



Secure Internet Traffic



COMPANYCRYPT®
The encryption module for MIMESweeper

Configuration Guide
CompanyCRYPT v1.5.0

Configuration Guide

CompanyCRYPT v1.5.0

© S.I.T. GmbH & Co. KG

Kaiser-Wilhelm-Str. 9 • 30559 Hannover • Germany

Telefon: +49 511 8999 710 • Telefax: +49 511 8999 712

Internet: www.companycrypt.com • eMail: info@companycrypt.com

© Copyright 2005-2014 by S.I.T. GmbH & Co. KG

Änderungen vorbehalten.

Das in dieser Dokumentation enthaltene Material ist das alleinige Eigentum der S.I.T.. Es ist untersagt die Veröffentlichung weder teilweise noch vollständig in irgendeiner Form oder unter zu Hilfenahme von jedweden elektronischen, mechanischen, fototechnischen, aufnahmetechnischen oder sonstigen widerherstellbaren Formen zu reproduzieren, verändern oder zu übermitteln, oder in einer sonstigen Art oder Weise zu Verwenden ohne die ausdrückliche Erlaubnis der S.I.T..

S.I.T. stellt diese Veröffentlichung „in der vorliegenden Form“ zur Verfügung und übernimmt keine Haftung für diese Dokumentation, auch nicht für ausdrückliche oder implizite Garantien oder die Eignung für einen bestimmten Zweck. Der Benutzer trägt das alleinige Risiko für die Benutzung dieser Information.

In keinem Fall kann S.I.T. für direkte oder indirekte, zufällige, spezielle oder resultierende Schäden haftbar gemacht werden, die auf irgendwelche Fehler in den Informationen beruhen, selbst wenn auf die Möglichkeit solcher Schäden hingewiesen wurde.

Weiterhin behält S.I.T. sich das Recht vor, diese Dokumentation ohne die Verpflichtung der vorherigen Benachrichtigung von Personen oder Organisationen von Zeit zu Zeit ohne Ankündigung zu verändern.

Die Verwendung der mit dieser Dokumentation gelieferten Software unterliegt der Lizenzvereinbarung von S.I.T.

Warenzeichen

MIMESweeper und *MAILSweeper* sind eingetragene Warenzeichen (TM) der Firma *CLEARSWIFT*.

CompanyCRYPT ist ein eingetragenes Warenzeichen (TM) der Firma *S.I.T. GmbH & Co. KG*.

Andere in dieser Dokumentation benutzten, aber hier nicht genannten Marken- oder Produktnamen sind Warenzeichen oder eingetragene Warenzeichen der entsprechenden Warenzeicheninhaber.



Secure Internet Traffic



COMPANYCRYPT®
The encryption module for MIMESweeper

Inhalt
Inhaltsverzeichnis

Configuration Guide
CompanyCRYPT v1.5.0

1. Inhalt



1.1. Inhaltsverzeichnis

1. Inhalt	2
1.1. Inhaltsverzeichnis	3
1.2. Dokumentinhalt	8
1.3. Begriffe	9
1.4. Support / Kontakt	10
2. Schnelleinstieg	11
2.1. Erstkonfiguration CompanyCRYPT	12
2.1.1. Hinterlegen der CompanyCRYPT-Lizenz	12
2.1.2. Definieren des Passwortes	12
Passphrase	12
2.1.3. Hinterlegen der Unternehmensdaten	13
2.1.4. Erstellen eines CA-Zertifikates	14
2.1.5. Erstellen der Unternehmensschlüssel	15
2.1.6. Erstellen von Schlüsseln für interne User	16
2.1.7. Schlüssel der externen Partner importieren	17
2.1.8. Automatischen Schlüsselimport aktivieren	18
2.2. Einrichtung der Ver-/Entschlüsselung	19
2.2.1. Einrichtung der Entschlüsselung	19
Einrichten der Classifications für die Entschlüsselung	19
Einrichten des CompanyCRYPT-Scenarios zur Entschlüsselung	21
2.2.2. Einrichtung Automatische Verschlüsselung mit Benutzersteuerung	22
Einrichten der Classifications für die automatische Verschlüsselung (Best Effort)	23
Erstellen des Szenarios für die automatische Verschlüsselung	24
Aktivieren der Benutzersteuerung	26
Konfiguration der Ad Hoc Encryption	26
2.2.3. Einrichtung einer Adressbasierten Verschlüsselung	27
Einrichten der Adresslisten	27
Einrichten der Classifications für die Adressbasierte Verschlüsselung	27
Erstellen des Scenario Folders	28
Einrichten des CompanyCRYPT-Scenarios für Adressbasierte Verschlüsselung	29
2.3. Funktionalität im Betrieb	32
2.3.1. Wie wird die Entschlüsselung aktiviert	32
2.3.2. Wie wird die Verschlüsselung aktiviert	32
Automatische Verschlüsselung „Best Effort“	32
Adressbasierte Verschlüsselung	32
2.3.3. Wie aktiviert der Benutzer die Verschlüsselung	32
Aktivierung durch Mailoption (Outlookintegration)	32
Aktivierung durch Schlüsselwort (Betreffzeilensteuerung)	32
2.3.4. Wie wird die Signierung aktiviert	33
Automatische Signierung „Company Signing“	33
Aktivierung durch Schlüsselwort (Betreffzeilensteuerung)	33
3. CompanyCRYPT	34



3.1. CompanyCRYPT–WebGUI	35
3.1.1. Aufruf der CompanyCRYPT–WebGUI	35
3.1.2. First Start / Initialisierung	36
3.2. CompanyCRYPT–SyncManager	37
3.2.1. Aufruf des CompanyCRYPT–SyncManager	37
3.3. Formateinstellungen	38
3.3.1. Spezifische Einstellungen für PGP	38
PGP-Verarbeitung Aktivieren/Deaktivieren	38
Passwort für PGP-Keys	38
3.3.2. Spezifische Einstellungen für S/MIME	38
S/MIME-Verarbeitung Aktivieren/Deaktivieren	39
Prüfung von Zertifikatsketten	39
Passwort für S/MIME-Zertifikate	39
3.3.3. Spezifische Einstellungen für Ad Hoc Encryption	40
Funktionsweise Verschlüsselung	40
Aktivierung der Ad Hoc Encryption	41
Konfiguration Ad Hoc Verschlüsselung	41
Referenznummer	42
Funktionsweise Entschlüsselung	43
Konfiguration Ad Hoc Entschlüsselung	44
Entschlüsselung beim Empfänger (Self Extracting ZIP)	44
Entschlüsselung beim Empfänger (Secure ZIP, Compatible ZIP)	45
3.4. Verschlüsselungsmöglichkeiten	46
3.4.1. Adressbasierte Verschlüsselung	46
Unterdrückung von Verschlüsselung und Signierung durch den Absender	46
3.4.2. Automatische Verschlüsselung „Best Effort“	46
Verarbeitung bei fehlendem Public Key des Empfängers	47
Ausnahmen zur Verschlüsselung	47
3.4.3. Benutzergesteuerte Verschlüsselung und/oder Signierung	47
Aktivierung von Verschlüsselung und Signierung	47
3.4.4. Automatische Signierung „Company Signing“	49
Signiereinstellungen für verschlüsselte Nachrichten	49
Signiereinstellungen für Klartextnachrichten	49
Ausnahmen zur Signierung von Klartextnachrichten	50
3.5. Keyserver + Keyresponder	51
3.5.1. Externe Keyserver	51
LDAP Verzeichnisdienste	51
Neuer LDAP-Dienst	51
Testabfrage	52
3.5.2. Interner Keyresponder – Schlüsselaustausch	52
Adresskonfiguration für automatischen Schlüsselversand	52
Automatische Schlüsselerstellung	53
Groupware-Schnittstelle (Referenzliste)	54
SMTP-Konfiguration für automatischen Schlüsselversand	55
SMTP-Konfiguration für automatischen Schlüsselversand per SyncManager	55
3.6. System Parameter	56
3.6.1. Statusanzeige	56
3.6.2. Backup und Restore	56
Backup / Restore Parameter	56
Automatisches Backup	56
Manuelles Backup	57
System wiederherstellen (Restore)	57
Backupdateien löschen	58
3.6.3. Einstellungen Systemdienste	58



Reprocess Service	58
Reprocess Service - Konfiguration per SyncManager	59
Reprocess Log	59
3.6.4. Logging	59
Trace Optionen und Logging-Parameter	59
Trace Log	60
3.6.5. Proxy Einstellungen	60
3.6.6. Zusammengefasste Verwaltungsfunktionen.....	61
Verwaltung der CompanyCRYPT-Dienste	61
Re-Initialisierung des Systems.....	61
MIMESweeper Einstellungen	62
3.7. Verteilte Systeme (Multi-Server)	63
3.7.1. Betriebsmodus.....	63
3.7.2. Modus: Single	63
3.7.3. Modus: Master	63
Modus: Master - Konfiguration per SyncManager	64
3.7.4. Modus: Slave	65
Modus: Slave - Konfiguration per SyncManager	66
Operational Log.....	67
3.8. Key-Management.....	68
3.8.1. Hinterlegen der Unternehmensdaten	68
Maildomänen und Systemadressen.....	68
Standardwerte für die Schlüsselerzeugung.....	68
Meldung Signatur/Entschlüsselungsergebnis (Decrypt Summary)	69
3.8.2. Unternehmensschlüssel – Central Signing Account (CSA).....	69
CSA-Schlüssel erstellen	70
CSA-Key anzeigen	71
3.8.3. Lokales Stammzertifikat (Onboard CA)	72
Erstellen eines CA-Zertifikates.....	72
Einbinden eines vorhandenen CA-Zertifikates	73
Anzeigen des CA-Zertifikates	74
Passwort für das CA-Zertifikat	75
Parameter zur Zertifikatserstellung	75
3.8.4. Trusted CA Store	76
Listendarstellung	76
Zertifikatseigenschaften.....	76
3.8.5. Verwaltung privater Schlüssel	77
Listendarstellung	77
Schlüsseleigenschaften – Private PGP Key.....	78
Schlüsseleigenschaften – Private S/MIME Certificate	79
Schlüssel per Mail versenden	80
Erstellen privater Schlüssel.....	80
Löschen privater Schlüssel.....	81
Signieren privater PGP-Schlüssel.....	82
3.8.6. Verwaltung öffentlicher (externer) Schlüssel	82
Listendarstellung	82
Schlüsseleigenschaften – Public PGP Key	83
Schlüsseleigenschaften – Public S/MIME Certificate	84
Löschen öffentlicher Schlüssel	86
Signieren öffentlicher PGP-Schlüssel	86
3.8.7. Import von Schlüsselmaterail	87
Import eines privaten PGP Schlüssels.....	87
Import eines privaten S/MIME Zertifikates.....	88
Import eines öffentlichen Schlüssels	90
Upload von Schlüsselmaterail.....	91
3.8.8. Automatischer Import.....	92
Automatische Schlüsselerkennung	92



Automatischer Import von öffentlichen Schlüsseln	93
Automatischer Import von privaten Schlüsseln	93
Benachrichtigungseinstellungen	93
3.8.9. Site to Site-Verschlüsselung	93
Anzeigen der Site to Site-Verbindungen	94
Anzeigen der Schlüsseleigenschaften für Site to Site-Verbindungen	94
Erstellen einer Site to Site-Verbindungen	94
Löschen einer Site to Site-Verbindungen	95
3.9. CompanyCRYPT Lizenz	96
3.9.1. Lizenz eingeben	96
Lizenz eingeben per SyncManager	96
3.9.2. Lizenz löschen	97
Lizenz löschen per SyncManager	97
4. Einrichtung der Ver-/Entschlüsselung	98
4.1. Aufruf des MIMesweeper Policy-Editors	99
4.2. Allgemeine Informationen	100
4.2.1. Adresslisten	100
Übersicht der Adresslisten	100
4.2.2. Classifications	100
Classifications für CompanyCRYPT	100
4.2.3. Scenario Folder	101
Übersicht der Scenario Folder	101
4.2.4. CompanyCRYPT Scenarios	102
CompanyCRYPT-Scenarios – Weiterführende Informationen	102
4.3. Entschlüsselung	104
4.3.1. Funktionsbild - Entschlüsselung	104
4.3.2. Einrichtungsschritte zusammengefasst	104
4.3.3. Einrichtung der Entschlüsselung	105
Einrichten der Classifications (Entschlüsselung)	105
Einrichten der CompanyCRYPT-Scenarios (Entschlüsselung)	106
4.4. Verschlüsselung – Grundlegende Unterscheidung	109
4.4.1. Funktionsbild – Unterscheidung der Verschlüsselungskategorien	109
4.5. Adressbasierte Verschlüsselung	110
4.5.1. Funktionsbild – Adressbasierte Verschlüsselung	110
4.5.2. Einrichtungsschritte zusammengefasst	110
4.5.3. Einrichtung der Adressbasierten Verschlüsselung	111
Einrichten der Adresslisten für die Adressbasierte Verschlüsselung	111
Einrichten der Classifications für die Adressbasierte Verschlüsselung	111
Erstellen der Scenario Folder für die Adressbasierte Verschlüsselung	113
Einrichten der CompanyCRYPT-Scenarios für die Adressbasierte Verschlüsselung	113
4.6. Site To Site Verschlüsselung	116
4.6.1. Funktionsbild – Site To Site Verschlüsselung	116
4.6.2. Einrichtungsschritte zusammengefasst	116
4.6.3. Einrichtung der Site To Site Verschlüsselung	117
Einrichten der Adresslisten für die Site To Site Verschlüsselung	117
Einrichten der Classifications für die Site To Site Verschlüsselung	117
Erstellen der Scenario Folder für die Site To Site Verschlüsselung	119
Einrichten der CompanyCRYPT-Scenarios für die Site To Site Verschlüsselung	119
Erzeugen eines Site to Site-Link	121



4.7. Automatische Verschlüsselung "Best Effort"	123
4.7.1. Funktionsbild – Automatische Verschlüsselung (Best Effort)	123
4.7.2. Einrichtungsschritte zusammengefasst	123
4.7.3. Einrichtung der Automatischen Verschlüsselung	124
Einrichten der Classifications für die automatische Verschlüsselung (Best Effort)	124
Erstellen des Szenarios für die automatische Verschlüsselung (Best Effort)	125
4.8. Anwender gesteuerte Verschlüsselung "User Control"	128
4.8.1. Funktionsbild – Anwender gesteuerte Verschlüsselung (User Control)	128
4.8.2. Einrichtungsschritte zusammengefasst	128
4.8.3. Einrichtung der Anwendergesteuerten Verschlüsselung	129
Einrichten der Classifications für die Anwender gesteuerte Verschlüsselung	129
Erstellen des Szenarios für die Anwender gesteuerte Verschlüsselung (User Control)	130
Aktivieren der Benutzersteuerung	132
4.9. Einrichtung der Signierung	134
Adressbasierte Signierung	134
Automatische Signierung „Company Signing“	134
Aktivierung durch Schlüsselwort (Betreffzeilensteuerung)	134
4.10. Keyresponder (MIKE - Mail Initiated Key Exchange)	135
4.10.1. Funktionsbild – Keyresponder für externe Partner	135
4.10.2. Einrichtungsschritte zusammengefasst	135
4.10.3. Einrichtung des Keyresponders	136
Einrichten der Classification für automatischen Schlüsselaustausch	136
Erstellen des Scenario Folder für automatischen Schlüsselaustausch	137
Einrichten des Keyresponder-Szenario (MIKE - Mail Initiated Key Exchange)	137
Adresskonfiguration für automatischen Schlüsselversand	140
4.10.4. Funktionsbild – Keyresponder für interne Anwender	141
4.10.5. Einrichtungsschritte zusammengefasst	142
4.10.6. Einrichtung des Keyresponders für interne Anwender	142
Weiterleitung der Keyserveradresse aus der Groupware	142
Erweiterung des Scenario Folder für automatischen Schlüsselaustausch	142
Domänenkonfiguration für automatischen Schlüsselversand	142
4.11. Erweiterte Konfiguration zur Funktionskontrolle	144
4.11.1. Protokollierung der Ver- und Entschlüsselung	144
Einrichten der Message Areas	144
Message Areas im MIMESweeper Manager einrichten	145
Erweitern der Entschlüsselungs Classification für die Protokollierung	147
Erweitern der Verschlüsselungs Classification für die Protokollierung	149
5. Anhänge	151
5.1. Anhang: Entschlüsselung	152
5.1.1. Entschlüsselung – Verfügbare Szenarios	152
5.1.2. Entschlüsselung – Verarbeitungsdetails	153
5.2. Anhang: Verschlüsselung	155
5.2.1. Verschlüsselung – Verfügbare Szenarios (Nach Methode gruppiert)	155
5.2.2. Verschlüsselung – Wahl des passenden Jobs	158
5.2.3. Site-to-Site/Gruppen Verschlüsselung – Wahl des passenden Jobs	159
Standard Verschlüsselung vs. Site-to-Site Verschlüsselung (Gruppen-Schlüssel)	159
6. Empfehlungen / Praxis	160



Secure Internet Traffic



COMPANYCRYPT®
The encryption module for MIMesweeper

Inhalt
Dokumentinhalt

Configuration Guide
CompanyCRYPT v1.5.0

1.2. Dokumentinhalt

Dieses Dokument beschreibt die Konfiguration von *CompanyCRYPT®* und die Einbindung in das Produkt *Clearswift® MIMesweeper for SMTP®*. Es gibt Ihnen Hilfestellung bei der Einrichtung der eMailverschlüsselung. Die Installation von *CompanyCRYPT®* wird in einem separaten Dokument – *Installation Guide* - beschrieben.



1.3. Begriffe

Für eine bessere Lesbarkeit werden folgende Begriffe, bzw. Vereinfachungen in diesem Dokument verwendet:

Ad Hoc Verschlüsselung	Passwortgestützte Verschlüsselungsmethode, die keine PGP- oder S/MIME-Software beim Empfänger voraussetzt.
Classification	Configurations/Policy Objekt welches im MIMESweeper benutzt wird.
CA	Certification Authority – Beglaubigende Instanz für S/MIME Zertifikate/Schlüssel.
Decrypt summary	Entschlüsselungszusammenfassung, die CompanyCRYPT in eine eMail befügt.
Detached	(Auch Clearsign) Eine Signaturform, bei der die Signatur an die signierten Daten ‚angehängt‘ wird. Die signierten Daten bleiben unverändert.
Inline PGP	Alternative Schreibweise für PGP/Inline
MIMESweeper for SMTP	Das Softwareprodukt MIMESweeper for SMTP® der Firma Clearswift®.
Opaque	Eine Signaturform, bei der die binäre Signatur mit den signierten Daten zu einem neuen Daten-Block verarbeitet wird.
OpenPGP	OpenPGP ist ein Standard für Verschlüsselungs-Software. Der Internet-Standard ist im RFC 4880 standardisiert.
PGP/Inline	Bezeichnet das durch den OpenPGP-Standard definierte Textformat für Verschlüsselung und Signatur.
PGP/MIME	Bezeichnet das durch den OpenPGP-Standard definierte Format für Verschlüsselung und Signatur von E-Mails. (MIME-Erweiterung nach RFC 3156)
Scenario	Configurations/Policy Objekt welches im MIMESweeper benutzt wird.
S/MIME	(Secure / Multipurpose Internet Mail Extensions) ist ein Standard für die Verschlüsselung und Signatur von E-Mails auf Basis eines asymmetrischen Kryptosystems.
WebGUI	Die Browser-basierte Konfigurationsoberfläche von CompanyCRYPT



Secure Internet Traffic



COMPANYCRYPT®
The encryption module for MIMESweeper

1.4. Support / Kontakt

Telefon	Hotline (werktags 09:00 - 17:00) +49 511 - 89 99 711
eMail	support@companycrypt.com
Internet	www.companycrypt.com

Bei Anmeldung: Zugang zu geschützten Bereichen mit:

- Aktuelle Versionen
- Hotfixes, Patches, MaintenancePacks
- Technische FAQ
- Dokumentation
- Ggf. Tech. Newsletter



2. Schnelleinstieg

Dieses Kapitel erklärt Ihnen Schritt für Schritt, welche Einstellungen in CompanyCRYPT und im MIMESweeper vorzunehmen sind, um die eMail-Verschlüsselung nutzen zu können. Ziel ist eine Konfiguration, mit welcher sowohl mit S/MIME- als auch PGP-verschlüsselte eMails mit Ihren eMail-Partnern ausgetauscht werden können.

Die Beschreibung bezieht sich auf die Konfiguration eines einzelnen Systems (Stand alone). Wird eine verteilte Umgebung mit mehreren MIMESweeper-Systemen eingesetzt, so sind ggf. Konfigurationsschritte auf allen Systemen notwendig.

Um die Einstellungen der nachfolgenden Abschnitte vornehmen zu können, muss CompanyCRYPT inklusive der Weboberfläche vollständig installiert sein. Die korrekte Vorgehensweise wird in einem separaten Dokument, der Installationsanleitung, beschrieben.

2.1. Erstkonfiguration CompanyCRYPT

Nachdem Sie die CompanyCRYPT-WebGUI entsprechend der Installationsanleitung eingerichtet haben, kann die Administrationsoberfläche durch Eingabe der entsprechenden Adresse im Browser aufgerufen werden.

`http://<MIMESweeper-Host>/CCWEB`

2.1.1. Hinterlegen der CompanyCRYPT-Lizenz

WebGUI → (Info) About → Licence

Um in CompanyCRYPT Konfigurationseinstellungen vornehmen zu können, ist es als erstes erforderlich die Lizenzangaben einzutragen. Beim Starten der WebGUI wird automatisch die entsprechende Seite geöffnet. Sollte nach dem ersten Start der Weboberfläche noch der Initialisierungsbildschirm angezeigt werden, so bestätigen Sie diesen mit OK.

Licence	
Status:	VALID
Company:	<input type="text" value="Company name"/>
Serial:	<input type="text" value="serial number"/>
Licence key:	<input type="text" value="licence key"/>
MSW Serial:	<input type="text" value="2129-0536-1004-6000"/>
Users:	<input type="text" value="50"/>
Valid until:	<input type="text" value="unlimited"/>
<input type="button" value="Store Licence"/>	

Unter Licence übertragen Sie bitte in die Felder **Company**, **Serial** und **Licence key** die Daten aus dem Licence Record. Achten Sie hierbei auf exakte Schreibweise (Groß-/Kleinschreibung) bei Company. Anschließend speichern Sie die erfassten Daten mit **Store Licence**.

Hinweis: Für die Eingabe des Licence keys ist die Groß-/Kleinschreibung ohne Bedeutung.

Wichtig: Wenn Ihr MIMESweeper als dedizierter *Primary Configuration Server* (PCS) konfiguriert ist, d.h. kein *Policy Server* (PS) auf dem System aktiv ist, werden die Lizenz Informationen durch den ersten Synchronisationskontakt mit einem anderen CompanyCRYPT (Slave) System übertragen. Weitere Informationen zu Multi-Server-Umgebungen entnehmen Sie bitte dem *Installation Guide*. Erst nach einem erfolgreichen Synchronisationskontakt werden Sie Zugang zu der vollständigen WebGUI auf diesem (Master) System erlangen.

2.1.2. Definieren des Passwortes

Das Passwort wird für die Erzeugung und Verwaltung der eigenen Schlüssel benötigt. Das Passwort sollte eine Länge von mindesten 10 Zeichen haben und idealerweise aus einer Kombination von Ziffern und Buchstaben bestehen.

Passphrase

WebGUI → (Configuration) Formats → PGP → Passphrase

Definieren Sie nun das Passwort. Dieses Passwort wird für den Zugriff auf alle internen PGP- und S/MIME-Schlüssel (Private Keys) sowie das CA-Zertifikat verwendet. Tragen Sie also in das Feld **New Passphrase** das gewünschte Passwort ein und wiederholen Sie die Eingabe im Feld **Confirm Passphrase**. Speichern Sie das Passwort mit dem Button **Set Passphrase**.

Passphrase Not set	
New Passphrase (8-128 char.):	<input style="width: 90%;" type="password"/>
Confirm Passphrase:	<input style="width: 90%;" type="password"/>
<input type="button" value="Set Passphrase"/>	

2.1.3. Hinterlegen der Unternehmensdaten

Damit später, bei der Erzeugung der Schlüssel für die internen User, nicht alle Daten immer wieder neu angegeben werden müssen, empfiehlt sich die Hinterlegung von Standardwerten.

WebGUI → (Key Management) Central Accounts → Company ID

Tragen Sie Ihre SMTP-Domäne unter **Primary SMTP domain** ein und ggf. weitere Domänen unter Additional domains. Wählen Sie eine Absender- sowie eine Zieladresse für den Versand von Systeminformationen. Geben Sie zusätzlich eine Absenderadresse für den Versand von User-Informationen an. Speichern Sie die Einstellungen mit **Apply Changes**.

Company SMTP Domain(s)	
Primary SMTP domain:	<input style="width: 90%;" type="text" value="@company.com"/>
Additional domains:	<div style="border: 1px solid #ccc; height: 30px; width: 100%;"></div>
System Notifications:	FROM: <input style="width: 80%;" type="text" value="CompanyCRYPT@company.com"/> TO: <input style="width: 80%;" type="text" value="admin@company.com"/>
User Notifications:	FROM: <input style="width: 80%;" type="text" value="CompanyCRYPT@company.com"/>

Company SMTP Domain(s)

- Primary SMTP domain: @<Internetdomäne>
- Additional domains: (Optional) <Alias-/Internetdomänen>
- System Notifications: CompanyCRYPT-Systeminformationen für die Administration
- From: <Absender-Mailadresse>
- To: <Empfänger-Mailadresse> (Optional kann eine zweite Adresse angegeben werden.)
- User Notifications: Informationen an den User
- From: <Absender-Mailadresse>

Tragen Sie die gewünschten Daten ein, welche für alle internen Schlüssel gelten sollen. Die Felder **Department** und **Location** können leer gelassen werden. Speichern Sie die Einstellungen mit **Apply Changes**.

Key Defaults	
Company Name:	<input style="width: 90%;" type="text" value="Company"/>
Department:	<input style="width: 90%;" type="text"/>
Location:	<input style="width: 90%;" type="text"/>
Country code:	<input style="width: 40%;" type="text" value="DE"/> (2 Letter)
Keylength:	<input style="width: 40%;" type="text" value="2048"/> Bit
S/MIME valid for:	<input style="width: 40%;" type="text" value="730"/> Days
PGP valid for:	<input style="width: 40%;" type="text" value="0"/> Days (0 = unlimited)

Default Key Parameters

- Company Name: <Firmenname/-bezeichnung>
- Department: (Optional) <Abteilung / Organisationseinheit>
- Location: (Optional) <Stadt / Ort>
- Country code: 2-stellige Buchstabenkombination (DE für Deutschland)



Keylength:	2048 (Diese Schlüssellänge bietet auch für die Zukunft ausreichende Sicherheit. Längere Schlüssellängen sind aus Gründen der Kompatibilität derzeit nicht empfohlen.)
S/MIME valid for:	730 (Dieser Wert entspricht einer Gültigkeit von 2 Jahren)
PGP valid for:	0 (Dieser Wert entspricht einer unbegrenzten Gültigkeitsdauer.)

2.1.4. Erstellen eines CA-Zertifikates

WebGUI → (Key Management) Central Accounts → Onboard CA → CA Certificate

Das CA-Zertifikat benötigen Sie für die Erstellung eigener Anwender-S/MIME-Zertifikate.

1. Schritt

Um ein CA-Zertifikat zu erstellen, klicken Sie auf den Button **Generate**.

CA Certificate	
CA Certificate Status	
Public key file	Not found
Private key file	Not found
Passphrase	No Access
<input type="button" value="Generate..."/>	

2. Schritt

Tragen Sie in die Eingabefelder die gewünschten Daten ein. Es ist nicht notwendig, alle Felder auszufüllen. Die Felder **Department** und **Location** können leer bleiben.

CA Certificate	
Name: (min. 5 char)	Company Mail CA
eMail:	Certification.Authority@company.com
Company:	Company Name
Department:	
Location:	
Country code:	DE (2 Letter)
S/MIME valid for:	3653 Days
Keylength:	2048 Bit (Note: Keys larger than 2048 Bit may cause compatibility problems.)
<input type="radio"/> S/MIME	
<input type="button" value="Generate"/>	

Beispiel für die Belegung der Felder für das CA-Zertifikat:

Name:	<Firmenname/Funktion>
eMail:	Certification.Authority@<Internetdomäne>
Company:	<Firmenname/-bezeichnung>
Department:	(Optional) <Abteilung Organisatorische Einheit>
Location:	(Optional) <Ortsname, Region>
Country code:	<2 Buchstaben Ländercode>
S/MIME valid for:	3653 (Dieser Wert entspricht einer Gültigkeit von 10 Jahren)
Keylength:	2048 (Diese Schlüssellänge bietet auch für die Zukunft ausreichende Sicherheit. Längere Schlüssellängen sind aus Gründen der Kompatibilität derzeit nicht empfohlen.)



3. Schritt

Starten Sie die Zertifikatserzeugung durch anklicken des Buttons **Generate**. Das Ergebnis der Zertifikatserstellung wird anschließend angezeigt.

2.1.5. Erstellen der Unternehmensschlüssel

WebGUI → (Key Management) Central Accounts → Central Signing Account [CSA] → CSA Status

Der Unternehmensschlüssel wird auch als Central Signing Account (CSA) bezeichnet. Ihm kommt unter CompanyCRYPT eine zentrale Bedeutung zu.

1. Schritt

Klicken Sie zunächst auf **Manage**.

Company Keys [CSA - Central Signing Account]		
Name:	<input type="text"/>	
Email:	<input type="text"/>	
	PGP	SMIME
Public key	No Access	No Access
Private key:	No Access	No Access
Passphrase:	No Access	No Access
Status:	Not usable	Not usable
Manage...		

2. Schritt

Um einen CSA-Key zu erstellen, klicken Sie auf den Button **Generate**.

CSA Status	
PGP Key	
Public key in keyring	Not found
Private key in keyring	Not found
Passphrase	No Access
S/MIME Certificate	
Public key file	Not found
Private key file	Not found
Passphrase	No Access
Back Generate...	

3. Schritt

Tragen Sie in die Eingabefelder die notwendigen Daten ein. Die Felder Department und Location können leer bleiben.

Central Signing Account (CSA)	
Name: (min. 5 char)	<input type="text" value="Encryption Gateway S.I.T."/>
eMail:	<input type="text" value="Encryption-Gateway@company.com"/>
Company:	<input type="text" value="Secure Internet Traffic"/>
Department:	<input type="text"/>
Location:	<input type="text"/>
Country code:	<input type="text" value="DE"/> (2 Letter) <input type="checkbox"/> S/MIME: Write CRL details to certificate
PGP valid for:	<input type="text" value="0"/> Days (0 = unlimited) <input type="checkbox"/> S/MIME: Usage is limited to email protection
S/MIME valid for:	<input type="text" value="3653"/> Days
Keylength:	<input type="text" value="2048"/> Bit (Note: Keys larger than 2048 Bit may cause compatibility problems.)

Beispiel für die Belegung der Felder für den Central Signing Account



Name: Encryption Gateway <Firmenname>
eMail: Encryption-Gateway@<Internetdomäne>
Company: <Firmenname/-bezeichnung>
Department: (Optional) <Abteilung Organisatorische Einheit>
Location: (Optional) <Ortsname, Region>
Country code: <2 Buchstaben Ländercode>
PGP valid for: 0 (Dieser Wert entspricht einer unbegrenzten Gültigkeitsdauer.)
S/MIME valid for: 3653 (Dieser Wert entspricht einer Gültigkeit von 10 Jahren)
Keylength: 2048 (Diese Schlüssellänge bietet auch für die Zukunft ausreichende Sicherheit. Längere Schlüssellängen sind aus Gründen der Kompatibilität derzeit nicht empfohlen.)
SMIME: WriteCRL ... (Nur für das S/MIME Zertifikat) Falls in den Standardwerten ein Link konfiguriert wurde unter dem eine Certificate Revocation List (CRL) publiziert wird, wird dies im Schlüssel angezeigt.
SMIME: Usage is limit ... (Nur für das S/MIME Zertifikat) Die v3 Erweiterungen im Zertifikat werden so angelegt, das eine anderweitige Verwendung (z.B. SSL-Client) nicht möglich ist.

4. Schritt

Wählen Sie nun **S/MIME + PGP** aus, um den CSA-Schlüssel für beide Formate zu erstellen.

CA certificate available - S/MIME key will be centrally signed by CA.

☐ PGP
☐ S/MIME
☒ S/MIME + PGP

5. Schritt

Starten Sie die Schlüsselerzeugung durch anklicken des Buttons **Generate**. Das Ergebnis der Zertifikaterstellung wird anschließend angezeigt.

2.1.6. Erstellen von Schlüsseln für interne User

WebGUI → (Key Management) Internal → New key

Klicken Sie im Bereich der Schlüsselverwaltung für interne Keys auf den Button **New Key**.

1. Schritt

Tragen Sie in die Felder Name und eMail die Daten des gewünschten Users ein. Belassen Sie in den übrigen Feldern die vorgeblendeten Default key parameters.

Internal User Keypair	
Name: (min. 5 char)	Jack Smith
eMail:	Jack.Smith@companycrypt.com
Company:	S.I.T. Secure Internet Traffic GmbH & Co. KG
Department:	
Location:	
Country code:	DE (2 Letter)
PGP valid for:	0 Days (0 = unlimited)
S/MIME valid for:	730 Days
Keylength:	2048 Bit (Note: Keys larger than 2048 Bit may cause compatibility problems.)
	<input type="checkbox"/> S/MIME: Write CRL details to certificate
	<input type="checkbox"/> S/MIME: Usage is limited to email protection

Internal User Keypair

Name: <Name des Users>
eMail: <Mailadresse des Users>

2. Schritt

Wählen Sie nun „**S/MIME + PGP**“ aus, um die Schlüssel für beide Verfahren zu erstellen.

CSA key available - PGP key will be centrally signed by CSA.	<input type="radio"/> PGP <input type="radio"/> S/MIME <input checked="" type="radio"/> S/MIME + PGP
CA certificate available - S/MIME key will be centrally signed by CA.	

3. Schritt

Starten Sie die Schlüsselerzeugung durch anklicken des Buttons **Generate**.

4. Schritt

Das Ergebnis der Schlüsselerstellung wird anschließend angezeigt.

2.1.7. Schlüssel der externen Partner importieren

Nach einer Neu- bzw. Erstinstallation von CompanyCRYPT ist zum Importieren der Schlüssel Ihrer externen Kontakte das Hochladen dieser Schlüssel in das Import-Verzeichnis von CompanyCRYPT notwendig.

Im späteren Betrieb erfolgt die Ablage der externen Schlüssel automatisch in diesem Verzeichnis.

WebGUI → (Key Management) Import

1. Schritt

Ist der Schlüssel noch nicht im Importverzeichnis vorhanden, so klicken Sie auf den Button **Durchsuchen** und wählen den gewünschten Schlüssel aus. Anschließend übertragen Sie ihn mittel **Upload File** zum Server.

Ist der Schlüssel bereits im Importverzeichnis vorhanden, markieren Sie den zu importierenden Key in der Listenansicht.

Import Area					
Type	Received	Name	Usable		
	2007-11-18 14:28	j-s-j@web.de.cer	✓		
	2007-11-18 15:56	wk@g10code.com.cer	✓		
	2007-11-09 20:52	Schneider-Jansohn@CompanyCRYPT.com.pfx	✓		
	2007-11-09 19:11	TestFirma_12345678.p12	✓		
	2007-10-18 22:15	CS-Root.cer	✓		
	2007-03-12 12:24	Peter.Lemcke@arcor.de.cer	✓		
	2005-12-07 18:19	domenik.niemayer@gmx.de.asc	✓		

2. Schritt

Prüfen Sie die Eigenschaften des gewählten Keys. Diese werden unterhalb der Listenansicht angezeigt. Die erweiterten Keydetails erhalten Sie bei Bedarf über den Button [+]. Die Feldbezeichnungen der angezeigten Eigenschaften entsprechen den **Key properties** im Bereich externe Schlüsselverwaltung.

PGP key properties													
Name	Domenik Niemayer												
eMail	domenik.niemayer@gmx.de												
Fingerprint	2E9D 70A6 740A AE72 0C5F 1F5F F7AB 22B9 D5F3 3047												
	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 50%;">Single PGP key</th> <th style="width: 50%;">Sub-Key</th> </tr> <tr> <td>Algorithm</td> <td>DH/DSA</td> </tr> <tr> <td>Keylength</td> <td>1024 Bit</td> </tr> <tr> <td>Key-ID</td> <td>F7AB22B9 x D5F33047</td> </tr> <tr> <td>Valid from</td> <td>2005-02-23</td> </tr> <tr> <td>Valid until</td> <td>unlimited</td> </tr> </table>	Single PGP key	Sub-Key	Algorithm	DH/DSA	Keylength	1024 Bit	Key-ID	F7AB22B9 x D5F33047	Valid from	2005-02-23	Valid until	unlimited
Single PGP key	Sub-Key												
Algorithm	DH/DSA												
Keylength	1024 Bit												
Key-ID	F7AB22B9 x D5F33047												
Valid from	2005-02-23												
Valid until	unlimited												

3. Schritt

Klicken Sie auf den Button **Import and Sign Key / Import Certificate** um den Importvorgang zu starten.

Import and Sign Key

By default, the imported key will be removed after import.

☐ Do not Remove

Do not Remove:

Aktivieren Sie diese Option um das Keyfile nicht zu löschen.

4. Schritt

Anschließend wird das Ergebnis des Schlüsselimports angezeigt.

2.1.8. Automatischen Schlüsselimport aktivieren

Zur effektiven Nutzung der automatischen Verschlüsselung sollte auch der automatische Import für public Keys aktiviert sein. Nur so ist gewährleistet, dass die durch den externen Partner per Mail publizierten Keys für die Verschlüsselung verwendet werden.

WebGUI → (Key Management) Import → Auto-Detect / Auto-Import → Auto-Import Keys and Certificates

1. Schritt

Markieren Sie die Optionen zum automatischen Import für **PGP Keys** und **S/MIME certificates**. Weiterhin markieren Sie die Option **Overwrite existing certificates** um vorhandene S/MIME-Zertifikate erneuern zu können.

Auto-Import Keys and Certificates

Activate public key import for:

☒ S/MIME certificates

☒ PGP keys

☐ Even for already existing address

S/MIME: New certificates will only be automatically imported, if complete chain of valid issuer can be verified via Trusted CA store

PGP: New keys will be automatically imported, if there is no key present for the email address(es).
Allowing autoimport for already existing addresses increases the risk for man-in-the-middle attacks.

Activate public key import for:

S/MIME certificates: Aktiviert/Deaktiviert den automatischen Import von Public S/MIME Zertifikaten

PGP keys: Aktiviert/Deaktiviert den automatischen Import von Public PGP Keys

Even for already existing address: Importiert auch PGP-Keys für eine Emailadresse, wo bereits ein gültiger PGP-Key im Keystore vorhanden ist.

2. Schritt

Speichern Sie die Änderungen durch **Apply Changes**.

2.2. Einrichtung der Ver-/Entschlüsselung

Die Aktivierung der Verschlüsselung/Entschlüsselung wird über die Einrichtung spezieller CompanyCRYPT-Szenarien im MIMESweeper realisiert. Die notwendigen Konfigurationen im MIMESweeper Policy Editor und die Einstellungen in der CompanyCRYPT WebGUI werden schrittweise erklärt.

Nach Durchführung aller in diesem Kapitel beschriebenen Schritte sind Sie in der Lage eingehende Mails automatisch zu entschlüsseln. Weiterhin werden alle ausgehenden Mails verschlüsselt, für deren Empfänger Schlüssel vorhanden sind.

Für die Kompatibilität mit älteren PGP-Clients wird eine Adressliste eingerichtet, in die alle Empfänger aufgenommen werden können, welche die Mails im Format PGP/Inline erhalten möchten.

Dank der Benutzersteuerung werden vertrauliche Dokumente auch an Empfänger ohne Verschlüsselungstechnologie sicher per Ad Hoc Encryption verschickt.

2.2.1. Einrichtung der Entschlüsselung

Einrichten der Classifications für die Entschlüsselung

Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Classifications

1. Schritt

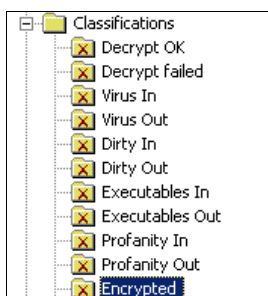
Klicken Sie mit der rechten Maustaste auf **Classifications** und wählen Sie dann **Neu → Classification** und benennen Sie die Classification **Decrypt OK**.

2. Schritt

Erstellen Sie nach dem gleichen Vorgehen eine weitere Classification und benennen Sie die Classification **Decrypt failed**.

3. Schritt

Verschieben Sie nun beide Classification nach oben, über die System-Classification **Encrypted**.

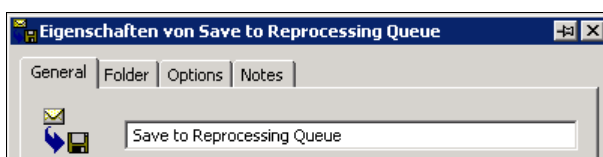


4. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **Decrypt OK** und wählen Sie **Neu → Save**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

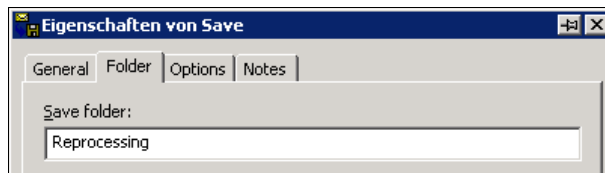
5. Schritt

Unter **Eigenschaften von Save → General** geben Sie den Namen **Save to Reprocessing Queue** ein



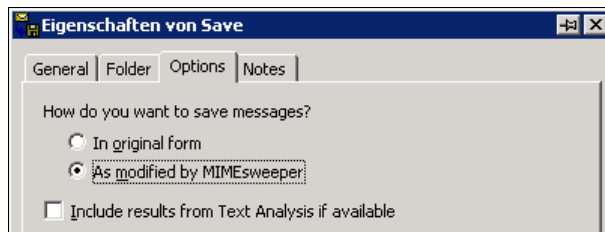
6. Schritt

Unter **Eigenschaften von Save → Folder** geben Sie den Folder-Namen **Reprocessing** an. Dieser Name muss den CompanyCRYPT-Einstellungen für den Reprocess Service entsprechen!



7. Schritt

Unter **Eigenschaften von Save** → **Options** markieren Sie die Option **As modified by MIMESweeper**. Include results from Text Analysis if available wird nicht markiert. Speichern Sie Einstellungen mit OK.

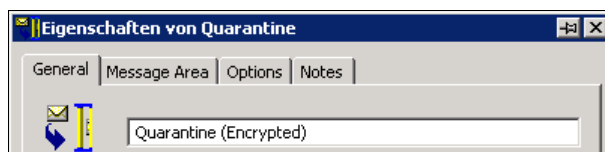


8. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **Decrypt failed** und wählen Sie **Neu** → **Quarantine**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

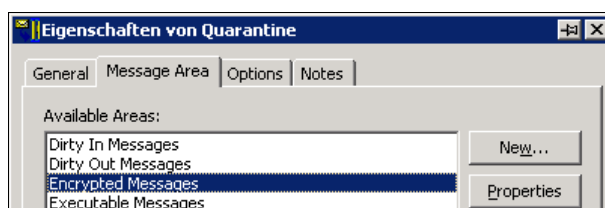
9. Schritt

Unter **Eigenschaften von Quarantine** → **General** geben Sie den Namen **Quarantine (Encrypted)** ein.



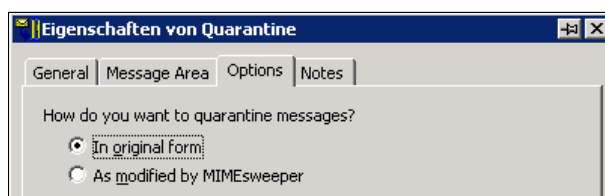
10. Schritt

Unter **Eigenschaften von Quarantine** → **Message Area** wählen Sie **Encrypted Messages** aus.



11. Schritt

Unter **Eigenschaften von Quarantine** → **Options** markieren Sie **In original form** und bestätigen die Einstellungen mit OK.





Einrichten des CompanyCRYPT-Szenarios zur Entschlüsselung

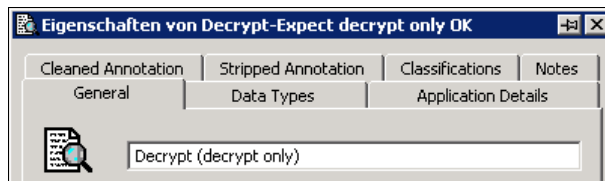
Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Scenarios → Incoming

1. Schritt

Klicken Sie mit der rechten Maustaste auf den Scenario Folder **Incoming** und wählen Sie dann **Neu → Virus Manager**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

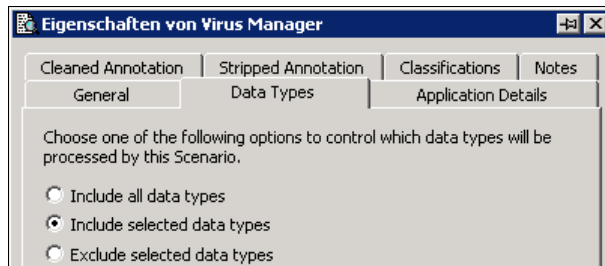
2. Schritt

Unter **Eigenschaften von Virus Manager → General** tragen Sie den Namen **Decrypt (decrypt only)** ein. Benutzen Sie selbsterklärende Namen.

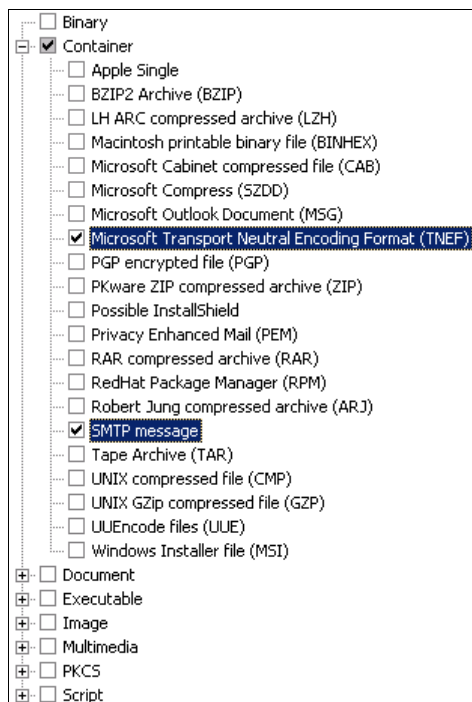


3. Schritt

Unter **Eigenschaften von Virus Manager → Data Types** wählen Sie die Option **Include selected data types**.



Bei der Auswahl der Data Types markieren Sie nur die beiden Container-Typen **Microsoft Transport Neutral Encoding Format (TNEF)** und **SMTP message**. Achten Sie darauf, dass keine weiteren Markierungen gesetzt sind.



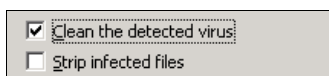


4. Schritt

Unter **Eigenschaften von Virus Manager** → **Application Details** markieren Sie das entsprechende CompanyCRYPT-Szenario **Decrypt-Expect decrypt only OK**.

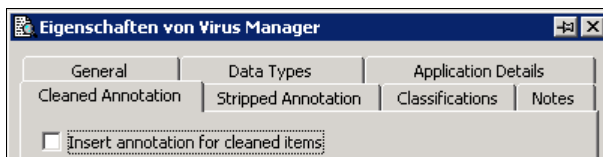


Aktivieren Sie anschließend die Option **Clean the detected virus** um eine Verschlüsselung des Mailinhaltes zu ermöglichen. Die Option **Strip infected files** darf nicht aktiviert sein.



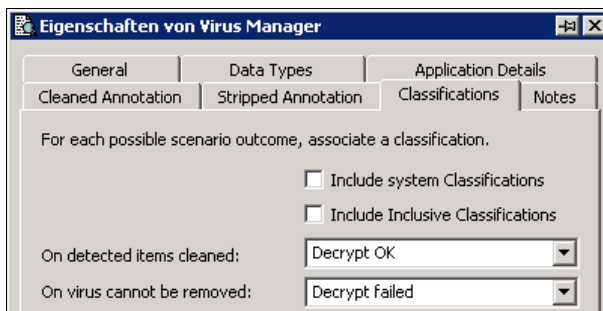
5. Schritt

Unter **Eigenschaften von Virus Manager** → **Cleaned Annotation** darf die Option **Insert annotation for cleaned items** nicht aktiviert sein.



6. Schritt

Unter **Eigenschaften von Virus Manager** → **Classification** setzen Sie die Classifications **On detected items cleaned: Decrypt OK** (erfolgreiche Entschlüsselung) und **On virus cannot be removed: Decrypt failed** (fehlgeschlagene Entschlüsselung). Speichern Sie die Einstellungen mit OK.



Eingehende Mails mit Signaturen oder verschlüsseltem Inhalt werden nun automatisch durch CompanyCRYPT entschlüsselt.

2.2.2. Einrichtung Automatische Verschlüsselung mit Benutzersteuerung

Mit der automatischen Verschlüsselung „Best Effort“ werden ausgehende Mails automatisch verschlüsselt. Entsprechend des vorhandenen Keys wird die Mail im Format S/MIME oder PGP/MIME verschlüsselt. Empfänger ohne Key erhalten die Mail unverschlüsselt.

Durch die Kombination mit der Benutzersteuerung kann der Anwender den verschlüsselten Versand einer Mail erzwingen. Empfänger ohne Key erhalten die Mail dann Ad Hoc verschlüsselt.

Einrichten der Classifications für die automatische Verschlüsselung (Best Effort)

Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Classifications

1. Schritt

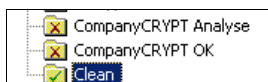
Klicken Sie mit der rechten Maustaste auf **Classifications** und wählen Sie dann **Neu → Classification** und benennen Sie die Classification **CompanyCRYPT OK**.

2. Schritt

Erstellen Sie nach dem gleichen Vorgehen eine weitere Classification und benennen Sie die Classification **CompanyCRYPT Analyse**.

3. Schritt

Verschieben Sie die Classification **CompanyCRYPT Analyse** in der Classification-Liste so, dass sie noch über der obersten Classification steht, die eine ausgehende Deliver Action enthält. Es ist jedoch zu beachten, dass beide Classifications unterhalb der Blocked-Classifications wie Virus oder Spam einzuordnen sind.

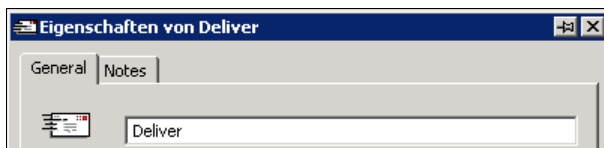


4. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **CompanyCRYPT OK** und wählen Sie **Neu → Deliver**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

5. Schritt

Unter **Eigenschaften von Deliver → General** geben Sie den Namen **Deliver** an und Bestätigen die Eingabe mit OK.

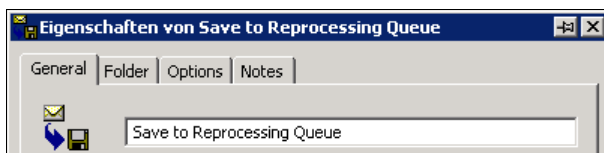


6. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **CompanyCRYPT Analyse** und wählen Sie **Neu → Save**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

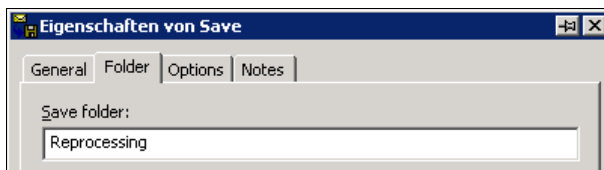
7. Schritt

Unter **Eigenschaften von Save → General** geben Sie den Namen **Save to Reprocessing Queue** ein



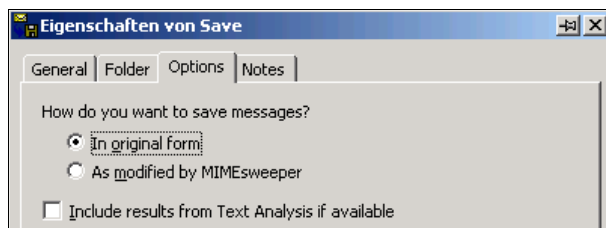
8. Schritt

Unter **Eigenschaften von Save → Folder** geben Sie den Folder-Namen **Reprocessing** an. Dieser Name muss den CompanyCRYPT-Einstellungen für den Reprocess Service entsprechen!



