

Ein SEPPmail Appliance **Cluster**³⁸³ wird betrieben, gegebenenfalls auch mit **Frontend/Backend**¹⁸⁰ Trennung. Eine **LFT-Lizenz**²²¹ ist für alle Cluster-Partner vorhanden.

Aufgabestellung:

Large File Transfer (LFT)¹⁰⁷ soll eingerichtet werden.

Vorgehen:

Jedem Cluster-Partner - auch Frontend Systemen - ist jeweils eine Festplatte mit identischer Größe hinzuzufügen. Anschließend sind die Maschinen nacheinander neu zu starten. Beim Neustart wird die hinzugefügte Festplatte erkannt und als LFT-Partition eingebunden. Nun kann die **Large File Transfer**⁴³⁹-Konfiguration an einem der Cluster-Partner (Backend) vorgenommen werden.



Hinweis:

LFT-Daten werden auf alle Cluster-Partner (auch auf Frontend Systeme!) synchronisiert. Liegen zwischen den Cluster-Partnern WAN-Strecken, so ist dies beim Dimensionieren dieser Strecken zu beachten.

9.84 LFT: Download von LFT-Nachrichten in einem E-Mail Format

Ausgangssituation:

Ein Kommunikationspartner hat eine LFT Nachricht erhalten. In den Einstellungen der zugehörigen **GINA Domain**^[416] ist das Herunterladen in einem E-Mail Format (MSG siehe **Allow messages to be downloaded as outlook message files**^[435], beziehungsweise EML siehe **Allow messages to be downloaded as MIME files**^[436]) zugelassen.

Frage:

Weshalb enthält die heruntergeladene Nachricht nur den Nachrichtentext, nicht jedoch die Anhänge, wie das bei einer „normalen“ GINA-Nachricht der Fall ist?

Antwort: Dies geht aus technischen Gründen nicht. Je nach Größe einer LFT-Nachricht, könnte diese beim E-Mail Client zum Absturz führen.

9.85 LFT: Größenbeschränkungen für LFT-Nachrichten

Ausgangssituation:

Auf der SEPPmail Appliance ist **Large File Transfer (LFT)** ^[128] aktiv.

Frage:

Wie Groß darf, beziehungsweise kann eine LFT-Nachricht maximal sein?

Antwort:

Limitierungen können generell kundenindividuell pro **GINA Domain** ^[416] unter **Change GINA Settings for** ^[423] **Large File Transfer** ^[439] vorgenommen werden.

Jedoch ergeben sich auch systembedingte Einschränkungen. In der Hauptsache ist dies die Größe der bereit gestellten LFT-Partition (siehe auch **LFT store** ^[223]).

Werden LFT-Mails über den „normalen“ E-Mail Strom, also vom Groupware Server direkt per SMTP eingeliefert, so entsteht aus den SMTP Partitionsgrößen eine systemabhängige Beschränkung. Die genaue Größe dieser Beschränkung kann dem Kommentar „(Note: cannot exceed xxxxx kB)“ aus **Max message size** ^[252] entnommen werden.

Nähere Informationen für das generelle Dimensionieren der SEPPmail Appliance sind dem Kapitel **Sizing** ^[78] zu entnehmen.

9.86 LFT: Mindestgröße für eine LFT-Disk/Partition

Ausgangssituation:

Für die SEPPmail Appliance wurden **Large File Transfer (LFT)** ^[128] Lizenzen erworben. Diese sind unter **Home** ^[220] **License** ^[220] **Large File Transfer (LFT) licenses** ^[221] bereits mit der Meldung *Note: You have LFT licenses, however your device has no disk to store Files. Please add an USB (or virtual) disk.* zu sehen.

Frage:

Gibt es eine Mindestgröße für eine LFT-Partition?

Antwort:

Ja. Diese ist dem Punkt **Large File Transfer (LFT) licenses** ^[221], beziehungsweise der Tabelle unter **Sizing** ^[78] zu entnehmen.

9.87 LFT: Unerwarteter LFT-Versand

Ausgangssituation:

LFT ist auf der SEPPmail Appliance aktiv und konfiguriert. Dabei wurde der gewünschte Schwellwert, ab welchem LFT verwendet werden soll (siehe **Size above which outgoing messages are treated as large files**⁴⁴⁰) gesetzt.

Frage:

Weshalb werden E-Mails als LFT-Nachrichten behandelt, obwohl deren Größe den eingestellten Schwellwert nicht überschreitet?

Antwort:

- a) LFT wurde manuell getriggert (siehe **Always use large file processing for mails with the following text in subject**³⁰³).
- b) Aufgrund der Base64 Codierung von Anhängen können E-Mails auf 4/3 der ursprünglichen Grösse anwachsen. Hierdurch wird der Schwellwert überschritten.

9.88 LFT: Verhalten bei Ablauf der LFT-Nachricht

Ausgangssituation:

LFT ist auf der SEPPmail Appliance aktiv und konfiguriert. Die Ablauffrist für LFT (siehe **Retention policy** ⁴⁴³) wurde gesetzt.

Frage 1:

Was passiert, wenn der Empfänger einer LFT-Nachricht diese nicht innerhalb der im Betreff der Benachrichtigungs-E-Mail angezeigten Frist öffnet?

Antwort:

Der Absender erhält 24 Stunden vor Ablauf der Frist eine Benachrichtigung, dass die LFT-Nachricht noch nicht geöffnet wurde.

Frage 2:

Was passiert, wenn der Empfänger einer LFT-Nachricht den darin befindlichen HTML Anhang nach dem im Betreff der Benachrichtigungs-E-Mail angezeigten Datum öffnet?

Antwort:

Der Empfänger erhält nach dem Öffnen der HTML Datei aus der Benachrichtigungs-E-Mail eine Fehlermeldung, dass die Nachricht abgelaufen ist.

9.89 LFT: Versand einer „normalen“ E-Mail anstatt einer LFT-Nachricht

Ausgangssituation:

LFT ist auf der SEPPmail Appliance aktiv und konfiguriert. Dabei wurde der gewünschte Schwellwert, ab welchem LFT verwendet werden soll (siehe **Size above which outgoing messages are treated as large files**^[440]) gesetzt.

Frage:

Weshalb werden E-Mails als „normale“ E-Mail versendet, obwohl deren Größe den eingestellten Schwellwert überschreitet, beziehungsweise LFT getriggert wurde (siehe)

Antwort:

- a) LFT wurde manuell unterdrückt (siehe **Do not use large file processing for mails with the following text in subject**^[303]).
- b) Das vorhandene LFT-Lizenz-Kontingent (siehe **Large File Transfer (LFT) Licenses**^[221] beziehungsweise **Large File Transfer (LFT)**^[128]) wurde überschritten.
- c) Nach dem Einrichten von LFT wurde das Ruleset nicht neu generiert (siehe **SMTP ruleset**^[286]).

9.90 LFT: Versand mit Passwort trotz Einstellung „Plain“

Ausgangssituation:

Large File Transfer (LFT) [107] ist auf der Appliance aktiviert und entsprechende Schwellwerte für das Senden als LFT-Nachrichten wurden definiert. Das Versenden von LFT-Nachrichten von internen Benutzern (also aus **Managed domains** [247]) erfolgt direkt über die GINA-Oberfläche. Für den LFT-Empfang wurde die Einstellung **Plain** [442] gewählt.

Frage:

Weshalb wird ein interner Empfänger (also ebenfalls aus einer **Managed domain** [247]) einer so generierten Nachricht zum Lesen, trotz der Einstellung **Plain** [442] sein Passwort eingeben?

Antwort:

Erreicht die über die GINA-Oberfläche erzeugte Nachricht den Schwellwert, wie er unter **Size (in KiB) above which incoming messages are treated as large files** [443] konfiguriert wurde, nicht, so an den externen Empfänger „normale“ SMTP-Mail versendet, auf wenn die Nachricht über die GINA-Oberfläche erzeugt wurde.

An interne Empfänger werden über GINA-Oberfläche erzeugte E-Mails generell verschlüsselt, da hier von **SEPPmail IME unter ausschließlichem Verwenden der GINA-Technologie** [118] ausgegangen wird.

Lösung:

- Der Absender ergänzt den Betreff der Nachricht mit dem unter Always use large file processing for mails with the following text in subject [303] konfiguriertem Schlüsselwort.
- Soll nur das Verwenden von GINA für die internen Empfänger unterdrückt werden, so kann dies in den **Custom commands** [308] unter **Custom macros and commands for all emails before processing** [309] zum Beispiel mit folgendem Code unterbunden werden:

Zeile	Code
01	# Begin: Custom macros and commands for all e-mails BEFORE processing
02	log('Begin: Custom macros and commands for all e-mails BEFORE processing');
03	# Begin: Disable encryption for internal e-mails from GINA and force LFT
04	log('Begin: Disable encryption for internal e-mails from GINA and force LFT');
05	if (internal()) {
06	if (compare('X-ESWmail-InternalEncrypt','match','Yes')) {
07	rmheader('X-ESWmail-InternalEncrypt');
08	}
09	}
13	log('End: Disable encryption for internal e-mails from GINA and force LFT');
14	# End: Disable encryption for internal e-mails from GINA and force LFT
15	log('End: Custom macros and commands for all e-mails BEFORE processing');
16	# End: Custom macros and commands for all e-mails BEFORE processing

Code

Wie häufig werden die Lizenzdaten der SEPPmail Appliance mit dem SEPPmail Lizenz-Server abgeglichen und ist ein manueller Abgleich möglich?

Antwort:

Die Lizenzdaten werden täglich um Mitternacht sowie bei jedem Reboot der SEPPmail Appliance automatisch abgeglichen.

Weiterhin werden die Daten bei Klicken einer der Schaltflächen **View release notes**, **Perform update (reboot automatically)** oder **Prefetch update (reboot manually)**, aus der Sektion **Update** des Menüs **Administration** adhoc abgeglichen.

Ein manueller Abgleich kann somit durch Klicken der Schaltfläche **View release notes** forciert werden.

9.92 Logs: Mehrere Einträge zu einer E-Mail

Ausgangssituation:

Zu einer E-Mail (identische Message ID) sind im **Log** ^[388] mehrfache Einträge zu finden.

Ursache:

Je nach Farbe der Empfänger-Adresse(n) im **Log** ^[388], kann dies unterschiedliche Ursachen haben:

1. Die Empfängeradresse ist bei allen Mehrfacheinträgen grün
Der abgebende Server erhält keine Empfangsbestätigung (250 ok) von der SEPPmail Appliance.
Dies wird gelegentlich durch Firewalls verursacht, welche – trotz der üblichen Keep Alives – nach einer zu kurzen Zeit die Verbindung zwischen abgebenden Server und SEPPmail Appliance unterbrechen.

Individuelle Abhilfe:

Firewall-Einstellungen prüfen/ändern

2. Die Empfängeradresse ist bei allen Mehrfacheinträgen schwarz, gegebenenfalls nur beim letzten Eintrag grün.
Das Verarbeiten einer E-Mail konnte SEPPmail Appliance-seitig nicht abgeschlossen werden oder wurde unterbrochen.
Ursächlich kann
 - a. ein zu lange dauernder Virensan, meist verursacht durch sehr große ZIP-Dateien mit mehreren Archivebenen,
 - b. ein Unterbrechen der E-Mail Verarbeitung aufgrund eines Dienste-Neustarts, wie er beispielsweise im Falle des Virensanners bei einem Engine-Update oder im Falle des Postfix durch das Generieren eines neuen Rulesets erfolgt,
 - c. das Warten auf den Zertifikatsbezug via **MPKI** ^[339]

sein.

Somit wird dem abgebenden Server entweder keine erfolgreiche Annahme der E-Mail (250 ok) durch die SEPPmail Appliance innerhalb einer annehmbaren Zeit signalisiert oder die Annahme der E-Mail temporär verweigert (4xx). In beiden Fällen wird der abgebende Server, nach einer dort eingestellten Wiederholungszeit, die E-Mail erneut senden. Hierdurch wird ein neuer Log-Eintrag zur selben E-Mail (Message-ID) generiert.

Individuelle Abhilfe:

Gegebenenfalls Virensan innerhalb von Archivdateien abschalten (siehe **Mail Processing** ^[286] **Ruleset generator** ^[287] **Protection pack** ^[303] „Block...“ „Search inside unencrypted zip archives“).

9.93 Mandanten: Signieren von E-Mails zwischen Mandanten

Ausgangssituation:

In einem mandantenfähigen System sollen E-Mails von **Managed domains** [247] an **Managed domains** [247] als signiert [signed ok] markiert werden oder tatsächlich signiert werden.

Lösung:

Zunächst ist die Option **Custom commands for incoming e-mails BEFORE decryption** [308] zu aktivieren und je nach gewünschten Verhalten (siehe **Mail Processing** [286] **Ruleset generator** [287] **Signing** [298]) der Variante entsprechende Code in das darunterliegende Eingabefeld einzugeben.

Beispiele

Bei allen Varianten (siehe folgende Punkte "Variante 1-4") muss zwingend sichergestellt sein, dass E-Mails auch tatsächlich vom korrekten Absender kommen. Hierzu eignen sich gegebenenfalls zusätzlich vorgelagerte Schutzkomponenten.

In der SEPPmail Appliance Konfiguration muss in jedem Fall pro **Managed domain** [247] die entsprechende Einschränkung für das Relaying unter **Settings** [266] **Allowed sending servers for this domain (leave empty to allow all relaying networks)**. **Note: Entering an address here does not automatically allow relaying**, beziehungsweise gegebenenfalls auch der **Header check** eingerichtet werden.

Weiterhin sollte unter **Mail Processing** [286] **Ruleset generator** [287] **Protection pack** [303] die Option „Reject incoming mails with spoofed sender domain.“ eingerichtet werden. Bei Verwenden der zuletzt genannten Option sind im Menü **Mail System** [247] die **Relaying** [254] IPs zusätzlich unter **Manual blacklisting / whitelisting** [258] einzutragen.

Bei Office 365 hosted **Managed domains** [247] kommt an dieser Stelle die Einstellung **Exchange Online Integration** [266] bezüglich des Überprüfens der Absender zum Tragen, da aufgrund des global zu aktivierenden **Exchange Online Relaying** [255] das Unterscheiden der sendenden IPs pro Mandant nicht möglich ist. Die genannten, SEPPmail Appliance internen Sicherheitsmechanismen werden im Code der unterschiedlichen Varianten berücksichtigt.

Folgende Befehle werden in den Beispielen der Varianten 1-4 verwendet:

Verwendete

Befehle

```
authenticated() [537]
bounce() [548]
compare() [525]
compareattr() [527]
createaccount() [539]
createkeys() [540]
drop() [552]
flag() [553]
from_managed_domain() [537]
has_smime_key() [592]
log() [534]
notify() [520]
rmheader() [562]
sign_smime() [593]
```

Funktionen

```
@TAGSIGNED@ [637]
```

9.93.1 Variante 1

Erzeugt bei intern gerouteten E-Mails in etwa das Verhalten der Option „Sign all outgoing mails if S/MIME certificate available“ (**Outgoing** ³⁰⁰) in Verbindung mit „Remove signature if S/MIME signature check succeeds“ (**Incoming** ²⁹⁸).

Zeile	Code
01	# Begin: Custom commands for incoming e-mails BEFORE decryption
02	log(1,'Begin: Custom commands for incoming e-mails BEFORE decryption');
03	# Begin: Tag all internally routed e-mails as SIGNED
04	log(1,'Begin: Tag all internally routed e-mails as SIGNED');
05	if (from managed domain()) {
06	log(1,'E-mail is from managed domain...');
07	if (!compareattr('connect from', 'equal', '127.0.0.1')) {
08	log(1,'...not form localhost...');
09	if (check sender(false, false, true)) {
10	log(1,'...but is not allowed to relay, dropping');
11	drop('554' '5.7.1 Relay access denied');
12	} else {
13	log(1,'...and is allowed to relay, tag as SIGNED');
14	@TAGSIGNED@
15	}
16	} else {
17	log(1,'...but generated on localhost, going on in standard ruleset');
18	}
19	}
20	log(1,'End: Tag all internally routed e-mails as SIGNED');
21	# End: Tag all internally routed e-mails as SIGNED
22	log(1,'End: Custom commands for incoming e-mails BEFORE decryption');
23	# End: Custom commands for incoming e-mails BEFORE decryption

[Code](#)

9.93.2 Variante 2

Erzeugt bei intern gerouteten E-Mails in etwa das Verhalten der Option „S/MIME sign outgoing mails with the following text in subject:“ (**Outgoing** ³⁰⁰) in Verbindung mit „Remove signature if S/MIME signature check succeeds“ (**Incoming** ²⁹⁸).

Zeile	Code
01	# Begin: Custom commands for incoming e-mails BEFORE decryption
02	log(1,'Begin: Custom commands for incoming e-mails BEFORE decryption');
03	# Begin: Tag internally routed e-mails, marked to be SIGNED
04	log(1,'Begin: Tag internally routed e-mails, marked to be SIGNED');
05	if (from managed domain()) {
06	log(1,'E-mail is from managed domain...');
07	if (!compareattr('connect from', 'equal', '127.0.0.1')) {
08	log(1,'...not form localhost...');
09	if (check sender(false, false, true)) {
10	log(1,'...but is not allowed to relay, dropping');
11	drop('554' '5.7.1 Relay access denied');
12	} else {
13	log(1,'...and is allowed to relay, tag as SIGNED if requested');
14	\$custom tag signed;
15	}
16	} else {
17	log(1,'...but generated on localhost, going on in standard ruleset');
18	}
19	}
20	log(1,'End: Tag internally routed e-mails, marked to be SIGNED');
21	# End: Tag all internally routed e-mails as SIGNED
22	log(1,'End: Custom commands for incoming e-mails BEFORE decryption');
23	# End: Custom commands for incoming e-mails BEFORE decryption

Code

Das in oben genannten Code verwendete Macro `$custom_sign` für das Signieren, muss bei dieser Variante zusätzlich unter **Custom macros and commands for all e-mails BEFORE processing** ³⁰⁰ wie folgt definiert werden:

Zeile	Code
01	# Begin: Custom macros and commands for all e-mails BEFORE processing
02	log(1,'Begin: Custom macros and commands for all e-mails BEFORE processing');
03	custom tag signed = {
04	if (compare('x-smsign','equal','yes')) {
05	log(1,'Signing requested by Add-In, tag as SIGNED');
06	rmheader('x-smenc');
07	tagsubject('[signed OK]');
08	}
09	if (compare('subject','substitute','@SIGNTEXT@')) {
10	log(1,'Signing requested by subject-tag, tag as SIGNED');
11	tagsubject('[signed OK]');

Zeile	Code
12	}
13	};
14	log(1,'End: Custom macros and commands for all e-mails BEFORE processing');
15	# End: Custom macros and commands for all e-mails BEFORE processing

Code

9.93.3 Variante 3

Erzeugt bei intern gerouteten E-Mails in etwa das Verhalten der Option „Sign all outgoing mails if S/MIME certificate available“ (**Outgoing**³⁰⁰).

Mit dieser Variante werden E-Mails tatsächlich signiert und nicht nur markiert.

Zeile	Code
01	# Begin: Custom commands for incoming e-mails BEFORE decryption
02	log(1,'Begin: Custom commands for incoming e-mails BEFORE decryption');
03	# Begin: Sign all internally routed e-mails, if keys are available
04	log(1,'Begin: Sign all internally routed e-mails, if keys are available');
05	if (from managed domain()) {
06	log(1,'E-mail is from managed domain...');
07	if (!compareattr('connect from', 'equal', '127.0.0.1')) {
08	log(1,'...not form localhost...');
09	if (check sender(false, false, true)) {
10	log(1,'...but is not allowed to relay, dropping');
11	drop('554','5.7.1 Relay access denied');
12	} else {
13	log(1,'...and is allowed to relay, signing e-mail, if keys are available');
14	\$custom sign;
15	}
16	} else {
17	log(1,'...but generated on localhost, going on in standard ruleset');
18	}
19	}
20	log(1,'End: Sign all internally routed e-mails, if keys are available');
21	# End: Sign all internally routed e-mails, if keys are available
22	log(1,'End: Custom commands for incoming e-mails BEFORE decryption');
23	# End: Custom commands for incoming e-mails BEFORE decryption

Code

Das in oben genannten Code verwendete Macro `$custom_sign` für das Signieren, muss bei dieser Variante zusätzlich unter **Custom macros and commands for all e-mails BEFORE processing**³⁰¹ wie folgt definiert werden:

Zeile	Code
01	# Begin: Custom macros and commands for all e-mails BEFORE processing
02	log(1,'Begin: Custom macros and commands for all e-mails BEFORE processing');
03	custom sign = {
04	if (authenticated()) {
05	if (has smime key()) {
06	if (sign smime()) {
07	tagsubject('[signed OK]');
08	log(1,'signing successful');
09	} else {
10	log(1,'signing failed, bouncing e-mail');
11	bounce('noseckey');
12	}

Zeile	Code
13	}
14	}
15	};
16	log(1, 'End: Custom macros and commands for all e-mails BEFORE processing');
17	# End: Custom macros and commands for all e-mails BEFORE processing

Code

Variation:

Um Kalendereinträge und RTF formatierte E-Mails vom automatischen signieren auszunehmen (siehe gegebenenfalls auch [Kalenderanfragen kommen zerstört beim Empfänger an](#) ^[670]), kann das Makro \$custom_sign wie folgt erweitert werden:

Zeile	Code
01	# Begin: Custom macros and commands for all e-mails BEFORE processing
02	log(1, 'Begin: Custom macros and commands for all e-mails BEFORE processing');
03	custom sign = {
04	if (iscalendar()) {
05	log(1, 'suppress automatic signing, because of calendar or incompatible mail format (RTF)');
06	} else if (compare('subject', 'substitute', '[nosign]')) {
07	log(1, 'signing suppressed by trigger');
08	} else {
09	if (authenticated()) {
10	if (has smime key()) {
11	if (sign smime()) {
12	tagsubject('[signed OK]');
13	log(1, 'signing successful');
14	} else {
15	log(1, 'signing failed, bouncing e-mail');
16	bounce('noseckey');
17	}
18	}
19	}
20	}
21	};
22	log(1, 'End: Custom macros and commands for all e-mails BEFORE processing');
23	# End: Custom macros and commands for all e-mails BEFORE processing

Code

9.93.4 Variante 4

Erzeugt bei intern gerouteten E-Mails in etwa das Verhalten der Option „S/MIME sign outgoing mails with the following text in subject:“ (**Outgoing**³⁰⁰).

Mit dieser Variante werden E-Mails tatsächlich signiert und nicht nur markiert.

Zeile	Code
01	# Begin: Custom commands for incoming e-mails BEFORE decryption
02	log(1,'Begin: Custom commands for incoming e-mails BEFORE decryption');
03	# Begin: Sign internally routed e-mails, marked to be SIGNED
04	log(1,'Begin: Sign internally routed e-mails, marked to be SIGNED');
05	if (from managed domain()) {
06	log(1,'E-mail is from managed domain...');
07	if (!compareattr('connect from', 'equal', '127.0.0.1')) {
08	log(1,'...not form localhost...');
09	if (check sender(false, false, true)) {
10	log(1,'...but is not allowed to relay, dropping');
11	drop('554' '5.7.1 Relay access denied');
12	} else {
13	log(1,'...and is allowed to relay, signing e-mail, if requested');
14	\$custom sign;
15	}
16	} else {
17	log(1,'...but generated on localhost, going on in standard ruleset');
18	}
19	}
20	log(1,'End: Sign internally routed e-mails, marked to be SIGNED');
21	# End: Sign internally routed e-mails, marked to be SIGNED
22	log(1,'End: Custom commands for incoming e-mails BEFORE decryption');
23	# End: Custom commands for incoming e-mails BEFORE decryption

Code

Das in oben genannten Code verwendete Macro `$custom_sign` für das Signieren, muss bei dieser Variante zusätzlich unter **Custom macros and commands for all e-mails BEFORE processing**³⁰⁹ wie folgt definiert werden:

Zeile	Code
01	# Begin: Custom macros and commands for all e-mails BEFORE processing
02	log(1,'Begin: Custom macros and commands for all e-mails BEFORE processing');
03	custom sign = {
04	if (compare('x-smsign','equal','yes')) {
05	log(1,'Signing requested by Add-In, tag as SIGNED');
06	rmheader('x-smenc');
07	flag('sign',1);
08	}
09	if (compare('subject','substitute','@SIGNTEXT@')) {
10	log(1,'Signing requested by subject-tag, tag as SIGNED');
11	flag('sign',1);

Zeile	Code
12	}
13	if (flag('sign',0) {
14	if (!authenticated()) {
15	createaccount();
16	createkeys('4');
17	}
18	if (authenticated()) {
19	if (has smime key()) {
20	log(1,'S/MIME key available, trying to sign');
21	if (sign smime()) {
22	log(1,'signing successful');
23	tagsubject('[signed OK]');
24	} else {
25	log(1,'signing failed, bouncing e-mail');
26	bounce('noseckey');
27	}
28	} else {
29	log(1,'no S/MIME key available, bouncing');
30	bounce('noseckey');
31	}
32	} else {
33	log(1,'user not authenticated, bouncing');
34	bounce('noauth');
35	}
36	}
37	};
38	log(1,'End: Custom macros and commands for all e-mails BEFORE processing');
39	# End: Custom macros and commands for all e-mails BEFORE processing

[Code](#)

9.94 Mandanten: GINA zwischen Mandanten erzwingen

Ausgangssituation:

Die SEPPmail Appliance wird als mandantenfähiges System (siehe [Customers](#)^[494]) betrieben. Anforderung der Mandanten ist, alle E-Mails mit einem Verschlüsselungskennzeichen zwischen den Mandanten mittels GINA-Technologie zu verschlüsseln.

Konfigurationsvorschlag

- Navigieren zu [Mail Processing](#)^[286] [Ruleset generator](#)^[287] [Custom Commands](#)^[308] [Custom commands for outgoing e-mails BEFORE decryption](#)^[308]
- Einfügen des folgenden Codes in das Eingabefeld:

Zeile	Code
01	# Begin: Custom commands for outgoing e-mails BEFORE encryption
02	log(1,'Begin: Custom commands for outgoing e-mails BEFORE encryption');
03	if (from managed domain()) {
04	if (compare('x-smenc','equal','yes')) {
05	log(1,'Encryption requested by Add-In, set x-header for GINA encryption');
06	setheader('x-smwebmail','yes');
07	rmheader('x-smenc');
08	}
09	if (compare('subject','substitute','@TRIGGERTEXT@')) {
10	log(1,'Encryption requested by tag @TRIGGERTEXT@, set x-header for GINA encryption');
11	setheader('x-smwebmail','yes');
12	}
13	if (compare('sensitivity','equal','companyconfidential')) {
14	log(1,'Encryption requested by sensitivity flag, set x-header for GINA encryption');
15	setheader('x-smwebmail','yes');
16	rmheader('sensitivity');
17	}
18	if (compare('subject','substitute','\[priv\]')) {
19	log(1,'GINA encryption requested by tag [priv], set x-header for GINA encryption');
20	setheader('x-smwebmail','yes');
21	}
22	if (compare('x-smwebmail','equal','yes')) {
23	log(1,'Encrypting with GINA technology');
24	rmheader('x-smwebmail');
25	compare('subject','substitute','\[.*?\].*?');
26	createaccount();
27	createkeys('@CREATEGPGKEYS@');
28	\$createwebuser;
29	if (encrypt webmail()) {
30	@TAGSIGNED@
31	} else {
32	log(1,'webmail encryption failed');
33	drop ('550','Mail not accepted');

Zeile	Code
34	}
35	}
36	}
37	log(1, 'End: Custom commands for outgoing e-mails BEFORE encryption');
38	# End: Custom commands for outgoing e-mails BEFORE encryption

Code

Beschreibung

Zunächst wird hier geprüft, ob die E-Mail von einer bekannten E-Mail-Domäne (siehe **Mail System** ^[247] **Managed domains** ^[247]) stammt (**Zeile 03**). In den nächsten Schritten wird jeweils geprüft, ob vom Absender ein anderes Verschlüsselungsmerkmal als der X-Header für die GINA-Verschlüsselung gesetzt wurde (**Zeile 04, 09, 13, 18**). Sollte ein anderes Verschlüsselungsmerkmal vorhanden sein, so wird dieses jeweils in den X-Header für das Triggern der GINA-Verschlüsselung umgesetzt, protokolliert und der Ursprungstrigger entfernt (**Zeile 04-07, 9-11, 13-16, 18-20**).

Abschließend wird nun auf den X-Header für die GINA-Verschlüsselung (x-smwebmail) geprüft (**Zeile 22**). Ist dieser vorhanden, so wird dies protokolliert (**Zeile 23**), der X-Header entfernt (**Zeile 24**), alle eventuell noch vorhandenen **Betreffzeilen Schlüsselwörter** ^[164] (im Beispiel müssten diese jeweils in eckigen Klammern [] stehen) entfernt (**Zeile 25**), ein Benutzer angelegt, sofern nicht bereits vorhanden (**Zeile 26, 27**), ein GINA-Account angelegt, sofern nicht bereits vorhanden (**Zeile 28**), und die E-Mail GINA verschlüsselt (**Zeile 29**). War das Verschlüsseln erfolgreich, so wird (optional) die E-Mail als erfolgreich signiert gekennzeichnet (**Zeile 30**). Anderfalls wird das Fehlschlagen der Verschlüsselung protokolliert (**Zeile 32**) und die Email verworfen (**Zeile 33**).

Variationen

Zurückweisen von E-Mails bei Fehlschlagen der GINA-Verschlüsselung anstatt diese zu verwerfen.
Hierfür ist folgende Zeile wie folgt zu ändern:

Zeile	Code
33	bounce('bounce noenc');

Verwendete

Befehle

```
bounce() [548]
compare() [525]
drop() [552]
encrypt_webmail() [595]
from_managed_domain() [537]
log() [534]
rmheader() [562]
setheader() [563]
```

Funktionen

```
$createanyuser [640]
$createwebuser [647]
@TAGSIGNED@ [637]
@TRIGGERTEXT@ [635]
```

9.95 Mandanten: Absichern der Verbindung zwischen SEPPmail Appliance und E-Mail Server

Ausgangssituation:

Die SEPPmail Appliance wird mandantenfähig betrieben. Dies impliziert, dass die Verbindungen zwischen der SEPPmail Appliance und den E-Mail Servern der Mandanten abgesichert werden, unabhängig davon wo sich diese physikalisch befinden (on premises, in der Cloud oder beim SEPPmail-Dienstleister).

Frage:

Wie sollten die Verbindungen abgesichert werden?

Antwort:

Für das Absichern der Strecke zwischen der SEPPmail Appliance und den E-Mail Servern der Mandanten (und umgekehrt) wird in der Regel TLS verwendet, idealerweise in der Ausprägung „fingerprint“ oder "secure", mindestens aber "verify".

Für das Konfigurieren von TLS hin zu den E-Mail Servern der Mandanten stehen in der SEPPmail Appliance hierfür in den Einstellungen der jeweiligen **Managed Domains** ^[247] (siehe **EDIT MANAGED DOMAIN** ^[266]) unter **TLS settings** ^[277] die entsprechenden Optionen bereit. Damit nur TLS gesicherte Verbindungen von der SEPPmail Appliance angenommen werden, sollte weiterhin die Option **Mail System** ^[247] **SMTP settings** ^[252] **Require TLS encryption** ^[253] aktiviert werden.

Das Absichern der Verbindung vom E-Mail Server hin zur SEPPmail Appliance muss auf dem jeweiligen E-Mail Server konfiguriert werden.

Unter Umständen ist in diesem Zusammenhang auch der Artikel **Admin: Mehrere SMTP-Authentifizierungen verwalten** ^[657] relevant.

Gegebenenfalls kann die Verbindung auch über einen VPN-Tunnel abgesichert werden. Dies muss dann allerdings über externe Komponenten realisiert werden. Die SEPPmail Appliance stellt nativ keine Möglichkeit für das Herstellen eines VPN-Tunnels bereit.

9.96 Mandanten: Umstellen auf Mandantenfähigkeit

Ausgangssituation:

Eine bestehende SEPPmail Appliance soll von single tenant auf multi tenant (mandantenfähig) umgestellt werden.

Frage:

Wie ist das korrekt vorgehen beim Umstellen auf Mandantenfähigkeit?

Antwort:

Zunächst sollte bei der Namensgebung der jeweils benötigten Konfigurationen darauf geachtet werden, dass jeweils ein Zusammenhang zum jeweiligen Mandanten (**Customer**^[494]) hergestellt werden kann.

Die Reihenfolge für das Einschalten der Mandantenfähigkeit sollte wie folgt aussehen:

1. Jeweils mindestens eine eigene **GINA-Domain**^[416] pro geplantem Mandant (**Customer**^[494]) anlegen (zum Beispiel **GINA name**^[416] **Mandant1**), sofern nicht bereits vorhanden (siehe auch **Achtung**^[495] aus **Notes**^[495])
2. Zuweisen der jeweiligen **GINA-Domain(s)**^[416] zur, beziehungsweise zu den **Managed Domain(s)**^[247] des zukünftigen Mandanten (zum Beispiel **GINA** Mandant1 zur **Managed Domain**^[247] Mandant1.tld).
3. Einschalten der Mandantenfähigkeit (siehe **Customers**^[494])
4. Einrichten eines neuen Mandanten (siehe **Create new customer**^[496])
 - a. Zuweisen eines Mandanten Admin (siehe **Customer administrators**^[496])
 - b. Zuweisen eines Lizenz-Kontingents (siehe **License limiter**^[497])
 - c. Zuweisen der jeweiligen **Managed Domain(s)**^[247] des Mandanten (siehe **Assigned managed domains**^[497])
 - d. Sofern bereits **GINA accounts**^[462] aus dem zuvorigem Betrieb vorhanden sind, müssen diese unter **Assigned GINA accounts**^[498] mittels **Manage accounts** zugewiesen werden (siehe auch **MANAGE ASSIGNED GINA ACCOUNTS**^[500])

Wird ein weiterer Mandant (zum Beispiel Mandant2) für (eine) bereits bestehende **Managed Domain(s)**^[247] (zum Beispiel mandant2.tld) eingerichtet, so erfolgt das Zuordnungsverfahren 1:1 zum Mandanten „Mandant1“.

9.97 Mandanten: Verschlüsseln von E-Mails zwischen Mandanten

Ausgangssituation:

Die SEPPmail Appliance wird mandantenfähig betrieben.

Frage:

Wie verhält sich die SEPPmail Appliance bei der E-Mail Kommunikation zwischen den Mandanten.

Antwort:

Auf mandantenfähigen Systemen ist das Standardverhalten bei der Kommunikation zwischen den Mandanten systembedingt anders, als bei der Kommunikation hin zu externen Kommunikationspartnern.

Wird zum Beispiel eine E-Mail vom Absender an einen anderen Mandanten auf der gleichen SEPPmail Appliance als zu verschlüsselnd markiert, so ergäbe es keinen Sinn diese zu verschlüsseln und anschließend sofort wieder zu entschlüsseln.

Nachdem bei mandantenfähigen Systemen die Sichere Kommunikation zwischen den jeweiligen E-Mail Servern der Mandanten und der gemeinsam genutzten SEPPmail Appliance Grundvoraussetzung ist (siehe auch **Mandanten: Absichern der Verbindung zwischen SEPPmail Appliance und E-Mail Server** ⁷⁷⁹), kommt dies quasi einer **Gateway-to-Gateway (Domänen) Verschlüsselung** ³¹ gleich. Somit sollten die E-Mails zwischen den Mandanten generell als „sicher“ markiert werden (siehe auch **Incoming e-mails** ²⁹²). **Add this text to message subject after decryption** ²⁹².

Dies kann über die Option **Consider internally routed mails as encrypted** ²⁹⁵ realisiert werden

9.98 Monitoring: Partitionen zum Teil bis zu 100% ausgelastet

Ausgangssituation:

Die SEPPmail Appliance wird durch ein Monitoring System (siehe gegebenenfalls [SNMP Daemon](#)^[24], beziehungsweise [NRPE Daemon](#)^[24]) überwacht. Dabei werden Warnungen über zum Teil bis zu 100% ausgelastete Partitionen ausgegeben.

Frage:

Weshalb sind auf der SEPPmail Appliance einzelne Partitionen derart ausgelastet?

Antwort:

Beim Überwachen von Partitions-Auslastungen ist zu beachten, dass nur die Partitionen berücksichtigt werden, welche auch unter [Home](#)^[22] [Disk statistics](#)^[23] aufgeführt sind. Alle anderen Partitionen (Firmware) sind read-only und bis zu 100% belegt. Ein Überwachen dieser Partitionen würde somit zu permanenten Meldungen führen.