9. Schritt

Unter **Eigenschaften von Save → Options** markieren Sie die Option **In original form**. Include results from Text Analysis if available wird nicht markiert. Speichern Sie Einstellungen mit OK.



Erstellen des Szenarios für die automatische Verschlüsselung

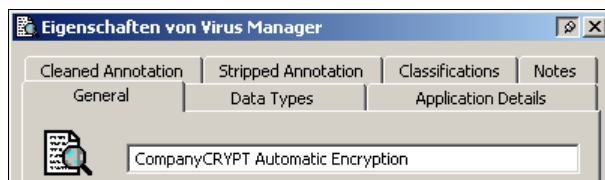
Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Scenarios → Outgoing

1. Schritt

Klicken Sie mit der rechten Maustaste auf den Scenario Folder **Outgoing** und wählen Sie dann **Neu → Virus Manager**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

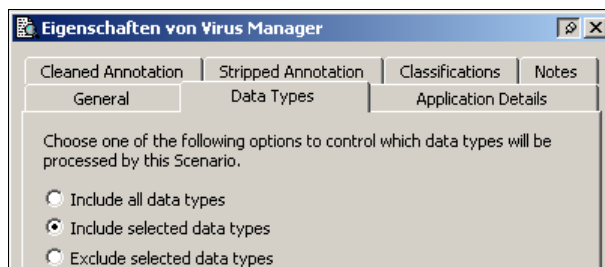
2. Schritt

Unter **Eigenschaften von Virus Manager** → **General** tragen Sie den Namen **CompanyCRYPT Automatic Encryption** ein.

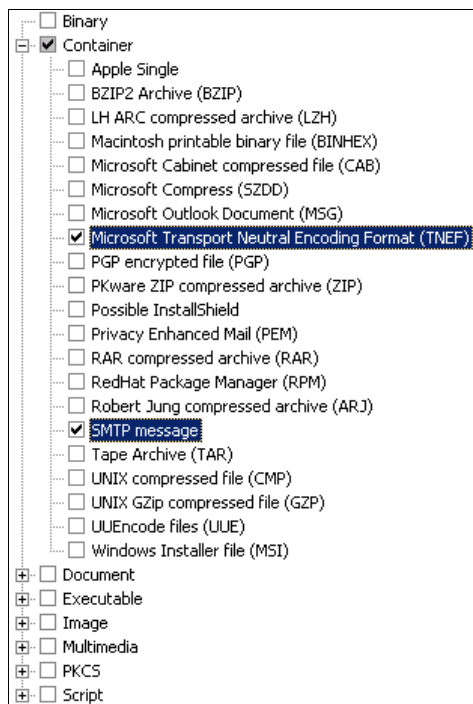


3. Schritt

Unter **Eigenschaften von Virus Manager** → **Data Types** wählen Sie die Option **Include selected data types**.



Bei der Auswahl der Data Types markieren Sie nur die beiden Container-Typen **Microsoft Transport Neutral Encoding Format (TNEF)** und **SMTP message**. Achten Sie darauf, dass keine weiteren Markierungen gesetzt sind.

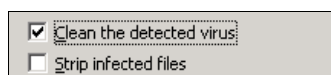


4. Schritt

Unter **Eigenschaften von Virus Manager** → **Application Details** markieren Sie **Encrypt – Automatic Encryption**.

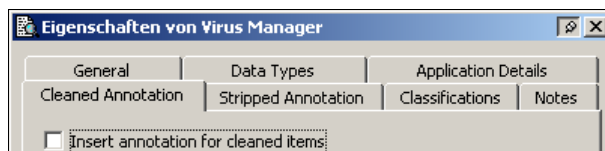


Aktivieren Sie anschließend die Option **Clean the detected virus** um eine Verschlüsselung des Mailinhaltes zu ermöglichen. Die Option 'Strip infected files' darf nicht aktiviert sein.



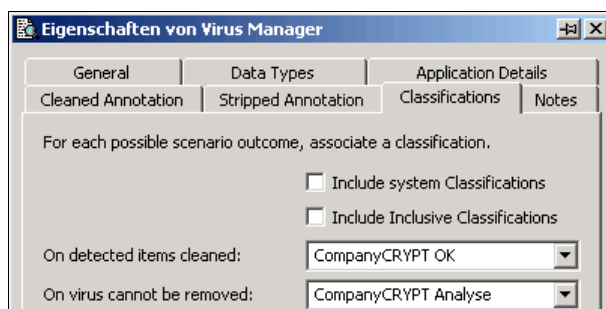
5. Schritt

Unter **Eigenschaften von Virus Manager** → **Cleaned Annotation** darf die Option 'Insert annotation for cleaned items' nicht aktiviert sein.



6. Schritt

Unter **Eigenschaften von Virus Manager** → **Classification** setzen Sie die Classifications **On detected items cleaned: CompanyCRYPT OK** und **On virus cannot be removed: CompanyCRYPT Analyse**. Speichern Sie die Einstellungen mit OK.



Aktivieren der Benutzersteuerung

WebGUI → (Configuration) Policies → User Control

1. Schritt

Klicken Sie zuerst auf den Button **More Options** um zu den erweiterten Einstellungen für die Benutzersteuerung zu gelangen.

2. Schritt

Aktivieren Sie die Option **by email property** und den **Confidential**. Aktivieren Sie ebenfalls das Kontrollkästchen **by subject keyword** und vergeben Sie ein Schlüsselwort für die Betreffzeile. Vorschlag **[vertraulich]**.

Let user activate Encryption: <input checked="" type="checkbox"/> by email property 'Sensitivity': <input checked="" type="checkbox"/> 'Confidential' <input type="checkbox"/> 'Personal' <input type="checkbox"/> 'Private'
<input checked="" type="checkbox"/> by subject keyword: <input style="width: 150px;" type="text" value="[vertraulich]"/> <input type="checkbox"/> Case sensitive

Let user activate Encryption:

By subject keyword: Schlüsselwort für die Aktivierung der Verschlüsselung, welches in der Betreffzeile der Mail angegeben werden muss (Betreffzeilensteuerung)

Case sensitive: Aktiviert/Deaktiviert die Unterscheidung von Groß- und Kleinbuchstaben für die Betreffzeilensteuerung

By email property: Die Aktivierung kann über Eigenschaften der eMail erfolgen. Die Markierung der Nachricht mit den dazugehörigen Eigenschaften ‚Vertraulich‘, ‚Persönlich‘ oder ‚Privat‘ wird im eMail-Programm durchgeführt.

3. Schritt

Belassen Sie die übrigen Optionen auf den Standardeinstellungen und Speichern Sie die Änderung mit **Apply Changes**.

Konfiguration der Ad Hoc Encryption

WebGUI → (Configuration) Formats → Ad Hoc Encryption

1. Schritt

Deaktivieren Sie die Option **Move subject line into encrypted bodytext** um die Betreffzeile von der Verschlüsselung im Ad Hoc Format auszunehmen.

Ad Hoc Encryption Properties	
Subject Protection:	<input type="checkbox"/> Move subject line into encrypted bodytext

Move subject line into encrypted bodytext:

Wenn aktiviert, dann wird das Betreff der Originalmail mit in den Bodytext der verschlüsselten Mail verschoben.

2. Schritt

Belassen Sie die übrigen Optionen auf den Standardeinstellungen und Speichern Sie die Änderung mit **Apply Changes**.

2.2.3. Einrichtung einer Adressbasierten Verschlüsselung

Mit der Adressbasierten Verschlüsselung können Sie für eingerichtete Adressen ein definiertes Verschlüsselungsformat vorgeben. Nachfolgend wird die Einrichtung für das Format PGP/Inline beschrieben. Diese Verschlüsselung können Sie für Partner nutzen, deren Clients noch nicht das Standardformat PGP/MIME entschlüsseln können. Tragen Sie bei Bedarf die Adresse des Empfängers in die angegebene Adressliste ein.

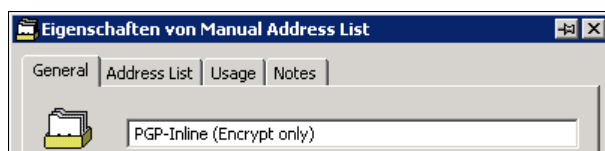
Einrichten der Adresslisten

Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Address Lists

1. Schritt

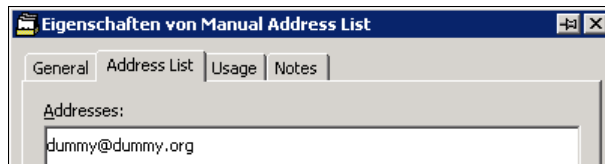
Klicken Sie mit der rechten Maustaste auf **Address List** und wählen Sie dann **Neu → Manual Address List**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

Unter **Eigenschaften von Manual Address List** → **General** tragen Sie den Namen der Adressliste ein. In diesem Beispiel **PGP-Inline (Encrypt Only)**



2. Schritt

Unter **Eigenschaften von Manual Address List** → **Address List** tragen Sie die eMailadressen der Empfänger ein. Sind noch keine Adressen verfügbar so tragen Sie einen Platzhalter ein, zum Beispiel **dummy@dummy.org** und speichern die Einstellungen mit OK.



3. Schritt

Die erstellte Adressliste wird anschließend in der Übersicht angezeigt.

Einrichten der Classifications für die Adressbasierte Verschlüsselung

Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Classifications

1. Schritt

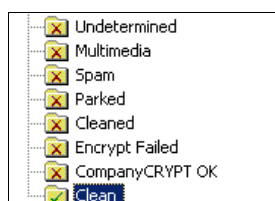
Wenn die Classification **CompanyCRYPT OK** noch nicht existiert, dann klicken Sie mit der rechten Maustaste auf **Classifications** und wählen Sie dann **Neu → Classification** und benennen Sie die Classification **CompanyCRYPT OK**.

2. Schritt

Erstellen Sie nach dem gleichen Vorgehen eine weitere Classification und benennen Sie die Classification **Encrypt failed**.

3. Schritt

Die Classifications müssen nicht nach oben verschoben werden. Es ist jedoch zu beachten, dass beide Classifications unterhalb der Blocked-Classifications wie Virus oder Spam einzuordnen sind.



4. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **CompanyCRYPT OK** und wählen Sie **Neu → Deliver**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

5. Schritt

Unter **Eigenschaften von Deliver → General** geben Sie den Namen **Deliver** an und Bestätigen die Eingabe mit OK.

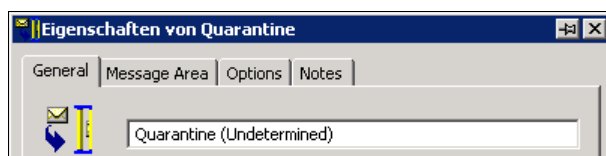


6. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **Encrypt failed** und wählen Sie **Neu → Quarantine**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

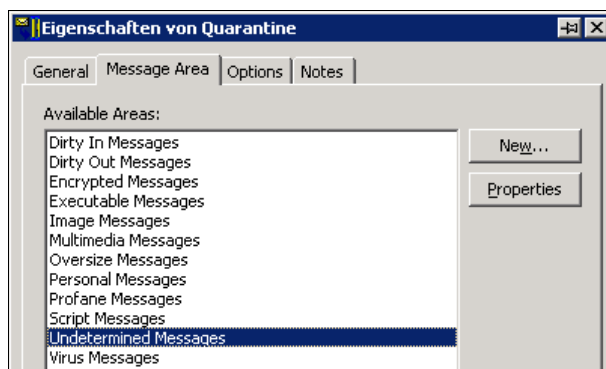
7. Schritt

Unter **Eigenschaften von Quarantine → General** geben Sie den Namen **Quarantine (Undetermined)** ein.



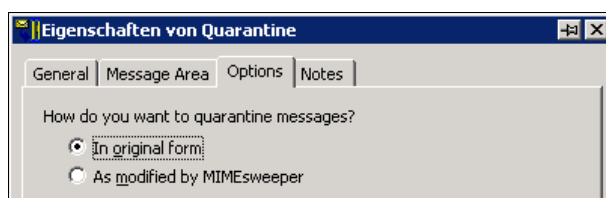
8. Schritt

Unter **Eigenschaften von Quarantine → Message Area** wählen Sie **Undetermined Messages** aus.



9. Schritt

Unter **Eigenschaften von Quarantine → Options** markieren Sie **In original form** und bestätigen die Einstellungen mit OK.



Erstellen des Scenario Folders

Policy Editor → MIMesweeper for SMTP Policy → MIMesweeper for SMTP → Policies → Scenarios → Outgoing

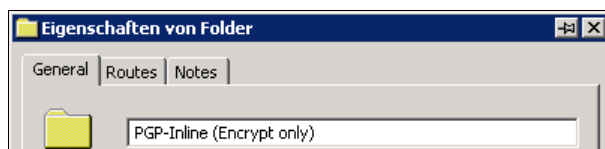
Beispielhaft wird hier die Erstellung eines Scenario Folders für die Inline-PGP -Verschlüsselung ohne Signatur beschrieben.

1. Schritt

Klicken Sie mit der rechten Maustaste auf den Scenario Folder **Outgoing** und wählen Sie dann **Neu → Folder**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

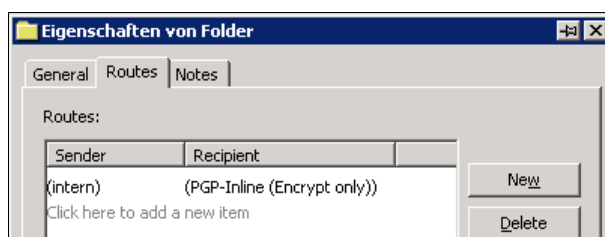
2. Schritt

Unter **Eigenschaften von Folder → General** geben Sie einen Namen an, welcher eine leichte Zuordnung zu jeweils verwendeten Funktion ermöglicht. In diesem Beispiel benutzen Sie **PGP-Inline (Encrypt only)**.



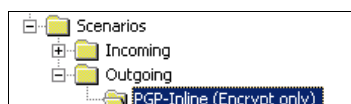
3. Schritt

Unter **Eigenschaften von Folder → Routes** geben Sie unter ‚Sender‘ die Adressliste der internen Domänen (intern) an. Unter ‚Recipient‘ wählen Sie die jeweilige Adressliste aus. In diesem Fall **PGP-Inline (Encrypt only)**. Anschließend bestätigen Sie mit OK.



4. Schritt

Der angelegte Folder wird anschließend in der Baumansicht unterhalb von Outgoing dargestellt.



Einrichten des CompanyCRYPT-Szenarios für Adressbasierte Verschlüsselung

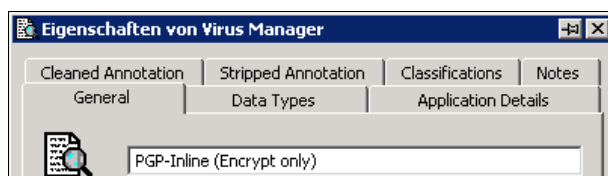
Policy Editor → MIMesweeper for SMTP Policy → MIMesweeper for SMTP → Policies → Scenarios → Outgoing

1. Schritt

Klicken Sie mit der rechten Maustaste auf den Scenario Folder **PGP-Inline (Encrypt only)** und wählen Sie dann **Neu → Virus Manager**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

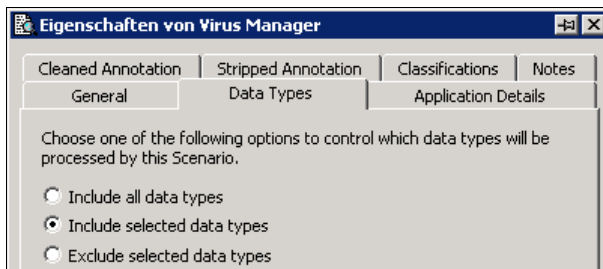
2. Schritt

Unter **Eigenschaften von Virus Manager → General** tragen Sie den Namen **PGP-Inline (Encrypt only)** ein.

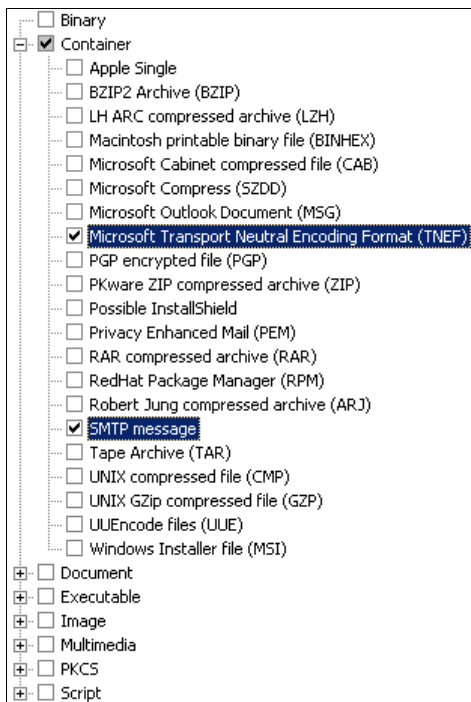


3. Schritt

Unter **Eigenschaften von Virus Manager → Data Types** wählen Sie die Option **Include selected data types**.

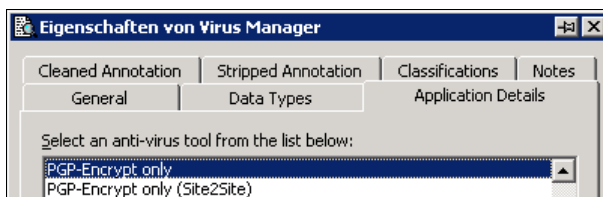


Bei der Auswahl der Data Types markieren Sie nur die beiden Container-Typen **Microsoft Transport Neutral Encoding Format (TNEF)** und **SMTP message**. Achten Sie darauf, dass keine weiteren Markierungen gesetzt sind.

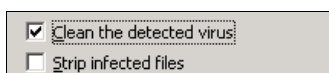


4. Schritt

Unter **Eigenschaften von Virus Manager** → **Application Details** markieren Sie **PGP-Encrypt only**.

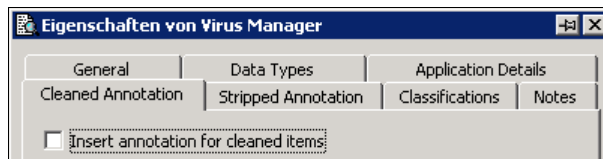


Aktivieren Sie anschließend die Option **Clean the detected virus** um eine Verschlüsselung des Mailinhaltes zu ermöglichen. Die Option 'Strip infected files' darf nicht aktiviert sein.



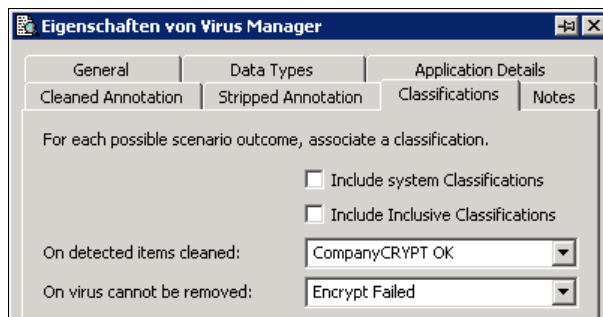
5. Schritt

Unter **Eigenschaften von Virus Manager** → **Cleaned Annotation** darf die Option 'Insert annotation for cleaned items' nicht aktiviert sein.



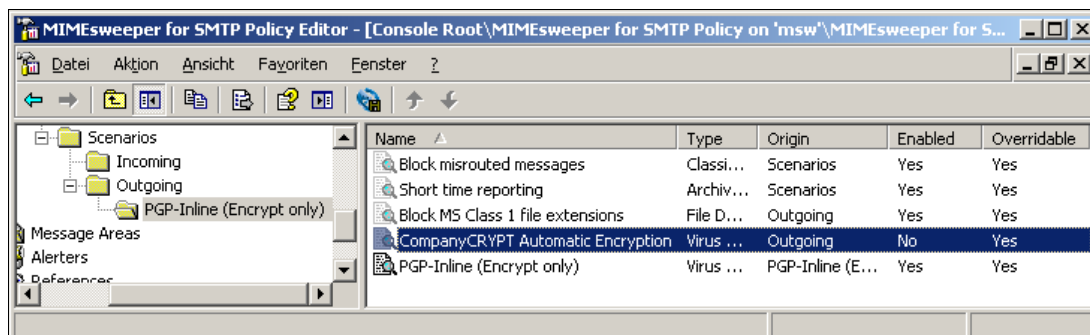
6. Schritt

Unter **Eigenschaften von Virus Manager** → **Classification** setzen Sie die Classifications **On detected items cleaned: CompanyCRYPT OK** (erfolgreiche Verschlüsselung) und **On virus cannot be removed: Encrypt failed** (fehlgeschlagene Verschlüsselung). Speichern Sie die Einstellungen mit OK.



7. Schritt

Deaktivieren Sie anschliessend im Ordner **PGP-Inline (Encrypt Only)** das Szenario **CompanyCRYPT Automatic Encryption** in dem Sie einen Rechtsklick auf dem Element ausführen und den Haken bei Enable entfernen.



Speichern Sie die Konfigurationsänderungen im MIMESweeper Policy Editor über die Schaltfläche „Save the MIMESweeper Policy“.

2.3. Funktionalität im Betrieb

2.3.1. Wie wird die Entschlüsselung aktiviert

Es bedarf keiner gesonderten Aktivierung der Entschlüsselung. Mit Einrichtung des CompanyCRYPT-Szenarios im MIMESweeper werden automatisch verschlüsselte und signierte Mails erkannt. Für diese Mails erfolgt dann ebenfalls automatisch die Entschlüsselung und Signaturprüfung.

2.3.2. Wie wird die Verschlüsselung aktiviert

Automatische Verschlüsselung „Best Effort“

Mit Einrichtung des CompanyCRYPT-Szenarios „Best Effort“ im MIMESweeper wird automatisch an alle Empfänger verschlüsselt, deren Schlüssel sich bereits in der Schlüsselverwaltung von CompanyCRYPT befinden oder über externe LDAP Dienste abgerufen werden können. Die Keys der externen Partner können automatisch oder manuell in CompanyCRYPT importiert werden.

Wird für einen Empfänger kein gültiger Key gefunden, so erfolgt der Versand der Mail an diesen Empfänger entweder unverschlüsselt oder digital signiert, je nach Konfigurationseinstellung.

Adressbasierte Verschlüsselung

Nach Hinterlegung der Empfängeradresse in der Adressliste des MIMESweepers erfolgt der verschlüsselte Mailversand an den betreffenden Empfänger. Für eine erfolgreiche Verschlüsselung ist es notwendig, dass der Key für die angegebene Empfängeradresse vorher in CompanyCRYPT importiert wird.

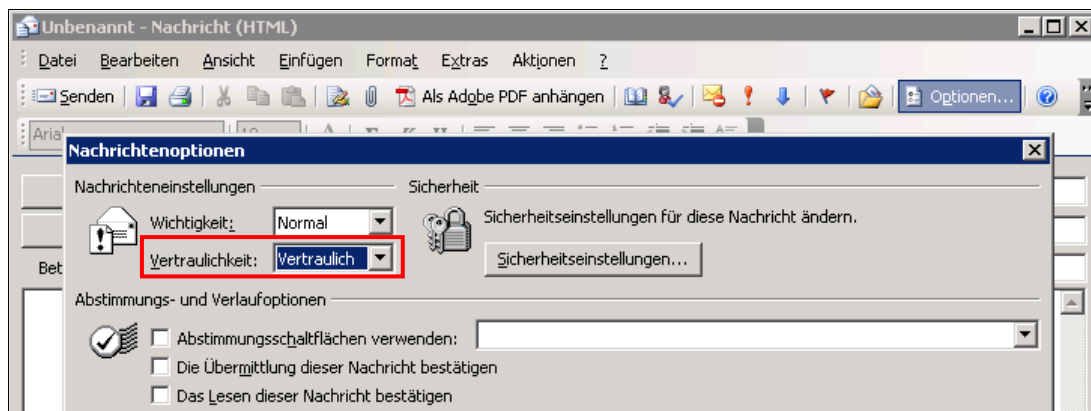
Die Mail an den Empfänger in der Adressliste wird in jedem verschlüsselt verschickt.

2.3.3. Wie aktiviert der Benutzer die Verschlüsselung

Durch die kombinierte Einrichtung der Automatischen Verschlüsselung mit der Benutzergesteuerten Verschlüsselung bzw. innerhalb des CompanyCRYPT-Szenarios „User Control“ hat der interne Anwender die Möglichkeit auch den verschlüsselten Versand an Empfänger ohne gültigen Key zu erzwingen. Dies wird durch die Nutzung des Ad Hoc Format möglich.

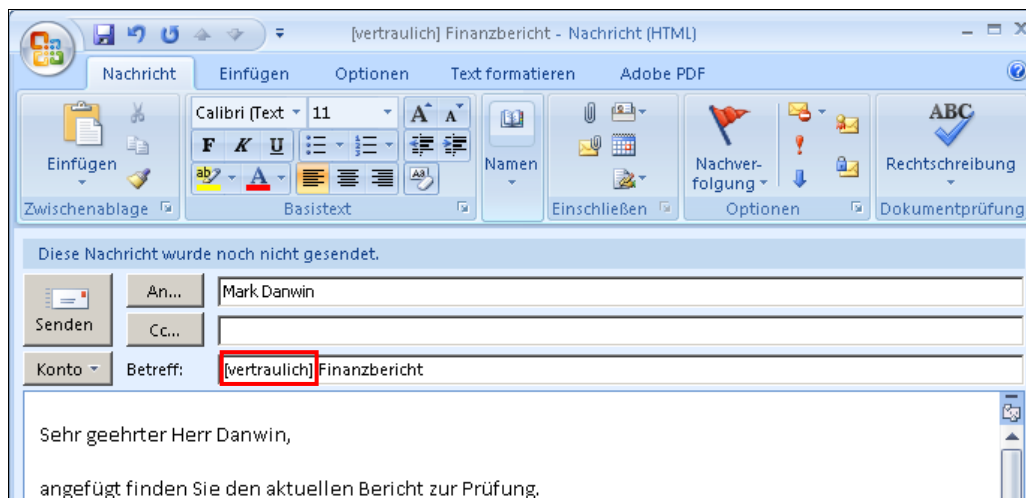
Aktivierung durch Mailoption (Outlookintegration)

Der Benutzer kann in den **Nachrichtenoptionen** die **Vertraulichkeit** seiner Mail definieren. Durch Angabe von **Vertraulich** wird die Mail dann von CompanyCRYPT verschlüsselt.



Aktivierung durch Schlüsselwort (Betreffzeilensteuerung)

Der Benutzer kann durch Angabe eines Schlüsselwortes in der Betreffzeile die Verschlüsselung durch CompanyCRYPT aktivieren.



2.3.4. Wie wird die Signierung aktiviert

Automatische Signierung „Company Signing“

Mit Einrichtung der CompanyCRYPT-Szenarios „Best Effort“, „User Control“ oder deren Kombination im MIMesweeper ist bereits alles eingerichtet, was zur zusätzlichen oder ausschließlichen Signierung von Nachrichten erforderlich ist.

Die entsprechende Funktion muss lediglich in der CompanyCRYPT-Konfiguration aktiviert bzw. gewählt werden (vergl. 3.4.4 Automatische Signierung „Company Signing“). Hierbei können verschlüsselte oder Klartext Nachrichten unterschiedlich behandelt werden. Liegt bereits eine verschlüsselte Nachricht vor, erfolgt die Signierung mit dem gleichen Verfahren (OpenPGP oder S/MIME).

Aktivierung durch Schlüsselwort (Betreffzeilensteuerung)

Innerhalb des CompanyCRYPT-Szenarios „User Control“ kann der Benutzer durch Angabe eines Schlüsselwortes in der Betreffzeile die Signierung durch CompanyCRYPT aktivieren.



3. CompanyCRYPT

CompanyCRYPT ist ein Verschlüsselungs-Plugin für den MIMESweeper for SMTP. Für Administration und Schlüsselverwaltung steht eine moderne Weboberfläche zur Verfügung.

Zur Einrichtung von Slave-Systemen in einer verteilten Umgebung steht der CompanyCRYPT SyncManager zur Verfügung.

3.1. CompanyCRYPT-WebGUI

3.1.1. Aufruf der CompanyCRYPT-WebGUI

Nachdem Sie die CompanyCRYPT-WebGUI entsprechend der Installationsanleitung eingerichtet haben, kann die Administrationsoberfläche durch Eingabe der entsprechenden Adresse im Browser aufgerufen werden.

1. Schritt

Öffnen Sie in einen Browser und starten Sie die WebGUI über die folgende Adresse:

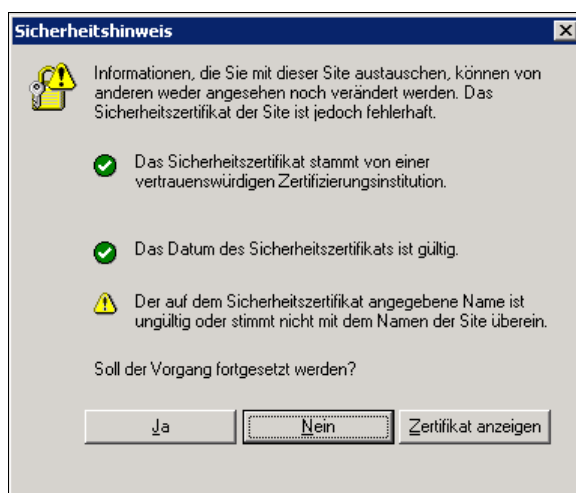
`http://<MIMesweeper-Host>/CCWeb`

Haben Sie die sichere Verbindung mittels SSL konfiguriert, dann ändern Sie das http in https. Starten Sie die WebGUI in diesem Fall über die folgende Adresse:

`https://<MIMesweeper-Host>/CCWeb`

2. Schritt

Bei Verwendung einer SSL-Verbindung ist es möglich, dass die Benutzung des vom Server verwendeten Zertifikats im Browser bestätigt werden muss.



Um den Vorgang fortzusetzen, ist diese Meldung mit **Ja** zu bestätigen.

3. Schritt

Melden Sie sich bitte mit einem Benutzer an, welcher über Administrationsrechte verfügt.

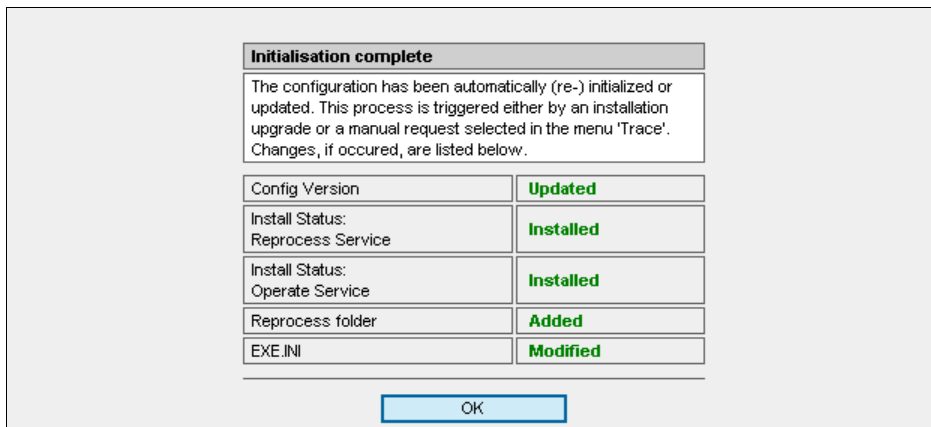




Wichtig: Für die Verwendung aller Verwaltungsfunktionen von CompanyCRYPT muss der angemeldete Benutzer Mitglied der lokalen Administratoren-Gruppe sein bzw. über lokale Administratoren-Rechte verfügen.

3.1.2. First Start / Initialisierung

Beim ersten Aufruf der CompanyCRYPT-WebGUI wird das CompanyCRYPT System initialisiert. Dieser vollautomatische Schritt ist erforderlich um die Installation abzuschließen. Eine Mitwirkung des Administrators ist nicht erforderlich. Die Anzeige hat lediglich informativen Charakter. Klicken Sie auf **OK** um fortzufahren



Initialisierungsschritte:

Config Version:	Normalisierung und Anpassung der Parameter in der CompanyCRYPT Konfigurationsdatei
Reprocess Service:	Installation des CompanyCRYPT-Reprocess-Service
Operate Service:	Installation des CompanyCRYPT-Operational-Service
Reprocess folder:	Einrichten eines Ordners als Mailqueue für den Reprocess Service
EXE.INI:	Hinzufügen der CompanyCRYPT-Szenarios zur EXE.INI des MIMesweepers



3.2. CompanyCRYPT-SyncManager

CompanyCRYPT unterstützt die Installation und den Betrieb auf verteilten Systemen. Hierfür ist die Konfiguration einer Master-Slave-Hierarchie erforderlich.

Die Einrichtung der Slave-Systeme erfolgt im ersten Schritt über den SyncManager. Im Betrieb synchronisieren sich die Slave-Systeme automatisch mit dem Master.

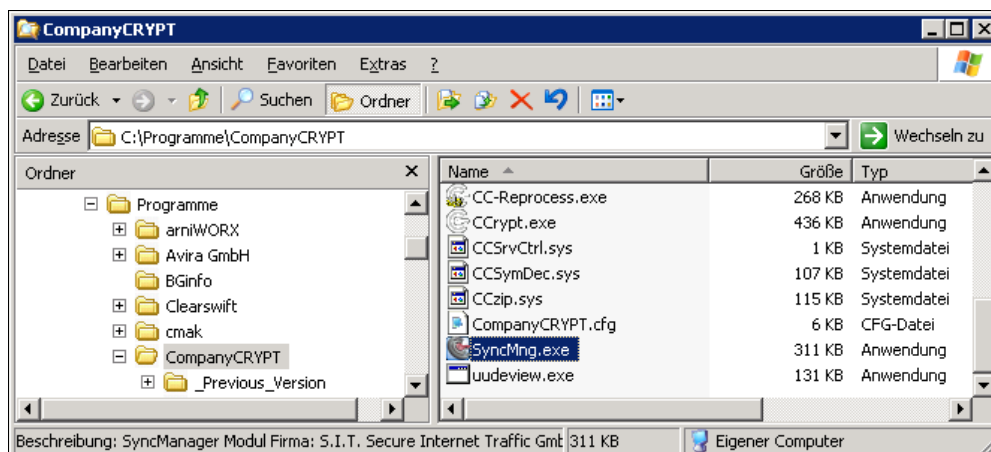
Wichtig: Bevor Sie Konfigurationsänderungen mit dem SyncManager vornehmen muss immer der Operational Service von CompanyCRYPT gestoppt werden um die Synchronisation anzuhalten! Andernfalls werden die Änderungen nicht übernommen. Nach Abschluss der Konfiguration ist der Operational Service wieder zu starten.

3.2.1. Aufruf des CompanyCRYPT-SyncManager

1. Schritt

Der SyncManager befindet sich im Installationsverzeichnis von CompanyCRYPT. In der Standardeinstellung ist dies:

C:\Programme\CompanyCRYPT\SyncMng.exe



2. Schritt

Starten Sie den SyncManager durch Doppelklick auf die Datei SyncMng.exe.

3.3. Formateinstellungen

CompanyCRYPT unterstützt neben den Standardformaten für Verschlüsselung – OpenPGP und S/MIME – auch die Verschlüsselung im Ad Hoc Format.

3.3.1. Spezifische Einstellungen für PGP

Unter diesem Menüpunkt erfolgt die Konfiguration von PGP-Parametern für das eingebundene Open-Source-Produkt GnuPG.

PGP-Verarbeitung Aktivieren/Deaktivieren

WebGUI → (Configuration) Formats → PGP → Processing

Processing	
Enable decrypt for:	<input checked="" type="checkbox"/> 'Inline PGP' <input checked="" type="checkbox"/> 'PGP/MIME'
Path to GnuPG binary:	(OK) <input type="text" value="C:\Programme\CompanyCRYPT\GnuPG"/>
PGP-Comment-Line:	<input type="text" value="GnuPG on CompanyCRYPT"/>
<input type="button" value="Apply Changes"/>	

- | | |
|-----------------------|--|
| Inline PGP: | Aktiviert bzw. Deaktiviert die Behandlung von PGP-Objekten im angegebenen Format. |
| PGP/MIME: | Aktiviert bzw. Deaktiviert die Behandlung von PGP-Objekten im angegebenen Format. |
| Path to GnuPG binary: | Verzeichnis der Datei <i>gpg.exe</i> . Der Standardwert verweist auf die mit dem Installationspaket gelieferten Executables und sollten nicht geändert werden. |
| PGP-Comment-Line: | Jeder PGP Verschlüsselungs- oder Signatur-Block kann eine (Klartext) Kommentarzeile beinhalten. Tragen Sie hier den Text ein, der angezeigt werden soll. Dieses Kommentar wird für jeden sichtbar sein, der PGP verschlüsselte oder signierte Daten von Ihnen erhält. Dies gilt sowohl für Inline-PGP als auch PGP/MIME. |

Passwort für PGP-Keys

WebGUI → (Configuration) Formats → PGP → Passphrase

Hier wird das Passwort für alle Schlüssel im CompanyCRYPT angegeben. Es gilt für die PGP-Schlüssel, S/MIME-Zertifikate und das CA-Zertifikat. Das Datum der letzten Änderung bzw. wenn noch kein Passwort hinterlegt wurde, wird entsprechend angezeigt. Bei der Ersthinterlegung des Passwortes ist das Feld Current Passphrase nicht verfügbar.

Passphrase Last changed on: 2003-01-01	
Current Passphrase:	<input type="password"/> *
New Passphrase (8-128 char.):	<input type="password" value="*****"/> P
Confirm Passphrase:	<input type="password" value="*****"/> P
<input type="button" value="Set Passphrase"/>	

- | | |
|---------------------|----------------------------|
| Current Passphrase: | aktuelles (altes) Passwort |
| New Passphrase: | neues Passwort |
| Confirm Passphrase: | neues Passwort bestätigen |

3.3.2. Spezifische Einstellungen für S/MIME

Unter diesem Menüpunkt erfolgt die Konfiguration für das eingebundene Open-Source-Produkt OpenSSL.

S/MIME-Verarbeitung Aktivieren/Deaktivieren

WebGUI → (Configuration) Formats → S/MIME → Processing

Processing

Enable decrypt for: ☒ S/MIME

Preferred Encryption Algorithm: DES3 (default)

Preferred Signing Algorithm: SHA1 (default)

Path to OpenSSL binary: (OK) C:\Program Files (x86)\CompanyCRYPT\Smime

- S/MIME:** Aktiviert bzw. Deaktiviert die Behandlung von S/MIME-Nachrichten
- Preferred Encryption Algorithm:** Gibt den zu verwendenden symmetrischen Verschlüsselungsalgorithmus an.
- Preferred Signing Algorithm:** Gibt den zu verwendenden symmetrischen Signierungsalgorithmus an.
- Path to OpenSSL binary:** Verzeichnis der Datei openssl.exe. Der Standardwert verweist auf die mit dem Installationspaket gelieferten Executables und sollten nicht geändert werden.

Prüfung von Zertifikatsketten

WebGUI → (Configuration) Formats → S/MIME → Signatures + Verification

Signatures + Verification

Include CA certificates: When Signing, include up to 10 certificates of the issuer chain in the signature.

Check external signing certificate: Do OCSP query for all certificates. (If link is provided by certificate)

Select Trustmodel: SHELL MODEL (All signatures need to be valid at time of verification)

- Include CA certificates:** Beim Signieren wird neben dem Signierzertifikat auch der Aussteller (CA) in die Signatur eingefügt. Bei Verwendung von Zwischenzertifizierern, werden alle Zertifikate bis zur angegebenen Tiefe in die Signatur eingefügt.
- Check external signing certificates:** Online Zertifikatsprüfung (Online Certificate Status Protocol). Die OCSP-Abfrage ist für S/MIME Signierzertifikate verfügbar, die einen OCSP-Link enthalten. Es wird der 'Revokation'-Status geprüft. Bei negativer Response ist die Signatur ungültig. Ist eine Abfrage nicht möglich, so wird die Signatur deshalb nicht ungültig.
- Do OCSP query for:**
 no Certificates – Deaktiviert die Online-Überprüfung
 qualified certificates only – Abfrage nur für Qualifizierte Signaturen durchführen
 all Certificates – Online-Überprüfung wird für alle Signaturen durchgeführt
- Select Trustmodel:**
 SHELL MODELL – (Standard) Zum Zeitpunkt der Signaturprüfung müssen alle Zertifikate der Zertifikatskette gültig sein.
 HYBRID MODELL – Zum Zeitpunkt der Signaturerstellung müssen alle Zertifikate der Zertifikatskette gültig sein.
 CHAIN MODELL – Jedes Zertifikat in der Zertifikatskette muss zum Zeitpunkt, als es signiert hat, gültig gewesen sein.

Passwort für S/MIME-Zertifikate

WebGUI → (Configuration) Formats → PGP → Passphrase

Hier wird das Passwort für alle Schlüssel im CompanyCRYPT angegeben. Es gilt für die PGP-Schlüssel, S/MIME-Zertifikate und das CA-Zertifikat. Das Datum der letzten Änderung bzw. wenn noch kein Passwort hinterlegt wurde, wird entsprechend angezeigt. Bei der Ersthinterlegung des Passwortes ist das Feld Current Passphrase nicht verfügbar.

Passphrase Last changed on: 2003-01-01	
Current Passphrase:	<input style="width: 90%;" type="password"/> *
New Passphrase (8-128 char.):	<input style="width: 90%;" type="password"/> ?
Confirm Passphrase:	<input style="width: 90%;" type="password"/> ?
<input style="background-color: #0070c0; color: white; padding: 2px 10px; border: none;" type="button" value="Set Passphrase"/>	

Current Passphrase: aktuelles (altes) Passwort

New Passphrase: neues Passwort

Confirm Passphrase: neues Passwort bestätigen

3.3.3. Spezifische Einstellungen für Ad Hoc Encryption

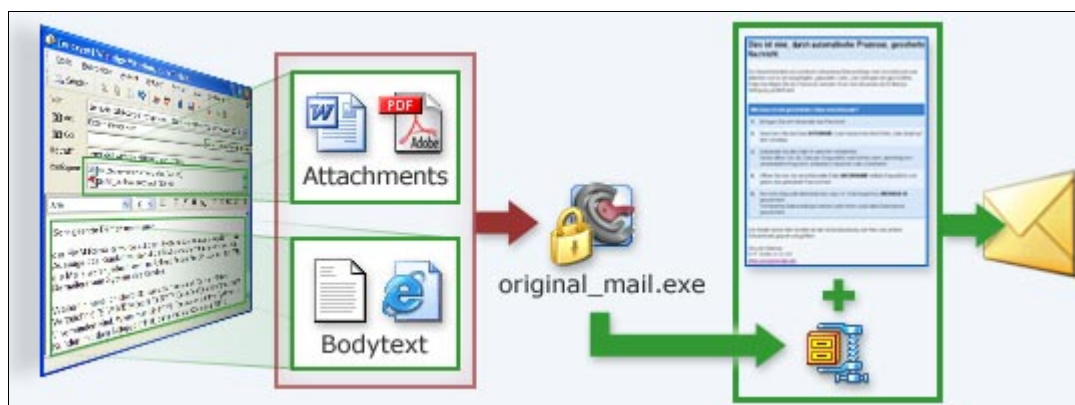
Als Alternative zu den Verschlüsselungsverfahren PGP und S/MIME wurde die Ad Hoc Verschlüsselung integriert. Diese Methode ist vor allem dort geeignet, wo der Empfänger keines der beiden Standardverfahren – PGP oder S/MIME – einsetzt. Die Ad Hoc Verschlüsselung kann sofort genutzt werden, ohne vorher Schlüsseldateien zwischen Empfänger und Sender austauschen zu müssen. Zur Entschlüsselung der Maildaten benötigt der Empfänger ein entsprechendes Passwort. Wählbare Verschlüsselungsformate

Self Extracting Zip:	Der Mailinhalt wird als verschlüsselte, selbstentpackende Datei in ein ZIP-Archiv eingebettet. Als Verschlüsselungsalgorithmus kommt eine 128 Bit AES-Blockchiffre zum Einsatz (AES-128 CBC). Durch das selbstentpackende Format ist beim Empfänger keine Zusatzsoftware notwendig.
Secure Zip:	Der Mailinhalt wird in ein verschlüsseltes ZIP-Archiv eingebettet. Als Verschlüsselungsalgorithmus kommt eine 128 Bit AES-Verschlüsselung zum Einsatz. Der Empfänger benötigt für das Entpacken eine spezielle Software.
Compatible Zip:	Der Mailinhalt wird in ein ZIP-Archiv eingebettet. Als Verschlüsselungsmethode kommt CryptoZIP zum Einsatz. Der Empfänger kann das ZIP-File mit Windows Bordmitteln öffnen.

Funktionsweise Verschlüsselung

Bei der Ad Hoc Verschlüsselung werden sowohl der Bodytext als auch die Mailanhänge zu einem verschlüsselten Archiv zusammengefasst. Die ZIP-Datei wird als Anhang mit einer entsprechenden Informationsmail (aus einem Template) an den Empfänger verschickt.

Um die Sicherheit weiter zu erhöhen, kann die Betreffzeile in den (verschlüsselten) Bodytext ‚verschoben‘ werden. Sie wird dort am Anfang des Bodytextes eingefügt. Der Betreff der eMail während der Übertragung ist dann ein generischer Text.



Da alle Inhalte der originalen Mail sich nun in dem neuen Attachment (original_mail.zip) befinden, wir die Nachricht selbst (Textinhalte und Hinweise) aus Templates generiert. Diese befinden sich unter folgenden Pfaden und können bei Bedarf angepasst werden.

Templates für Self Extracting Zip:

- <CompanyCRYPT Installation>\Templates\AdHocEncrypt\Bodytext_sda.htm
- <CompanyCRYPT Installation>\Templates\AdHocEncrypt\Bodytext_sda.txt

Templates für Secure ZIP und Compatible ZIP:



- <CompanyCRYPT Installation>\Templates\AdHocEncrypt\Bodytext_zip.htm
- <CompanyCRYPT Installation>\Templates\AdHocEncrypt\Bodytext_zip.txt

Aktivierung der Ad Hoc Encryption

Die Ad Hoc Verschlüsselung wird durch 3 Szenarios aktiviert.

Szenario: Ad Hoc Encryption

Jede Nachricht wird grundsätzlich mit diesem Verfahren und den dazu konfigurierten Optionen (Signierung, Passwortmethode, ...) verarbeitet.

Szenario: User Controlled Encryption

Wenn nicht für alle Empfänger PGP oder S/MIME Schlüssel verfügbar sind, wird die Ad Hoc Verschlüsselung als Fallbackmethode angewendet.

Szenario: Automatic Encryption

Die Automatic Encryption kombiniert die Verfahren Best Effort und User Controlled Encryption. Die für die User Controlled Encryption konfigurierten Einstellungen gelten auch für die Automatic Encryption.

Konfiguration Ad Hoc Verschlüsselung

WebGUI → (Configuration) Formats → Ad Hoc Encryption

Diese Funktionalität erlaubt den Versand verschlüsselter Nachrichten auch an Empfänger, die weder über einen PGP-Schlüssel noch über ein S/MIME-Zertifikat verfügen. Die Verschlüsselung erfolgt hier mittels eines symmetrischen Verfahrens. Zur Entschlüsselung der Datei benötigt der Empfänger ein Passwort.

Encryption container type:	Compatible ZIP	Security	AES	Encrypted file names	ZIP compatibility (Native MS Windows)	Active Elements
	Self Extracting ZIP	High	Yes	Yes	All (Yes)	Yes
	Secure ZIP	Good	Yes	No	Most (No)	No
	Compatible ZIP	Fair	No	No	All (Yes)	No

Encryption container type: Auswahl der Ad Hoc Methode

Self Extracting ZIP: 128 Bit AES-Blockchiffre verschlüsselte EXE-Datei, welche in ein ZIP eingebettet ist. Durch das Windows-Executable ist beim Empfänger keine Zusatzsoftware notwendig.

Secure ZIP: 128 Bit AES-Blockchiffre verschlüsselte ZIP-Datei. Der Empfänger benötigt ein Programm zum Entpacken der verschlüsselten ZIP-Datei. (z.B. 7zip, WinZIP, WinRAR)

Compatible ZIP: CryptoZIP verschlüsselte ZIP-Datei. Dieses einfache ZIP-Format bietet das geringste Sicherheitsniveau und kann mit aktuellen Windows-Systemen ohne zusätzliche Programme geöffnet werden.

Container content:	<input checked="" type="radio"/> Single EML File:	The complete message is converted into a single file (<i>Message.eml</i>). This format is suitable for import in various email clients like MS Outlook or Thunderbird.
	<input type="radio"/> Multiple Files:	Each part of the message is converted into a file. Body text parts will become 'bodytext.txt' and/or 'bodytext.htm'. Other attachments are contained with their original name and extension.

Container content:

Single EML File: Die komplette Email wird in der ursprünglichen Form beibehalten. Im EML-Format kann die Email dann nach dem Entschlüsseln vom Empfänger im Mailclient importiert werden.

Multiple Files: Die einzelnen Bestandteile der Email werden separat gespeichert. Der Body wird als Text und als HTML-Datei gespeichert und enthaltene Attachments werden mit originalem Dateinamen im originalen Dateiformat gespeichert.

Subject Protection:	<input type="checkbox"/> Move the subject line into encrypted bodytext (The first line from the template file <i>AdHocEncrypt/bodytext_xx_sda.txt</i> will be used as the message subject instead)
---------------------	--

Subject Protection: Diese Funktion dient zum Verbergen der Betreffzeile

Move subject line into encrypted bodytext:

Wenn aktiviert, dann wird das Betreff der Originalmail mit in den Bodytext der verschlüsselten Mail verschoben.



Password method: <input type="radio"/> Common Password: Confirm: <input checked="" type="radio"/> Random Password	Common Password: <input type="password"/> Confirm: <input type="password"/> Security: <input type="text" value="2 Blocks - equiv. 48 bit (Minimum)"/> Example: EXNx-HgBs <input checked="" type="checkbox"/> Keep log of passwords and reference ID's Password notifications are being send from: <input type="text" value="CompanyCRYPT@company.com"/>
--	--

- Password method:** Auswahl zwischen festem und automatisch generiertem Passwort für die Ad Hoc Verschlüsselung
- Common Password:** Passwort, Dieses Passwort gilt für alle mittels Ad Hoc Methode verschlüsselten Mails.
- Confirm (Password):** Passwort bestätigen
- Random Password:** Aktiviert die Verwendung eines automatisch generierten Passwortes. Dieses Passwort wird für jede zu verschlüsselnde Mail neu erzeugt und zusammen mit einer Referenznummer per Mail an den Absender verschickt. Das Passwort selbst besteht aus Buchstaben (a-z, A-Z) und Ziffern (0-9).
- Security:** Sicherheitsstufe für die Erzeugung des automatischen Passwortes, wobei 1 Block aus jeweils 4 Zeichen besteht.
- 2 Blocks - equiv. 48 Bit
 - 3 Blocks - equiv. 72 Bit
 - 4 Blocks - equiv. 96 Bit
 - 5 Blocks - equiv. 120 Bit (Empfohlen)
 - 6 Blocks - equiv. 144 Bit
 - 7 Blocks - equiv. 168 Bit
 - 8 Blocks - equiv. 192 Bit
- Keep log of passwords and reference ID's:** Aktiviert/Deaktiviert das Protokollieren der automatisch generierten Passwörter und der zugehörigen Referenznummern. Die dazugehörige Datei befindet sich in:
→ <CompanyCRYPT Installation>\Logs\AdHoc_Pw.txt
- Password notifications are being send from:** Mailadresse, unter welcher die automatisch generierten Passwörter und Referenznummern verschickt werden

Die Passwort-Benachrichtigung wird aus Template Dateien generiert. Diese befinden sich unter folgenden Pfaden und können bei Bedarf angepasst werden.