9.99 MS Azure: Installation

Ausgangssituation:

Die SEPPmail Appliance soll in Microsoft Azure installiert werden.

Frage:

Ist die SEPPmail Appliance in Microsoft Azure lauffähig und wie wird sie dort installiert?

Antwort / Lösung:

Die SEPPmail Appliance kann über den Azure Marketplace bezogen werden.

Weiterführende Informationen sind unter <https://www.seppmail.de/produkte/seppmail365/> zu finden,

Wichtig!

Zum Beispiel bei Azure Pay-As-You-Go und CSP-caffee Lizenzen ist - anders als bei Enterprise Lizenzen - Port 25 per Standard gesperrt. Somit muss beim Verwenden von Pay-As-You-Go oder CSP-caffee Lizenzen das Freischalten des Ports zusätzlich über den Microsoft Support beantragt werden (siehe auch <https://www.seppmail.de/produkte/seppmail365/> **Wichtige Informationen zur SEPPmail/Azure-Installation**).

Ein Test der Port 25 Verbindung kann via Kommandozeile (siehe **Rudimentäre Systembefehle**^[189] "Port probe") ausgeführt werden.

Ein Test via Network Watcher ist an dieser Stelle nicht aussagekräftig, da dieser Test nicht aus dem gehosteten System (SEPPmail Appliance) direkt ausgeführt wird!

Weiterhin ist auf der genannten Seite ein Verweis auf das „Github Repository“, in welchem bei Bedarf ein Skript zur automatischen Konfiguration eine **Cluster**^[383] bereit steht.

9.100 MS Azure: Migrieren von on premises

Ausgangssituation:

Eine on premises Instanz der SEPPmail Appliance soll nach Microsoft Azure migriert werden.

Frage:

Wie ist die korrekte vorgehensweise für eine Migration nach MS Azure?

Antwort / Lösung:

Zunächst ist das Vorhaben beim Support (support@seppmail.de) anzuzeigen.

Der Support wird daraufhin zu den bestehenden on premises Lizenzen kostenfrei weitere Lizenzen für den Parallelbetrieb in MS Azure für den Migrationszeitraum ausstellen.

Nach dem Beenden der Migration werden die on premises Lizenzen deaktiviert.

Nun kann die erforderliche Anzahl von SEPPmail Appliances in MS Azure installiert werden. Hierzu sind die Artikel [MS Azure Installation](#)^[783] und [MS Azure Sizing](#)^[785] zwingend zu beachten.

Im nächsten Schritt ist ein [Cluster](#)^[383] der on premises SEPPmail Appliance(s) und der MS Azure SEPPmail Appliance(s) zu bilden (siehe auch [Add this device to existing cluster](#)^[383]).

Ist mit dem Migrieren der SEPPmail Appliance(s) von on premises zu MS Azure auch eine Migration von Exchange on premises hin zu Microsoft 365 verbunden, so ist vor dem Schwenk des MX records von on premises hin zu Microsoft 365 / Exchange Online

- o zunächst die [Faktoren für eine reibungslose Integration](#)^[790] aus [Anbinden von MS Office365 unter Beibehaltung von ATP / EOP](#)^[789] zu beachten.
- o der Punkt [Vorbereitung](#)^[795] ff. aus [Anbinden von MS Office365 unter Beibehaltung von ATP / EOP](#)^[789] abzuarbeiten.
- o der [Cluster](#)^[383] zwischen on premises SEPPmail Appliance Installationen und MS Azure SEPPmail Appliance Installationen zu trennen (siehe auch [Remove from cluster](#)^[383]).
- o auf den MS Azure SEPPmail Appliance Installationen der E-Mail Fluss gemäß [Mail System](#)^[797] ff. aus [Anbinden von MS Office365 unter Beibehaltung von ATP / EOP](#)^[789] anzupassen.
- o mit der [Exchange Online Konfiguration](#)^[802] aus [Anbinden von MS Office365 unter Beibehaltung von ATP / EOP](#)^[789] fortzufahren.

Andernfalls ist der [Cluster](#)^[383] zwischen on premises SEPPmail Appliance Installationen und MS Azure SEPPmail Appliance Installationen zu trennen (siehe auch [Remove from cluster](#)^[383]), bei Bedarf der E-Mail Fluss unter [Mail System](#)^[247] an die neuen gegebenheiten anzupassen.

Der DNS-Eintrag für den FQDN zur GINA-Oberfläche entsprechend anzupassen.

9.101 MS Azure: Sizing

Ausgangssituation:

Die SEPPmail Appliance soll in Microsoft Azure installiert werden.

Frage:

Welche virtuellen Ressourcen sind für die SEPPmail Appliance in Microsoft Azure bereit zu stellen?

Antwort / Lösung:

Als Maschinen-Größe wird mindestens „Standard B2s“ empfohlen.

Sollte beim Versuch eines Resizings in der Azure Oberfläche der gewünschte Maschinentyp nicht angezeigt werden oder nicht auswählbar sein, muss die Appliance unter Umständen für das Resizing heruntergefahren werden.

Initial sollten die virtuellen Ressourcen gemäß der Tabelle des Kapitels [Sizing](#) gewählt werden.

Zeigt die Datenanzeige für die CPU bei Null-Last bereits zehn oder mehr Prozent, so ist die Maschine zu klein gewählt.

Im laufenden Betrieb wird empfohlen, zyklisch den von Microsoft kostenfrei bereit gestellten Azure Advisor auszuführen. Dieser macht anhand der konkreten Auslastung Vorschläge zu den tatsächlich benötigten Ressourcen, um die ideale Balance zwischen Performance und Kosten herauszufinden. Mittels dieser Vorschläge kann dann entsprechend nachjustiert werden.

9.102 MS Azure: Temporär hohe Auslastung der Datenbank Partition

Ausgangssituation:

Die in Microsoft Azure hosted SEPPmail Appliance zeigt temporär eine hohe Auslastung der Datenbank Partition. Gegebenenfalls werden diesbezüglich Watchdog-Meldungen an den **Postmaster**^[247] und Mitglieder der **Gruppe**^[413] **admins**^[413] gesendet.

Frage:

Weshalb ist temporär die Auslastung der Datenbank Partition so hoch und wie lässt sich dieses Verhalten abstellen?

Ursache:

Ursächlich für die temporären Auslastungsspitzen ist der **Microsoft Azure Guest Agent**^[246], welcher für das Sammeln von Daten für die in Microsoft Azure verfügbaren Statistiken den Speicher belegt

Lösung:

Abschalten der Option **Enable Microsoft Azure Guest Agent**^[246] aus der Sektion **Virtualisation tools**^[246] des Menüs **System**^[224].

9.103 MS Exchange: Verify recipient addresses using SMTP-Lookups

Ausgangssituation:

Die SEPPmail Appliance wird im E-Mail-Fluss direkt vor einen Microsoft Exchange Server platziert.

Nach dem Aktivieren der Option **Verify recipient addresses using SMTP-Lookups** in der Administrationsoberfläche der SEPPmail Appliance unter **Mail System** ^[247] **Managed domains** ^[247], lehnt die SEPPmail Appliance eingehende E-Mails mit der Meldung „550 5.1.1 Recipient address rejected“ ab. Die Hinweise aus dem Handbuch zu dieser Option wurden beachtet.

Frage:

Was muss zusätzlich beachtet werden, damit die Funktion erfolgreich im Zusammenspiel mit Microsoft Exchange genutzt werden kann.

Antwort / Lösung:

Ab Exchange 2013 (gilt auch für 2016 und 2019) funktioniert der AD Lookup im SMTP Front End Connector nicht mehr direkt. Für die korrekte Funktion der SMTP AD Recipient Verification muss deshalb der Backend Connector auf Port 2525 verwendet werden.

Beim Installieren der CAS Rolle wird der SMTP Frontend Server per Standard mit installiert. Das hat zur Folge, dass der AntiSpam Agent für die Recipient Verification doppelt greift, zunächst beim Empfang der E-Mail über Port 25 und im Anschluss bei der Proxy Weiterleitung via Port 2525. Hierdurch werden E-Mails, welche auch nur eine ungültige Empfängeradresse beinhalten abgelehnt.

Wird die E-Mail hingegen direkt an Port 2525 übergeben, so greift der AntiSpam Agent nur einfach, wodurch die Recipient Verification wie erwartet funktioniert. Im Detail wird dabei jeder Empfänger einer E-Mail überprüft. Ist wenigstens einer der adressierten Empfänger gültig, so wird die E-Mail angenommen.

Für den Empfang von E-Mails sollten bei den Permission Groups des Default Receive Connector HUB Transport

- Anonymous Users
(für den E-Mail Empfang via Port 2525)
- Exchange Users
(sofern eine Login Verifikation benötigt wird, zum Beispiel wenn das Frontend die Authentication via SMTP Login vornimmt.)

Weitere erforderliche Aktionen über die Exchange Admin Shell:

- Install Antispam Agents
& \$env:ExchangeInstallPath\Scripts\Install-AntiSpamAgents.ps1
- Benötigte Transport Agents aktivieren
Enable-TransportAgent "Recipient Filter Agent"
- Spam Filters Konfigurieren
set-recipientFilterConfig -Enabled \$true
set-recipientFilterConfig -RecipientValidationEnabled \$true
set-ContentFilterConfig -Enabled \$false
set-SenderIDConfig -Enabled \$false
Set-IPAllowListConfig -Enabled \$false
Set-IPAllowListProvidersConfig -Enabled \$false
Set-IPBlockListConfig -Enabled \$false
Set-IPBlockListProvidersConfig -Enabled \$false
Set-SenderfilterConfig -Enabled \$false
Set-SenderIDConfig -Enabled \$false
Set-SenderReputationConfig -Enabled \$false

Theoretisch könnten noch verschiedene Filter aktiviert werden, was in der Regel jedoch bei einem System mit externen Front End nicht notwendig ist.

Eventuell muss die Recipient Domain noch überprüft / angepasst werden

Get-AcceptedDomain |fl name,AddressBookEnabled

Ebenso muss für den Lookup - sofern noch nicht geschehen das Adressbuch aktiviert werden:

set-recipientDomain xxxxx.ch AddressBookEnabled \$true

Restart Transport Services

Abschließend sind die Exchange Transportdienste neu zu starten

Restart-Service MExchangeTransport

Das Front End System, also die SEPPmail Appliance kann nun eingehende E-Mails unter Verwendung der Option **Verify recipient addresses using SMTP-Lookups** an den Exchange Backend Server auf Port 2525 übergeben (siehe **Mail System** ^[247] **Managed domains** ^[247], Tabelle, Spalte Server IP Address).

9.104 MS Office365: Anbinden von Exchange Online mit ATP / EOP

Diese Anleitung dient dem Integrieren der SEPPmail Appliance in eine Microsoft Office 365 Exchange Online (in diesem Dokument O365EO genannt) E-Mail-Infrastruktur. Ziel dieser Integration ist, alle Funktionen und Features der SEPPmail Appliance bei gleichzeitigem Ausschöpfen der vorhandenen Exchange Online Sicherheits- und Schutzfunktionen wie Advanced Threat Protection (ATP) oder Exchange Online Protection (EOP) bereitzustellen.

Somit sind auch Kunden, welche Ihre E-Mail Infrastruktur in der Cloud unter O365EO aufgebaut, beziehungsweise dorthin von einer bestehenden lokalen (on premises) Installation umgezogen haben, in der Lage die Vorteile der SEPPmail Appliance zu nutzen.

Auch die SEPPmail Appliance selbst kann dabei in der Cloud betrieben werden. So ist die Appliance zum Beispiel in Microsoft Azure bequem über den Marketplace zu beziehen.

Das Dokument basiert auf den aktuellen Versionen von Office 365 und der SEPPmail Appliance, wie sie im April 2019 verfügbar waren.

9.104.1 Faktoren für eine reibungslose Integration

Folgende Gegebenheiten waren der Ausgangspunkt für das Konfigurieren der beteiligten Systeme sowie das Erstellen dieser Anleitung:

- O365EO bleibt das MX-Ziel für die E-Mail-Kommunikation.
- Alle E-Mails von und an externe Empfänger werden über die SEPPmail Appliance verarbeitet
- Die SEPPmail Appliance kann in jeder beliebigen Umgebung betrieben werden (Public Cloud, Housing Provider, On-Premises, ...), welche für die O365EO-Hosts via IP oder FQDN erreichbar ist
- Die SEPPmail Appliance darf nicht für Open Relaying verwendet werden
- Die Kommunikation zwischen der SEPPmail Appliance und O365EO (und umgekehrt) basiert auf TLS-Verschlüsselung
- X-Header, die für das Steuern des internen E-Mail-Flusses zwischen O365EO und der SEPPmail Appliance verwendet werden, dürfen für externe Kommunikationspartner nicht sichtbar sein.
- Minimaler Einfluss auf den E-Mail-Verkehr während des Konfigurationsprozesses
- Einfache Konfiguration

9.104.2 Technischer Überblick

Die O365EO-Umgebung bleibt unverändert.

Das heißt die MX-Einträge im öffentlichen DNS zeigen unverändert auf die von Microsoft bereitgestellten Standard Server. Somit bleiben alle O365EO-Gateway-Funktionen zum Schutz der O365-Umgebung wie Anti-SPAM und Anti-Virus im vollen Umfang verfügbar.

E-Mails der Organisation - egal ob diese eingehend oder ausgehend sind - werden generell an die SEPPmail Appliance weitergeleitet und dort verarbeitet. Im Anschluss werden die E-Mails wieder an O365EO zurückgegeben und von dort an den Empfänger zugestellt.

9.104.3 Konfigurationsschema

9.104.3.1 Eingehender E-Mail Fluss

Die folgende Darstellung zeigt den Nachrichtenfluss von E-Mails aus dem Internet, welche über Exchange Online und die SEPPmail Appliance verarbeitet werden. Dabei kommen „Regeln“ und „Konnektoren“ zum Einsatz, auf deren Generieren in den folgenden Punkten noch näher eingegangen wird.

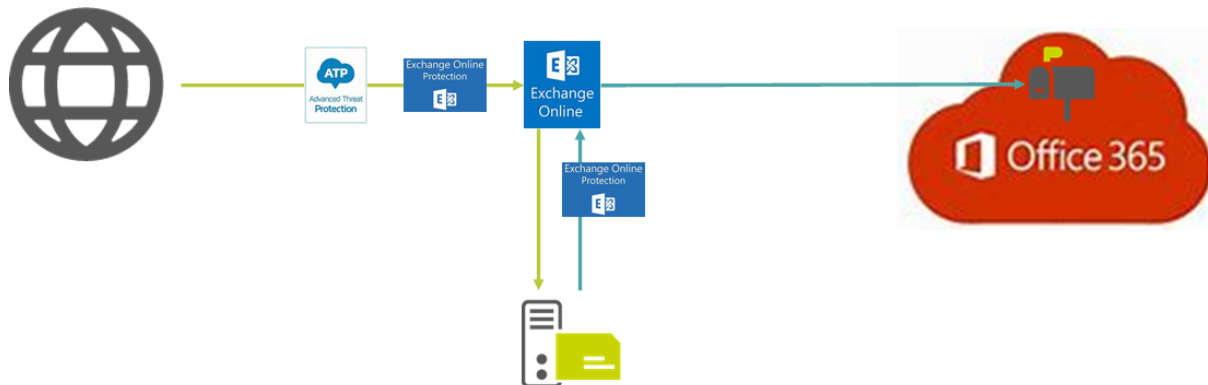


Abbildung 1

Der MX-Record für die interne E-Mail Domäne zeigt auf den Office 365 FQDN, , beispielsweise **contoso-de.mail.protection.outlook.com**.

Dadurch können alle Schutzmechanismen von Office 365 genutzt werden.

Eine aus dem Internet an die interne Organisation adressierte E-Mail passiert somit zunächst die „Advanced Threat Protection“ - kurz „ATP“ - und die „Exchange Online Protection“ - kurz „EOP“.

Am „Exchange Online“ der eigenen Organisation angelangt, wird die E-Mail aufgrund eines entsprechenden Regelwerks – ein Skript für eine Basiskonfiguration dieses Regelwerks wird auf Anfrage bereit gestellt – an die SEPPmail Appliance weitergeleitet.

Auf der SEPPmail Appliance wird die E-Mail gemäß deren Regelwerk Einstellungen verarbeitet und an „Exchange Online“ zurück übertragen. Dabei wird die E-Mail zunächst erneut mittels „EOP“ auf Malware geprüft. Somit werden auch die Inhalte ursprünglich verschlüsselter Nachrichten geprüft.

„Exchange Online“ erkennt anhand des Regelwerks, dass die E-Mail nicht aus dem Internet, sondern von der SEPPmail Appliance zugestellt wurde und legt diese somit in Office 365 ab.

Wo und wie die SEPPmail Appliance in diesem Konstrukt betrieben wird, ist dabei unerheblich. Das heißt, sie kann on premises, in der Cloud oder als Service eingebunden sein.

In Kombination mit Office 365 wird häufig „Microsoft Azure“ als Hosting Plattform genutzt (siehe gegebenenfalls auch **MS Azure: Installation** ⁷⁸³).

9.104.3.2 Ausgehender E-Mail Fluss

Die folgende Abbildung zeigt den Nachrichtenfluss für E-Mails, die von einem organisationsinternen Postfach an Empfänger außerhalb des Unternehmens gesendet werden. Auf das Generieren der hierfür benötigten „Regeln“ und „Konnektoren“ wird in den folgenden Punkten noch näher eingegangen.

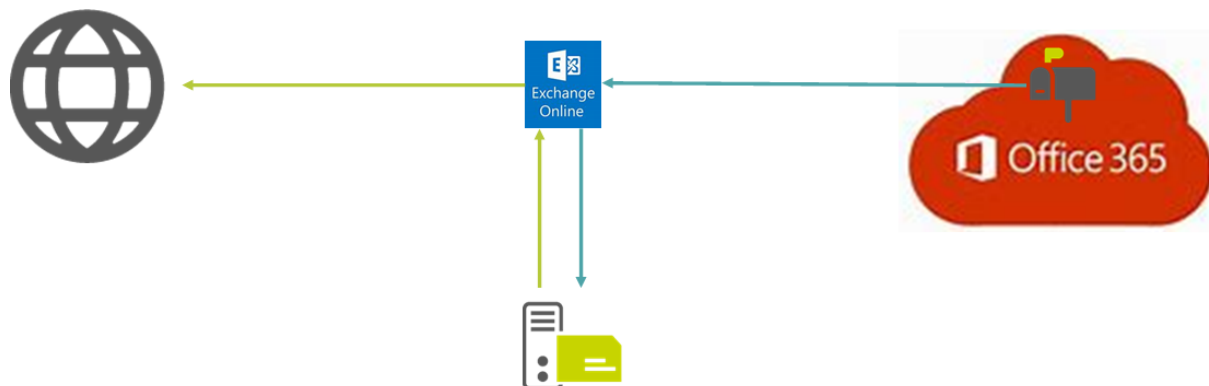


Abbildung 2

E-Mails, welche von innerhalb der Organisation an externe Empfänger (Internet) gesendet werden, werden von „Exchange Online“ anhand des Regelwerks zunächst an die SEPPmail Appliance weitergeleitet. Auf der SEPPmail Appliance wird die E-Mail gemäß Regelwerk Einstellungen verarbeitet und an „Exchange Online“ zurück übertragen. [„Exchange Online“ erkennt anhand des Regelwerks, dass die E-Mail nicht aus Office 365 direkt, sondern von der SEPPmail Appliance kommt und stellt die E-Mail direkt im Internet zu.

9.104.3.3 Interner E-Mail Fluss

Die folgende Abbildung zeigt den Nachrichtenfluss organisationinterner E-Mails.

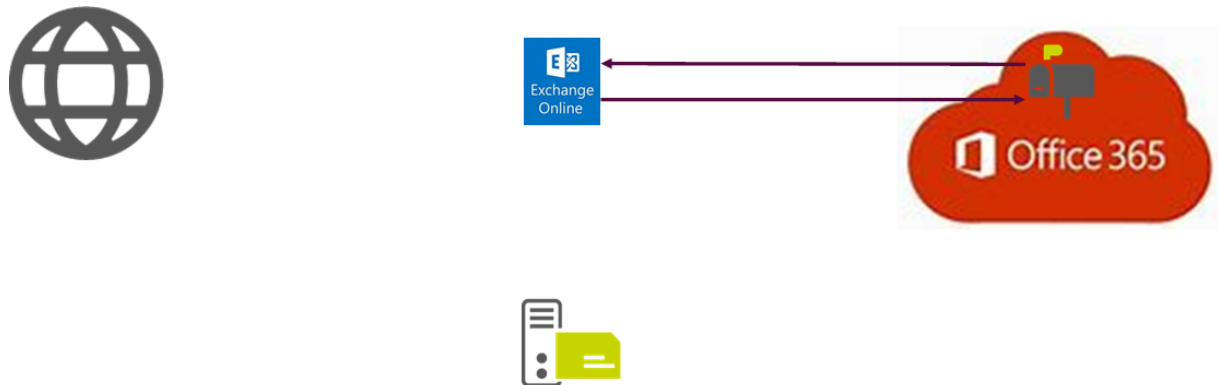


Abbildung 3

Organisationsinterne E-Mails bleiben in diesem Konstrukt unberührt. Das heißt, sie gehen über „Exchange Online“ nicht hinaus.

9.104.4 Vorbereitung

Die folgenden Schritte müssen abgeschlossen sein, um die SEPPmail Appliance erfolgreich in O365EO konfigurieren zu können. Somit ist sicherzustellen, dass diese Schritte bereits VOR dem Umstellen des Nachrichtenflusses in O365EO ausgeführt wurden. Fehlkonfigurationen können an dieser Stelle zum Verlust, beziehungsweise zum endlosen Weiterleiten (Loop) von E-Mails, bis hin zum Erliegen des gesamten E-Mail-Verkehrs führen.

9.104.4.1 Allgemein

- 1.) Exchange Online muss VOLL funktionsfähig sein.
Das heißt, alle internen Absender sind korrekt eingerichtet beziehungsweise migriert. E-Mails, welche aus dem Internet an die Domäne(n) der eigenen Organisation adressiert sind, werden an den O365EO MX-Host gesendet.
- 2.) Die SEPPmail Appliance ist in Betrieb und über die öffentliche IP-Adresse auf folgenden Ports und Protokolle erreichbar:
 - a. 8443 HTTPS für das Admin-Portal
 - b. 25 SMTP für den E-Mail-Verkehr
 - c. 443 HTTPS für das GINA Web-Interface
- 3.) In der SEPPmail Appliance sind unter **X.509 Root Certificates** ⁴⁸⁰ die Zertifikate importiert und als vertrauenswürdig (trusted) eingestuft, über welche Microsoft die Office 365 TLS Zertifikate bezieht. Derzeit sind das
GlobalSign Root CA
- 4.) Für die SEPPmail Appliance liegt ein SSL Zertifikat einer akkreditierten Zertifizierungsstelle vor. Dieses Zertifikat muss als Antragsteller den FQDN, welcher für die [default] GINA verwendet wird beinhalten. Dies kann also ein Einzel- ein SAN- oder ein Wildcardzertifikat sein.
- 5.) Die öffentliche IP-Adresse der SEPPmail Appliance ist über einen entsprechenden öffentlichen DNS-Eintrag erreichbar, beispielsweise **securemail.contoso.de**.
- 6.) Sowohl für O365EO, als auch der SEPPmail Appliance sind Administratorrechte vorhanden .
- 7.) Der FQDN des O365EO MX Eintrags liegt vor. Dieser ist im Office365 Admin Center unter Domains → Select the managed domain from the list → Edit domain zu finden, wo - beziehungsweise auf das Beispiel - in etwa folgender Eintrag zu sehen sein sollte:

^ Required DNS settings

Your DNS records must be set to the following values for your Office 365 services to run smoothly.

You can also download or print this data.

Export options ▾

^ Exchange Online

Type	Priority	Host name	Points to address or value	TTL	Actions
MX	0	@	contoso-de.mail.protection.outlook.com	1 Hour	
TXT	-	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour	
CNAME	-	autodiscover	autodiscover.outlook.com	1 Hour	

9.104.4.2 Zertifikate

Office 365 stellt ein Zertifikat für den O365EO-Host bereit. Bezugnehmend auf das vorherige Beispiel wäre dieses für die Domäne **contoso-de.mail.protection.outlook.com** ausgestellt. Dieses Zertifikat wird für das Absichern der Strecke von der SEPPmail Appliance zu O365EO mittels TLS benötigt. In der Regel ist dabei die TLS-Sicherheitsstufe „sicher (secure)“ möglich.

Um den Weg von O365EO zur SEPPmail Appliance zu sichern, wird ein SSL Zertifikat einer akkreditierten Zertifizierungsstelle (CA) benötigt. Dieses Zertifikat muss als Antragsteller den FQDN, welcher für die [default] GINA verwendet wird - im Beispiel **securemail.contoso.de** - beinhalten. Dies kann also ein Einzel- ein SAN- oder ein Wildcardzertifikat sein.

Um die TLS-Verbindung zu Ihrem O365EO-Host zu konfigurieren, ist zum Menü **Mail System**^[247] der Administrationsoberfläche der SEPPmail Appliance zu navigieren. In der **Sektion Managed Domains**^[247] ist nun auf den E-Mail-Domain-Name (im Beispiel **contoso.de**) zu klicken. Darauf folgend erscheint ein Untermenü, in welchem in der **Sektion TLS Settings**^[251] die Option **Secure: Only send mail if TLS is possible and the certificate is valid and its common name can be checked (not expired or revoked, and signed by a trusted certificate authority)** gewählt werden sollte. Abschließend müssen die Änderungen über die Schaltfläche **Save changes** links unten im Untermenü gespeichert werden. Daraufhin wechselt die Anzeige wieder in das Menü **Mail System**^[247].

Nun ist in der **Sektion SMTP Settings**^[252], im Abschnitt **TLS Encryption** die Option **Require TLS Encryption**^[253] zu aktivieren. Das bedeutet, dass ausschließlich TLS-gesicherte SMTP-Verbindungen von der SEPPmail Appliance angenommen werden.

Um das Zertifikat zu importieren, welches von O365EO für das Verbinden von der SEPPmail Appliance geprüft wird, muss im Menü **SSL** das oben genannte Zertifikat der akkreditierten CA über die Schaltfläche **Import existing certificate...** importiert oder via **Request or create new certificate...** ein CSR (Certificate Signing Request) für das Signieren des von der Appliance selbst generierten öffentlichen Schlüssel zu erzeugen (siehe auch **SSL**^[319]).

9.104.5 SEPPmail Appliance Konfiguration

Vor Beginn der Konfiguration einer initial aufgesetzten SEPPmail Appliance-Instanz sind unbedingt die grundlegenden Konfigurationsschritte (siehe [Inbetriebnahme der Secure E-Mail Gateway Appliance](#) ^[131], insbesondere [Benötigte Informationen zur Inbetriebnahme](#) ^[133] und [Firewall / Router einrichten](#) ^[135]) zu beachten.

Nachdem die oben genannten Schritte abgeschlossen ist, kann die SEPPmail Appliance für die sichere Kommunikation mit O365 vorbereitet werden.

Für eine Installation in Azure steht die SEPPmail Appliance im Azure Marketplace zur Verfügung. Ein Skript für das automatische Aufbauen eines [Cluster](#) ^[383] ist bei Bedarf in den weiterführenden Informationen unter <https://www.seppmail.de/produkte/seppmail365/> zu finden (siehe Verweis auf das „Github Repository“).

9.104.5.1 Mail System

Im Menü [Mail System](#) ^[247] wird der E-Mail-Fluss durch die SEPPmail Appliance konfiguriert.

Damit die SEPPmail Appliance keine ungesicherten Verbindungen annimmt, sollte weiterhin die Option *Require TLS encryption* ^[253] (siehe auch [SMTP settings](#) ^[252]) aktiviert werden.

Die Systeme, welche über die SEPPmail Appliance E-Mails an unbekannte Empfänger übermitteln dürfen ([Relaying](#) ^[254]) müssen angegeben werden. Für alle Office365 Server kann dies bequem über die Option *Allow relaying for Exchange Online servers* ^[255] (siehe [Exchange Online Relaying](#) ^[255]) eingestellt werden.

Mail System Settings

[Edit mail disclaimer...](#)[Edit mail templates...](#)

Managed domains		+																																																								
Managed services status		+																																																								
Outgoing server		+																																																								
TLS settings		+																																																								
SMTP settings		-																																																								
max. message size (KiB) (Note: cannot exceed 1000000 KiB)	 The size of a mail is not the sum of attachments due to encoding overheads. This means that a mail with a single 7M attachment usually has a size of about 10M.																																																									
Postmaster address	postmaster@contoso.de																																																									
SMTP server banner string (optional)																																																										
SMTP server HELO string (optional)																																																										
SMTP bind address (use with care)	IPv4: IPv6:																																																									
TLS encryption	☒ Require TLS encryption 																																																									
Extended settings (use with care)	Extended Postfix MTA settings...																																																									
Relaying		+																																																								
Exchange Online Relaying		-																																																								
Enable relay integration	☒ Allow relaying for Exchange Online servers (remember to set correct tenant IDs for managed domains) 																																																									
Currently registered MTAs	<table border="1"> <tbody> <tr> <td>IPv4:</td> <td>40 . 92 . 0 . 0</td> <td>15</td> <td>▼</td> </tr> <tr> <td>IPv4:</td> <td>40 . 107 . 0 . 0</td> <td>16</td> <td>▼</td> </tr> <tr> <td>IPv4:</td> <td>52 . 100 . 0 . 0</td> <td>14</td> <td>▼</td> </tr> <tr> <td>IPv4:</td> <td>104 . 47 . 0 . 0</td> <td>17</td> <td>▼</td> </tr> <tr> <td>IPv6:</td> <td>2a01:111:f400::</td> <td>48</td> <td>▼</td> </tr> <tr> <td>IPv6:</td> <td>2a01:111:f403::</td> <td>48</td> <td>▼</td> </tr> <tr> <td>IPv4:</td> <td>51 . 4 . 72 . 0</td> <td>24</td> <td>▼</td> </tr> <tr> <td>IPv4:</td> <td>51 . 4 . 80 . 0</td> <td>27</td> <td>▼</td> </tr> <tr> <td>IPv4:</td> <td>51 . 5 . 72 . 0</td> <td>24</td> <td>▼</td> </tr> <tr> <td>IPv4:</td> <td>51 . 5 . 80 . 0</td> <td>27</td> <td>▼</td> </tr> <tr> <td>IPv6:</td> <td>2a01:4180:4050:400::</td> <td>64</td> <td>▼</td> </tr> <tr> <td>IPv6:</td> <td>2a01:4180:4050:800::</td> <td>64</td> <td>▼</td> </tr> <tr> <td>IPv6:</td> <td>2a01:4180:4051:400::</td> <td>64</td> <td>▼</td> </tr> <tr> <td>IPv6:</td> <td>2a01:4180:4051:800::</td> <td>64</td> <td>▼</td> </tr> </tbody> </table>		IPv4:	40 . 92 . 0 . 0	15	▼	IPv4:	40 . 107 . 0 . 0	16	▼	IPv4:	52 . 100 . 0 . 0	14	▼	IPv4:	104 . 47 . 0 . 0	17	▼	IPv6:	2a01:111:f400::	48	▼	IPv6:	2a01:111:f403::	48	▼	IPv4:	51 . 4 . 72 . 0	24	▼	IPv4:	51 . 4 . 80 . 0	27	▼	IPv4:	51 . 5 . 72 . 0	24	▼	IPv4:	51 . 5 . 80 . 0	27	▼	IPv6:	2a01:4180:4050:400::	64	▼	IPv6:	2a01:4180:4050:800::	64	▼	IPv6:	2a01:4180:4051:400::	64	▼	IPv6:	2a01:4180:4051:800::	64	▼
IPv4:	40 . 92 . 0 . 0	15	▼																																																							
IPv4:	40 . 107 . 0 . 0	16	▼																																																							
IPv4:	52 . 100 . 0 . 0	14	▼																																																							
IPv4:	104 . 47 . 0 . 0	17	▼																																																							
IPv6:	2a01:111:f400::	48	▼																																																							
IPv6:	2a01:111:f403::	48	▼																																																							
IPv4:	51 . 4 . 72 . 0	24	▼																																																							
IPv4:	51 . 4 . 80 . 0	27	▼																																																							
IPv4:	51 . 5 . 72 . 0	24	▼																																																							
IPv4:	51 . 5 . 80 . 0	27	▼																																																							
IPv6:	2a01:4180:4050:400::	64	▼																																																							
IPv6:	2a01:4180:4050:800::	64	▼																																																							
IPv6:	2a01:4180:4051:400::	64	▼																																																							
IPv6:	2a01:4180:4051:800::	64	▼																																																							
Antispam / Antivirus		+																																																								
Blacklists (RBL)		+																																																								
Manual blacklisting / whitelisting		+																																																								
Save																																																										

Alle weiteren Einstellungen sind für jede Managed Domain ²⁴⁷ individuell vorzunehmen.

9.104.5.1.1 Managed domains

Jede E-Mail-Domäne, welche die SEPPmail Appliance in ihrer Funktion nutzen soll, muss innerhalb der Appliance konfiguriert werden und wird als **Managed Domain** bezeichnet.

Eine neue **Managed Domain** wird über die Schaltfläche **Add Managed Domain...** hinzugefügt.

SEPPMAIL

Added "contoso.de" to the list of managed domains.

MAIL SYSTEM SETTINGS

Managed domains

Domain Name	Server IP Address	TLS level	Smarthost	GINA	Disclaimer	Postmaster	SEPPmail domain encryption
contoso.de	[contoso-de.mail.protection.outlook.com]	may		[default]			unmanaged

Im Folgemenu wird im Abschnitt **Domain Name** die E-Mail-Domäne der Organisation - laut Beispiel **contoso.de** - eingetragen. Unter **Forwarding Server** ist der FQDN des O365EO der eigenen Organisation einzutragen, laut Beispiel also wieder **[contoso-de.mail.protection.outlook.com]**. Da dieser DNS-Name als A- und nicht MX-Record behandelt werden muß, ist der Eintrag durch eckige Klammern [] zu begrenzen.

SEPPMAIL

MAIL SYSTEM SETTINGS » ADD MANAGED DOMAIN

Settings

Domain Name: contoso.de
Use space to separate multiple domains

Forwarding server: [contoso-de.mail.protection.outlook.com]
Possible settings:
• [IP Address]
• [IP Address]:port
• [hostname] (no MX lookups)
• [hostname]:port (no MX lookups)
• domain (MX lookups)
• domain:port (MX lookups)

S/MIME domain keys: ☒ Create S/MIME domain keys for managed domain encryption for this domain and send public key to vendor pool

Use GINA domain: [default]

Save Cancel

Nach erfolgreichem Erstellen der **Managed Domain** wechselt die SEPPmail Appliance wieder in das Hauptmenü. Dort ist in der Spalte **Domain Name** der Tabelle in der **Sektion Managed Domains** auf den neu erstellten Eintrag **contoso.de** zu klicken.

SEPPMAIL

Added "contoso.de" to the list of managed domains.

MAIL SYSTEM SETTINGS

Managed domains

Domain Name	Server IP Address	TLS level	Smarthost	GINA	Disclaimer	Postmaster	SEPPmail domain encryption
contoso.de	[contoso-de.mail.protection.outlook.com]	may		[default]			unmanaged

Im Folgemenu sind in der **Sektion Settings** die Abschnitte **Domain Name** und **Forwarding Server** bereits mit den zuvor getätigten Eingaben belegt.

Im Abschnitt **Exchange Online Integration**^[266] wird festgelegt, dass nur E-Mails mit der zur E-Mail Domäne (im Beispiel **contoso.de**) gehörigen Tenant ID für das Relaying akzeptiert werden.

Im Abschnitt **Send ALL outgoing mails from this domain to the following SMTP server (optional)**^[267] wird der Eintrag aus **Forwarding Server**^[268] (im Beispiel also wieder **[contoso-de.mail.protection.outlook.com]**) übernommen. Dadurch werden E-Mails aus der eigenen Organisation an Empfänger außerhalb der Organisation nach dem Verarbeiten durch die SEPPmail Appliance wieder an den individuellen FQDN des O365EO der eigenen Organisation abgegeben.