- <CompanyCRYPT Installation>\Templates\AdHocEncrypt\Bodytext_Pw.htm
- <CompanyCRYPT Installation>\Templates\AdHocEncrypt\Bodytext_Pw.txt

Referenznummer

Bei automatisch erstellten Passwörtern wird eine Referenznummer erstellt. Es handelt sich hierbei um eine 10-stellige Zufallszahl deren einziger Zweck die einfachere Zuordnung des Passworts mit der dazugehörigen Nachricht ist. Die Referenznummer ist an 3 Stellen zu finden:

- Im Betreff der Passwort Benachrichtigung (Absender)
- Im Text der Passwort Benachrichtigung (Absender)
- In der Passwort-Abfragemaske beim Empfänger beim Self Extracting ZIP



Passwort Benachrichtigung

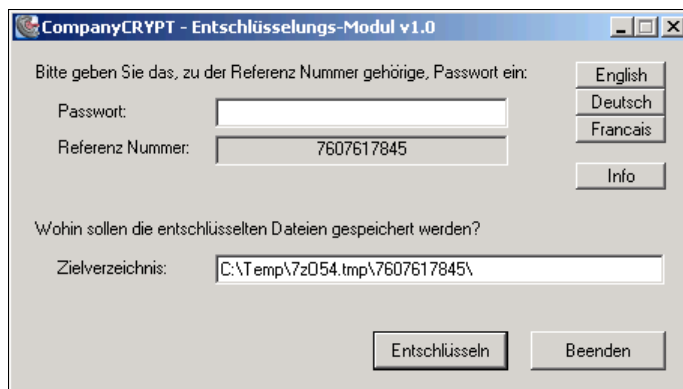
Ihre Mail wurde verschlüsselt an den Empfänger verschickt. Um auf den Inhalt Ihrer E-Mail zugreifen zu können, benötigt der Empfänger das angegebene Passwort.

Maildetails:

Betreff: Finanzbericht
Empfänger: Bob.Darning@domain.com
Referenz-Nummer: 5336907111

Passwort: Ph3Q-d0bp

Stellen Sie das angegebene Passwort dem Empfänger mit der entsprechenden Referenz-Nummer zur Verfügung.



Funktionsweise Entschlüsselung

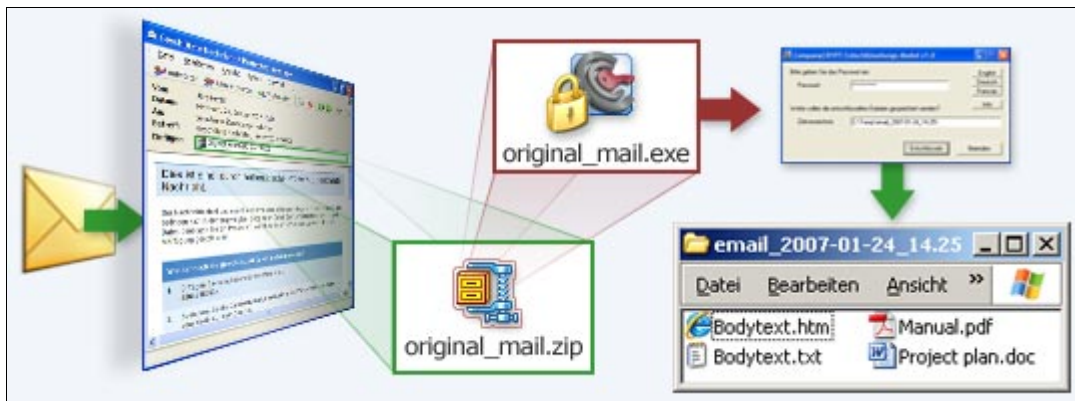
Der Empfänger erhält eine Mail, welche eine Anleitung zum Entpacken bzw. Entschlüsseln des mitgelieferten Anhangs enthält.

Self Extracting ZIP

Die ZIP-Datei wird gespeichert und extrahiert. Anschliessend wird das verschlüsselte Archiv original_mail.exe gestartet. Nach der Ausführung überprüft das Executable automatisch die Konsistenz der verschlüsselten Daten und bestimmt den lokalen (eigenen) Ordner. Anschliessend wird ein Fenster mit zwei Eingabefeldern angezeigt. In ein Feld wird das Passwort zur Entschlüsselung eingetragen. In das andere Feld wird der Ort zum Speichern der entschlüsselten Daten eingetragen. Hier wird automatisch ein Unterverzeichnis des aktuellen Ordners vorgeblendet.

Die Ausgaben erfolgen in der jeweiligen Sprache, welche im CompanyCRYPT unter „Ad Hoc Encryption“ definiert wurde. Der Anwender hat jedoch die Möglichkeit, beliebig zwischen den Sprachen Deutsch, Englisch und Französisch zu wählen.

Durch den Button „Entschlüsseln“ startet der Prozess. Zuerst erfolgt die Prüfung des Passwortes. Ein falsches Passwort erzeugt eine entsprechende Meldung. Weiterhin wird die Existenz des Ziellordners geprüft und dieser bei Bedarf angelegt. Beim Speichern wird die Mail selbst als „Bodytext.txt“ abgespeichert. War die Mail im HTML-Format, so wird zusätzlich noch eine Datei „Bodytext.htm“ gespeichert. Alle vorhandenen Dateianhänge werden unter ihrem originalen Dateinamen gespeichert. Existieren im Zielverzeichnis bereits Dateien mit gleichem Namen, so werden die aktuellen Dateien mit einer fortlaufenden Nummer versehen um ein Überschreiben der vorhandenen Dateien zu vermeiden.



Secure ZIP

Die ZIP-Datei wird gespeichert und mittels eines speziellen Entpack-Programmes geöffnet. Zum Entpacken wird vom Entpackprogramm eine Eingabeaufforderung für die Passwordeingabe angezeigt. Nach korrekter Passwordeingabe wird der Mailinhalt auf dem Computer des Empfängers extrahiert. Beim Speichern wird die Mail selbst als „Bodytext.txt“ abgespeichert. War die Mail im HTML-Format, so wird zusätzlich noch eine Datei „Bodytext.htm“ gespeichert. Alle vorhandenen Dateianhänge werden unter ihrem originalen Dateinamen gespeichert.

Compatible ZIP

Die ZIP-Datei wird gespeichert und direkt mit Windows oder mittels eines speziellen Entpack-Programmes geöffnet. Zum Entpacken wird eine Eingabeaufforderung für die Passwordeingabe angezeigt. Nach korrekter Passwordeingabe wird der Mailinhalt auf dem Computer des Empfängers extrahiert. Beim Speichern wird die Mail selbst als „Bodytext.txt“ abgespeichert. War die Mail im HTML-Format, so wird zusätzlich noch eine Datei „Bodytext.htm“ gespeichert. Alle vorhandenen Dateianhänge werden unter ihrem originalen Dateinamen gespeichert.

Konfiguration Ad Hoc Entschlüsselung

WebGUI → (Configuration) Formats → Ad Hoc Encryption → AdHoc Encryption Properties

Primary Localisation:	DEU ▼	This setting selects the template for the outgoing message. It also sets the initial language of the Self Extracting ZIP decryption interface. The language remains selectable to the recipient.
-----------------------	-------	--

Primary Localisation: Gibt an, in welcher Sprache die Email und das verschlüsselte Executable beim Empfänger geöffnet werden soll.

Entschlüsselung beim Empfänger (Self Extracting ZIP)

Der Empfänger erhält eine eMail mit dem Dateianhang „original_mail.zip“. Die Mail enthält eine Schritt-für-Schritt Anleitung zum Entschlüsseln der Daten.

1. Schritt

Das Passwort zum Entschlüsseln der gesicherten Daten muss vom Absender der Mail erfragt werden.

2. Schritt

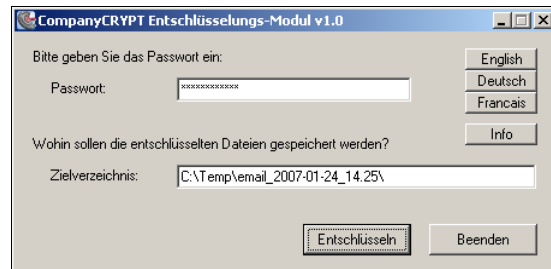
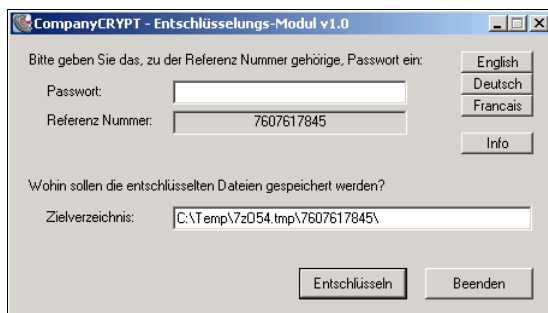
Abspeichern der Datei **original_mail.zip** in ein beliebiges Verzeichnis.

3. Schritt

Entpacken Sie die Datei im gleichen Verzeichnis. Hierzu öffnen Sie die Datei per Doppelklick und wählen dann, abhängig vom verwendeten Programm, entweder Entpacken oder Extrahieren.

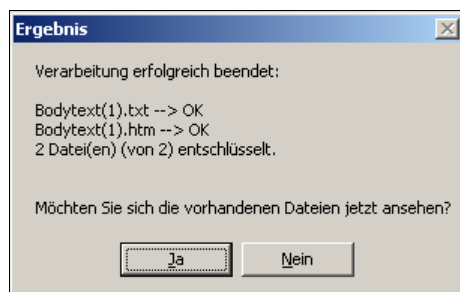
4. Schritt

Öffnen Sie nun das verschlüsselte Archiv **original_mail.exe** mittels Doppelklick und geben Sie das geforderte Passwort ein. In Abhängigkeit der verwendeten Passwort Methode während der Verschlüsselung erscheint unterhalb des Passwortfeldes eine Referenznummer. Diese Nummer erleichtert dem Absender die Zuordnung des richtigen Passworts zu dieser Nachricht. Im Feld Zielverzeichnis tragen Sie den Ordner zum Speichern der entschlüsselten Daten ein. Standardmäßig wird hier ein Unterordner des aktuellen Ordners vorgeblendet. Klicken Sie auf **Entschlüsseln**.



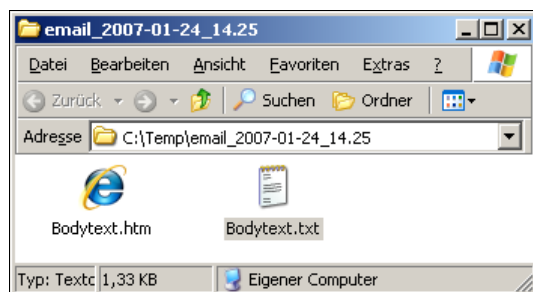
5. Schritt

Nach dem erfolgreichen Entschlüsseln klicken Sie auf **Ja**, um den Ordner mit den gespeicherten Daten anzuzeigen.



6. Schritt

Zum Anschauen des Mailtextes öffnen Sie die Datei **Bodytext.txt** per Doppelklick. Sofern die eMail im HTML-Format verschickt wurde, liegt der Mailinhalt auch als **Bodytext.htm** vor. Vorhandene Dateianhänge finden Sie im gleichen Ordner unter ihrem originalen Dateinamen.



Entschlüsselung beim Empfänger (Secure ZIP, Compatible ZIP)

Der Empfänger erhält eine eMail mit dem Dateianhang „original_mail.zip“. Die Mail enthält eine Schritt-für-Schritt Anleitung zum Entschlüsseln der Daten.

1. Schritt

Das Passwort zum Entschlüsseln der gesicherten Daten muss vom Absender der Mail erfragt werden.

2. Schritt

Abspeichern der Datei **original_mail.zip** in ein beliebiges Verzeichnis.

3. Schritt

Öffnen der Datei mittels eines speziellen Entpackprogrammes. Abhängig vom verwendeten Programm entweder Entpacken oder Extrahieren wählen und dann das Passwort eingeben. Die Daten werden dann im gewählten Verzeichnis entpackt.

3.4. Verschlüsselungsmöglichkeiten

Zur Verfügung stehen Adressbasierte Verschlüsselung, Benutzergesteuerte Verschlüsselung und die automatische Verschlüsselung. Durch eine Kombination der einzelnen Möglichkeiten bietet CompanyCRYPT eine flexible Verschlüsselung für alle Anforderungen.

3.4.1. Adressbasierte Verschlüsselung

Dies ist die klassische Methode zur Einrichtung einer Verschlüsselung. Die Konfiguration erfolgt hier komplett über die MIMESweeper-Policy. Über dedizierte CompanyCRYPT-Adresslisten und deren Zuordnung zu speziellen Szenarien werden im MIMESweeper feste Verschlüsselungsregeln erstellt. Diese wissen dann den definierten Empfängern das entsprechende Verschlüsselungsformat zu.

Unterdrückung von Verschlüsselung und Signierung durch den Absender

WebGUI → (Configuration) Policies → Suppression

Diese Option erlaubt es dem internen Absender eine permanent eingerichtete Verschlüsselung und Signierung über Schlüsselwörter in der Betreffzeile zu unterdrücken. Diese Eigenschaft kann für Verschlüsselung und Signierung mit unterschiedlichen Schlüsselwörtern separat aktiviert werden.

Hinweis: Gefundene Schlüsselwörter zur Unterdrückung werden nicht aus dem Betreff entfernt.

Hinweis: - Dies ist eine globale Einstellung und hat deshalb ggf. Einfluss auf andere Szenarios.

Suppress Encryption or Signing

Note: This option will enable the internal sender to suppress encryption or signing functions by placing the following key words in the subject line.

Allow user to:

Suppress Encryption:	<input type="checkbox"/> by subject keyword: <input style="width: 150px;" type="text"/>	<input type="checkbox"/> Case sensitive
Suppress Signing:	<input type="checkbox"/> by subject keyword: <input style="width: 150px;" type="text"/>	<input type="checkbox"/> Case sensitive

- | | |
|----------------------|---|
| Suppress Encryption: | Aktiviert/Deaktiviert die Benutzergesteuerte Unterdrückung Verschlüsselung |
| By subject keyword: | Schlüsselwort zum Unterdrücken der Verschlüsselung, welches in der Betreffzeile der Mail angegeben werden muss (Betreffzeilensteuerung) |
| Case sensitive: | Aktiviert/Deaktiviert die Unterscheidung von Groß- und Kleinbuchstaben für die Betreffzeilensteuerung |
| Suppress Signing: | Aktiviert/Deaktiviert die Benutzergesteuerte Unterdrückung Signierung |
| By subject keyword: | Schlüsselwort zum Unterdrücken der Signierung, welches in der Betreffzeile der Mail angegeben werden muss (Betreffzeilensteuerung) |
| Case sensitive: | Aktiviert/Deaktiviert die Unterscheidung von Groß- und Kleinbuchstaben für die Betreffzeilensteuerung |

3.4.2. Automatische Verschlüsselung „Best Effort“

WebGUI → (Configuration) Policies → Best Effort

Neben der adressenbasierten Verschlüsselung, welche durch die Einrichtung von Adresslisten und den Verschlüsselungsszenarien auf dem Mailgateway realisiert wird, unterstützt CompanyCRYPT auch die automatische Verschlüsselung „Best Effort“. In diesem Modus verschlüsselt CompanyCRYPT die Mail automatisch für alle Empfänger, für die ein Schlüssel vorhanden ist.

Verarbeitung bei fehlendem Public Key des Empfängers

Definieren der Kondition, wenn für einen Empfänger kein Schlüssel vorhanden ist.

Encrypt policy: If possible use PGP or S/MIME, else: <div style="display: inline-block; vertical-align: middle;"> <input checked="" type="radio"/> Send unencrypted <input type="radio"/> Stop with 'Encrypt Fail' </div>

Send unencrypted: Die Mail wird unverschlüsselt verschickt

Stop with „Encrypt fail“: Der Verschlüsselungsjob liefert den Rückgabewert „Failed“ (Classification „Encrypt Failed“) an dem MIMESweeper zurück. Die eMail wird nicht weitergeleitet.

Ausnahmen zur Verschlüsselung

Zum unterdrücken der automatischen Verschlüsselung können Sie sowohl Absender als auch Empfängeradressen angeben, für die der Mailverkehr nicht verschlüsselt werden soll.

Exceptions: Do not encrypt, if sender or recipient is named in either of the following lists: (Available wildcards: ? *)		
From: <div style="border: 1px solid black; height: 30px; margin-top: 5px;"></div>	OR	To: <div style="border: 1px solid black; height: 30px; margin-top: 5px;"></div>

From: Absenderadressen, von denen die Mail nicht verschlüsselt verschickt werden soll.

To: Empfänger, an die eine Mail nicht verschlüsselt werden soll. Durch die Nutzung von Wildcards kann zum Beispiel auch eine Domäne angegeben werden

Hinweis: Die Angaben in den Feldern From und To werden einzeln berücksichtigt und nicht als Kommunikationsverbindung betrachtet. Das bedeutet, die Verschlüsselung wird nicht durchgeführt sofern eine Übereinstimmung - entweder Empfänger oder der Absender – in der Liste gefunden wird.

3.4.3. Benutzergesteuerte Verschlüsselung und/oder Signierung

WebGUI → (Configuration) Policies → User Control

CompanyCRYPT unterstützt auch die benutzergesteuerte Verschlüsselung. Bei diesem Modus entscheidet der User beim Versand einer Mail, ob diese verschlüsselt bzw. signiert gesendet werden soll. Die Verschlüsselung wird hierbei über einen entsprechenden Trigger aktiviert.

Aktivierung von Verschlüsselung und Signierung

Diese Option erlaubt dem internen Anwender (Absender) die Verschlüsselung und Signierung zu aktivieren. Dabei stehen mehrere Möglichkeiten zur Verfügung.

Betreffzeilensteuerung – Aktivierung durch Schlüsselworte in der Betreffzeile.

Mailoption „Vertraulichkeit“ – Aktivierung über die in Mailclients verfügbaren Eigenschaften: vertraulich, persönlich, etc.

Custom eMail Header – Aktivierung über beliebige Felder des Mailheaders

Die dazugehörigen Szenarios sind „User Controlled Encryption“ und „Automatic Encryption“, welche nur bei Vorhandensein der definierten Aktivierungsoption die eingestellten Verarbeitungsschritte an der Nachricht vornehmen.

- User Controlled Encryption
- Automatic Encryption

Vergleichen Sie hierzu bitte das Flussdiagramm 4.8.1 Funktionsbild – Adressbasierte Verschlüsselung, welches den Ablauf und die möglichen Verarbeitungsschritte darstellt.

Hinweis: Gefundene Schlüsselworte werden automatisch aus dem Betreff entfernt.

Hinweis: Adressbasierte Szenarios sind grundsätzlich nicht betroffen.



Let user activate Encryption: ☒ by email property 'Sensitivity': ☒ 'Confidential' ☐ 'Personal' ☐ 'Private'

☒ by subject keyword: [vertraulich] ☐ Case sensitive

☐ by custom value in email header: (Example: X-Notes-Item: 1; name=Encrypt)

X-CC-Trigger : doencrypt or

Encryption method:

☐ Ad Hoc encryption only

☒ If possible use PGP or S/MIME, else: ☒ Encrypt AdHoc using Secure ZIP

☐ Stop with 'Encrypt Fail'

☐ Send unencrypted

☐ Prefer PGP, if PGP and S/MIME is possible

☐ Prefer Inline-PGP, when PGP is selected

Hinweis: Um alle verfügbaren Optionen für die „User controlled encryption“ anzuzeigen, müssen diese erst über den Button „More Options“ eingeblendet werden.

Let user activate Encryption:

Aktiviert/Deaktiviert die Benutzergesteuerte Verschlüsselung

By email property:

Die Aktivierung kann über Eigenschaften der eMail erfolgen. Einige Mail-Programme ermöglichen die Markierung der Nachricht mit den dazugehörigen Eigenschaften ‚Vertraulich‘, ‚Persönlich‘ oder ‚Privat‘.

By subject keyword:

Schlüsselwort für die Aktivierung der Verschlüsselung, welches in der Betreffzeile der Mail angegeben werden muss (Betreffzeilensteuerung)

Case sensitive:

Aktiviert/Deaktiviert die Unterscheidung von Groß- und Kleinbuchstaben für die Betreffzeilensteuerung

By custom value in email header:

Die Aktivierung kann alternativ auch über Felder erfolgen, die im eMail Header notiert sind.

Encryption method:

Auswahl der Verschlüsselungsmethode

Ad Hoc encryption only:

Die Mail wird mit der Ad Hoc Verschlüsselungsmethode verschlüsselt, unabhängig davon, ob für den/die Empfänger ein Schlüssel vorhanden ist.

if possible use PGP or S/MIME, else:

Wenn für den/die Empfänger durchgängig PGP oder S/MIME Schlüssel vorhanden sind, dann wird mit der jeweiligen Methode verschlüsselt.

Encrypt Ad Hoc using ...:

Ist für einen Empfänger kein PGP oder S/MIME-Schlüssel vorhanden, so wird die konfigurierte Ad Hoc Verschlüsselung angewendet. Das Format der Ad Hoc Verschlüsselung wird angezeigt.

Stop with Encrypt Fail:

Die Mail wird mit „Verschlüsselungsfehler“ geblockt, wenn für einen Empfänger kein PGP oder S/MIME-Schlüssel vorhanden ist.

Send unencrypted:

Der Versand erfolgt unverschlüsselt, sofern für einen Empfänger kein PGP oder S/MIME-Schlüssel vorhanden ist.

Prefer PGP, if PGP and S/MIME is possible:

Wenn aufgrund der zur Verfügung stehenden Schlüssel beide Verfahren möglich sind, wird bei Aktivierung das PGP Verfahren angewendet.

Prefer Inline-PGP, when PGP is selected:

Schaltet zwischen dem Verfahren PGP/MIME und Inline-PGP um.

Let user activate Signing: ☒ by subject keyword: [sign] ☒ Case sensitive

Signing key: ☐ Company ☒ User (if key is not available: Company signing is fallback)

Let user activate Signing:

Aktiviert/Deaktiviert die Benutzergesteuerte Signierung

By subject keyword:

Schlüsselwort zum Signieren, welches in der Betreffzeile der Mail angegeben werden muss (Betreffzeilensteuerung)

Case sensitive:

Aktiviert/Deaktiviert die Unterscheidung von Groß- und Kleinbuchstaben für die Betreffzeilensteuerung



Signing key: Auswahl, ob der Unternehmensschlüssel (CSA) zum Signieren verwendet werden soll, oder der Schlüssel des Users (Absenders). Ist kein Userkey vorhanden wird automatisch der Unternehmensschlüssel verwendet.

3.4.4. Automatische Signierung „Company Signing“

WebGUI → (Configuration) Policies → Company Signing

An dieser Stelle lassen sich Einstellungen zur automatischen Signierung von Nachrichten vornehmen. Hierbei können die Signiereinstellungen für verschlüsselte und unverschlüsselte Nachrichten unterschiedlich eingestellt werden

Signiereinstellungen für verschlüsselte Nachrichten

Hierüber wählen Sie, welche Signiereinstellung angewendet wird, wenn die Mail verschlüsselt ist. Das Format – PGP oder S/MIME – wird durch die Verschlüsselung bzw. durch den Key des Empfängers vorgegeben.

Encrypted messages:	Signing policy	<input checked="" type="radio"/> Don't sign <input type="radio"/> Always sign with company key (CSA) <input type="radio"/> Always sign with user key (Fallback is company key) <input type="radio"/> If available, sign with user key
----------------------------	-----------------------	--

Signing Policy: Signiereinstellung bei gleichzeitiger Verschlüsselung

Don't Sign: Die Mail wird nicht signiert

Always sign with Company key (CSA):
Signierung erfolgt stets mit dem Central Signing Account/Company Key

Always sign with user key (Fallback is company key):
Signierung erfolgt mit dem Key des Absenders. Ist für den Absender kein Key vorhanden, so erfolgt die Signierung mit dem Central Signing Account/Company Key

If available sign with user key:
Signierung erfolgt mit dem Key des Absenders. Ist für den Absender kein Key vorhanden, so erfolgt keine Signierung

Signiereinstellungen für Klartextnachrichten

Hier definieren Sie die Signiereinstellungen für unverschlüsselte Klartextnachrichten.

Plain messages:	Signing Policy:	<input checked="" type="radio"/> Don't sign <input type="radio"/> Always sign with company key (CSA) <input type="radio"/> Always sign with user key (Fallback is company key) <input type="radio"/> If available, sign with user key
------------------------	------------------------	--

Signing Policy: Signiereinstellung für Klartextnachrichten

Don't Sign: Die Mail wird nicht signiert

Always sign with Company key (CSA):
Signierung erfolgt stets mit dem Central Signing Account/Company Key

Always sign with user key (Fallback is company key):
Signierung erfolgt mit dem Key des Absenders. Ist für den Absender kein Key vorhanden, so erfolgt die Signierung mit dem Central Signing Account/Company Key

If available sign with user key:
Signierung erfolgt mit dem Key des Absenders. Ist für den Absender kein Key vorhanden, so erfolgt keine Signierung

Das Signiermethode kann bei Klartextnachrichten festgelegt werden.

Use method:	<input checked="" type="radio"/> S/MIME <input type="radio"/> PGP/MIME <input type="radio"/> Inline-PGP
--------------------	---

Use method: Auswahl der Signiermethode zwischen S/MIME, PGP/MIME und Inline PGP



Ausnahmen zur Signierung von Klartextnachrichten

Sie können sowohl Absender als auch Empfängeradressen angeben, für die keine Signierung der Nachrichten angewendet werden soll.

Exceptions: Do **not** sign message, if sender or recipient is named in either of the following lists: (Available wildcards: ? *):

From:		To:
Test@test.de	OR	*@company.com

From: Absenderadressen, von denen eine Mail nicht signiert werden soll.

To: Empfänger, an die eine Mail nicht signiert werden soll. Durch die Nutzung von Wildcards kann zum Beispiel auch eine Domäne angegeben werden

Hinweis: Die Angaben in den Feldern From und To werden einzeln berücksichtigt und nicht als Kommunikationsverbindung betrachtet. Das bedeutet, die Signierung wird nicht durchgeführt sofern eine Übereinstimmung - entweder Empfänger oder der Absender – in der Liste gefunden wird.

3.5. Keyserver + Keyresponder

3.5.1. Externe Keyserver

Die CompanyCRYPT Verschlüsselungsszenarios ‚Best Effort‘ und ‚UserControl‘ können fehlende S/MIME-Zertifikate ggf. über LDAP Verzeichnisdienste ergänzen.

Wichtig: Bedenken Sie, dass LDAP Abfragen Zeit beanspruchen, die für die Verarbeitung nicht mehr zur Verfügung steht. Nutzen Sie deshalb die Filtereinstellungen so weit wie möglich und halten die Anzahl der globalen Abfragen so klein wie möglich (*@* → Jede Adresse wird abgefragt).

LDAP Verzeichnisdienste

WebGUI → (Configuration) Key Server → External Keyserver

Eingetragene Dienste werden in Listenform angezeigt. Der Abfragesyntax selber steht hierbei in einer Zeile und kann beliebig editiert werden.

Nr.	Target-Link	Filter	
1.	<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> <div style="border: 1px solid #ccc; padding: 2px;">S/MIME ▼</div> <div style="margin-top: 5px;"> <input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Use Proxy <input type="checkbox"/> Autoimport </div> </div> <div> <div style="border: 1px solid #ccc; padding: 2px;">ldap://directory.d-trust.net:389/c=de??sub?mail=%EMAIL%</div> <div style="margin-top: 5px; text-align: center;">Test</div> </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;">*@*</div>	<div style="margin-bottom: 5px;">Apply</div> <div>Remove</div>
2.	<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> <div style="border: 1px solid #ccc; padding: 2px;">S/MIME ▼</div> <div style="margin-top: 5px;"> <input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Use Proxy <input type="checkbox"/> Autoimport </div> </div> <div> <div style="border: 1px solid #ccc; padding: 2px;">ldap://directory.swissign.net:389/o=swissign, c=ch??sub?mail=%E</div> <div style="margin-top: 5px; text-align: center;">Test</div> </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;">*@*</div>	<div style="margin-bottom: 5px;">Apply</div> <div>Remove</div>
3.	<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> <div style="border: 1px solid #ccc; padding: 2px;">PGP ▼</div> <div style="margin-top: 5px;"> <input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Use Proxy <input type="checkbox"/> Autoimport </div> </div> <div> <div style="border: 1px solid #ccc; padding: 2px;">ldap://keyserver.pgp.com:389/o=PGP keys??sub?pgpUserId=%EM!</div> <div style="margin-top: 5px; text-align: center;">Test</div> </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;">*@*</div>	<div style="margin-bottom: 5px;">Apply</div> <div>Remove</div>

- | | |
|--------------|--|
| Nr: | Fortlaufende Nummer welche bei Testabfragen die Zuordnung zum jeweiligen Server ermöglicht |
| Enabled: | Aktiviert/Deaktiviert eine Abfrage für den Betrieb (Testsabfragen sind immer noch möglich) |
| Use Proxy: | Aktiviert/Deaktiviert die Nutzung eines SOCKS-Proxy |
| Autoimport: | Keys vom Keyserver werden heruntergeladen und in der Import-Area abgelgt. |
| Target Link: | Hier steht der Syntax der eigentlichen Abfrage. Diese Zeile ist frei editierbar. |
| Filter: | <p>Schränkt die Abfragen auf die aufgeführten Zieladressen oder Adressräume ein (Default: *@* = Alle). Es stehen folgende Platzhalter zur Verfügung:</p> <ul style="list-style-type: none"> ○ ? → ersetzt ein beliebiges Zeichen ○ * → ersetzt eine beliebige Anzahl Zeichen ○ ! (Als erstes Zeichen) → Invertiert die Abfrage Logik:
Diese Adress(en) (-Räume) werden nicht abgefragt. Filtereinträge die mit einem !-Zeichen beginnen müssen jedoch vor globaleren Einträgen (z.B. *@*) stehen, um wirksam zu sein. |

Änderungen bei „Enabled“, „Proxy“, „Autoimport“, „Target-Link“ oder „Filter“ werden mit Click auf den jeweiligen Button **Apply** übernommen. Über den Button **Remove** wird ein Eintrag sofort und ohne weitere Bestätigung entfernt.

Neuer LDAP-Dienst

Über die Felder am Fuß der Liste können neue Abfragen hinzugefügt werden .

New Entry

Server+Port:

☐ Use Proxy (SOCKS)
☒ Autoimport

Search Root:

Available wildcards: * ? !
 (! as first char inverts logic)

- Use Proxy (SOCKS):** Aktiviert/Deaktiviert die Nutzung eines SOCKS Proxy (Einstellung unter 3.6.2 Proxy Einstellungen)
- Autoimport:** Keys vom Keyserver werden heruntergeladen und in der Import-Area abgelgt.
- Server+Port:** Tragen Sie hier den Servernamen und den Serverport (verbunden mit einem ;) ein
- Search Root:** Bisweilen muss ein sogenannter Einsprung-Punkt Teil des Aufrufes sein. Die Syntax erfahren Sie vom Anbieter eines Verzeichnisdienstes. Tragen Sie diesen hier ein.
- Filter:** Schränkt die Abfragen auf die aufgeführten Zieladressen oder Adressräume ein (Default: *@* = Alle). Es stehen folgende Platzhalter zur Verfügung:
- ? → ersetzt ein beliebiges Zeichen
 - * → ersetzt eine beliebige Anzahl Zeichen
 - ! (Als erstes Zeichen) → Invertiert die Abfrage Logik:
Diese Adress(en) (-Räume) werden nicht abgefragt. Filtereinträge die mit einem !-Zeichen beginnen müssen jedoch vor globaleren Einträgen (z.B. *@*) stehen, um wirksam zu sein.

Um die Abfrage der Liste hinzuzufügen klicken Sie abschließend auf den Button **Add**.

Testabfrage

Um einen eingetragenen Dienst zu testen, tragen Sie einfach eine Emailadresse in das Feld links neben dem Button Test des jeweiligen Servers und klicken dann auf den Button **Test**.

Am unteren Ende der Liste (ggf. ist herunterscrollen erforderlich) wird das Ergebnis der Abfrage angezeigt. Der grüne Schriftzug „Query OK“ zeigt an, dass der technische Abfragemechanismus erfolgreich durchlaufen wurde. Darunter werden dann die Anzahl der gefundenen Zertifikate und ggf. deren Details angezeigt.

Query: Server #1 for Support@companycrypt.com

Query OK

There is 1 certificate listed for Support@companycrypt.com

[OK] CompanyCRYPT Support, DE / 2008-08-20 until 2009-08-21
 Serial: 2E9200010002AAB65F094A70CDFB / ID: 9A9057CA9DC650EDB328B8DFA4879E8F6AF837CA

3.5.2. Interner Keyresponder – Schlüsselaustausch

Zur Nutzung der Standardformate OpenPGP und S/MIME ist der Austausch der Public Keys zwischen den Kommunikationspartnern erforderlich. CompanyCRYPT bietet mit seinem mailbasierten Keyserver eine komfortable Art des Schlüsselaustausches.

Adresskonfiguration für automatischen Schlüsserversand

WebGUI → (Configuration) Key Server → MIKE

Ausgelöst durch einen Key-Request kann CompanyCRYPT einen angeforderten Schlüssel per Mail verschicken. Existiert für die angegebene Adresse kein Schlüssel, oder wurde gar keine Mailadresse angegeben, so erfolgt der Versand einer entsprechenden Information. Dieses Feature nennt sich MIKE (Mail Initiated Key Exchange).



MIKE (Mail Initiated Key Exchange)	
Listener Address:	<input type="text" value="MIKE@companycrypt.com"/>
Sender Address:	<input type="text" value="companycrypt@CompanyCRYPT.com"/>
Local / Internal domains:	<input type="text" value="@CompanyCRYPT.com"/> <input type="text" value="@sit-internet.com"/> <input type="text" value="@netformat.de"/>
<p>Send only - If addressed to, no reply is generated. Used as sender address for 'Key-Unavailable' and 'Quickguide' notifications.</p> <p>Requests from these domains are considered internal. (Enter additional domains beginning with '@'.)</p>	
Send Keys/Certificates:	<p>From: <input checked="" type="radio"/> User address = <input type="text" value="The address of the Key owner"/></p> <p><input type="radio"/> Sender address = <input type="text" value="companycrypt@CompanyCRYPT.com"/></p> <p>Language: <input type="text" value="DEU"/></p> <p><input type="checkbox"/> Apply ZIP compression on attachments (Recipient with MS Outlook may require this to access key material.)</p>
S/MIME key reply option:	<input checked="" type="checkbox"/> Always sign S/MIME reply with user key. (Recipients may be able to import key from signature.)
Quickguide option:	<input type="checkbox"/> Avoid reply by subject keyword <input type="text" value="public key"/> <input type="checkbox"/> Case sensitive

- Listener Address:** Mails an diese Adresse werden als Schlüsselanforderungen durch MIKE verarbeitet.
- Sender Address:** Ist ein angeforderte Schlüssel nicht vorhanden, so wird eine Information (Reply) unter dieser Mailadresse an den Anfordernden verschickt. Mails an diese Adresse werden von MIKE ignoriert, um Mail-Loops zu vermeiden, ausgelöst durch Spam bzw. Mails mit ungültigen Absendern.
- Local / Internal Domains:** Hier werden alle intern verwalteten Internetdomänen angegeben. Diese Information dient zur Unterscheidung, ob der Keyserver von Intern oder von Extern angesprochen wird.
- Send Keys/Certificates from:** Unter welcher Absenderadresse sollen die Schlüssel versand werden.
- User address:** Der Schlüssel wird unter der Adresse des Schlüsselinhabers verschickt. (Diese Adresse ist auch in den Schlüsseleigenschaften hinterlegt.)
- Listener address:** Der Versand des Schlüssels erfolgt unter der Adresse, welche im Feld Listener address definiert wurde.
- Apply ZIP compression:** Die Schlüssel werden als ZIP-Archiv verpackt und an die Email anhängt. Der Empfänger kann dann das Schlüsselmaterial aus der Email extrahieren, anders als wenn die Schlüssel direkt als Anlage in der Email enthalten sind, verweigern Emailprogramme den Zugriff.
- S/MIME key reply option:** Zusätzliche Funktion für S/MIME-Schlüssel
- Always sign S/MIME reply with user key:** Aktiviert/Deaktiviert das Signieren der Mails (Replies) für S/MIME-Schlüssel. Die S/MIMEStandardmäßig werden die Schlüssel als Attachment verschickt.
- Quickguide option:** Im Quickguide wird die Handhabung des Keyserver für den Benutzer beschrieben. Der Quickguide wird automatisch verschickt, wenn eine Mail ohne Schlüsselanforderung an die Listener Address geschickt wird
- Avoid reply by subject keyword:** Schlüsselwort zum Unterdrücken des Quickguide-Versandes, welches in der Betreffzeile der Mail angegeben werden muss.
- Case sensitive:** Aktiviert/Deaktiviert die Unterscheidung von Groß- und Kleinbuchstaben

Automatische Schlüsselerstellung

WebGUI → (Configuration) Key Server → On-demand Key Generation

CompanyCRYPT kann automatisiert Schlüssel für interne User generieren. Per Keyrequest (Mail an MIKE) wird der jeweils angeforderte Schlüssel – sofern noch nicht vorhanden - anhand einer definierten Referenzliste erstellt und verschickt. Diese Funktion wird vom Operational Dienst realisiert.



Synchronise Internal Keys with Groupware (Reference list)			
Enable generation of:	<input type="checkbox"/> PGP keys	<input type="checkbox"/> S/MIME keys	
List File Location:	(OK)	C:\Programme\CompanyCRYPT\Listings\KeyRefExample.txt	
Check Interval:	10 Min.	Generate max.	5 Keys/Interval

Enable generation of: Automatische Schlüsselerstellung

PGP keys: Aktiviert/Deaktiviert die Erstellung von PGP-Schlüsseln

S/MIME keys: Aktiviert/Deaktiviert die Erstellung von S/MIME-Zertifikaten

List File Location: Verweis auf die Referenzliste

Check Interval: Zeitintervall in Minuten, nachdem CompanyCRYPT auf neue Anforderungen zur Schlüsselerstellung prüft

Generate max. Keys/Interval: Maximale Anzahl der, innerhalb eines Intervalls, zu erstellenden Schlüssel (Standardwert: 2 / 1min). Da die Schlüsselerstellung vor allem CPU-Zeit beansprucht, sollte dieser Wert nicht zu hoch eingestellt werden, um eine mögliche Beeinträchtigung anderer Systemprozesse zu vermeiden.

Groupware-Schnittstelle (Referenzliste)

WebGUI → (Configuration) Key Server → On-demand Key Generation → Synchronize Internal Keys with Groupware

Die Referenzliste dient als Vorlage für die automatische Schlüsselerstellung. Sie enthält detaillierte Angaben für jeden zu erstellenden Schlüssel.

```

# Example 1
Email: Mr.Smith@Agency.com
Name: Mr. Smith
Company: Agency
Department:
Location:
Country: US
PGPValidity: 0
SMIMEValidity:
KeyLength: 2048

# Example 2
Email: Alice.Strawberry@warehouse.com
Name: Alice Strawberry
Company: Warehouse
Department: Marketing
Location:
Country:
PGPValidity:
SMIMEValidity:
KeyLength: 1024

```

Aufbau der Referenzliste

Die Referenzliste enthält pro Zeile eine Feldbezeichnung und den jeweiligen Wert. Als Trennzeichen wird ein Doppelpunkt gefolgt von einem Leerzeichen verwendet. Für jeden einzelnen Schlüssel (user) sind die folgende Werte zu definieren.

#	Kommentarzeilen
Email:	eMailadresse des Users (Pflichtfeld)
Name:	Vor- und Zuname bzw. Bezeichnung des Users (Pflichtfeld)
Company:	Firmenbezeichnung
Department:	Abteilung
Location:	Ort
Country:	Landeskürzel (2-stellig)
PGPValidity:	Gültigkeitsdauer für PGP-Keys in Tagen (0 = ohne Ablaufdatum)
SMIMEValidity:	Gültigkeitsdauer für S/MIME-Zertifikate in Tagen

KeyLength: Schlüssellänge in Bit (gilt für PGP und S/MIME)

Sind hinter einem Feld keine Daten angegeben, so werden für die Schlüsselerzeugung die Voreinstellungen aus dem Bereich **Key Defaults** verwendet.

SMTP-Konfiguration für automatischen Schlüsselversand

WebGUI → (Configuration) Key Server → Alternative Target Host

Ausgelöst durch einen Key-Request kann CompanyCRYPT einen angeforderten Schlüssel per Mail an die anfordernde Adresse (Absender) schicken. Existiert für die angegebene Adresse kein Schlüssel, oder wurde gar keine Mailadresse angegeben, so erfolgt der Versand einer entsprechenden Information.

Alternative Target Host

Send to this host: Port:

Use local Hostname: Select the local host name used during SMTP-HELO/EHLO command.

☒ Default

☐ Custom

Send to this Host/port: Hostname oder IP-Adresse und Port des Systems, an welche die angeforderten Schlüssel gesendet werden. Standardmäßig wird hier das lokale System eingetragen.

Use local Hostname: Erlaubt die Anpassung des HELO/EHLO-Parameters. Dies kann notwendig sein, sofern die Weiterleitung der Keyreplies vom Zielsystem verweigert wird.

Default: FQDN aus den Netzwerkeinstellungen des Betriebssystems wird benutzt.

Custom: Benutzerdefinierte Angabe

Hinweis: Um den Schlüsselversand über den MIMESweeper for SMTP zu ermöglichen, ist die Eintragung des CompanyCRYPT-Systems unter Relay Hosts in der MIMESweeper-Konfiguration notwendig.

Hinweis: In einer verteilten Umgebung ist diese Konfiguration per SyncManager für jedes Slave-System individuell anzupassen!

SMTP-Konfiguration für automatischen Schlüsselversand per SyncManager

SyncManager → Configuration → Local System → Key Replies

Wichtig: Bevor Sie Konfigurationsänderungen mit dem SyncManager vornehmen muss immer der Operational Service von CompanyCRYPT gestoppt werden um die Synchronisation anzuhalten! Andernfalls werden die Änderungen nicht übernommen. Nach Abschluss der Konfiguration ist der Operational Service wieder zu starten.

Key-Replies werden in der Standardkonfiguration immer an das eigene System weitergeleitet. Daher ist in verteilten Umgebungen dieser Eintrag für jedes Slave-System anzupassen.

KEY-REPLIES (MIKE)

Send to host: on port:

SMTP-EHLO-Name: ☐ Custom

☒ Default

Send to Host/port: Hostname oder IP-Adresse und Port des Systems, an welche die angeforderten Schlüssel gesendet werden. Standardmäßig wird hier das lokale System eingetragen.

SMTP-EHLO-Name: Erlaubt die Anpassung des HELO/EHLO-Parameters. Dies kann notwendig sein, sofern die Weiterleitung der Keyreplies vom Zielsystem verweigert wird.

Default: FQDN aus den Netzwerkeinstellungen des Betriebssystems wird benutzt.

Custom: Benutzerdefinierte Angabe

3.6. System Parameter

3.6.1. Statusanzeige

WebGUI → (Configuration) System → Status

Der Statusbildschirm zeigt Ihnen, ob die CompanyCRYPT-Dienste gestartet oder gestoppt sind. Weiterhin erhalten Sie Auskunft über die Mails, welche noch in der Reprocessor-Queue zur Verarbeitung warten.

Status Chart			
System	Status	Last Action	
MASTER msw.companycrypt.com	Operational Service: Running	Started up at 2010-01-05_16:25:55	<button>Stop</button>
	Reprocess Service: Running	Started up at 2010-01-05_16:47:39	<button>Stop</button>
	Last Processing: 0 Messages		
	In Queue: 0 Messages		

In verteilten Umgebungen mit Master und Slave-Konfiguration werden die Statusinformationen aller Systeme angezeigt.

SLAVE ps.companycrypt.com	Operational Service: Running	Started up at 2010-01-05_16:22:05
	Reprocess Service: Running	Started up at 2010-01-05_16:53:36
	Last Processing: 0 Messages	
	In Queue: 0 Messages	

- System: Name oder IP-Adresse des Systems
- Status: Zeigt den Dienststatus – gestartet oder gestoppt – an.
 Last Processing: Zeigt die Zahl der beim letzten Durchgang verarbeiteten Mails.
 In Queue: Zeigt die Anzahl der noch zu verarbeitenden Mails an.
- Last Action: Zeitstempel zum letzten Status

3.6.2. Backup und Restore

Backup / Restore Parameter

WebGUI → (Configuration) System → Backup / Restore → Common parameter

Im ersten Abschnitt werden das Verzeichnis und das Passwort für Backup und Restore festgelegt.

Common parameter	
Backup/Restore folder: (OK)	<input style="width: 90%;" type="text" value="C:\Programme\CompanyCRYPT\Backup"/> <input style="float: right;" type="button" value="Save"/>
Common password:	<input style="width: 90%;" type="text" value="5P180-YMYK0-7L5Q2-0MP0P-JVJ6JZ-29CMP"/> <input style="float: right;" type="button" value="Apply"/>

- Backup/Restore folder: Verzeichnis für die Speicherung der Backups
- Common password: Passwort für den Zugriff auf die Backupdateien. Der CompanyCRYPT-Licence Key ist das Standardpasswort für das automatische Backup. Ein individuelles Passwort kann nur für ein manuelles Backup eingetragen aber nicht dauerhaft gespeichert werden.

Automatisches Backup

WebGUI → (Configuration) System → Backup / Restore → Automatic Backup

CompanyCRYPT erlaubt die zeitgesteuerte Sicherung des Schlüsselmaterials sowie der Konfigurationseinstellungen. Durch anklicken der Schaltfläche **Save**, speichern Sie die Daten.

Automatic Backup

Daily job activated: Yes

Keep History (Days): 7

Schedule Job (HH:MM): 23:55 Save

- Daily job activated: Aktivierung bzw. Deaktivierung des automatischen Backups
- Keep History (Days): Angabe der Tage für die Backuphistorie, ältere Backups werden automatisch gelöscht
- Schedule Job (HH:MM): Angabe der Uhrzeit für das automatische Backup

Manuelles Backup

WebGUI → (Configuration) System → Backup / Restore → Manual Backup

Zum Erstellen eines manuellen Backups geben Sie im Feld **Filename** den gewünschten Dateinamen an und starten das Backup anschließend durch anklicken der Schaltfläche **Backup Now**.

Manual Backup

Filename CompanyCRYPT_2007-01-22.bac

Backup Now

System wiederherstellen (Restore)

WebGUI → (Configuration) System → Backup / Restore → Restore

Zur Wiederherstellung von gesicherten CompanyCRYPT-Einstellungen sowie Schlüsselmaterial dient der Restore-Bereich. Die Listenansicht zeigt die Backupdateien des unter **Common folder** angegebenen Verzeichnisses.

Restore

Select file from list (12 files)

CompanyCRYPT_2006-10-10.bac

CompanyCRYPT_2007-01-22.bac

_CompanyCRYPT_2007-01-12_23-55-03.bac

_CompanyCRYPT_2007-01-13_23-55-03.bac

_CompanyCRYPT_2007-01-14_23-55-03.bac

_CompanyCRYPT_2007-01-15_23-55-03.bac

_CompanyCRYPT_2007-01-16_23-55-03.bac

Restore
Delete File

Soll ein Backup wiederhergestellt werden, so wählen Sie den entsprechenden Dateinamen aus der Liste. Es wird jetzt automatisch geprüft, ob der Zugriff auf das Backupfile mit dem Standardpasswort möglich ist. Durch Betätigen der Schaltfläche **Restore** wird der Datenbestand vom gewählten Backupfile wiederhergestellt.

Restore

Select file from list (12 files)

CompanyCRYPT_2006-10-10.bac

CompanyCRYPT_2007-01-22.bac

_CompanyCRYPT_2007-01-12_23-55-03.bac

_CompanyCRYPT_2007-01-13_23-55-03.bac

_CompanyCRYPT_2007-01-14_23-55-03.bac

_CompanyCRYPT_2007-01-15_23-55-03.bac

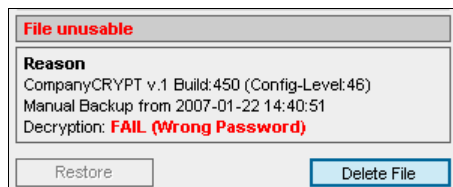
_CompanyCRYPT_2007-01-16_23-55-03.bac

Valid Restore File

Details:
CompanyCRYPT v.1 Build: 450 (Config-Level: 46)
Manual Backup from 2007-01-22 14:40:51
Decryption: **OK**

Restore
Delete File

Ist der Zugriff auf die Backupdatei mit dem Standardpasswort nicht möglich, so ist ein Restore nicht möglich. In diesem Fall tragen Sie bitte das korrekte Passwort unter **Common password** ein und bestätigen dies mit der Schaltfläche **Apply**.



Backupdateien löschen

WebGUI → (Configuration) System → Backup / Restore → Restore

Markieren Sie den entsprechenden Dateinamen und bestätigen Sie den Löschvorgang mit **Delete File**.

3.6.3. Einstellungen Systemdienste

Reprocess Service

WebGUI → (Configuration) System → Reprocess Service

Unter diesem Punkt werden Einstellungen zum Reprocess Service vorgenommen. Der Reprocess Service ist ein SMTP-Agent, welcher die eMails aus der Reprocessing-Queue verarbeitet.

Reprocess Service	
Service status:	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #d9ead3; color: green; font-weight: bold;">Installed and Running</div> <div style="margin-left: 10px; border: 1px solid #ccc; padding: 2px 10px; background-color: #d9ead3;">Stop Service</div> </div>
Reprocess to Host/Port:	<div style="display: flex; align-items: center;"> <input style="width: 150px;" type="text" value="127.0.0.1"/> <input style="width: 50px; margin-left: 10px;" type="text" value="25"/> </div>
Reprocess folder:	<div style="display: flex; align-items: center;"> (OK) <input style="width: 500px;" type="text" value="C:\Programme\Cleaswift\MIMesweeper for SMTP\Mail\SaveAction\Reprocessing"/> </div>
Max reprocessing:	<div style="display: flex; align-items: center;"> <input style="width: 50px;" type="text" value="5"/> Cycles </div>
Reprocess log:	<div style="display: flex; align-items: center;"> <input checked="" type="checkbox"/> Yes </div>

Service status: Anzeige und Steuerung des Betriebsstatus für den Reprocess Service. In Abhängigkeit des Status ändert sich die Funktion des Buttons.

Service Status Button-Status

Installed and Running	Stop Service
Installed and Stop pending	Query Status
Installed and Stopped	Start Service
Installed and Start pending	Query Status
Not installed	-

Reprocess to Host/Port: Host-Name oder IP-Nummer und Port des Zielsystems, an welches die Mails aus der Reprocessing-Queue zugestellt werden sollen. Bei der Initialisierung von CompanyCRYPT wird hier standardmäßig die IP des lokalen Systems und der SMTP-Standardport (25) eingetragen.

Reprocess folder: Verzeichnis, Reprocessing-Queue

Max reprocessing: Maximale Anzahl von Entschlüsselungsdurchläufen für eine eMail (Standard: 3). Diese Option berücksichtigt die Möglichkeit der mehrfachen (verschachtelten) Verschlüsselung. Werden also in einer entschlüsselten Mail weitere verschlüsselte Inhalte entdeckt, so erfolgen weitere Entschlüsselungsdurchläufe. Dieser Wert sollte nicht ohne Rücksprache mit dem Support geändert werden.

Reprocess log: Aktiviert bzw. Deaktiviert die Ausgabe der Verarbeitungsinformationen des Reprocess Services in ein Logfile. Diese Datei befindet sich im gemeinsamen Log Ordner und ist nach folgendem Muster benannt: *RP-Log_yyyy-mm-dd.txt*. Die Logdateien werden automatisch nach 7 Tagen gelöscht.

Hinweis: Um das Reprocessing über den MIMESweeper for SMTP zu ermöglichen, ist die Eintragung des CompanyCRYPT-Systems unter Relay Hosts in der MIMESweeper-Konfiguration notwendig.

Reprocess Service - Konfiguration per SyncManager

SyncManager → Configuration → Local System → Reprocess Service

Der Reprocess Service ist ein SMTP-Agent, welcher die eMails aus der Reprocessing-Queue verarbeitet. Diese eMails werden in der Standardkonfiguration immer an das eigene System weitergeleitet. Daher ist in verteilten Umgebungen dieser Eintrag für jedes Slave-System anzupassen.

Wichtig: Bevor Sie Konfigurationsänderungen mit dem SyncManager vornehmen muss immer der Operational Service von CompanyCRYPT gestoppt werden um die Synchronisation anzuhalten! Andernfalls werden die Änderungen nicht übernommen. Nach Abschluss der Konfiguration ist der Operational Service wieder zu starten.

REPROCESS SERVICE

Reprocess to host: on port:

Reprocess to Host/Port: Host-Name oder IP-Nummer und Port des Zielsystems, an welches die Mails aus der Reprocessing-Queue zugestellt werden sollen.

Reprocess Log

WebGUI → (Configuration) System → Reprocess Service → Reprocess Log

Hier erfolgt die Anzeige des aktuellen CompanyCRYPT-Logfiles für den Reprocess Service. Standardmäßig werden nur die letzten Einträge angezeigt. Über den Button **Expanded View** kann auch die Anzahl der angezeigten Logeinträge erweitert werden. Aus Performancegründen werden jedoch maximal 100 KB des Logfiles ausgegeben.