» Login/Logout » Home » System » **Mail System** » Mail Processing » SSL » CA » MPKI » Administration » Cluster » Logs » Statistics » Users » Groups » GINA Domains » GINA Accounts » LFT Accounts » OpenPGP Public Keys » X.509 Certificates » X.509 Root Certificates » Domain Certificates » Customers

MAIL SYSTEM SETTINGS » EDIT MANAGED DOMAIN "CONTOSO.DE"

Settings							
Domain Name	contoso.de						
Forwarding server	[contoso-de.mail.protection.outlook.com] Possible settings: [IP Address] [IP Address]:port [hostname] (no MX lookups) [hostname]:port (no MX lookups) - domain (MX lookups) - domain:port (MX lookups)						
Header check	Mails from this domain must have a header with the following value:						
Exchange Online Integration	Allow relaying from Exchange Online Servers if the following Tenant ID is found: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX						
Allowed sending servers for this domain (leave empty to allow all relaying networks). Note: Entering an address here does not automatically allow relaying	<table border="1"> <thead> <tr> <th>Add allowed network:</th> <th>IPv4:</th> <th>32 ▼</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td>128 ▼</td> </tr> </tbody> </table>	Add allowed network:	IPv4:	32 ▼			128 ▼
Add allowed network:	IPv4:	32 ▼					
		128 ▼					
Send ALL outgoing mails from this domain to the following SMTP server (optional)	[contoso-de.mail.protection.outlook.com]						

In der **Sektion TLS settings**^[277] wird die Verbindung von der SEPPmail Appliance zum O365EO via TLS abgesichert. Dieser kann je nach Sicherheitsanforderung vorgenommen werden. Empfohlen wird die Einstellung „Secure“, welche eine Balance zwischen Sicherheit und vertretbarem Verwaltungsaufwand darstellt. Die Einstellung „Secure“ setzt voraus, dass der Eintrag **contoso-de.mail.protection.outlook.com** als A- und nicht MX-Record behandelt wird. also an den entsprechenden Stellen jeweils durch eckige Klammern [] begrenzt eingetragen wurde.

TLS settings	
☐ None: No TLS encryption ☐ May: Use TLS encryption if receiving mailserver supports it ☐ Encrypt: Only send mail if TLS encryption is possible ☐ Verify: Only send mail if TLS is possible and the certificate is valid (not expired or revoked, and signed by a trusted certificate authority) ☒ Secure: Only send mail if TLS is possible and the certificate is valid and its common name can be checked (not expired or revoked, and signed by a trusted certificate authority) ☐ Fingerprint: Only send mail if TLS is possible and the fingerprint of the server certificate has the following fingerprint:	
Use to separate multiple fingerprints. A fingerprint has the following format: C4:F8:39:9F:61:66:79:2B:4C:79:6C:32:1B:C2:56:D5	

Weitere Konfigurationsschritte einer **Managed Domain**^[247] sind unter **Mail System**^[247] zu finden.

9.104.5.2 Mail Processing

Im Menü **Mail Processing** ²⁸⁶⁾ wird die Art und Weise des Verarbeitens von E-Mails konfiguriert. Der Standardregelsatz kann dabei gegebenenfalls an die individuellen Bedürfnisse angepasst werden.

Damit das E-Mail-Routing mittels „Exchange Online“ „Regeln“ gewährleistet werden kann, werden bereits per Standard - also ohne zusätzlich notwendigen Konfigurationseingriff - folgende X-Header gesetzt:

```
X-SM-incoming=yes
X-SM-outgoing=yes
X-SM-internal=yes
X-SM-encrypted=yes
X-SM-decrypted=yes
```

Ob für das Anbinden der SEPPmail Appliance an Office 365 / Exchange Online eine spezielle Konfiguration erforderlich ist, hängt von Sicherheitseinstellungen in Microsoft 365 ab.

Wird beispielsweise „DKIM“ eingesetzt, so muss die DKIM Signatur, welche beim ersten Durchlauf durch „Exchange Online“ (siehe auch **Ausgehender E-Mail Fluss** ⁷⁹³⁾) gesetzt wird entfernt werden, da die E-Mail durch die SEPPmail Appliance gegebenenfalls kryptographisch behandelt und somit verändert wird. „Exchange Online“ wird beim zweiten Durchlauf die DKIM Signatur erneut anhängen.

Für das Löschen der ersten DKIM Signatur auf der SEPPmail Appliance ist folgender Code unter einzugeben

Zeile	Code
01	# Begin: Custom commands for outgoing e-mails BEFORE encryption
02	log (1, 'Begin: Custom commands for outgoing e-mails BEFORE encryption');
03	# Begin: Delete DKIM headers
04	log(1, 'Begin: Delete DKIM headers');
05	rmheader('DKIM-Signature');
06	rmheader('ARC-Authentication-Results');
07	rmheader('ARC-Message-Signature');
08	rmheader('ARC-Seal');
09	log(1, 'End: Delete DKIM headers');
10	# End: Delete DKIM headers
11	log(1, 'End: Custom commands for outgoing e-mails BEFORE encryption');
12	# End: Custom commands for outgoing e-mails BEFORE encryption

Code

9.104.6 Exchange Online Konfiguration

**Achtung:**

Die benötigten „Konnektoren“ und „Regeln“ in „Exchange Online“ sind zwingend via „PowerShell“ von einem Microsoft Windows System aus zu generieren, da die graphische Oberfläche von „Exchange Online“ nicht alle erforderlichen Optionen anbietet.

SEPPmail stellt für das geführte Generieren der erforderlichen Konnektoren und Regeln entsprechende Module über die „PowerShell Gallery“ www.powershellgallery.com/packages/SEPPMail365/ zur Verfügung. Nähere Informationen hierzu sind im zugehörigen Github Repository <https://github.com/seppmail/SEPPMail365> zu finden.

Wird die „Exchange Online“ Konfiguration über diesen Weg bewerkstelligt, so sind für die Lauffähigkeit keine weiteren Konfigurationsschritte im **Mail Processing** ^[286] erforderlich.

**Hinweis:**

Beim den genannten Modulen handelt es sich um einen von SEPPmail kostenfrei und unverbindlich bereit gestellten Service zur Konfiguration eines Drittanbieter Systems (Office365/Exchange Online).

In komplexen Umgebungen, insbesondere mit Beteiligung weiterer Drittsystem kann unter Umständen dennoch ein manuelles Anpassen beziehungsweise Konfigurieren durch entsprechend geschulte Personen erforderlich sein.

Weiterführende Informationen sind gegebenenfalls auch unter <https://www.seppmail.de/produkte/seppmail365/> zu finden.

9.105 MS Office365: Folgende Nachricht konnte nicht gesendet werden

Ausgangssituation:

Aus Office 365 heraus wird versucht eine E-Mail zu senden. Dies wird mit der Meldung

Folgende Nachricht konnte nicht gesendet werden:

<Betreff der Nachricht>

Weitere Details

quittiert.

Frage:

Weshalb können vom entsprechenden Office 365 Account keine oder nur sporadisch Nachrichten gesendet werden.

Antwort:

Dies hängt meist mit einem Eintrag in der „Office 365-Antispam-IP-Liste“ zusammen. Dies scheint keine „an/aus“ Liste zu sein, sondern vielmehr ein „Ranking“ zu beinhalten. Das verursacht unter Umständen, dass E-Mails sporadisch dennoch gesendet werden können.

Lösung:

Über das „Office 365-Antispam-IP-Listenentfernungsportal“ (<https://sender.office.com>) E-Mail Adresse und IP entsperren.

9.106 MS Office365: Fehler ATTR35 bei der Übergabe an Exchange Online

Ausgangssituation:

In einer Office / Microsoft 365 Umgebung können E-Mails von der SEPPmail Appliance nicht mehr zurück an Exchange Online (ExO) übergeben werden. In den Logs  ist in der Detail-Ansicht einer Betroffenen E-Mail die Meldung

451 4.4.62 Mail sent to the wrong Office 365 region. ATTR35.

zu sehen.

Lösung:

Über die „PowerShell Gallery“ (siehe auch www.powershellgallery.com/packages/SEPPMail365/) sollte die jeweils aktuelle Version des „SEPPmail365 Module“ in die PowerShell importiert werden.

Im Anschluss sind über dieses Modul zunächst die vorhandenen, SEPPmail Appliance-bezogenen ExO-Regeln und dann die Konnektoren zu entfernen.

Sind diese gelöscht, so werden nun zunächst die Konnektoren und dann die Regeln mittels dem „SEPPmail365 Module“ wieder angelegt.

Eine Dokumentation des „SEPPmail365 Module“ ist im zugehörigen Github Repository <https://github.com/seppmail/SEPPmail365> zu finden.

9.107 MS Office365: Verteilerlisten Alias-Adressen und Weiterleitungen

Ausgangssituation:

In einer MS Office365 Umgebung werden E-Mail-Alias-Adressen, Verteilerlisten und/oder E-Mail Weiterleitungen verwendet. E-Mails, welche an diese Adressen gesendet werden, landen verschlüsselt in den Postfächern der Empfänger.

Hintergrund:

Exchange Online ersetzt die ursprünglich adressierten E-Mails Adressen im E-Mail Header bereits beim Empfang aus dem Internet, anstatt nach dem Empfang durch die SEPPmail Appliance (siehe gegebenenfalls auch [Eingehender E-Mail Fluss](#) ^[792]).

Dies ist eine Eigenart von Exchange Online und kann - zumindest derzeit - nicht abgestellt werden.

Nachdem die SEPPmail Appliance den privaten Schlüssel zum Entschlüsseln der E-Mail anhand der Empfänger-Adresse ermittelt, passt der private Schlüssel nicht zum Zertifikat, welches zum Verschlüsseln verwendet wurde (Ursprüngliche Empfängeradresse vor dem Umschreiben).

durch die der Zeitpunkt des Umschreibens des From-Headers gemäss Weiterleitung nicht steuern lässt, gelangt die weitergeleitete E-Mail bereits mit dem umgeschriebenen To-Header zur SEPPmail Appliance. Somit wird dort der falsche Schlüssel, nämlich der des durch die Weiterleitung adressierten, anstatt der des ursprünglichen Empfängers verwendet. Ein Entschlüsseln der entsprechenden E-Mail schlägt somit fehl.

Frage:

Wie kann das korrekte Entschlüsseln einer E-Mail, trotz eingerichteter Weiterleitung gewährleistet werden?

Lösung:

Verteilerlisten

Anstatt von Verteilerlisten sollten Freigegebene Postfächer (Shared Mailbox) verwendet werden.

Alias-Adressen

Diese sollten generell vermieden werden. Diese verursachen abgesehen von der hier dargestellten Problematik auch zusätzliche Kosten, da für das signierte Versenden von E-Mails von Alias Adressen (und damit in der Folge den möglichen Erhalt verschlüsselter E-Mails an diese Adressen) auch jeweils ein Zertifikat erforderlich ist.

Eventueller Workaround auf der SEPPmail Appliance bei Domänen basierten Umschreibungen:

Zunächst sollten folgende Punkte gewährleistet sein:

1. Hinter beiden Adressen, ursprünglicher und weitergeleiteter Empfänger, steht dieselbe Person beziehungsweise derselbe Personenkreis.
2. Für beide Empfängeradressen existiert auf der SEPPmail Appliance ein Benutzerkonto (siehe [Users](#) ^[396]) mit entsprechendem Schlüsselmaterial.

Nun kann durch entsprechende **Custom Commands** ^[308] das Entschlüsseln unter Verwendung beider Empfängeradressen erfolgen. Hierzu ist in **Custom commands for incoming e-mails BEFORE decryption:** ^[308] in etwa folgender Code einzugeben:

Zeile	Code
01	# Begin: Custom commands for incoming e-mails BEFORE decryption
02	log(1,'Begin: Custom commands for incoming e-mails BEFORE decryption');
03	# Begin: Decrypt forwarded e-mails
04	log(1,'Begin: Decrypt forwarded e-mails');
05	if (smime encrypted()) {
06	if (replace rcpt('@original.tld', '@forwarded.tld',1)) {
07	log(1, 'Encrypted mail to @original.tld, check if we can decrypt with @forwarded-tld keys');
08	if (decrypt smime()) {
09	@REMOVETAGS@
10	log(1, 'S/MIME decrypted with user certificate');

Zeile	Code
11	@TAGDECRYPTED@
12	@TAGHEADERDECRYPTED@
13	@SETDECRYPTED@
14	} else if (decrypt domain smime()) {
15	@REMOVETAGS@
16	log(1, 'S/MIME decrypted using domain certificate');
17	@TAGDECRYPTED@
18	@TAGHEADERDECRYPTED@
19	@SETDECRYPTED@
20	} else {
21	log(1, 'Decryption for @forwarded.tld FAILED, going on with decryption for @original.tld');
22	}
23	replace rcpt('@forwarded.tld', '@original.tld', 1);
24	}
25	}
26	log(1, 'End: Decrypt forwarded e-mails');
27	# End: Decrypt forwarded e-mails
28	log(1, 'End: Custom commands for incoming e-mails BEFORE decryption');
29	# End: Custom commands for incoming e-mails BEFORE decryption

[Code](#)

9.108 MS Outlook: Der Name Ihrer digitalen ID kann im zugrunde liegenden Sicherheitssystem nicht gefunden werden.

Ausgangslage:

Outlook wird als E-Mail Client hinter einer SEPPmail Appliance eingesetzt. Über die Konfiguration wird die SEPPmail Appliance angewiesen, nicht entschlüsselbare E-Mails dennoch anzunehmen und an den Empfänger auszuliefern (**Reject mails if S/MIME decryption fails**  deaktiviert). Beim Versuch eine verschlüsselte, aus dem Internet stammende E-Mail in Outlook zu öffnen, erscheint die Meldung „Dieses Element kann nicht geöffnet werden. Der Name Ihrer digitalen ID kann im zugrunde liegenden Sicherheitssystem nicht gefunden werden.“

Ursache:

1. SEPPmail verfügt über keinen privaten Schlüssel, um die Nachricht zu entschlüsseln.

Individuelle Abhilfe:

- a) Sofern möglich die Option **Reject mails if S/MIME decryption fails**  aktivieren.
 - b) Mit dem Absender klären, woher er den öffentlichen Schlüssel des Empfängers hat. Dieser falsche Schlüssel sollte vom Absender gelöscht werden und der adressierte Empfänger sollte dem Absender seinen aktuellen Schlüssel zur Verfügung stellen (bei S/MIME durch eine signierte E-Mail).
2. Weiterhin wurde dieses Phänomen beim Einsatz von ScanMail von Trend MicroTM beobachtet. Die ausgelieferten E-Mails sind dann sehr klein (ein paar kb) anstelle der eigentlichen Grösse. Trend MicroTM hat(te) seit längerer Zeit einen Bug, welcher dazu führt, dass signierte E-Mails zerstört werden (genauer: Der Inhalt wird gelöscht). Outlook reagiert dann mit oben genannter Fehlermeldung, welche eigentlich falsch ist, da die Nachricht gar nicht mehr vorhanden ist.

Individuelle Abhilfe:

Prüfen ob gegebenenfalls entsprechende Updates für ScanMail zur Verfügung stehen.

9.109 SEPPmail Microsoft Outlook Cross-Platform-Add-In: Ablageort der LOG-Dateien

Ausgangssituation:

Zur Analyse des Verhaltens des SEPPmail Microsoft Outlook Cross-Platform-Add-In sollen LOG Einträge herangezogen werden.

Frage:

Wo sind die LOG Einträge des SEPPmail Microsoft Outlook Cross-Platform-Add-In zu finden?

Antwort:

Die LOG Einträge werden jeweils getrennt für die jeweils angemeldeten Benutzer geschrieben und werden unter
%USERPROFILE%\AppData\Roaming\SEPPmail\Outlook AddIn\
abgelegt.

Für den jeweils aktuellen Tag sind im Normalfall die Dateien

Info.txt

Trace.txt

Im Fehlerfall kommt die Datei

Error.txt

hinzu.

Die Dateien werden täglich rotiert und erhalten dabei jeweils Ziffern am Ende der jeweiligen Namen angefügt.

9.110 SEPPmail Microsoft Outlook Cross-Platform-Add-In: Wiederholtes Deaktivieren durch Outlook

Ausgangssituation:

SEPPmail Microsoft Outlook Cross-Platform-Add-In ist auf dem MS-Outlook Client installiert. Jedoch sind beim Öffnen einer neuen E-Mail keine **Schaltflächen für den Versand von E-Mails** [208] zu sehen.

Ursache:

- a) Das SEPPmail Microsoft Outlook Cross-Platform-Add-In wird vom MS-Outlook Client automatisch deaktiviert. In der Regel tritt dieses Verhalten nur in stark ausgelasteten Terminalserver Umgebungen auf.

Individuelle Abhilfe:

An dieser Stelle kann über die SEPPmail Microsoft Outlook Cross-Platform-Add-In Konfiguration keine Lösung herbeigeführt werden, da die Steuerung über MS-Outlook selbst vorgenommen wird.

Wie MS-Outlook angewiesen werden kann, das SEPPmail Microsoft Outlook Cross-Platform-Add-In nicht mehr zu deaktivieren, ist unter

<https://docs.microsoft.com/de-de/visualstudio/vsto/registry-entries-for-vsto-add-ins?view=vs-2019> zu finden.

- b) In der Konfiguration des angemeldeten Benutzers ist vorgegeben, dass keine **Schaltflächen für den Versand von E-Mails** [208] angezeigt werden sollen.

Individuelle Abhilfe:

Aktivieren der entsprechenden Schaltflächen direkt in der **Registry** [203] oder über die **Addin Verwaltung** [212].

9.111 MPKI: Beauftragen/Anbinden SwissSign

Ausgangssituation:

Für den Bezug von S/MIME Zertifikaten soll ein Antrag bei SwissSign gestellt werden.

Mögliche Varianten:

1. Einzelkunde mit eigenem MPKI Zugang (Auto-RAO Zertifikat)
2. Managed Service Provider (MSP) mit eigenem MPKI Zugang (Auto-RAO Zertifikat)
 - a. welcher Kunden-Domänen selbst validieren kann (nur E-Mail ID Silver Zertifikate möglich).
Da hier die Validierung durch den MSP vorgenommen werden kann, ist kein Vertragswerk zwischen MSP-Kunden und SwissSign erforderlich!
 - b. welcher über seinen MPKI Zugang (Auto-RAO Zertifikat) Zertifikate für SwissSign Kunden bezieht, welche bei Vertragsschluss den MSP für den Zertifikatsbezug über seinen Zugang berechtigen (siehe Antragsformular, Seite 1, Option „Zertifikate für diese Organisation werden bezogen durch bestehende Managed PKI für folgende Organisation:“)
Über diese Variante sind auch höherwertige Zertifikate (wie zum Beispiel E-Mail ID Gold) möglich.

Bestellung:

Für das Bestellen des SwissSign MPKI Zugangs wenden Sie sich bitte an certificates@seppmail.de.

Weiterhin steht das für die Bestellung benötigte **Antragsformular** (Stand 3/2021), sowie eine **Ausfüllhilfe zum Antragsformular** bereit.

Einrichten des MPKI [339] Zugangs nach erfolgreicher Bestellung auf der SEPPmail Appliance:

- Anmelden an der Administrationsoberfläche der SEPPmail Appliance
- Navigieren zu **MPKI** [339] **Connector** [339]
 - Auswahl von „SwissSign“ unter **MPKI type** [339] und Klicken von **Select...**
 - Unter **MPKI managed domains** [340] sind diejenigen **Managed domains** [247] auszuwählen (Mehrfachauswahl mit gedrückter Hochsteltaste möglich), für welche Zertifikate über die **MPKI** [339]-Schnittstelle bezogen werden sollen.
 - Speichern der vorgenommenen Einstellungen durch Klicken von **Save**

Variante 1 und 2:

- Wechseln in **Default parameters** ^[364] und übernehmen der Konfigurationsdaten aus der SwissSign Willkommens-E-Mail in die gleichnamigen Konfigurationsfelder
 - **Service URL:** ^[364] <https://ra.swisssign.net/ws/cmc>
 - **Static subject part:** ^[364] <Attribute>
 - **Account name:** ^[365] <Kontoname>
 - **Product name :** ^[365] <Produktname>
- Herunterladen des „operator certificate“ (Auto-RAO) über das SwissSign Konto.
Die Zugangsdaten versendet SwissSign via IncaMail in einer separaten E-Mail (gegebenenfalls auch im Spam Ordner des E-Mail Clients suchen!)
- Nach **Certificate** ^[366] wechseln
 - Die heruntergeladene PKCS#12 Datei unter **PKCS12 identity file** ^[366] auswählen
 - Das zur PKCS#12 Datei gehörige Passwort zum Schutz des privaten Schlüssels unter **PKCS12 password** ^[367] eingeben
- im Menü ganz unten rechts mit **Save** speichern.
Nun sollte bei der Meldung
 an operator certificate with valid password has been found.
erscheinen.
- Nun zu **Settings** ^[367] wechseln
 - Über **Add or update...** **Chain certificates (needed to sign e-mails)** ^[368] bereitstellen ^[368]
 - Gewünschte Überschneidung der Zertifikatslaufzeit via **PKCS12 identity file** ^[366] einstellen
- im Menü ganz unten rechts erneut mit **Save** speichern.

Variante 2a

Da in dieser Variante Zertifikate mit den **Default parameters** ^[364] des MSPs ausgestellt werden, kann dieser Kundendomänen selbst validieren.
Die Kundendomänen müssen nach dem Validieren nur zur Auswahl unter **Connector** ^[339] **MPKI managed domains** ^[340] hinzugefügt werden.

Variante 2b

In diesem Fall schließt der (MSP) Kunde direkt einen Vertrag mit SwissSign. Dementsprechend muss von ihm auch das Antragsformular (siehe oben) ausgefüllt und an SwissSign übermittelt werden. Im Antrag wird der SwissSign über die Option „Zertifikate für diese Organisation werden bezogen durch bestehende Managed PKI für folgende Organisation:“ mitgeteilt, dass kein eigener MPKI Zugang für das Beziehen von Zertifikaten gewünscht ist, sondern dass die Zertifikate über den Zugang des MSPs - welcher in der Option auch benannt werden muss - bezogen werden sollen,

- Wechseln in **Domain specific parameters** ^[365]
 - Eintragen der jeweiligen **Managed domain** ^[247] des Kunden unter
 - **Domain:** ^[365] <Managed domain ^[247] des Kunden>
(bei mehreren Kunden-Domänen können mehrere Einträge erstellt werden, welche jeweils die identischen, folgenden Parameter beinhalten)
 - Übernehmen der Konfigurationsdaten aus der SwissSign Willkommens-E-Mail in die gleichnamigen Konfigurationsfelder
 - **Product name :** ^[366] <Produktname>
 - **Static subject part:** ^[366] <Attribute>

**Achtung:**

Werden die Zugangsdaten direkt aus der „Willkommens-E-Mail“ in die Konfigurationsoberfläche kopiert, so kann es aufgrund des HTML-E-Mail-Formats zu Problemen bei der Interpretation von Zeichen und somit zur Fehlfunktion kommen. Wir empfehlen daher, die Zugangsdaten zunächst in einen Texteditor zu kopieren oder die Daten manuell einzugeben.

Insbesondere Zeichen wie zum Beispiel Hochkommata können bezüglich der Schreibweise `` , problematisch sein. Hier müssen bei Bedarf die unterschiedlichen Varianten durchgetestet werden.

Weiterhin ist darauf zu achten, dass bei der Eingabe beziehungsweise beim Kopieren nicht versehentlich führende oder abschliessende Leerzeichen mit eingefügt werden.

Bei fehlenden

- Konfigurationsdaten
- Zugangsdaten, beziehungsweise Auto-RAO Zertifikat
- Fehlern (Fehlermeldung immer beifügen!) beim Ausstellen von Zertifikaten

steht der SwissSign Support unter mpki@swissign.com zur Verfügung.

9.112 MPKI: Bezogene Zertifikate für weitere Zwecke einsetzen

Ausgangssituation:

In der SEPPmail Appliance ist die **Managed PKI** ^[29] Schnittstelle (siehe auch **MPKI** ^[339]) für den automatischen Bezug von S/MIME Zertifikaten eingerichtet. Dabei werden von der angebundenen CA Zertifikate mit einer Güte bezogen, welche zum Beispiel auch das Signieren von Dokumenten zuließe.

Frage:

Können die über die **Managed PKI** ^[29] Schnittstelle bezogenen Zertifikate von der SEPPmail Appliance im PKCS#12 Format heruntergeladen werden um diese für eine Dokumentensignatur zu verwenden?

Antwort:

Grundsätzlich können von der SEPPmail Appliance aus Sicherheitsgründen keine privaten Schlüsselinformationen heruntergeladen werden. Somit ist das Verwenden des von der SEPPmail Appliance generierten Schlüssels für andere Zwecke ausser E-Mail Verschlüsselung/Signierung nicht möglich.

Jedoch bieten manche **MPKI** ^[339] Anbieter (CAs) das Ausstellen eines weiteren Zertifikates (über eine Web-Oberfläche des Anbieters) zu diesem Zweck zum Nulltarif an.

Setzen Sie sich gegebenenfalls mit Ihrem CA-Anbieter diesbezüglich in Verbindung.

9.113 MPKI: Bezug von Zertifikaten funktioniert nicht mehr

Ausgangssituation:

Beim Versuch Zertifikate über die **Managed PKI** ^[29] Schnittstelle zu beziehen, erscheint die Meldung

Could not issue <MPKI-provider> certificate: Failed to issue certificate with subject /CN=<email address of user>/email=<email address of user>/o=...

Frage:

Weshalb erscheint diese Meldung?

Antwort:

Die aktuellen Sicherheitsanforderungen für S/MIME Zertifikate erlauben im subject-name (CN) des Antragstellers eines Zertifikates keine E-Mail Adressen mehr.

Beim Anfordern von Zertifikaten mit personalisiertem „Subject“, wird der Eintrag aus dem Feld „Name“ des jeweiligen **Users** ^[396] hierfür herangezogen. Wurde hier beim Anlegen des **Users** ^[396] die E-Mail Adresse eingetragen, so scheitert der Zertifikatsbezug. In diesem Fall muss bei den betroffenen Users der Eintrag im Feld „Name“ durch den Klarnamen ersetzt werden.

Zusatzinformation:

Das Standardverhalten für das automatische Anlegen von **Users** ^[396] ist im gleichnamigen Kapitel beschrieben.

Steht für das Anlegen von **Users** ^[396] eine LDAP Verbindung zur Verfügung, so können über diese die Felder „Name“ und „User ID“ befüllt werden (siehe auch **Benutzer: Anlage mittels LDAP Abfrage** ^[687] beziehungsweise **Benutzer: Berechtigung mittels LDAP Abfrage** ^[689]).

9.114 MPKI: DigiCert versendet Validierungs-E-Mails

Ausgangssituation:

DigiCert  ist als **MPKI**  für den automatischen Bezug von S/MIME Zertifikaten eingerichtet. Beim Bezug wird jedoch an die E-Mail Adresse des Antragstellers eine Validierungs-E-Mail gesendet, wodurch der automatisierte Prozess fehlschlägt.

Frage:

Wie kann die Validierungs-E-Mail in diesem automatisierten Prozess unterbunden werden?

Lösung:

Die Organisationen und deren E-Mail Domänen, für deren Benutzer S/MIME Zertifikate bezogen werden sollen, müssen bei DigiCert validiert werden.

Stichwörter für den DigiCert Support:

- OV - Normal Organization Validation
- EV - Extended Organization Validation (EV)
- DCV - DomainControlValidation DCV
- CS - Code Signing Organization Validation*
- EV CS - Code Signing Organization Extended Validation (EV CS)

9.115 MPKI: Umstellen des Zertifikatsanbieters (CA)

Ausgangssituation:

Für den automatische Zertifikatsbezug via **MPKI**^[339] soll der Zertifikatsanbieter (CA) gewechselt werden.

Frage:

1. Was passiert mit den bestehenden Zertifikaten des alten Anbieters?

Antwort:

Sofern die Zertifikate nicht zurückgewiesen (revoked) werden, bleiben sie bis zum Ende der Laufzeit (validity) gültig.

2. Werden ablaufende Zertifikate der alten CA – oder auch manuell importierte – automatisiert durch neue Zertifikate der aktuell in der **MPKI**^[339] eingestellten CA automatisch erneuert?

Antwort:

Sofern das automatische Erneuern von Zertifikaten (**Automatically renew expiring certificates if validity days left less than**) in den **MPKI**^[339]-Einstellungen des jeweiligen Anbieters aktiviert ist, spielt es keine Rolle, welche CA das ablaufende Zertifikat erstellt hat. Der Erneuerungsprozess orientiert sich ausschließlich an der Gültigkeit des jeweils vorhandenen Zertifikats mit der längsten Laufzeit.

Ausnahme:

Self-Signed Zertifikate, siehe Hinweis zur Option (**Automatically renew expiring certificates if validity days left less than**) des jeweiligen **MPKI**^[339]-Anbieters.

Hinweis:

Nachdem die abzulösende CA nach dem Ändern der **MPKI**^[339]-Konfiguration durch die SEPPmail Appliance nicht mehr erreichbar ist, ist ein Revozieren der Zertifikate dieser CA über die SEPPmail Appliance nicht mehr möglich.

Besteht der Wunsch, ab dem Zeitpunkt des Umstellens mit Zertifikaten des neuen Anbieters zu arbeiten, so müssten

- die Zertifikate des abzulösenden Anbieters noch vor dem Ändern der Konfiguration revoziert werden
- nach dem Ändern der Konfiguration für alle Benutzer der Neubezug von Zertifikaten über die Option **Automatically create certificates for active users without certificates** in den **MPKI**^[339]-Einstellungen des aktuellen Anbieters angestoßen werden



Achtung:

Durch diese Aktion ginge der Vorteil der Überschneidung (**Automatically renew expiring certificates if validity days left less than**) verloren.

Das heißt, unter Umständen steht dem Kommunikationspartner das benötigte Zertifikat zum Verschlüsseln an interne **Users**^[398] bis zum Erhalt der ersten signierten E-Mail nicht zur Verfügung.

9.116 Schnittstellen: legacy.app

Die SEPPmail Appliance bietet bei Bedarf eine weitere Schnittstelle, über welche diverse Informationen der Appliance abgefragt und gegebenenfalls auch GINA-Accounts erzeugt beziehungsweise angepasst werden können.

SEPPmail stellt für den Zugriff auf diese Schnittstelle Module über die „PowerShell Gallery“ www.powershellgallery.com/packages/SEPPmailLegacy/0.8.2-RC2 zur Verfügung. Nähere Informationen hierzu sind im zugehörigen Github Repository <https://github.com/seppmail/SEPPmailLegacy> zu finden.



Hinweis:

Beim den genannten Modulen handelt es sich um einen von SEPPmail kostenfrei und unverbindlich bereit gestellten Service außerhalb jeglicher Supportansprüche.

9.117 Sicherheit: Path traversal attack

Ausgangssituation:

In der Administrationsoberfläche der SEPPmail Appliance, beziehungsweise im **IMPORTANT: Daily Report** ⁹⁶ wird die Meldung

Possible path traversal attack in webmail. Please contact the support

angezeigt.

Ursache:

Auf der SEPPmail Appliance wurde eine „path traversal“ Attacke auf das GINA-Interface festgestellt.

Abhilfe:

Zunächst ist durch Senden einer E-Mail an support@seppmail.de ein Support Ticket zu erstellen. Nach Erhalt der Eingangsbestätigung kann unter Verwendung der darin enthaltenen Ticket-Nummer eine **Support Connection** ³⁷⁰ geöffnet werden. Sobald diese etabliert ist, sollte dies dem Support als Antwort auf die Eingangsbestätigungs-E-Mail Mitgeteilt werden.

Der Support wird über die **Support Connection** ³⁷⁰ die Ursache der Meldung prüfen und den Status zurücksetzen und das Ticket wieder schließen.

9.118 Sicherheit: RC4 Attacken möglich / alte TLS Version

Ausgangssituation:

Die SEPPmail Appliance wurde einem Sicherheits Test (Pen-Test) unterzogen. Dabei wurde festgestellt, dass das Web-Interface (GINA) unter anderem anfällig auf RC4 Attacken sei oder auch eine alte TLS Version verwendet würde.

Ursache 1:

Meist ist die Ursache für solche Meldungen, dass der TLS Tunnel gar nicht an der SEPPmail Appliance, sondern einer vorgelagerten Komponente (Firewall) terminiert wird.

individuelle Abhilfe:

Beseitigen der Sicherheitslücken auf dem vorgelagerten System.

Ursache 2:

Treten die Sicherheitslücken auch bei direktem Terminieren des TLS Tunnels auf der SEPPmail Appliance auf, so werden die entsprechenden Einstellungen für eine maximale Kompatibilität verwendet.

individuelle Abhilfe:

Setzen des Hakens unter **GINA Domains** ☐ **Settings** ☐ **Disallow insecure ciphers** ☐. Dadurch wird die Anfälligkeit auf RC4 Attacken auf der SEPPmail Appliance abgeschaltet, führt jedoch zur Inkompatibilität mit älteren Systemen.

9.119 Sicherheit: TLS 1.0 abschalten

**Hinweis:**

Mit dem 30. Juni 2018 ist TLS 1.0 für PCI (Payment Card Industry Data Security Standard) Umgebungen abgekündigt.

Ausgangssituation:

Um den Sicherheitsstandard der SEPPmail Appliance zu erhöhen, soll TLS 1.0 abgeschaltet werden.

Lösung:

TLS 1.0 sowie weitere, sicherheitstechnisch nur bedingt zu empfehlende Protokolle und Verfahren (siehe auch **Ciphers** ¹⁰³) sind auf der SEPPmail Appliance durch Aktivieren der Option

Disallow insecure ciphers (breaks compatibility with older browsers, but necessary for PCI compliance)
(siehe **GINA Domains** ⁴¹⁶ **Settings** ⁴¹⁶) abzustellen.

**Hinweis:**

Wird der SSL/TLS Tunnel an einem vorgelagerten E-Mail Relay / Firewall terminiert, so sind dort entsprechende Maßnahmen zu ergreifen.

9.120 Sicherheit: TLS Zertifikat kann nicht validiert werden

Ausgangssituation:

Die SEPPmail Appliance bildet den Übergang zum Internet und nimmt somit TLS-Verbindungen direkt entgegen. Ein Prüfen der TLS Verbindung von außen, zum Beispiel via CheckTLS(.com), zeigt an, dass das auf der SEPPmail Appliance unter **SSL**  eingebundene Zertifikat nicht validiert werden konnte, obwohl dieses von einer akkreditierten CA stammt.

Frage:

Woraus resultiert die Meldung, dass das Zertifikat nicht validiert werden konnte?

Ursache:

Dienste wie CheckTLS sind nur die Root Zertifikate der üblichen akkreditierten CAs bekannt. Meist werden jedoch SSL Zertifikate nicht durch die Root CA direkt, sondern durch Sub CAs ausgestellt. Wurde beim Import in die SEPPmail Appliance ausschließlich das SSL Zertifikat eingebunden, also ohne die Zwischen- (Intermediate-) Zertifikate der ausstellenden Sub CAs, so kann der externe Dienst die Zertifikatskette nicht vervollständigen, was zur entsprechenden Meldung führt.

Lösung:

Zunächst müssen die erforderlichen Zwischen- (Intermediate-) Zertifikate von der Web-Seite der ausstellenden CA heruntergeladen werden und anschließend im Menü **SSL**  mittels **Import existing certificate...** importiert werden.

9.121 Sicherheit: Zertifikat für TLS gesicherte SMTP-Anfragen

Ausgangssituation:

Zur SEPPmail Appliance hin soll eine TLS gesicherte SMTP Verbindung aufgebaut werden.

Frage:

Welches Zertifikat wird der Gegenstelle beim Aufbau einer TLS Verbindung von der SEPPmail Appliance präsentiert?

Antwort:

Das unter **SSL** ³¹⁹ eingebundene Zertifikat wird für TLS gesicherte SMTP-Anfragen präsentiert.

9.122 Signatur: Auswirkung von Änderungen im Header von E-Mails auf eine Signatur

Ausgangssituation:

Aus diversen Gründen muss auf einem der SEPPmail Appliance vor-, beziehungsweise nachgelagertem System (X-) Header manipuliert werden.

Frage:

Wird durch Manipulationen im Header einer signierten E-Mail die Signatur zerstört?

Antwort:

Die Header einer E-Mail werden bei der Signatur nicht berücksichtigt. Somit wird durch das Verändern von Headern (und somit auch der Betreffzeile / Subject) die Signatur nicht zerstört.

9.123 Signatur: Log-Meldung „Warning: Could not find certificate chain. Add certificates to x.509 root certificates“ beim Signieren

Ausgangssituation:

Bei einer ausgehenden E-Mail wurde vom Absender die kryptographische „Signatur“ der E-Mail angefordert. In den **Logs** [388] der SEPPmail Appliance wird zum Signaturvorgang die Meldung

Warning: Could not find certificate chain. Add certificates to x.509 root certificates angezeigt. Dennoch wurde die E-Mail signiert.

Frage:

Was bedeutet diese Meldung und wie kann sie beseitigt werden?

Ursache:

In Zertifikaten, welche für das Signieren verwendet werden, ist normalerweise die Zertifikatskette nicht enthalten. Die SEPPmail Appliance ergänzt erst beim Vorgang des Signierens die Zertifikatskette, damit der Empfänger Seite das Zertifikat der Signatur auch dann erfolgreich geprüft werden kann, wenn dort nur das Root Zertifikat als vertrauenswürdig eingestuft ist, die Zertifikatskette – also die Zwischen- oder auch Intermediate- Zertifikate – jedoch nicht bekannt ist.

Lösung:

Damit die Appliance die Zertifikatskette wie beschrieben ergänzen kann, muss diese auch bekannt sein. Das heißt, das Root- sowie die Intermediate- Zertifikate der ausstellenden CA der internen **User** [398] **Zertifikate** [404] müssen unter **X.509 Root Certificates** [480] importiert und das Vertrauen (trust) ausgesprochen werden.

Kommt eine **MPKI** zum Einsatz, so kann dieser Vorgang durch Klicken von Add or Update... im Abschnitt **Chain certificates (needed to sign e-mails)** der Sektion **Settings** der jeweiligen MPKI Detail-Einstellungen automatisch durchgeführt werden.

9.124 Signatur: Signieren aller ausgehenden E-Mail mit einem einzigen Domänenzertifikat

Ausgangssituation:

Alle ausgehenden E-Mails sollen generell S/MIME signiert werden. Jedoch soll aus Kostengründen hierfür nur ein Zertifikat – domänenübergreifend – verwendet werden.

Hintergrundinfo:

Zwar erscheint die Domänensignatur, also das Signieren aller ausgehender E-Mails mit nur einem S/MIME (Domänen-) Schlüssel, zunächst als günstige Alternative zum Signieren mit jeweils personalisierten S/MIME Schlüsseln. Tatsächlich wird dieses Verfahren jedoch über Kurz oder Lang zu Problemen beziehungsweise enormen Verwaltungsaufwänden führen.

Zur Funktionsweise:

Damit der Antragsteller eines Domänenzertifikates mit dem Absender der E-Mail übereinstimmt, und somit die Signaturprüfung beim Empfänger erfolgreich durchgeführt werden kann, muss der Absender der E-Mail bei jeder ausgehenden E-Mail manipuliert werden, so dass er mit dem Antragsteller des Domänenzertifikats übereinstimmt. Somit wird bei jeder E-Mail die eigentliche Absenderadresse (zum Beispiel max.mustermann@meinefirma.tld) in den „reply to“ Header geschrieben und Inhalt des „from“ Header (max.mustermann@meinefirma.tld) durch die Adresse des Antragstellers des Zertifikates (zum Beispiel signatur@meinefirma.tld) ersetzt.

Antwortet der Empfänger einer solchen E-Mail direkt, so wird die Adresse des „reply to“ Headers verwendet und alles funktioniert wie erwartet.

Nimmt der Empfänger jedoch den Absender der E-Mail in sein Adressbuch auf (Max, Mustermann), so wird unter dessen Namen nicht wie erwartet die E-Mail Adresse (max.mustermann@meinefirma.tld) des angezeigten Absenders (max.mustermann@meinefirma.tld) in das Adressbuch übernommen, sondern die umgesetzte Adresse aus dem „from“ Header (signatur@meinefirma.tld). Sendet der ursprüngliche Empfänger nun eine E-Mail an den ursprünglichen Absender max.mustermann@meinefirma.tld, so wird diese an signatur@meinefirma.tld anstatt max.mustermann@meinefirma.tld gesendet.

Ebenso werden sogenannte Non Delivery Reports (NDR) immer an den tatsächlichen Absender einer E-Mail gesendet. Das heißt, erreicht die E-Mail eines Absenders aus der Domäne meinefirma.tld den externen Empfänger gar nicht, so wird der NDR statt an den ursprünglichen Absender an signatur@meinefirma.tld gesendet. Somit ist für den Absender nicht ersichtlich, dass seine E-Mail nicht zugestellt wurde.

Fazit:

Je länger mit einer Domänen Signatur gearbeitet wird, desto mehr und desto häufiger werden E-Mails – irrtümlich – an die Antragsteller Adresse aus dem Zertifikat gesendet. Das heisst auch, dieses Postfach muss in regelmäßigen, kurzen Abständen von einer Person überprüft und die falsch zugestellten E-Mails manuell an die richtigen Empfänger (sofern überhaupt möglich/erkennbar) weitergeleitet werden. Unterbleibt dies, können daraus nicht zuletzt rechtliche Nachteile entstehen.

Vom Verwenden dieser Option ist deshalb dringendst abzuraten!

Konsequenterweise wurde die entsprechende Option mit der Version 10.0 der SEPPmail Appliance aus der Administrationsoberfläche entfernt.

9.125 Signatur: Unterschiedliche Prüfergebnisse

Ausgangssituation:

Bei einer eingehenden, signierten E-Mail wurde die Signatur von der SEPPmail Appliance als gültig erkannt. Im Betreff der E-Mail ist das entsprechende Kennzeichen (im Standard [signed OK]) zu sehen. Die SEPPmail Appliance ist so konfiguriert, dass erfolgreich geprüfte Signaturen nicht abgeschnitten werden. Im empfangenden E-Mail Client wird nun die Signatur jedoch als ungültig angezeigt. Wird die Signatur im Detail geprüft, lautet die Meldung, dass

a) die E-Mail verändert worden sei.

Ursache:

1. Die E-Mail wurde zwischen SEPPmail Appliance und E-Mail Client durch einen unbefugten Dritten verändert. Bei korrekter Konfiguration der Systeme ist der Weg von der SEPPmail Appliance bis zum E-Mail Client verschlüsselt und diese Möglichkeit somit ausgeschlossen.
2. Zwischen SEPPmail Appliance und dem E-Mail Client wurde die E-Mail durch ein dazwischen liegendes Relay verändert (zum Beispiel ein Zeilenumbruch oder ähnliches).

Individuelle Abhilfe:

In diesem Fall wären die dazwischenliegenden Relays zu prüfen.

3. Der Absender hat beim Signieren der E-Mail das Padding-Verfahren RSA-PSS verwendet, der E-Mail Client kann jedoch mit diesem Verfahren nicht umgehen. RSA-PSS wird zum Beispiel nach EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) gefordert. Da die SEPPmail Appliance mit diesem Standard umgehen kann, wird die Signatur hier als gültig erkannt. Da die meisten E-Mail Clients jedoch nicht mit RSA-PSS umgehen können, erkennen diese die Signatur als ungültig.

Individuelle Abhilfe:

Erfolgreich geprüfte Signaturen sollten von der SEPPmail Appliance abgeschnitten werden (siehe **Mail Processing** ^[286] **Ruleset generator** ^[287] **Signing** ^[298] **Incoming e-mails** ^[298] Remove signature if S/MIME signature check succeeds ^[299]).

Hinweis:

Aufgrund dieser Problematik wird dringend vom Verwenden des Padding-Verfahrens RSA-PSS als globale Einstellung für das Signieren abgeraten.

b) das Zertifikat von einer unbekannten Zertifizierungsstelle stammt

Ursache:

4. Die ausstellende CA ist an der SEPPmail Appliance unter „X.509 Root Certificates“ vorhanden und als „trusted“ eingestuft. Im E-Mail Client ist dieselbe CA nicht bekannt oder als „untrusted“ eingestuft.
5. Die Signatur wurde beim Absender nicht RFC konform erstellt. Benötigte Zwischenzertifikate fehlen. Auf der SEPPmail Appliance sind die fehlenden Zwischenzertifikate bekannt, weshalb die Zertifikatskette nachvollzogen und die Herkunft des Zertifikats dennoch festgestellt werden kann. Am E-Mail Client sind die Zwischenzertifikate nicht bekannt. Die Zertifikatskette ist dort somit nicht bekannt. Die Herkunft des Zertifikats kann somit nicht festgestellt werden.

Individuelle Abhilfe:

Zwischenzertifikate dezentral in den E-Mail-Clients importieren.

c) der Absender der E-Mail nicht mit dem Antragsteller des Zertifikats in der Signatur übereinstimmt.

Ursache:

Für das Verifizieren des Absenders einer E-Mail prüft die SEPPmail Appliance sowohl den FROM-, wie auch den SENDER- Header auf das Übereinstimmen mit dem Antragsteller des Zertifikates. Der eingesetzte E-Mail Client prüft anhand anderer Kriterien auf das Übereinstimmen des Absenders mit dem Antragsteller des Zertifikates.

Individuelle Abhilfe:

Erfolgreich geprüfte Signaturen sollten von der SEPPmail Appliance abgeschnitten werden (Remove signature if S/MIME signature check succeeds).

Generelle Abhilfe:

In der SEPPmail Appliance Konfiguration sollten erfolgreich geprüfte Signaturen abgeschnitten werden (siehe **Mail Processing** ²⁸⁶ **Ruleset generator** ²⁸⁷ **Signing** ²⁹⁸ **Incoming e-mails** ²⁹⁸ Remove signature if S/MIME signature check succeeds ²⁹⁹).

9.126 Signatur: Verwendeter Schlüssel bei Microsoft Vertreterregelung

Ausgangssituation:

Als E-Mail System ist Microsoft Outlook / Exchange im Einsatz. Die Microsoft proprietäre Funktion „Senden im Auftrag von“ soll zum Einsatz kommen.

Frage:

Welcher Schlüssel wird bei einer über MS-Exchange Vertreterregelung gesendeten E-Mail verwendet?

Antwort:

Für das Versenden von E-Mails mittels „Senden im Auftrag von“, werden die Header gemäss der Tabelle unten gesetzt. Dabei sendet **Max Mustermann** als **Vertreter** des Sammelpostfachs **Support** (Vertretener), also „**max.mustermann@firma.tld** im Auftrag von **support@firma.tld**“.

	Vertreter	Vertretener
Name	Max Mustermann	Support (Sammelpostfach)
SMTP-Adresse	max.mustermann@firma.tld	support@firma.tld
Envelope-Sender	X	
From-Header		X
Sender-Header	X	

Die SEPPmail Appliance zieht im Standard den **Absender** aus dem **From-Header** für die Auswahl des Signaturzertifikates heran. Somit wird mit dem Schlüssel des **Vertretenen** signiert. Dadurch wird die Signatur von allen üblichen E-Mail Clients als gültig erkannt, sofern die E-Mail auf dem Übertragungsweg nicht verändert wurde.

9.127 Signatur: Zum Signieren verwendetes Zertifikat

Ausgangssituation:

Auf der SEPPmail Appliance liegen für einen **User**^[396] mehrere gültige Zertifikate vor.

Frage:

Welches der Zertifikate eines **Users**^[396] wird für das Signieren verwendet?

Antwort:

Für das Signieren wird jeweils der Schlüssel / das Zertifikat des Absenders mit der längsten Gültigkeit herangezogen. Generell gilt jedoch, per **MPKI**^[339] ausgestellte Zertifikate werden bevorzugt zur Signierung verwendet („Bonus“ von 10 Jahren). Damit wird verhindert, dass „Umsteiger“, welche zunächst Zertifikate einer selbst signierten Zertifizierungsstelle (diese stellt in der Standard-Einstellung Zertifikate mit einer Laufzeit von zehn Jahren aus) im Einsatz hatten, weiterhin mit diesen Zertifikaten anstatt der über die **MPKI**^[339] bezogenen Trusted Zertifikate (diese werden in der Regel mit einer Laufzeit von nur einem Jahr ausgestellt) signieren (siehe auch **Mail Processing**^[286] **Ruleset generator**^[287] **Signing**^[298] **Outgoing e-mails**^[300]).

9.128 Signatur: Gründe einer ungültigen Signatur

Ausgangssituation:

Die SEPPmail Appliance ist so konfiguriert, dass S/MIME Signaturen eingehender E-Mail geprüft werden.

Frage:

Was sind die Gründe für das Einstufen einer Signatur als ungültig?

Antwort:

Beim Überprüfen einer S/MIME E-Mail Signatur werden folgende Gegebenheiten überprüft:

1. Stammt das Zertifikat, mit welchem die Signatur ausgeführt wurde von einer vertrauenswürdigen CA?
Um dies überprüfen zu können muss die Signatur Kette bekannt sein, das heißt
 - a. das Root CA Zertifikat der ausstellenden CA im Menü **X.509 Root Certificates** ^[480] gelistet sein und den **Trust state** ^[480] **trusted** aufweisen.
 - b. gegebenenfalls benötigte Zwischen- oder auch Intermediate-Zertifikate bekannt sein
Laut RFC müssen diese Zwischenzertifikate ebenfalls bei signieren beigefügt werden. Ist dies dennoch nicht der Fall, so kann die Kette dennoch ergänzt werden, sofern die Zwischenzertifikate ebenfalls unter **X.509 Root Certificates** ^[480] (eingerückt) gelistet sind.
2. Stimmt der Antragsteller des Zertifikates (CN, Common Name) mit dem Absender der E-Mail (From-Header) überein
3. Wurde die E-Mail nach dem Signieren verändert?
Mögliche Gründe hierfür sind
 - a. mutwillig durch einen Dritten
 - b. durch das Anhängen zum Beispiel eines Disclaimers nach dem Signieren
 - c. durch ein ungewolltes Umcodieren an einem zwischengelagerten E-Mail Server

Siehe gegebenenfalls auch **Mail Processing** ^[286] **Ruleset generator** ^[287] **Signing** ^[298] **Incoming e-mails** ^[298]
Add this text to message subject if S/MIME signature check succeeds ^[298] **Hinweis**, beziehungsweise
Signatur: Unterschiedliche Prüfergebnisse ^[829].

9.128.1 Barracuda

Ausgangssituation:

Im E-Mail Strom ist eine Barracuda Schutzkomponente. Signierte E-Mails kommen mit zerstörter Signatur an.

Abhilfe:

In der Barracuda Schutzkomponente die Option

LinkProtect in Inbound > Anti Phishing
deaktivieren.

Weiterführende Information:

<https://campus.barracuda.com/product/essentials/doc/49055519/understanding-link-protection/>

9.129 Sophos UTM: Erneute Virenprüfung nach dem Entschlüsseln

Ausgangssituation:

Die SEPPmail Appliance soll in eine bestehende E-Mail-Infrastruktur integriert werden. Als vorgelagertes AntiSpam Relay ist bereits ein Sophos UTM vorhanden. Um dort auch eingehende, verschlüsselte E-Mails scannen zu können, sollen von der SEPPmail Appliance entschlüsselte E-Mails erneut an Sophos UTM gesendet werden, ohne dabei eine Loop zu erzeugen.

Lösung:

Sophos UTM sendet generell alle E-Mails an die SEPPmail Appliance. Diese entscheidet aufgrund zu setzender Kennzeichen (X-Header), ob die E-Mail für einen erneuten Scan an Sophos UTM, oder an den internen E-Mails-Server gesendet werden soll (siehe auch [Routing auf der SEPPmail Appliance](#) ⁸⁴).

9.129.1 Vorbereitung auf Sophos UTM

Auf der UTM müssen die eingehenden E-Mails zur SEPPmail weitergeleitet werden. Die UTM darf dabei keinen Footer im SMTP Proxy setzen, da dieser sonst die Struktur einer S/MIME verschlüsselten E-Mail zerstört.



Checkbox nicht aktivieren

9.129.2 Erforderliche Aktionen auf der SEPPmail Appliance

Die SEPPmail Appliance muss eingehende E-Mails für ihre **Managed Domains** an die internen E-Mail Server weiterleiten (siehe **Mail System** Spalte **Server IP address**). Damit E-Mails nach dem Entschlüsseln durch die SEPPmail Appliance noch einmal zu Sophos UTM geschickt werden, muss zunächst über das Regelwerk (**Mail Processing** **Ruleset generator** **Header tagging**) der Header **X-SEPPmail-STATUS** auf den Wert **DECRYPT** für alle entschlüsselten E-Mails (For all mails that have been decrypted) gesetzt und aktiviert werden:

Header tagging	☐ Set header	X-	to value		For all incoming mails
	☐ Set header	X-	to value		For all outgoing mails
	☐ Set header	X-	to value		For all mails that have been encrypted
	☒ Set header	X-SEPPMAIL-STATUS	to value	DECRYPT	For all mails that have been decrypted

Somit werden entschlüsselte E-Mails mit dem X-Header **X-SEPPmail-STATUS** mit dem Wert **DECRYPT** versehen.

Per „Custom command“ (**Mail Processing** **Ruleset generator** **Custom commands**) kann nun dieser Header nach dem Entschlüsseln ausgewertet und auf den Wert **RESEND** umgeschrieben werden, bevor die E-Mail erneut zu Sophos UTM (im folgenden Beispiel mit der IP-Adresse **192.168.10.1**) gesendet wird. Hierfür ist in den **Custom commands for incoming e-mails AFTER decryption** folgender Code notwendig:

Zeile	Code
01	# Begin: Custom commands for incoming e-mails AFTER decryption
02	log(1, 'Begin: Custom commands for incoming e-mails AFTER decryption');
03	if (compare('X-SEPPmail-STATUS', 'substitute', 'DECRYPT')) {
04	log(1, 'send decrypted e-mail from \$header_from for recipient(s) \$header to \$header cc back to UTM for content scanning');
05	setheader('X-SEPPmail-STATUS', 'RESEND');
06	deliver('192.168.10.1');
07	}
08	log(1, 'End: Custom commands for incoming e-mails AFTER decryption');
09	# End: Custom commands for incoming e-mails AFTER decryption

Code

Damit auch via GINA generierte E-Mails durch Sophos UTM geprüft werden, ist weiterhin unter **Custom commands for e-mails from GINA** folgender Code erforderlich:

Zeile	Code
01	# Begin: Custom commands for e-mails from GINA
02	log(1, 'Begin: Custom commands for e-mails from GINA');
03	log(1, 'send e-mail from GINA from sender \$header_from for recipient(s) \$header to \$header cc back to UTM for content scanning');
04	setheader('X-SEPPmail-STATUS', 'RESEND');
05	deliver('192.168.10.1');
06	log(1, 'End: Custom commands for e-mails from GINA');
07	# End: Custom commands for e-mails from GINA

Code

Damit die E-Mail nach erneutem Erhalt von der Sophos UTM durch die SEPPmail Appliance nicht erneut dorthin, sondern nun an den Standard E-Mail Server der jeweiligen **Managed Domain** gesendet wird, wird bereits vor dem eigentlichen Verarbeiten der E-Mail erneut der X-Header Eintrag **X-SEPPmail-STATUS** geprüft. Aufgrund des ersten Durchlaufs durch die SEPPmail Appliance hat dieser X-Header nun den Wert **RESEND**, worauf SEPPmail

Appliance an die, der **Managed Domain** [247] zugeordneten **Server IP address** (siehe oben) sendet. Damit wird auch verhindert, dass die bereits im ersten SEPPmail Appliance-Durchlauf gesetzten Kennzeichen (im Standard [secure], [signed OK], [signed INVALID] siehe auch **Mail Processing** [286] **Ruleset generator** [287] **Encryption** [292] **Incoming e-mails** [292] beziehungsweise **Signing** [298] **Incoming e-mails** [298])

Encryption	Incoming e-mails ☒ Add this text to message subject after decryption: \[secure\] ☐ Set confidential flag after decryption ☐ Reject mails if S/MIME decryption fails
Signing	Incoming e-mails ☒ Add this text to message subject if S/MIME signature check succeeds: \[signed\sOK\] ☒ Add this text to message subject if S/MIME signature fails: \[signed\sINVALID\]

aus dem Betreff der E-Mail entfernt werden.

Die entsprechende Anweisung hierfür ist unter **Custom commands for incoming e-mails BEFORE decryption**: [308] wie folgt vorzunehmen:

Zeile	Code
01	# Begin: Custom commands for incoming e-mails BEFORE decryption
02	log(1, 'Begin: Custom commands for incoming e-mails BEFORE decryption');
03	if (compare('X-SEPPmail-STATUS', 'substitute', 'RESEND')) {
04	log(1, 'decrypted e-mail, resent after content scanning, delivering without further actions');
05	rmheader('X-SEPPmail-STATUS');
06	if (!compare('subject', 'match', '\[secure\]')) {tagsubject('[secure]');
07	tagsubject('[secure]');
08	}
09	deliver();
10	}
11	log(1, 'End: Custom commands for incoming e-mails BEFORE decryption');
12	# End: Custom commands for incoming e-mails BEFORE decryption

Code

9.130 Verschlüsselung: Globales Unterdrücken oder Forcieren kryptographischer Aktionen

Ausgangssituation:

Von einer oder mehreren **Managed domains** [247] oder einzelnen daraus stammenden E-Mail Adressen gesendete E-Mails oder E-Mails an bestimmte Empfänger Domänen oder Adressen oder eine Kombination daraus sollen generell in einer bestimmten Art und Weise kryptographisch behandelt werden.

Frage:

Können parallel zum globalen Ruleset weitere Regeln für eine spezielle E-Mail Verarbeitung angelegt werden?

Antwort:

Ja, das entsprechende Konfigurationsmenü (**ENCRYPTION POLICY** [313]) wird unter **Mail Processing** [286] mittels **Edit policy table...** aufgerufen. Die Möglichkeiten der **ENCRYPTION POLICY** [313] sind unter **Add/Edit Encryption Policy** [314] beschrieben.

9.131 Verschlüsselung: Domänenverschlüsselung mit einem Dritthersteller-System

Ausgangssituation:

Zu einem Kommunikationspartner, welcher ein Verschlüsselungsgateway eines anderen Herstellers einsetzt soll eine bidirektionale Domänenverschlüsselung eingerichtet werden.

Lösung:

Sofern das Verschlüsselungs-Gateway des Kommunikationspartners diese Funktion ebenfalls unterstützt, müssen die öffentlichen Domänenschlüssel (bevorzugt S/MIME, wobei auch OpenPGP möglich ist) zwischen den Kommunikationspartnern ausgetauscht werden.

Einrichten der Domänenverschlüsselung zum Kommunikationspartner:

Nach dem Prüfen des Fingerprints/Hashs des öffentlichen Domänenschlüssels des Kommunikationspartners kann dieser unter **Domain Certificates** ^[489], je nach Schlüsselmaterial via **S/MIME domain certificates...**, beziehungsweise **OpenPGP domain keys...** importiert werden.

Bereitstellen des eigenen öffentlichen Domänenschlüssels für den Kommunikationspartner:

Der öffentliche Domänenschlüssel der SEPPmail Appliance kann vom Kommunikationspartner direkt über die GINA-Oberfläche heruntergeladen werden, sofern diese Funktion freigeschaltet ist (siehe **CHANGE GINA SETTINGS FOR** ^[423] **Extended settings** ^[431] **Allow download of public domain keys/domain certificates** ^[434]). Das Prüfen des Fingerprints, beziehungsweise Hashs des öffentlichen Domänenschlüssels entfällt an dieser Stelle, da der Schlüssel in diesem Fall über einen SSL gesicherten Kanal bezogen wurde.

Andernfalls ist der Schlüssel in den Detailsinstellungen der jeweiligen **Managed domain** ^[247] **EDIT MANAGED DOMAIN** ^[266] unter **S/MIME domain encryption** ^[274], beziehungsweise **OpenPGP domain encryption** ^[274] herunterzuladen und dem Kommunikationspartner zur Verfügung zu stellen. Erfolgte das Übermitteln auf einem ungesicherten Kanal (zum Beispiel unverschlüsselte E-Mail) so sollte der Fingerprint, beziehungsweise Hash des öffentlichen Domänenschlüssels vom Kommunikationspartner vor dem Verwenden unbedingt überprüft werden.

9.132 Verschlüsselung: Domänenverschlüsselung zu einer anderen SEPPmail Appliance

Ausgangssituation:

Zu einem Kommunikationspartner, welcher ebenfalls eine SEPPmail Appliance im Einsatz hat, soll eine bidirektionale Domänenverschlüsselung eingerichtet werden.

Lösung:

Aufgrund des SEPPmail **Managed Domain Service** ^[31] werden die öffentlichen Domänenschlüssel aller SEPPmail Appliances automatisch untereinander ausgetauscht. Somit werden alle E-Mails von und zu Kommunikationspartnern, welche eine SEPPmail Appliance betreiben automatisch mindestens über diesen Service verschlüsselt. Somit ist über diesen Service - entgegen der manuell eingerichteten **Domänen-Verschlüsselung** ^[31] - in der Regel sichergestellt, dass auch Antworten des Kommunikationspartner mindestens über diesen Service verschlüsselt ankommen. Weiterhin sind über den **Managed Domain Service** ^[31] im Gegensatz zu den anderen Verschlüsselungsvarianten auch die Betreffzeilen der E-Mail verschlüsselt.

9.133 Verschlüsselung: Domänenzertifikat mit Aussteller (Issuer)

Ausgangssituation:

Der Kommunikationspartner fordert entgegen des RFC für die Domänenverschlüsselung ein S/MIME Zertifikat mit Zertifikatskette (Aussteller). Das selbst generierte Zertifikat der Managed Domain enthält jedoch keinen Aussteller.

Frage:

Kann die SEPPmail Appliance auch Domänenzertifikate von einem eigenen Aussteller (Issuer) erzeugen?

Antwort:

Ja. Hierzu wird zunächst die **CA** ^[328] innerhalb der SEPPmail Appliance eingerichtet. Jedes danach erstellte Domänenzertifikat wird von dieser **CA** ^[328] ausgestellt und enthält diese somit als Antragsteller. Dem Kommunikationspartner müssen somit für das Einrichten der Domänenverschlüsselung sowohl das nach dem Einrichten der **CA** ^[328] erstellte Domänenzertifikat (siehe auch **Domänenverschlüsselung mit einem Dritthersteller-System** ^[835]), sowie das Root-Zertifikat der internen **CA** ^[328] übergeben werden. Dabei kann das Root-Zertifikat der **CA** ^[328] gegebenenfalls ebenso über die GINA-Oberfläche bereitgestellt werden, wie die Domänenzertifikate (siehe **CHANGE GINA SETTINGS FOR** ^[423] **Extended settings** ^[431] **Publish local CA certificate on the search page to allow recipients to perform S/MIME signature verification** ^[434]).

Alternativ könnte auch ein Kauf-Zertifikat einer akkreditierten CA in den Detailsinstellungen der jeweiligen **Managed domain** ^[247] **EDIT MANAGED DOMAIN** ^[266] unter **S/MIME domain encryption** ^[274] eingebunden und dem Kommunikationspartner bereit gestellt werden.

9.134 Verschlüsselung: E-Mails von Google nicht lesbar

Ausgangssituation:

E-Mails von Absendern, deren E-Mail Domäne bei Google hosted sind, werden auf der SEPPmail Appliance zwar als **[signed OK]** gekennzeichnet, jedoch nicht entschlüsselt. Somit können sie vom internen Empfänger nicht gelesen werden.

Im **Log** der SEPPmail Appliance zur betroffenen E-Mail ist folgender Hinweis zu finden:

INFO Found possible S/MIME encryption in incorrectly nested MIME structure: application/pkcs7-mime

Ursache:

Laut RFC müssen E-Mails erst signiert und dann verschlüsselt werden. Diese Reihenfolge resultiert aus der Tatsache, dass durch das Entschlüsseln lesbar gemacht und somit verändert wird. Würde die Signatur also nach dem Verschlüsseln aufgebracht, so wird diese, durch das Verändern des Inhalts beim Entschlüsseln, zerstört.

Google propagiert derzeit seine GSuite Lösung inklusive E-Mail Verschlüsselung. Entgegen des RFC wird von Google jedoch erst verschlüsselt und dann signiert.

Die SEPPmail Appliance stoppt daher bei eingehenden E-Mails - RFC-konform - nach dem Prüfen der Signatur jegliches weitere kryptographische Verarbeiten. Somit gelangen von Google verschlüsselte E-Mails zwar signaturgeprüft, jedoch unentschlüsselt in die Postfächer der Empfänger.

Lösung:

Nachdem Gespräche seitens SEPPmail mit Google diesbezüglich bisher erfolglos blieben, bleibt folgender Workaround:

Wie im folgenden Beispiel-Code dargestellt, wird über die **Custom commands for incoming e-mails BEFORE decryption** zunächst geprüft, ob eine E-Mail bekanntermaßen von einer Google hosted E-Mail Domäne stammt (**Zeile 05**). Ist dies der Fall, so wird geprüft, ob die E-Mail signiert ist (**Zeile 07**) und die Signatur entfernt (**Zeile 08**). Somit kann die E-Mail im weiteren Verlauf des Regelwerks entschlüsselt werden.

Zeile	Code
01	# Begin: Custom commands for incoming e-mails BEFORE decryption
02	log(1,'Begin: Custom commands for incoming e-mails BEFORE decryption');
03	# Begin: check for sender domains hosted by Google
04	log(1,'Begin: check for sender domains hosted by Google');
05	if (compare('from', 'match', 'sender-domain1\.tld sender-domain2\.tld sender-domainn\.tld')) {
06	log(1,'found Google hosted sender domain, removing signature if exists');
07	if (smime signed()) {
08	delete smime sig();
09	}
10	}
11	log(1,'End: check for sender domains hosted by Google');
12	# End: check for sender domains hosted by Google
13	log(1,'End: Custom commands for incoming e-mails BEFORE decryption');
14	# End: Custom commands for incoming e-mails BEFORE decryption

[Code](#)

9.135 Verschlüsselung: Lokal abliegende E-Mails erneut entschlüsseln

Ausgangssituation:

Im E-Mail Client des Benutzers liegen verschlüsselte und somit für ihn nicht lesbare E-Mails ab.

Ursache:

1. Schlüsselmaterial wurde von einer dezentralen Verschlüsselungsstruktur auf die zentrale SEPPmail Appliance migriert. Die noch verschlüsselt im Client abliegenden E-Mails können daher nicht mehr gelesen werden.
2. E-Mails gelangen an der SEPPmail Appliance vorbei bis zum Internen E-Mail Server

Individuelle Abhilfe:

Der E-Mail Fluss ist so zu steuern, dass alle eingehenden E-Mails über die SEPPmail Appliance geroutet werden.

3. Die SEPPmail Appliance kann die eingehenden E-Mails nicht entschlüsseln, ist aber so konfiguriert, dass Sie diese nicht ablehnt (siehe **Mail Processing** [286] **Ruleset generator** [287] **Encryption** [292] **Incoming e-mails** [292] **Reject mails if S/MIME decryption fails** [293])

Individuelle Abhilfe:

- a. **Reject mails if S/MIME decryption** [293] **fails** [293] aktivieren
- b. Prüfen, woher die so verschlüsselten E-Mails kommen. Eventuell ist der **Managed Domain Service** [31] für eine Domäne freigeschaltet, welche den passenden privaten Schlüssel nicht zur Verfügung haben (siehe auch **EDIT MANAGED DOMAIN** [266] **Settings** [266] **S/MIME domain keys** [267] **Create S/MIME domain keys for managed domain encryption for this domain and send public key to vendor pool** [268]).

Frage:

Wie können im E-Mail Client lokal abliegende verschlüsselte E-Mails entschlüsselt werden?

Antwort:

Zunächst muss die Option **Reprocess mails sent to reprocess@decrypt.reprocess** [288] (siehe **Mail Processing** [286] **Ruleset generator** [287] **General settings** [288]) aktiviert sein.

Der Benutzer muss die verschlüsselte E-Mail als Anhang in eine neue (Träger-)E-Mail (**nicht weiterleiten!!!**) packen und an die Adresse „reprocess@decrypt.reprocess“ senden. Auf der SEPPmail Appliance wird die Träger-E-Mail verworfen und die darin befindliche, ursprünglich verschlüsselte Nachricht erneut verarbeitet und zugestellt. Dies setzt natürlich voraus, dass der für das Entschlüsseln benötigte private Schlüssel der SEPPmail Appliance bekannt ist.

9.136 Verschlüsselung: Outlook Confidential Flag trotz gegenteiliger Einstellung gesetzt

Ausgangssituation:

Auf der SEPPmail Appliance wurde das Kennzeichnen entschlüsselter E-Mails via Sensitivity-Header (in MS Outlook Confidential-Flag) abgestellt (siehe **Set confidential flag after decryption**^[293]). Dennoch ist dieser Header bei einigen eingehenden E-Mails gesetzt und mit dem Wert „comany-confidential“ belegt. Dies führt zum Beispiel beim Einsatz von IBM Notes dazu, dass die E-Mail weder weitergeleitet noch gedruckt werden kann.

Frage:

Weshalb ist der Header Sensitivity trotz anders lautender Einstellung gesetzt?

Antwort:

Wurde der Header durch den Absender bereits vor dem Verschlüsseln auf die Vertraulichkeitsstufe / sensitivity „company-confidential“ gesetzt, so bleibt dieser auch nach dem Entschlüsseln durch die SEPPmail Appliance erhalten. Das heisst der Header wird durch die SEPPmail Appliance nach der Entschlüsselung NICHT entfernt.

Falls gewünscht, können Header - in diesem Fall Sensitivity - generell über **Custom commands**^[308] entfernt werden. Für den speziellen Fall wäre somit die Option **Custom commands for incoming e-mails AFTER decryption**^[308] zu aktivieren und folgender Befehl in das darunter liegende Eingabefeld einzutragen:

Zeile	Code
01	# Begin: Custom commands for incoming e-mails AFTER decryption
02	log(1, 'Begin: Custom commands for incoming e-mails AFTER decryption');
03	# Begin: Remove sensitivity header from incoming e-mails
04	log(1, 'Begin: Remove sensitivity header from incoming e-mails');
05	if (compare('sensitivity', 'match', '*.*')) {
06	rmheader('sensitivity');
07	log(1, 'sensitivity header found and removed');
08	}
09	log(1, 'End: Remove sensitivity header from incoming e-mails');
10	# End: Remove sensitivity header from incoming e-mails
11	log(1, 'End: Custom commands for incoming e-mails AFTER decryption');
12	# End: Custom commands for incoming e-mails AFTER decryption

[Code](#)

Diese Aktion ist durch Klicken von **Save and Create ruleset** abzuschließen.



Hinweis:

Das Entfernen des Headers muss unbedingt nach dem Entschlüsseln (**Custom commands for incoming e-mails AFTER decryption**^[308]) erfolgen. Somit wird sichergestellt, dass auch eingehende, mittels **Managed Domain Service**^[311] verschlüsselte E-Mails entsprechend behandelt werden.

9.137 Verschlüsselung: TLS als gültige Verschlüsselungsvariante

Ausgangssituation:

TLS wird als eine mögliche, zur Verfügung stehende Verschlüsselungsvariante genannt. In der Praxis zeigt sich jedoch, dass TLS immer nur eine zusätzliche Sicherheitsoption ist, die in Verbindung mit einem anderen Verfahren (S/MIME, OpenPGP, GINA) zum Einsatz kommt.

Frage:

Kann TLS auch als weitere, alleinige Verschlüsselungsvariante konfiguriert werden?

Antwort:

TLS ist im Gegensatz zu den anderen genannten Verfahren keine Inhalts-, sondern lediglich eine Transport-(Verbindungs-)Verschlüsselung. Somit kann TLS immer nur bis zum nächsten E-Mail System gewährleistet werden. Da E-Mails jedoch meist über mehrere E-Mail Systeme geroutet werden, ist mit TLS in der Regel keine durchgängige Verschlüsselung zu gewährleisten.

Aus diesem Grund taucht TLS per Standard nicht in der **Verschlüsselungshierarchie** [66] auf.

Jedoch kann unter gewissen Gegebenheiten TLS als weitere Verschlüsselungstechnologie in die **Verschlüsselungshierarchie** [66] mit aufgenommen werden:

- Die SEPPmail Appliance bildet den Übergang zum Internet
Das heißt E-Mails werden direkt an den Empfänger adressiert.
- Der Empfänger hat signalisiert, dass sein aus dem Internet E-Mail empfangendes System in seinem eigenen Netzwerk liegt.
- Auf der SEPPmail Appliance wurde zu diesem Kommunikationspartner unter **Mail System** [247] **TLS settings** [251] die TLS-Verschlüsselung mit einem Grad höher „may“ (siehe **ADD TLS DOMAIN** [282] **TLS settings** [282]) eingerichtet.

Das eigentliche Einbinden in die **Verschlüsselungshierarchie** [66] erfolgt abschließend durch Aktivieren der Option „Consider „forced TLS“ as encrypted“ unter **Mail Processing** [286] **Ruleset generator** [287] **Encryption** [292]

Outgoing e-mails [293]

Fortan würde TLS an die entsprechend eingerichteten Zieldomänen als zulässiges Verschlüsselungsverfahren, noch vor GINA zum Einsatz kommen.