Reprocessor Log: Today Last Refresh: 16:55:46 [Expanded View](#)

```

2008-01-04 16:55:46 Reprocess Service STARTED
2008-01-04 16:55:46 Reprocess Target Mailto 127.0.0.1 (Port_25)
2008-01-04 16:55:46 Daily Job Cleanup old logs(Keep last 7) --> OK
                
```

<< Prev
RP-Log_2008-01-04.txt
Show Today
Size: 0.199 kB
Next >>

Unter dem Anzeigefenster für das Logfile befinden sich Navigationsbutton, welche das Wechseln zwischen den früheren und späteren Logdateien erlauben.

3.6.4. Logging

Trace Optionen und Logging-Parameter

WebGUI → (Configuration) System → Trace / Logging → Trace and Logging

CompanyCRYPT bietet für die integrierten Module erweiterte Optionen für die Fehleranalyse.

Trace and Logging			
Log folder:	(OK)	D:\CompanyCRYPTLogs	
Tracelog Level:	1 - Short Summary	History:	7 days
Operational Log Level:	1 - Normal Mode	History:	7 days
Reprocess Log Level:	1 - Normal Mode	History:	7 days
		<input type="checkbox"/>	Show SMTP talk
		<input type="checkbox"/>	Keep temporary files
		<input type="checkbox"/>	Verbose CMDline
		<input type="checkbox"/>	Verbose key processing

Log folder:	Verzeichnis für die Ablage der CompanyCRYPT-Logdateien
Tracelog Level:	Aktivieren/Deaktivieren und Einstellung des Loglevels für das Protokollieren aller Encrypt/Decrypt-Prozesse im Tracelog.
Operational Log Level:	Wahl zwischen Aktivieren/Deaktivieren und Debug-Mode für das Operational Log.
Reprocess Log Level:	Aktivieren/Deaktivieren der Protokollierung für den Reprocessor Service.
History:	Angabe der Logfile History in Tagen. Ältere Logfiles werden automatisch gelöscht.
Show SMTP talk:	Erweiterte Programmausgabe beim manuellen Versand eines Public Keys aus der WebGUI
Keep temporary files:	Beibehalten der, bei der Ver- und Entschlüsselung erzeugten, temporären Dateien im temporären Arbeitsverzeichnis des MIMESweepers. (Vom System definierten Ordner für temporäre Dateien.)
Verbose CMDline:	Kommandozeilen-orientiertes Troubleshooting (für Entwickler)
Verbose key processing:	Erweiterte Programmausgaben bei der Erstellung und dem Import von Schlüsseln

Trace Log

WebGUI → (Configuration) System → Trace / Logging → Trace and Logging → Trace Log

Sofern die Protokollierung ins Tracelog aktiviert wurde, erfolgt hier die Anzeige des aktuellen Tracelogs. Standardmäßig werden nur die letzten Einträge angezeigt. Über den Button **Expanded View** kann auch die Anzahl der angezeigten Logeinträge erweitert werden. Aus Performancegründen werden jedoch maximal 100 KB des Logfiles ausgegeben.

Trace Log: Today		Last Refresh: 17:07:22		Expanded View			
<p>File not found or empty.</p>							
<< Prev		Trace-Log_2008-01-04.txt		Show Today		Size: 0.000 kB	
						Next >>	

Unter dem Anzeigefenster für das Logfile befinden sich Navigationsbutton, welche das Wechseln zwischen den früheren und späteren Logdateien erlauben.

3.6.5. Proxy Einstellungen

WebGUI → (Configuration) System → Proxy

HTTP Proxy

Für die automatische Aktualisierungsprüfung von CompanyCRYPT ist eine Internetverbindung auf Port 80 (http) Voraussetzung. Die Kommunikation kann auch per Proxy realisiert werden.



HTTP Proxy [Used for update check]	
HTTP Proxy Server:	<input type="text"/> Port: <input type="text"/>
Authenticate as:	<input type="text"/>
with Password:	<input type="text"/>

HTTP Proxy Server / Port: IP oder DNS-Name des Proxy-Servers und TCP/IP-Port

Authenticate as: Benutzername sofern der Proxy eine Anmeldung erfordert

With Password: Passwort für Proxyanmeldung

SOCKS Proxy

Die CompanyCRYPT Verschlüsselungsszenarios „Automatic Encryption“, „Best Effort“ und „User Control“ können fehlende Schlüssel ggf. über LDAP Verzeichnisdienste ergänzen. Diese Kommunikation kann auch per SOCKS-Proxy realisiert werden.

SOCKS Proxy [Used for internet key server queries]	
SOCKS Proxy Server:	<input type="text"/> Port: <input type="text"/>
Authenticate as:	<input type="text"/>
with Password:	<input type="text"/>

SOCKS Proxy Server / Port: IP oder DNS-Name des Proxy-Servers und TCP/IP-Port

Authenticate as: Benutzername sofern der Proxy eine Anmeldung erfordert

With Password: Passwort für Proxyanmeldung

3.6.6. Zusammengefasste Verwaltungsfunktionen

Verwaltung der CompanyCRYPT-Dienste

WebGUI → (Configuration) System → Service Control / MIMESweeper → Service Control

Diese Optionen dienen der Steuerung der CompanyCRYPT-Dienste.

Service Control	
Reprocess service:	<input type="button" value="Stop"/> <input type="button" value="Uninstall"/>
Operational service:	<input type="button" value="Start"/> <input type="button" value="Uninstall"/>

Installation parts

Reprocess service: Starten/Stoppen bzw. Install/Uninstall des CompanyCRYPT Reprocess Service

Operational Service: Starten/Stoppen bzw. Install/Uninstall des CompanyCRYPT Operational Service

Re-Initialisierung des Systems

WebGUI → (Configuration) System → Service Control / MIMESweeper → Remove / Reinitialise

Diese Optionen dienen zur Re-Initialisierung der CompanyCRYPT-Parameter im Fehlerfall oder zur Deinstallation.

Remove / Reinitialise Installation Components	
EXE.INI entries:	<input type="button" value="Remove"/>
Configuration:	<input type="button" value="Re-Initialise"/>

EXE.INI entries: Add/Remove für Hinzufügen und Löschen der CompanyCRYPT-Einträge in der MIMESweeper –Konfigurationsdatei EXE.INI

Configuration: Erneutes Initialisieren der CompanyCRYPT-Installation, Prüfen und Setzen von benötigten Programmparametern



Secure Internet Traffic



COMPANYCRYPT®
The encryption module for MIMesweeper

CompanyCRYPT
System Parameter

Configuration Guide
CompanyCRYPT v1.5.0

MIMesweeper Einstellungen

WebGUI → (Configuration) System → Service Control / MIMesweeper → MIMesweeper

MIMesweeper	
EXE.INI location:	(OK) C:\Programme\Cleaswift\MIMesweeper for SMTP\MSV_Program\EXE.INI
Reprocess folder:	(OK) C:\Programme\Cleaswift\MIMesweeper for SMTP\Mail\SaveAction\Reprocessing
Max eMail size:	<input type="text" value="75"/> MByte
Note: The MIMesweeper interface allows any external szenario-job a processing time frame of 30 seconds. To avoid unexpected termination of CompanyCRYPT processes, set this value to a maximum of 50 MByte per GHz CPU (3 GHz = 150 MByte).	
<input type="button" value="Save"/>	

EXE.INI location: Zeigt den Pfad zur MIMesweeper-Konfigurationsdatei EXE.INI

Reprocess folder: Zeigt den Pfad für die Reprocessor Queue

Max eMail size: Maximale Mailgröße in MByte, bis zu welcher CompanyCRYPT Ver- und Entschlüsselt (Standard: 500). Dieser Wert ist CPU Performance abhängig.

3.7. Verteilte Systeme (Multi-Server)

3.7.1. Betriebsmodus

WebGUI → (Configuration) Sync

CompanyCRYPT ist sowohl für den Einsatz auf einzelnen Systemen als auch für verteilte Umgebungen mit mehreren Servern konzipiert. Damit unterstützt es das zentrale Management für verteilte Systeme analog der Multi-Serverfähigkeit des MIMESweepers.

Entsprechend den Anforderungen kann CompanyCRYPT für den erforderlichen Modus konfiguriert werden. Unterstützt werden die Modi Single, Master und Slave.

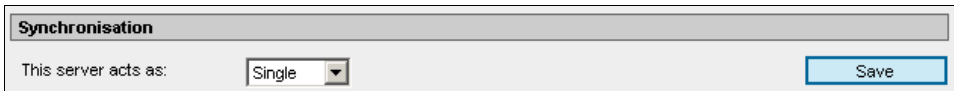
Modus

Single	Standalone-System
Master	Zentrales Konfigurationssystem, welches Konfigurationsänderungen für Slave-Systeme bereitstellt. Schlüssel-Erzeugungsanfragen (MIKE) werden durch dieses System verarbeitet.
Slave	Übernimmt Konfigurationsänderungen vom Master-System. Neues Schlüsselmaterial aus dem Import Ordner wird zum Master-System übertragen

3.7.2. Modus: Single

WebGUI → (Configuration) Sync → Synchronisation

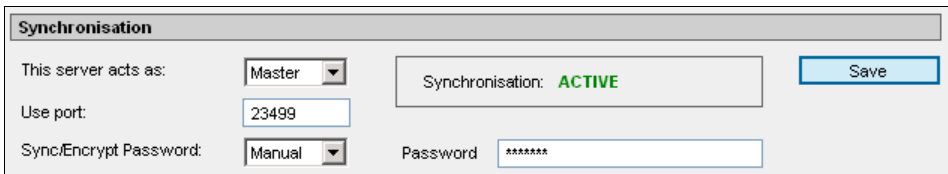
Um CompanyCRYPT im Single-Modus zu betreiben, stellen Sie die Option **This server acts as:** auf **Single**. Dies stellt auch die Standardeinstellung dar.



3.7.3. Modus: Master

WebGUI → (Configuration) Sync → Synchronisation

Um CompanyCRYPT im Master-Modus zu betreiben, stellen Sie die Option **This server acts as:** auf **Master**. Dieser Modus entspricht in den Funktionen dem Single-Modus. Zusätzlich werden aber noch Anfragen von Slave-Systemen bearbeitet.



Use port: IP-Port für Master-Slave-Kommunikation

Sync/Encrypt Password: Für die Master-Slave-Kommunikation wird ein Passwort verwendet. Die Einstellung Auto verwendet den CompanyCRYPT-Lizenzkey (Standard). Werden CompanyCRYPT-Systeme mit unterschiedlichen Lizenzen verwendet, so muss die Einstellung Manual gewählt werden und ein Passwort definiert werden.

Password: Passwort für die Master-Slave-Kommunikation (Nur verfügbar bei Manual Sync/Encrypt Passw.)



Start Service: Wenn der CompanyCRYPT Operational Service im Zustand 'gestopped' ist, kann er über den Button *Start Service* gestartet werden.



Hinweis: Zum Deaktivieren der Synchronisation wählen Sie den Modus „Single“. Die eingetragene Werte (Hostnamen, Passwort, ...) bleiben erhalten.

Auf dem Master-System müssen alle Slave-Systeme hinterlegt werden, damit die Kommunikationsanfragen der Slave-Systeme berücksichtigt werden.

Accepted Slave Hosts	Last Status	Last Connect	Save IP's
192.168.0.150	Unreachable	Unknown	Query Status
localhost	IP reachable	2007-03-15 15:28:30	Reset Status

Accepted Slave Hosts: Hostnamen oder IP-Adressen der Slave-Systeme

Last Status: Anzeige Kommunikationsstatus
 Unreachable: System nicht erreichbar
 IP reachable: System netzwerkseitig erreichbar
 Abort Connect: Verbindungsabbruch durch Remote host
 CONNECT:Unknown Host: Verbindungsabbruch: Master kennt Slave nicht
 CONNECT:Wrong Password: Verbindungsaufbau durch falsches Sync-Passwort gescheitert
 CONNECT:Qualified Host: Erfolgreicher Verbindungsaufbau
 SYNC in Progress: aktueller Synchronisationsvorgang
 SYNC failed: Synchronisation fehlgeschlagen
 SYNC OK: Erfolgreiche Synchronisation

Last Connect: Datum des letzten Status

Query Status: Aktualisieren der Statusanzeige (= Aktualisierung der Anzeige)

Reset Status: Löschen der Statusanzeige auf 'Unknown'

Modus: Master - Konfiguration per SyncManager

SyncManager → Configuration

Wichtig: Bevor Sie Konfigurationsänderungen mit dem SyncManager vornehmen muss immer der Operational Service von CompanyCRYPT gestoppt werden um die Synchronisation anzuhalten! Andernfalls werden die Änderungen nicht übernommen. Nach Abschluss der Konfiguration ist der Operational Service wieder zu starten.

Wählen Sie unter Configuration **This Server act as: Master** aus und tragen Sie unter **Valid Sync Host** die IP-Adressen oder den DNS-Namen der Slave-Systeme ein. Speichern Sie die Einstellungen mit **Apply**.

CONFIGURATION

This Server acts as: Password Source:

Use Port: Manual Password:

Sync Interval (sec):

Valid Sync Hosts	Last Status	Last Connect
slave-host.doamin.com	SYNC OK	2010-01-06 17:25:44

Apply

Use port: IP-Port für Slave-Master -Kommunikation

Password Source: Für die Slave-Master-Kommunikation wird ein Passwort verwendet. Die Einstellung Auto verwendet den CompanyCRYPT-Lizenzkey (Standard). Werden CompanyCRYPT-Systeme mit unterschiedlichen Lizenzen verwendet, so muss die Einstellung Manual gewählt werden und ein Passwort definiert werden.



Password:	Passwort für die Slave-Master-Kommunikation, welches nur verwendet wird, wenn die Password Source auf Manual steht.
Sync Interval:	Zeitintervall in Sekunden für die Synchronisationsanfragen des Slave-System beim Master-System (Standard: 30 Sekunden)
Valid Sync Hosts:	Hostnamen oder IP-Adressen der Master-Systeme
Last Status:	Anzeige Kommunikationsstatus Unreachable: System nicht erreichbar IP reachable: System netzwerkseitig erreichbar Abort Connect: Verbindungsabbruch durch Remote host CONNECT:Unknown Host: Verbindungsabbruch: Master kennt Slave nicht CONNECT:Wrong Password: Verbindungsaufbau durch falsches Sync-Passwort gescheitert CONNECT:Qualified Host: Erfolgreicher Verbindungsaufbau SYNC in Progress: aktueller Synchronisationsvorgang SYNC failed: Synchronisation fehlgeschlagen SYNC OK: Erfolgreiche Synchronisation
Last Connect:	Datum der letzten Synchronisation

3.7.4. Modus: Slave

WebGUI → (Configuration) Sync → Synchronisation

Um CompanyCRYPT im Slave-Modus zu betreiben, stellen Sie die Option **This server acts as:** auf **Slave**. In diesem Modus erhält CompanyCRYPT alle Einstellungen und Keys von einem bzw. mehreren Master-Systemen.

Synchronisation	
This server acts as:	Slave <input type="button" value="v"/>
Use port:	23499 <input type="button" value="v"/>
Sync/Encrypt Password:	Manual <input type="button" value="v"/>
Slave Sync Interval (sec):	30 <input type="button" value="v"/>
Synchronisation: ACTIVE <input type="button" value="Save"/>	
Password: <input type="password" value="....."/>	

Use port:	IP-Port für Slave-Master -Kommunikation
Sync/Encrypt Password:	Für die Slave-Master-Kommunikation wird ein Passwort verwendet. Die Einstellung Auto verwendet den CompanyCRYPT-Lizenzkey (Standard). Werden CompanyCRYPT-Systeme mit unterschiedlichen Lizenzen verwendet, so muss die Einstellung Manual gewählt werden und ein Passwort definiert werden.
Password:	Passwort für die Slave-Master-Kommunikation (Nur verfügbar bei <i>Manual</i> Sync/Encrypt Passw.)
Slave Sync Interval:	Zeitintervall in Sekunden für die Synchronisationsanfragen des Slave-System beim Master-System

Hinweis: Zum Deaktivieren der Synchronisation wählen Sie den Modus „Single“. Die eingetragene Werte (Hostnamen, Passwort, ...) bleiben erhalten.

Auf einem Slave-System können mehrere Master-Systeme hinterlegt werden, um eine redundante, ausfallsichere Umgebung zu ermöglichen.

Available <u>Master Hosts</u>	Last Status	Last Connect	<input type="button" value="Save IP's"/>
192.168.0.150	Unreachable	2007-03-15 15:33:07	<input type="button" value="Query Status"/>
localhost	IP reachable	2007-03-15 15:33:20	<input type="button" value="Reset Status"/>

Available Master Hosts:	Hostnamen oder IP-Adressen der Master-Systeme
Last Status:	Anzeige Kommunikationsstatus Unreachable: System nicht erreichbar IP reachable: System netzwerkseitig erreichbar Abort Connect: Verbindungsabbruch durch Remote host CONNECT:Unknown Host: Verbindungsabbruch: Master kennt Slave nicht



CONNECT:Wrong Password: Verbindungsaufbau durch falsches Sync-Passwort gescheitert
 CONNECT:Qualified Host: Erfolgreicher Verbindungsaufbau
 SYNC in Progress: aktueller Synchronisationsvorgang
 SYNC failed: Synchronisation fehlgeschlagen
 SYNC OK: Erfolgreiche Synchronisation

Last Connect: Datum der letzten Synchronisation
 Query Status: Aktualisieren der Statusanzeige
 Reset Status: Löschen der Statusanzeige

Modus: Slave - Konfiguration per SyncManager

SyncManager → Configuration

Wichtig: Bevor Sie Konfigurationsänderungen mit dem SyncManager vornehmen muss immer der Operational Service von CompanyCRYPT gestoppt werden um die Synchronisation anzuhalten! Andernfalls werden die Änderungen nicht übernommen. Nach Abschluss der Konfiguration ist der Operational Service wieder zu starten.

Wählen Sie unter Configuration **This Server act as: Slave** aus und tragen Sie unter **Valid Sync Host** die IP-Adresse oder den DNS-Namen des Master-Systems ein. Speichern Sie die Einstellungen mit **Apply**.

Valid Sync Hosts	Last Status	Last Connect
master-host.domain.com	SYNC OK	2008-01-15 15:03:31

Use port: IP-Port für Slave-Master -Kommunikation

Password Source: Für die Slave-Master-Kommunikation wird ein Passwort verwendet. Die Einstellung Auto verwendet den CompanyCRYPT-Lizenzkey (Standard). Werden CompanyCRYPT-Systeme mit unterschiedlichen Lizenzen verwendet, so muss die Einstellung Manual gewählt werden und ein Passwort definiert werden.

Password: Passwort für die Slave-Master-Kommunikation, welches nur verwendet wird, wenn die Password Source auf Manual steht.

Sync Interval: Zeitintervall in Sekunden für die Synchronisationsanfragen des Slave-System beim Master-System (Standard: 30 Sekunden)

Valid Sync Hosts: Hostnamen oder IP-Adressen der Master-Systeme

Last Status: Anzeige Kommunikationsstatus
 Unreachable: System nicht erreichbar
 IP reachable: System netzwerkseitig erreichbar
 Abort Connect: Verbindungsabbruch durch Remote host
 CONNECT:Unknown Host: Verbindungsabbruch: Master kennt Slave nicht
 CONNECT:Wrong Password: Verbindungsaufbau durch falsches Sync-Passwort gescheitert
 CONNECT:Qualified Host: Erfolgreicher Verbindungsaufbau
 SYNC in Progress: aktueller Synchronisationsvorgang
 SYNC failed: Synchronisation fehlgeschlagen
 SYNC OK: Erfolgreiche Synchronisation

Last Connect: Datum der letzten Synchronisation



Operational Log

WebGUI → (Configuration) Sync → Operational Log

Hier erfolgt die Anzeige des aktuellen Operational-Logs. Standardmäßig werden nur die letzten Einträge angezeigt. Über den Button **Expanded View** kann auch die Anzahl der angezeigten Logeinträge erweitert werden. Aus Performancegründen werden jedoch maximal 100 KB des Logfiles ausgegeben.

Operational Log: Today			Last Refresh: 17:37:24	Expanded View	
2008-01-04 17:35:55	Sync status	0 current connections			
2008-01-04 17:36:14	Sync	10.14.24.16 (ps.companycrypt.com) - Incoming connection			
2008-01-04 17:36:15	Sync status	1 current connections			
2008-01-04 17:36:19	Sync	10.14.24.16 Handshake OK			
2008-01-04 17:36:19	Sync	10.14.24.16 Password OK			
2008-01-04 17:36:23	Sync	10.14.24.16 Requests sync checksum			
2008-01-04 17:36:30	Sync	10.14.24.16 Closed session (Sync OK)			
2008-01-04 17:36:30	Sync	10.14.24.16 Connection closed by remote host			
2008-01-04 17:36:30	Sync status	0 current connections			
2008-01-04 17:36:52	Sync	10.14.24.16 (ps.companycrypt.com) - Incoming connection			
2008-01-04 17:36:53	Sync status	1 current connections			
2008-01-04 17:36:57	Sync	10.14.24.16 Handshake OK			
2008-01-04 17:36:58	Sync	10.14.24.16 Password OK			
2008-01-04 17:37:02	Sync	10.14.24.16 Requests sync checksum			
2008-01-04 17:37:10	Sync	10.14.24.16 Closed session (Sync OK)			
2008-01-04 17:37:10	Sync	10.14.24.16 Connection closed by remote host			
2008-01-04 17:37:10	Sync status	0 current connections			

<< Prev

OP-Log_2008-01-04.txt

Show Today

Size: 827.793 kB

Next >>

Unter dem Anzeigefenster für das Logfile befinden sich Navigationsbutton, welche das Wechseln zwischen den früheren und späteren Logdateien erlauben.

3.8. Key-Management

3.8.1. Hinterlegen der Unternehmensdaten

Maildomänen und Systemadressen

WebGUI → (Key Management) Central Accounts → Company ID → Company SMTP Domain(s)

Hier hinterlegen Sie Ihre Maildomänen und Mailadressen für das System. Diese Mailadressen können in der CompanyCRYPT-Konfiguration für den Versand von Statusinformationen und Userbenachrichtigungen gewählt werden.

Company SMTP Domain(s)	
Primary SMTP domain:	<input type="text" value="@company.com"/>
Additional domains:	<input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/>
System Notifications:	FROM: <input type="text" value="CompanyCRYPT@company.com"/> TO: <input type="text" value="admin@company.com"/> <input style="width: 100%;" type="text"/>
User Notifications:	FROM: <input type="text" value="CompanyCRYPT@company.com"/>

Primary SMTP domain: @<Internetdomäne>

Additional domains: (Optional) @<Alias-/Internetdomänen>

System Notifications: CompanyCRYPT-Systeminformationen für die Administration

From: <Absender-Mailadresse>

To: <Empfänger-Mailadresse> (Optional kann eine zweite Adresse angegeben werden.)

User Notifications: Informationen an den User

From: <Absender-Mailadresse>

Standardwerte für die Schlüsselerzeugung

WebGUI → (Key Management) Central Accounts → Company ID → Key Defaults

Diese Daten werden zur automatischen Schlüsselerstellung genutzt und bei der manuellen Schlüsselerzeugung vorgeblendet.

Key Defaults	
Company Name:	<input type="text" value="Company"/>
Department:	<input style="width: 100%;" type="text"/>
Location:	<input style="width: 100%;" type="text"/>
Country code:	<input style="width: 50px;" type="text" value="DE"/> (2 Letter)
Keylength:	<input style="width: 50px;" type="text" value="2048"/> <input type="button" value="Bit"/>
S/MIME valid for:	<input style="width: 50px;" type="text" value="730"/> Days
PGP valid for:	<input style="width: 50px;" type="text" value="0"/> Days (0 = unlimited)

Company Name: <Firmenname/-bezeichnung>

Department: (Optional) <Abteilung / Organisationseinheit>

Location: (Optional) <Stadt / Ort>

Country code: 2-stellige Buchstabenkombination (DE für Deutschland)

Keylength: 2048 (Diese Schlüssellänge bietet auch für die Zukunft ausreichende Sicherheit. Längere Schlüssellängen sind aus Gründen der Kompatibilität derzeit nicht empfohlen.)

S/MIME valid for: 730 (Dieser Wert entspricht einer Gültigkeit von 2 Jahren)



PGP valid for: 0 (Dieser Wert entspricht einer unbegrenzten Gültigkeitsdauer.)

Meldung Signatur/Entschlüsselungsergebnis (Decrypt Summary)

WebGUI → (Key Management) Central Accounts → Company ID → Decrypt Summary

Hier definieren Sie die Meldung, welche den internen Anwender über die Entschlüsselung und Signaturprüfung einer eMail informiert.

Summary language: Aktiviert bzw. Deaktiviert das Einfügen einer Entschlüsselungs-Zusammenfassung in eingehende, entschlüsselte eMails (Wird am Anfang des Bodytext eingefügt.). Mögliche Einstellungen sind English, German, French, Italian und Polish.

HTML Style: Auswahl der verwendeten HTML-Formatierungen

Style	Beschreibung
CSS based	Darstellung basiert auf CSS-Definitionen mit grafischen Elementen
CSS with line wrap	wie CSS based jedoch mit festgelegten Zeilenumbrüchen
Simple HTML	Darstellung ohne grafische Elemente (Empfohlen bei Verwendung von Lotus Notes)

HTML Font Size: Auswahl der Schriftgröße. Mögliche Einstellungen: Small, Medium, Large

Summary title: Überschrift für die Decrypt Summary

Create X-Header entry: Die Entschlüsselungsinformation wird als X-Header „X-CC-Status“ im Header der Mail eingefügt. Diese Information dient zum automatisierten Auslesen durch Client-Agents.

S/MIME Verify protocol:

For Attachments: Für Dokumentsignaturen wird ein Protokoll mit Details zur Signaturprüfung im HTML-Format angefügt.

For Messages: Für Emailsignaturen wird ein Protokoll mit Details zur Signaturprüfung im HTML-Format angefügt.

3.8.2. Unternehmensschlüssel – Central Signing Account (CSA)

WebGUI → (Key Management) Central Accounts → Company ID → Company Keys [CSA]

Der Central Signing Account (CSA) ist der wichtigste Account/Schlüssel in CompanyCRYPT und hat drei Aufgaben zu erfüllen:

- PGP Schlüssel Erzeugung**
Er übernimmt für die PGP-Schlüssel die Aufgabe einer Certification Authority. Allen in CompanyCRYPT verwalteten PGP-Schlüsseln wird das Vertrauen ausgesprochen, indem Sie durch den CSA-Key signiert werden.
- Firmen-Signatur (PGP und S/MIME)**
Durch den CSA können ausgehende eMails im Namen der Firma signiert werden. Daher wird der CSA-Key auch als Unternehmensschlüssel bezeichnet.
- Zusätzliche Verschlüsselung für Revisions-Account (PGP und S/MIME)**
Um gesetzlichen Nachweispflichten nachkommen zu können, fungiert der CSA auch als Revisions-Account. Alle eMails werden zusätzlich für diesen Account verschlüsselt.

CSA-Schlüssel erstellen

WebGUI → (Key Management) Central Accounts → Company ID → Company Keys [CSA]

1. Schritt

Klicken Sie zunächst auf **Manage**.

Company Keys [CSA - Central Signing Account]		
Name:	<input style="width: 90%;" type="text"/>	
Email:	<input style="width: 90%;" type="text"/>	
	PGP	SMIME
Public key	No Access	No Access
Private key:	No Access	No Access
Passphrase:	No Access	No Access
Status:	Not usable	Not usable
<input style="border: 1px solid blue; padding: 2px 10px;" type="button" value="Manage..."/>		

2. Schritt

Um einen CSA-Key zu erstellen, klicken Sie auf den Button **Generate**. Wenn bereits ein CSA-Key vorhanden ist, so wechselt die Beschriftung des Buttons auf **Re-Generate**.

CSA Status	
PGP Key	
Public key in keyring	Not found
Private key in keyring	Not found
Passphrase	No Access
S/MIME Certificate	
Public key file	Not found
Private key file	Not found
Passphrase	No Access
<input style="border: 1px solid blue; padding: 2px 10px;" type="button" value="Back"/> <input style="border: 1px solid blue; padding: 2px 10px;" type="button" value="Generate..."/>	

3. Schritt

Tragen Sie in die Eingabefelder die notwendigen Daten ein. Bitte bedenken Sie, dass die Daten für externe Partner sichtbar sein werden, und sollten deshalb so selbst-erklärend wie möglich gehalten werden (für einen technischen Account).

Central Signing Account (CSA)		
Name: (min. 5 char)	<input style="width: 80%;" type="text" value="Central_Signing_Account"/>	
eMail:	<input style="width: 80%;" type="text" value="Signing.Account@company.com"/>	
Company:	<input style="width: 80%;" type="text" value="Company Name"/>	
Department:	<input style="width: 80%;" type="text"/>	
Location:	<input style="width: 80%;" type="text"/>	
Country code:	<input style="width: 40px;" type="text" value="DE"/> (2 Letter)	<input type="checkbox"/> S/MIME: Write CRL details to certificate
PGP valid for:	<input style="width: 40px;" type="text" value="0"/> Days (0 = unlimited)	<input type="checkbox"/> S/MIME: Usage is limited to email protection
S/MIME valid for:	<input style="width: 40px;" type="text" value="3653"/> Days	
Keylength:	<input style="width: 40px;" type="text" value="2048"/> <input style="width: 20px;" type="text" value="Bit"/> (Note: Keys larger than 2048 Bit may cause compatibility problems.)	

Central Signing Account (CSA)

Name: Angezeigter Name für das Zertifikat.

eMail: Mailadresse

Company: Firmenname

Department: Abteilung

Location: Ort



Country code:	Landeskürzel (2-stellig)
PGP valid for:	Gültigkeitsdauer in Tagen (0 = unbegrenzt gültig)
S/MIME valid for:	Gültigkeitsdauer in Tagen
Keylength:	Schlüssellänge in Bit
SMIME: WriteCRL ...	(Nur für das S/MIME Zertifikat) Falls in den Standardwerten ein Link angegeben wurde unter dem eine Certificate Revokation List (CRL) publiziert wird, wird dies im Schlüssel angezeigt.
SMIME: Usage is limit ...	(Nur für das S/MIME Zertifikat) Die v3 Erweiterungen im Zertifikat werden so angelegt, das eine anderweitige Verwendung (z.B. SSL-Client) nicht möglich ist.

4. Schritt

Wählen Sie nun das Verfahren aus, für welches der CSA-Key erzeugt werden soll. Empfohlen ist die Erzeugung sowohl für PGP als auch für S/MIME. S/MIME ist nur verfügbar, wenn ein gültiges CA-Zertifikat gefunden wurde.

Sollten Sie die Schlüssel für PGP und S/MIME separat erzeugen, achten Sie bitte darauf, dass beide Schlüssel die gleiche eMailadresse besitzen.

CA certificate available - S/MIME key will be centrally signed by CA.

☐ PGP
☐ S/MIME
☒ S/MIME + PGP

5. Schritt

Starten Sie die Schlüsselerzeugung durch anklicken des Buttons **Generate**. Bitte berücksichtigen Sie die ergänzenden Informationen über das Erstellen von Schlüsselmateriale im unteren Bereich der Anzeige.

Das Ergebnis der Schlüsselerzeugung wird anschließend angezeigt.

CSA-Key anzeigen

WebGUI → (Key Management) Central Accounts → Company ID → Company Keys [CSA] → Manage

In dieser Ansicht haben Sie Zugriff auf die Eigenschaften des CSA-Keys für PGP und für S/MIME. Durch anklicken der Schaltfläche **[+]** erhalten Sie eine erweiterte Detailansicht.

In dieser Ansicht haben Sie Zugriff auf den Fingerprint sowie die Gültigkeit der Schlüssel.

PGP Key		PGP key properties (PRIVATE KEY)	
Public key in keyring	Detected	Name	Central_Signing_Account
Private key in keyring	Detected	eMail	Signing.Account@companycrypt.com
Passphrase	OK	Fingerprint	6F53 2071 83DE F040 8277 5E58 5A90 6DE5 8FE7 69E2
		Single PGP key	Sub-Key
		Comment	(S.I.T. Secure Internet Traffic GmbH & Co. KG, DE)
		Algorithm	DH/DSSA ElGamal (encrypt)
		Keylength	1024 Bit 2048 Bit
		Key-ID	5A906DE5 x 8FE769E2 BEF1BE8D x 18CF2672
		Valid from	2008-01-03 2008-01-03
		Valid until	unlimited unlimited
		Trustlevel:	[u] Ultimate -> OK [u] Ultimate -> OK



S/MIME Certificate		S/MIME certificate properties (PRIVATE KEY)	
Public key file	Detected	Name	Central_Signing_Account
Private key file	Detected	eMail	Signing_Account@companycrypt.com
Passphrase	OK	Fingerprint	(md5) 54DB C2BD BD19 8B83 32E4 BD8C E015 9C57 (sha) 493B AD49 C2DB 28EC 736F F26F 7D99 B1B4 0468 13FA
		Key-ID	6711 BDDE BEC5 7003 75ED 3694 B894 FF3D 7824 9920
		Single S/MIME certificate	
		Subject	Central_Signing_Account, S.I.T. Secure Internet Traffic GmbH & Co. KG, DE
		Keylength	2048 Bit (RSA)
		Serial	20
		Usage	Intended: Digital Signature, Key Encipherment, Data Encipherment Intended: Email Protection
		Valid	2008-01-03 -> 2018-01-03
		Trustlevel:	[f] Full -> OK
		Available Issuer/Authority Details	
		Issuer	SIT Mail CA, S.I.T. Secure Internet Traffic GmbH & Co. KG, DE (ca@companycrypt.com)
		Key-ID	D08F FA41 6FAC 9E77 B161 5D62 12F5 C7B0 20DC 0939
		Status:	This is a trusted issuer...

3.8.3. Lokales Stammzertifikat (Onboard CA)

Das CA-Zertifikat benötigen Sie für die Erstellung eigener Anwender-S/MIME-Zertifikate.

Erstellen eines CA-Zertifikates

WebGUI → (Key Management) Central Accounts → Onboard CA

1. Schritt

Definieren Sie zuerst das Passwort unter WebGUI → (Configuration) Formats → PGP → Passphrase.

2. Schritt

Um ein CA-Zertifikat zu erstellen, klicken Sie auf den Button **Generate**.

CA Status	
S/MIME Certificate	
Public key file	Not found
Private key file	Not found
Passphrase	No Access
Generate...	

3. Schritt

Tragen Sie in die Eingabefelder die gewünschten Daten ein. Es ist nicht notwendig, alle Felder auszufüllen. Die Felder **Department** und **Location** können leer bleiben.



CA Certificate	
Name: (min. 5 char)	SIT Mail CA
eMail:	ca@companycrypt.com
Company:	S.I.T. Secure Internet Traffic GmbH & Co. KG
Department:	
Location:	
Country code:	DE (2 Letter)
S/MIME valid for:	3653 Days
Keylength:	2048 Bit (Note: Keys larger than 2048 Bit may cause compatibility problems.)
<input checked="" type="radio"/> S/MIME	
<input type="button" value="Generate"/>	

Beispiel für die Belegung der Felder für das CA-Zertifikat:

Name: <Firmenname>
 eMail: ca@<Internetdomäne>
 Company: <Firmenname/-bezeichnung>
 Department: (Optional) <Abteilung Organisatorische Einheit>
 Location: (Optional) <Ortsname, Region>
 Country code: <2 Buchstaben Ländercode>
 S/MIME valid for: 3653 (Dieser Wert entspricht einer Gültigkeit von 10 Jahren)
 Keylength: 2048 (Diese Schlüssellänge bietet auch für die Zukunft ausreichende Sicherheit. Längere Schlüssellängen sind aus Gründen der Kompatibilität derzeit nicht empfohlen.)

4. Schritt

Starten Sie die Zertifikatserzeugung durch anklicken des Buttons **Generate**. Das Ergebnis der Zertifikatserstellung wird anschließend angezeigt.

Hinweis: Das erstellte Zertifikat wird automatisch dem 'Trusted-CA-Store' hinzugefügt.

Einbinden eines vorhandenen CA-Zertifikates**1. Schritt**

WebGUI → (Key Management) Import

Laden Sie das CA-Zertifikat zunächst in die Import-Area von CompanyCRYPT. Hierzu klicken Sie auf die Schaltfläche **Datei auswählen** und wählen die Zertifikatsdatei (PFX/P12). Anschließend klicken Sie auf die Schaltfläche **Upload File**.

Import Area			
Type	Received	Email / Name	Usable
	2014-09-25 15:08	_CA.pfx	✓
	2014-09-10 07:41	COMODO RSA Organization Validation Secure Server	✓

Total: 2 Files Folder: C:\Program Files (x86)\CompanyCRYPT\Keys\Import

Keine ausgewählt

2. Schritt

Markieren Sie das Zertifikat in der Listenansicht und geben Sie das Passwort ein. Bestätigen Sie mit **Apply**.

Enter passprase to access private key	<input type="password"/>	<input type="button" value="Apply"/>
---------------------------------------	--------------------------	--------------------------------------

3. Schritt

Die Eigenschaften des Zertifikates werden angezeigt. Bestätigen Sie mit **Import CA**.

S/MIME certificate properties (PRIVATE KEY)	
Name	S.I.T. Root CA
eMail	support@companycrypt.com
Fingerprint	(md5) 11B7 FFF2 B74B 333E B19B 4EB8 A18B 3BD7
Received:	2014-09-25 15:08:09
Usability:	For Signing and Decryption and Certificate Validation
Issuer:	Selfsigned

Import CA







By default, the imported key will be removed after import.

☐ Do not Remove

4. Schritt

WebGUI → (Key Management) Central Accounts → Trusted CA Store

Sortieren Sie die Listenansicht im CA Store nach Importdatum indem Sie auf die Spalte **Added** klicken. So werden die zuletzt importierten Zertifikate zuerst angezeigt.

Trusted CA store					
Type	Expires	eMail	Name	Added ▼	
[..any..] ▼		[..any..]	[..any..]	[..any..] ▼	
	2040-10-10	support@companycrypt.com	S.I.T. Root CA	2014-09-25	 
	2018-08-07		Bayerische VPki Class3 Issuing CA-2012	2014-02-17	 

5. Schritt

Unter den **S/MIME certificate properties** markieren Sie den Inhalt des Feldes **Keystore ID** und kopieren den Inhalt in die Zwischenablage.

S/MIME certificate properties (PRIVATE KEY)	
Name	S.I.T. Root CA
eMail	support@companycrypt.com
Fingerprint	(md5) 11B7 FFF2 B74B 333E B19B 4EB8 A18B 3BD7 (sha) 9158 38D9 232F 1E8F EDD7 4077 7B80 F0FF E7AF D0C5
Keystore ID	c222841e-47ad-cf1c-c5a9-4ab92297

6. Schritt

...\Programme\CompanyCRYPT\CompanyCRYPT.CFG

Öffnen Sie die Konfigurationsdatei **CompanyCRYPT.CFG** im Editor und suchen Sie den Abschnitt **[CA-Cert]**. Hier ersetzen Sie den Wert des Schlüssels **CA-SMIME-UUID** mit der **Keystore ID** aus der Zwischenablage. Speichern Sie die Änderung.

```

companycrypt.cfg - Editor
Datei Bearbeiten Format Ansicht ?

[CA-Cert]
Company = S.I.T. Secure Internet Traffic GmbH&Co.KG
Location = Hannover
Department = IT-Security
Contact = Certification.Authority@CompanyCrypt.com
Country = DE
Keylength = 2048
Validity = 3650
Date = 2005-08-04
CA-SMIME-UUID = c222841e-47ad-cf1c-c5a9-4ab92297
    
```

Anzeigen des CA-Zertifikates

WebGUI → (Key Management) Central Accounts → Onboard CA

Hier können Sie sich die Eigenschaften des CA-Zertifikates anzeigen lassen. Über die Schaltfläche **[+]** erhalten Sie eine erweiterte Detailansicht.

In dieser Ansicht haben Sie Zugriff auf den Fingerprint sowie die Gültigkeit des Zertifikates.



S/MIME Certificate		CA certificate properties (PRIVATE KEY)	
Public key file	Detected	Name	SIT Mail CA
Private key file	Detected	eMail	ca@companycrypt.com
Passphrase	OK	Fingerprint	(md5) D291 7372 7A50 FCEE 5873 7C5D 9DE8 D40F (sha) 1455 9C8F 330E 6318 DE18 7EEA 3459 8312 2861 0E5D
		Key-ID	D08F FA41 6FAC 9E77 B161 5D62 12F5 C7B0 20DC 0939
		Single S/MIME certificate	
		Subject	SIT Mail CA, S.I.T. Secure Internet Traffic GmbH & Co. KG, DE
		Keylength	2048 Bit (RSA)
		CA Usage	Restricted: Use as Certification Authority (CA)
			Restricted: Certificate Signing, CRL Signing
		Valid	2008-01-03 -> 2018-01-03
		Trustlevel:	[f] Full -> OK
		Available Issuer/Authority Details	
		Issuer	Selfsigned

Passwort für das CA-Zertifikat

WebGUI → (Configuration) Formats → PGP → Passphrase

Hier wird das Passwort für alle Schlüssel im CompanyCRYPT angegeben. Es gilt für die PGP-Schlüssel, S/MIME-Zertifikate und das CA-Zertifikat. Das Datum der letzten Änderung bzw. wenn noch kein Passwort hinterlegt wurde, wird entsprechend angezeigt. Bei der Ersthinterlegung des Passwortes ist das Feld Current Passphrase nicht verfügbar.

Passphrase Last changed on: 2003-01-01	
Current Passphrase:	<input type="password"/> *
New Passphrase (8-128 char.):	<input type="password"/> ⓘ
Confirm Passphrase:	<input type="password"/> ⓘ
<input type="button" value="Set Passphrase"/>	

Current Passphrase: aktuelles (altes) Passwort

New Passphrase: neues Passwort

Confirm Passphrase: neues Passwort bestätigen

Parameter zur Zertifikatserstellung

WebGUI → (Key Management) Central Accounts → Onboard CA → Generating User Certificates

Generating User Certificate	
Adjustable v3 Extension:	<input type="checkbox"/> Limit certificate usage to email protection (Keyusage = critical)
Certificate Revocation List:	<input type="checkbox"/> Write URL or email contact to certificate
	CRL - Distribution URL: <input type="text"/>
	CRL - eMail contact: <input type="text"/>
CRL expires after:	<input type="text" value="30"/> days
Note: The local CRL is generated and updated automatically. The files are located at: <CompanCRYPT install dir>\smime\CRL.crl (and CRL.pem).	
Important: Please make the files available for download, prior to adding the URL to certificates.	

Adjustable v3 Extensions: Die sogenannten v3-Erweiterungen über die Nutzungsmöglichkeiten des Zertifikats werden als bindend (critical) deklariert. Eine anderweitige Verwendung (z.B. als SSL-Client Zertifikat ist dann nicht mehr zulässig.

Certificate Revocation List (CRL):

Die (lokale) CRL wird automatisch mitgeführt und vom Operational Service täglich aktualisiert. Sie steht als 2 gleichwertige Dateien (CRL.crl und CRL.pem) mit unterschiedlicher Kodierung im Verzeichnis ..\CompanyCRYPT\Smime\ zur Verfügung.





- CRL – Distribution URL:** Die Internet-Adresse unter der Sie die CRL publizieren. Die URL ist vollständig, also inklusive http/https/ftp anzugeben. Beispiel: http://mail.host.com/crl.
Bitte achten Sie auf korrekte Angabe der URL. Die Einrichtung der URL für Sperrlistenabfrage - CRL ist im Installation Guide beschrieben.
- CRL – eMail contact:** Die eMail Adresse unter der externe Partner die CRL anfordern können
- CRL expires after:** Die Gültigkeit einer CRL erlischt automatisch nach diesem Zeitraum (in Tagen).

Hinweis: Die CRL wird nicht automatisch publiziert. Sie muß vielmehr auf einem geeigneten http/Ftp-Server zur Verfügung gestellt werden. Die Einrichtung der URL für Sperrlistenabfrage (CRL) ist im Installation Guide beschrieben. Erst danach macht es Sinn, die URL bei der Erstellung von Zertifikate mit aufzunehmen.

3.8.4. Trusted CA Store


































Im 'Trusted CA Store' werden die Zertifikate von vertrauenswürdigen Ausstellern verwaltet und von dort zur Überprüfung von Signaturen, sowie unbekannter oder neuer Zertifikate herangezogen. Es werden hierbei zwei Typen unterschieden:

-  **Root-CA** Stammzertifikat: Dieses Zertifikat ist selbstsigniert und kennzeichnet das Ende einer Ausstellerkette.
-  **Sub-CA** Zwischenzertifikat: Diese Zertifikate wurden ihrerseits durch einen Aussteller beglaubigt (unterschrieben). Es entstehen dadurch Aussteller-Ketten, die je nach Einstellung (General → PGP, S/MIME and MSW → S/MIME) auch durchgängig zur Bestimmung der Vertrauenswürdigkeit eines Zertifikats herangezogen werden.

Listendarstellung

WebGUI → (Key Management) Central Accounts → Trusted CA Store

Über diesen Bereich haben Sie Zugriff auf die vertrauenswürdigen Ausstellerzertifikate (Trusted CA Store). Die Liste lässt sich nach Spalten sortieren.

Trusted CA store						
Type	Expires	eMail	Name ▲	Added		
[..any..] ▼		[..any..]	[..any..]	[..any..] ▼		
	2016-07-24		14R-CA 1:PN	2012-10-31		
	2014-12-13		a-sign-light-02	2012-04-25		
	2014-11-30		A-Trust-nQual-01	2012-04-25		
	2015-08-17		A-Trust-nQual-03	2012-04-25		
	2014-11-30		A-Trust-Qual-01	2012-04-25		
	2014-12-02		A-Trust-Qual-02	2012-04-25		
	2028-12-31		AAA Certificate Services	2012-04-25		
	2036-02-08		AC RAIZ DNIE	2012-04-25		
	2020-05-30		AddTrust External CA Root	2012-04-25		
	2037-08-12	ance@certification.tn	Agence Nationale de Certification Electronique	2012-04-25		
	2037-08-12	ance@certification.tn	Agence Nationale de Certification Electronique	2012-04-25		
Total: 378 Keys			Page 1 of 4		Keys per Page: 10 25 [100]	

- Type Zertifikatstyp: Issuer, Wurzelzertifikat (Root-CA), Zwischenzertifikat (Sub-CA).
- Expires Gültigkeit / Ablaufdatum des Zertifikats (abgelaufene Zertifikate werden grau dargestellt)
- eMail Im Zertifikat hinterlegte Emailadresse.
- Name Im Zertifikat hinterlegter Name (CN).
- Added Datum, an dem das Zertifikat dem Speicher hinzugefügt wurde.

Zertifikatseigenschaften

WebGUI → (Key Management) Central Accounts → Trusted CA Stores → S/MIME certificate properties

Unter dem Listenbereich werden die Eigenschaften und Details des gewählten Zertifikats angezeigt.



S/MIME certificate properties	
Name	14R-CA 1:PN
eMail	[... not provided ...]
Fingerprint	(md5) B7FC 1F98 6D80 E7AA 92E2 A098 0758 C078 (sha) B4AA 2AC9 DCC7 4CDC 141E E68E D95B BF2B 151C 3996
Keystore ID	14c36b8d-4afe-2f80-9c6f-e8a06ef6
Single S/MIME certificate	
Subject	14R-CA 1:PN, Bundesnetzagentur, DE
Keylength	2048 Bit (RSA)
Key-ID	FDF3 5084 308E EC23 9AF5 33B2 E381 07DD E4EF 80AE
Serial	322
CA Usage	Restricted: Use as Certification Authority (CA)
	Restricted: Certificate Signing
OCSP link	http://ocsp.nrca-ds.de:8080/ocsp-ocspreponder
Valid	2011-07-25 -> 2016-07-24
Trustlevel:	[f] Full -> OK
Available Issuer/Authority Details	
Issuer	Selfsigned

3.8.5. Verwaltung privater Schlüssel

WebGUI → (Key Management) Internal

Über diesen Bereich haben Sie Zugriff auf die Schlüssel der internen User (Private Keys). Zu den Managementfunktionen gehören das Erstellen neuer Schlüssel, Signieren von Schlüsseln, das Löschen von Schlüsseln und das Anzeigen der Schlüsseldetails.

Listendarstellung

WebGUI → (Key Management) Internal → Internal Key Store

Über diesen Bereich haben Sie Zugriff auf alle in CompanyCRYPT verwalteten Private Keys. Die Liste lässt sich nach Spalten sortieren.

Internal Key Store						
Type	Expires	eMail ▲	Name	Added		
[..any..] ▼		[..any..]	[..any..]	[..any..] ▼		
	2016-09-09	A1.Name@companycrypt.com	A1.Name	2014-09-10		
	2016-09-09	A2.Name@companycrypt.com	A2 Name	2014-09-10		
	2020-04-19	A3.Name@CompanyCRYPT.com	A3 Name	2014-09-10		
	2016-04-27	Achim.Mueller@CompanyCRYP...	Achim Mueller	2014-04-28		
	unlimited	Adam.Sandler@CompanyCRYP...	Adam Sandler	2014-02-14		
	2016-04-27	Agnes.Kraus@CompanyCRYPT...	Agnes Kraus	2014-04-28		
	2016-04-13	Alec.Baldwin@CompanyCRYPT...	Alec Baldwin	2014-04-14		
	unlimited	Anja.Kling@CompanyCRYPT.co...	Anja Kling	2014-04-17		
	2016-05-22	Anthony.Hopkins@CompanyCR...	Anthony Hopkins	2014-05-23		
	2016-09-03	anton.tiroler@CompanyCRYPT...	Anton Tiroler	2014-09-04		
	unlimited	Armin.Mueller.Stahl@Company...	Armin Müller Stahl	2014-04-28		
Total: 60 Keys		Page 1 of 1		Keys per Page: 10 25 [100]		

Spalten der Listenansicht

Type:	Format des Keys (PGP oder S/MIME)
Expires:	Gültigkeitsdatum des Schlüssels, Bei Keys ohne Ablaufdatum wird unlimited angezeigt. Abgelaufene Schlüssel werden durch ein Ausrufungszeichen markiert
eMail:	eMailadresse des Keys, Die Adresse wird gekürzt dargestellt, sofern die Spaltenbreite überschritten wird.



Name:	Name bzw. Bezeichnung des Schlüssels, Der Name wird gekürzt dargestellt, sofern die Spaltenbreite überschritten wird.
Added	Datum, an dem das Zertifikat dem Speicher hinzugefügt wurde.
Symbol Details:	Durch klicken auf dieses Symbol werden die Keydetails angezeigt.
Symbol Löschen:	Durch klicken auf das Symbol (Papierkorb) wird der Schlüssel gelöscht

Schlüsseleigenschaften – Private PGP Key

WebGUI → (Key Management) Internal → PGP key properties

Unter der Listenansicht werden die primären Eigenschaften des gewählten Schlüssels angezeigt. Durch anklicken der Schaltfläche [+] wird eine erweiterte Ansicht mit allen Details des Schlüssels dargestellt.