TLS kommt weiterhin als zusätzliche Verschlüsselungsmethode immer zum Einsatz.

9.138 Verschlüsselung: Verwenden abgelaufener OpenPGP-Schlüssel

Ausgangssituation:

Die SEPPmail Appliance ist so eingestellt, dass auch abgelaufene S/MIME Zertifikate für das Verschlüsseln verwendet werden, sofern kein aktuelles **X.509 Certificate** vorhanden ist (siehe **ADVANCED SETTINGS** **Advanced settings**, **Expiration**, beziehungsweise **Policies** **Refuse usage of expired certificates for encryption**).

Frage:

Können auch abgelaufene **OpenPGP Public Keys** weiterhin für das Verschlüsseln benutzt werden?

Antwort:

Nein. Technologiebedingt ist dies nicht möglich. Sollte kein weiterer, gültiger OpenPGP-Key vorhanden sein, so wird je nach Konfiguration entweder ein alternatives Verschlüsselungsverfahren angewandt, oder die E-Mail abgewiesen (bounced).

9.139 Verschlüsselung: Verwendetes Zertifikat

Ausgangssituation:

Auf der SEPPmail Appliance liegen für einen Kommunikationspartner unter **X.509 Certificates**^[47] mehrere gültige Zertifikate vor.

Frage:

Welches der vorhandenen Zertifikate wird für das Verschlüsseln verwendet?

Antwort:

Die E-Mail – beziehungsweise genauer, der symmetrische Session-Key – wird jeweils mit allen gültigen, unter **X.509 Certificates**^[47] vorhandenen Zertifikaten des Empfängers verschlüsselt. Der Empfänger kann die E-Mail somit mit jedem, zu einem dieser Zertifikate gehörigen Schlüssel entschlüsseln.

Sollten ausschließlich abgelaufene Zertifikate des Empfängers bekannt sein, so wird das aktuellste dieser Zertifikate für das Verschlüsseln herangezogen.

9.140 Zertifikate: SwissSign: Einlösen von Vouchers

Ausgangssituation:

In der Regel zu Testzwecken wurden von SwissSign sogenannte Vouchers bereit gestellt, um darüber Zertifikate, beziehungsweise Schlüsselpaare zu beziehen. Die so bezogenen Zertifikate sollen im Anschluss als Bulk Import in die SEPPmail Appliance importiert werden.

Frage:

Wie beziehe ich SwissSign Zertifikate mittels der bereit gestellten Vouchers?

Antwort:

Zum Einlösen der Vouchers ist wie folgt vorzugehen:

- Öffnen der Seite folgenden Link:
www.swisssign.net

- Klicken der Schaltfläche **Weiter ohne Konto**

The screenshot shows the SwissSign AG [CH] website. The navigation bar includes links for Startseite, Support, Zertifizierungsstelle, Shop, Zertifikat für ungültig erklären, and Help. The main heading is 'Zertifikate Suchen / Verwalten'. On the left, there are sections for 'Konto' (Anmelden, Erstellen) and 'Login mit Zertifikat' (Anmelden). The main content area has a 'Konto anmelden' section with a note: 'Ein Konto ist optional und ist unabhängig vom Shop bei swisssign.com'. Below this is a 'Neue Benutzer' section with options: 'Weiter ohne Konto (schnelle Einzelzertifikatsanforderung)' and 'Konto erstellen (um mehrere Zertifikate zu verwalten)'. On the right, there is an 'Anmelden' form with fields for 'Benutzername' and 'Passwort', and a 'Weiter ohne Konto' button highlighted with a red box.

- Klicken von **Neu**

The screenshot shows the SwissSign AG [CH] website. The navigation bar is the same. The main heading is 'Zertifikate Suchen / Verwalten'. On the left, there is a 'Zertifikate' section with a 'Neu' button highlighted with a red box. Below it are 'Suchen / Verwalten', 'Konto', and 'Login mit Zertifikat'. The main content area has an 'Öffentliche Suche' section with a 'Text suchen' field, a 'Lizenz' field, and a 'Seitengröße' field. A 'Suchen' button is at the bottom.

- Eingabe des 24-stelligen Codes für die Testlizenz in das dafür **vorgesehene Feld** und anschließendes Klicken von **Weiter**

The screenshot shows the SwissSign AG [CH] website. The navigation bar is the same. The main heading is 'E-Mail ID Silver Certificate'. On the left, there is a 'Zertifikate' section with a 'Neu' button highlighted with a red box. Below it are 'Suchen / Verwalten', 'Konto', and 'Login mit Zertifikat'. The main content area has an 'Einreichen' section with a 'Gutscheincode' field, a 'Zertifikatslaufzeit' field, and a 'Teilnehmerbedingungen' section. A 'Weiter' button is at the bottom.

- Setzen des **Hakens** für das Akzeptieren der Teilnehmerbedingungen und anschließendes Klicken auf **Ich akzeptiere diese Bedingungen**

SwissSign AG [CH] | <https://swissign.net/mpki/request?account=>

Startseite Support Zertifizierungsstelle Shop Zertifikat für ungültig erklären Help

SwissSign E-Mail ID Silver Certificate

• Zertifikatsgutschein (Lizenz) • Gültigkeit • Teilnehmerbedingungen • CSR • Einreichen

Zertifikate

- Neu
- Suchen / Verwalten

Konto

- Anmelden
- Erstellen

Login mit Zertifikat

- Anmelden

Teilnehmerbedingungen

Teilnehmerbedingungen : ☒ Ich bestätige die Akzeptanz und Einhaltung der Bedingungen der Teilnahmevereinbarung

Zurück **Ich akzeptiere diese Bedingungen**

- Klicken von **Weiter** ohne jegliche weitere Eingabe

SwissSign AG [CH] | <https://swissign.net/mpki/request?account=>

Startseite Support Zertifizierungsstelle Shop Zertifikat für ungültig erklären Help

SwissSign E-Mail ID Silver Certificate

• Zertifikatsgutschein (Lizenz) • Gültigkeit • Teilnehmerbedingungen • CSR • Einreichen

Zertifikate

- Neu
- Suchen / Verwalten

Konto

- Anmelden
- Erstellen

Login mit Zertifikat

- Anmelden

CSR

Fügen Sie Ihre pkcs#10 Zertifikatsregistrierungsanforderung (CSR) ein, falls Sie eine erstellt haben. Ansonsten lassen Sie das Feld leer und fahren Sie weiter.

PKCS#10 :

Zurück **Weiter**

- Eingabe der E-Mail Adresse, für welche das Zertifikat ausgestellt werden soll in das dafür **vorgesehene Feld** und anschließendes Klicken auf **Weiter**

SwissSign AG [CH] | <https://swissign.net/mpki/request?account=>

Startseite Support Zertifizierungsstelle Shop Zertifikat für ungültig erklären Help

SwissSign E-Mail ID Silver Certificate

• Zertifikatsgutschein (Lizenz) • Gültigkeit • Teilnehmerbedingungen • CSR • E-Mail • Kontakt • Einreichen

Zertifikate

- Neu
- Suchen / Verwalten

Konto

- Anmelden
- Erstellen

Login mit Zertifikat

- Anmelden

E-Mail

E-Mail :

Zurück **Weiter**

- Sollten Benachrichtigungen zu diesem Zertifikatsantrag an eine andere Adresse als der für die Zertifikatserstellung genannten gewünscht sein, so ist diese in das dafür **vorgesehene Feld** einzugeben. Anderfalls ist das **Feld** leer zu lassen.
Auswahl der gewünschten Sprache durch Setzen des **Radio Buttons**.
Optionale Eingabe eines **Kommentars**.

Abschließendes Klicken auf **Weiter**

- Überprüfen der zuvor gemachten Angaben, Eingabe eines Passworts in das dafür **vorgesehene Feld** und bestätigen desselben im dafür **vorgesehenen Feld**. Dabei ist darauf zu achten, dass im Falle der Einlösung mehrerer Zertifikatsgutscheine immer das selbe Passwort verwendet wird! Dies ermöglicht im Nachgang einen Bulk Import auf der SEPPmail Appliance.

Abschließendes Klicken auf **Zertifikat anfordern**.

Die heruntergeladenen PKCS#12 Dateien (Dateiendung .p12 oder .pfx) sind in eine ZIP-Datei ohne Ordnerstruktur und Passwort zu packen. Diese ZIP-Datei kann im Anschluss in der Administrationsoberfläche unter **Administration** ³⁶⁹ **Bulk import** ³⁷⁴ **Import X.509 keys and certificates** ³⁷⁴ über die Schaltfläche **Import** unter Angabe der für alle PKCS#12 Dateien gültigen Passphrase importiert werden. Dadurch werden zugleich die zu den Dateien passenden **User** ³⁹⁶ angelegt.

9.141 Zertifikate: Unterstützen von SAN Zertifikaten

Ausgangssituation:

Auf der SEPPmail Appliance sollen MultiDomain, sogenannte Subject Alternate Name (SAN) Zertifikate eingesetzt werden.

Frage:

Unterstützt die SEPPmail Appliance den einsatz von SAN Zertifikaten?

Antwort:

Die SEPPmail Appliance unterstützt

- SSL SAN Zertifikate in allen Modi, also auch für „Virtual Hosting“, sowie beim Generieren und Signieren.
- S/MIME SAN Zertifikate in den Signaturen eingehender E-Mails

9.142 Aktuelle Sicherheitslücken / Exploits

Generell ist die SEPPmail Appliance aufgrund der zum Einsatz kommenden Komponenten und deren Härtung äußerst selten von Sicherheitslücken / Exploits betroffen. Sollte dies dennoch der Fall sein, reagiert SEPPmail innerhalb kürzester Zeit mit einem Sicherheitsupdate (siehe auch [Sicherheit](#) ¹⁰¹).

9.142.1 Amnesia 33**Frage:**

Ist die SEPPmail Appliance von der Amnesia 33 Lücke betroffen?

Antwort:

Nein. Von der Sicherheitslücke sind nur embedded - Systeme betroffen.

SEPPmail Appliance verwendet nur virtuelle Appliances oder standardisierte Serversysteme, zum Beispiel von Hewlett Packard.

9.142.2 Vulnerability in LibreSSLv3.2.2 (CVE-2020-1971)**Frage:**

Ist die SEPPmail Appliance von der Sicherheitlücke Amnesia 33 Lücke CVE-2020-1971 in LibreSSLv3.2.2 betroffen?

Antwort:

Die Schwachstelle ist ab der Version 12.0.9 gepatcht,
Aufgrund des fehlenden Angriffsvektors bestand jedoch auch vor dem Patch keine Gefahr.

9.142.3 GLIBC**Frage:**

Ist die SEPPmail Appliance von der GLIBC Lücke betroffen?

Antwort:

Nein. Die SEPPmail Appliance basiert auf OpenBSD und ist somit nicht betroffen.

9.142.4 Heartbleed**Frage:**

Ist die SEPPmail Appliance von der Heartbleed Bug betroffen?

Antwort:

Nein. Aufgrund der verwendeten Basis-Systeme ist die SEPPmail Appliance davon nicht betroffen.

9.142.5 Poodle**Frage:**

Ist die SEPPmail Appliance von der Poodle Attack betroffen?

Antwort:

Nein. Aufgrund der verwendeten Basis-Systeme ist die SEPPmail Appliance davon nicht betroffen.

9.143 Regularien

9.143.1 EDIFACT

Nachdem die EDIFACT Konformität bereits durch die E-Mail generierenden Instanzen gewährleistet werden muss, ist ein zusätzliches Prüfen im Normalfall nicht notwendig (siehe auch [Regelung zum sicheren Austausch von EDIFACT Übertragungsdateien](#) ^[73]).

Dennoch können durch die SEPPmail Appliance entsprechende Prüfungen, Benachrichtigungen und E-Mail Ausleitungen vorgenommen werden.

9.143.1.1 Zu implementierende Prüfungen

E-Mails, welche den EDI@Energy Vorgaben nicht entsprechen, sollen dem Absender gegenüber abgelehnt werden und zusätzliche mit einem entsprechenden Report an ein internes Postfach gesendet werden.

9.143.1.2 Erforderliche Maßnahmen auf der SEPPmail Appliance

9.143.1.2.1 Erstellen einer E-Mail Vorlage

Für das Generieren der Reports, welcher an die interne Adresse (Clearing-Postfach) gesendet werden sollen, wird vom System eine Schablone benötigt, welche während des Prüfens der Konformität befüllt wird. Diese kann im Text-, im HTML- oder in beiden Formaten erstellt und verwendet werden.

Für das Erstellen der E-Mail Vorlage ist zunächst das Untermenü **LIST TEMPLATE** ^[263] über **Mail System** ^[247] **Edit mail templates...** zu öffnen. Dort ist über die Schaltfläche **Add** eine neue Schablone zu erstellen.

Im Folgemenü ist unter **Create new template** **Template name** der Name der Schablone einzugeben. Dieser muss

EDIFACT_report_attachmail

lauten. Nach dem Generieren der Schablone mittels **Create** wechselt die Ansicht wieder in **LIST TEMPLATE** ^[263].

Hier ist nun unter **Template name** die neue Schablone zu finden. Diese muss mittels  konfiguriert werden.

Im Folgemenü sollte unter **Template settings** ^[264] nun **Name** bereits mit **EDIFACT_report_attachmail** vorgelegt sein. In **Subject** wird der Betreff der zu versendenden Report-E-Mail eingetragen, beispielsweise „EDIFACT Report“. Unter **Advanced** ist der Haken des, beziehungsweise der gewünschten Formate für die Report-E-Mail zu setzen.

9.143.1.2.1.1 Im HTML-Format

Wurde unter **Template settings** ²⁶⁴ **Advanced** der Haken bei **Add HTML part** ²⁶⁴ gesetzt, so kann rudimentär unter **Template as HTML** ²⁶⁴ folgender HTML Code eingegeben werden:

```
<!doctype html public "-//w3c//dtd html 4.01 transitional//en">
<body>
<html lang="de">
<meta charset="UTF-8" />

<p>
<h1>Result</h1>
<br/>
$result
<br/>
</p>

<p>
<h2>E-Mail Metadata</h2>
<br/>

<table border="1">
<thead>
  <tr>
    <th>Header</th>
    <th>Value</th>
  </tr>
</thead>
<tbody>
<tr>
  <td>Direction</td>
  <td>$direction</td>
</tr>
<tr>
  <td>Sender</td>
  <td>$from</td>
</tr>
<tr>
  <td>Recipient</td>
  <td>$to</td>
</tr>
<tr>
  <td>Subject</td>
  <td>$subject</td>
</tr>
<tr>
  <td>Message ID</td>
  <td>$mailid</td>
</tr>
<tr>
  <td>Date</td>
  <td>$date</td>
</tr>
</tbody>
</table>
<br/>
</p>

<p>
<h2>E-Mail Checks</h2>
<br/>
<table border="1">
<thead>
```



```
<tr>
<th>Check</th>
<th>Result</th>
</tr>
</thead>
  <tbody>
    <tr>
      <td>EDI Sender</td>
      <td>${EDIFACTsender}</td>
    </tr>
    <tr>
      <td>EDI Recipient</td>
      <td>${EDIFACTrecipient}</td>
    </tr>
    <tr>
      <td>Subject</td>
      <td>${subject_check}</td>
    </tr>
    <tr>
      <td>Attachment</td>
      <td>${filetype_check}</td>
    </tr>
    <tr>
      <td>Encryption information</td>
      <td>${encryption_check}</td>
    </tr>
    <tr>
      <td>Encryption result</td>
      <td>${encryption_result}</td>
    </tr>
    <tr>
      <td>Signature information</td>
      <td>${signature_check}</td>
    </tr>
    <tr>
      <td>Signature result</td>
      <td>${signature_result}</td>
    </tr>
  </tbody>
</table>
</p>
</html>
</body>
```

[Code](#)

9.143.1.2.1.2 Im Text-Format

Wurde unter **Template settings** ²⁶⁴ **Advanced** ²⁶⁴ der Haken bei **Add text part** ²⁶⁴ gesetzt, so ist unter **Template as text** ²⁶⁵ folgender Text einzugeben:

```
#####
#   Result   #
#####

$result

#####
#   E-Mail Metadata   #
#####

Header                | Value
-----
Direction              | $direction
Sender                 | $from
Recipient              | $to
Subject                | $subject
Message ID             | $mailid
Date                   | $date

#####
#   E-Mail Checks     #
#####

Check                  | Result
-----
EDI Sender             | $EDIFACTsender
EDI Recipient          | $EDIFACTrecipient
Subject                | $subject_check
Attachment             | $filetype_check
Encryption information | $encryption_check
Encryption result      | $encryption_result
Signature information   | $signature_check
Signature result       | $signature_result
Code
```

9.143.1.2.2 Erstellen von Custom Commands

Weiterhin ist unter **Mail Processing** ²⁸⁶ **Ruleset generator** ²⁸⁷ **Custom commands** ³⁰⁸ das Aktivieren und Befüllen folgender Optionen erforderlich:

9.143.1.2.2.1 Custom macros and commands for all e-mails BEFORE processing

Die **rot markierten Teile** des Codes sind individuell zu ersetzen.

Zeile	Code
001	# Begin: Custom macros and commands for all e-mails BEFORE processing
002	log(1,'Begin: Custom macros and commands for all e-mails BEFORE processing');
003	# Begin: Setting EDIFACT informations
004	setvar('edifact mailbox regex',' email\address@domain.tld ');
005	setvar('clearing mailbox',' clearing@domain.tld ');
006	setvar('keywords','ALOCAT APERAK CONTRL CREMUL DELFOR DELJIT DESADV IFCSUM IFTDGN IFTMBC IFTMBF IFTMBP IFTMIN IFTSTA IMBNOT INSDS INSRPT INVOIC INVRPT MSCONS NOMINT NOMRES ORDCHG ORDERS ORDRSP QUOTES PAYMUL PAYORD PRICAT PRODAT RECADV REMADV REQOTE SLSRPT UTILMD');
007	setvar('allowed_filetypes','!txt,!gzip,application,audio,image,text,video,message/news,message/rfc822,model/vrmlx-epoc/x-sisx-app');
008	## set variables to empty. Otherwise e.g. \$reason would be handled as string "\$reason" and not as variable
009	setvar('result','undefined');
010	setvar('reason','');
011	setvar('encryption check','');
012	setvar('encryption result','');
013	setvar('signature check','');
014	setvar('signature result','');
015	# End: Setting EDIFACT informations
016	EDIFACT address check = {
017	# Begin: EDIFACT address check
018	if (compareattr('to','match','.*@.*')) {
019	log(1,'Found more than one recipient');
020	setvar('EDIFACTrecipient','more than one recipient: \$header_to \$header cc');
021	setvar('reason','more than one recipient');
022	flag('drop',1);
023	}
024	if (compare('cc','match','.*@.*')) {
025	log(1,'Found more than one recipient, dropping e-mail');
026	setvar('EDIFACTrecipient','more than one recipient: \$header_to \$header cc');
027	setvar('reason','more than one recipient');
028	flag('drop',1);
029	}
030	log(1,'Delete all information from from- and to-header except SMTP-address');
031	replace rcpt('(.*) (\<.*\>\$)', '\$2');
032	setvar('EDIFACTrecipient', '\$to');
033	replace sender('(.*) (\<.*\>\$)', '\$2');
034	setvar('EDIFACTsender', '\$from');
035	# End: EDIFACT address check

Zeile	Code
036	};
037	EDIFACT file type check = {
038	# Begin: EDIFACT file type check
039	log(1,'Checking if e-mail contains forbidden file types');
040	if (partoftype('\$allowed filetypes','info','false')) {
041	setvar('filetype check','forbidden');
042	log(1,'Forbidden file types found');
043	if (empty('\$reason')) {
044	setvar('reason','forbidden file type');
045	} else {
046	setvar('reason','\$reason / forbidden file type');
047	}
048	flag('drop',1);
049	} else {
050	log(1,'No forbidden file types found');
051	setvar('filetype check','OK');
052	}
053	# End: EDIFACT file type check
054	};
055	EDIFACT subject check = {
056	# Begin: EDIFACT subject check
057	log(1,'Checking if subject contains EDIFACT keyword');
058	if (compare('subject','match','\$keywords')) {
059	log(1,'Found EDIFACT keyword');
060	setvar('subject check','OK');
061	} else {
062	log(1,'No EDIFACT keyword found');
063	setvar('subject check','No keyword found');
064	if (empty('\$reason')) {
065	setvar('reason','wrong subject content');
066	} else {
067	setvar('reason','\$reason / wrong subject content');
068	}
069	flag('drop',1);
070	}
071	# End: EDIFACT subject check
072	};
073	EDIFACT encryption subcheck = {
074	# Begin: EDIFACT encryption subcheck
075	if (compareattr('key encryption algorithm','match','RSAES-OAEP')) {
076	log(1,'...with RSAES-OAEP');
077	setvar('encryption check','\$encryption check with RSAES-OAEP');
078	} else {
079	log(1,'...but not using RSAES-OAEP');
080	setvar('encryption result','not OK');
081	setvar('encryption check','\$encryption check, incorrect padding');
082	if (empty('\$reason')) {
083	setvar('reason','incorrect S/MIME encryption padding');
084	} else {
085	setvar('reason','\$reason / incorrect S/MIME encryption padding');

Zeile	Code
086	}
087	flag('drop',1);
088	}
089	if (compareattr('content encryption algorithm','match','AES-128 AES128')) {
090	log(1,'...with cipher AES128');
091	setvar('encryption check','\$encryption check, cipher AES128');
092	} else if (compareattr('content_encryption_algorithm','match','AES-192 AES192')) {
093	log(1,'...with cipher AES192');
094	setvar('encryption check','\$encryption check, cipher AES192');
095	} else if (compareattr('content_encryption_algorithm','match','AES-256 AES256')) {
096	log(1,'...with cipher AES256');
097	setvar('encryption check','\$encryption check, cipher AES256');
098	} else {
099	log(1,'...but with incorrect cipher');
100	setvar('encryption result','not OK');
101	setvar('encryption check','\$encryption check, incorrect cipher');
102	if (empty('\$reason')) {
103	setvar('reason','incorrect S/MIME cipher');
104	} else {
105	setvar('reason','\$reason / incorrect S/MIME cipher');
106	}
107	flag('drop',1);
108	}
109	# End: EDIFACT encryption subcheck
110	};
111	EDIFACT encryption check = {
112	# Begin: EDIFACT encryption check / decryption
113	if (smime encrypted()) {
114	log(1,'E-mail is S/MIME encrypted...');
115	setvar('encryption check','S/MIME encrypted');
116	\$EDIFACT encryption subcheck;
117	if (!flag('drop')) {
118	if (decrypt smime()) {
119	log(1,'E-mail successfully S/MIME decrypted');
120	setvar('encryption result','OK');
121	} else {
123	log(1,'E-mail could not be S/MIME decrypted');
124	setvar('encryption result','not OK');
125	setvar('encryption_check','\$encryption_check, could not be S/MIME decrypted');
126	if (empty('\$reason')) {
127	setvar('reason','could not be S/MIME decrypted');
128	} else {
129	setvar('reason','\$reason / could not be S/MIME decrypted');
130	}
131	flag('drop',1);
132	}
133	}
134	} else {
135	log(1,'E-mail is not S/MIME encrypted, dropping e-mail');
136	setvar('encryption result','not OK');

Zeile	Code
137	setvar('encryption check','not S/MIME encrypted');
138	if (empty('\$reason')) {
139	setvar('reason','not S/MIME encrypted');
140	} else {
141	setvar('reason','\$reason / not S/MIME encrypted');
142	}
143	flag('drop',1);
144	}
145	# End: EDIFACT encryption check
146	};
147	EDIFACT signature subcheck = {
148	# Begin: EDIFACT signature subcheck
149	if (compareattr('signature algorithm','match','RSASSA-PSS')) {
150	log(1,'...with RSASSA-PSS');
151	setvar('signature check','\$signature check with RSASSA-PSS');
152	} else {
153	log(1,'...but not using RSASSA-PSS');
154	setvar('signature result','not OK');
155	setvar('signature check','\$signature check, incorrect padding');
156	if (empty('\$reason')) {
157	setvar('reason','incorrect S/MIME signing padding');
158	} else {
159	setvar('reason','\$reason / incorrect S/MIME signing padding');
160	}
161	flag('drop',1);
162	}
163	if (compareattr('digest algorithm','match','SHA-256 SHA256')) {
164	log(1,'...with digest SHA-256');
165	setvar('signature check','\$signature check, digest SHA-256');
166	} else {
167	log(1,'...but with incorrect digest');
168	setvar('signature result','not OK');
169	setvar('signature check','\$signature check, incorrect digest');
170	if (empty('\$reason')) {
171	setvar('reason','incorrect digest');
172	} else {
173	setvar('reason','\$reason / incorrect digest');
174	}
175	flag('drop',1);
176	}
177	# End: EDIFACT signature subcheck
178	};
179	EDIFACT signature check = {
180	# Begin: EDIFACT signature check /validation
181	if (smime signed()) {
182	log(1,'E-mail is S/MIME signed...');
183	setvar('signature check','S/MIME signed');
184	\$EDIFACT signature subcheck;
185	if (!flag('drop')) {
186	if (validate smime sig('1')) {
187	log(1,'Signature is valid');

Zeile	Code
188	setvar('signature result','OK');
189	setvar('signature check','\$signature check, signature is valid');
190	} else {
191	log(1,'Signature is invalid');
192	setvar('signature result','not OK');
193	setvar('signature check','\$signature check, signature is invalid');
194	if (empty('\$reason')) {
195	setvar('reason','S/MIME signature validation failed');
196	} else {
197	setvar('reason','\$reason / S/MIME signature validation failed');
198	}
199	flag('drop',1);
200	}
201	}
202	}else {
203	log(1,'E-mail is not S/MIME signed');
204	setvar('signature result','not OK');
205	setvar('signature check','not S/MIME signed');
206	if (empty('\$reason')) {
207	setvar('reason','not S/MIME signed');
208	} else {
209	setvar('reason','\$reason / not S/MIME signed');
210	}
211	flag('drop',1);
212	}
213	# End: EDIFACT signature check / validation
214	};
215	EDIFACT sign = {
216	# Begin: EDIFACT sign
217	log(1,'S/MIME signing e-mail');
218	if (has smime key()){
219	log(1,'S/MIME key available');
220	if (sign smime('sha256;pss')) {
221	log(1,'Signing successful');
222	setvar('signature result','OK');
223	setvar('signature check','S/MIME signed');
224	} else {
225	log(1,'Signing failed');
226	setvar('signature check','signing failed');
227	setvar('signature result','not OK');
228	if (empty('\$reason')) {
229	setvar('reason','S/MIME signing failed');
230	} else {
231	setvar('reason','\$reason / S/MIME signing failed');
232	}
233	flag('drop',1);
234	}
235	} else {
236	log(1,'No S/MIME key available for signing');
237	setvar('signature result','not OK');
238	setvar('signature check','no signing key available');
239	if (empty('\$reason')) {

Zeile	Code
240	setvar('reason','no S/MIME signing key available');
241	} else {
242	setvar('reason','\$reason / no S/MIME signing key available');
243	}
244	flag('drop',1);
245	}
246	# End: EDIFACT sign
247	};
248	EDIFACT encrypt = {
249	# Begin: EDIFACT encrypt
250	if (smime keys avail()) {
250	log(1,'S/MIME certificate available for recipient \$to');
251	if (encrypt smime('','','aes192:oaep')) {
252	log(1,'Encryption successful');
253	setvar('encryption check','S/MIME encrypted');
254	setvar('encryption result','OK');
255	} else {
256	log(1,'Encryption failed');
257	setvar('encryption result','not OK');
258	setvar('encryption check','S/MIME encryption failed');
269	if (empty('\$reason')) {
260	setvar('reason','S/MIME encryption failed');
261	} else {
262	setvar('reason','\$reason / S/MIME encryption failed');
263	}
264	flag('drop',1);
265	}
266	} else {
267	log(1,'No S/MIME certificate available for encryption');
268	setvar('encryption result','not OK');
269	setvar('encryption check','no S/MIME certificate available');
271	if (empty('\$reason')) {
272	setvar('reason','no S/MIME certificate available');
273	} else {
274	setvar('reason','\$reason / no S/MIME certificate available');
275	}
276	flag('drop',1);
277	}
278	# End: EDIFACT encrypt
279	};
280	log(1,'End: Custom macros and commands for all e-mails BEFORE processing');
281	# End: Custom macros and commands for all e-mails BEFORE processing

Code

9.143.1.2.2.2 Custom commands for incoming e-mails BEFORE decryption

Zeile	Code
01	# Begin: Custom commands for incoming e-mails BEFORE decryption
02	log(1,'Begin: Custom commands for incoming e-mails BEFORE decryption');
03	# Begin: Special processing for EDIFACT
04	log(1,'Begin: Special processing for EDIFACT');

Zeile	Code
05	if (rmatch('\$edifact mailbox regex')) {
	if (!compareattr('SENDER','equal','<>')) {
06	setvar('direction','inbound');
07	\$EDIFACT address check;
08	\$EDIFACT file type check;
09	\$EDIFACT subject check;
10	\$EDIFACT encryption check;
11	\$EDIFACT signature check;
12	if(flag('drop',0)) {
13	setvar('result','F A I L E D');
14	notify('\$clearing mailbox','EDIFACT report attachmail');
15	drop('553','Requested action not taken: \$reason');
16	} else {
17	setvar('signature result','OK');
18	setvar('encryption result','OK');
19	setvar('result',' O K ');
20	notify('\$clearing mailbox','EDIFACT report');
21	deliver();
22	}
23	}
	}
24	log(1,'End: Special processing for EDIFACT');
25	# End: Special processing for EDIFACT
26	
27	log(1,'End: Custom commands for incoming e-mails BEFORE decryption');
28	# End: Custom commands for incoming e-mails BEFORE decryption

[Code](#)

9.143.1.2.2.3 Custom commands for outgoing e-mails BEFORE encryption

Zeile	Code
01	# Begin: Custom commands for outgoing e-mails BEFORE encryption
02	log(1,'Begin: Custom commands for outgoing e-mails BEFORE encryption');
03	# Begin: Special processing for EDIFACT
04	log(1,'Begin: Special processing for EDIFACT');
05	if (compare('from','match','\$edifact mailbox regex')) {
06	setvar('direction','outbound');
07	\$EDIFACT address check;
08	\$EDIFACT file type check;
09	\$EDIFACT subject check;
10	\$EDIFACT sign;
11	\$EDIFACT signature subcheck;
12	\$EDIFACT encrypt;
13	\$EDIFACT encryption subcheck;
14	if(flag('drop',0)) {
15	setvar('result','F A I L E D');
16	notify('\$clearing mailbox','EDIFACT report attachmail');
17	bounce('EDIFACT report attachmail');
18	} else {
19	setvar('signature result','OK');
20	setvar('encryption result','OK');
21	setvar('result',' O K ');
22	notify('\$clearing mailbox','EDIFACT report');

Zeile	Code
23	<code>deliver();</code>
	<code>}</code>
	<code>}</code>
24	<code>log(1,'End: Special processing for EDIFACT');</code>
25	<code># End: Special processing for EDIFACT</code>
26	
27	<code>log(1,'End: Custom commands for outgoing e-mails BEFORE encryption');</code>
28	<code># End: Custom commands for outgoing e-mails BEFORE encryption</code>

Code

10 Versionsverlauf (englisch)

Version 12.0 (Released 2020-11-13)

(neu in 12.0)

Upgrade is only possible for appliances with a log partition size of at least 2 GB and must otherwise be cloned to a new appliance using the "clone device" feature found under "Administration".

Warning for customers with HIN connector using GLOBAL encryption: The current update corrects a misbehavior of the old ruleset that led to GLOBAL encryption for users without a local account even ignoring the settings in "Mail processing". Please check that GLOBAL encryption still works as expected after creating a new ruleset.

The following rule set macros are provided for replacement of legacy variables:

- @ADDDISCLAIMER@ -> \$disclaimer;
- @ARCHIVE@ -> \$archive;
- @KEYSERVER@ -> \$keyserver;
- @LOGSUBJECT@ -> \$logsubject;
- @PLUGIN@ -> \$plugin;
- @RELAY@ -> \$relay;
- @REMOVELFMTAGS@ -> \$removelfmtags;
- @VSCAN@ -> \$vscan;
- @VSCANSEL@ -> \$vscan_crypt_only;

Administration:

- Allow public X.509 certificates, root CAs and OpenPGP key bulk export
- Make sure the system time is in sync when using hardware sensors
- Automatic frontend sync for mail processing and GINA
- Show more relevant information in blocked mails log
- Allow frontends to update vendor domain certificates
- Test mail console menu option

Processing:

- Runtime disclaimer selection using extended signature marker
- Log reject code and message for internally rejected mails
- Option to trust imported CA certificates automatically
- Properly tag non-managed domain encryption in log
- Domain-based default and reply disclaimer
- Skip PTR check if sender is authenticated

GINA:

- New GINA password reset option: SMS or hotline without question/answer
- Disable reply button when reply to default recipient list is empty
- Confirmation password feature for additional authentication factor
- Provide relevant local issuer CA along with certificate on search
- Improved GINA secure attachment language selection and support
- Allow to disable strict Server Name Indication (SNI) checks
- Allow multiple authentication methods in one GINA domain
- Limit session access to User Agent / IP combination
- Prevent error when uploading empty keys to GINA
- Prevent improper log entries in GINA user log
- Implement 12 hour hard timeout

MPKI:

- GlobalTrust MPKI connector

System:

- Update to OpenBSD 6.8 / LibreSSL 3.2
- OpenSSL 1.1.1h

Patch release 1, 2020-11-13

(neu in 12.0.1)

- Interpret waiting status in D-TRUST MPKI revoke as success
- Correctly handle private S/MIME RSA keys in PKCS#8 format
- Prevent display of invalid entries in mail log overview
- Remove LDAP bind failed message when LDAP is reachable
- Improve CSV user imports

Patch release 2, 2020-11-17

(neu in 12.0.2)

- Correctly recover mail service on unrelated watchdog error
- Allow HIN domain-encrypted subjects to appear in mail log
- Properly replace subject tags for plugin use
- Fix issue with external GINA authentication
- Fix fetchmail startup issue

Patch release 3, 2020-11-27

(neu in 12.0.3)

- nslookup for all record types in consolemenu
- Fix issue with registration process

Patch release 4, 2020-12-14

(neu in 12.0.4)

- Show lock for HIN encrypted mails
- Do not allow PKCS7 in SSL import
- Allow frontend server backups
- Disable vioscsi and correctly detect Nutanix Hosts
- Do not set accountLastUsed for domain for internal mails
- Fix sporadic syntax error in system view
- Fix race condition in watchdog starting GINA portal
- Fix missing fromemail in GINA secure attachment
- Fix customer/mailroute assignment issue

Patch release 5, 2021-01-05

(neu in 12.0.5)

- Better error handling for all MPKI connectors
- Read vioscsi with manual disable possibility
- Fix azure provisioning
- Fix bad formatting in tracker
- Fix case where frontends are detected as cluster members

Patch release 6, 2021-01-27

(neu in 12.0.6)

- GINA GUI code hardening
- improved license usage for LFT users
- notify() with parameter 'admin' now also notifies the postmaster of the managed domain
- Improve GINA domain configuration speed with large number of installed managed domains
- Add SMS provider prosms.dds.a1.net
- Fix issue where where smarthost redentials are used for internal delivery

-
- Fix bad DN formatting for S/MIME certificates issued by rule engine
 - Fix bad encoding in D-Trust MPKI connector
 - Fix IncaMail tag handling
 - Fix ldap proxy crash

Patch release 7, 2021-02-01*(neu in 12.0.7)*

- Fix issue with appliances that have a very old ruleset

Patch release 8, 2021-03-08*(neu in 12.0.8)*

- Fix issue with not starting GINA portal
- Fix issue with GINA replies from unknown domains

Patch release 9, 2021-03-08*(neu in 12.0.9)*

- generate internal CA list after a transfer of a CA from a cluster member
- session invalid message after session timeout in GINA portal
- suppress logging of the value in setvar()
- allow import of domain PGP keys without email
- add warning message for Hyper-V appliances with a legacy network controller
- Fix GINA portal configuration issue with virtual hosting
- Fix issue with GINA portal registration
- Fix service restart on frontend/backend system
- Fix memory leak in system libraries

Patch release 10, 2021-03-26*(neu in 12.0.10)*

- Enhance connection stability when using a proxy to connect to the update/license server
- Add new policy to emulate a HIN MGW
- Correct handling of long MIME lines (RFC 2821)
- Correctly remove forbidden headers from decrypted S/MIME mails
- Fix display problem with CRL and CA Issuers URI in S/MIME details
- Fix GINA language text file handling with master template dependency
- Update ClamAV to 0.103.1
- Update OpenSSL to 1.1.1j
- Update OpenLDAP to 2.4.58

Patch release 11, 2021-04-29*(neu in 12.0.11)*

- Update root hints for bind
- Sync CRL from backend to frontend
- better TLS compatibility for external LDAP authentication
- Fix CRL generation for local CA
- Fix PKCS12 password encoding
- Fix managed domain assignment in customer settings
- Fix header handling in GINA mails
- Fix PGP secret key import
- Fix sporadic PGP signature verification failure
- Fix handling of long MIME lines (RFC 2821)
- Fix handling of forbidden headers from decrypted S/MIME mails
- Prevent whitelisting for auto-reply messages
- Update OpenSSL to 1.1.1k

Patch release 12, 2021-06-11

(neu in 12.0.12)

- Update ClamAV to 0.103.2
- Use gaurd pattern to prevent time consuming PGP signature detection in large HTML mails
- CSM module improvements
- Fix search for LFT partition
- Fix rare case when a mail has to be redirected to a cluster member because of a bypass LFT upload
- Fix access rights for MPKI operator certificates
- Fix creation of local CRL to track all revoked certificates
- Fix verification of static subject inputs in the admin GUI
- Fix rare case of corrupted mail structure after S/MIME decryption
- Fix nrpe SSL handshake failure

Patch release 13, 2021-08-19

(neu in 12.0.13)

Version 12.0.13 fixes a possible path traversal attack issue in the GINA frontend. We recommend to install this update as soon as possible,

The system automatically checks if an attack has been performed or tried on the appliance and will issue a warning if traces are found.