PGP key properties (PRIVATE KEY) +	
Name	A3 Name
eMail	A3.Name@CompanyCRYPT.com
Fingerprint	0D84 BF5F 56BA 3766 D70F FDF9 197C 5257 FA2E F880
Status:	Usable

Primäre Schlüsseleigenschaften (PGP):

Name:	Name bzw. Bezeichnung des Keys
eMail:	eMailadresse des Keys
Fingerprint:	eindeutiger Fingerabdruck des Keys (Berechnet durch MD5 Algorithmus)
Status:	Anzeige, ob der Key verwendbar ist, mögliche Anzeige: OK-usable, Not usable (weitere Informationen enthält die erweiterte Ansicht)

PGP key properties (PRIVATE KEY) -																	
Name	A3 Name																
eMail	A3.Name@CompanyCRYPT.com																
Encrypt Alias																	
Fingerprint	0D84 BF5F 56BA 3766 D70F FDF9 197C 5257 FA2E F880																
Keystore ID	376270c1-6f36-ab3e-7f13-feec8537																
	<table border="1"> <thead> <tr> <th>Single PGP key</th> <th>Sub-Key</th> </tr> </thead> <tbody> <tr> <td>Comment</td> <td>S.I.T. Secure Internet Traffic GmbH, Hannover, DE</td> </tr> <tr> <td>Algorithm</td> <td>RSA</td> </tr> <tr> <td>Keylength</td> <td>4096 Bit</td> </tr> <tr> <td>Key-ID</td> <td>197C5257 x FA2EF880</td> </tr> <tr> <td>Valid from</td> <td>2014-09-10</td> </tr> <tr> <td>Valid until</td> <td>2020-04-19</td> </tr> <tr> <td>Trustlevel:</td> <td>[u] Ultimate -> OK</td> </tr> </tbody> </table>	Single PGP key	Sub-Key	Comment	S.I.T. Secure Internet Traffic GmbH, Hannover, DE	Algorithm	RSA	Keylength	4096 Bit	Key-ID	197C5257 x FA2EF880	Valid from	2014-09-10	Valid until	2020-04-19	Trustlevel:	[u] Ultimate -> OK
Single PGP key	Sub-Key																
Comment	S.I.T. Secure Internet Traffic GmbH, Hannover, DE																
Algorithm	RSA																
Keylength	4096 Bit																
Key-ID	197C5257 x FA2EF880																
Valid from	2014-09-10																
Valid until	2020-04-19																
Trustlevel:	[u] Ultimate -> OK																

Erweiterte Schlüsseleigenschaften (PGP):

Keystore ID:	Eindeutiger Identifier des Schlüssels im Keystore
Single PGP key:	Daten des Key
Sub-Key:	Daten des Subkeys für Verschlüsselung
Comment:	Kann Angaben zu Firma, Abteilung, Ort, Land enthalten
Algorithm:	verwendeter Algorithmus
Keylength:	Schlüssellänge
KEY-ID:	eindeutige Schlüssel-ID
Valid from:	erster Tag der Gültigkeit (Ausstellungsdatum)
Valid until:	letzter Tag der Gültigkeit (Ablaufdatum)
Trustlevel:	Vertrauensstufe, zeigt die Verwendbarkeit des Schlüssels an



Schlüsseigenschaften – Private S/MIME Certificate

WebGUI → (Key Management) Internal → S/MIME certificate properties

Unter der Listenansicht werden die primären Eigenschaften des gewählten Zertifikates angezeigt. Durch anklicken der Schaltfläche [+] wird eine erweiterte Ansicht mit allen Details des Schlüssels angezeigt.

S/MIME certificate properties (PRIVATE KEY) [+]	
Name	Achim Mueller
eMail	Achim.Mueller@CompanyCRYPT.com
Fingerprint	(md5) AE2A 6E46 06CF 0171 CADC A616 BB5F 6215
Status:	Usable

Primäre Schlüsseigenschaften (S/MIME):

Name: Name bzw. Bezeichnung des Keys

eMail: eMailadresse des Keys

Fingerprint: eindeutiger Fingerabdruck des Keys (Berechnet durch MD5 und SHA Algorithmus)

Status: Anzeige, ob der Key verwendbar ist, mögliche Anzeige: OK-usable, Not usable (weitere Informationen enthält die erweiterte Ansicht)

S/MIME certificate properties (PRIVATE KEY) [-]	
Name	Achim Mueller
eMail	Achim.Mueller@CompanyCRYPT.com
Encrypt Alias	
Fingerprint	(md5) AE2A 6E46 06CF 0171 CADC A616 BB5F 6215 (sha) 0DB7 9006 7B85 B3AF EABA 4CB5 117A 9672 A4F7 360F
Keystore ID	6b821216-a761-ffe3-6f66-e6b1d07f
Single S/MIME certificate	
Subject	Achim Mueller, S.I.T. Secure Internet Traffic GmbH, Hannover, DE
Keylength	2048 Bit (RSA)
Key-ID	51E7 755E 212E F0A4 C12F 8FE5 8F45 1091 14FD 95A7
Serial	200
Usage	Intended: Digital Signature, Key Encipherment, Data Encipherment Intended: Email Protection
Valid	2014-04-28 -> 2016-04-27
Trustlevel:	[f] Full -> OK
Available Issuer/Authority Details	
Issuer	CompanyCRYPT_Certification_Authority, S.I.T. Secure Internet Traffic GmbH&Co.KG, IT-Security, Hannover, DE (Certification.Authority@CompanyCrypt.com)
Key-ID	5F65 CAC9 FF5E 1B66 2903 DB72 6B09 810D AA35 E187
Status:	This is a trusted issuer... [x]

Erweiterte Schlüsseigenschaften (S/MIME):

Keystore ID: Eindeutiger Identifier des Schlüssels im Keystore

Single S/MIME certificate: Daten des Keys

Subject: Zusätzliche Angaben des Eigentümers des Zertifikats:
Firma, Abteilung, Land/Region, Ländercode

Keylength: Schlüssellänge und verwendeter Algorithmus in Klammern

Key-ID: Eindeutige Identifizierungsnummer des Zertifikats (soweit in den v3-Erweiterungen verfügbar)

Comment: (Falls durch Aussteller gesetzt) Kommentar

Serial: Seriennummer des Keys

Usage: Angaben zur Verwendung des Zertifikats (soweit in den v3-Erweiterungen verfügbar)

Valid: Zeitraum der Gültigkeit (Ausstellungsdatum → Ablaufdatum)

Trustlevel: Vertrauensstufe, zeigt die Verwendbarkeit des Schlüssels an

Available Issuer/Authority Details: Nähere Angaben zum Zertifikatsaussteller



Issuer:	Angaben zu Name, Firma, Abteilung, Ort/Region, Ländercode und eMail-Adresse des Ausstellers
Key-ID:	Eindeutige Identifizierungsnummer des <u>beglaubigenden</u> Zertifikats (soweit in den v3-Erweiterungen verfügbar)
Status:	Wenn das (oder die) ausstellende(n) Zertifikat(e) im 'Trusted CA Store' vorliegen und positiv überprüfbar sind, wird der Status in grüner Schrift angezeigt. Per Klick kann dann die ausstellende CA angezeigt werden.

Schlüssel per Mail versenden

WebGUI → (Key Management) Internal → Send public key to eMail address

Für alle internen Schlüssel besteht die Möglichkeit, den jeweiligen Public Key per Mail zu versenden. Hierzu muss lediglich die gewünschte eMailadresse des Empfängers im angegebenen Feld eingetragen werden und per Send-Button wird dann eine eMail mit dem gewählten Public Key verschickt.

Erstellen privater Schlüssel

WebGUI → (Key Management) Internal → New key

Klicken Sie im Bereich der Internen Schlüsselverwaltung auf den Button **New Key**. Unter diesem Punkt haben Sie die Möglichkeit manuell neue Schlüssel zu erstellen.

1. Schritt

Tragen Sie gewünschten Daten in die Felder ein. Die vorgeblendeten Default key parameters können bei Bedarf überschrieben werden.

Internal User Keypair

Name:	Name, Inhaber bzw. Bezeichnung des Keys
eMail:	Mailadresse
Company:	Firmenname
Department:	Abteilung
Location:	Ort
Country code:	Landeskürzel (2-stellig)
Default PGP valid for:	Gültigkeitsdauer des PGP-Keys in Tagen (0 = ohne Ablaufdatum)
S/MIME valid for:	Gültigkeitsdauer des S/MIME-Zertifikates in Tagen
Keylength:	Schlüssellänge in Bit
SMIME: WriteCRL ...	(Nur für das S/MIME Zertifikat) Falls in den Standartwerten ein Link angegeben wurde unter dem eine Certificate Revokation List (CRL) publiziert wird, wird dies im Schlüssel angezeigt.
SMIME: Usage is limit ...	(Nur für das S/MIME Zertifikat) Die v3 Erweiterungen im Zertifikat werden so angelegt, das eine anderweitige Verwendung (z.B. SSL-Client) nicht möglich ist.

2. Schritt

Wählen Sie nun das Verfahren aus, für welches der Key erzeugt werden soll. PGP ist nur verfügbar, wenn ein gültiger CSA-Key vorhanden ist. S/MIME ist nur verfügbar, wenn ein gültiges CA-Zertifikat gefunden wurde.

CSA key available - PGP key will be centrally signed by CSA.	<input checked="" type="radio"/> PGP <input type="radio"/> S/MIME <input type="radio"/> S/MIME + PGP
CA certificate available - S/MIME key will be centrally signed by CA.	

3. Schritt

Starten Sie die Schlüsselerzeugung durch anklicken des Buttons **Generate**.

4. Schritt

Das Ergebnis der Zertifikatserstellung wird anschließend angezeigt.

Keypair generation

PGP key generation SUCCESSFUL

PGP process details - Generating Internal User Keypair

STARTING - Generate PGP Keypair

--> Preparing data

--> Generate key (This may take several minutes)

--> Sign new key with central signing account

--> Export public key .asc file

--> Update listings

--> Public key file stored:

Back







Neu erstellte Schlüssel sind sofort in der Listenansicht der internen Schlüsselverwaltung sichtbar.

Löschen privater Schlüssel

WebGUI → (Key Management) Internal

1. Schritt

Markieren Sie in der Listenansicht den zu löschenden Schlüssel durch klicken auf den Name oder die eMailadresse oder das Detailsymbol. Klicken Sie anschließend auf den Button Delete Key/Certificate. Alternativ können Sie direkt auf das Papierkorbsymbol des zu löschenden Keys klicken.

Internal private keys					
Type	Expires	eMail ▲	Name		
	2010-01-02	Jack.Smith@companycrypt.com	Jack Smith		
	unlimited	Jack.Smith@companycrypt.c...	Jack Smith		

2. Schritt

Die Eigenschaften des zum löschen markierten Keys werden zur Überprüfung angezeigt. Durch nochmaliges klicken auf den Button Delete Key/Certificate bestätigen Sie die Löschung.



PGP key properties (PRIVATE KEY)																	
Name	Jack Smith																
eMail	Jack.Smith@companycrypt.com																
Fingerprint	CD82 AA73 68C7 3EBC 3C35 1EC9 4693 FA2B F369 58C5																
<table border="1"> <tr> <th>Single PGP key</th><th>Sub-Key</th></tr> <tr> <td colspan="2">Comment: (S.I.T. Secure Internet Traffic GmbH & Co. KG, DE)</td></tr> <tr> <td>Algorithm: DH/DSSA</td><td>ElGamal (encrypt)</td></tr> <tr> <td>Keylength: 1024 Bit</td><td>2048 Bit</td></tr> <tr> <td>Key-ID: 4693FA2B x F36958C5</td><td>55F92E78 x 8DF5B205</td></tr> <tr> <td>Valid from: 2008-01-03</td><td>2008-01-03</td></tr> <tr> <td>Valid until: unlimited</td><td>unlimited</td></tr> <tr> <td>Trustlevel: [u] Ultimate -> OK</td><td>[u] Ultimate -> OK</td></tr> </table>		Single PGP key	Sub-Key	Comment: (S.I.T. Secure Internet Traffic GmbH & Co. KG, DE)		Algorithm: DH/DSSA	ElGamal (encrypt)	Keylength: 1024 Bit	2048 Bit	Key-ID: 4693FA2B x F36958C5	55F92E78 x 8DF5B205	Valid from: 2008-01-03	2008-01-03	Valid until: unlimited	unlimited	Trustlevel: [u] Ultimate -> OK	[u] Ultimate -> OK
Single PGP key	Sub-Key																
Comment: (S.I.T. Secure Internet Traffic GmbH & Co. KG, DE)																	
Algorithm: DH/DSSA	ElGamal (encrypt)																
Keylength: 1024 Bit	2048 Bit																
Key-ID: 4693FA2B x F36958C5	55F92E78 x 8DF5B205																
Valid from: 2008-01-03	2008-01-03																
Valid until: unlimited	unlimited																
Trustlevel: [u] Ultimate -> OK	[u] Ultimate -> OK																

Gelöschte Keys sind unwiderruflich gelöscht. Es besteht keine Möglichkeit der Wiederherstellung!

Hinweis: Das Löschen eines Private Keys bedeutet immer das Löschen des Schlüsselpaares – Private Key und zugehöriger public Key!

Signieren privater PGP-Schlüssel

WebGUI → (Key Management) Internal

Unter Umständen bzw. im Fehlerfall kann es notwendig sein, Schlüssel manuell zu signieren bzw. nachzusignieren. Durch das Signieren wird dem jeweiligen Schlüssel das Vertrauen ausgesprochen. Das Signieren im Sinne der Vertrauensstellung ist nur für PGP-Keys verfügbar.

1. Schritt

Markieren Sie in der Listenansicht den zu signierenden PGP-Schlüssel durch klicken auf den Name oder die eMailadresse oder das Detailsymbol. Klicken Sie anschließend auf den Button **Sign Key**.

Internal private keys					
Type	Expires	eMail ▲	Name		
	2010-01-02	Jack.Smith@companycrypt.com	Jack Smith		
	unlimited	Jack.Smith@companycrypt.c...	Jack Smith		

2. Schritt

Anschließend wird Ihnen das Ergebnis des Signierungsvorganges angezeigt.

3.8.6. Verwaltung öffentlicher (externer) Schlüssel

WebGUI → (Key Management) External

Über diesen Bereich haben Sie Zugriff auf die öffentlichen Schlüssel der externen Kontakte (Public Keys). Zu den Managementfunktionen gehören das Signieren von Schlüsseln, das Löschen von Schlüsseln und das Anzeigen der Schlüsseldetails.

Listendarstellung

WebGUI → (Key Management) External → External Key Store

In einer Listenansicht werden alle in CompanyCRYPT verwalteten externen Public Keys angezeigt. Die Liste lässt sich nach Spalten sortieren.



External Key Store						
Type	Expires	eMail	Name	Added		
[..any..]		[..any..]	[..any..]	[..any..]		
	2014-12-19	achim.grosser@intellicomp.de	Secure Mail: SEPPmail Certificate	2014-02-06		
	unlimited	administrator@bafin.de	administrator	2012-04-25		
	unlimited	administrator@bafin.de	BaFin Secure Mail PGP Root	2012-04-25		
	unlimited	administrator@forestris.de	Administrator Forestris	2013-12-04		
	2024-04-27	administrator@klinikum-kempen...	Encryption Gateway Klinikverbund Kempen-Obe...	2014-05-05		
	unlimited	AHG-CSA@ahg.de	AHG AG - Security CSA SYSTEM	2013-05-08		
	unlimited	AlexanderStrobel@gmx.de	Alexander Strobel	2012-04-25		
	2015-04-01	alyn.hockey@clearswift.com	alyn.hockey@clearswift.com	2014-08-29		
	unlimited	andrea.foret@m-net.de	Foret.Andrea	2012-04-25		
	2013-03-25	andreas.wuebben@kampmann...	Andreas Wuebben	2012-04-25		
	unlimited	andreas.wuebben@kampmann...	Andreas Wuebben	2012-04-25		
Total: 302 Keys		Page 1 of 4		Keys per Page: 10 25 [100]		

Spalten der Listenansicht

Type:	Format des Keys (PGP oder S/MIME)
Expires:	Gültigkeitsdatum des Schlüssels, Bei Keys ohne Ablaufdatum wird unlimited angezeigt. Abgelaufene Schlüssel werden durch ein Ausrufungszeichen markiert
eMail:	eMailadresse des Keys, Die Adresse wird gekürzt dargestellt, sofern die Spaltenbreite überschritten wird.
Name:	Name bzw. Bezeichnung des Schlüssels, Der Name wird gekürzt dargestellt, sofern die Spaltenbreite überschritten wird.
Added	Datum, an dem das Zertifikat dem Speicher hinzugefügt wurde.
Symbol Details:	Durch klicken auf dieses Symbol werden die Keydetails angezeigt.
Symbol Löschen:	Durch klicken auf das Symbol (Papierkorb) wird der Schlüssel gelöscht

Schlüsseleigenschaften – Public PGP Key

WebGUI → (Key Management) External → PGP key properties

Unter der Listenansicht werden die primären Eigenschaften des gewählten Schlüssels angezeigt. Durch anklicken der Schaltfläche [+] wird eine erweiterte Ansicht mit allen Details des Schlüssels dargestellt.

PGP key properties	
Name	Domenik Niemayer
eMail	domenik.niemayer@gmx.de
Fingerprint	2E9D 70A6 740A AE72 0C5F 1F5F F7AB 22B9 D5F3 3047
Status:	Usable

Primäre Schlüsseleigenschaften (PGP):

Name:	Name bzw. Bezeichnung des Keys
eMail:	eMailadresse des Keys
Fingerprint:	eindeutiger Fingerabdruck des Keys
Status:	Anzeige, ob der Key verwendbar ist, mögliche Anzeige: OK-usable, Not usable (weitere Informationen enthält die erweiterte Ansicht)



PGP key properties															
Name	Domenik Niemayer														
eMail	domenik.niemayer@gmx.de														
Encrypt Alias															
Fingerprint	2E9D 70A6 740A AE72 0C5F 1F5F F7AB 22B9 D5F3 3047														
Keystore ID	85296a14-e6ad-ae59-7cae-04dd6bfd														
	<table border="1"> <thead> <tr> <th>Single PGP key</th> <th>Sub-Key</th> </tr> </thead> <tbody> <tr> <td>Algorithm</td> <td>ElGamal (encrypt)</td> </tr> <tr> <td>Keylength</td> <td>2048 Bit</td> </tr> <tr> <td>Key-ID</td> <td>747A10EA x 11DE9B24</td> </tr> <tr> <td>Valid from</td> <td>2005-02-23</td> </tr> <tr> <td>Valid until</td> <td>unlimited</td> </tr> <tr> <td>Trustlevel:</td> <td>[f] Full -> OK</td> </tr> </tbody> </table>	Single PGP key	Sub-Key	Algorithm	ElGamal (encrypt)	Keylength	2048 Bit	Key-ID	747A10EA x 11DE9B24	Valid from	2005-02-23	Valid until	unlimited	Trustlevel:	[f] Full -> OK
Single PGP key	Sub-Key														
Algorithm	ElGamal (encrypt)														
Keylength	2048 Bit														
Key-ID	747A10EA x 11DE9B24														
Valid from	2005-02-23														
Valid until	unlimited														
Trustlevel:	[f] Full -> OK														

Erweiterte Schlüsseigenschaften (PGP):

Encrypt Alias:	Weitere Emailadressen, die dem Key zugeordnet sind.
Keystore ID:	Eindeutiger Identifier des Schlüssels im Keystore
Single PGP key:	Daten des Key
Sub-Key:	Daten des Subkeys für Verschlüsselung
Comment:	Kann Angaben zu Firma, Abteilung, Ort, Land enthalten
Algorithm:	verwendeter Algorithmus
Keylength:	Schlüssellänge
KEY-ID:	eindeutige Schlüssel-ID
Valid from:	erster Tag der Gültigkeit (Ausstellungsdatum)
Valid until:	letzter Tag der Gültigkeit (Ablaufdatum)
Trustlevel:	Vertrauensstufe, zeigt die Verwendbarkeit des Schlüssels an

Schlüsseigenschaften – Public S/MIME Certificate

WebGUI → (Key Management) External → S/MIME key properties

Unter der Listenansicht werden die primären Eigenschaften des gewählten Schlüssels angezeigt. Durch anklicken der Schaltfläche [+] wird eine erweiterte Ansicht mit allen Details des Schlüssels dargestellt.

S/MIME certificate properties	
Name	Faruk Unlu
eMail	faruk.unlu@comodo.com
Fingerprint	(md5) A733 E486 BFCE 8D88 5CB6 8D0D BB75 94FF
Status:	Usable

Primäre Schlüsseigenschaften (S/MIME):

Name:	Name bzw. Bezeichnung des Keys
eMail:	eMailadresse des Keys
Fingerprint:	eindeutiger Fingerabdruck des Keys nach MD5
Status:	Anzeige, ob der Key verwendbar ist, mögliche Anzeige: OK-usable, OK-usable [Encryption only], OK-usable [Signatures only], Not usable (weitere Informationen enthält die erweiterte Ansicht)



S/MIME certificate properties	
Name	Faruk Unlu
eMail	faruk.unlu@comodo.com
Encrypt Alias	
Fingerprint	(md5) A733 E486 BFCE 8D88 5CB6 8D0D BB75 94FF (sha) 59D7 1C2D 38F4 C283 18B0 3DC1 667D 4437 5022 C1F2
Keystore ID	28f65f49-0af2-9c46-ac80-d22c1f46
Single S/MIME certificate	
Subject	Faruk Unlu, Comodo Group Inc., Clifton, NJ, US
Keylength	2048 Bit (RSA)
Key-ID	F3A6 9A7E 9322 4E57 DEB5 D891 29CF 3E48 47E7 FDCB
Serial	FF51 6BF9 C47E A493 567D 6B90 768E 9CB1
Usage	Restricted: Digital Signature, Key Encipherment Intended: Email Protection, SSL/TLS Client
OCSP link	http://ocsp.comodoca.com
Valid	2013-09-04 -> 2016-09-04
Trustlevel:	[f] Full -> OK
Available Issuer/Authority Details	
Issuer	COMODO Client Authentication and Secure Email CA, COMODO CA Limited, Salford, Greater Manchester, GB
Key-ID	7A13 4E00 745B C678 6364 27C1 2FE2 A05B BC79 C57B
Status:	This is a trusted issuer...

Erweiterte Schlüsseleigenschaften (S/MIME):

Encrypt Alias:	Weitere Emailadressen, die dem Zertifikat zugeordnet sind.
Keystore ID:	Eindeutiger Identifier des Schlüssels im Keystore
Fingerprint:	eindeutiger Fingerabdruck des Keys (Berechnet durch SHA Algorithmus)
Single S/MIME certificate:	Daten des Key
Subject	Zusätzliche Angaben des Eigentümers des Zertifikats: Firma, Abteilung, Land/Region, Ländercode
Keylength:	Schlüssellänge und verwendeter Algorithmus in Klammern
Key-ID:	Eindeutige Identifizierungsnummer des Zertifikats (soweit in den v3-Erweiterungen verfügbar)
Comment:	(Falls durch Aussteller gesetzt) Kommentar
Serial:	Seriennummer des Keys
Usage:	Angaben zur Verwendung des Zertifikats (soweit in den v3-Erweiterungen verfügbar)
OCSP link:	(Falls durch Aussteller gesetzt) Link für die Online Zertifikats Validierung
Valid:	Zeitraum der Gültigkeit (Ausstellungsdatum → Ablaufdatum)
Trustlevel:	Vertrauensstufe, zeigt die Verwendbarkeit des Schlüssels an
Available Issuer/Authority Details: Nähere Angaben zum Zertifikatsaussteller	
Issuer:	Angaben zu Name, Firma, Abteilung, Ort/Region, Ländercode und eMail-Adresse des Ausstellers
Key-ID:	Eindeutige Identifizierungsnummer des <u>beglaubigenden</u> Zertifikats (soweit in den v3-Erweiterungen verfügbar)
Status:	Wenn das (oder die) ausstellende(n) Zertifikat(e) im 'Trusted CA Store' vorliegen und positiv überprüfbar sind, wird der Status in grüner Schrift angezeigt.



Löschen öffentlicher Schlüssel

WebGUI → (Key Management) External

1. Schritt

Markieren Sie in der Listenansicht den zu löschenden Schlüssel durch klicken auf den Name oder die eMailadresse oder das Detailsymbol. Klicken Sie anschließend auf den Button **Delete Key/Certificate**. Alternativ können Sie direkt auf das Papierkorbsymbol des zu löschenden Keys klicken.

External Key Store						
Type	Expires	eMail ▲	Name	Added		
[..any..] ▼		[..any..]	[..any..]	[..any..] ▼		
unlimited	unlimited	Crypto.Postmaster@harting.c...	Central_Signing	2012-04-25		
unlimited	unlimited	Crypto.Postmaster@Landkreis.L...	Signatur Server	2012-04-25		
unlimited	unlimited	Crypto.Postmaster@make-it.de	Central_Signing_Account	2012-04-25		

2. Schritt

Die Eigenschaften des zum löschen markierten Keys werden zur Überprüfung angezeigt. Durch nochmaliges klicken auf den Button **Delete Key** bestätigen Sie die Löschung.

PGP key properties																	
Name	Central_Signing																
eMail	Crypto.Postmaster@harting.com																
Encrypt Alias																	
Fingerprint	D4A1 1416 31E2 3EAF 7B6B 62BF 7C87 B778 F66B 7E5F																
Keystore ID	55cd04fc-08bd-2bd3-7525-39c1d982																
	<table border="1"> <thead> <tr> <th>Single PGP key</th> <th>Sub-Key</th> </tr> </thead> <tbody> <tr> <td>Comment</td> <td>HARTING, DE</td> </tr> <tr> <td>Algorithm</td> <td>DH/DSA</td> </tr> <tr> <td>Keylength</td> <td>1024 Bit</td> </tr> <tr> <td>Key-ID</td> <td>7C87B778 x F66B7E5F</td> </tr> <tr> <td>Valid from</td> <td>2007-11-06</td> </tr> <tr> <td>Valid until</td> <td>unlimited</td> </tr> <tr> <td>Trustlevel:</td> <td>[f] Full -> OK</td> </tr> </tbody> </table>	Single PGP key	Sub-Key	Comment	HARTING, DE	Algorithm	DH/DSA	Keylength	1024 Bit	Key-ID	7C87B778 x F66B7E5F	Valid from	2007-11-06	Valid until	unlimited	Trustlevel:	[f] Full -> OK
Single PGP key	Sub-Key																
Comment	HARTING, DE																
Algorithm	DH/DSA																
Keylength	1024 Bit																
Key-ID	7C87B778 x F66B7E5F																
Valid from	2007-11-06																
Valid until	unlimited																
Trustlevel:	[f] Full -> OK																

Delete Key

Cancel

Gelöschte Keys sind unwiderruflich gelöscht. Es besteht keine Möglichkeit der Wiederherstellung!

Signieren öffentlicher PGP-Schlüssel

WebGUI → (Key Management) External

Unter Umständen bzw. im Fehlerfall kann es notwendig sein, Schlüssel manuell zu signieren bzw. nachzusignieren. Durch das Signieren wird dem jeweiligen Schlüssel das Vertrauen ausgesprochen. Das Signieren im Sinne der Vertrauensstellung ist nur für PGP-Keys verfügbar.

1. Schritt

Markieren Sie in der Listenansicht den zu signierenden Schlüssel durch klicken auf den Name oder die eMailadresse oder das Detailsymbol. Klicken Sie anschließend auf den Button **Sign Key**.

External Key Store						
Type	Expires	eMail ▲	Name	Added		
[..any..] ▼		[..any..]	[..any..]	[..any..] ▼		
unlimited	unlimited	administrator@bafin.de	administrator	2012-04-25		
unlimited	unlimited	administrator@bafin.de	BaFin Secure Mail PGP Root	2012-04-25		
unlimited	unlimited	administrator@forestris.de	Administrator Forestris	2013-12-04		

2. Schritt

Anschließend wird Ihnen das Ergebnis des Signierungsvorganges angezeigt.



```

Signing key SUCCESSFUL
STARTING - Signing PGP Key

--> Signing public PGP key with Central encryption account
--> Signing key: Signing.Account@companycrypt.com
--> Key to be signed: domenik.niemayer@gmx.de (ID:F7AB22B9D5F33047)
1
--> Key not changed (Already signed with CSA key).

Done.

```

3.8.7. Import von Schlüsselmateriale

Import eines privaten PGP Schlüssels

WebGUI → (Key Management) Import → Import Area

Sie können private PGP Schlüssel in CompanyCRYPT importieren. Für den Import wird immer das Schlüsselpaar - bestehend aus private und public Key - benötigt. Die erforderliche Form für den Import ist eine einzelne, ASCII kodierte Datei, welche den privaten und den öffentlichen Schlüssel enthält. Um dies zu überprüfen, können Sie die Datei in einem Text-Editor öffnen. Sie sollten dort folgende Textabschnitte, welche die Schlüsseldaten umschließen, sehen: BEGIN PGP PRIVATE KEY BLOCK, END PGP PRIVATE KEY BLOCK, BEGIN PGP PUBLIC KEY BLOCK and END PGP PUBLIC KEY BLOCK. (Die Sequenz '-----' wurde zur besseren Lesbarkeit weggelassen.)

Hinweis: - Nur ein Schlüsselpaar pro Datei ist zulässig.
- Der Dateiname kann frei gewählt werden.

1. Schritt

Wählen Sie die Import-Datei indem Sie auf den Dateinamen klicken.

Import Area					
Type	Received	Name	Usable		
	2008-01-03 11:31	domenik.niemayer@gmx.de.asc	✓		
	2007-11-18 14:28	i-s-j@web.de.cer	✓		
	2007-11-18 15:56	wk@g10code.com.cer	✓		
	2007-11-09 20:52	Schneider-Jansohn@CompanyCRYPT.com.pfx	✓		
	2007-11-09 19:11	TestFirma_12345678.p12	✓		
	2007-10-16 22:15	CS-Root.cer	✓		
	2007-03-12 12:24	Peter.Lemcke@arcor.de.cer	✓		
	2006-08-23 14:04	PGP_Inline@gmx.de_0x7BB1C109.sec.asc	✓		
Total: 9 Files					
Folder: C:\Programme\CompanyCRYPT\Keys\Import					

2. Schritt

Prüfen Sie die Eigenschaften des Schlüssels. Diese werden unterhalb der Dateiliste angezeigt. Wenn es sich um ein Schlüsselpaar handelt, sollten Sie den Schriftzug (PRIVATE KEY) sehen. Die erweiterten Keydetails erhalten Sie bei Bedarf über den Button [+]. Die Feldbezeichnungen der angezeigten Eigenschaften entsprechen den Key properties im Bereich internen Schlüsselverwaltung.



PGP key properties (PRIVATE KEY)	
Name	PGP_Inline@gmx.de
eMail	PGP_Inline@gmx.de
Fingerprint	B5B1 51F0 5E3E D581 87D5 3856 370B 51C6 7BB1 C109
Received:	2006-08-23 14:04:02
Usability:	For Signing and Decryption

Um Zugriff auf den Schlüssel zu erhalten, muss die Passphrase, welche den Schlüssel ggf. schützt, in das Feld unterhalb der Schlüsseleigenschaften eingegeben werden. Während des Imports wird die Passphrase des Schlüssels automatisch auf die zentrale Passphrase von CompanyCRYPT umgestellt. Die Importdatei selbst bleibt unverändert.

Enter passphrase to import private key
<input type="text"/>

3. Schritt

Klicken Sie auf den Button **Import and Sign Key** um den Importvorgang zu starten.

Import and Sign Key
By default, the imported key will be removed after import.
<input type="checkbox"/> Do not Remove

Do not Remove:

Standardmäßig wird das Keyfile im Importverzeichnis gelöscht, nachdem der Schlüssel erfolgreich importiert wurden. Aktivieren Sie diese Option um das Keyfile nicht zu löschen.

4. Schritt

Anschließend wird das Ergebnis des Schlüsselimports angezeigt.

Process details:
Importing key from file (PGP_Inline@gmx.de_0x7BB1C109.sec.asc)
STARTING - Private PGP Key import
--> Calling GPG.EXE to import new key
--> Change passphrase of private key
--> Signing public PGP key with Central encryption account
--> Signing key: Signing.Account@companycrypt.com
--> Key to be signed: PGP_Inline@gmx.de (ID:370B51C67BB1C109) 1
--> Signing with CSAkey OK.
--> Update listings
--> Public Key stored: with filename: PGP_Inline@gmx.de.asc in folder: C:\Programme\CompanyCRYPT\Keys\Public\PGP-Intern
Import SUCCESSFUL

Import eines privaten S/MIME Zertifikates

WebGUI → (Key Management) Import → Import Area

Sie können private S/MIME Zertifikate in CompanyCRYPT importieren. Für den Import wird immer das Schlüsselpaar - bestehend aus private und public Key - benötigt. Die erforderliche Form für den Import ist eine einzelne, P12 kodierte Datei, welche den privaten und den öffentlichen Schlüssel enthält. Um dies zu überprüfen, können Sie die Datei im MS Datei Explorer öffnen. Dies startet einen Zertifikats-Import-Assistenten. Wenn Sie diesem Dialog ungefähr drei Fenster folgen, können Sie die Passphrase, welche die Datei schützt, überprüfen. Der Vorgang kann ohne Folgen nach Eingabe der Passphrase abgebrochen werden, ohne dass das Zertifikat in Windows importiert wurde

























Hinweis:

- Nur ein Schlüsselpaar pro Datei ist zulässig.
- Der Dateiname kann frei gewählt werden.

Um den Import zu starten, wählen Sie bitte 'Key-Management' → 'Etern' und klicken Sie auf den Button **Import Key**.

1. Schritt

Wählen Sie die Import-Datei indem Sie auf den Dateinamen klicken.

Import Area					
Type	Received	Name	Usable		
	2008-01-03 11:31	domenik.niemayer@gmx.de.asc	✓		
	2007-11-18 14:28	i-s-j@web.de.cer	✓		
	2007-11-16 15:56	wk@g10code.com.cer	✓		
	2007-11-09 20:52	Schneider-Jansohn@CompanyCRYPT.com.ptx	✓		
	2007-11-09 19:11	TestFirma_12345678.p12	✓		
	2007-10-16 22:15	CS-Root.cer	✓		
	2007-09-19 16:08	support@CompanyCRYPT.com.pfx	✓		
	2007-03-12 12:24	Peter.Lemcke@arcor.de.cer	✓		
Total: 9 Files			Folder: C:\Programme\CompanyCRYPT\Keys\Import		

2. Schritt

Die P12-Datei ist möglicherweise durch eine Passphrase geschützt. Um Zugriff auf den Inhalt der Datei zu erhalten geben Sie bitte diese in das unten dargestellte Feld ein und klicken auf den Button **Apply**.

Protected S/MIME Certificate


This appears to be a protected private key.
A passphrase may be required.
 Please enter it in the field below and click on 'Apply'.

Enter passphrase to access private key

3. Schritt

Prüfen Sie die Eigenschaften des Zertifikats. Diese werden unterhalb der Dateiliste angezeigt. Wenn es sich um ein Schlüsselpaar handelt, sollten Sie den Schriftzug (PRIVATE KEY) sehen. Die erweiterten Keydetails erhalten Sie bei Bedarf über den Button [+]. Die Feldbezeichnungen der angezeigten Eigenschaften entsprechen den Key properties im Bereich internen Schlüsselverwaltung.

Während des Imports wird die Passphrase des Schlüssels automatisch auf die zentrale Passphrase von CompanyCRYPT umgestellt. Die Importdatei selbst bleibt unverändert.

S/MIME certificate properties (PRIVATE KEY) +	
Name	CompanyCRYPT Support
eMail	support@companycrypt.com
Fingerprint	(md5) 5498 C8C7 F5F0 5484 65A9 8569 B5A4 6085
Received:	2007-09-19 16:08:29
Usability:	For Signing and Decryption
Issuer:	This is a trusted issuer... 

4. Schritt

Klicken Sie auf den Button **Import Certificate** um den Importvorgang zu starten.

Import Certificate

By default, the imported key will be removed after import.

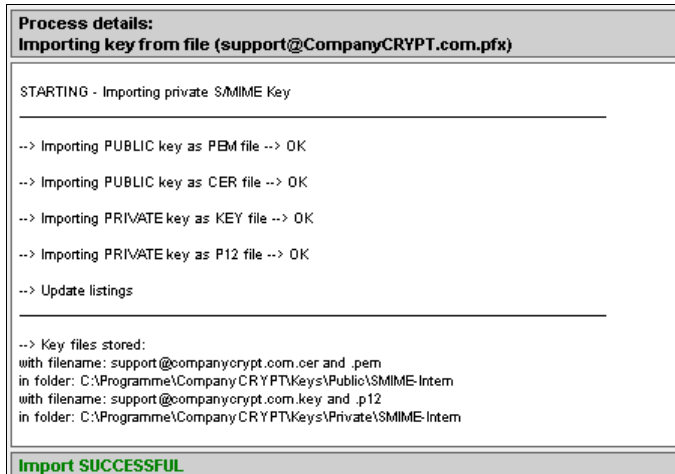
☐ Do not Remove



Do not Remove: Standardmäßig wird des Keyfile im Importverzeichnis gelöscht, nachdem der Schlüssel erfolgreich importiert wurden. Aktivieren Sie diese Option um das Keyfile nicht zu löschen.

5. Schritt

Anschließend wird das Ergebnis des Schlüsselimports angezeigt.



Import eines öffentlichen Schlüssels

WebGUI → (Key Management) Import → Import Area

Sie können neue Public Keys von externen Kontakten manuell in CompanyCRYPT importieren.

1. Schritt

Markieren Sie den zu importierenden Key in der Listenansicht des Importverzeichnisses.

Import Area					
Type	Received	Name	Usable		
	2008-01-03 11:31	domenik.niemayer@gmx.de.asc	✓		
	2007-11-18 14:28	j-s-j@web.de.cer	✓		
	2007-11-16 15:56	wk@g10code.com.cer	✓		
	2007-11-09 20:52	Schneider-Jansohn@CompanyCRYPT.com.pfx	✓		
	2007-11-09 19:11	TestFirma_12345678.p12	✓		
	2007-10-16 22:15	CS-Root.cer	✓		
	2007-03-12 12:24	Peter.Lemcke@arcor.de.cer	✓		
Total: 8 Files			Folder: C:\Programme\CompanyCRYPT\Keys\Import		

2. Schritt

Prüfen Sie die Eigenschaften des gewählten Keys. Diese werden unterhalb der Listenansicht angezeigt. Die erweiterten Keydetails erhalten Sie bei Bedarf über den Button [+]. Die Feldbezeichnungen der angezeigten Eigenschaften entsprechen den Key properties im Bereich externe Schlüsselverwaltung.



PGP key properties	
Name	Domenik Niemayer
eMail	domenik.niemayer@gmx.de
Fingerprint	2E9D 70A6 740A AE72 0C5F 1F5F F7AB 22B9 D5F3 3047
Single PGP key	Sub-Key
Algorithm	DH/DSSA
Keylength	1024 Bit
Key-ID	F7AB22B9 x D5F33047
Valid from	2005-02-23
Valid until	unlimited

3. Schritt

Klicken Sie auf den Button **Import and Sign Key / Import Certificate** um den Importvorgang zu starten.

Import and Sign Key

By default, the imported key will be removed after import.

☐ Do not Remove

Do not Remove:

Standardmäßig wird das Keyfile im Importverzeichnis gelöscht, nachdem der Schlüssel erfolgreich importiert wurden. Aktivieren Sie diese Option um das Keyfile nicht zu löschen.

4. Schritt

Anschließend wird das Ergebnis des Schlüsselimports angezeigt.

Process details:

Importing key from file (domenik.niemayer@gmx.de.asc)

STARTING - Importing public PGP Key

--> Calling GPG.EXE to import key

--> Signing public PGP key with Central encryption account

--> Signing key: Crypto.Postmaster@CompanyCRYPT.com

--> Key to be signed: domenik.niemayer@gmx.de (ID:F7AB22B9D5F33047)

--> Signing with CSA key OK.

--> Copy public key file to key storage directory

--> Update listings

--> Public Key stored:
with filename: domenik.niemayer@gmx.de.asc
in folder: D:\CompanyCRYPT\Keys\Extern\PGP-Extern

Import SUCCESSFUL

Upload von Schlüsselmaterial

WebGUI → (Key Management) Import → Import Area

Wenn ein gewünschter Key noch nicht auf dem Mail-Gateway vorhanden ist, dann können Sie das gewünschte Schlüsselmaterial auch per Upload direkt über die Weboberfläche von CompanyCRYPT importieren.

1. Schritt

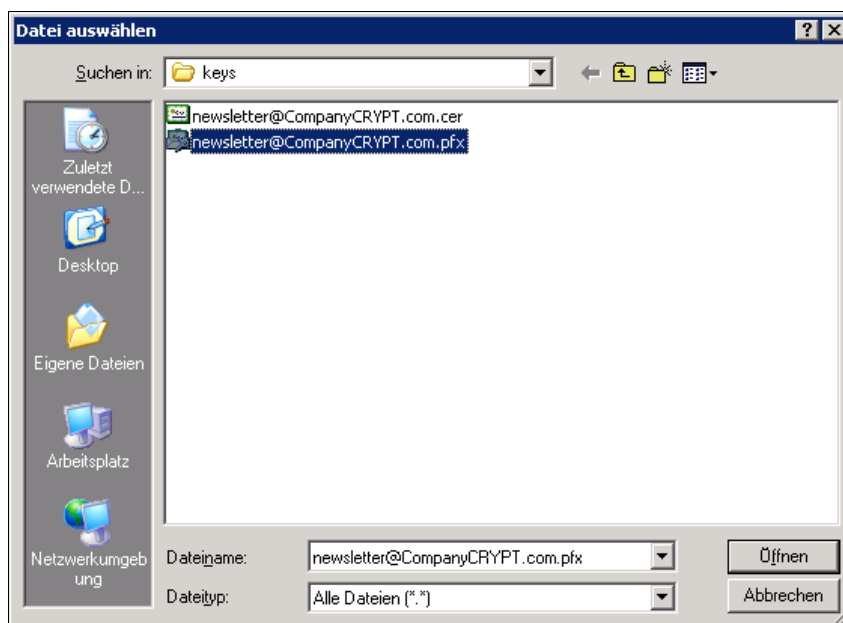
Wählen Sie unter der Listenansicht der Import Area den Button **Durchsuchen**.

Durchsuchen...

Upload File

2. Schritt

Navigieren Sie jetzt zur gewünschten Schlüsseldatei und bestätigen Sie die Auswahl mit **Öffnen**.



3. Schritt

Die markierte Datei wird komplettem Pfad im Auswahlfeld angezeigt. Durch Klick auf den Button **Upload File** starten Sie die Übertragung der Datei zum Server.



Abhängig vom übertragenen Schlüsseltyp sind dann die beschriebenen Schritte für den Import eines privaten oder öffentlichen Schlüssels durchzuführen.

3.8.8. Automatischer Import

WebGUI → (Key Management) Import → Auto-Detect / Auto-Import

Zur Erleichterung der Administration erlaubt CompanyCRYPT den automatisierten Import von Schlüsselmaterial.

Automatische Schlüsselerkennung

WebGUI → (Key Management) Import → Auto-Detect / Auto-Import → Auto-Detect New Keys

CompanyCRYPT erkennt automatisch neue – noch nicht in der Schlüsselverwaltung vorhandene – Schlüssel in eMails und extrahiert diese aus der jeweiligen eMail.

Auto-Detect New (Unknown) Keys	
Extract new keys:	<input checked="" type="radio"/> All Decrypt Jobs <input type="radio"/> Only MIKE Jobs (Keyserver)
Save new keys to:	(OK) C:\Programme\CompanyCRYPT\Keys\Import
Maintenance:	<input type="checkbox"/> Automatically remove unused files from import area after: 60 days.

- | | |
|--|--|
| Extract new keys: | Wann soll neues Schlüsselmaterial extrahiert werden? |
| All Decrypt Jobs: | CompanyCRYPT erkennt und exportiert bei Bedarf neue Keys aus allen eMails, welche verarbeitet werden. (Standard) |
| Only MIKE Jobs: | Es werden nur noch neue Keys aus den eMails exportiert, welche an MIKE adressiert wurden. (= Verarbeitung durch das Szenario 'Keyserver extern') |
| Save new keys to: | Verzeichnis für die Ablage der extrahierten (neuen) Schlüssel |
| Maintenance: | Aktiviert/Deaktiviert das Löschen ungenutzter Schlüssel aus der Import Area |
| Automatically remove unused files from import area after days: | Extrahierte Schlüssel werden nach der angegeben Zeit gelöscht. |

Automatischer Import von öffentlichen Schlüsseln

WebGUI → (Key Management) Import → Auto-Detect / Auto-Import → Auto-Import Keys and Certificates

Die Funktion ermöglicht den Import der öffentlichen Schlüssel aus der Import Area.

Auto-Import Keys and Certificates	
Activate public key import for: <div style="margin-left: 20px;"> <input checked="" type="checkbox"/> S/MIME certificates <input checked="" type="checkbox"/> PGP keys <input type="checkbox"/> Even for already existing address </div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> S/MIME: New certificates will only be automatically imported, if complete chain of valid issuer can be verified via Trusted CA store </div> <div style="border: 1px solid #ccc; padding: 5px;"> PGP: New keys will be automatically imported, if there is no key present for the email address(es). Allowing autoimport for already existing addresses increases the risk for man-in-the-middle attacks. </div>

Activate public key import for:

S/MIME certificates: Aktiviert/Deaktiviert den automatischen Import von Public S/MIME Zertifikaten

PGP keys: Aktiviert/Deaktiviert den automatischen Import von Public PGP Keys

Even for already existing address: Importiert auch PGP-Keys für eine Emailadresse, für die bereits ein Key im Keystore vorhanden ist.

Der automatische Import für öffentliche S/MIME-Zertifikate ist nur möglich, wenn sich die jeweilige ausstellende CA im Trusted CA Store befindet.

Automatischer Import von privaten Schlüsseln

WebGUI → (Key Management) Import → Auto-Detect / Auto-Import → Auto-Import Private Keys

Auto-Import Private Keys	
Private Key Import	<input type="checkbox"/> Activated Use Passphrase:

Private Key Import: Aktiviert/Deaktiviert den Import privater Schlüssel

Use Passphrase: Passwort für den Zugriff auf die zu importierenden privaten Schlüssel

Benachrichtigungseinstellungen

WebGUI → (Key Management) Import → Auto-Detect / Auto-Import → Notifications

Notifications	
Notification Events:	<input type="checkbox"/> Key Extracted <input type="checkbox"/> Auto-Import Successful <input type="checkbox"/> Auto-Import not possible

Notification Events:

Key Extracted: Email-Information wenn neuer Schlüssel extrahiert wurde

Auto-Import Successful: Email-Information wenn neuer Schlüssel importiert wurde

Auto-Import not possible: Email-Information wenn Schlüssel nicht importiert wurde

3.8.9. Site to Site-Verschlüsselung

WebGUI → (Key Management) Site to Site

Hinter diesem Feature verbirgt sich eine komfortable Methode für die Verschlüsselung zwischen zwei Partnern anhand der eMaildomäne. Mails für eine bestimmte Domäne werden unabhängig vom empfangenden User immer mit dem gleichen Key verschlüsselt. Es wird also nicht für jede externe Adresse des Partners ein separater Key benötigt.

Voraussetzung für die Nutzung dieser Funktion ist natürlich das Vorhandensein entsprechender Mailinfrastruktur auf beiden Seiten. Vorzugsweise ist für die Umsetzung eine Gatewaylösung auf der Partnerseite zu empfehlen, da die Site to Site-Funktionalität bisher nur bei wenigen Verschlüsselungsprodukten für den Desktop Unterstützung findet.

Anzeigen der Site to Site-Verbindungen

WebGUI → (Key Management) Site to Site → Site-to-Site connections

In der Listenansicht werden alle Schlüssel angezeigt, denen über das Feld Encrypt Alias mehrere Emailadressen zugeordnet sind. Zur Realisierung einer Site to Site Verschlüsselung (Domänen-Verschlüsselung) wird in das Feld Encrypt Alias die Domäne mit Wildcards eingetragen.

Sit-To-Site Connections					
Type	Expires	Encrypt Alias ▲	Name	Added	
[..any..] ▼		[..any..]	[..any..]	[..any..] ▼	
	2023-01-22	*@aerodata.de	Aerodata AG	2013-01-24	
	unlimited	*@ahg.de	AHG AG - Security CSA SYSTEM	2013-05-08	
	unlimited	*@august-faller.de	August_Faller_KG - Central_Signing_Account	2012-04-25	
	2023-05-01	*@bethel.de	vBS Bethel Signature Gateway	2013-05-03	
	unlimited	*@bkkmitte.de	BKK-LV Ost	2012-04-25	
	unlimited	*@bremerlandesbank.de	Bremer_Landesbank_Encryption_Account	2012-04-25	
	unlimited	*@cor.fja.com *@fja.com	Signature Gateway COR.FJA	2012-04-25	
	unlimited	*@ewv.de	Encryption Gateway EWV GmbH	2012-04-25	
	unlimited	*@gebr-heinemann.de	Gebrueder-Heinemann_Signing_Account	2012-04-25	
	2022-09-17	*@gildemeister.com	GILDEMEISTER_CRYPTO_ACCOUNT	2012-12-13	
	unlimited	*@khv.de	Signatur Gateway der Hamburger Kassenvereine	2012-04-25	
Total: 40 Keys		Page 1 of 1		Keys per Page: 10 25 [100]	

Spalten der Listenansicht

Type:	Format des Keys (PGP oder S/MIME)
Expires:	Gültigkeitsdatum des Schlüssels, Bei Keys ohne Ablaufdatum wird unlimited angezeigt. Abgelaufene Schlüssel werden durch ein Ausrufungszeichen markiert
Encrypt Alias:	Zugewiesene Mailadressen des Keys, Die Adresse wird gekürzt dargestellt, sofern die Spaltenbreite überschritten wird.
Name:	Name bzw. Bezeichnung des Schlüssels, Der Name wird gekürzt dargestellt, sofern die Spaltenbreite überschritten wird.
Added	Datum, an dem das Zertifikat dem Speicher hinzugefügt wurde.
Symbol Details:	Durch klicken auf dieses Symbol werden die Keydetails angezeigt.

Anzeigen der Schlüsseleigenschaften für Site to Site-Verbindungen

WebGUI → (Key Management) Site to Site → PGP / S/MIME key properties

Durch klicken auf die Domäne, die eMailadresse oder das Detailsymbol gelangen Sie zu den Eigenschaften des jeweiligen Public Keys. Die gewählte Verbindung wird blau hinterlegt dargestellt. Unter der Listenansicht werden die primären Eigenschaften des gewählten Schlüssels angezeigt.

PGP key properties +

Name	Landeskrankenhilfe V.V.a.G - Signatur
eMail	Signatur@lkh.de
Encrypt Alias	*@landeslebenshilfe.de *@lkh.de
Fingerprint	27D5 3771 5445 22D5 8079 4F6E B90E 8F97 A235 6D94
Status:	Usable

Durch anklicken der Schaltfläche [+] wird eine erweiterte Ansicht mit allen Details des Schlüssels angezeigt.

Erstellen einer Site to Site-Verbindungen

WebGUI → (Key Management) External

1. Schritt

Wählen Sie aus der Liste den Public Key für die Site to Site-Verbindung.



External Key Store					
Type	Expires	eMail ^	Name	Added	
[..any..] ▼		[..any..]	[..any..]	[..any..] ▼	
2024-04-27	administrator@klinikum-kemp...	Encryption Gateway Klinikverbund Kempten...	2014-05-05		
unlimited	AHG-CSA@ahg.de	AHG AG - Security CSA SYSTEM	2013-05-08		
unlimited	AlexanderStrobel@gmx.de	Alexander Strobel	2012-04-25		

2. Schritt

Klicken Sie bei den Key Properties auf **[+]** um alle Keyeigenschaften anzuzeigen.

PGP key properties	
Name	Encryption Gateway Klinikverbund Kempten-Oberallgaeu
eMail	administrator@klinikum-kempten.de
Encrypt Alias	
Fingerprint	B788 262F 6C94 980B 6765 DD64 ABF4 D1F8 C695 2E03
Keystore ID	caf868a0-0cb1-ffc9-e84d-21debd23

3. Schritt

Tragen Sie die gewünschte Zieldomäne beginnend mit ***@** in das Feld **Encrypt Alias** ein und klicken Sie auf den **Save**-Button.

PGP key properties	
Name	Encryption Gateway Klinikverbund Kempten-Oberallgaeu
eMail	administrator@klinikum-kempten.de
Encrypt Alias	*@klinikum-kempten.de
Fingerprint	B788 262F 6C94 980B 6765 DD64 ABF4 D1F8 C695 2E03
Keystore ID	caf868a0-0cb1-ffc9-e84d-21debd23

Sign key

Save

Delete Key

Löschen einer Site to Site-Verbindungen

WebGUI → (Key Management) Site to Site

1. Schritt

Markieren Sie die den zu löschenden Eintrag in der Listenansicht.

Sit-To-Site Connections					
Type	Expires	Encrypt Alias ^	Name	Added	
[..any..] ▼		[..any..]	[..any..]	[..any..] ▼	
2024-04-27	*@klinikum-kempten.de	Encryption Gateway Klinikverbund Kempten...	2014-05-05		
unlimited	*@komsa.com	Central_Signing_Account	2012-04-25		
2019-07-22	*@ksb-intax.de	pseudo: Secure Mail Gateway	2014-07-22		

2. Schritt

Bei den Key Properties entfernen Sie den Eintrag aus dem Feld **Encrypt Alias** und klicken Sie auf den **Save**-Button.

PGP key properties	
Name	Encryption Gateway Klinikverbund Kempten-Oberallgaeu
eMail	administrator@klinikum-kempten.de
Encrypt Alias	
Fingerprint	B788 262F 6C94 980B 6765 DD64 ABF4 D1F8 C695 2E03
Status:	Usable

Sign key

Save

Delete Key

3.9. CompanyCRYPT Lizenz

Zur Konfiguration bzw. Administration von CompanyCRYPT ist es erforderlich, dass eine gültige Lizenz eingetragen wird.