If this warning is issued please contact the vendor for further investigation and log analysis.

- fix security issue in web.app

Patch release 14, 2021-08-23

(neu in 12.0.14)

- fix GINA attachment handling in reassemble

Version 11.1 (Released 2019-11-14)

(neu in 11.1)

DKIM use prior to version 11.1 requires correcting the DNS entries due to compatibility improvements.

Major changes:

- Substantial S/MIME performance improvements
- Office 365 relay and tenant ID support
- Outlook Addin 2.0 with IME and LFT integration

Administration:

- DKIM DNS entry changes for better compatibility
- Show last license refresh date in home screen
- Allow to refresh license from home screen
- Do not restrict password field input length in admin GUI
- Fix overflow of serial number in OpenSSL-generated S/MIME certificates
- Show MPKI use in mail domain overview
- Added port probe feature to support console menu
- Added web services restart feature to support console menu
- Added support for Office365 tenant ID and automatic relay
- List public OpenPGP keys and X.509 certificates as "DISABLED" when manually disabled
- Allow optional admin GUI login with user mail address instead of ID
- S/MIME certificate and OpenPGP key aliases are only valid for encryption recipients
- User-based IP alias passwords can now be set as an alternative to the hardwired default
- External authentication tester in managed domain now supports direct password login test
- Prevent firmware update download being stuck on download aborts
- Warn about managed domain fingerprint mismatch in edit page
- Prevent deletion of managed domain when fingerprint certificate is active
- Show statistics about top level domains provided by managed domain encryption
- Fix issue with CRL fetch on GUI-based certificate check

- Fix possible GUI not available issue on mail processing reload
- UX improvements for SCEP integration

Logging:

- Support Postfix "enable_long_queue_ids" parameter and use it by default
- Log structural errors in MIME when scanning for S/MIME encrypted mails
- Send new CA certificate notifications to members of "x509rootcertificatesadmin" group
- Do not store custom user creation ruleset when it is equal to the default ruleset
- Move MPKI auto-renew error message to top warning messages
- Allow manual deletion of GINA logs like mail logs
- Improve read speed of log archive files

Processing:

- Reusable macros for user creation in rule engine (see manual for details)
- Autofill comment for X.509 certificates origin imported via incoming mails
- HIN connector will now also sign mails for HIN domain recipients
- Rewrote S/MIME subsystem for maximum performance
- Allow shared smarthost with different credentials per mail domain
- Remove internal control headers from managed domain encrypted mails
- Protect Thread-Topic and Thread-Index headers for managed domain encrypted mails
- Header tagging option for internal mails
- Archiving option now triggers before encryption policies and custom rules
- Allow import of S/MIME certificates with duplicated mail addresses in SAN
- Send watchdog message when user-based license pool is depleted
- Improve scanning for disclaimer markers
- Support legacy mail address format in header From
- Reprocess encrypted mails from Lotus Notes

GINA:

- No longer require user accounts for local GINA messages
- Allow configuration of initial GINA password sender address
- Start of GINA portal is now asynchronous for faster appliance boot

Large files:

- Introduce token-based authentication for server-side LFT API / plugin support

Patch release 1, 2019-12-11

(neu in 11.1.1)

- Allow access to variables \$user_name and \$user_mail currently selected by authenticated()
- Append user stats to user currently selected by authenticated() if possible
- Correctly treat LFTs as secure as per user request when using LFT API
- Stray CA certificates in LDAP imports no longer force a runtime error
- When using tagsubject() with multi-word regex only use the first word
- Prevent log index generation failures by detecting log rotation
- Use configured admin address in hotline password reset mails
- Fix rule engine fatal error on malformed mail address
- 1-year log read would sometimes stop prematurely
- Improve disclaimer positioning and add a timeout
- Switch MPKI RSA key generator to 4096 bit keysize
- Do not show date for unread LFT messages
- Fix per-certificate revocation check
- Fix manual IME certificate import
- ClamAV 0.101.5, WALinuxAgent 2.2.45

Patch release 2, 2019-12-19

(neu in 11.1.2)

- Support console can now force a reinstall of an already installed version
- Remove unnecessary hidden form values on GINA self-registration
- Fix cleanup of unregistered customer GINA accounts
- Fix key server response on frontend servers
- Fix special encoding read in certificates
- Assorted LFT API improvements

Patch release 3, 2020-01-15

(neu in 11.1.3)

- Show "implicit" trust of previously imported root certificates
- Allow select / edit of OpenPGP key delivery template
- Fix edge cases with X.509 certificate import
- Fix crafted GINA registration form disabled bypass
- Fix GINA reply check for default customer domains
- Properly add disclaimer to Addin-based LFT mails
- Add timeout for stuck PGP key generation issue
- Correct chain certificates on signature write
- Use stored postmaster to deliver OpenPGP key

Patch release 4, 2020-02-05

(neu in 11.1.4)

- Improve validation of Office 365 forwarding server hostnames
- Indicate encrypted status of secure GINA-based replies
- GINA portal auto-keepalive to prevent LFT timeouts
- Fix parsing of leading zeros in serial numbers
- Fix import of unknown OID in cert DNs

Patch release 5, 2020-03-25

(neu in 11.1.5)

- SMS empty from address will now use configured GINA admin address
- Fix SNMP queue statistics read for "enable_long_queue_ids" use
- Improve mail index write on appliances with many log archives
- Fix truncated bulk export of PGP keys and S/MIME certificates
- Keep special characters in full name during user creation
- Warn about expired state of MPKI operator certificate
- Rewrote log index generation to use multiple CPUs
- Relax validation on S/MIME certificate import
- Fix OCSP check fatal error in rule engine
- Validate GINA proxy target input
- Improve SPF input validation

Patch release 6, 2020-04-16

(neu in 11.1.6)

- Improved tagsubject() parsing of regular expression input
 - Allow ruleset policy to use same GINA satellite settings
 - Skip RSA-specific options on EC certificate actions
 - Prevent locked users from authenticating via SMTP
 - Fix possible error in customer backup creation
 - Rewrote queue handling in rule engine
 - Event-based SMS OTP support for GINA
 - Sectigo MPKI connector
 - OpenSSL 1.1.1f
-
- Hotfix 1: Fix GUI bug while setting up Sectigo connector

- Hotfix 2: Fix regression in ruleset handling

Patch release 7, 2020-05-20

(neu in 11.1.7)

- Improve reprocess() for Lotus Notes so that only RFC-compliant mails are processed
- Only append "<>" to sender address in change_webmail_sender() if not already found
- Fix check for valid certificate during domain decrypt with HIN connector
- Fix incorrect handling of "<tab>\$" character sequence in custom rulesets
- Check MPKI state before revoking certificates to avoid spurious errors
- Automatically add X.509 Root Certificates from issued MPKI certificates
- Only offer users with passwords when adding new group members
- Sign LFT mails in the same way that GINA mails are handled
- Fix incompatibility with newer customer backups during import
- Fix possible external auth tester error on too many results
- Fix missing user creation in ruleset generator edge case
- Fix issue with password escaping during PKCS#12 import
- Fix recently used domain certificate details display
- Fix PGP inline signed status on multiple parts
- Allow collapse/expand in admin GUI for main tables
- Tweak GINA HTTPS server settings
- Add disclaimers to internal mails
- Virus scan internal LFT mails

Patch release 8, 2020-05-29

(neu in 11.1.8)

- Allow independent OCSP/CLR bulk check for public and root certificates
- Properly add Sectigo MPKI to nightly auto-renewal
- Avoid double-escape of PKCS#12 in relevant spots
- Fix possible duplicated parts in PGP decryption
- Allow relay servers in Office 365 hybrid setups
- Scrub trigger tags on default encrypt deliver

Patch release 9, 2020-07-16

(neu in 11.1.9)

- Provide root certificates that cannot be downloaded from trust store if available
- Better handling of incoming and internal relay of managed Exchange Online domains
- LFT bypass can now create new users with external authentication
- Provide manual flush button for address verification cache
- Fix file type extension handling on multiple MIME parts
- Prevent LDAP import of non-encryption S/MIME certificates
- Do not abort OpenPGP key import after invalid first key
- Add new Sectigo intermediate CA to MPKI connector
- Separate fetchmail from local injection queue
- Prevent deadlocks in background task handler
- Fix saving additional PGP key addresses
- Do not sign to be modified LFT content
- Fix issue with OpenPGP public key bulk export
- Fix OCSP check before revoke
- OpenSSL 1.1.1g

Patch release 10, 2020-09-10

(neu in 11.1.10)

- encrypt_webmail() second parameter allows to skip password mail if SMS can be sent
- When renewing S/MIME MPKI certificates skip imported disabled certificates
- Select proper smarthost credentials for mails with empty SMTP sender
- Authentication log was mistakenly called "audit" log for a long time

- Use exception for edge case logging instead of connection check
- New function getheader() can store header content in variable
- disclaimer() can now auto-position in GINA carrier mails
- Allow company/footer logo opt-out in GINA carrier mails
- Allow to disable WAAgent in Azure without disabling DHCP
- Correctly remove revoked certificates in deduplication
- Allow domain-encrypted subjects to appear in mail log
- Improve whitespace trim for email address reading
- Fix revocation date display in S/MIME certificates
- Check S/MIME revocation status on signature verify
- Allow browser auto-complete in GINA login form

Patch release 11, 2020-11-11

(neu in 11.1.11)

- Users without accounts now correctly trigger domain encryption only in manual user creation
- Function reprocess() now supports attached message only mode
- Always replace revoked certificates in key server lookup
- CRL/OCSP check via X.509 user and root certificate details
- Delete last update for domain keys when importing a backup
- Restrict internal() and external() From header fallback
- Optionally allow group member selector for all users
- Fix selective smarthost parsing with port number
- Allow to specify the mail log search limit
- Do not alter effective plugin subject tags
- Support UTF-8 characters in PKCS12 export
- Correct initial statistic graph content
- Use multiple CRL/OCSP URI if necessary
- Prepare for the update to version 12.0

Version 11.0 (Released 2019-06-20)

(neu in 11.0)

Major changes:

- New policy editor features and ordering support
- Improved spoofing detection
- GINA GUI security hardening
- D-TRUST MPKI
- DKIM support

Administration:

- Prevent creation of wildcard managed domains
- Allow selection for MPKI-capable managed domains
- S/MIME bulk import advanced usage options
- Let S/MIME certificate deduplication default to off in new installs
- Unofficial antivirus signatures now default to off in new installs
- Validate maximum message size value
- Support bulk imports in X.509 certificates and OpenPGP public keys
- Remove non-user bulk imports in administration section
- Show current ruleset creation data
- List mobile number in GINA account overview
- Reject SSL certificate upload if non-server certificate was presented
- Allow use of internal CA for virtual host SSL certificate creation
- Create PGP keys immediately when requesting them in the GUI
- Added D-TRUST MPKI connector
- Policy editor now supports selecting GINA template
- Allow reordering policies in policy editor

-
- Add mail disclaimers to policy editor
 - Updated layout of key server input
 - Automatically delete non-managed users after 6 months of inactivity
 - Improve import to accept OpenPGP user IDs without "<>" characters
 - Indicate managed domain participation value correctly when global setting is used
 - Remove carriage returns from templates to avoid spurious newlines
 - Correct fetchmail SSL support
 - Fix edit bug in multiple customer management
 - Add SEPPmail version to backup file name
 - Warn about auto-renew issues in daily report
 - Warn on version mismatch in cluster

Logging:

- Allow filtering mail logs by encryption, signature, large file or unencrypted property
- Audit and system log now always display 1 full year of log entries
- Make message ID column optional in mail log overview
- Fix property display mismatch in mail log overview
- Improved parsing in technology statistics generation
- Log ruleset version in mail log

Processing:

- Add separate dispatch queue for locally injected mails
- Distinguish between external and outgoing communication
- Wait for internal database to come up instead of failing to process mails
- Defer creation of S/MIME certificates to keep mail processing responsive
- Automatic managed domain relay checks now also enforce global relay permission
- Allow managed domain request header check result to persist
- Improved check_sender() mail header validity check
- Allow variable replacement in setvar() and empty()
- Change LDAP import to add new addresses to existing certificates on key match
- Fix calculation of mail size when reassembling GINA attachments
- Allow reversal of large file processing in deliver()
- Removed obsolete getcustomer() function
- Added support for opaque S/MIME signature creation
- iscalendar() will now treat RTF just like plain calendar entries
- Optional DKIM support for managed domains
- Allow precise disclaimer positioning with "##MAILDISCLAIMER##" placeholder
- Always remove [emptypw] tag from processed mails
- Fix MIME-Version Header misplacement in domain encryption
- Do not allow notify() delete the original message in edge case
- Improved recipient rewrite internals

GINA:

- Use HTML instead of text part when generating a PDF download
- Optionally disallow manual input of GINA recipients
- Create unique message ID for all GINA mails
- Use minimal UTF-8 encoding in mail headers
- GINA GUI code, script and object security hardening
- Add viewport meta values to secure attachment
- Improved GINA GUI responsiveness
- Update to Bootstrap 3.4.1

Large files:

- New LFT disks will now require a size of at least 30 GB
- Split LFT maximum size for outgoing and incoming mails

System:

- Update to OpenBSD 6.5 / LibreSSL 2.9
- Hardening of NTP configuration
- Improved Azure integration

Patch release 1, 2019-06-24*(neu in 11.0.1)*

- Validate sender addresses before processing starts
- archive() usage now correctly appears in mail log
- Fix issue in periodic domain certificate update

Patch release 2, 2019-06-27*(neu in 11.0.2)*

- Let vsn() check if antivirus daemon is off to avoid spurious mail bounces
- Wrap GINA header from and to addresses in "<>" for better spam avoidance
- Fix PDF preview with new GINA content security policies
- Do not check global relay servers for incoming/internal mails
- DFN MPKI connector awareness for email/email-host setting
- Fix pending rule engine S/MIME certificates mismatch
- Correct domain name in GINA message ID headers
- Fix import of S/MIME certificates

Patch release 3, 2019-07-10*(neu in 11.0.3)*

- Let issn() check if antispam engine is off to warn about skipped spam check
- Correctly attach mail body or header report in bounce() and notify()
- Show potential errors in CRL/OCSP certificate check fetch
- CA root addition notification with details about new certificate
- Daily report lists all undefined CA root certificates
- Correct error in default recipient display on GINA send
- Fix saving miscellaneous options in mail processing
- Do not support auto-customer option in encryption policy
- Fix processing of mails from mails starting with a plus sign
- Let admin decide about customer association on user/bulk import
- Always clear previous daily report MPKI autorenew error
- Retain advanced MTA settings on mail system edit
- Correct error in DKIM signature append
- Add ability to scan LFT attachment for viruses
- Fix missing LFT in split recipient scenario

Patch release 4, 2019-07-31*(neu in 11.0.4)*

- Avoid incorrect HIN domain certificate fingerprint mismatches
- Properly remove subject tags in "do not encrypt" policies
- Add domain encryption-only users to daily CSV report
- Allow to skip createkeys() deferral with custom rule
- Fix regression in saving attributes in setuserattr()
- Fix migration of policies to new position-based approach
- Do not list unlocked GINA accounts in daily report
- Allow secure LFT bump via Outlook sensitivity header
- Fix issues with user creation and deletion
- Show user language GINA account details

Patch release 5, 2019-08-08

(neu in 11.0.5)

- Fix OpenPGP key generation where the secret key was not saved
- Fix issue where the list of users could not be displayed
- Fix GINA issue where the dsn notification was not sent
- Fix regression in saving GINA accounts
- Fix restore of pre version 11 backups

Patch release 6, 2019-09-10

(neu in 11.0.6)

- Do not mark daily reports with undefined root certificates as important
- Follow-up change for HIN domain certificate fingerprint mismatches
- Fix import edge case with Arbeitsagentur S/MIME certificates
- Make it possible to distinguish licensed users in daily CSV
- Proper enforcement of multi-tenancy customer license limits
- Header validity checks now allow superfluous whitespaces
- Show account and last message status in GINA details
- Better mobile number validation on GINA CSV import
- Support encryption policies in GINA remote setups
- Show issuer in GINA S/MIME certificate display
- Add confirmation dialog to OpenPGP key deletion
- Fix a faulty certificate issue in D-TRUST MPKI
- Refuse import of unsupported ECC OpenPGP keys
- Fix save delay for GINA domain settings
- Allow import of OpenPGP keys of unusual size
- Custom generation for EDIFACT mail reports
- Fix GINA frontend OCSP HTTP proxy URL
- Log S/MIME retention check in system log
- Add support for new aspsms SMS interface
- Fix issue with Azure agent service
- ClamAV 0.101.4

Patch release 7, 2019-10-01

(neu in 11.0.7)

- Fix customer association in multi-tenancy GINA portals for uppercase mail addresses
- Only add encrypted attached mail as separate mail on incoming direction
- S/MIME digest selection is now effective in "do not encrypt" policies
- Rule engine key and certificate generation now correctly sets CN attribute
- Do not append disclaimers to calendar entries (requires ruleset reload)
- Only get host name and domain name from Azure DHCP if not set manually
- Optionally allow static subject override for SwissSign MPKI
- Improve parsing of sloppy whitespace patterns in mail headers
- OpenSSL 1.1.1d

Patch release 8, 2019-10-24

(neu in 11.0.8)

Only send passwords mails via private mail queue to avoid potential deadlocks
 Remove trigger tags on plain or already encrypted messages
 Expire stale pending certificate/key requests
 Always try to skip approval in DigiCert MPKI
 Only create DKIM keys per user request
 Fixed MSG format export encoding issue
 Prepare for the update to version 11.1

Version 10.1 (Released 2018-11-29)

(neu in 10.1)

Major changes:

- Improved ease of use for SSL certificate import, renewal and cluster distribution
- Improved logging capabilities and log view analysis for custom rulesets and policies
- Elliptic-curve encryption support for imported S/MIME certificates
- Optional removal of OpenPGP signatures during mail processing
- Support console menu with network and administration utilities
- Improved performance of file type scanning
- Full OCSP stapling support in GINA proxy
- Removed unsupported SignTrust MPKI
- QEMU and Xen host integration

New admin group privileges "readonlyuser" are not being added to existing installations, but can be added manually by using this exact name if required.

You can reach the support console via user "support" and password "support". The menu will allow you to open a support connection even when the GUI is unavailable.

Administration:

- Check SSL import for matching private key and automatically handle it as the primary certificate
- Allow to import a renewed certificate without private key as long as the previous one matches
- Allow to push current SSL and CA settings to all other cluster members
- Allow to set CRL validity for local CA
- Vendor domain services are now indicated by "managed", "unmanaged", and "mismatch"
- Delete all domain keys after confirmation of deletion of a managed domain
- Allow to test a managed domain's external authentication settings
- Several new and updates notes as well as clarified option names
- Prevent overlapping GUI output when using administration tools
- Allow to restore a backup without overwriting system-specific settings
- Allow to trigger a backup mail via administration tools
- Support console menu with network and administration utilities
- Manual domain encryption overview now shows active column in overview
- Mail disclaimer and templates can now be forced to UTF-8 for maximum compatibility
- Mail disclaimer and templates relocated to mail system category
- Importing a previously known domain key will yield a more descriptive error message
- Allow bulk import of X.509 root certificates
- Fix edit language encoding issue on save
- New "readonlyuser" group for selective GUI access in combination with existing groups
- Fixes for "readonlyadmin" group usage
- QEMU host integration (no settings necessary)
- Xen host integration (no settings necessary)
- Action button support and other visual tweaks

Logging:

- Internally encrypted mail recipients are now properly indicated as encrypted
- Allow policies and custom rulesets to indicate encrypted and signed status as well
- Use "S/MIME" and "certificate" instead of "smime" and "key" in log messages
- Administrative mails generated by the appliance are now visible in the logs
- Protection pack software now logs to system log instead of mail log
- Remote logging now sends system log along with mail log
- Added CC and Date header to message metadata logging option
- Distinguish between incoming and internal communication
- Regenerate mail log index after updates
- Local mail logging may be disabled completely

S/MIME:

- Automatically add SAN to generated S/MIME domain certificates
- SHA-256 is now the signature message digest default

- Support import of elliptic-curve certificates
- Correct CSR creation for wildcard domain

OpenPGP:

- Honour OpenPGP key capabilities, e.g. refuse encryption if capability is not available
- PGP/MIME now prefers AES-256, SHA-512, ZLIB (or lower depending on recipient key)
- Force the use of MDC even when the recipient key does not meet the criteria
- Optional removal of OpenPGP signatures is now available

MPKI:

- Fix internal selected MPKI mismatch for connectors added in version 10
- Only issue certificates for users from managed domains
- Trust all GlobalSign chain certificates via GUI button
- Trust all DigiCert chain certificates via GUI button
- Trust all DFN chain certificates via GUI button
- Unsupported SignTrust connector has been removed

Rule engine:

- Removed obsolete functions `smime_create_key()`, `swissign_create_key()` and `signtrust_get_cert()`
- Fix issue with stripped secure tag on "Consider internally routed mails as encrypted"
- Move custom outgoing ruleset before encryption in front of encryption policies
- Function `createaccount()` no longer creates keys, see `createkeys()`
- Key server checks are now done before starting encryption policies
- Add `ldap_init()` function for maintenance tasks such as cache flush
- Allow key generation even when user creation is set to manual
- Allow use of variables in `replace_rcpt()` and `replace_sender()`
- Allow tags to be appended to the beginning of the subject by default
- Implement `$one_recipient` and `$all_recipients` in `ldap_read()`
- Implement custom search filter support in `ldap_getpgpkeys()`
- Implement custom search filter support in `ldap_getcerts()`
- Warn when RTF-formatged MIME parts have been detected
- Case-insensitive match of `incoming()` domain check
- Removed obsolete function `webmail_password()`
- File type scan speedup

GINA:

- Support `web.app?subject=` parameter in Base64 encoding to prefill the subject field after login
- Warn when GINA domain is associated with managed domains of more than one customer
- Add setting to prevent registration of GINA accounts for associated managed domains
- Always use message arrival time as base for read time in notification message
- Extended MSG support will now show address book entries for sender and recipients
- Optional HTTPS proxy now logs correct user IP regardless of proxy request header setting
- Log TLS protocol and cipher for user login when using GINA via direct HTTPS
- Do not advertise revoked domain certificates in domain key listing
- Change transfer-encoding of attached EML files to 8-bit
- Allow to publish local CA on the certificate search page
- Use more robust MIME structure in generated GINA mails
- Allow indirect OCSP stapling only via OCSP HTTP proxy
- Optional HTTPS proxy now supports OCSP stapling

Large files:

- Allow override of configured LFT plain and secure mode via several control headers and subject tags
- Plain LFT is no longer indicated as encrypted in mail log

Patch release 1, 2018-12-07

(neu in 10.1.1)

- Prevent display of unassociated partial mail entries for customer admins
- Fix external GINA authentication test when multiple servers were given
- Prevent invalid characters when creating a new GINA domain
- Fix mixed charset detection when displaying GINA messages
- Always decode disclaimer text like HTML variant
- Separated mail log indicator for general LFT message usage
- Create persistent backup copy for support-based recovery
- Only create internal users for managed domains
- Fix truncating large DNS zone configurations

Patch release 2, 2019-01-07

(neu in 10.1.2)

- Remove spurious case-insensitive markers from internal compare() statements
- Improve local HTTPS GINA proxy interoperability in Exchange environments
- Avoid potential truncation of long certificates when reading from system
- Also escape characters ";" and "\" in ldap_read() and ldap_compare()
- allow replace_rcpt() to use variables with multiple enclosed recipients
- Storing variables using setvar() no longer accepts names starting with a number
- Compare LDAP certificates e-mail addresses as case-insensitive
- Option to use remote POP3 mail fetch with pure SSL port
- Only create one message abstraction for all associated GINA messages
- Fix a regression in customer association for GINA users
- Send daily report even when individual statistics are damaged
- Hardening of OpenSSL S/MIME key encryption parameters
- Use configured whitelisted subnets to skip SPF check
- Do not store empty values in system configuration
- Fix import of binary LDAP certificates
- Allow IncaMail and HIN connector to coexist
- Fix faulty year wrap in statistics parser
- Show OpenPGP subkey ID on detail page
- Show IPv6 source address in mail logs
- Sort local DNS zones alphabetically

Patch release 3, 2019-01-09

(neu in 10.1.3)

- Automatically trust previously known MPKI certificates on "add or update"
- Correct issue in new SPF whitelist range check
- Avoid partial display of listed user state

Patch release 4, 2019-01-23

(neu in 10.1.4)

- Only replace certificates from remote LDAP if expire date is higher
- Correctly load and store disclaimer parts as UTF-8 in the GUI
- Correctly load and store custom rules sets as UTF-8 in the GUI
- Only accept MPKI P12 password when uploading a new P12 or old password is wrong
- Log relevant S/MIME signature information when detecting or signing
- Exclusively use latest OpenSSL 1.1.1 in S/MIME operations
- Allow to turn off archive scanning in executable and script file scans
- Do not automatically issue or renew keys for users who may not sign or encrypt
- Fix MSG render error by providing an additional codepage mapping
- Fix PDF render error for file names with umlauts
- Fix customer license limiter regression in version 10.1
- Remove default relay network from factory reset
- Prevent use of disclaimer names with "#" characters
- Use charset from original part when decoding

Patch release 5, 2019-03-06*(neu in 10.1.5)*

- Allow to hide domain certificates from GINA by disabling signing capability
 - Immediately restart ClamAV on connection failure
 - Do not reorder DNS servers on system settings save
 - Use all available CRL points to check revocation status
 - Treat sender "<>" as empty to allow fallback to "From" header
 - Accept non-conforming RFC 2045 quoted-printable parts
 - Fix operating system panic on heavy statistics write
 - Do not MIME-encode "<>" in "From" header
 - Fix race in internal statistics increment
 - Correctly handle HIN Global in policy editor
 - Fix export encoding of GINA translation files
 - Update DFN MPKI certificate authority chain
 - Prevent storing duplicated local DNS zones
 - Add NTP sensor mode for virtual machines
 - Improve traditional NTP synchronisation
 - Increase S/MIME bulk import speed
 - Update to OpenSSL 1.1.1b
-
- Hotfix 1: Bring back missing log messages

Patch release 6, 2019-03-29*(neu in 10.1.6)*

- Remove duplicated counter values to avoid cluster sync issues
 - compareattr() "M_Sender" attribute changed to "SENDER"
 - Warn when NTP cannot find qualified servers to sync with
 - Fix import of certificates with telephone numbers
 - Fix setting multiple DNS servers via DHCP
 - Improved performance of background tasks
 - Add SMS provider certifi.llnwd.net
 - Use correct PDF encoding for date
-
- Hotfix 1: Prevent library error on GINA read
 - Hotfix 1: Correct license calculation

Patch release 7, 2019-04-15*(neu in 10.1.7)*

- Fix sending daily report when MPKI operator certificate expires
- Fix empty initial GINA password user in conjunction with external auth
- Ignore pseudo domain @local in daily reports
- Retain sender behaviour from 10.1.4 and below
- Policy sender match now works for empty sender using "<>"
- Avoid sporadic background service exit
- Support "/" in local mail address part
- Amazon Web Services support
- Add SMS provider playSMS
- ClamAV 0.101.2

Patch release 8, 2019-05-23*(neu in 10.1.8)*

- Allow creating users with a previous user ID but different mail address
- Special variable \$from in LDAP functions now replaces correctly with empty envelope sender
- Correctly disable SNMP R/W community when no password was set
- Do not show logs for customer admins without managed domains

- Properly quote LDAP attribute for search in ldap_compare()
- Add missing timeout setting for OCSP HTTP proxy
- Always properly generate mail log index
- Prepare for the update to version 11.0

Version 10.0 (Released 2018-07-05)

(neu in 10.0)

Major changes:

- Performance improvements in mail processing, GINA and admin GUI
- Preempt mode to temporarily stop mail flow through appliance
- OpenPGP subject tags for positive and negative signature verification
- Assorted improvements in frontend / backend clustering
- Allow to specify credentials for each smarthost
- Added a number of new policy editor conditions
- Allow to sign an arbitrary CSR with local CA
- New MPKI connector for Deutsches Forschungsnetz
- New MPKI connector for GlobalSign
- Allow to specify different modes for incoming and outgoing LFT mails
- GINA legacy layout has been removed

New admin group privileges "webmaildomainsadmin" and "mpkiadmin" are not being added to existing installations, but can be added manually by using these exact names if required.

(Groups -> Create new user group)

Please take note that the old GINA design was removed from this version. All remaining users will automatically switch to the new GINA layout and may require a manual style update.

(GINA Domains -> Change GINA Settings -> Edit GINA layout)

Before proceeding with this update, make sure to back up your device.

Admin:

- Require confirmation on user removal and delete/revoke all certificates automatically
- Show current user and device name in footer when logged in
- Redirect users to first viable page after login
- Show user lock state in list (bad password count, locked)
- Redirect to home section when performing a firmware update and show reboot status afterwards
- Do not redirect to logout page after logging back in after logging out there
- Added "webmaildomainsadmin" group access privilege for GINA domains section
- Added "mpkiadmin" group access privilege for MPKI section
- Allow read-only admin to view and filter mail logs
- Add summary to individual mail log detail view
- Add sign and encrypt indicator icons in mail log
- Performance improvements in mail log view
- Avoid temporary purge of SSL trust bundle on frontend servers on save
- Create backup file on startup to allow immediate SCP backup
- Properly encode certificate or key file names on export
- Assorted improvements in frontend / backend clustering
- Preempt mode to temporarily stop mail flow through appliance
- Allow to disable DNS resolver prefetch disable
- GINA 30 day log and full archive download
- Optimized visual spacing used between GUI elements
- Use monospace font in statistics images
- Statistics reset button

Mail System:

- Allow to specify credentials for each smarthost
- Never rate-limit local mail relay
- Added option for mandatory TLS

SSL/CA/MPKI:

- Automatically add CA certificate to internally created SSL certificates on export
- Show correct SSL certificate details if import contained multiple certificates
- Allow to sign an arbitrary CSR with local CA
- Immediately propagate trusted MPKI CA chain during manual update via button
- Use a negative grace period of 30 days for renewing previously expired MPKI certificates
- Warn about expiring MPKI operator certificate in daily report
- New MPKI connector for Deutsches Forschungsnetz
- New MPKI connector for GlobalSign
- Send all MPKI requests to system log
- Verify given MPKI static subject

Rule Engine:

- Sign mail in "do not encrypt" policy if requested
- Properly validate CIDR whitelist ranges in spam and spoof checks
- Fix encoding issues in user-generated notifications
- Improve spoof check to test for match in relay domain
- Authentication header checks must also pass relay network check to succeed
- Always use 30 seconds timeout for LDAP certificate and key lookups
- Allow to use a manual flag as a policy trigger
- Filter policy according to sender too
- Use internal flag mechanism to avoid tagging a subject temporarily
- Always replace the emptypw tag according to the user setting
- "mpkiSubjectPart" attribute support for setuserattr()
- Prevent excessive substitution in compare()
- Accept flat RFC 822 messages in reprocess()
- Allow to force disclaimer usage even when message does not contain the necessary parts
- Automatic disclaimer placement for Microsoft Outlook, Apple Mail and Mozilla Thunderbird
- Domain-sign is no longer available from the ruleset generator
- Properly generate accounts in policies when account creation for all users is selected
- Improve parsing of the message disposition notification header
- Performance improvements for reading incoming messages
- File detection performance improvements

S/MIME:

- Allow to refuse use of certificates that can not be checked for a number of days
- Optionally refuse the import of certificates using SHA-1 or lower
- Optionally refuse to use expired certificates for encryption
- Certificates now have a default validity of 825 days
- Properly escape special characters in common name
- Avoid generating multiple domain certificates in a cluster environment
- Unhide same-subject certificates in X.509 Root Certificates
- Separate page for manual domain encryption management
- Show prominent expired warning for certificates in detail view
- Allow immediate check of certificates in detail view
- Limit the number of external certificates shown by default
- Managed domain encryption switches to OAEP
- Also treat non-multipart message as S/MIME

OpenPGP:

- Properly trust all known keys in PGP/MIME to align with inline PGP behavior
- Make PGP/MIME the default mode for OpenPGP encryption if not set otherwise
- Optional subject tags for positive and negative signature verification
- Allow selection of OpenPGP mode in policy editor as a fallback
- Show prominent expired warning for keys in detail view
- Separate page for manual domain encryption management
- Added validation of signatures

GINA:

- Notifications now default to domain setting, but individual user settings can override
- Do not submit question / answer when it is no longer required by password reset mode
- Do not provide disabled or revoked user certificates in search
- Clarify error message when encryption was requested but account is missing
- Send all password mails to envelope sender to fix an "in behalf of" case
- Automatically add "On ..., ... wrote:" to reply text
- SMS support for vapi2.infinite-convergence.com
- Do not generate accounts for HIN GLOBAL
- Add originating IP to authentication log messages
- CSS handling improvements for secure attachment customization
- EML / MSG downloads now have their date and subject in the file name
- Fix character encoding in MSG export
- Add insecure mail text to basic translation edit view
- Adjust secure copy mail text for clarity
- Annotate use of background images in CSS / LESS file
- Correct time offset in GINA delivery status page
- Added GINA proxy health check to watchdog
- Allow sending GINA logs to remote syslog server
- Allow optional virtual hosting per domain
- GINA legacy layout has been removed
- Performance improvements

Large Files:

- File API version 1.0 can receive files without having to attach them to the initial mail
- Allow to specify different modes for incoming and outgoing files

Patch release 1, 2018-07-09*(neu in 10.0.1)*

- Correctly append system settings during boot up
- Fix MIME part parsing error during disclaimer add
- Fix SCP backup user login

Patch release 2, 2018-07-10*(neu in 10.0.2)*

- Add SOAP service alias to default GINA domain
- Fix VGA hardware boot for OEM hardware
- Fix manual S/MIME domain list display
- Fix Nagios service start
- Fix GINA PDF export

Patch release 3, 2018-07-16*(neu in 10.0.3)*

- Allow empty subject trigger tags to revert to their default
- Use cleaned from address in policies
- Fix GINA secure copy licensing error
- Fix error in external user creation

-
- Fix import of PGP keys from GINA
 - Fix automatic fetch of license

Patch release 4, 2018-07-19*(neu in 10.0.4)*

- Do not fail on first action of special group member after login
- Improved robustness S/MIME certificate attribute parsing
- Allow to create domain keys without a local CA present
- Verify alternative mail addresses for S/MIME signer
- Handle malformed mail addresses in mail log

Patch release 5, 2018-08-02*(neu in 10.0.5)*

- Fix CVS user import for previously whitelisted senders
- Correct domain encryption user count to license overview
- Assume default domain message delivery notification setting if not set
- HIN connector now always uses latest set of trigger texts
- Create default bounce templates during bootup if not found
- Fix case where message tracker was not loading its stylesheet
- Add GINA encryption user count to license overview
- Add SMS support for Interactive Digital Media
- Fix mixed encoding issue with GINA replies
- Improved faked HIN subject tag detection
- Fix possible hang in PGP/MIME encryption
- Fix nightly MPKI auto-renew
- ClamAV 0.100.1

Patch release 6, 2018-08-14*(neu in 10.0.6)*

- Fix boot hang in Windows Server 2008 R2 with Hyper-V 6.1
- Also parse elaborate message disposition notification header values
- Improved detection for incoming / outgoing direction in GINA / LFT
- Fix GINA resource path in preview, translations and password mail
- Align GINA secure reply envelope sender with from header change in 10.0.3
- Set proper permissions on work directory after nightly MPKI run
- Correctly search for external user certificate in edge case
- Only test each sender domain once in anti-spoof check
- Allow keyserver lookup in Internal Mail Encryption
- Further fixing for import of PGP keys from GINA

Patch release 7, 2018-09-11*(neu in 10.0.7)*

- Support GINA HTTPS OCSP stapling (incompatible with "Enable local https proxy")
- Do not warn about ruleset regeneration when using uploaded rulesets
- Do not emit final newline character in SMS password messages
- Tweak RAM usage according to available system resources
- Allow enabling serial console in system settings
- Fix possible decryption error with HTML parts in OpenPGP
- Make LFT tag removal case-insensitive

Patch release 8, 2018-09-20*(neu in 10.0.8)*

- Correct domain replacement issue in HIN connector
- GINA high-performance toggle option, now defaults to off
- Fix display error in Internet Explorer in log detail view

- Correctly delete datasets no longer used in version 10
- Backend task scheduler reworked

Patch release 9, 2018-10-17

(neu in 10.0.9)

- Correctly skip expired certificates in `smime_keys_avail()` when required
- Improve GINA portal speed with large number of installed managed domains
- Correctly save and apply all extended MTA settings values
- Do not partially match on user certificate / key search in GINA
- Allow special HIN prefix on incoming encrypted mails in HIN connector
- Avoid a potential charset issues when displaying GINA messages
- Disable OAEP usage in managed domain encryption
- Improved background task cleanup in scheduler
- Fix customer backup decryption during import

Patch release 10, 2018-10-26

(neu in 10.0.10)

- Allow HA backup to become master when master crashes and hangs at "syncing disks..."
- Raise limits for concurrent GUI access to make GINA and admin GUI more responsive
- Escape special characters in CN of locally generated certificates via mail processing
- Fix expire check when generating new OpenPGP keys via mail processing
- Fix IncaMail connector when sending mail to a real incamail.ch recipient
- Updates for ClamAV 0.100.2 and SpamAssassin 3.4.2

Patch release 11, 2018-11-09

(neu in 10.0.11)

- Variables and flags are now appended and edited using their associated message only
- Improve accessibility of HTTP-only admin GUI missed in patch release 10
- Fix issue with CID replacement of embedded images in disclaimers
- Use UTF-8 encoding for Infinite Convergence SMS service
- Correctly flag use of LFT subject tags for custom rulesets
- Fix OAEP decryption which would occur sporadically
- Create required accounts in sign-only policies

Patch release 12, 2018-11-22

(neu in 10.0.12)

- Allow longer function argument strings in custom rule set
- Fix issue with disclaimer attach on very large messages
- Fix daily report calculation of MPKI operator certificate expire
- Fix off-by-one in X.509 root certificates expire GUI display
- Relax concurrent connection limits on all web servers
- Verify postmaster address input in mail settings
- Do match case when removing subject tags
- Prepare for the update to version 10.1

Version 9.6 (Released 2018-05-17)

(neu in 9.6)

- Only show support connection message warning for users with access to the feature
- Reserve mail log green, orange and red status for remote server status
- Correctly abort mail processing when certificate generation fails
- Outlook Plugin header mode corrections for LFT
- Only log invalid Bind-DNs during LDAP operations
- Tweak LDAP multi-master synchronization configuration
- Display used product version in each mail log
- Fix queued mail log always being one entry short

- Fix memory leak in HIN connector
- Properly enable the Microsoft Azure integration service when selected
- Properly delete expired X.509 Root Certificates when selected
- Prevent removal of certificate bundles on frontend appliances
- Allow leading dot for TLS domain names
- Fix possible problems with LFT resize feature
- Fix special character encoding issue in generated GINA mails
- Display PGP user keys without expiry in GINA key search

Version 9.5 (Released 2018-03-06)

(neu in 9.5)

Patch release 1 is a mandatory update for QuoVadis Swiss Advanced CA G3 S/MIME certificate interoperability. In case of QuoVadis MPKI usage please also refresh the chain certificates via MPKI: Settings: "Add or update".