3.9.1. Lizenz eingeben

WebGUI → (Info) About → Licence

Hier übertragen Sie bitte in die Felder **Company**, **Serial** und **Licence key** die Daten aus dem Licence Record. Achten Sie hierbei auf exakte Schreibweise (Groß-/Kleinschreibung) im Feld Company. (Buchstaben im Licence Key werden automatisch in Grossbuchstaben konvertiert.) Anschließend speichern Sie die erfassten Daten mit **Store Licence**.

Licence	
Status:	VALID
Company:	Company name
Serial:	serial number
Licence key:	licence key
MSW Serial:	2129-0536-1004-6000
Users:	50
Valid until:	unlimited
<input type="button" value="Store Licence"/>	

Hinweis: Für die Eingabe des Licence keys ist die Groß-/Kleinschreibung ohne Bedeutung.

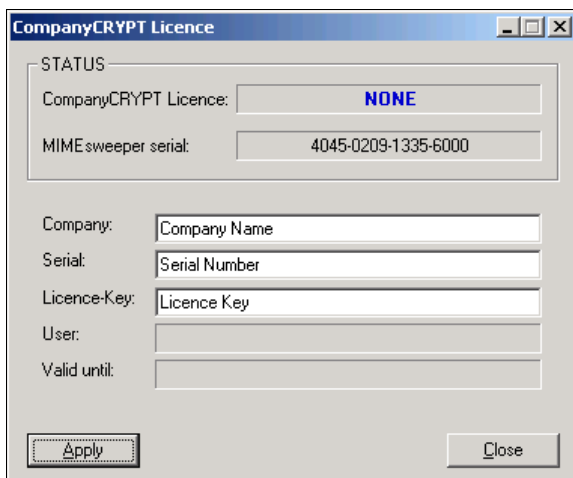
Wichtig: Wenn Ihr MIMesweeper ausschließlich ein *Primary Configuration Server* (PCS) ist, d.h. kein *Policy Server* (PS) auf dem System aktiv ist, werden die Lizenz Informationen durch den ersten Synchronisationskontakt mit einem anderen CompanyCRYPT (Slave) System übertragen. Weitere Informationen zu Multi-Server-Umgebungen entnehmen Sie bitte dem *Installation Guide*. Erst nach einem erfolgreichen Synchronisationskontakt werden Sie Zugang zu der vollständigen WebGUI auf diesem (Master) System erlangen.

Lizenz eingeben per SyncManager

SyncManager → Licence → Add / Edit

Wichtig: Bevor Sie Konfigurationsänderungen mit dem SyncManager vornehmen muss immer der Operational Service von CompanyCRYPT gestoppt werden um die Synchronisation anzuhalten! Andernfalls werden die Änderungen nicht übernommen. Nach Abschluss der Konfiguration ist der Operational Service wieder zu starten.

Hier übertragen Sie bitte in die Felder **Company**, **Serial** und **Licence key** die Daten aus dem Licence Record. Achten Sie hierbei auf exakte Schreibweise (Groß-/Kleinschreibung) im Feld Company. (Buchstaben im Licence Key werden automatisch in Grossbuchstaben konvertiert.) Anschließend speichern Sie die erfassten Daten mit **Apply** und schliessen Sie das Fenster mit **Close**.



CompanyCRYPT Licence

STATUS

CompanyCRYPT Licence: **NONE**

MIMESweeper serial: 4045-0209-1335-6000

Company:

Serial:

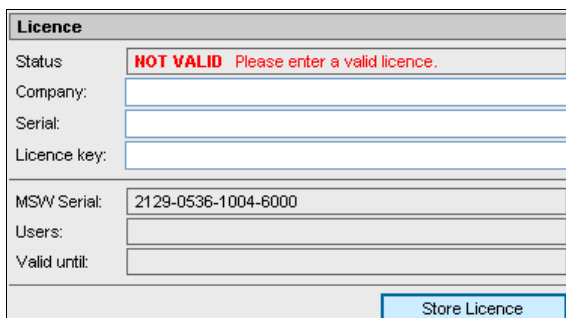
Licence-Key:

User:

Valid until:

3.9.2. Lizenz löschen

WebGUI → (Info) About → Licence



Licence

Status: **NOT VALID** Please enter a valid licence.

Company:

Serial:

Licence key:

MSW Serial: 2129-0536-1004-6000

Users:

Valid until:


Hier löschen Sie die Felder **Company**, **Serial** und **Licence key** und speichern anschließend mit **Store Licence**.

Lizenz löschen per SyncManager

SyncManager → Licence → Delete

Wichtig: Bevor Sie Konfigurationsänderungen mit dem SyncManager vornehmen muss immer der Operational Service von CompanyCRYPT gestoppt werden um die Synchronisation anzuhalten! Andernfalls werden die Änderungen nicht übernommen. Nach Abschluss der Konfiguration ist der Operational Service wieder zu starten.

Bestätigen Sie das Löschen der Lizenzinformationen mit dem Button **OK**.



Delete CompanyCRYPT Licence

 Please confirm to delete this CompanyCRYPT Licence

Company: Company Name

User: 20

Valid until: 2008-01-31



Secure Internet Traffic



COMPANYCRYPT®
The encryption module for MIMESweeper

4. Einrichtung der Ver-/Entschlüsselung

Die Aktivierung der Verschlüsselung/Entschlüsselung wird über die Einrichtung spezieller CompanyCRYPT-Szenarien im MIMESweeper realisiert. Die notwendigen Konfigurationen im MIMESweeper Policy Editor und die Einstellungen in der CompanyCRYPT WebGUI werden schrittweise erklärt.



Secure Internet Traffic



COMPANYCRYPT®
The encryption module for MIMESweeper

Einrichtung der Ver-/Entschlüsselung
Aufruf des MIMESweeper Policy-Editors

Configuration Guide
CompanyCRYPT v1.5.0

4.1. Aufruf des MIMESweeper Policy-Editors

Start → Alle Programme → MIMESweeper for SMTP → MIMESweeper Policy Editor

Bei einer Standardinstallation des MIMESweepers wird automatisch eine gleichnamige Programmgruppe im Startmenü angelegt.

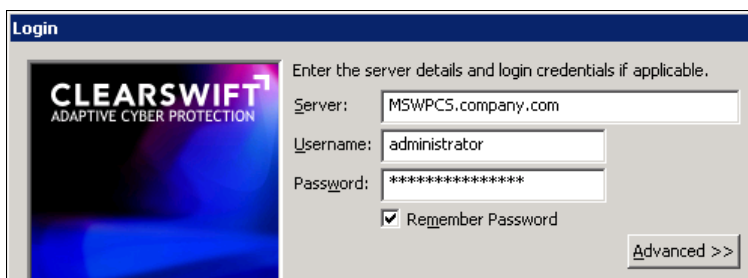
1. Schritt

Starten Sie den MIMESweeper Policy Editor direkt durch Doppelklick auf die Desktopverknüpfung oder aus dem Startmenü.



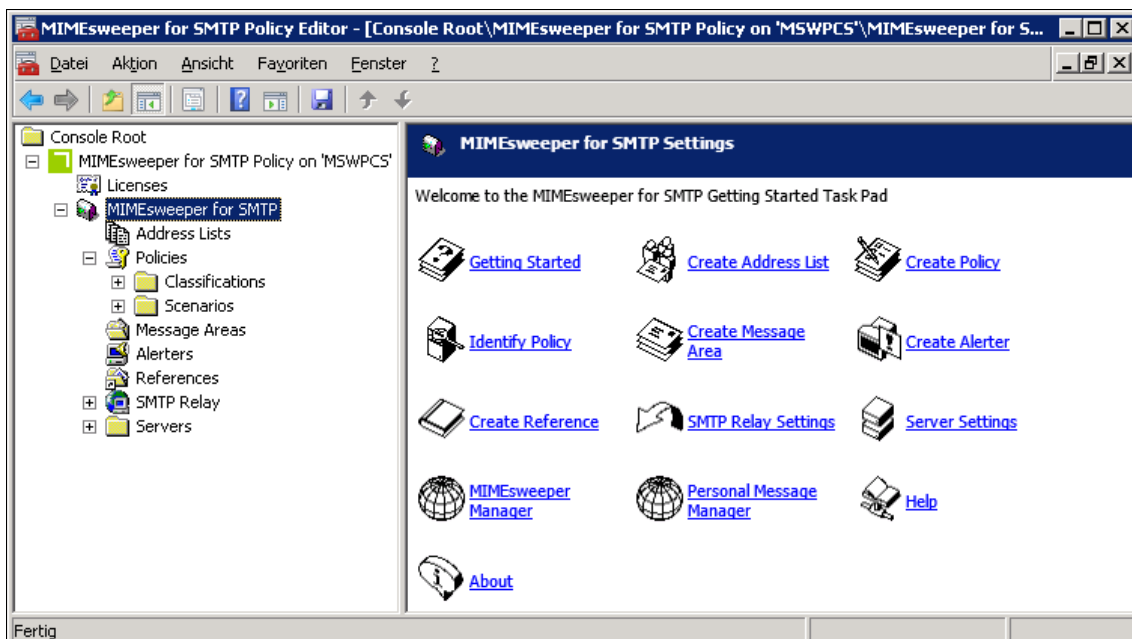
2. Schritt

Tragen Sie die Anmeldeinformationen ein und bestätigen Sie diese mit OK.



3. Schritt

Der Policy Editor öffnet sich und Sie haben Zugriff auf die einzelnen Bereiche/Module des MIMESweepers.





4.2. Allgemeine Informationen

4.2.1. Adresslisten

Adresslisten werden nur für die Einrichtung von Adressbasierten Verschlüsselungsbeziehungen benötigt. Sie dienen als Referenzen innerhalb der Szenarios. Pro Verschlüsselungsformat wird eine Adressliste angelegt. Beispiel: Alle Partner, die S/MIME-verschlüsselte Mails von Ihnen empfangen wollen kommen in eine Adressliste, alle mit PGP-Verschlüsselung in eine weitere Liste und mit PGP-Signierung wieder in eine separate Liste, usw.

Übersicht der Adresslisten

Die Anzahl der für CompanyCRYPT einzurichtenden Adresslisten richtet sich nach der Menge der genutzten Verschlüsselungsverfahren und deren Kombinationen. Beachten Sie bei der Vergabe der Namen, dass eine leichte Zuordnung zur jeweils verwendeten Funktion bzw. Ver-/Entschlüsselungsmethode möglich ist.

Empfehlung für die Namensgebung der Adresslisten

SMIME (Encrypt only)	Empfängeradressen, welche S/MIME-verschlüsselte eMails ohne Signatur erhalten sollen, verwendet wird das Format S/MIME
PGP-MIME (Encrypt only)	Empfängeradressen, welche PGP-verschlüsselte eMails ohne Signatur erhalten sollen, verwendet wird das empfohlene Format PGP/MIME
PGP-Inline (Encrypt only)	Empfängeradressen, welche PGP-verschlüsselte eMails ohne Signatur erhalten sollen, verwendet wird das Format Inline-PGP
SMIME (Encrypt and Sign Company)	Empfängeradressen, welche S/MIME-verschlüsselte eMails erhalten sollen, die zusätzlich noch durch den Firmenschlüssel signiert werden,
SMIME (Encrypt and Sign User)	Empfängeradressen, welche S/MIME-verschlüsselte eMails erhalten sollen, die zusätzlich mit dem Schlüssel des Absenders signiert werden,
SMIME (Sign only Company)	Empfängeradressen, welche eMails erhalten sollen, die durch den Firmenschlüssel signiert werden (PGP-Signatur) , Format PGP/MIME
PGP-MIME (Site2Site)	Domänen, mit denen eMails per Site to Site-Verschlüsselung ausgetauscht werden sollen, Format PGP/MIME

4.2.2. Classifications

Die Verarbeitung aus den CompanyCRYPT-Szenarios mündet in eine Klassifikation. Nach der Verschlüsselung innerhalb der Szenarios findet dann die eigentliche Reaktionen auf diese Nachricht (Antwort, Benachrichtigung, Zustellung mit Hinweis, ...) statt.

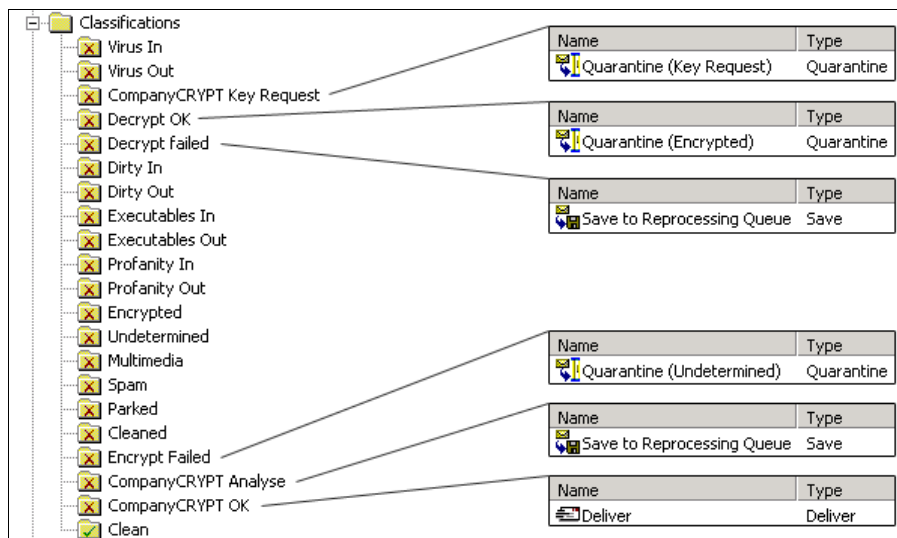
Classifications für CompanyCRYPT

Die Inhaltsüberprüfungen aus den 'Szenarios' münden in eine oder mehrere Klassifikationen. Bei mehreren Klassifikationen wird die erste zutreffende gewählt. Nach der Ver- oder Entschlüsselung innerhalb der Szenarios findet dann die eigentliche Reaktionen auf diese Nachricht (Antwort, Benachrichtigung, Zustellung mit Hinweis, ...) statt.

Nachfolgend sind beispielhaft die für die Ver- und Entschlüsselung angelegten Klassifikationen und die entsprechenden Verarbeitungsaufgaben dargestellt.

Policy Editor → MIMesweeper for SMTP Policy → MIMesweeper for SMTP → Policies → Classifications

Die Abbildung zeigt beispielhaft die Anordnung der für die Ver- und Entschlüsselung verwendeten Classifications und den jeweils enthaltenen Aktionen.

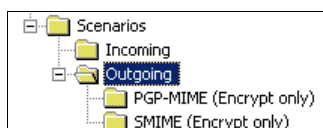


Die Anordnung der Classifications ist relativ zu betrachten. Wichtig für die Funktionalität des Entschlüsselns ist die Positionierung der Decrypt OK-Classification oberhalb der MIMESweeper-eigenen System-Classification Encrypted.

4.2.3. Scenario Folder

Die Scenario Folder werden nur für die Einrichtung von Adressbasierten Verschlüsselungsbeziehungen benötigt. Sie stellen den Beginn der Verarbeitung dar. Die hier in den Eigenschaften festgelegten Sender-Empfänger-Kombinationen bestimmen die Aufgaben, die an einer Nachricht durchgeführt werden sollen. Die Zuordnungssuche beginnt am Stamm (Scenarios = *@* an *@*), durchläuft den Baum von oben, verzweigt an ‚zutreffenden‘ Unterordnern und endet bei der am besten ‚passenden‘ Kombination.

Die Abbildung zeigt beispielhaft die Anordnung der für die Adressbasierte Verschlüsselung angelegten Scenario Folder. Die Anzahl der für CompanyCRYPT einzurichtenden Scenario Folder richtet sich nach der Menge der genutzten Verschlüsselungsverfahren und deren Kombinationen.



Übersicht der Scenario Folder

Beachten Sie bei der Vergabe der Namen für die Scenario Folder, dass eine leichte Zuordnung zur jeweils verwendeten Funktion bzw. Ver-/Entschlüsselungsmethode möglich ist.

Empfehlung für die Namensgebung der Scenario Folder

SMIME (Encrypt only)

Empfänger, welche S/MIME-verschlüsselte eMails ohne Signatur erhalten sollen, verwendet wird das Format S/MIME

PGP-MIME (Encrypt only)

Empfänger, welche PGP-verschlüsselte eMails ohne Signatur erhalten sollen, verwendet wird das empfohlene Format PGP/MIME

PGP-Inline (Encrypt only)

Empfänger, welche PGP-verschlüsselte eMails ohne Signatur erhalten sollen, verwendet wird das Format Inline-PGP

SMIME (Encrypt and Sign Company)

Empfänger, welche S/MIME-verschlüsselte eMails erhalten sollen, die zusätzlich noch durch den Firmenschlüssel signiert werden,

SMIME (Encrypt and Sign User)

Empfänger, welche S/MIME-verschlüsselte eMails erhalten sollen, die zusätzlich mit dem Schlüssel des Absenders signiert werden,

**SMIME (Sign only Company)**

Empfänger, welche eMails erhalten sollen, die durch den Firmenschlüssel signiert werden (PGP-Signatur) , Format PGP/MIME

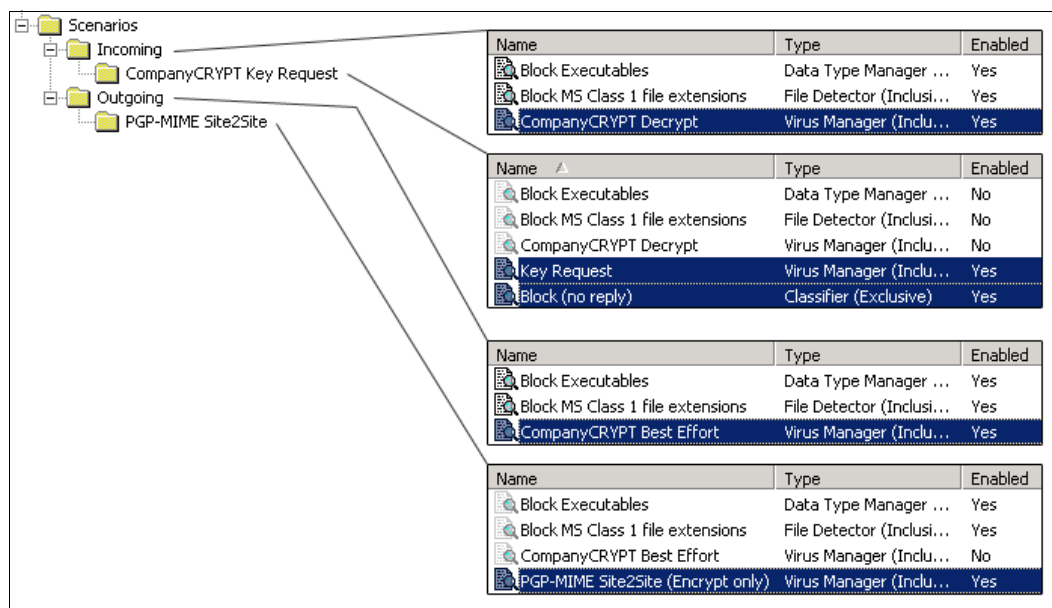
PGP-MIME (Site2Site)

Domänen, mit denen eMails per Site to Site-Verschlüsselung ausgetauscht werden sollen, Format PGP/MIME

4.2.4. CompanyCRYPT Scenarios

Die Scenarios bezeichnen die eigentlichen Aufgaben, die an einer Nachricht durchgeführt werden sollen. Die Einrichtung der Scenarios erfolgt in den Scenario Foldern.

Die Abbildung zeigt beispielhaft die Anordnung der für die Ver- und Entschlüsselung angelegten Scenario Folder und den jeweils enthaltenen Scenarios.



Die Anordnung der Sceanrio-Jobs ist von Bedeutung. Wichtig für die Funktionalität des Verschlüsselns ist die Positionierung des CompanyCRYPT-Scenarios (Encrypt) an unterster Stelle im jeweiligen Scenario Folder.

Hinweis: Wenn Sie CompanyCRYPT-Scenarios in Unterordnern verwenden, ist es erforderlich, dass die Adresskombinationen (Sender/Empfänger), welche in dem Unterordner definiert wurden, zumindest eine Teilmenge der Adresskombinationen des übergeordneten Ordners sind. Andernfalls werden die Scenarios des Unterordners nie angesprochen.

Wichtig: Stellen Sie bitte sicher, das jeweils nur ein CompanyCRYPT-Szenario pro Ordner aktiv ist, und dass vererbte CompanyCRYPT-Scenarios entsprechend deaktiviert sind. **Mehrfachverarbeitungen führen zu undefinierten Verarbeitungsergebnissen.**

CompanyCRYPT-Scenarios – Weiterführende Informationen

Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Scenarios → Virus Manager

CompanyCRYPT unterstützt die Verschlüsselungs-/Signiermethoden PGP/MIME, Inline-PGP, S/MIME und die Ad Hoc Verschlüsselung. Dies resultiert in einer großen Anzahl möglicher Verarbeitungsprozesse, welche als 'Scenario'-Jobs innerhalb des *Virus Manager Scenarios* vordefiniert sind.

Alle verfügbaren Entschlüsselungs-Scenarios sind unter 5.1.1 "Entschlüsselung – Verfügbare Scenarios" aufgelistet.



Secure Internet Traffic



COMPANYCRYPT®
The encryption module for MIMESweeper

Einrichtung der Ver-/Entschlüsselung
Allgemeine Informationen

Configuration Guide
CompanyCRYPT v1.5.0

Eine grafische Darstellung der verfügbaren Entschlüsselungs-Scenarios finden Sie unter 5.1.2 "Entschlüsselung – Verarbeitungsdetails".

Alle verfügbaren Verschlüsselungs-Scenarios sind unter 5.2.1 "Verschlüsselung – Verfügbare Scenarios (Nach Methode gruppiert)" aufgelistet.

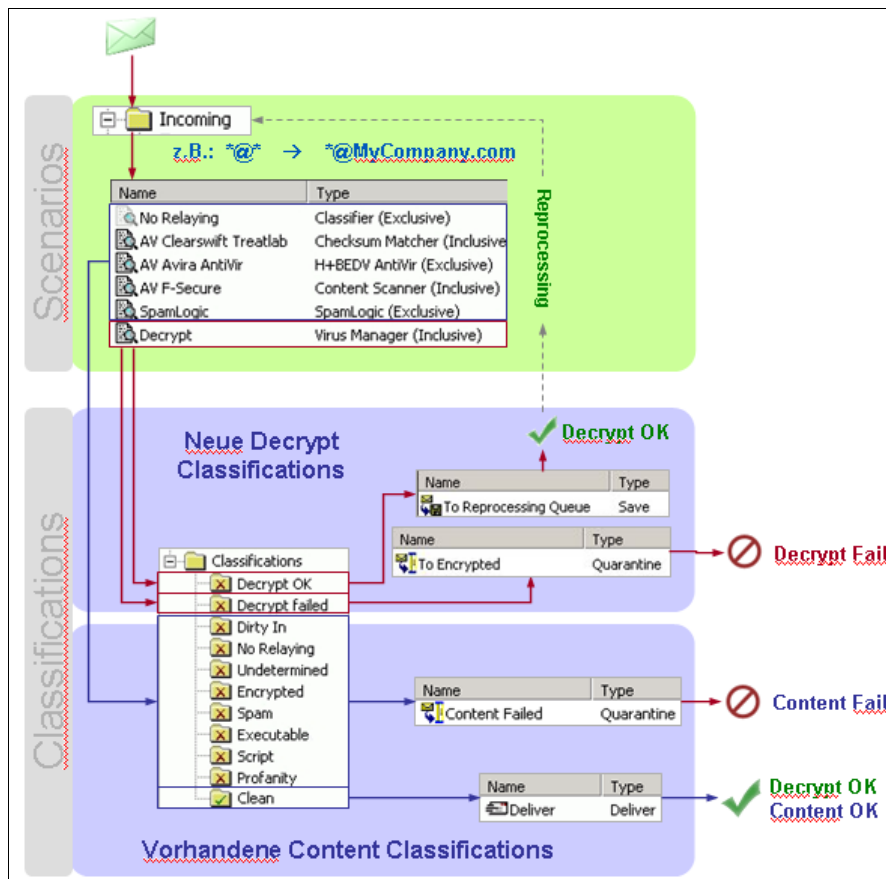
Eine grafische Darstellung der verfügbaren Verschlüsselungs-Scenarios finden Sie unter 5.2.2 „Verschlüsselung – Wahl des passenden Jobs“ and 5.2.3 "Site-to-Site/Gruppen Verschlüsselung – Wahl des passenden Jobs".



4.3. Entschlüsselung

Die Entschlüsselung wird über das Zusammenspiel zwischen Classifications, Szenarios und über einen Reprocessing Mechanismus realisiert. Hierüber ist es insbesondere möglich Mehrfach-Verschlüsselungen zu verarbeiten.

4.3.1. Funktionsbild - Entschlüsselung



4.3.2. Einrichtungsschritte zusammengefasst

1. Schritt

Erzeugen Sie 2 neue 'Classifications' und verschieben Sie diese an den Anfang der Classifications Liste.

- | | | |
|----------------|---|--|
| Decrypt OK | → | Save Action mit Ziel 'Reprocessing' |
| Decrypt failed | → | Quarantine Action zu beliebiger Message area |

2. Schritt

Erzeugen Sie im eingehenden Szenario Ordner (z.B. Incoming) ein Virus Manager Job und wählen Sie Decrypt- Expect decrypt only OK. Diesen verknüpfen Sie dann mit den erzeugten Classifications.

- | | | |
|----------------------------|---|----------------|
| On detected items cleaned | → | Decrypt OK |
| On virus cannot be removed | → | Decrypt failed |

4.3.3. Einrichtung der Entschlüsselung

Einrichten der Classifications (Entschlüsselung)

Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Classifications

1. Schritt

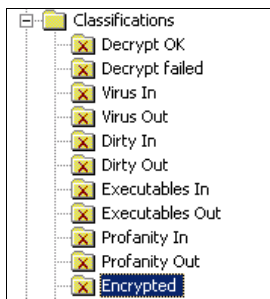
Klicken Sie mit der rechten Maustaste auf **Classifications** und wählen Sie dann **Neu → Classification** und benennen Sie die Classification **Decrypt OK**.

2. Schritt

Erstellen Sie nach dem gleichen Vorgehen eine weitere Classification und benennen Sie die Classification **Decrypt failed**.

3. Schritt

Verschieben Sie nun beide Classification nach oben, über die System-Classification **Encrypted**.

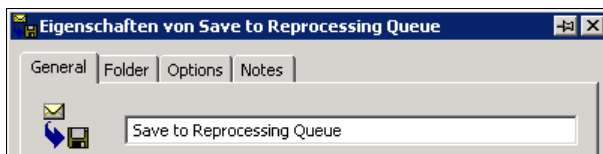


4. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **Decrypt OK** und wählen Sie **Neu → Save**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

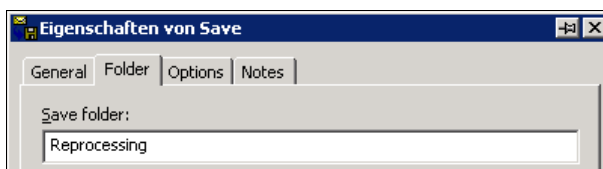
5. Schritt

Unter **Eigenschaften von Save → General** geben Sie den Namen **Save to Reprocessing Queue** ein



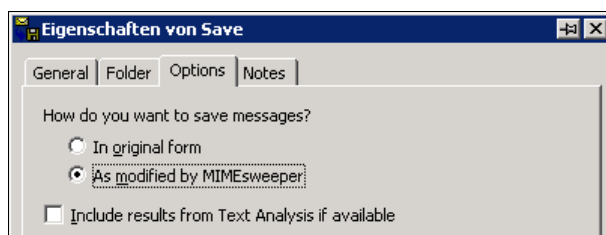
6. Schritt

Unter **Eigenschaften von Save → Folder** geben Sie den Folder-Namen **Reprocessing** an. Dieser Name muss den CompanyCRYPT-Einstellungen für den Reprocess Service entsprechen!



7. Schritt

Unter **Eigenschaften von Save → Options** markieren Sie die Option **As modified by MIMESweeper**. Include results from Text Analysis if available wird nicht markiert. Speichern Sie Einstellungen mit OK.

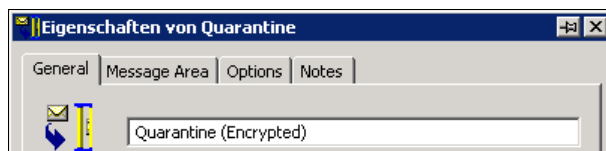


8. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **Decrypt failed** und wählen Sie **Neu → Quarantine**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

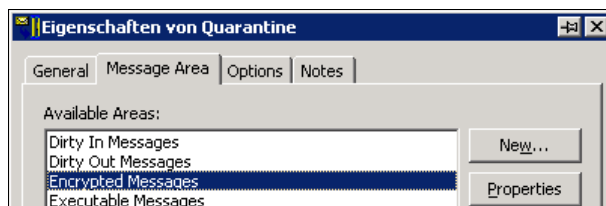
9. Schritt

Unter **Eigenschaften von Quarantine → General** geben Sie den Namen **Quarantine (Encrypted)** ein.



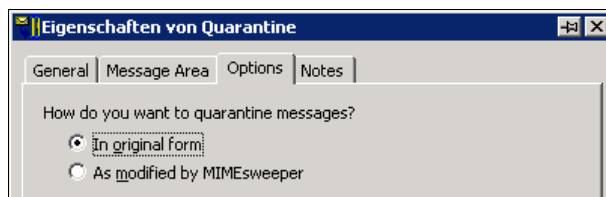
10. Schritt

Unter **Eigenschaften von Quarantine → Message Area** wählen Sie **Encrypted Messages** aus.



11. Schritt

Unter **Eigenschaften von Quarantine → Options** markieren Sie **In original form** und bestätigen die Einstellungen mit OK.



Einrichten der CompanyCRYPT-Scenarios (Entschlüsselung)

Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Scenarios → Incoming

Hinweis: Anders als bei der ausgehenden Verschlüsselung ist es für eingehende eMails nicht erforderlich zwischen den Methoden Inline-PGP, PGP/MIME oder S/MIME zu unterscheiden. Die Methode wird automatisch erkannt und entsprechend verarbeitet.

Beispielhaft wird hier die Erstellung eines Szenarios für Entschlüsselung ohne Signatur beschrieben. Wird zur Erstellung der CompanyCRYPT-Scenarios der Scenario-Wizards verwendet, werden vordefinierte Einstellungen aus der Datei EXE.INI automatisch übernommen und die manuelle Zuordnung der Data Types entfällt. Zur Erläuterung der notwendigen Einstellungen wird im folgenden Beispiel auf die Verwendung des Scenario-Wizards verzichtet.

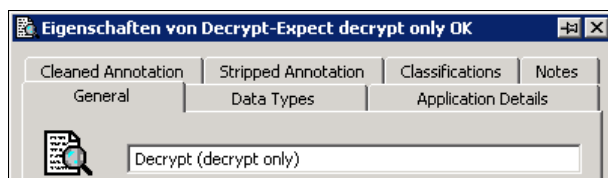
Zum Verständnis der folgenden Schritte sei erklärt, dass CompanyCRYPT wie ein weiterer Virens Scanner in den MIMESweeper eingebunden wird.

1. Schritt

Klicken Sie mit der rechten Maustaste auf den Scenario Folder **Incoming** und wählen Sie dann **Neu → Virus Manager**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

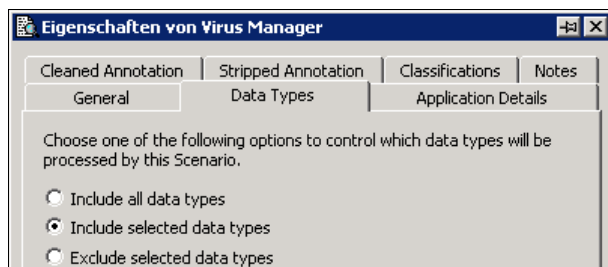
2. Schritt

Unter **Eigenschaften von Virus Manager → General** tragen Sie den Namen **Decrypt (decrypt only)** ein. Benutzen Sie selbsterklärende Namen.

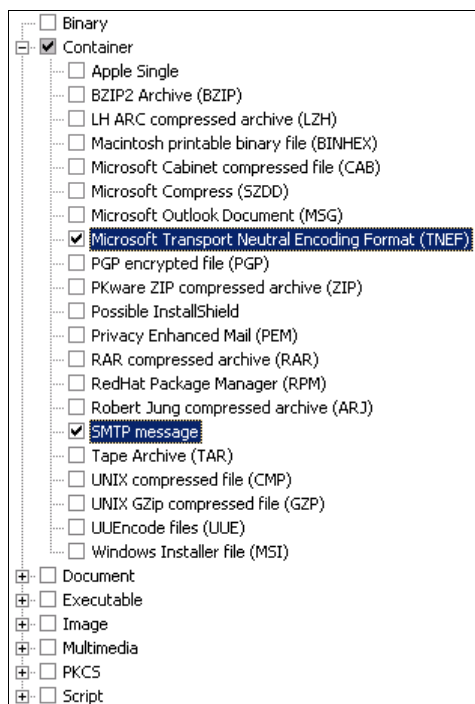


3. Schritt

Unter **Eigenschaften von Virus Manager → Data Types** wählen Sie die Option **Include selected data types**.

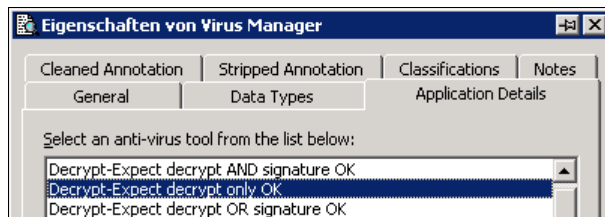


Bei der Auswahl der Data Types markieren Sie nur die beiden Container-Typen **Microsoft Transport Neutral Encoding Format (TNEF)** und **SMTP message**. Achten Sie darauf, dass keine weiteren Markierungen gesetzt sind.

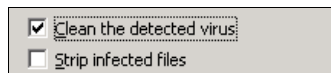


4. Schritt

Unter **Eigenschaften von Virus Manager → Application Details** markieren Sie das entsprechende CompanyCRYPT-Scenario **Decrypt-Expect decrypt only OK**.

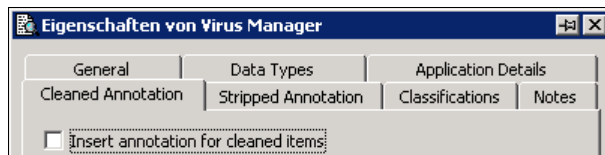


Aktivieren Sie anschließend die Option **Clean the detected virus** um eine Verschlüsselung des Mailinhaltes zu ermöglichen. Die Option Strip infected files darf nicht aktiviert sein.



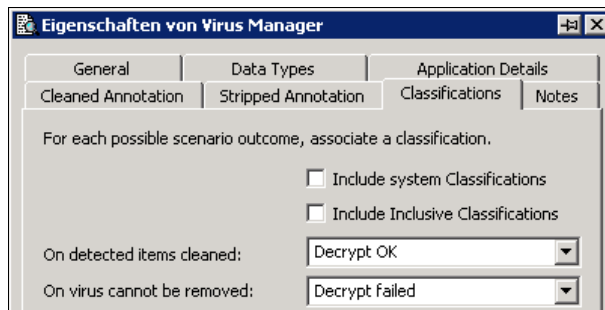
5. Schritt

Unter **Eigenschaften von Virus Manager** → **Cleaned Annotation** darf die Option Insert annotation for cleaned items nicht aktiviert sein.



6. Schritt

Unter **Eigenschaften von Virus Manager** → **Classification** setzen Sie die Classifications **On detected items cleaned: Decrypt OK** (erfolgreiche Entschlüsselung) und **On virus cannot be removed: Decrypt failed** (fehlgeschlagene Entschlüsselung). Speichern Sie die Einstellungen mit OK.



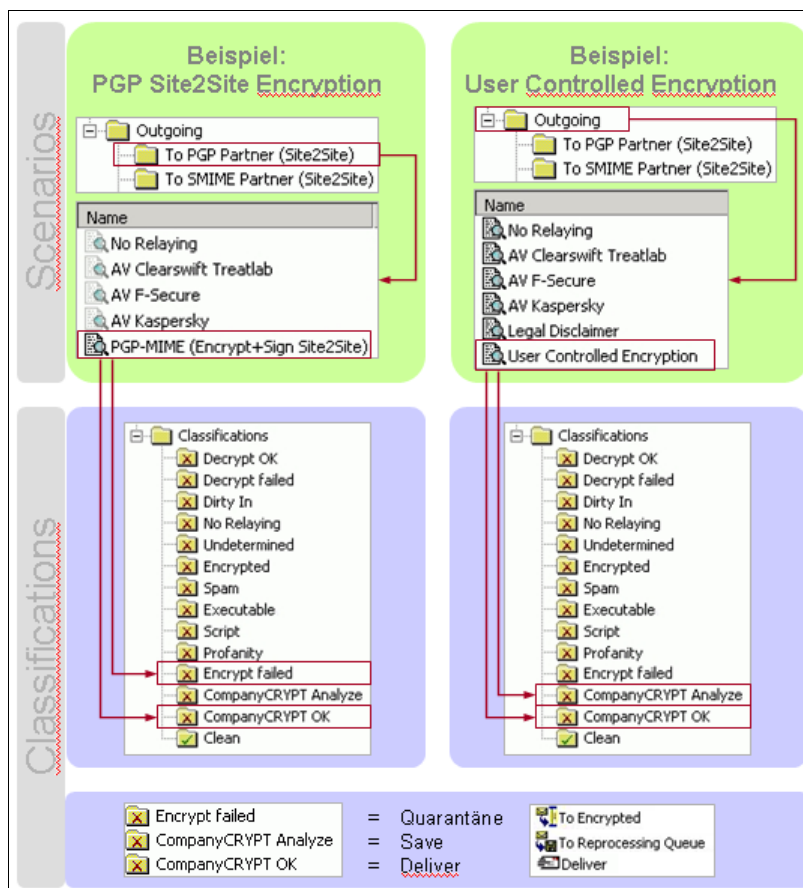


4.4. Verschlüsselung – Grundlegende Unterscheidung

In CompanyCRYPT stehen zwei grundsätzlich verschiedene Verschlüsselungsmethoden zur Verfügung, deren Verwendung sich aus dem jeweiligen Verschlüsselungsbedarf ergibt.

Adressbasierte Verschlüsselung	Anwendergesteuerte oder Best-Effort Verschlüsselung
Adresslisten-gesteuert	Usergesteuert und/oder Best Effort
Verfahren S/MIME, OpenPGP, mit oder ohne Signatur ist festgelegt	OpenPGP, S/MIME, Nur-Signiert oder Klartext nach Verfügbarkeit der Schlüssel (Selbständige Aufteilung in mehrere Nachrichten)
Je ein Scenario-Folder pro Verfahren	Keine Scenario-Folder erforderlich
Externe Keyserver werden nicht verwendet	Externe Keyserver nutzbar
Mittlerer Administrationsaufwand	Kein Administrationsaufwand
Verwendung bei Site-To-Site-Verbindungen, oder geforderter zuverlässiger Verschlüsselung	Ermöglicht die maximale Nutzung der Verschlüsselungstechnik

4.4.1. Funktionsbild – Unterscheidung der Verschlüsselungskategorien

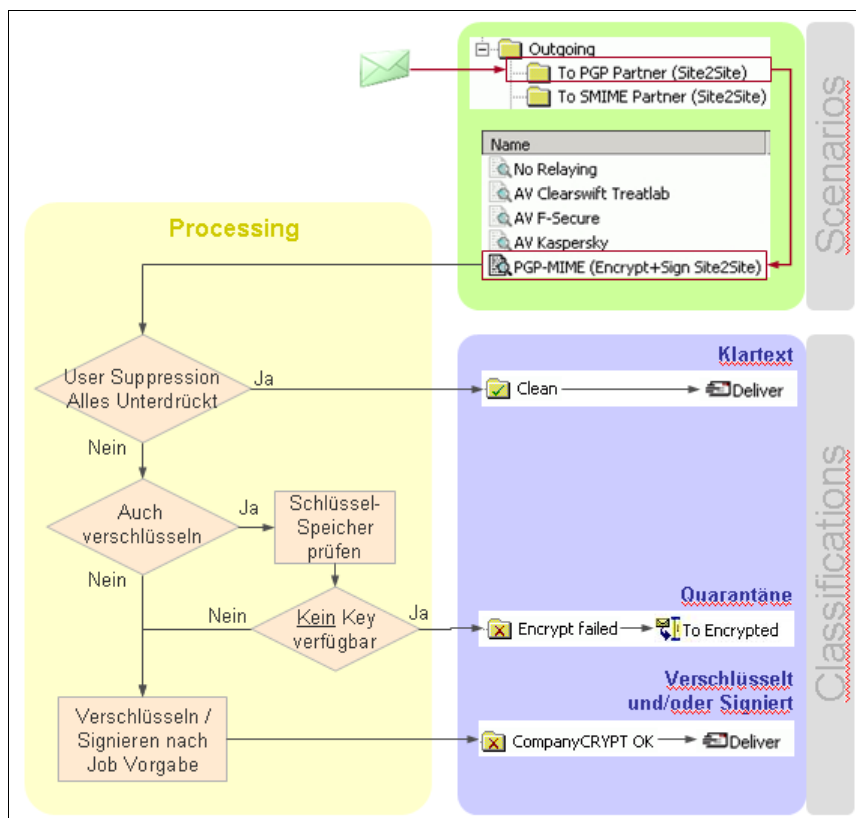




4.5. Adressbasierte Verschlüsselung

Die Adressbasierte Verschlüsselung wird durch die Definition von aufeinander abgestimmten Adresslisten, Szenarios und Classifications realisiert. Der Administrator hinterlegt für jeden Empfänger bzw. Domäne das gewünschte Verschlüsselungsformat und die Signiereinstellungen.

4.5.1. Funktionsbild – Adressbasierte Verschlüsselung



4.5.2. Einrichtungsschritte zusammengefasst

1. Schritt

Erzeugen Sie 2 neue 'Classifications' (falls noch nicht vorhanden) und verschieben Sie diese an das Ende der Classifications Liste (aber noch vor 'Clean').

CompanyCRYPT OK	→	Deliver Action
Encrypt failed	→	Quarantine Action zu beliebiger Message area

2. Schritt

Erzeugen Sie im ausgehenden Szenario Ordner einen neuen Unterordner, z.B. PGP-MIME (Encrypt only).

3. Schritt

Erzeugen Sie in diesem Unterordner ein Virus Manager Job und wählen Sie z.B. **OpenPGP-Encrypt only**. Diesen verknüpfen Sie dann mit den erzeugten Classifications.

On detected items cleaned	→	CompanyCRYPT OK
On virus cannot be removed	→	Encrypt failed

4.5.3. Einrichtung der Adressbasierten Verschlüsselung

Einrichten der Adresslisten für die Adressbasierte Verschlüsselung

Policy Editor → MIMesweeper for SMTP Policy → MIMesweeper for SMTP → Address Lists

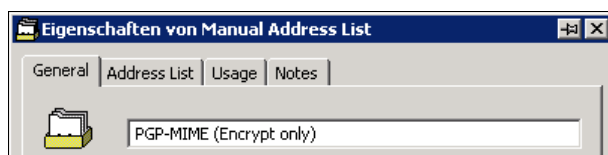
Beispielhaft wird hier die Erstellung einer Adressliste für die PGP/MIME Verschlüsselung ohne Signatur beschrieben.

1. Schritt

Klicken Sie mit der rechten Maustaste auf **Address List** und wählen Sie dann **Neu → Manual Address List**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards. Bei Verwendung des Wizards unterscheiden sich sowohl die dargestellten Fenster als auch die Reihenfolge der Schritte.

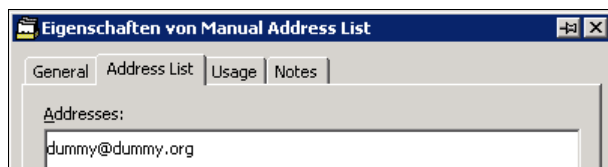
2. Schritt

Unter **Eigenschaften von Manual Address List → General** tragen Sie den Namen der Adressliste ein. In diesem Beispiel **PGP-MIME (Encrypt Only)**



3. Schritt

Unter **Eigenschaften von Manual Address List → Address List** tragen Sie die eMailadressen der Empfänger ein. Sind noch keine Adressen verfügbar so tragen Sie einen Platzhalter ein, zum Beispiel **dummy@dummy.org** und speichern die Einstellungen mit OK.



Bei großen Adressmengen, kann es sinnvoll sein, entsprechende Textfiles parallel zu den Adresslisten anzulegen und daraus zu importieren, da diese übersichtlicher zu pflegen sind (manuelle Sortierung möglich). Grundsätzlich sollen Nutzer nur einmal in den Adresslisten vorkommen.

4. Schritt

Die erstellte Adressliste wird anschließend in der Übersicht angezeigt.

Name	Type
PGP-MIME (Encrypt only)	Manual Address List
SMIME (Encrypt only)	Manual Address List

Einrichten der Classifications für die Adressbasierte Verschlüsselung

Policy Editor → MIMesweeper for SMTP Policy → MIMesweeper for SMTP → Policies → Classifications

1. Schritt

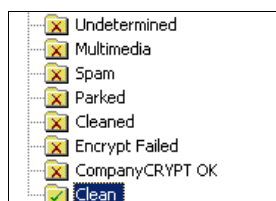
Klicken Sie mit der rechten Maustaste auf **Classifications** und wählen Sie dann **Neu → Classification** und benennen Sie die Classification **CompanyCRYPT OK**.

2. Schritt

Erstellen Sie nach dem gleichen Vorgehen eine weitere Classification und benennen Sie die Classification **Encrypt failed**.

3. Schritt

Die Classifications müssen nicht nach oben verschoben werden. Es ist jedoch zu beachten, dass beide Classifications unterhalb der Blocked-Classifications wie Virus oder Spam einzuordnen sind.



4. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **CompanyCRYPT OK** und wählen Sie **Neu → Deliver**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

5. Schritt

Unter **Eigenschaften von Deliver → General** geben Sie den Namen **Deliver** an und Bestätigen die Eingabe mit OK.

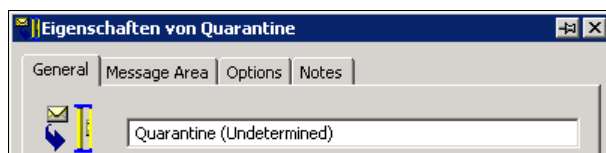


6. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **Encrypt failed** und wählen Sie **Neu → Quarantine**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

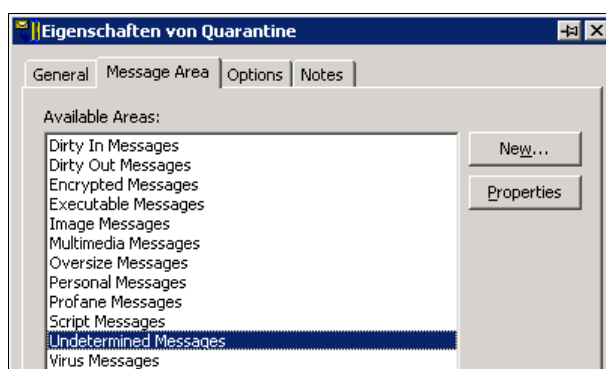
7. Schritt

Unter **Eigenschaften von Quarantine → General** geben Sie den Namen **Quarantine (Undetermined)** ein.



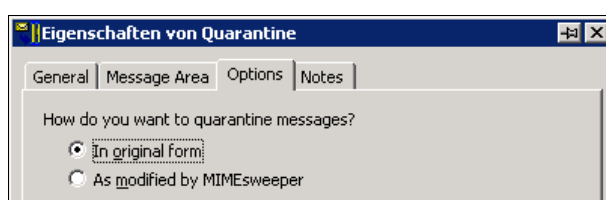
8. Schritt

Unter **Eigenschaften von Quarantine → Message Area** wählen Sie **Undetermined Messages** aus.



9. Schritt

Unter **Eigenschaften von Quarantine → Options** markieren Sie **In original form** und bestätigen die Einstellungen mit OK.



Erstellen der Scenario Folder für die Adressbasierte Verschlüsselung

Policy Editor → MIMesweeper for SMTP Policy → MIMesweeper for SMTP → Policies → Scenarios → Outgoing

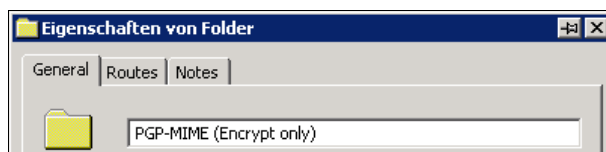
Beispielhaft wird hier die Erstellung eines Scenario Folders für die PGP/MIME-Verschlüsselung ohne Signatur beschrieben.

1. Schritt

Klicken Sie mit der rechten Maustaste auf den Scenario Folder **Outgoing** und wählen Sie dann **Neu → Folder**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

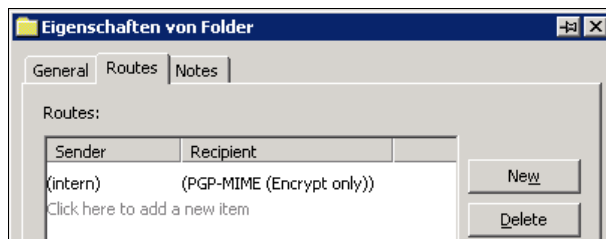
2. Schritt

Unter **Eigenschaften von Folder** → **General** geben Sie einen Namen an, welcher eine leichte Zuordnung zu jeweils verwendeten Funktion ermöglicht. In diesem Beispiel benutzen Sie **PGP-MIME (Encrypt only)**.



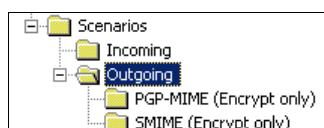
3. Schritt

Unter **Eigenschaften von Folder** → **Routes** geben Sie unter 'Sender' die Adressliste der internen Domänen (intern) an. Unter 'Recipient' wählen Sie die jeweilige Adressliste aus. In diesem Fall **PGP-MIME (Encrypt only)**. Anschließend bestätigen Sie mit OK.



4. Schritt

Die angelegten Folder werden anschließend in der Baumansicht unterhalb von Outgoing dargestellt.



Einrichten der CompanyCRYPT-Scenarios für die Adressbasierte Verschlüsselung

Policy Editor → MIMesweeper for SMTP Policy → MIMesweeper for SMTP → Policies → Scenarios → Outgoing

Beispielhaft wird hier die Erstellung eines Scenarios für die PGP/MIME-Verschlüsselung ohne Signatur beschrieben. Wird zur Erstellung der CompanyCRYPT-Scenarios der Scenario-Wizards verwendet, werden vordefinierte Einstellungen aus der Datei EXE.INI automatisch übernommen und die manuelle Zuordnung der Data Types entfällt. Zur Erläuterung der notwendigen Einstellungen wird im folgenden Beispiel auf die Verwendung des Scenario-Wizards verzichtet.

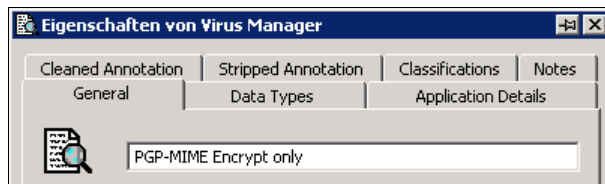
Zum Verständnis der folgenden Schritte sei erklärt, dass CompanyCRYPT wie ein weiterer Virens Scanner in den MIMesweeper eingebunden wird.

1. Schritt

Klicken Sie mit der rechten Maustaste auf den Scenario Folder **PGP-MIME (Encrypt only)** und wählen Sie dann **Neu → Virus Manager**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

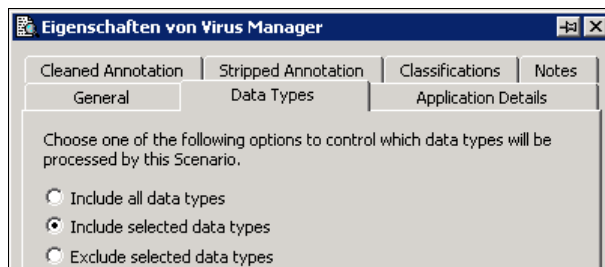
2. Schritt

Unter **Eigenschaften von Virus Manager** → **General** tragen Sie den Namen **PGP-MIME Encrypt only** ein.

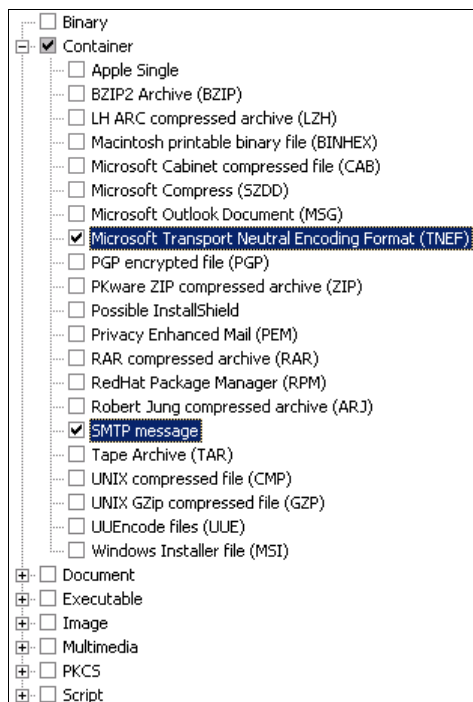


3. Schritt

Unter **Eigenschaften von Virus Manager** → **Data Types** wählen Sie die Option **Include selected data types**.

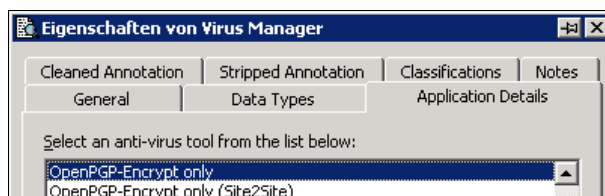


Bei der Auswahl der Data Types markieren Sie nur die beiden Container-Typen **Microsoft Transport Neutral Encoding Format (TNEF)** und **SMTP message**. Achten Sie darauf, dass keine weiteren Markierungen gesetzt sind.



4. Schritt

Unter **Eigenschaften von Virus Manager** → **Application Details** markieren Sie **OpenPGP-Encrypt only**.



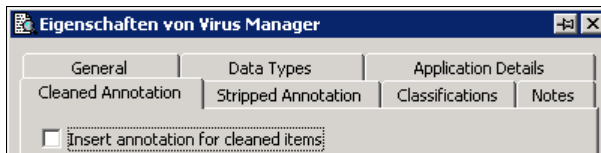
Aktivieren Sie anschließend die Option **Clean the detected virus** um eine Verschlüsselung des Mailinhaltes zu ermöglichen. Die Option 'Strip infected files' darf nicht aktiviert sein.



- ☒ Clean the detected virus:
☐ Strip infected files

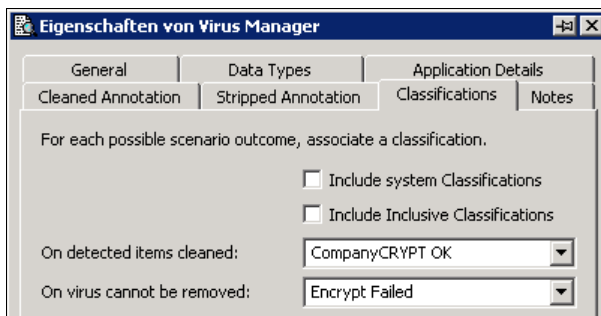
5. Schritt

Unter **Eigenschaften von Virus Manager** → **Cleaned Annotation** darf die Option 'Insert annotation for cleaned items' nicht aktiviert sein.



6. Schritt

Unter **Eigenschaften von Virus Manager** → **Classification** setzen Sie die Classifications **On detected items cleaned: CompanyCRYPT OK** (erfolgreiche Verschlüsselung) und **On virus cannot be removed: Encrypt failed** (fehlgeschlagene Verschlüsselung). Speichern Sie die Einstellungen mit OK.

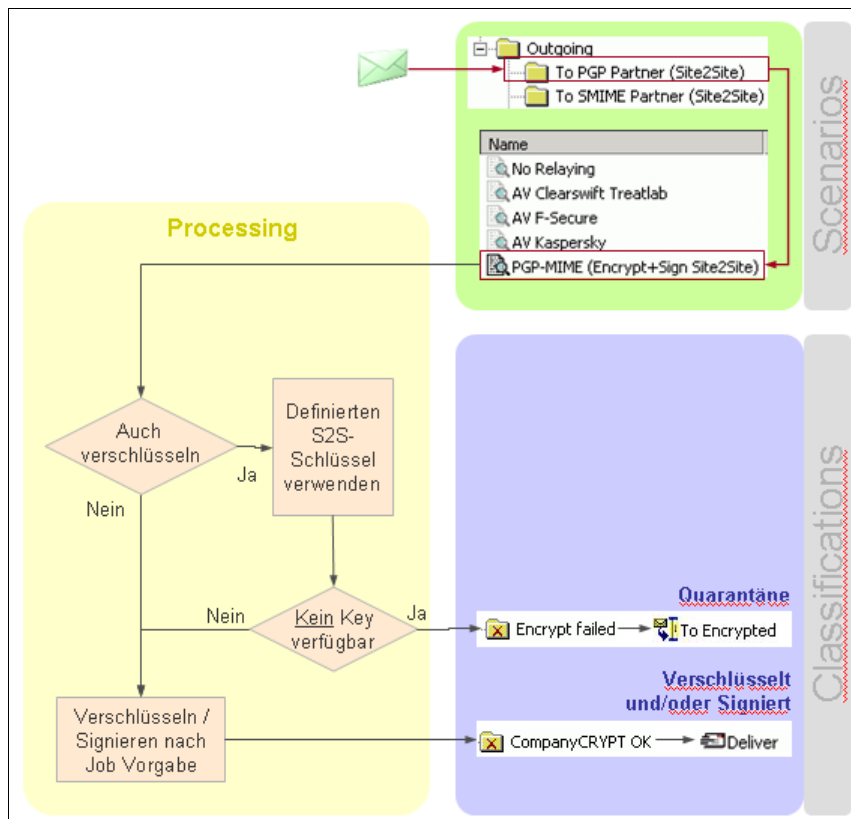




4.6. Site To Site Verschlüsselung

Die Site To Site Verschlüsselung ist eine spezielle Form der Adressbasierten Verschlüsselung. Der Administrator hinterlegt die gewünschten Verschlüsselungseinstellungen pro Domäne.

4.6.1. Funktionsbild – Site To Site Verschlüsselung



4.6.2. Einrichtungsschritte zusammengefasst

1. Schritt

Erzeugen Sie 2 neue 'Classifications' (falls noch nicht vorhanden) und verschieben Sie diese an das Ende der Classifications Liste (aber noch vor 'Clean').

- | | | |
|-----------------|---|--|
| CompanyCRYPT OK | → | Deliver Action |
| Encrypt failed | → | Quarantine Action zu beliebiger Message area |

2. Schritt

Erzeugen Sie im ausgehenden Szenario Ordner einen neuen Unterordner, z.B. PGP-MIME (Encrypt+Sign Site2Site).

3. Schritt

Erzeugen Sie in diesem Unterordner ein Virus Manager Job und wählen Sie z.B. **OpenPGP-Encrypt+Sign (Site2Site)**. Diesen verknüpfen Sie dann mit den erzeugten Classifications.

- | | | |
|----------------------------|---|-----------------|
| On detected items cleaned | → | CompanyCRYPT OK |
| On virus cannot be removed | → | Encrypt failed |

4. Schritt

Erzeugen Sie im CompanyCRYPT einen Site To Site Link für die gewünschte Domäne

Domain → Key

4.6.3. Einrichtung der Site To Site Verschlüsselung

Einrichten der Adresslisten für die Site To Site Verschlüsselung

Policy Editor → MIMesweeper for SMTP Policy → MIMesweeper for SMTP → Address Lists

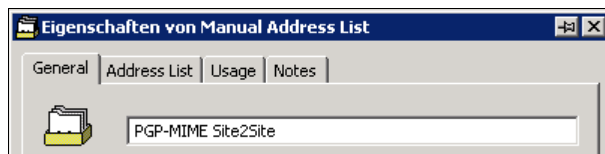
Beispielhaft wird hier die Erstellung einer Adressliste für die PGP-MIME Verschlüsselung ohne Signatur beschrieben.

1. Schritt

Klicken Sie mit der rechten Maustaste auf **Address List** und wählen Sie dann **Neu → Manual Address List**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards. Bei Verwendung des Wizards unterscheiden sich sowohl die dargestellten Fenster als auch die Reihenfolge der Schritte.

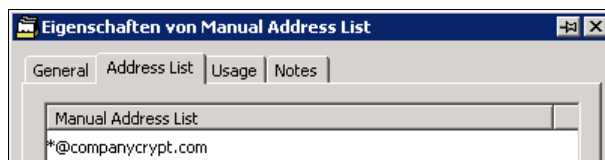
2. Schritt

Unter **Eigenschaften von Manual Address List** → **General** tragen Sie den Namen der Adressliste ein. In diesem Beispiel **PGP-MIME Site2Site**



3. Schritt

Unter **Eigenschaften von Manual Address List** → **Address List** tragen Sie unter Verwendung von Wildcards die eMailmaske der Empfängerdomäne ein, Beispiel: ***@companycrypt.com**. Speichern die Einstellungen mit OK.



4. Schritt

Die erstellte Adressliste wird anschließend in der Übersicht angezeigt.

Einrichten der Classifications für die Site To Site Verschlüsselung

Policy Editor → MIMesweeper for SMTP Policy → MIMesweeper for SMTP → Policies → Classifications

1. Schritt

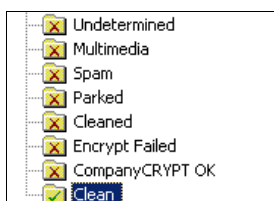
Klicken Sie mit der rechten Maustaste auf **Classifications** und wählen Sie dann **Neu → Classification** und benennen Sie die Classification **CompanyCRYPT OK**.

2. Schritt

Erstellen Sie nach dem gleichen Vorgehen eine weitere Classification und benennen Sie die Classification **Encrypt failed**.

3. Schritt

Die Classifications müssen nicht nach oben verschoben werden. Es ist jedoch zu beachten, dass beide Classifications unterhalb der Blocked-Classifications wie Virus oder Spam einzuordnen sind.



4. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **CompanyCRYPT OK** und wählen Sie **Neu → Deliver**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

5. Schritt

Unter **Eigenschaften von Deliver → General** geben Sie den Namen **Deliver** an und Bestätigen die Eingabe mit OK.

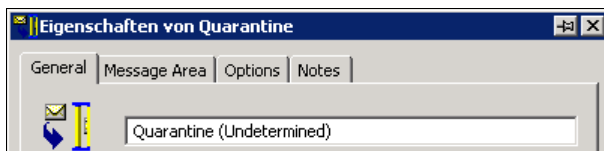


6. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **Encrypt failed** und wählen Sie **Neu → Quarantine**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

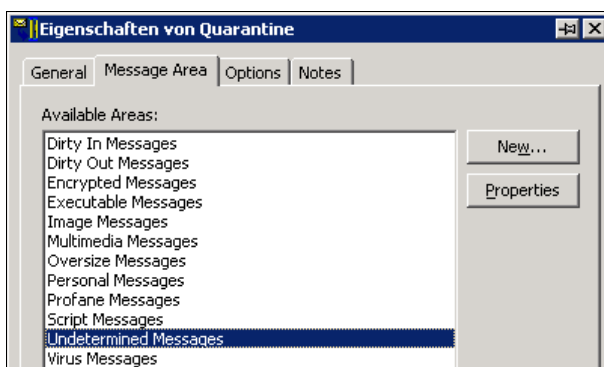
7. Schritt

Unter **Eigenschaften von Quarantine → General** geben Sie den Namen **Quarantine (Undetermined)** ein.



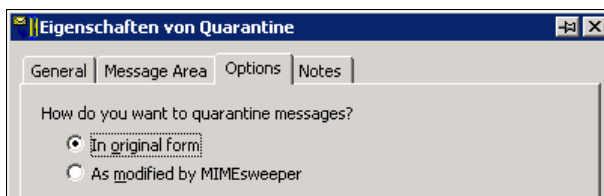
8. Schritt

Unter **Eigenschaften von Quarantine → Message Area** wählen Sie **Undetermined Messages** aus.



9. Schritt

Unter **Eigenschaften von Quarantine → Options** markieren Sie **In original form** und bestätigen die Einstellungen mit OK.



Erstellen der Scenario Folder für die Site To Site Verschlüsselung

Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Scenarios → Outgoing

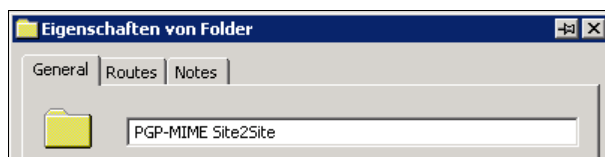
Beispielhaft wird hier die Erstellung eines Scenario Folders für die PGP/MIME-Verschlüsselung ohne Signatur beschrieben.

1. Schritt

Klicken Sie mit der rechten Maustaste auf den Scenario Folder **Outgoing** und wählen Sie dann **Neu → Folder**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

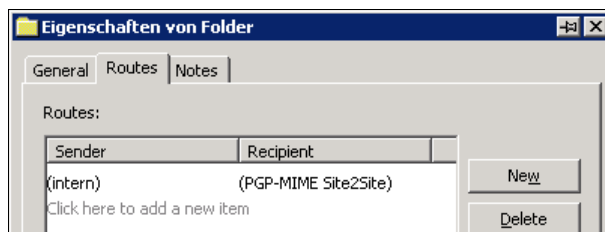
2. Schritt

Unter **Eigenschaften von Folder** → **General** geben Sie einen Namen an, welcher eine leichte Zuordnung zu jeweils verwendeten Funktion ermöglicht. In diesem Beispiel benutzen Sie **PGP-MIME Site2Site**.



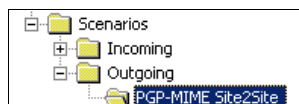
3. Schritt

Unter **Eigenschaften von Folder** → **Routes** geben Sie unter 'Sender' die Adressliste der internen Domänen (intern) an. Unter 'Recipient' wählen Sie die jeweilige Adressliste aus. In diesem Fall **PGP-MIME Site2Site**. Anschließend bestätigen Sie mit OK.



4. Schritt

Die angelegten Folder werden anschließend in der Baumansicht unterhalb von Outgoing dargestellt.



Einrichten der CompanyCRYPT-Scenarios für die Site To Site Verschlüsselung

Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Scenarios → Outgoing

Beispielhaft wird hier die Erstellung eines Scenarios für die PGP/MIME-Verschlüsselung ohne Signatur beschrieben. Wird zur Erstellung der CompanyCRYPT-Scenarios der Scenario-Wizards verwendet, werden vordefinierte Einstellungen aus der Datei EXE.INI automatisch übernommen und die manuelle Zuordnung der Data Types entfällt. Zur Erläuterung der notwendigen Einstellungen wird im folgenden Beispiel auf die Verwendung des Scenario-Wizards verzichtet.

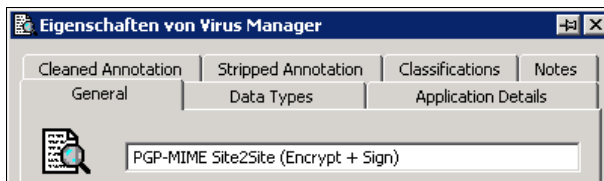
Zum Verständnis der folgenden Schritte sei erklärt, dass CompanyCRYPT wie ein weiterer Virens Scanner in den MIMESweeper eingebunden wird.

1. Schritt

Klicken Sie mit der rechten Maustaste auf den Scenario Folder **PGP-MIME Site2Site** und wählen Sie dann **Neu → Virus Manager**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

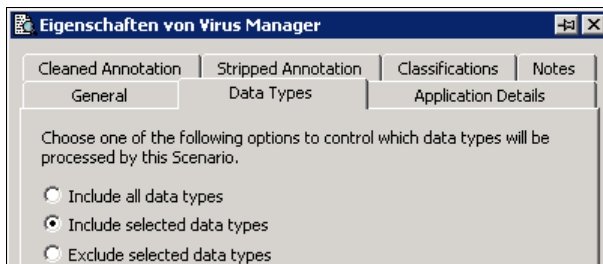
2. Schritt

Unter **Eigenschaften von Virus Manager** → **General** tragen Sie den Namen **PGP-MIME Site2Site (Encrypt + Sign)** ein.

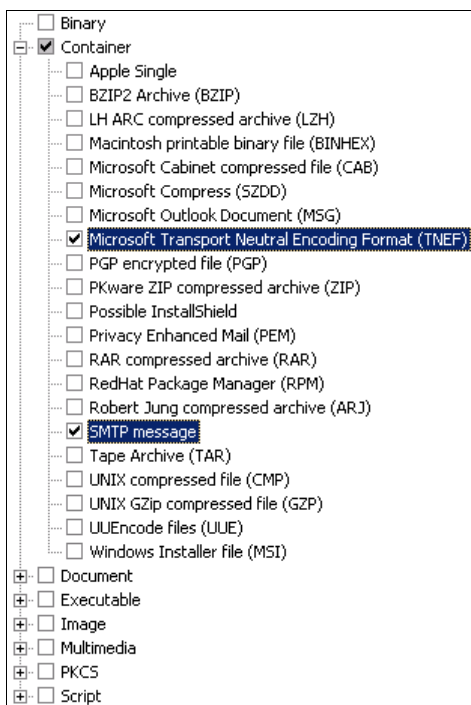


3. Schritt

Unter **Eigenschaften von Virus Manager** → **Data Types** wählen Sie die Option **Include selected data types**.

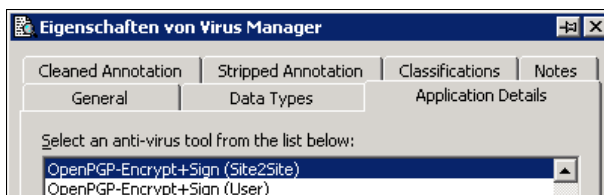


Bei der Auswahl der Data Types markieren Sie nur die beiden Container-Typen **Microsoft Transport Neutral Encoding Format (TNEF)** und **SMTP message**. Achten Sie darauf, dass keine weiteren Markierungen gesetzt sind.



4. Schritt

Unter **Eigenschaften von Virus Manager** → **Application Details** markieren Sie **OpenPGP-Encrypt only**.

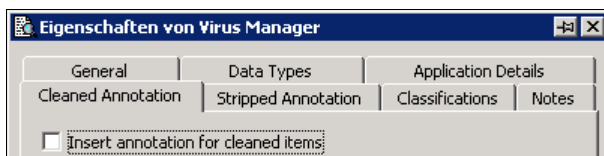


Aktivieren Sie anschließend die Option **Clean the detected virus** um eine Verschlüsselung des Mailinhaltes zu ermöglichen. Die Option 'Strip infected files' darf nicht aktiviert sein.

☒ Clean the detected virus
☐ Strip infected files

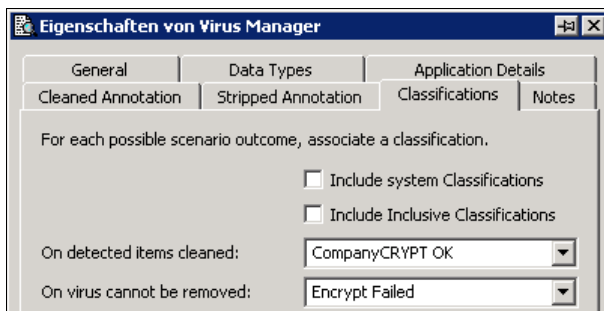
5. Schritt

Unter **Eigenschaften von Virus Manager** → **Cleaned Annotation** darf die Option 'Insert annotation for cleaned items' nicht aktiviert sein.



6. Schritt

Unter **Eigenschaften von Virus Manager** → **Classification** setzen Sie die Classifications **On detected items cleaned: CompanyCRYPT OK** (erfolgreiche Verschlüsselung) und **On virus cannot be removed: Encrypt failed** (fehlgeschlagene Verschlüsselung). Speichern Sie die Einstellungen mit OK.



Erzeugen eines Site to Site-Link

WebGUI → (Key Management) External

1. Schritt

Wählen Sie aus der Liste den Public Key für die Site to Site-Verbindung.

External Key Store						
Type	Expires	eMail	Name	Added		
[..any..]		[..any..]	[..any..]	[..any..]		
🔑	2024-04-27	administrator@klinikum-kemp...	Encryption Gateway Klinikverbund Kempten...	2014-05-05	📄	🔑
🔑	unlimited	AHG-CSA@ahg.de	AHG AG - Security CSA SYSTEM	2013-05-08	📄	🔑
🔑	unlimited	AlexanderStrobel@gmx.de	Alexander Strobel	2012-04-25	📄	🔑

2. Schritt

Klicken Sie bei den Key Properties auf **[+]** um alle Keyeigenschaften anzuzeigen.

PGP key properties

Name: Encryption Gateway Klinikverbund Kempten-Oberallgaeu

eMail: administrator@klinikum-kempten.de

Encrypt Alias:

Fingerprint: B788 262F 6C94 980B 6765 DD64 ABF4 D1F8 C695 2E03

Keystore ID: caf868a0-0cb1-ffcfe84d-21debd23

3. Schritt

Tragen Sie die gewünschte Zieldomäne beginnend mit ***@** in das Feld **Encrypt Alias** ein und klicken Sie auf den **Save**-Button.



Secure Internet Traffic



COMPANYCRYPT®
The encryption module for MIMESweeper

Einrichtung der Ver-/Entschlüsselung
Site To Site Verschlüsselung

Configuration Guide
CompanyCRYPT v1.5.0

PGP key properties	
Name	Encryption Gateway Klinikverbund Kempten-Oberallgaeu
eMail	administrator@klinikum-kempten.de
Encrypt Alias	*@klinikum-kempten.de
Fingerprint	B788 262F 6C94 980B 6765 DD64 ABF4 D1F8 C695 2E03
Keystore ID	caf868a0-0cb1-ffcfe84d-21debd23

[Sign key](#)
[Save](#)
[Delete Key](#)

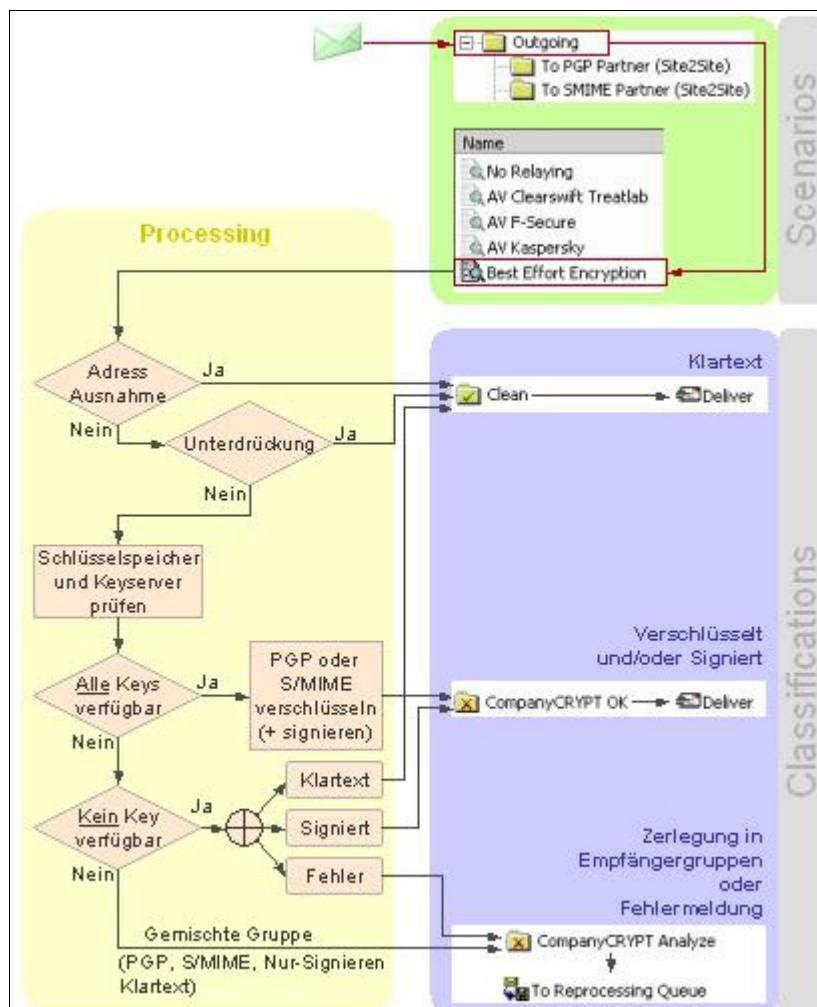
Neu erstellte Links werden sofort in der Listenansicht der Site to Site-Verbindungen angezeigt.



4.7. Automatische Verschlüsselung "Best Effort"

Die automatische Verschlüsselung und Signierung mittels Best Effort wird durch ein einzelnes Szenario im MIMESweeper for SMTP realisiert. Das gewünschte Verschlüsselungsformat wird anhand der vorhandenen Empfängerschlüssel automatisch durch CompanyCRYPT angewendet. Adresslisten sind nicht erforderlich.

4.7.1. Funktionsbild – Automatische Verschlüsselung (Best Effort)



4.7.2. Einrichtungsschritte zusammengefasst

1. Schritt

Erzeugen Sie 2 neue ‚Classifications‘ (falls noch nicht vorhanden) und verschieben Sie diese wie folgt:

CompanyCRYPT OK	→	Deliver Action	Direkt oberhalb der Classification 'Clean'
CompanyCRYPT Analyze	→	Save Action mit Ziel ‚Reprocessing‘	Über der obersten <u>ausgehenden</u> 'Deliver' Classification

2. Schritt

Erzeugen Sie im ausgehenden Szenario Ordner (z.B. Outgoing) ein Virus Manager Job und wählen Sie Best Effort Encryption. Diesen verknüpfen Sie dann mit den erzeugten Classifications.

On detected items cleaned	→	CompanyCRYPT OK
On virus cannot be removed	→	CompanyCRYPT Analyse

4.7.3. Einrichtung der Automatischen Verschlüsselung

Einrichten der Classifications für die automatische Verschlüsselung (Best Effort)

Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Classifications

1. Schritt

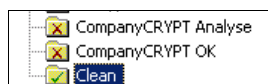
Klicken Sie mit der rechten Maustaste auf **Classifications** und wählen Sie dann **Neu → Classification** und benennen Sie die Classification **CompanyCRYPT OK**.

2. Schritt

Erstellen Sie nach dem gleichen Vorgehen eine weitere Classification und benennen Sie die Classification **CompanyCRYPT Analyse**.

3. Schritt

Verschieben Sie die Classification **CompanyCRYPT Analyse** in der Classification-Liste so, dass sie noch über der obersten Classification steht, die eine ausgehende Deliver Action enthält. Es ist jedoch zu beachten, dass beide Classifications unterhalb der Blocked-Classifications wie Virus oder Spam einzuordnen sind.



4. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **CompanyCRYPT OK** und wählen Sie **Neu → Deliver**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

5. Schritt

Unter **Eigenschaften von Deliver → General** geben Sie den Namen **Deliver** an und Bestätigen die Eingabe mit OK.

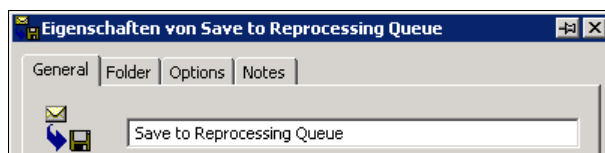


6. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **CompanyCRYPT Analyse** und wählen Sie **Neu → Save**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

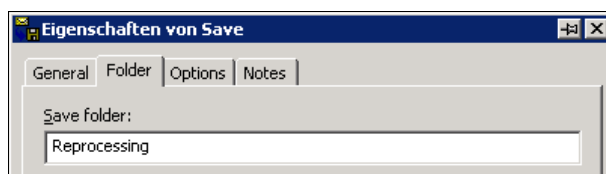
7. Schritt

Unter **Eigenschaften von Save → General** geben Sie den Namen **Save to Reprocessing Queue** ein



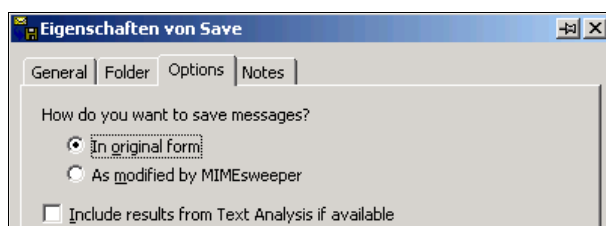
8. Schritt

Unter **Eigenschaften von Save → Folder** geben Sie den Folder-Namen **Reprocessing** an. Dieser Name muss den CompanyCRYPT-Einstellungen für den Reprocess Service entsprechen!



9. Schritt

Unter **Eigenschaften von Save** → **Options** markieren Sie die Option **In original form**. Include results from Text Analysis if available wird nicht markiert. Speichern Sie Einstellungen mit OK.



Erstellen des Szenarios für die automatische Verschlüsselung (Best Effort)

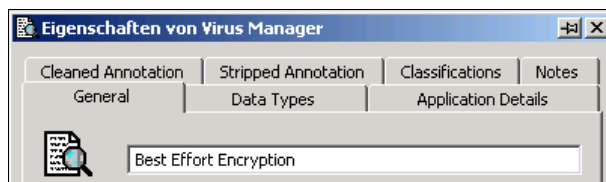
Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Scenarios → Outgoing

1. Schritt

Klicken Sie mit der rechten Maustaste auf den Scenario Folder **Outgoing** und wählen Sie dann **Neu** → **Virus Manager**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

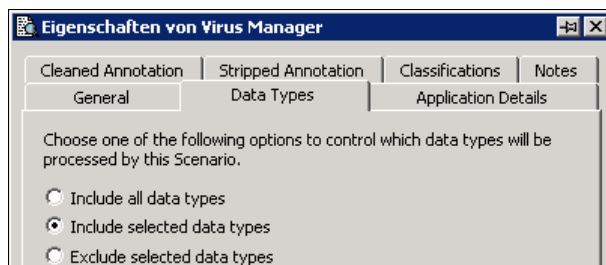
2. Schritt

Unter **Eigenschaften von Virus Manager** → **General** tragen Sie den Namen **Best Effort Encryption** ein.

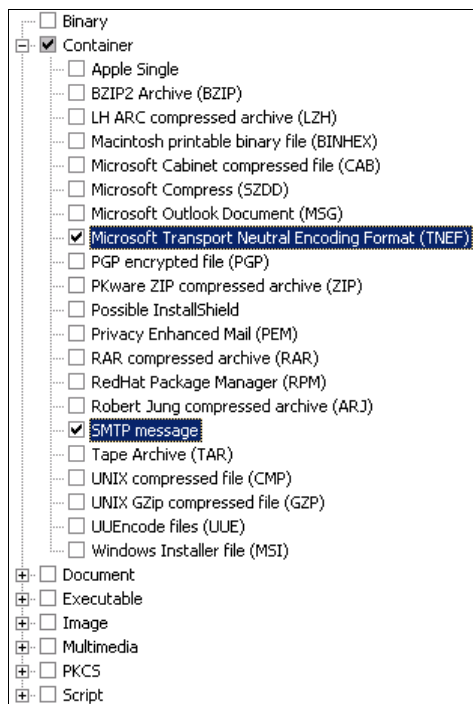


3. Schritt

Unter **Eigenschaften von Virus Manager** → **Data Types** wählen Sie die Option **Include selected data types**.

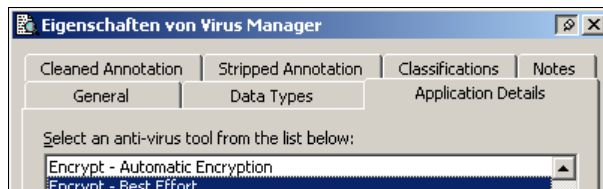


Bei der Auswahl der Data Types markieren Sie nur die beiden Container-Typen **Microsoft Transport Neutral Encoding Format (TNEF)** und **SMTP message**. Achten Sie darauf, dass keine weiteren Markierungen gesetzt sind.



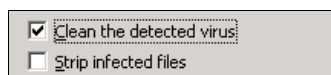
4. Schritt

Unter **Eigenschaften von Virus Manager** → **Application Details** markieren Sie **Encrypt – Best Effort**.



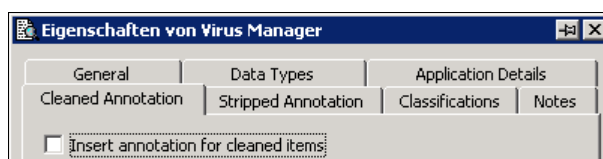
Hinweis: Wollen Sie den Modus Best Effort zusammen mit der Benutzergesteuerten Verschlüsselung nutzen, dann wählen Sie den Eintrag **Encrypt – Automatic Encryption** aus.

Aktivieren Sie anschließend die Option **Clean the detected virus** um eine Verschlüsselung des Mailinhaltes zu ermöglichen. Die Option 'Strip infected files' darf nicht aktiviert sein.



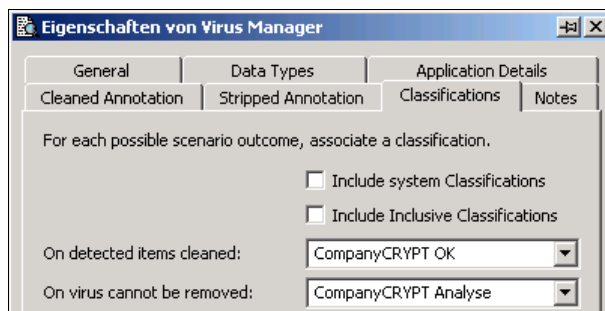
5. Schritt

Unter **Eigenschaften von Virus Manager** → **Cleaned Annotation** darf die Option 'Insert annotation for cleaned items' nicht aktiviert sein.



6. Schritt

Unter **Eigenschaften von Virus Manager** → **Classification** setzen Sie die Classifications **On detected items cleaned: CompanyCRYPT OK** und **On virus cannot be removed: CompanyCRYPT Analyse**. Speichern Sie die Einstellungen mit OK.

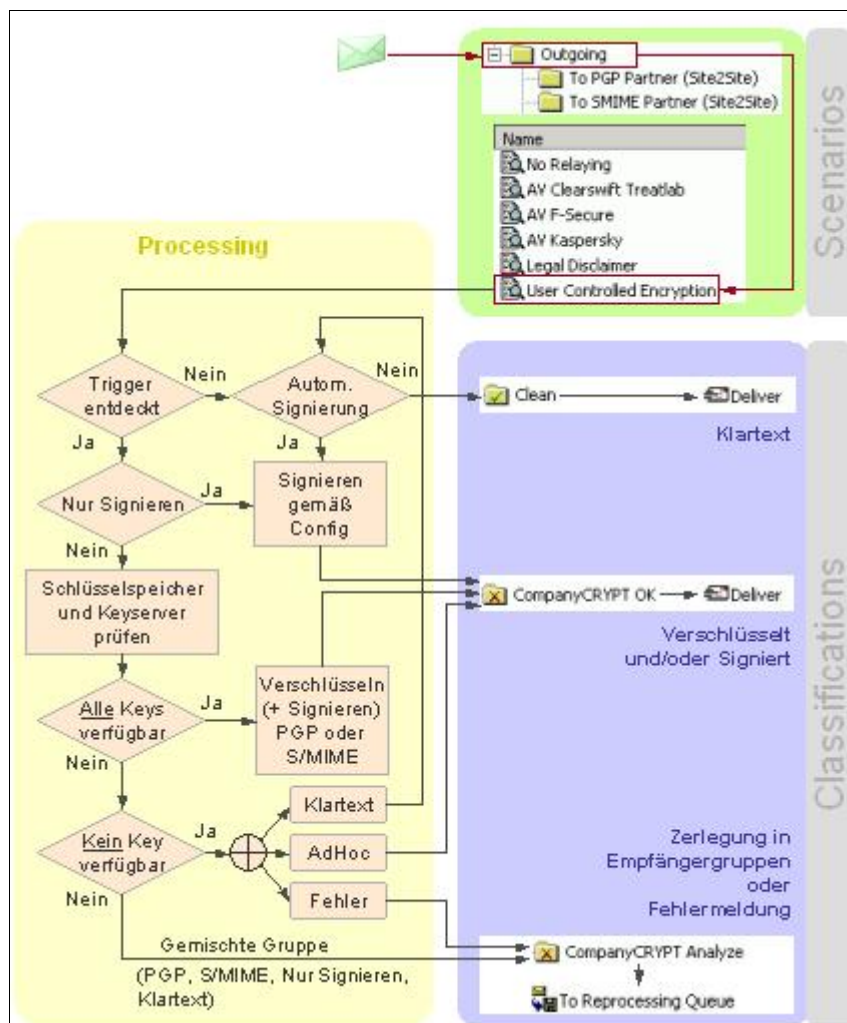




4.8. Anwender gesteuerte Verschlüsselung "User Control"

Die Anwendergesteuerte Verschlüsselung wird durch ein einzelnes Szenario „Encryption – User Control“ oder als Zusatzfunktion innerhalb des Szenarios „Encryption – Best Effort + User Control“ im MIMESweeper for SMTP realisiert. Im letzteren Fall führt die Erkennung eines eingestellten Triggers (Betreffzeile, Header) dazu, dass das Szenario als „User Control“ durchgeführt wird. Das gewünschte Verschlüsselungsformat wird anhand der vorhandenen Empfängerschlüssel automatisch durch CompanyCRYPT angewendet. Adresslisten sind nicht erforderlich.

4.8.1. Funktionsbild – Anwender gesteuerte Verschlüsselung (User Control)



4.8.2. Einrichtungsschritte zusammengefasst

1. Schritt

Erzeugen Sie 2 neue ‚Classifications‘ (falls noch nicht vorhanden) und verschieben Sie diese wie folgt:

CompanyCRYPT OK	→	Deliver Action	Oberhalb der Classification 'Clean'
CompanyCRYPT Analyse	→	Save Action mit Ziel ‚Reprocessing‘	Über der obersten <u>ausgehenden</u> 'Deliver' Classification

2. Schritt

Erzeugen Sie im ausgehenden Szenario Ordner (z.B. Outgoing) einen Virus Manager Job und wählen Sie User Controlled Encryption. Diesen verknüpfen Sie dann mit den erzeugten Classifications.

On detected items cleaned	→	CompanyCRYPT OK
On virus cannot be removed	→	CompanyCRYPT Analyse

3. Schritt

Konfigurieren Sie die Aktivierungsoption für die Benutzersteuerung.

Mailoption aktivieren	→	Vertraulich
-----------------------	---	-------------

4.8.3. Einrichtung der Anwendergesteuerten Verschlüsselung

Einrichten der Classifications für die Anwender gesteuerte Verschlüsselung

Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Classifications

1. Schritt

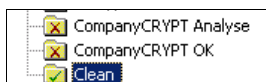
Klicken Sie mit der rechten Maustaste auf **Classifications** und wählen Sie dann **Neu → Classification** und benennen Sie die Classification **CompanyCRYPT OK**.

2. Schritt

Erstellen Sie nach dem gleichen Vorgehen eine weitere Classification und benennen Sie die Classification **CompanyCRYPT Analyse**.

3. Schritt

Verschieben Sie die Classification **CompanyCRYPT Analyse** in der Classification-Liste so, dass sie noch über der obersten Classification steht, die eine ausgehende Deliver Action enthält. Es ist jedoch zu beachten, dass beide Classifications unterhalb der Blocked-Classifications wie Virus oder Spam einzuordnen sind.

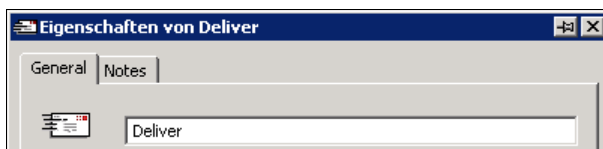


4. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **CompanyCRYPT OK** und wählen Sie **Neu → Deliver**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

5. Schritt

Unter **Eigenschaften von Deliver** → **General** geben Sie den Namen **Deliver** an und Bestätigen die Eingabe mit OK.

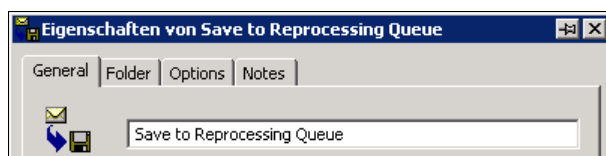


6. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **CompanyCRYPT Analyse** und wählen Sie **Neu → Save**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

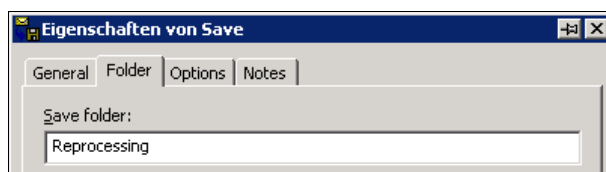
7. Schritt

Unter **Eigenschaften von Save** → **General** geben Sie den Namen **Save to Reprocessing Queue** ein



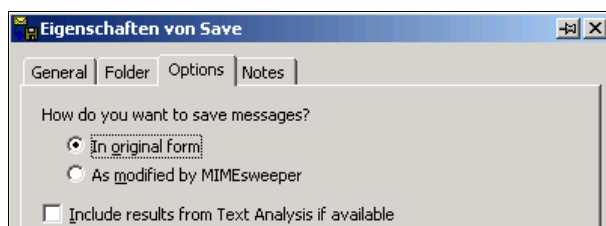
8. Schritt

Unter **Eigenschaften von Save** → **Folder** geben Sie den Folder-Namen **Reprocessing** an. Dieser Name muss den CompanyCRYPT-Einstellungen für den Reprocess Service entsprechen!



9. Schritt

Unter **Eigenschaften von Save** → **Options** markieren Sie die Option **In original form**. Include results from Text Analysis if available wird nicht markiert. Speichern Sie Einstellungen mit OK.



Erstellen des Szenarios für die Anwender gesteuerte Verschlüsselung (User Control)

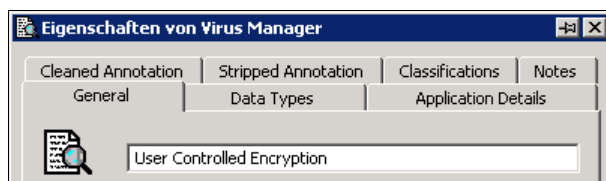
Policy Editor → MIMesweeper for SMTP Policy → MIMesweeper for SMTP → Policies → Scenarios → Outgoing

1. Schritt

Klicken Sie mit der rechten Maustaste auf den Scenario Folder **Outgoing** und wählen Sie dann **Neu** → **Virus Manager**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

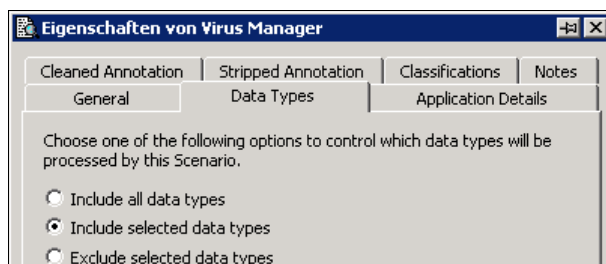
2. Schritt

Unter **Eigenschaften von Virus Manager** → **General** tragen Sie den Namen **User Controlled Encryption** ein.

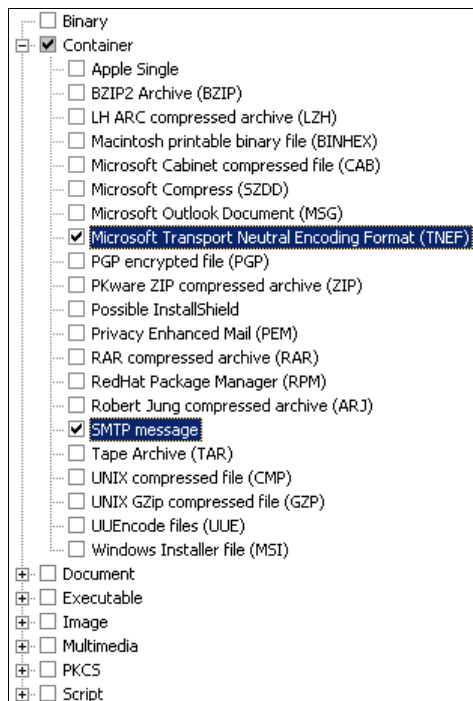


3. Schritt

Unter **Eigenschaften von Virus Manager** → **Data Types** wählen Sie die Option **Include selected data types**.

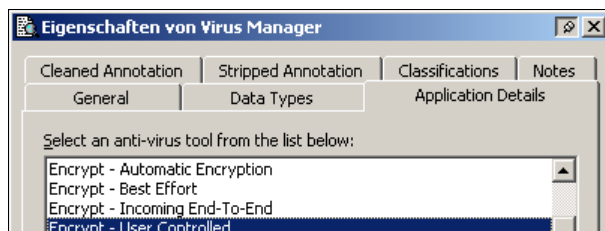


Bei der Auswahl der Data Types markieren Sie nur die beiden Container-Typen **Microsoft Transport Neutral Encoding Format (TNEF)** und **SMTP message**. Achten Sie darauf, dass keine weiteren Markierungen gesetzt sind.



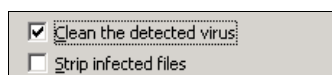
4. Schritt

Unter **Eigenschaften von Virus Manager** → **Application Details** markieren Sie **Encrypt – User Controlled**.



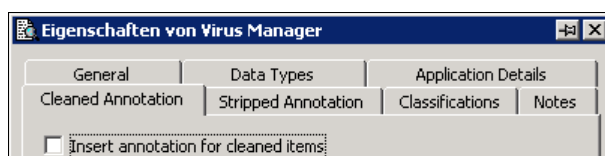
Hinweis: Wollen Sie den Modus Best Effort zusammen mit der Benutzergesteuerten Verschlüsselung nutzen, dann wählen Sie den Eintrag **Encrypt – Automatic Encryption** aus.

Aktivieren Sie anschließend die Option **Clean the detected virus** um eine Verschlüsselung des Mailinhaltes zu ermöglichen. Die Option 'Strip infected files' darf nicht aktiviert sein.



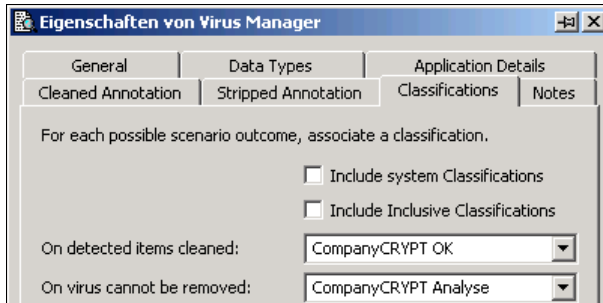
5. Schritt

Unter **Eigenschaften von Virus Manager** → **Cleaned Annotation** darf die Option 'Insert annotation for cleaned items' nicht aktiviert sein.



6. Schritt

Unter **Eigenschaften von Virus Manager** → **Classification** setzen Sie die Classifications **On detected items cleaned: CompanyCRYPT OK** und **On virus cannot be removed: CompanyCRYPT Analyse**. Speichern Sie die Einstellungen mit OK.



Aktivieren der Benutzersteuerung

WebGUI → (Configuration) policies → User Control

1. Schritt

Klicken Sie zuerst auf den Button **More Options** um zu den erweiterten Einstellungen für die Benutzersteuerung zu gelangen.

2. Schritt

Aktivieren Sie das Kontrollkästchen **by subject keyword** und vergeben Sie ein Schlüsselwort für die Betreffzeile. Vorschlag: **[encrypt]**. Aktivieren Sie ebenfalls die Option **by email property** und den **Confidential**.

Let user activate Encryption: <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 40%;"> <input checked="" type="checkbox"/> by email property <input checked="" type="checkbox"/> by subject keyword: </div> <div style="width: 50%;"> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <i>'Sensitivity':</i> <input checked="" type="checkbox"/> 'Confidential' <input type="checkbox"/> 'Personal' <input type="checkbox"/> 'Private' </div> <div style="width: 5%; text-align: center;"> <input type="checkbox"/> Case sensitive </div> </div> <div style="border: 1px solid #ccc; padding: 2px; width: 45%;">[encrypt]</div> </div> </div>
--

Let user activate Encryption:

- | | |
|---------------------|---|
| By email property: | Die Aktivierung kann über Eigenschaften der eMail erfolgen. Die Markierung der Nachricht mit den dazugehörigen Eigenschaften ‚Vertraulich‘, ‚Persönlich‘ oder ‚Privat‘ wird im eMail-Programm durchgeführt. |
| By subject keyword: | Schlüsselwort für die Aktivierung der Verschlüsselung, welches in der Betreffzeile der Mail angegeben werden muss (Betreffzeilensteuerung) |
| Case sensitive: | Aktiviert/Deaktiviert die Unterscheidung von Groß- und Kleinbuchstaben für die Betreffzeilensteuerung |

3. Schritt

Um sicherzustellen, dass die Mail in jedem Fall verschlüsselt verschickt wird, kontrollieren Sie unter **Encryption method** die aktiven Einstellungen **If possible use PGP or S/MIME** und als Alternative **Encrypt Ad Hoc**.

Encryption method: <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 40%;"> <input type="radio"/> Ad Hoc encryption only <input checked="" type="radio"/> If possible use PGP or S/MIME, else: </div> <div style="width: 55%;"> <input checked="" type="radio"/> Encrypt AdHoc using <i>Secure ZIP</i> <input type="radio"/> Stop with 'Encrypt Fail' <input type="radio"/> Send unencrypted </div> </div>
--

- | | |
|--------------------------------------|--|
| Encryption method: | Auswahl des Verschlüsselungsformats |
| Ad Hoc encryption only: | Die Mail wird mit der Ad Hoc Verschlüsselungsmethode verschlüsselt, unabhängig davon, ob für den/die Empfänger ein Schlüssel vorhanden ist. |
| if possible use PGP or S/MIME, else: | Wenn für den/die Empfänger durchgängig PGP oder S/MIME Schlüssel vorhanden sind, dann wird mit der jeweiligen Methode verschlüsselt. |
| Encrypt Ad Hoc: | Ist für einen Empfänger kein PGP oder S/MIME-Schlüssel vorhanden, so wird die konfigurierte Ad Hoc Verschlüsselung angewendet. Das gewählte Format wird angezeigt. |
| Stop with Encrypt Fail: | Die Mail wird mit „Verschlüsselungsfehler“ geblockt, wenn für einen Empfänger kein PGP oder S/MIME-Schlüssel vorhanden ist. |



Secure Internet Traffic



COMPANYCRYPT®
The encryption module for MIMesweeper

Einrichtung der Ver-/Entschlüsselung
Anwender gesteuerte Verschlüsselung "User Control"

Configuration Guide
CompanyCRYPT v1.5.0

Send unencrypted: Der Versand erfolgt unverschlüsselt, sofern für einen Empfänger kein PGP oder S/MIME-Schlüssel vorhanden ist.

4. Schritt

Speichern Sie die Änderung mit **Apply Changes**.



Secure Internet Traffic



COMPANYCRYPT®
The encryption module for MIMESweeper

Einrichtung der Ver-/Entschlüsselung
Einrichtung der Signierung

Configuration Guide
CompanyCRYPT v1.5.0

4.9. Einrichtung der Signierung

Hierzu sind keine gesonderten Einrichtungsschritte erforderlich. Je nach vorliegender Konfiguration muss aus den folgenden Optionen gewählt werden.

Adressbasierte Signierung

Analog zur Einrichtung der Adressbasierten Verschlüsselung, wählen Sie lediglich den gewünschten „Sign-Only“ Job oder modifizieren den bereits gewählten Verschlüsselungs-Job zu der vergleichbaren „... + sign...“-Variante.

Automatische Signierung „Company Signing“

Mit Einrichtung der CompanyCRYPT-Scenarios „Automatic Encryption“, „Best Effort“ oder „User Control“ im MIMESweeper ist bereits alles eingerichtet, was zur zusätzlichen oder ausschließlichen Signierung von Nachrichten erforderlich ist.

Die entsprechende Funktion muss lediglich in der CompanyCRYPT-Konfiguration aktiviert bzw. gewählt werden (vergl. 3.4.4 Automatische Signierung „Company Signing“). Hierbei können verschlüsselte oder Klartext Nachrichten unterschiedlich behandelt werden. Liegt bereits eine verschlüsselte Nachricht vor, erfolgt die Signierung mit dem gleichen Verfahren (OpenPGP oder S/MIME).

Aktivierung durch Schlüsselwort (Betreffzeilensteuerung)

Innerhalb des CompanyCRYPT-Scenarios „User Control“ kann der Benutzer durch Angabe eines Schlüsselwortes in der Betreffzeile die Signierung durch CompanyCRYPT aktivieren (Vergleiche vorheriges Kapitel). Die entsprechende Funktion muss lediglich in der CompanyCRYPT-Konfiguration aktiviert bzw. eingestellt werden (vergl. 3.4.3 Benutzergesteuerte Verschlüsselung und/oder Signierung unterer Abschnitt).