- Domain encryption is now part of the default encryption in the policy editor
- Added IncaMail, RSA-OAEP and RSA-PSS options to policy editor
- Separate sign option to unify policy editor with ruleset generator
- Do not strip brackets from outgoing server when entering host names
- Prevent password reset for GINA users with empty initial passwords
- Do not mention password expiration during initial GINA registration
- Always update relevant master template settings during relevant GINA domain edits
- Correctly use domain encryption when user-based S/MIME and OpenPGP is disabled
- Speed up creation of multiple domains under mail system
- LDAP connector improvements for anonymous bind and mail-based Bind-DN
- Global switch for auto-publishing managed domain certificates
- Allow to specify the use of text and HTML disclaimer parts
- Disclaimer positioning tweaks for multiple mail clients
- Add disclaimer attachments to mails even when no disclaimer parts could be added
- Log metadata option now includes message from, sender and to headers
- Prevent logging large amounts of data per line
- Added confirmation dialog to full mail log delete
- Allowed deletion of mail log index
- Correct plugin header usage for [plain] and [noenc]
- Allow login for users with single statisticsadmin group
- Improve statistics write for more accurate results
- Unify GINA time format display between languages
- Allow IME certificate import
- Meltdown mitigation
- ClamAV 0.99.4

Patch release 1:

(neu in 9.5.1)

- Correct import of QuoVadis Swiss Advanced CA G3 issued certificates
- Add QuoVadis Swiss Advanced CA G3 chain to optional MPKI trust bundle

Version 9.4 (Released 2018-02-01)

(neu in 9.4)

- Fix translation of timestamp in GINA tracker
- Correctly handle ".asc" extension during PGP inline decrypt
- Always strip encryption tag on incoming mails
- Gracefully deal with an empty from header during account generation
- Added customer info to user CSV in daily report if applicable
- Use same sender extraction for initial key generation and subsequent regeneration
- Always convert PGP/MIME incompatible incoming mails to allow encryption thereof
- Fix an issue with PGP/MIME bulk sending
- Better error message on LDAP bind failures
- Fix GINA password reset mentioning e-mail if only SMS was set

- Do not show unused images in GINA preview
- Do not add unused inline attachments to disclaimers in e-mails
- Allow \$rcptdomain and \$rcptaddress in ldap_compare()
- Improved sender verification
- New OpenPGP public key bulk import
- Allow initial DHCP assignment and add agent for Azure deployments
- Update ClamAV to version 0.99.3

Patch release 1:

(neu in 9.4.1)

- Allow e-mail address as bind DN in LDAP queries

Version 9.3 (Released 2017-12-14)

(neu in 9.3)

- Wrap individual versions in release note viewer
 - Correctly interpret all MPKI auto-renew failures
 - Do not truncate content ID of disclaimer attachments
 - Bring back usage of leading dot in mail domain
 - Do not override key creation result during user creation
 - Remove enabled subject tags from incoming mails
 - Fix initial display of default recipients when writing a new GINA mail
 - Fix user-based GINA ZIP support in mixed recipient list
 - Fix GINA mobile number subject parsing for special encodings
 - Fix spurious display of "=" characters in GINA messages
 - Fix an error in device cloning that could prevent database replication
 - Add CA certificate to exported SSL certificates if available
 - Correctly preset disabled proxy and OSCP selection in system settings
 - Do not search for disabled LFT tags
 - Allow use of SwissSign Demo MPKI
- Correct typo in LFT resize feature

Patch release 1:

(neu in 9.3.1)

- Add rule generator option to prefer RSA-OAEP for S/MIME encryption

Patch release 2:

(neu in 9.3.2)

- Add rule generator option to prefer RSA-PSS for S/MIME signatures
- Correctly verify the non-backwards-compatible RSA-PSS signatures
- Correct mails that are not compliant with PGP/MIME before encryption

Version 9.2 (Released 2017-11-27)

(neu in 9.2)

- New LFT tag was set to enabled by default for backwards-compatibility
- If there are no LFT attachments use original mail for GINA mail download
- Allow master template selection during GINA domain creation
- Correct line endings in GINA mail download
- Fix the nested attachment parsing in GINA mails
- Allow obsolete protocol, cipher and key exchange in SMS connector
- Show correct search entries in domain certificates
- Prevent GINA login when clicking "Forgot password"
- Stripped spurious markup and whitespace from GINA text notifications
- Make internally secured subject tagging opt-in
- Show GINA SOAP connector 400 rejects as deferred in log view
- Always add inline file data for disclaimer

- Do not mention passwords in plain LFT mails
- Correct proxy usage in MPKI connectors
- Correct quoting during S/MIME sequence read
- Raised overall memory limit for mail processing

Version 9.1 (Released 2017-11-08)

(neu in 9.1)

- Fixed SwissSignCMC connection problems
- Fetch correct product's name_id for DigiCert MPKI connector
- Add all languages in GINA notification mails
- Fixed runtime error when adding disclaimer
- Use UTF-8 charset for user import

Patch release 1:

(neu in 9.1.1)

- Show HIN Global activation in managed domains if HIN connector is enabled
- Fix a bug with character sets in disclaimer

Version 9.0 (Released 2017-10-30)

(neu in 9.0)

This major release contains a rework of the Large File Transfer feature. If you previously used LFT and set it to allow unsafe LFT for your domains, your mails will be sent as unsafe by default. If that is not what you expect, please disable the unsafe LFT mode prior to upgrade. Both modes can still be used flexibly using multiple new key words, see below for details.

Please also note that the old GINA design is no longer the default and will not be available in the next major release. All remaining users are encouraged to activate the new GINA layout.

(GINA Domains -> Change GINA Settings -> Edit GINA layout -> Use mobile-friendly web templates)

The database will be reorganized during this update. This means that the update can take longer than usually (up to 30 minutes on large installations)

The Legacy SwissSign connector has been removed. Please change to the new CMC connector before updating.

Before proceeding with this update, make sure to back up your device.

Admin:

- Look and feel of the UI has been improved for all of its elements and the menu
- Revamped disclaimer management with variable support, custom attachments / inline files (requires a valid license)
- Policy editor allows to set fine-grained outbound encryption policies without custom ruleset
- Managed domain service participation can now be selected per mail domain
- Allow to specify subject alternative names for SSL certificates
- Allow to sign a SSL certificate with the local CA during creation
- Certificate usage can be restricted to not encrypt, not decrypt or not sign depending on its capabilities
- Make sure that S/MIME fingerprints are always calculated immediately after import
- Added internal user OpenPGP public key or S/MIME certificate bulk export tool under "Administration"
- Added LFT partition resizing tool under "Administration"
- Per-customer limits for encryption and large file license
- Templates can now set subject and add custom attachments / inline files
- A new system template for policy-based bounce was added
- System default templates can no longer be deleted
- System default templates may be customized per mail domain
- The system info on the "Home" page will now show current memory usage and load averages
- The "Home" page will periodically refresh and show firmware update progress
- Firmware update progress is now fully accurate in terms of percent downloaded
- The import and create pages for "SSL" and "CA" have been separated for clarity

- X.509 Root Certificates now has a retention policy setting for expired certificates
- The mail queue page under "Syslog" now shows a count of all (filtered) mails and their active / hold state
- Security hardening of the admin login process and authorization tokens

MPKI:

- Added support for DigiCert client premium
- MPKI settings move from "CA" to "MPKI" in the menu
- Replaced and unified the client used for issuing MPKI requests
- Treat expired certificates like revoked certificates during auto-renewal

GINA:

- GINA domain settings move from "Mail Processing" to "GINA domains" in the menu
- The user profile welcome page was removed from the GINA portal
- Login will now open the write mail page by default if this page is enabled in the settings
- Support web.app?rcpt= parameter in Base64 encoding to prefill the recipient field after login
- Secure attachment works by default since iOS 11, help button is no longer necessary
- A new password reset option was added: Reset by E-mail verification, no reminder question/answer
- The non-table e-mail layout has been removed as it is incompatible with the newer mobile layout
- Language selectors will now hide if no languages were selected and the default language is used exclusively
- Reduced downtime of GINA portal when reconfiguring GINA domains on installations with multiple domains
- The PDF format was added to the list of possible mail export formats
- Always show maximum attachment size in GINA portal
- Hide mail export in GINA when viewed via iOS
- Fixed ico file import in GINA layout editor

LFT:

- Available operational modes simplified to be either "secure" or "plain"
- The subject tags for "lft:crypt" and "lft:nocrypt" have been removed
- Two new customizable subject tags have been added to force or prevent LFT
- In plain mode, enabled GINA subject tag can force "secure" mode
- In secure mode, enabled plain subject tag can force "plain" mode
- All previous improvements have also been made operable via headers
- Transfer can now be rejected via custom rules for unauthorized users without consuming a license
- Separated automated threshold for incoming and outgoing mails to be set individually
- All messages can now be exported like their GINA counterparts, but will not include the attachments

Rule Engine:

- Warnings are now issued after major upgrades to regenerate the ruleset for the current version
- Improved internal mail encryption to deliver fully encrypted mails to gateway via Outlook plugin
- New function createkeys() to ensure key creation without calling createaccount()
- Tag messages as secure when crossing customer domains on the same appliance
- PGP/MIME can now be set as the preferred outgoing mail format instead of inline PGP
- The reject() rule command alias has been removed, please use drop() instead
- It is now possible to declare reusable macros in the custom commands

Version 8.8 (Released 2017-10-30)

(neu in 8.8)

This is the End-Of-Life release for version 8. Appliances with small disk sizes of under 5 GB (VM 500) are not able to perform the upgrade to version 9 due to lack of available disk space and must therefore be cloned to a new appliance using the "clone device" feature found under "administration".

Use a 9.x image to clone any existing 8.8 appliance which is not capable of upgrading.

- Fix a performance issue in GINA portal with large number of mail domains
- Always fall back to admin mail on GINA password reset if self-registered

- Correctly interpret MPKI generation result in all cases
- Target version 9 for subsequent firmware updates

Version 8.7 (Released 2017-09-27)*(neu in 8.7)*

- Restore secure tagging for internal GINA replies
- Fix an error on password reset in GINA interface
- Improved mail score of GINA mails
- Treat attached messages correctly during LFT processing
- Allow to import same GINA account for multiple customers
- Sort OpenPGP and S/MIME count in user listing numerically
- Improved S/MIME logging for undecipherable messages
- Make POP3 fetch interval configurable in mail system settings
- Reprocess attached S/MIME encrypted messages automatically
- Added managed domain encryption status to overview
- Show X.509 root certificates as orphaned even when they are orphaned
- Correct edge case in subject tagging with multiple encodings
- Skip spam scan for known active correspondents
- Skip spam scan for mail size over 1 MB
- Always use first NTP server in forced time sync

Version 8.6 (Released 2017-08-31)*(neu in 8.6)*

- Improve S/MIME and OpenPGP import process
- Mark installed root chain certificates as orphaned if their signing certificate is missing
- OpenPGP keys without an expire date were falsely presented as expired
- Correctly restart the key server on a rules reload
- Use UTF-8 encoding for SMS connector when needed
- Add all currently locked GINA accounts to daily report
- Correct error in GINA user import
- Fix edit of relay hosts in managed domains
- Let user and certificate cleanup tasks log to the new system log
- Fix special character handling in SNMPv3 user name and password
- When user-based S/MIME and OpenPGP is turned off completely still create users required for GINA encryption
- Slightly change the subject MIME encoding to always preserve whitespaces between words
- Add additional hostnames for virtual hosting GINA domains
- Change the managed domain certificate update interval from 12 to 6 hours
- Allow to specify requested header in managed domains
- Allow larger input in recipient mask for key server search
- Remove JavaScript from secure GINA attachment to avoid false positives in antivirus software
- Fix GINA edge case in improper invalidation of criteria during password change
- Improved content type detection for PDF attachments in the GINA GUI
- Security hardening of the GINA GUI
- Shorten navigation link names in GINA GUI
- Allow to export secure LFT mail without attachments

Version 8.5 (Released 2017-07-21)*(neu in 8.5)*

- Allow selection of default S/MIME digest: SHA-1, SHA-256, SHA-512
- Fix certificate generation regression for internal CA
- Improve file system synchronisation in VM scenarios
- Add loading indicator for mail log detail dialog

Version 8.4 (Released 2017-07-14)*(neu in 8.4)***Admin:**

- Download GINA translation with all applied modifications
- Run GINA reconfiguration in the background for faster editing
- Made AlgorithmIdentifier optional in X.509 root CA import
- Better ZIP and PB7 handling in X.509 root CA import
- Added missing text inputs for S/MIME certificate and OpenPGP key imports
- Support for daily log file rotation and cleanup
- Show mail log entries even if they miss a host name
- Improved coloring of re-injected and bounced mails in mail log
- Fixed parsing of log files that resulted in wrong years to be shown
- Show mail log details in an embedded dialog to retain search filter
- Added a system services log file
- Added a lock/unlock history for GINA users to the daily report
- Fix OpenPGP key generation for e-mails with unusual characters
- UTF-8 support for GINA domain descriptions
- Allow to filter external S/MIME and OpenPGP domain keys
- Prevent the DNS resolver from sending queries in forward mode

Managed PKI:

- Fixed auto-renewal of local OpenPGP keys and SCEP certificates
- Improved error reporting on connection errors
- Abort auto-renewal after too many failures

GINA/LFT:

- New setting to allow self-deletion of GINA accounts
- Fix display of special characters in status mails
- Increased the size of the company logo in the default CSS
- Make inline images responsive so that they always fit the screen
- Interactive confirmation dialog for user key/certificate removal
- Added a preview button to each attachment for in-browser viewing
- Visually indicate password confirmation match during register, edit and reset
- Do not advertize expired S/MIME certificates and OpenPGP keys during search
- Prevent sending the same LFT notification multiple times in a cluster
- Unconditionally sign all messages and notifications when forced sender is set

Rule Engine:

- Allow selection of default S/MIME cipher: 3DES, AES-128, AES-192 and AES-256
- Allow CIDR notation for postfix access map
- Use access maps for HELO checks
- Improved detection for S/MIME encrypted mails
- Improved matching for user and domain certificates
- Log issuer and serial number of decrypted S/MIME messages
- Move user creation to the top of IME handling
- Stop renaming ASC files during OpenPGP decryption
- Better umlaut handling in subject tags for mixed encodings
- Allow override of subject in autoreply()

Version 8.3 (Released 2017-06-01)

(neu in 8.3)

Admin:

- Permit bulk import of single PKCS#12 file
- Ask for old password to be able to set a new one
- Allow import of OpenPGP keys without email addresses
- Only allow download of public certificate in SSL settings
- GINA HTTPS proxy input field validates host name or IP

- Make X.509 User, Root and OpenPGP tables sortable
- Handle import of domain certificates case-insensitive
- Allow limited / unlimited search in mail log
- Show last mail sent in user list
- Correct CSV import of users
- Allow to filter TLS domain display
- Fix MPKI proxy setting affecting the proxy setting for updates
- Improved MPKI SSL connection error reporting

GINA:

- Prevent import of same GINA users into other multi-customer accounts
- Enable mobile layout automatically when no custom CSS is been specified
- Gracefully handle special characters in attachment names
- Show error when creating a new GINA domain without having a default host name set
- Alternative logging of proxied IP addresses
- Allow the HTTPS proxy to work with the new mobile layout
- Avoid UTF-8 file name encoding for secure attachment if possible
- Always use windows CR/LF when downloading EML file
- Correctly embed inlined images into encrypted mails
- Removed custom URL from SMS settings
- Support SMS link for e-mail passwords
- Added language preselection for SMS link

Rule Engine:

- Support IPv6 servers for mail relay
- Prefer resolving IPv6 servers in relay if DNS was set to prefer IPv6 also
- Warn about use of AES-256 as it may not always be supported by the receiver
- Factor GINA mail size into mail log size message
- Strip subject tag [priv] where [emptypw] is also stripped
- Allow to use the characters "{" and "}" in e-mail addresses
- Fix integrity issue with writing MIME structures
- Correct CR/LF in OpenPGP and GINA encryption
- Eliminate duplicate Message-ID header if present in encrypted mail
- Accept CIDR notation for whitelisting spoofed/spam domains
- Allow specifying subject in notify headers
- Update Postgrey whitelist domains and senders

Version 8.2 (Released 2017-03-29)

(neu in 8.2)

- fix display of double-encoded UTF-8 in OpenPGP user ID
- sort drop-down selectors in multi-customer edit
- fix publishing of managed domain certificates
- improve error reporting in the SwissSign CMC connector
- solely use display name for GINA default recipient selection
- fix rare case of false positive invalid S/MIME signature
- force CR/LF line endings for increased S/MIME signature compatibility
- slightly improve generated MIME headers

Version 8.1 (Released 2017-03-21)

(neu in 8.1)

- Show outgoing mail server name port when not equal to 25
- Show correct setting for GINA initial mail password length
- Properly delete previous cluster inconsistency messages
- Fix import of PKCS#12 user key when CA certificate is present
- Revert Postfix hardening to prevent TLS handshake errors
- Create all existing partitions on device clone

- Allow "mobile-optional" to also remove mobile number from GINA profile
- Fix missing subject/message after file upload while writing GINA mail
- Avoid potential cropping of company logos in GINA attachments
- Properly detect PDF in GINA attachments

Version 8.0 (Released 2017-03-17)

(neu in 8.0)

This release features a completely new GINA frontend. To activate it edit the GINA layout and select "Use mobile-friendly web templates". Please note that this will also reset all previously applied CSS changes.

The old GINA frontend is scheduled for removal in an upcoming major release.

Admin:

- new mail processing GINA domain table overview
- correct case sensitivity error in group editing
- correct problem with text input of OpenPGP keys
- option to disable the encryption feature for external S/MIME certificates during import
- option to disable the encryption feature for external OpenPGP keys during import
- add comment field to relay network entries
- correct problem with X.509 certificate import with long lifetimes
- simplify e-mail security settings to avoid ambiguous behaviour with account security section
- improved IPv6 handling in mail routes
- the language reset button for GINA domains moved to the overview page
- import all e-mail addresses within OpenPGP keys
- device clone feature for simplified hardware / virtual machine migration
- properly report that non-RSA X.509 certificates cannot be imported
- warn about in-use GINA domain during deletion confirmation
- warn about in-use disclaimer during deletion confirmation
- correctly handle out of range disk space system readings on home section
- changed active encryption user count to only include active users of the last 6 months
- allow to make each key server lookup optional via ruleset generator
- add group membership info to daily report CSV
- only one cluster member will automatically renew MPKI certificates
- various help text corrections and improvements

GINA:

- new mobile friendly and accessibility-aware layout based on Twitter Bootstrap
- always show native language in drop-down selection
- disable password reset link after first use or successful login
- allow removal of logout and key search menu items via CSS
- allow removal of name and mobile number during registration via CSS
- allow removal of previously set language selectors for login/registration via CSS
- optional contrast improvement for accessibility in mobile layout via CSS
- predefined security questions for new layout
- support multiple servers for external authentication
- the password send app is now translatable into the default domain language
- added feature to present default recipients when writing mail
- display of remaining attachment size when writing mail
- added upload progress bar in secure attachment
- provide both UTF-8 and ASCII fallback name for secure attachment
- suppress login page if logout was selected
- suppress login page if an error occurred while not logged in
- display mail server reject reason in user error message
- add password quality indicators in new layout
- make the initial password length a per-domain setting

LFT:

- add 24 hour pre-expiry notification delivery status notification
- clean up all cached incoming files after 4 hours
- fix potential upload problem with very large files

Rule Engine:

- fix disclaimer() top argument handling
- fully deprecate the use of reject() in favour of drop()
- prevent OpenPGP decrypt from consuming too much memory
- correctly match on ISO-encoded subjects with special characters in trigger text
- improved trigger text removal within subject lines
- compatibility fix in OpenPGP for K-9 mail app for Android
- partoftype() now completely removes ZIP files with matching content instead of rewriting the attachment
- clarify the bounce log entry by not mentioning recipients as the whole mail is being bounced
- allow use of variables in setheader()

Version 7.4.8 (Released 2016-11-22)

(neu in 7.4.8)

Admin:

- corrected problematic encoding of characters in PGP keys
- user listings can now be sorted by each individual column
- correct spurious admin GUI errors on factory reset
- redirect to administrator page after issuing shutdown, reboot or factory reset
- support for downloading of log messages from the last 30 days only
- added confirm dialog for canceling a certificate signing request
- allow to assign / release all accounts for for a customer in multi-customer environments
- correct date and mime type in backup mail
- improved mail log filtering results display
- tweaked spacing in admin GUI header status messages
- correct default logout time in GINA settings
- added SFTP support to backup user login
- added SFTP support to LFT archiver

Managed PKI:

- fixed QuoVadis revoke to adhere to correct domain-specific setting
- added option to automatically request MPKI keys for users without certificates for QuoVadis and SwissSign CMC
- added root certificate import to QuoVadis and SwissSign CMC
- fixed encoding in certificate signing request for QuoVadis

GINA/LFT:

- switched translations to full UTF-8 for non-latin language support
- translations can now fallback to English if no translation was found
- added Russian and Czech translation
- fixed redirect for multiple hosted domains when URL was not ending with a trailing slash
- added help button in iOS Mail preview
- support iOS banner on GINA landing pages
- fixed possible truncated download in GINA attachments

Rule Engine:

- correct domain encryption when GINA and user-based S/MIME disabled
- splitrecipient() now supports setting To header for each CC entry
- generate unique message IDs for all duplicated emails
- adhere to RSA/4096 bits when generating PGP keys unless specified otherwise
- lowered threshold for recursion when checking archived files with partoftype()

- remove duplicated part in bounced emails
- bounce if signing fails before creating GINA account
- properly handle PGP decryption when malformed input was found
- added the autoreply() rule engine command
- run SPF checks after greylisting

Other:

- keep track of non-created users that send mails
- remove 3DES from allowed web server ciphers
- updated OpenSSL to version 1.0.2j

Patch Release 1 (Released 2016-11-25):

(neu in 7.4.8.1)

- Re-enable Nagios plugin
- Revert backup to scp (sftp support will be added for next release)

Patch Release 2 (Released 2016-12-21):

(neu in 7.4.8.2)

- correctly separate sessions for GINA domain edit pages in multicustomer mode
- build domain groups for S/MIME domain encryption to prevent duplicate mails
- direction indicators for sortable user listings
- New Ruleset compiler option to exclude calendar entries from opportunistic encryption
- auto-focus and enter key support in reboot/shutdown/factory reset
- fix display of active support connection hint after reboot
- correct SwissSign CMC revoke per product domain
- correct a bug that would prevent a backup restore
- remove [sign] from subject also when sign all is used
- do not include sender in reply-all recipient list in GINA
- correctly remove previous CC and Sender in bounce mail
- remove [nosign] from calendar entry
- only bounce header of mails in Postfix
- correct a bug that would prevent PGP key import

Version 7.4.7 (Released 2016-08-18)

(neu in 7.4.7)

NOTE: If you are using OpenPGP signing, prompt update is recommended

- GINA password per email feature added, allows individual passwords per email without user registration
- New, enhanced rule compiler with support for comments, procedures etc.
- fix SMTP authentication
- SNMP now properly advertizes mail statistics
- Adjusted RAM warning threshold
- ignore NDRs for whitelisting
- do not send identical watchdog messages every 10 minutes
- use postmaster address as virus scanner notification from address
- Security fix for OpenPGP: fix a rule engine bug that could result in sending unencrypted attachments in rare cases when legacy keys are used and attachments could not be signed

Version 7.4.6.1 (Released 2016-07-21)

(neu in 7.4.6.1)

- POP3 fetcher
- Smarthost port
- backup copy using scp
- SSL CSR import
- save of system comments

-
- support for Kentix SMS gateway

Version 7.4.6 (Released 2016-07-08)*(neu in 7.4.6)***Admin:**

- Added Nagios Remote Executor Plugin support
- Show active support connection on every page
- x509 root certificates are now ordered per trust state and alphabetically
- Autofocus and enter support for various filters and login screen
- Filter for managed domains listing
- Read-only admins can now change their passwords
- Read-only admins can now apply mail log filters
- Rearranged mail log navigation
- Added feature to filter and delete queued mails

Managed PKI:

- Correctly set static subject in new SwissSign MPKI on manual override
- Product name can now be set per domain for new SwissSign MPKI
- Separate proxy settings for MPKI connectors

GINA:

- Allow users to disable their uploaded S/MIME certificates or OpenPGP keys
- Added customer association to user creation message in logs
- Attachment download now reports the download size
- Do not allow users to log in directly after a password reset trigger
- Can now set preferred type for user key upload to exclude a certain technology
- Language selection is no longer displayed if previously given in web interface
- Added Cc to displayed messages
- Allow change of secure attachment name per domain
- Fixed display of unicode characters in SSL certificates, CA and CSR
- Ruleset generator for script file blocking
- Proxy setting now honoured by spam filter update

LFT:

- Delete LFT users older than 30 days
- Added Cc to displayed messages

Rule Engine:

- Prefer sender header to from header for authentication
- Multiple alt names for email in S/MIME certificates and OpenPGP keys
- Immediately adhere to OSCP check outcome
- Allow to specify digest when signing mails

Protection Pack:

- Add unofficial signatures for ClamAV virus protection

Other:

- Base system update
- DNS service has been added to watchdog
- Webservers have been added to watchdog
- Low swap warning was added to watchdog
- Migrated SNMP from net-snmp to OpenBSD snmpd

- Activate sender verification for newer exchange servers
- Periodic time sync option to address clock skew in Hyper-V VMs

Version 7.4.5 (Released 2016-05-04)*(neu in 7.4.5)*

- The security patch applied in 7.4.4 was incompatible with some ASN structures. This leads to problems with some encrypted mails. This patch update resolves this problem. We apologize for any inconvenience there was only time for basic QA testing for 7.4.4

Version 7.4.4 (Released 2016-05-04)*(neu in 7.4.4)***Security update. Fixes the following OpenSSL / LibreSSL issues:**

- Memory corruption in the ASN.1 encoder (CVE-2016-2108)
- Padding oracle in AES-NI CBC MAC check (CVE-2016-2107)
- EVP_EncodeUpdate overflow (CVE-2016-2105)
- EVP_EncryptUpdate overflow (CVE-2016-2106)
- ASN.1 BIO excessive memory allocation (CVE-2016-2109)

We recommend all customers to update to 7.4.4 promptly.

Version 7.4.3 (Released 2016-04-26)*(neu in 7.4.3)*

- Significant performance enhancements (for all platforms)
- Enhancements in SwissSign and QuoVadis MPKI
- Allow to use mail queue partition on second disk
- Fix GINA without reminder/answer
- Allow to use expired PGP keys for encryption
- Fix authentication / user creation for users with subdomains
- Allow to disable GINA for a single managed domain

Version 7.4.2 (Released 2016-04-08)*(neu in 7.4.2)*

- Fix Preview of GINA layout in GUI
- Add sender based routing
- Fix display of Users in Admin GUI for large number of entries
- Allow automatic unregistered GINA account cleanups for single customer environments
- Allow to bind admin GUI to specific IP
- Enhancements in file type detection
- Allow to specify specific postfix settings in Admin GUI
- better error handling when local or remote LDAP fails

NOTE: unlike older versions, user authentication is done using the mail address in the "From" header instead of the envelope address. If you use LDAP lookups to check if a sender is allowed to encrypt mails you should use "\$from" instead of "\$sender" in LDAP queries.

Version 7.4.1 (Released 2016-03-10)*(neu in 7.4.1)*

NOTE: For security reasons, TLSv1 is disabled for the admin GUI (and the GINA GUI if PCI ciphers under mail processing is enabled) . Use a recent browser to access the GUI (e.g. IE 9 will not work)

Managed PKI:

- Added SwissSign CMC MPKI connector

Protection Pack:

- Added SPF (Sender Policy Framework) feature to Antispam
- Added check for spoofed domains

Admin GUI:

- Fixed rare case of GINA log dates not showing the correct year
- Encryption counter improvements, now also counts HIN and Incamail
- Fixed CSV import preview behaviour for users and GINA users
- Fixed time display on lockout messages in GINA GUI
- Fixed time display in audit log and reversed order for consistency
- Improved LFT settings behaviour on save in admin GUI
- Added settings to allow specific servers / networks to send from a specific domain
- Fixed display of full name in group listing and edit view
- Display users by ID in customer admin selection for unambiguous select
- Don't display disabled user / password input block when already logged in

Rule Engine:

- LDAP commands now failover if server not reachable / timed out
- Show details in log if S/MIME signature verify fails
- Allow empty pw param in subject when sending LFT from GINA
- Fixed replace of PLAINTEXT and CREATEPGPKEYS templates in custom rule set
- Corrections in ruleset if user-based S/MIME and PGP disabled
- Added option to consider forced TLS as encrypted
- Prefer stronger AES256 for OpenPGP when applicable

GINA technology:

- Moved "Send copy to myself" option beneath send button in GINA interface

Version 7.4.0 (Released 2016-02-15)

(neu in 7.4.0)

Main features added:

- Added LDAP key server feature (S/MIME and PGP)
- LFT can now archive to an external server
- New security level for GINA: reset by SMS without question/answer
- Allow multiple NTP server entries
- Cache LDAP connections
- Avoid signing of Outlook calendar sharing requests
- Added audit log page
- Extend S/MIME certificate management to be able to automatically deduplicate certificates
- Extend S/MIME certificate management to be able to automatically delete expired certificates
- Allow automatic unregistered GINA account cleanups per customer
- Added a backup user to download backups via SCP
- Added GINA domain setting to override the sender for GINA emails

Admin GUI:

- Added comment fields for S/MIME certificates
- Allow leading numbers in domain names
- Allow to change a user's ID
- Allow to filter mail log entries by colour
- Cap number of user accounts displayed on overview pages
- Changed date formats in admin GUI to consistently use ISO 8601
- Fix certificate import with special control characters
- Increase file size restrictions of import forms
- Mail size in log now properly accounts for all types of attachments
- PGP Import and delete now properly refreshes the overview page

- Show log entry number on details page
- Correctly sort users when adding to group
- Allow to specify multiple syslog servers for forwarding

Crypto Engine:

- Don't corrupt PGP attachments on decrypt when files are incorrectly tagged as text files from sender
- Change default OpenPGP keysize to 4096

GINA technology:

- Added real IP to access log when using reverse proxy (X-Forwarded-For)
- Adjusted the GINA login failure messages to not leak account information
- Allow creation of local accounts from managed GINA domains that have external authentication enabled
- Always set Strict-Transport-Security header with max-age 30 days
- Fix password reset link in e-mail verification
- Fixed GINA attachment filenames with special characters for IE11
- Fixed GINA email sending in IE 9 and below
- Further harden HTTP requests against XSS
- Restrict CORS headers to hostname and GET,POST,HEAD method if requested
- Verify phone number in GINA account details

Rule Engine:

- Adapt `replace_sender()` to work like `replace_rcpt()`
- Added rule set generator option to automatically sign using PGP after encryption
- Allow attachmail for bounces as well
- Allow evaluation of regular expressions in `replace_rcpt()`
- Allow usage of `@NOSIGNTXT@` and `@NOENCTEXT@` in custom rule set
- Don't generate GINA accounts when license is invalid or sender is not allowed to encrypt
- Fix template selection in `encrypt_webmail()`
- Respect nosign flag for GINA mails

System:

- Added device ID to backup filename
- Added log message if no PGP key was found for a domain
- Allow to specify threshold for load balancer
- Automatically copy initial console network setup to GUI system settings
- Extended SMS service support
- Multi-customer support for backup features

Version 7.3.3 (Released 2015-12-04)*(neu in 7.3.3)*

- Make sure named is always restarted correctly when saving settings in system and local zones are defined

Version 7.3.2 (Released 2015-10-23)*(neu in 7.3.2)*

- Allow to specify threshold for load balancer, lower default threshold to 4 connections
- Add support for simmcomm sms provider
- Ignore revoked S/MIME certificates when signing
- Fix import of certificates with special characters

*NOTE: Security update for libressl (CVE-2015-5333 and CVE-2015-5334)***Version 7.3.1 (Released 2015-08-27)***(neu in 7.3.1)*

- Fix a bug in the SwissSign MPKI for silver light certificates
- Fix shutdown by amdin GUI
- Increase stability of SNMP daemon

Version 7.3.0 (Released 2015-08-13)

(neu in 7.3.0)

- Update base system
- Enhanced css templates for GINA mails (optimized for Outlook)
- Add support for www.sms4.de
- Allow to specify HELO
- IPV6 support
- Add support for Safenet HSM encrypted LDAP partition
- Allow to exclude specific ClamAV patterns
- Allow to block executable files in mails
- OCSP / CRL checks
- Enhanced S/MIME certificate information in GUI
- Allow to use \$recipient as a variable in LDAP queries
- Add QuoVadis MPKI support
- Add SCEP MPKI support (e.g. for Microsoft CA)
- Add domain-specific parameters to SwissSign MPKI
- Enhancements in HIN connector

Version 7.2.4 (Released 2015-06-22)

(neu in 7.2.4)

- Fix character set issues in GINA GUI
- Performance enhancements for Microsoft Hyper-V appliances
- Update ClamAV engine
- Security update for CVE-2015-1788, CVE-2015-1789 and CVE-2015-1792

- Correctly create user account for IME when sending from new account
- Changes in HIN connector

Version 7.2.3 (Released 2015-06-03)

(neu in 7.2.3)

- Update apache to version 2.4.12
- Show creator in GINA account overview
- Add support for www.sms4.de sms provider
- Fix an error in max mail size calculation for LFT

NOTE: Security update for logjam vulnerability

Version 7.2.2 (Released 2015-05-09)

(neu in 7.2.2)

- Fix decryption using expired OpenPGP keys
- Fix type check in archives
- Fix SOAP connector for attachments with special characters in name
- Allow to specify HELO name
- Add command to add SwissSign intermediate certificates

NOTE: If you use the SwissSign MPKI connector you should add the new SHA2 intermediate certificates. You can add them manually under "X.509 Root Certificates" or click "Add or update" in "CA" "External CA" "Configure MPKI" "SwissSign Connector" "Settings"

Version 7.2.1 (Released 2015-04-24)

(neu in 7.2.1)

- Allow underscore in GINA admin mail address
- Show hint if password reset is attempted by locked GINA account

- Correct URL in GINA pw reset / init mails when using virtual hosting
- Fix log file download (remove trailing HTML code)
- Fix log search for IP addresses
- Fix load balancer activation when using chrome browser
- Fix backup import for multi-tenancy
- Fix sync of LFT files in cluster
- Limit uploaded certificates/openpgp keys to max 5 MiB in GINA interface
- Add support for domain encryption for subdomains with one single key
- Allow to edit mail addresses for OpenPGP public keys
- Enhancements in LFT

Version 7.2.0 (Released 2015-03-30)

(neu in 7.2.0)

- Add option to authenticate internal GINA or LFT against with LDAP / AD server
- Send Samhain messages to syslog server
- Allow to set max LFT message size (independant from SMTP max message size)
- Relallow GUI over http
- Enhancement in LFT file upload: Disable send and attach buttons during send/upload operations, add spinning waiting indicator
- Add audit user functionality (readonlyadmin group)
- Disable autocompletion in admin GUI
- Some cosmetic changes in admin GUI (mainly add some help texts)
- Make sure smtpd is correctly restarted after config changes
- Patch for CVE-2015-0209, CVE-2015-0286, CVE-2015-0287, CVE-2015-0288 and CVE-2015-0289 for libressl
- Patch https://www.openssl.org/news/secadv_20150319.txt (note: openssl is only used internally, no services using openssl are reachable over the network)
- Note for customers with reverse proxies: New file [URL]/img/waiting.gif, new elements on write-mail page: id="messageBody", id="subjectText", id="input-add-recipient", id="submit-add-recipient"
- Automatically renew OpenPGP keys
- Add support for domain encryption for subdomains with one single key

Version 7.1.2 (Released 2015-03-06)

(neu in 7.1.2)

- Revert change for signature algorithm for S/MIME as there are too many systems around which cannot handle SHA-256

Version 7.1.1 (Released 2015-02-15)

(neu in 7.1.1)

- Update clamAV
- Stability / DOS enhancements for GINA / LFT interface
- Progress bar for File uploading in GINA GUI
- Performance enhancements for ESX (no multiprocessor support)
- Update apache to version 2.2.29
- Change default signature algorithm for S/MIME to SHA256

Version 7.1.0 (Released 2014-12-15)

(neu in 7.1.0)

- Update base system
- Switch from OpenSSL to LibreSSL
- Enhancements in LFT
- LFT without authentication (use [lfm:nocrypt] in subject to trigger)
- "Reply all" function for GINA

Version 7.0.4.2 (Released 2014-12-03)

(neu in 7.0.4.2)

- Correct log detail display for rejected mails
- Fix date and character set in msg download in GINA
- Fix SwissSign revocation for certificates with odd serial numbers
- Do not detect mails with spoofed domains as virus
- Monitor snmpd in watchdog

Version 7.0.4.1 (Released 2014-10-20)

(neu in 7.0.4.1)

- Completely remove sslv3, even from opportunistic postfix TLS
- Correct a bug when tagging a subject that contains double quotation marks
- Repair statistics for GINA mails

Version 7.0.4 (Released 2014-10-10)

(neu in 7.0.4)

- SNMP V3
- Enhancements in HIN connector
- Notify in GUI if important settings are missing (postmaster address, DNS)
- Add filter for GINA ausers in admin GUI
- Allow sending sms through proxy
- Enhancemenets in SOPA connector
- Make virus scan use less memory
- Final changes for PCI compliance
- Allow disks larger than 1TB for LFT partition
- Allow domain cert refresh over https

Version 7.0.3 (Released 2014-09-05)

(neu in 7.0.3)

- Fix backup restore
- Check size of attachemnts uploaded in GINA GUI
- Allow to enable / disable vmware tools
- Allow firmware upload in admin GUI
- Include cutom files in backup
- Speed up display of log details
- Enhancements in outlook message download in GINA
- Make sure domain encryption counters are used for non-registered users (until now domain encryption was only counted if sent / received by a registered user)
- Optimize backup file size
- Show list of recently used managed domain keys
- PCI: Allow LDAP partition unlocking over network
- openssl security fixes (see http://www.openssl.org/news/secadv_20140806.txt for details)

NOTE: This update includes openssl security fixes. Prompt update is recommended

Version 7.0.2 (Released 2014-08-04)

(neu in 7.0.2)

- Show LFT user in admin GUI
- Do not create Encryption users when using LFT
- Show max possible message size in GUI
- Introduce teaming for network adapters
- Updated CSS files for better compatibility
- Correct sms link in multi-tenancy environment

Version 7.0.1 (Released 2014-07-12)

(neu in 7.0.1)

- Enhancements in mail-to-sms service

- Add auto-renewal function for LFT keys
- Log console commands to audit log
- Enhance postfix TLS (custom dhparams)
- Changes for 2500B and 5000B hardware
- Allow deletion of users with S/MIME or OpenPGP keys
- PFS for SMTP
- Fix splitrecipients command
- Fix backup download in GUI
- Fix a bug in OpenPGP decryption and key creation

Version 7.0.0 (Released 2014-06-27)

(neu in 7.0.0)

- Make multi-tenancy available in default version
- Password rules for admin users including password history
- Password history / forced password change for GINA users
- Encrypted database directory with boot password
- CEF (Arcsight) Logging in admin GUI
- GUI timeout configurable
- Non-ambiguous initial passwords for GINA
- Samhain integration
- Update base system
- Support for ESX VMNET3
- Support for ESX paravirtual SCSI

Version 6.5.5.7 (Released 2014-07-16)

(neu in 6.5.5.7)

- Allow deletion of users with keys / certificates

Version 6.5.5.6/6.6.5.6 (Released 2014-06-13)

(neu in 6.5.5.6)

(neu in 6.6.5.6) multitenant version

This update addresses CVE-2014-0224 and several other openssl security issues. Customers who are using the local proxy (under System/Advanced/GINA https Protocol/Enable local https proxy) should update as soon as possible.

Additional information: The openssl library used for normal operation (without local proxy) is known to be vulnerable, but appears not to be exploitable. If you are concerned about this security issue you should upgrade to this version and activate the local proxy.

If you are also concerned about the admin GUI, you can request an update to the (pre-)release version 7.0.0

Version 6.5.5.5/6.6.5.5 (Released 2014-06-03)

(neu in 6.5.5.5)

(neu in 6.6.5.5) multitenant version

- Fix SwissSign revocation
- Fix Reboot issue
- Fix OpenPGP key generation

Version:6.5.5.4/6.6.5.4 (Released 2014-05-20)

(neu in 6.5.5.4)

(neu in 6.6.5.4) multitenant version

(Info: 6.6.x is the multitenancy version)

- Add optional "restrictive" setting for Antivirus Check (Do not allow encrypted attachments)
- Allow specifying AES-256 / 3DES in ruleset. (set parameter 3 in encrypt_smime or parameter 1 in encrypt_domain_smime to 'aes256' if needed)

Note: You have to set AES256 / 3DES in ruleset generator AGAIN if you did so in a previous version

Note: Domain encryption always uses AES256

- Optimize ciphers for PFS

- Add new command "splitrecipients" to split up mails per recipient
- Enhancements in Outlook message download in GINA
- Add new languages (Dutch, Polish) to GINA GUI
- Add possibility to automatically delete old log archives
- Make GUI filter case-insensitive
- Show fingerprint in root certificates in GUI
- Only show GINA log in GUI when requested to speed up display
- Allow LFT users to use GINA GUI to send out large files
- Fix restore: apply system settings
- Fix root certificate import in GUI
- Fix hanging OpenPGP key creation if trying to issue a key for a user with an invalid mail address
- Fix cron job (automatic update of domain certificates, backup)

Version:6.5.5.3/6.6.5.3 (Released 2014-04-24)

(neu in 6.5.5.3)

(neu in 6.6.5.3) multitenant version

- Patch release: under certain circumstances, issuing SwissSign certificates with firmware 6.5.5.1 or 6.5.5.2 / 6.6.5.1 or 6.6.5.2 crashes the appliance. This update corrects this bug.

Version:6.5.5.2/6.6.5.2 (Released 2014-04-09)

(neu in 6.5.5.2)

(neu in 6.6.5.2) multitenant version

- Patch for CVE-2014-0160.
- Update clamav

NOTE: CVE-2014-0160 ("Heartbleed") only affects the local proxy. Update is only necessary if you do not want (or cannot) disable the local proxy under System/Advanced/GINA https Protocol/Enable local https proxy..."

Version:6.5.5.1/6.6.5.1 (Released 2014-04-01)

(neu in 6.5.5.1)

(neu in 6.6.5.1) multitenant version

- Correct error in setting cipher
- Automatically create LFT partition
- Enhancements in HIN Connector
- Add function to delete expired X.509 certificates
- Disable OpenPGP Secret key download
- Enhancements in SMS interface
- Enhancements in ldap_getcerts: Handle multiple entries with same mail address

Version:6.5.5 (Released 2014-02-24)

(neu in 6.5.5.)

- Allow to set cipher for S/MIME

NOTE: Default value is 3DES as quite a lot of recipients appear to have problems with AES-256

- Reprocessing support for OpenPGP has been added
- Bug fixes in SignTrust connector
- Enhancements in internal encryption
- Allow to specify key servers in ruleset generator
- Enhance GUI performance when DNS server not reachable

Version 6.5.4.1 (Released 2013-11-11)

(neu in 6.5.4.1)

- Make sure sender address is used when replying to a GINA mail

Version 6.5.4 (Released 2013-11-08)

(neu in 6.5.4)

- Allow https backends for local proxy
- Perfect Forward Security for most browsers if local proxy is enabled
- Allow pkcs12 upload for ssl certificates
- Update ClamAV Engine
- Fix some minor issues in GINA GUI
- Add loadbalancer for SMTP connections
- Add filter functionality for some parts of the admin GUI
- use AES256 as default cipher for S/MIME (replacing 3DES)
- Show information about used S/MIME cipher in log

Version 6.5.3 (Released 2013-09-23)

(neu in 6.5.3)

- Add a certificate cleanup function to delete unneeded S/MIME certificates
- Add function to make GINA initial password change optional
- Fix domain certificate refresh invoked from GUI
- Fix an issue with domain encryption to recipients with solutions from another vendors
- Fix log detail display
- Move AV patterns to different location

Version 6.5.2 (Released 2013-08-22)

(neu in 6.5.2)

- Changes in HIN Connector
- Use RFC-compliant S/MIME encryption for S/MIME domain encryption with other gateways
- Correct a bug when using more than one GINA domains (special settings not applied to different domains)
- Performance / stability enhancements

Version 6.5.1 (Released 2013-07-06)

(neu in 6.5.1)

- Changes in HIN Connector
- Make proxy for GINA PCI compliant
- Update sms connector
- Send all public keys in daily statistics
- Ldap public key retrieval for S/MIME and OpenPGP
- Better memory management for GINA mail creation
- Allow use of variables in ldap queries
- Changes for 5000B appliances
- Corrections in S-TRUST connector (cn in automated user generation, leading zeroes in serial for key revocation)

Version 6.5.0 (Released 2013-04-04)

(neu in 6.5.0)

- Update base system
- Large File Transfer: Allow to send large files by mail
- Disable legacy GINA interface (old messages can still be read)
- Add audit log

Version 6.1.6 (Released 2013-01-08)

(neu in 6.1.6)

- Allow to change the SMTP greeting
- Make sure log index creation is only started once on very slow systems
- Correct a html error in the GINA attachment (better compatibility with some webmail systems like gmail)

NOTE: After the update, Expect about 30% more space requirement on the log partition.

Version 6.1.5 (Released 2012-12-13)

(neu in 6.1.5)

- Enhanced log search
- Enhanced S/MIME v 3.1 support for decrypting

Version 6.1.4 (Released 2012-11-29)

(neu in 6.1.4)

- Enhancements in HIN connector
- Allow / keep disclaimer in OpenPGP encrypted mails
- Correctly handle pgp encryption if mail part has no character set attribute
- Fix file upload in GUI (e.g. backup restore)
- Correctly display opaque signed mails in GINA
- Enhancements in HIN connector

Version 6.1.3 (Released 2012-10-31)

(neu in 6.1.3)

- Update ClamAV
- Make sure /tmp partition gets cleaned up
- Add Device ID in subject of backup mail
- Do not display question / answer in GINA registration if no question / answer is required
- Corrections in SignTrust connector
- Make admin GUI cross-site scripting resistant
- Send authlog to syslog server, include GUI and GINA logins
- Enhancements in SMS sender
- SMS text for passwords can now be edited

Version 6.1.2 (Released 2012-10-03)

(neu in 6.1.2)

- Update ClamAV
- Re-enable GINA security level without reminder / question
- Correct "last used" date in daily statistics mail
- Always use utf-8 for OpenPGP encryption
- Prevent kernel panics when restarting services with active CARP connections

Version 6.1.1 (Released 2012-08-15)

(neu in 6.1.1)

- Better recognition of OpenPGP encrypted mails
- Nicer Admin GUI
- is_calendar also recognizes Lotus Notes calendar entries
- Changes in HIN Connector
- Update Clam Antivirus
- Allow setting headers in ruleset generator
- Fix Backup Download

Version 6.1.0 (2012-05-22)

(neu in 6.1.0)

- Completely remove cookies for GINA
- Allow Wildcard certificate creation for ssl
- Add Spanish as GINA language
- Add Support for S-Trust MPKI
- Add Support for SignTrust MPKI
- Enhanced sms password support (allow to specify mobile number in subject, pre-store numbers entered in sms link and subject, send sms from Admin GUI)
- Allow to add comments for CA and OpenPGP keys in GUI
- Enhanced group editing

- Enhancements for HIN connector
- Create nightly backup without restarting services
- Use signed domain certificates for domain encryption (instead of self-signed)
- *Note: If you are planning to use domain based encryption with java based secure e-mail gateways from other vendors, you should create new domain keys after updating. You do not need to revoke / delete the exiting keys.*
- Allow searching domain keys in GINA portal
- Enhanced sms support (allow sending OTP to sms from Admin GUI)
- Recipient does not have to enter mobile number if password reset is set to "let user choose between sms and hotline"
- GUI used to send sms can be made accessible in public interface
- Bulk import for S/MIME certificates

Version 6.0.0 (2011-11-10)

(neu in 6.0.0)

- Base system update
- VMware tools
- New Enhanced Secure Webmail viewer (called GINA)
- Outlook plugin available (<http://dl.seppmail.ch>)

NOTE: To enable the new webmail interface "GINA", activate "Use extended Webmail functionality" in "Mail Processing"

Version 5.3.7 (2011-11-10)

(neu in 5.3.7)

- Changes in HIN connector
- Enhanced SNMP support
- Allow update prefetch, show download status
- Move antivirus signatures to larger partition
- Allow update / support connections through SOCKS proxy
- Allow editing hosts file in GUI
- Show number of queued mails in GUI
- Enhanced OpenPGP filename detection
- Enable DSN for delayed mails

NOTE: You should check your time zone in System / Advanced after this update

Version 5.3.6.1 (2011-10-04)

(neu in 5.3.6.1)

- Hotfix for 5.3.6 Release: Make sure header changes are always written
- Enhancements for 3000B hardware
- Changes in HIN Auditing
- Enhanced recognition of special charsets in Webmail viewer
- Add correction for leap seconds to ntp
- Add bulk import for S/MIME certificates
- Show e-mail size in GUI log
- retain leading comment lines in uploaded ruleset

Version 5.3.5 (2011-07-30)

(neu in 5.3.5)

- Changes in HIN connector / HIN Auditing
- Allow local DNS overriding
- Update virus engine
- Correctly handle mails that are encrypted twice
- Do not re-encrypt mails that are already S/MIME encrypted
- Automatically repair simple cluster failuers
- Corrections in ESW viewer for special character sets

Version 5.3.4 (2011-04-14)

(neu in 5.3.4)

- Enhancements in HIN connector
- Correctly change filenames when encrypting text attachments with OpenPGP
- Only activate proxy when a correct servername is specified
- Correct an error in webmail password reset
- Only use self-signed GUI certificate if the official certificate fails to load
- Add new Ruleset generator open "Do not encrypt, but sign"

Version 5.3.3 (2011-03-10)

(neu in 5.3.3)

- Enhancements in HIN connector
- Enhancements in OpenPGP attachment handling / charset handling
- Enhancements in header encoding

Version 5.3.2 (2011-01-15)

(neu in 5.3.2)

- Enhancements in HIN connector
- Check outgoing mails for viruses instead of only incoming
- Correct watchdog to ignore domain refresh errors if "Auto-Update S/MIME Domain Certificates" is not checked
- Make sure S/MIME and OpenPGP keys are used if a mail is marked as confidential and "Always use S/MIME or OpenPGP if keys are available" is not enabled

Version 5.3.1 (2011-01-15)

(neu in 5.3.1)

- Enhancements in HIN connector
- Allow to attach disclaimers to "in-reply-to" messages

Version 5.3.0 (2011-01-12)

(neu in 5.3.0)

- Add optional HIN (Health Information Net) connector
- Update Incamail Connector to support Incamail 3
- Add OpenPGP/MIME functionality for OpenPGP domain encrypted mails
- Switch to SHA1 for TLS fingerprint checking. *(Note: You must manually change fingerprint settings if you use fingerprint checking)*
- Allow same tag for "decrypted" and "confidential"
- Clean up mail received headers (localhost)
- Show RAID status in GUI for 3000B hardware
- Add S/MIME Version 3.1 support
- Watchdog now also watches ntp daemon
- user-friendly colors in GUI
- Allow to edit user names

Version 5.2.2.1 (2010-09-15)

(neu in 5.2.2.1)

- Add line breaks in long lines in Webmail Viewer text view

Version 5.2.2 (2010-09-15)

(neu in 5.2.2)

- SuisselD support for Webmail authentication
- New web server for enhanced https Support
- Show RAID status in GUI on enterprise hardware
- Allow adding disclaimer in base64-encoded emails

Version 5.2.1 (2010-06-21)

(neu in 5.2.1)

- Daily reports are sent to members of group statsadmins (and to members of group admin and the postmaster if they are important)
- Enhancements in displaying embedded graphics in secure webmails
- New rule engine wizard option "create all users"
- New rule engine command to parse email body
- Allow sending virus notifications to a pre-defined email address

Version 5.2.0 (2010-04-30)

(neu in 5.2.0)

- Update base system
- Consolidated statistics in clustered environment
- Display embedded images in webmail viewer
- Strictly use POST instead of GET in webmail viewer
- Text-only webmail container
- Allow to disable msg download in webmail viewer (note: Defaults to on)
- New security level for simpler use (no question / reminder)
- PCI compliance for SMTP TLS in opportunistic mode
- Allow hiding mail subject in log files
- Enhanced watchdog with cluster connectivity checks
- New rule engine wizard option to delete smime signatures from incoming mail
- Per-user / per-domain usage counters
- New state "undefined" for unknown CA certificates
- Automatically renew locally issued Certificates if existing certificates are about to expire
- Automatically renew SwissSign Certificates if existing certificates are about to expire
- Daily status / throughput report mail
- Selective Reverse Proxy (for customers with one single IP address)
- Additional "undefined" state for auto-collected CA root certificates
- New rule engine command to disable a user

Version 5.1.7.3 (2010-01-20)

(neu in 5.1.7.3)

- Revert Changes for normalized subjects in log as it leads to delayed delivery of emails if the subject is malformed

Version 5.1.7.2 (2010-01-18)

(neu in 5.1.7.2)

- Allow to use non-selfsigned pgp keys
- Include Antivirus Engine in watchdog
- Display normalized subject in Log

Version 5.1.7.1 (2010-01-06)

(neu in 5.1.7.1)

- Make sure spamassassin updates are fetched
- cosmetic change in SwissSign connector setup

Version 5.1.7 (2009-12-22)

(neu in 5.1.7)

- Correct an issue with entering the phone number when the recipient forgets his password
- Re-schedule nightly domain certificates update to prevent update server overload
- Show last successful domain certificates refresh in GUI
- Correct an issue with S/MIME signed and encrypted mails in domain encryption mode

Version 5.1.6 (2009-12-10)

(neu in 5.1.6)

-
- Strict input checking for Webmail viewer
 - No RFC compliance check for incoming signed mails
 - Template based webmail domains
 - Enhancements in secure webmail password reset
 - New ruleset wizard option: Do not sign single emails

Version 5.1.5 (2009-11-24)*(neu in 5.1.5)*

- Template-based webmail domains
- Enhancements in secure webmail password reset

Version 5.1.4 (2009-11-11)*(neu in 5.1.4)*

- Enhancements in pgp key generation
- Allow bulk import of OpenPGP secret keys
- Add header info about spam check
- Enhancements in disclaimer
- Prepare for base system upgrade

Version 5.1.3 (2009-10-27)*(neu in 5.1.3)*

- Add chain to signed emails
- Update root certificates
- Automatically purge expired root certificates
- Enhanced signature detection
- Stricter license Checking
- Allow SMTP recipient verification without antispam license
- Hide domain cert list
- Hide subject in domain encrypted emails

Version 5.1.2 (2009-09-27)*(neu in 5.1.2)*

- Enhanced detection of S/MIME signed / encrypted emails
- Enhanced detection of OpenPGP encrypted emails
- More detailed logging
- Display basic network configuration on console
- Small corrections in default disclaimer
- Do not sign outlook calendar entries if "sign all"
- Enhancements in SwissSign connector

Version 5.1.1 (2009-08-24)*(neu in 5.1.1)*

- Add support for OpenPGP/MIME for incoming mails
- Enhanced filename detection for pgp encrypted emails
- RFC conform headers in webmail viewer
- Prevent ntpd from blocking if network is unreachable
- Do not add disclaimer in replies
- Allow to trust untrusted root CAs
- Enhanced factory reset (overwrite data with random numbers)

Version 5.1.0 (2009-08-07)*(neu in 5.1.0)*

- New ruleset command "create key"
- Enhancements in CA including revocation and revocation lists

- Enhancements in SwissSign connectivity including revocation
- TLS logging in mail log
- Allow to disable encryption / signing for specific users
- Change pgp key sender
- Allow disabling automatic pgp key delivery for new users
- Easy "disclaimer per domain" settings
- Automatically add unknown root certificates as "untrusted"
- Added new command to remove S/MIME signatures
- Updated ruleset generator: Always use webmail accounts, mark signed mails
- Secure factory reset (10 x random overwrite of data partitions)
- Enhanced logging for certificate harvesting
- Enhanced certificate harvesting, now also works for "exotic" certificates
- Auto rollout for communication initiated by external communication partners
- Correct Carriage Return / Line feed for HTML headers

Version 5.0.6 (2009-07-02)*(neu in 5.0.6)*

- Include Extended user attributes in user display
- Include certificate chain in S/MIME signatures
- Correctly handle empty ldap attributes in ldap_read and ldap_compare
- Enhanced reprocess to re-decrypt emails
- change format of openpgp filenames to utf-8 when encrypting
- Enhancements in openpgp decryption
- Prepare for new Hardware with larger memory

Version 5.0.5 (2009-06-25)*(neu in 5.0.5)*

- New ruleset command to set extended user attributes
- enhancements in pgp compatibility
- add a workaround for PIX smtp proxy
- remember language chosen in webmail viewer
- add favicon
- CA parameters can be configured
- allow multi-value in ldap requests
- re-enable SMTP out for smarthost

Version 5.0.4 (2009-06-19)*(neu in 5.0.4)*

- Add zipped HTML can be activated on a per-user basis
- Automatically activate zipped HTML if the recipient uses OWA
- Optimized user generation in conjunction with ldap lookups
- Allow multivalue ldap compares
- Make sure pgp keys are only created once in clustered environments
- Re-enable disclaimer and template editor
- update some third party applications
- Use blacklist / whitelisting entries for greylisting

Version 5.0.3.1 (2009-06-03)*(neu in 5.0.3.1)*

- Re-activate disclaimer
- Correct occasional problem in zipped webmail delivery

Version 5.0.3 (2009-06-01)*(neu in 5.0.3)*

- Allow to use SMS gateway to send webmail passwords

- Allow to use [zip] or [owa] in subject to force zipped webmail attachment
- Enhancements in queueless mode
- Allow password reset in "Secure contact form"
- ASPSMS connection using xml to send password by sms
- Some cosmetic codepage corrections in webmail Viewer

Version 5.0.2 (2009-05-17)

(neu in 5.0.2)

- Increase compatibility for webmail with some webmail clients
- Correct display of text-only mails in webmail Viewer

Version 5.0.1 (2009-05-13)

(neu in 5.0.1)

- Queueless mode can be configured with GUI
- Allow to configure default language for webmail viewer
- Allow to completely change webmail display using CSS and additional images
- Allow querying redundant LDAP servers
- Include message subjects in log display
- Allow to enable "send copy to myself" by default
- More detailed license display
- Prepare webmail for arabic language
- New "Secure Contact Form" allows user initiated webmail communication

Version 5.0.0 (2009-04-14)

(neu in 5.0.0)

- Complete Incamail integration
- New ruleset wizard option: Reject mails that cannot be decrypted
- Optimize service start order
- Restrict https to high security ciphers
- Allow to specify TLS settings for internal domains
- webmail password complexity can be specified
- Additional cookie security for webmail viewer
- Add "Change Password" to login page
- Prepare for PCI compliance audit
- Optionally add webmail HTML messages in ZIP file (for OWA compatibility)
- Whitelisting entries for greylisting
- Allow different webmail templates for same domain
- Correct bug: password mail if more than one webmail user is created
- Correct bug: Display of queued mails
- Correct bug: complex filenames in OpenPGP encrypted emails

NOTE: For PCI compliance, IE 7 or higher must be used for GUI access

Version 4.8.2 (2009-02-08)

(neu in 4.8.2)

- Enhanced Frontend server
- Correct Error in Watchdog
- Disable spam checking for mails fetched from remote POP3 server
- New feature to re-process old emails that were received encrypted

Version 4.8.1 (2009-02-02)

(neu in 4.8.1)

- Allow definition of sender mail addresses in password mails
- Less restrictive syntax checking for webmail replies

Version 4.8.0 (2009-01-26)*(neu in 4.8.0)*

- Enhancements in SwissSign connector
- Enhanced pgp key generation
- "Secure contact" frontend for external users
- Allow disabling "Powered by..." logo in User frontend

Version 4.7.1 (2008-12-31)*(neu in 4.7.1)*

- SNMP Support
- Automatic SwissSign CA certificate rollout
- Enhanced Rule Generator
- Queue-less mode for reinjection
- Enhanced signing key selection
- Frontend server without local database
- Include VMWare tools
- Restrict user access to defined GUI sections
- New rule engine commands for direct LDAP / AD connection

Version 4.7.0 (2008-07-25)*(neu in 4.7.0)*

- Antivirus Engine Update
- Enhanced virus scanning
- Exchange 2007 compatibility improvements
- Enhanced memory management
- Minor improvements in webmail viewer
- Introduce bridging mode
- Improvements in cluster environment.

Version 4.6.1 (2008-05-12)*(neu in 4.6.1)*

- Better support for OpenPGP keys
- Support for intermediate certificates for ssl
- Enhanced log search
- Some cosmetic changes in webmail viewer
- Update base system
- Enhanced anti-spam features

Version 4.6.0 (2008-03-31)*(neu in 4.6.0)*

- Automatically fetch new license files
- Enhanced license management
- Enhancements in Antispam
- Allow site-specific TLS setup
- Allow to specify alternate SMTP port
- New, enhanced webmail viewer
- Automatically reboot after update
- Allow webmail download as outlook message files (beta)

Version 4.5.3 (2008-03-04)*(neu in 4.5.3)*

- allow automatic issuing of OpenPGP keys
- accelerated OpenPGP key generation
- correct small bug in Backup routine

- Allow ssh connections through http proxy
- add subject tagging of decrypted emails

Version 4.5.2 (2008-02-24)

(neu in 4.5.2)

- correct small bug in Backup routine

Version 4.5.1 (2008-02-20)

(neu in 4.5.1)

- Include license violation display
- New ruleset option: Do not auto-encrypt with S/MIME or oePGP
- Allow disabling console login
- Update notification in home section
- Introduced virtual appliances flavours
- Allow to specify a syslog server for maillogs

Version 4.5.0 (2008-01-10)

(neu in 4.5.0)

- Change position of "Powered by..." logo
- Update AV Engine
- Allow to specify webmail pw length in ruleset
- Allow specification of "[emptypw]" in default ruleset
- Cleanup trigger values in subject before sending

Version 4.4.1 (2007-12-21)

(neu in 4.4.1)

- Show network / carp status in GUI
- Allow mail addresses with underscore for users
- Correct statistics for domain encryption
- Correct error in GUI when first carp disabled
- Enable direct SMS delivery for webmail passwords
- Update S/MIME root certificates
- Add "Powered by..." logo to webmail display

Version 4.4.0 (2007-11-22)

(neu in 4.4.0)

- Introduced a learning mode for Greylisting
- Enhanced webmail confirmations
- Allow specification of SMTP port
- Add new ruleset command "rmatch" to check recipients
- Add new ruleset command "webmail_password" to re-send password to sender
- Support for new hardware platform
- Added spam information to log files
- Added dcc and pyzor functionality to VSPP
- Include SSL/CA Certificates in Backup

Version 4.3.3 (2007-10-10)

(neu in 4.3.3)

- Increase stability of SMTP daemon under high load
- Enhanced watchdog
- Optimize webmail for Firefox

Version 4.3.2 (2007-10-04)

(neu in 4.3.2)

- Small bug fix (enable password reset for locked accounts)

Version 4.3.1 (2007-09-31)*(neu in 4.3.1)*

- Enable Postmaster warnings
- correct bug in pgp_detect
- Include mail fetcher for POP3 accounts
- Allow "low security" password retrieval for webmail
- New "queue-less" mode

Version 4.3.0 (released 2007-09-10)*(neu in 4.3.0)*

- Internal CA / RA
- Enhanced webmail logging
- webmail Delivery Reports
- Only accept emails for existing users
- Optional internal mailserver
- Enhanced antispam settings (PTR check)
- Ruleset enhancements: Allow force webmail encryption

Version 4.2.4 (2007-05-14)*(neu in 4.2.4)*

- Update base system to OpenBSD 4.1
- Enhanced performance for Appliances with CF cards
- Added italian support in webmail
- Added a rule for LDAP lookups on remote hosts
- Enhanced statistics, include CPU and memory load
- Fixed condition with non-restarting mail daemon after backup
- Fixed "too many recipients" error
- Fixed condition under which CARP interfaces did not reclaim lost IP
- Add handling for aliases in OpenPGP keys
- Minor bug fixes

Version 4.2.3 (2007-05-14)*(neu in 4.2.3)*

not released, see 4.2.4

Version 4.2.2*(neu in 4.2.2)*

not released, see 4.2.4

Version 4.2.1*(neu in 4.2.1)*

not released, see 4.2.4

Version 4.2.0*(neu in 4.2.0)*

not released, see 4.2.4

Version 4.1.0 (2007-03-26)*(neu in 4.1.0)*

- Generate S/MIME certificates
- S/MIME-based domain encryption

- S/MIME-based domain signature
- Anti-Spam / Anti-Virus module
- Corrected error in SMTP authentication for outgoing emails
- No clear text password in GUI for webmail passwords
- Creator of webmail accounts stored
- introduced an "expired" flag for webmail passwords
- allow http protocol for webmail
- allow specification of webmail port(s)
- Enhanced error handling in webmail reply
- Allow adding multiple managed domains in one step
- Implemented process for automated reset of forgotten passwords
- Allow permanent change of root password
- Added a restricted backup user
- Added a tmp partition on S3000 systems
- Added a permanent partition for user-specific data
- Major performance improvements
- Added functionality to archive emails
- Possibility to request a copy of a webmail reply to the sender
- Auto-generate and publish / download domain certificates
- (note: activated by default!)
- Only user with an account can encrypt E-mails

Version 4.0.0 (2007-01-31)

(neu in 4.0.0)

- Registration
- Drivers for new Hardware
- Allow easy remote support connection (reverse ssh tunnel)
- Allow removal of webmail domain settings
- Add support for user-defined mail disclaimers
- Multi master cluster / load balancing
- Virtual IP Addresses based on CARP for failover
- optimized openldap indexes
- speed enhancements in webmail encryption
- allow specifying password length for webmail passwords in GUI
- allow empty webmail passwords (must be set by recipient on first use)
- Enhancements in ssl certificate generation (well, actually fixed some bugs)
- remove Windows CR/LF in cert Upload
- removed obsolete lcd driver for pyramid displays
- Allow deletion of IP addresses in GUI (thus allowing specifying empty name servers)
- fixed problem of non-responding appliance if no DNS server can be found
- Update base system to OpenBSD 4.0
- Update postfix to 2.3.6
- Update openldap to 2.3.31
- Allow webmail recipients to specify a password reminder
- changed NIC name convention
- introduced TLS support
- include revision history
- Disable password-based ssh login

Version 3.3.0 (2007-01-24)

(neu in 3.3.0)

- Registration
- Drivers for new Hardware (SEPPmail 3000)
- Allow easy remote support connection (reverse ssh tunnel)
- Allow removal of SEPPmail domain settings
- Add support for user-defined mail disclaimers
- Multimaster cluster / load balancing

- Virtual IP Addresses based on CARP for failover
- optimized openldap indexes
- speed enhancements in seppmail encryption
- allow specifying password length for seppmail passwords in GUI
- allow empty SEPPmail passwords (must be set by recipient on first use)
- enhancements in ssl certificate generation (well, actually fixed some bugs)
- remove Windows CR/LF in cert Upload
- removed obsolete lcd driver for pyramid displays
- Allow deletion of IP addresses in GUI (thus allowing specifying empty nameservers)
- fixed problem of non-responding appliance if no DNS server can be found
- Update base system to OpenBSD 4.0
- Update postfix to 2.3.6
- Update openldap to 2.3.31
- Allow SEPPmail recipients to specify a password reminder
- changed NIC name convention
- introduced TLS support

Version 3.2.222 (2006-11-02)

(neu in 3.2.222)

- Group management
- graphical statistics for mail throughput based on rrd
- license management / import
- Allow CSV import / batch creation for webmail Users
- introduced webmail domains ("Mandantenfaehigkeit")
- HTML support in webmail messages display
- allow empty passwords for standard users
- support for multiple relay networks
- send pgp public key by mail
- include domain encryption in standard ruleset
- enhanced log display with search / archive
- allow upload of ssl certificates
- log rotation
- added smime root certificate manager
- added trustcenter and quovadis root certificates in base installation
- initial page with basic mail statistics
- webmail logs on per-user basis
- allow specification of max mail size
- webmail recipient interface in french

Version 3.2.0 (2006-07-21)

(neu in 3.2.0)

- LDIF Import
- Support for Pyramid LCD Displays
- Update to OpenBSD 3.8
- Enhancements in Backup procedure (Backup is sent by email)