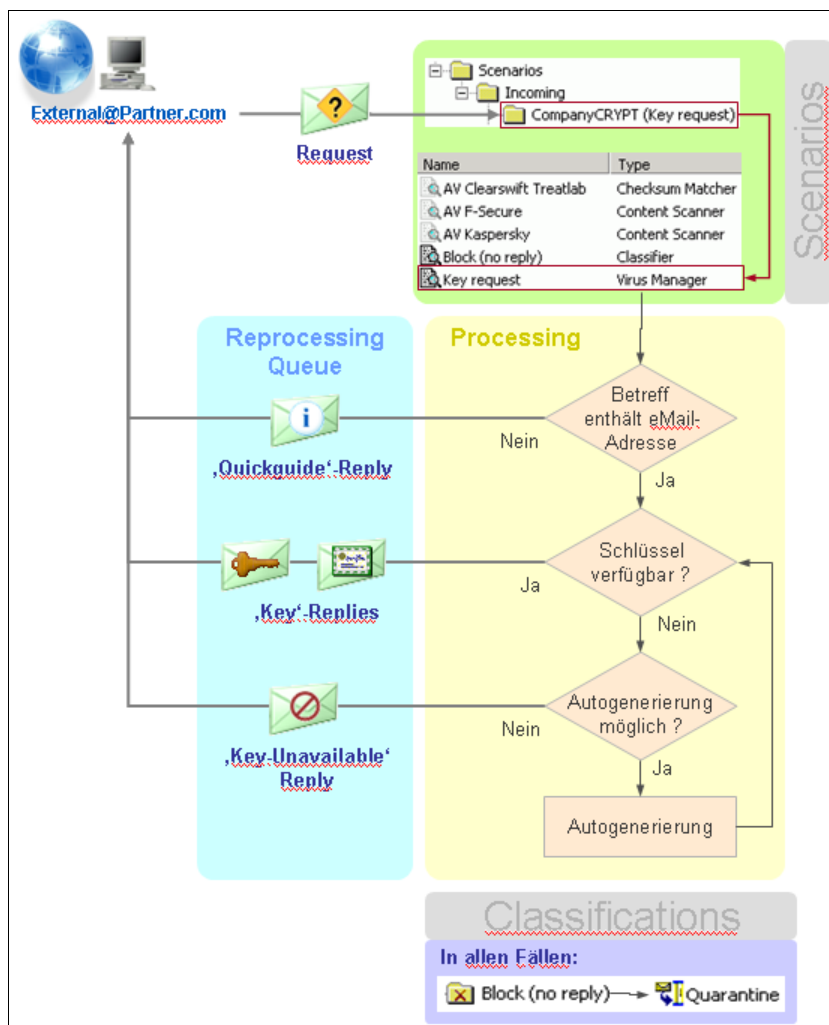


4.10. Keyresponder (MIKE - Mail Initiated Key Exchange)

Das 'Keyserver-Szenario' analysiert die Betreffzeile und sendet Antwort-eMails an den Sender zurück. Der Inhalt der Antworten ist abhängig von den folgenden Bedingungen:

- Anmerkung 1:** Dieses Szenario prüft immer auf neue (unbekannte) Schlüssel und extrahiert diese.
- Anmerkung 2:** Die Antworten 'Kein Schlüssel verfügbar' und 'Kurzanleitung' können durch ein anderes Schlüsselwort unterdrückt werden. Lesen sie hierzu das Kapitel 3 Schlüsselverteilung und die Option 'Inhibit other replies by'.

4.10.1. Funktionsbild – Keyresponder für externe Partner



4.10.2. Einrichtungsschritte zusammengefasst

1. Schritt

Erzeugen Sie eine neue 'Classification'.

Keyserver → Quarantine Action zu beliebiger Message area

2. Schritt

Erzeugen Sie im eingehenden Szenario Ordner einen Unterordner mit folgender Adresskombination.

CompanyCRYPT (Key request): *@* → z.B. Keyserver@<Mycompany.com>

3. Schritt

Erzeugen Sie in dem neuen Unterordner ein Virus Manager Job und wählen Sie External Keyserver. Diesen verknüpfen Sie dann mit den erzeugten Classification.

On detected → Keyserver

4. Schritt

Erzeugen Sie in dem neuen Unterordner zusätzlich ein Classifier-Szenario und verknüpfen Sie diese ebenfalls mit den erzeugten Classification → Keyserver

4.10.3. Einrichtung des Keyresponders

Einrichten der Classification für automatischen Schlüsselaustausch

Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Classifications

Für die Funktionalität des Schlüsselaustausches, ist es nicht erforderlich, eine neue Classification einzurichten. Benötigt wird eine Classification die keine Reply, Deliver oder sonstige Zustelloptionen enthält.

1. Schritt

Klicken Sie mit der rechten Maustaste auf **Classifications** und wählen Sie dann **Neu → Classification** und benennen Sie die Classification **CompanyCRYPT Key Request**.

2. Schritt

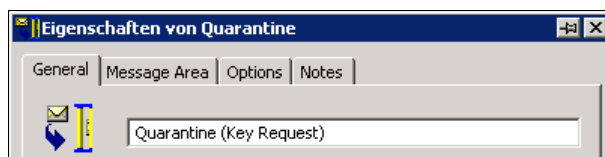
Verschieben Sie nun die Classification **CompanyCRYPT Key Request** über die Encrypted-Classification.

3. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **CompanyCRYPT Key Request** und wählen Sie **Neu → Quarantine**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

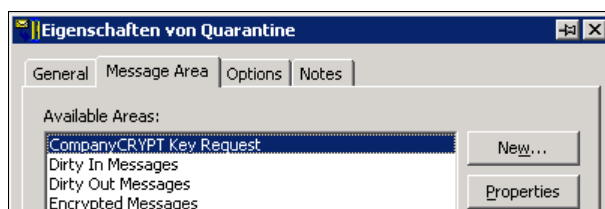
4. Schritt

Unter **Eigenschaften von Quarantine → General** geben Sie den Namen **Quarantine (Key Request)** ein.



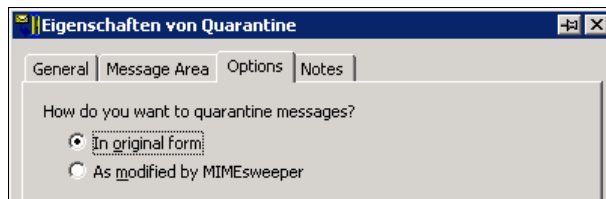
5. Schritt

Unter **Eigenschaften von Quarantine → Message Area** wählen Sie eine vorhandene Message Area aus oder legen Sie eine neuen an. In unserem Beispiel mit dem Namen **CompanyCRYPT Key Request**.



6. Schritt

Unter **Eigenschaften von Quarantine → Options** markieren Sie **In original form** und bestätigen die Einstellungen mit OK.



Erstellen des Scenario Folder für automatischen Schlüsselaustausch

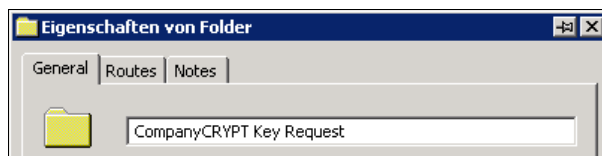
Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Scenarios → Incoming

1. Schritt

Klicken Sie mit der rechten Maustaste auf den Scenario Folder **Incoming** und wählen Sie dann **Neu → Folder**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

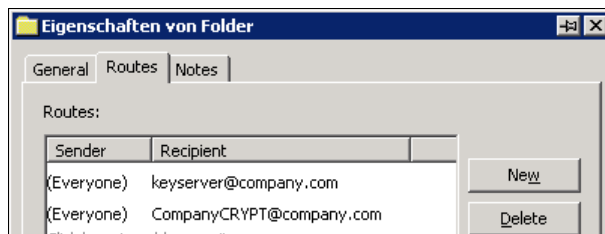
2. Schritt

Unter **Eigenschaften von Folder → General** geben Sie einen Namen an, welcher eine leichte Zuordnung zu jeweils verwendeten Funktion ermöglicht. In diesem Beispiel benutzen Sie **CompanyCRYPT Key Request**.



3. Schritt

Unter **Eigenschaften von Folder → Routes** wählen Sie unter Sender die Adressliste (Internet) bzw. (Everyone) für alle externen User aus. Unter Recipient geben Sie die gewünschte interne eMailadresse für Keyrequests an (CompanyCRYPT Listener Address). Zusätzlich muss die „CompanyCRYPT Sender Address“ hinterlegt werden. Anschließend bestätigen Sie mit OK.



4. Schritt

Der angelegte Folder wird anschließend in der Baumansicht unterhalb von Incoming dargestellt.



Einrichten des Keyresponder-Scenario (MIKE - Mail Initiated Key Exchange)

Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Scenarios → Incoming

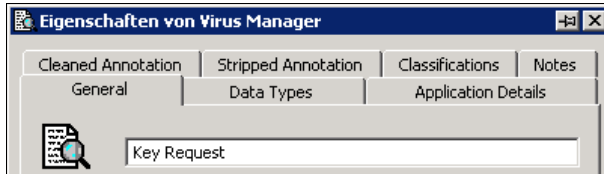
Wird zur Erstellung der CompanyCRYPT-Scenarios der Scenario-Wizards verwendet, werden vordefinierte Einstellungen aus der Datei EXE.INI automatisch übernommen und die manuelle Zuordnung der Data Types entfällt. Zur Erläuterung der notwendigen Einstellungen wird im folgenden Beispiel auf die Verwendung des Scenario-Wizards verzichtet.

1. Schritt

Klicken Sie mit der rechten Maustaste auf den Scenario Folder **CompanyCRYPT Key Request** und wählen Sie dann **Neu → Virus Manager**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

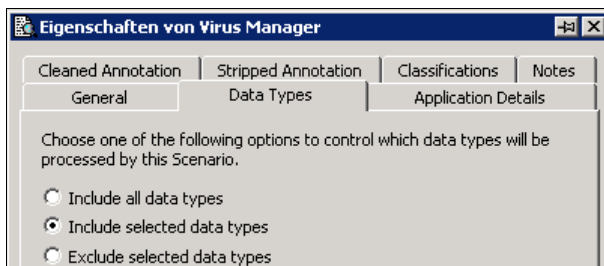
2. Schritt

Unter **Eigenschaften von Virus Manager** → **General** tragen Sie den Namen **Key Request** ein.

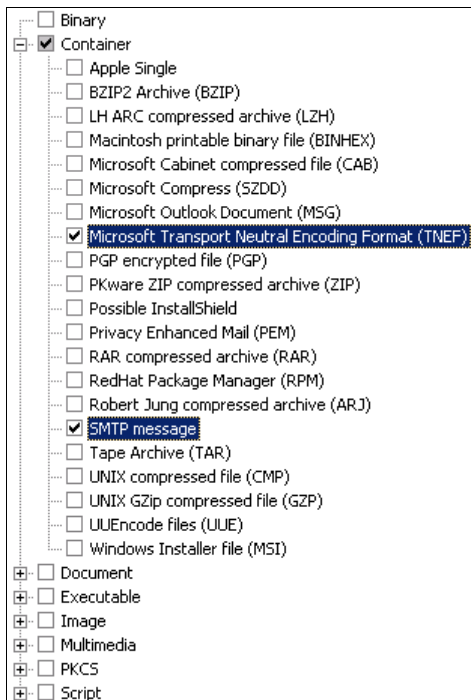


3. Schritt

Unter **Eigenschaften von Virus Manager** → **Data Types** wählen Sie die Option **Include selected data types**.

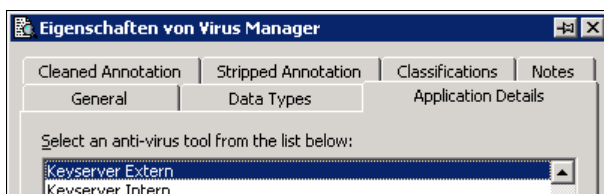


Bei der Auswahl der Data Types markieren Sie nur die beiden Container-Typen **Microsoft Transport Neutral Encoding Format (TNEF)** und **SMTP message**. Achten Sie darauf, dass keine weiteren Markierungen gesetzt sind.



4. Schritt

Unter **Eigenschaften von Virus Manager** → **Application Details** markieren Sie das entsprechende CompanyCRYPT-Szenario **Keyserver Extern**.

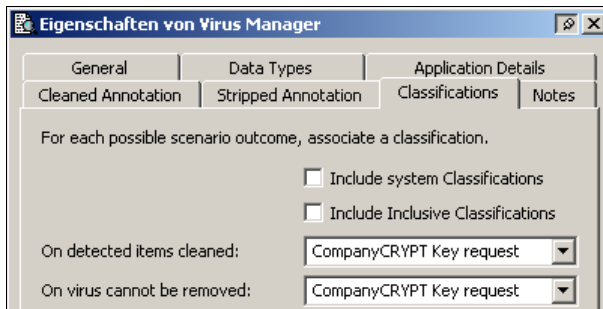


Markieren Sie die Option **Clean the detected virus**.

☒ Clean the detected virus
☐ Strip infected files

5. Schritt

Unter **Eigenschaften von Virus Manager** → **Classification** weisen Sie den Optionen **On detected items cleaned** und **On virus cannot be removed** die Classification **CompanyCRYPT Key Request** zu. Speichern Sie die Einstellungen mit OK.



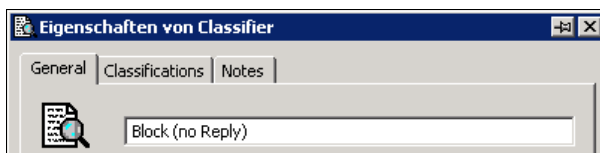
Um eine Weiterverarbeitung der eigentlichen Mail durch MIMESweeper-Routinen zu unterbinden, sollte das Keyserver-Szenario auf eine Classification verweisen, welche keine Reply, Deliver oder sonstige Zustelloptionen enthält.

6. Schritt

Klicken Sie mit der rechten Maustaste auf den Scenario Folder **CompanyCRYPT Key Request** und wählen Sie dann **Neu** → **Classifier**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

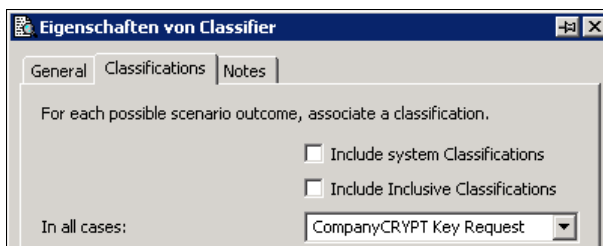
7. Schritt

Unter **Eigenschaften von Classifier** → **General** tragen Sie den Namen **Block (no Reply)** ein.



8. Schritt

Unter **Eigenschaften von Classifier** → **Classification** wählen Sie die Classification **CompanyCRYPT Key Request**, die gleiche wie für das Keyserver-Szenario.



Wenn das Keyserver-Szenario keinen Befund zurückliefert, dann dient der Classifier zur Sicherheit und verhindert eine Weiterverarbeitung der eigentlichen Mail durch MIMESweeper-Routinen.

9. Schritt

Deaktivieren Sie im Scenario Folder **CompanyCRYPT Key Request** alle anderen CompanyCRYPT-Szenarios. Klicken Sie diese Szenarien mit der rechten Maustaste an und entfernen Sie den Haken vor dem Punkt Enable.

Name	Type	Enabled
Block Executables	Data Type Manager ...	No
Block MS Class 1 file extensions	File Detector (Inclusi...	No
CompanyCRYPT Decrypt	Virus Manager (Inclu...	No
Key Request	Virus Manager (Inclu...	Yes
Block (no Reply)	Classifier (Exclusive)	Yes



Adresskonfiguration für automatischen Schlüsselsversand

WebGUI → (Configuration) Key Server → MIKE

1. Schritt

Definieren Sie die Adressen für den mailbasierten Keyserver. Tragen Sie in das Feld **Listener Address** die Adresse ein, unter welcher der Keyserver erreichbar ist. Unter **Sender Address** definieren Sie die Antwortadresse (Absenderadresse) für den Keyserver.

MIKE (Mail Initiated Key Exchange)	
Listener Address:	<input type="text" value="keyserver@company.com"/>
Sender Address:	<input type="text" value="CompanyCRYPT@company.com"/>
Send only - If addressed to, no reply is generated. Used as sender address for 'Key-Unavailable' and 'Quickguide' notifications.	

Listener Address: Mails an diese Adresse werden als Schlüsselanforderungen durch MIKE verarbeitet.

Sender Address: Ist ein angeforderte Schlüssel nicht vorhanden, so wird eine Information (Reply) unter dieser Mailadresse an den Anfordernden verschickt. Mails an diese Adresse werden von MIKE ignoriert, um Mail-Loops zu vermeiden, ausgelöst durch Spam bzw. Mails mit ungültigen Absendern.

Wichtig: Verwenden Sie für die Felder **Listener Address** und **Sender Address** bitte die gleichen Angaben wie bei der Routendefinition für den Folder CompanyCRYPT Key Request im MIMESweeper.

Sender	Recipient
(Everyone)	keyserver@company.com
(Everyone)	CompanyCRYPT@company.com

2. Schritt

Die übrigen Einstellungen können Sie auf den Standardwerten belassen. Speichern Sie die Änderungen mit **Apply Changes**.

Local / Internal domains:	<input type="text" value="@CompanyCRYPT.com"/>	Requests from these domains are considered internal. (Enter additional domains beginning with '@'.)
	<input type="text" value="@sit-internet.com"/> <input type="text" value="@netformat.de"/>	
Send Keys/Certificates:	From: <input checked="" type="radio"/> User address = <input type="text" value="The address of the Key owner"/> <input type="radio"/> Sender address = <input type="text" value="companycrypt@CompanyCRYPT.com"/>	
Language:	<input type="text" value="DEU"/>	
	<input type="checkbox"/> Apply ZIP compression on attachments (Recipient with MS Outlook may require this to access key material.)	
S/MIME key reply option:	<input checked="" type="checkbox"/> Always sign S/MIME reply with user key. (Recipients may be able to import key from signature.)	
Quickguide option:	Avoid reply by subject keyword <input type="text" value="public key"/> <input type="checkbox"/> Case sensitive	

Local / Internal Domains: Hier werden alle intern verwalteten Internetdomänen angegeben. Diese Information dient zur Unterscheidung, ob der Keyserver von Intern oder von Extern angesprochen wird.

Send Keys/Certificates from: Unter welcher Absenderadresse sollen die Schlüssel versandt werden.

User address: Der Schlüssel wird unter der Adresse des Schlüsselinhabers verschickt. (Diese Adresse ist auch in den Schlüsseleigenschaften hinterlegt.)

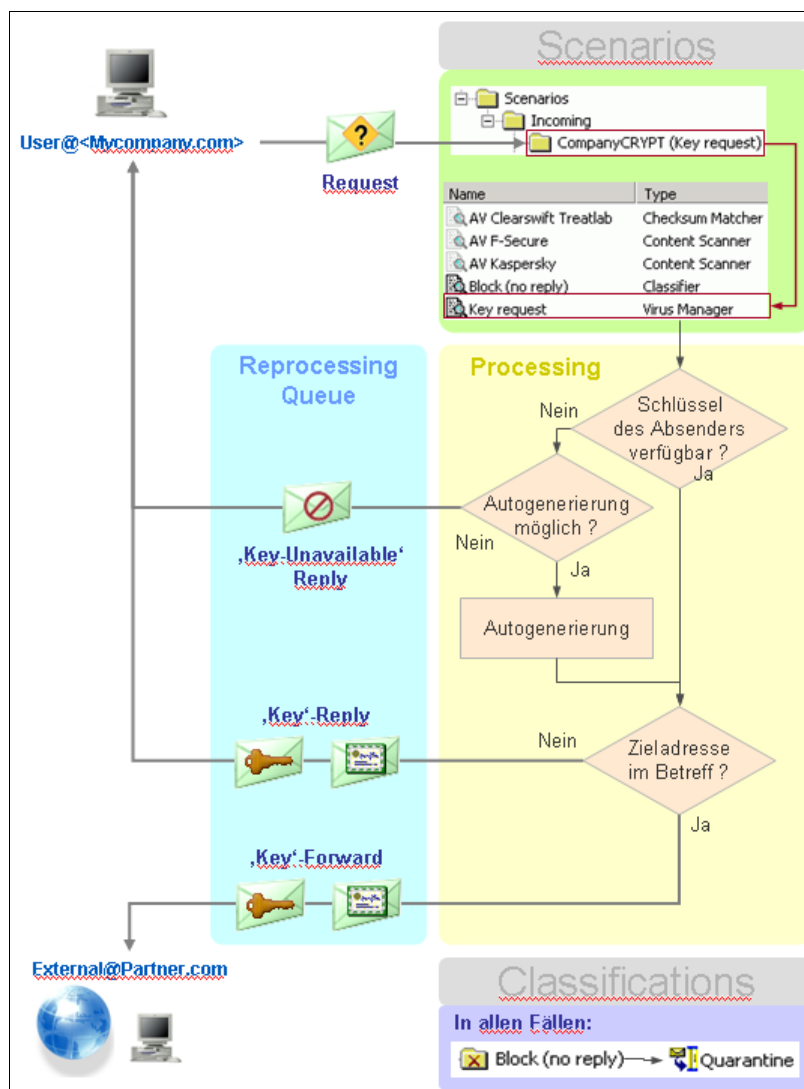
Sender address: Der Versand des Schlüssels erfolgt unter der Adresse, welche im Feld Sender address definiert wurde.

Apply ZIP compression: Die Schlüssel werden in ein ZIP-Archiv gepackt und dann an die Email angehängt.



- S/MIME key reply option: Zusätzliche Funktion für S/MIME-Schlüssel
- Always sign S/MIME reply with user key:
Aktiviert/Deaktiviert das Signieren der Mails (Replies) für S/MIME-Schlüssel. Standardmäßig werden die Schlüssel als Attachment verschickt.
- Quickguide option:
Im Quickguide wird die Handhabung des Keyserverns für den Benutzer beschrieben. Der Quickguide wird automatisch verschickt, wenn eine Mail ohne Schlüsselanforderung an die Listener Address geschickt wird
- Avoid reply by subject keyword:
Schlüsselwort zum Unterdrücken des Quickguide-Versandes, welches in der Betreffzeile der Mail angegeben werden muss.
- Case sensitive:
Aktiviert/Deaktiviert die Unterscheidung von Groß- und Kleinbuchstaben

4.10.4. Funktionsbild – Keyresponder für interne Anwender





Local / Internal domains:	<input type="text" value="@company.com"/>	Requests from these domains are considered internal. (Enter additional domains beginning with '@'.)
	<input type="text"/>	

Local / Internal Domains: Hier werden alle intern verwalteten Internetdomänen angegeben. Diese Information dient zur Unterscheidung, ob der Keyserver von Intern oder von Extern angesprochen wird.

2. Schritt

Die übrigen Einstellungen können Sie auf den Standardwerten belassen. Speichern Sie die Änderungen mit **Apply Changes**.

4.11. Erweiterte Konfiguration zur Funktionskontrolle

Diese erweiterten Konfigurationsanpassungen beeinflussen die Ver- und Entschlüsselungsfunktionalität von CompanyCRYPT nicht. Sie dienen der Funktionsüberwachung und können im Fehlerfall zur besseren Problemanalyse genutzt werden.

4.11.1. Protokollierung der Ver- und Entschlüsselung

Diese Konfiguration dient zur Analyse der Ver- und Entschlüsselungsfunktion. Durch die Protokollierung der eingehenden Mails und des Verarbeitungsergebnisses kann einmal die korrekte Funktion überprüft werden. Zum anderen können die Daten im Störfall zur Fehlereingrenzung dienen.

Einrichten der Message Areas

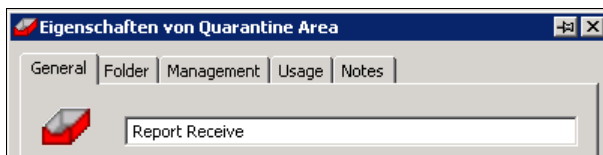
Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Message Areas

1. Schritt

Klicken Sie mit der rechten Maustaste auf **Message Areas** und wählen Sie dann **Neu → Quarantine Area**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards. Bei Verwendung des Wizards unterscheiden sich sowohl die dargestellten Fenster als auch die Reihenfolge der Schritte.

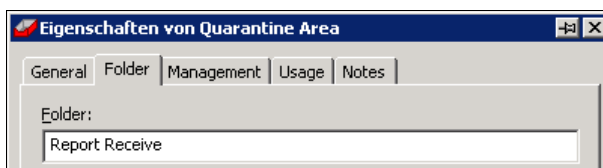
2. Schritt

Unter **Eigenschaften von Quarantine Area → General** tragen Sie den Namen der Message Area ein.



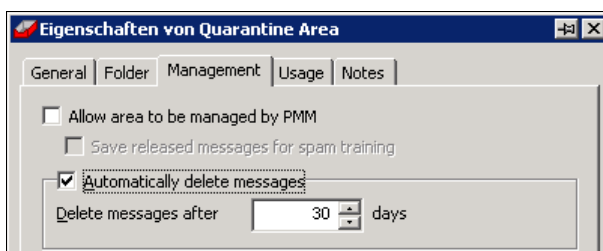
3. Schritt

Unter **Eigenschaften von Quarantine Area → Folder** tragen Sie den Namen für den Dateiordner ein. Nehmen Sie hier den gleichen Namen wie für die Message Area.



4. Schritt

Unter **Eigenschaften von Quarantine Area → Management** aktivieren Sie die Option **Automatically delete messages** und tragen 30 Tage in das entsprechende Feld ein. Die Option Allow area to be managed by PMM darf nicht aktiviert sein. Bestätigen Sie die Eingaben durch OK.



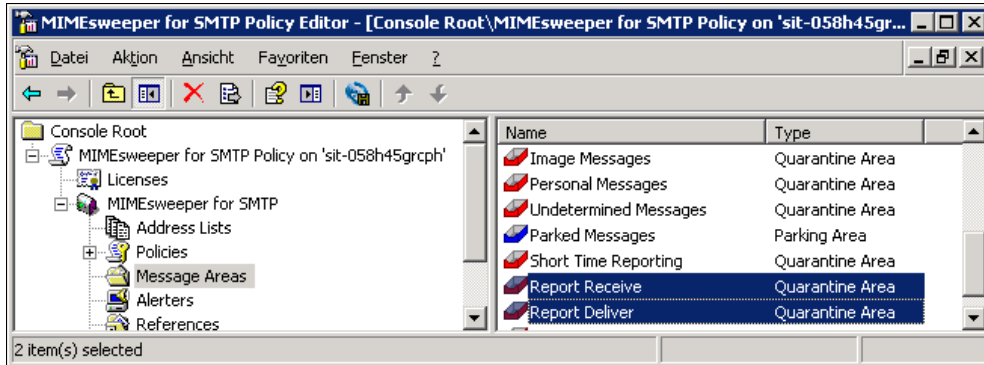
5. Schritt

Erstellen Sie nach den genannten Schritten eine weitere **Quarantine Area**. Unter **General** und **Folder** vergeben Sie hier die Bezeichnung **Report Deliver**.



6. Schritt

Die erstellten Message Areas werden anschließend in der Übersicht angezeigt.

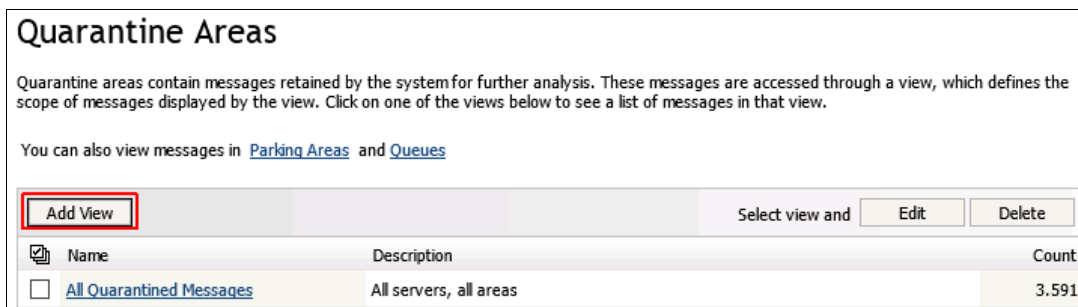


Message Areas im MIMesweeper Manager einrichten

MIMesweeper Manager → Message Center → Quarantine Areas

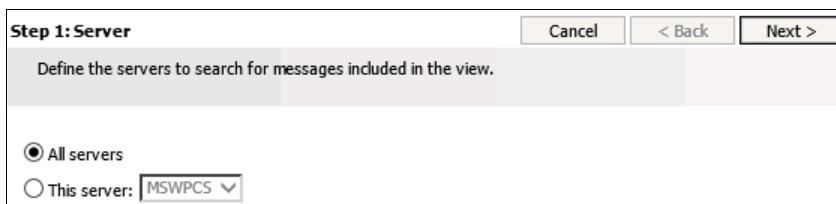
1. Schritt

Klicken Sie auf den Button **Add View**.



2. Schritt

Wählen Sie **All servers** und klicken Sie auf den Button **Next**.



3. Schritt

Wählen Sie **These areas** und markieren Sie **Report Receive**. klicken Sie anschliessend auf den Button **Next**.



Step 2: Area Cancel < Back Next >

Define the areas to search for messages included in the view.

☐ All areas

☒ These areas:

<input checked="" type="checkbox"/>	Name
<input type="checkbox"/>	Dirty Messages
<input type="checkbox"/>	Virus Messages
<input type="checkbox"/>	Undetermined Messages
<input type="checkbox"/>	Encrypted Messages
<input checked="" type="checkbox"/>	Report Receive
<input type="checkbox"/>	Report Deliver
<input type="checkbox"/>	Key Request
<input type="checkbox"/>	Support Messages
<input type="checkbox"/>	Misrouted Messages
<input type="checkbox"/>	Short Time Reporting

4. Schritt

Tragen Sie im Feld **Name** die Bezeichnung **Report Receive** ein und bestätigen Sie mit **Finish**.

Step 3: Name Cancel < Back Finish

Specify a name for the view.

Name:

5. Schritt

Klicken Sie erneut auf den Button **Add View**.

Add View Select view and Edit Delete

6. Schritt

Wählen Sie **All servers** und klicken Sie auf den Button **Next**.

Step 1: Server Cancel < Back Next >

Define the servers to search for messages included in the view.

☒ All servers

☐ This server:

7. Schritt

Wählen Sie **These areas** und markieren Sie **Report Deliver**. klicken Sie anschliessend auf den Button **Next**.



Step 2: Area Cancel < Back Next >

Define the areas to search for messages included in the view.

☐ All areas

☒ These areas:

<input checked="" type="checkbox"/> Name
<input type="checkbox"/> Dirty Messages
<input type="checkbox"/> Virus Messages
<input type="checkbox"/> Undetermined Messages
<input type="checkbox"/> Encrypted Messages
<input type="checkbox"/> Report Receive
<input checked="" type="checkbox"/> Report Deliver
<input type="checkbox"/> Key Request
<input type="checkbox"/> Support Messages
<input type="checkbox"/> Misrouted Messages
<input type="checkbox"/> Short Time Reporting

8. Schritt

Tragen Sie im Feld **Name** die Bezeichnung **Report Deliver** ein und bestätigen Sie mit **Finish**.

Step 3: Name Cancel < Back Finish

Specify a name for the view.

Name:

Erweitern der Entschlüsselungs Classification für die Protokollierung

Policy Editor → MIMesweeper for SMTP Policy → MIMesweeper for SMTP → Policies → Classifications → Decrypt OK

Durch die nachfolgenden Schritte werden die verschlüsselten Mails im Originalzustand, also vor der Entschlüsselung, und nach der Entschlüsselung in den definierten Message Areas gespeichert.

1. Schritt


Klicken Sie mit der rechten Maustaste auf die Classification **Decrypt OK** und wählen Sie **Neu → Quarantine**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

2. Schritt

Unter **Eigenschaften von Quarantine** → **General** geben Sie den Namen **Quarantine (Report Receive)** ein.

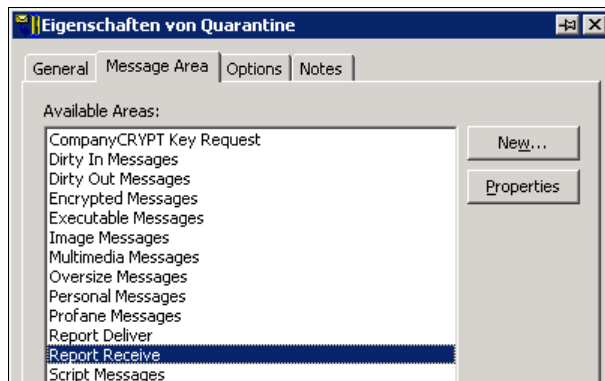
Eigenschaften von Quarantine + - x

General | Message Area | Options | Notes



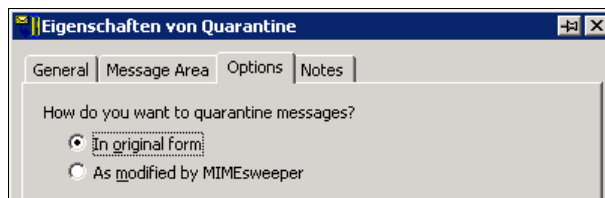
3. Schritt

Unter **Eigenschaften von Quarantine** → **Message Area** wählen Sie **Report Receive** aus.



4. Schritt

Unter **Eigenschaften von Quarantine** → **Options** markieren Sie **In original form** und bestätigen die Einstellungen mit OK.

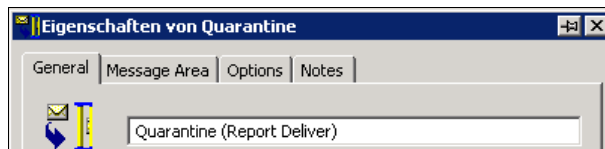


5. Schritt

Klicken Sie mit der rechten Maustaste wieder auf die Classification **Decrypt OK** und wählen Sie **Neu** → **Quarantine**.

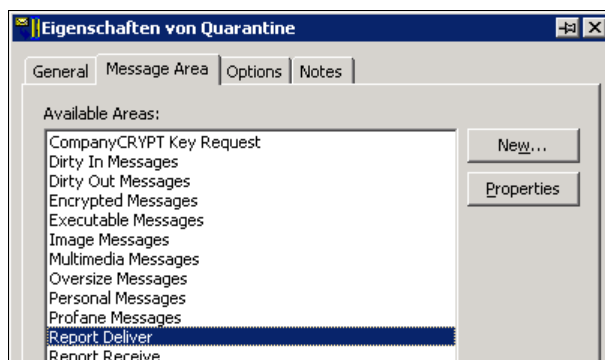
6. Schritt

Unter **Eigenschaften von Quarantine** → **General** geben Sie den Namen **Quarantine (Report Deliver)** ein.



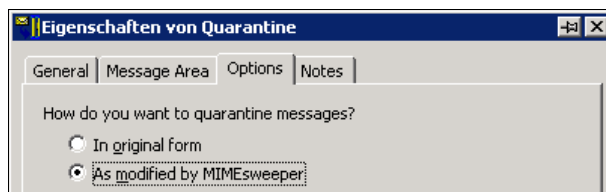
7. Schritt

Unter **Eigenschaften von Quarantine** → **Message Area** wählen Sie **Report Deliver** aus.



8. Schritt

Unter **Eigenschaften von Quarantine** → **Options** markieren Sie **As modified by MIMESweeper** und bestätigen die Einstellungen mit OK.



Erweitern der Verschlüsselungs Classification für die Protokollierung

Policy Editor → MIMESweeper for SMTP Policy → MIMESweeper for SMTP → Policies → Classifications → CompanyCRYPT OK

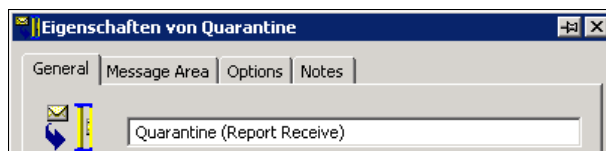
Durch die nachfolgenden Schritte werden die Mails im Originalzustand, also vor der Verschlüsselung, und nach der Verschlüsselung in den definierten Message Areas gespeichert.

1. Schritt

Klicken Sie mit der rechten Maustaste auf die Classification **CompanyCRYPT OK** und wählen Sie **Neu → Quarantine**. Die nachfolgenden Schritte beschreiben die Einrichtung ohne Nutzung des Wizards.

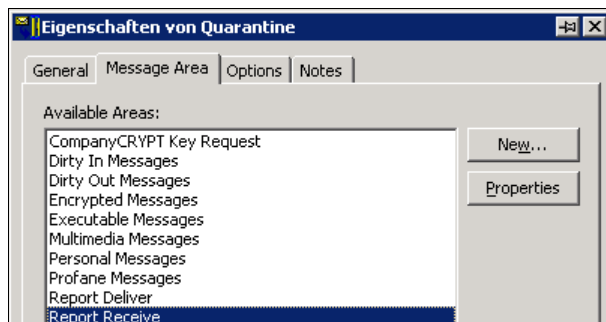
2. Schritt

Unter **Eigenschaften von Quarantine → General** geben Sie den Namen **Quarantine (Report Receive)** ein.



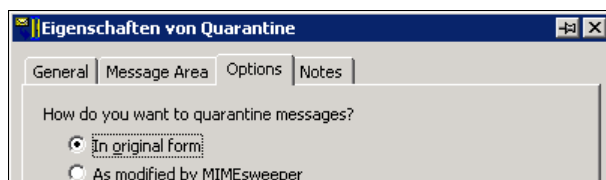
3. Schritt

Unter **Eigenschaften von Quarantine → Message Area** wählen Sie **Report Receive** aus.



4. Schritt

Unter **Eigenschaften von Quarantine → Options** markieren Sie **In original form** und bestätigen die Einstellungen mit OK.



5. Schritt

Klicken Sie mit der rechten Maustaste wieder auf die Classification **CompanyCRYPT OK** und wählen Sie **Neu → Quarantine**.

6. Schritt

Unter **Eigenschaften von Quarantine → General** geben Sie den Namen **Quarantine (Report Deliver)** ein.



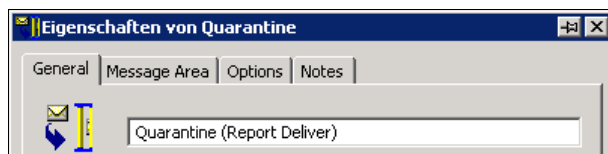
Secure Internet Traffic



COMPANYCRYPT®
The encryption module for MIMESweeper

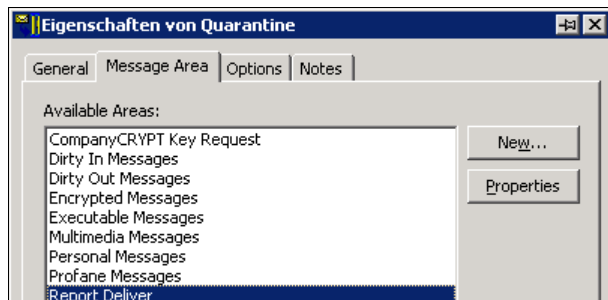
Einrichtung der Ver-/Entschlüsselung
Erweiterte Konfiguration zur Funktionskontrolle

Configuration Guide
CompanyCRYPT v1.5.0



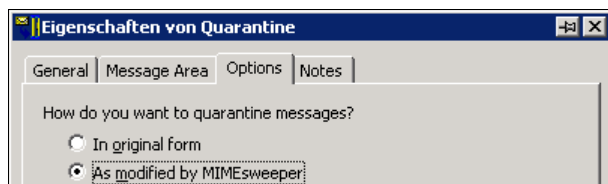
7. Schritt

Unter **Eigenschaften von Quarantine** → **Message Area** wählen Sie **Report Deliver** aus.



8. Schritt

Unter **Eigenschaften von Quarantine** → **Options** markieren Sie **As modified by MIMESweeper** und bestätigen die Einstellungen mit OK.





Secure Internet Traffic



COMPANYCRYPT®
The encryption module for MIMESweeper

5. Anhänge



5.1. Anhang: Entschlüsselung

5.1.1. Entschlüsselung – Verfügbare Szenarios

Hinweis: Anders als bei der ausgehenden Verschlüsselung ist es für eingehende eMails nicht erforderlich zwischen den Methoden Inline-PGP, PGP/MIME oder S/MIME zu unterscheiden. Die Methode wird automatisch erkannt und entsprechend verarbeitet.

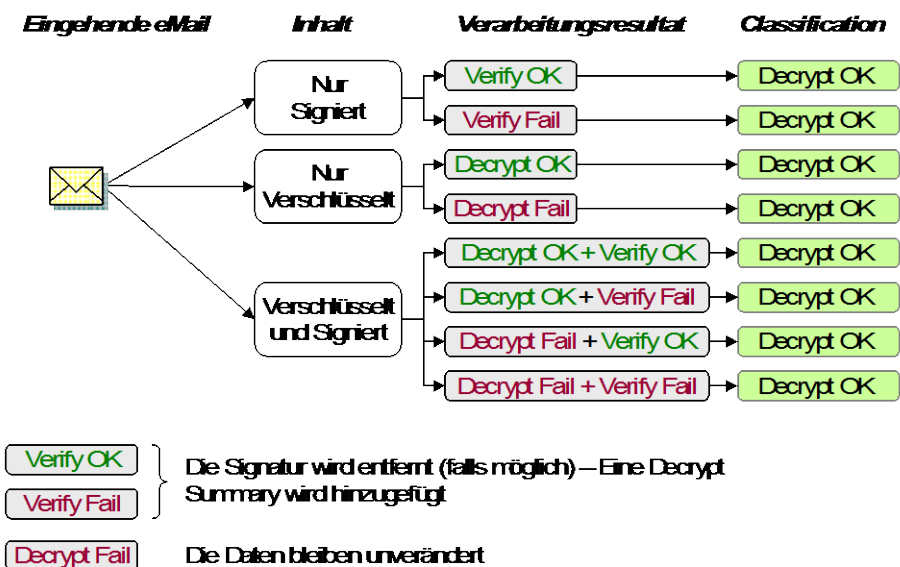
Szenario Name	Beschreibung
Decrypt Accept all	-- Entschlüsselung und Signaturprüfung -- Weiterverarbeitung erfolgt in jedem Falle. Die Entschlüsselung und Signaturprüfung wird durchgeführt, das Ergebnis dieser Prozesse spielt aber ,keine Rolle' (kein Entschlüsselungsfehler). Wenn entschlüsselt wurde oder eine Signatur überprüft wurde, wird eine ,Decrypt Summary' in den Bodytext eingefügt.
Decrypt-Expect decrypt only OK	-- Entschlüsselung und Signaturverarbeitung -- Weiterverarbeitung erfolgt nur bei erfolgreicher Entschlüsselung. Evtl. vorhandene Signaturen werden zwar überprüft und entfernt, jedoch spielt das Ergebnis der Signaturprüfung keine Rolle (kein Entschlüsselungsfehler). Wenn entschlüsselt wurde oder eine Signatur überprüft wurde, wird eine ,Decrypt Summary' in den Bodytext eingefügt.
Decrypt-Site2Site (Decrypt only OK)	Entspricht Decrypt-Expect decrypt only OK, jedoch wird keine Decrypt-Summary in den Bodytext geschrieben
Decrypt-Expect decrypt OR signature OK	-- Entschlüsselung und Signaturprüfung -- Weiterverarbeitung erfolgt nur bei erfolgreicher Entschlüsselung, die Signatur wird dann ignoriert. Bei signierten Mails (ohne verschlüsselten Inhalt) erfolgt die Weiterverarbeitung nur bei erfolgreicher Signaturprüfung. Wenn entschlüsselt wurde oder eine Signatur überprüft wurde, wird eine ,Decrypt Summary' in den Bodytext eingefügt.
Decrypt-Site2Site (Decrypt OR Sign OK)	Entspricht Decrypt-Expect decrypt OR signature OK, jedoch wird keine Decrypt-Summary in den Bodytext geschrieben
Decrypt- Expect decrypt AND signature OK	-- Entschlüsselung und Signaturprüfung -- Weiterverarbeitung erfolgt nur bei erfolgreicher Entschlüsselung und erfolgreicher Signaturprüfung. Das Fehlen von Verschlüsselung oder Signatur gilt als Entschlüsselungsfehler. Wenn entschlüsselt wurde oder eine Signatur überprüft wurde, wird eine ,Decrypt Summary' in den Bodytext eingefügt.
Decrypt-Site2Site (Decrypt AND Sign OK)	Entspricht Decrypt-Expect decrypt AND signature OK, jedoch wird keine Decrypt-Summary in den Bodytext geschrieben



5.1.2. Entschlüsselung – Verarbeitungsdetails

Scenario:

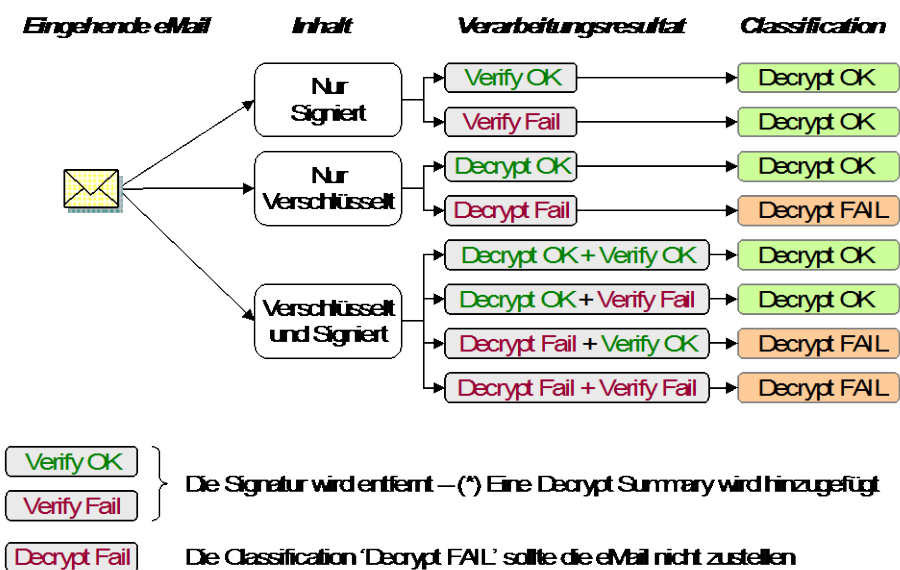
Decrypt (Accept all)



Scenario:

Decrypt-Expect decrypt only OK (*)

Decrypt-Site2Site (Decrypt only OK)

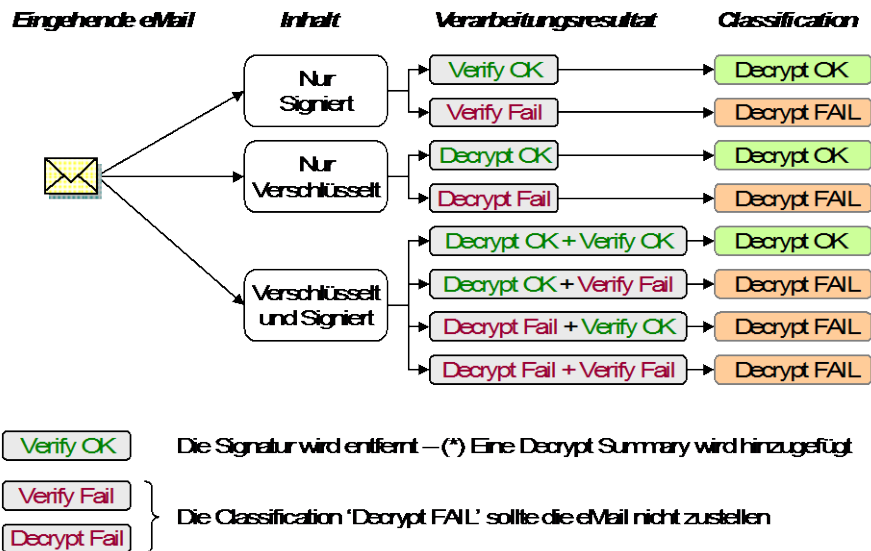




Szenario:

Decrypt-Expect decrypt OR signature OK (*)

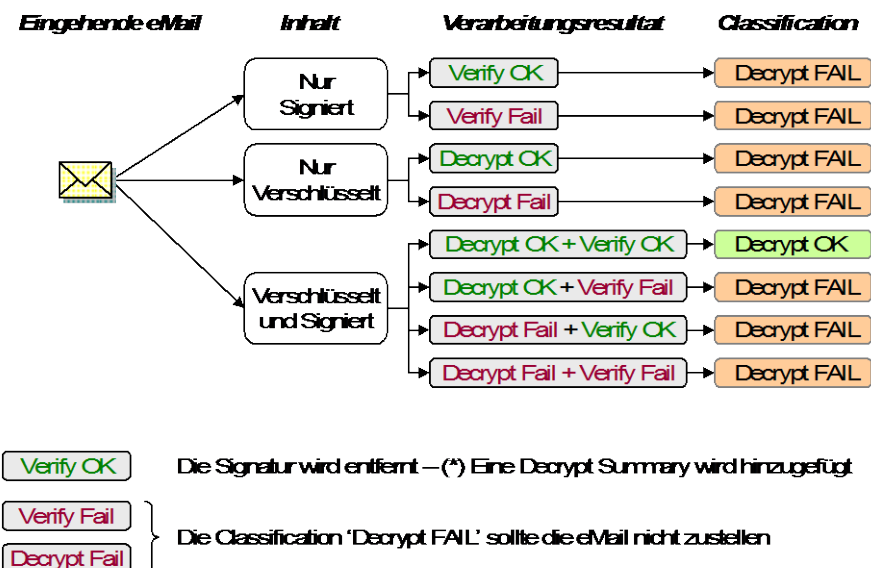
Decrypt-Site2Site (Decrypt OR Sign OK)



Szenario:

Decrypt-Expect decrypt AND signature OK (*)

Decrypt-Site2Site (Decrypt AND Sign OK)





5.2. Anhang: Verschlüsselung

5.2.1. Verschlüsselung – Verfügbare Szenarios (Nach Methode gruppiert)

PGP/MIME (OpenPGP)	
Szenario Name	Beschreibung
OpenPGP-Encrypt only	Verschlüsselung für Empfänger Adresse.
OpenPGP-Encrypt only (Site2Site)	Verschlüsselung für Zieldomäne (Site to Site-Verbindungen).
OpenPGP-Encrypt+Sign (Company)	Verschlüsselung für Empfängeradresse und Signieren mit dem Unternehmensschlüssel (CSA-Key).
OpenPGP-Encrypt+Sign (User)	Verschlüsselung für Empfängeradresse und Signieren im Namen des Users (mit dem Schlüssel des Absenders).
OpenPGP-Encrypt+Sign (Site2Site)	Verschlüsselung für Zieldomäne (Site to Site-Verbindungen) und Signieren mit dem Unternehmensschlüssel (CSA-Key).
OpenPGP-Only Sign (Company)	Signieren mit dem Unternehmensschlüssel (CSA-Key).
OpenPGP-Only Sign (User)	Signieren im Namen des Users (mit dem Schlüssel des Absenders).

Inline-PGP ('Classic' PGP)	
Szenario Name	Beschreibung
PGP-Encrypt only	Verschlüsselung der gesamten eMail für Empfängeradresse.
PGP-Encrypt only (Site2Site)	Verschlüsselung der gesamten eMail für Zieldomäne (Site to Site-Verbindungen).
PGP-Encrypt only Attachment	Verschlüsselung aller Attachments für Empfängeradresse, Der Bodytext bleibt unverändert.
PGP-Encrypt only Attachment (Site2Site)	Verschlüsselung aller Attachments für Zieldomäne (Site to Site-Verbindungen), Der Bodytext bleibt unverändert.
PGP-Encrypt+Sign (Company)	Verschlüsselung der gesamten eMail für Empfängeradresse und Signieren mit dem Unternehmensschlüssel (CSA-Key).
PGP-Encrypt+Sign (User)	Verschlüsselung der gesamten eMail für Empfängeradresse und Signieren im Namen des Users (mit dem Schlüssel des Absenders)
PGP-Encrypt+Sign (Site2Site)	Verschlüsselung der gesamten eMail für Zieldomäne (Site to Site-Verbindungen) und Signieren mit dem Unternehmensschlüssel (CSA-Key).
PGP-Encrypt+Sign Attachment (Company)	Verschlüsselung aller Attachments für Empfängeradresse und Signieren mit dem Unternehmensschlüssel (CSA-Key). Der Bodytext bleibt unverändert.
PGP-Encrypt+Sign Attachment (User)	Verschlüsselung aller Attachments für Empfängeradresse und Signieren im Namen des Users (mit dem Schlüssel des Absenders). Der Bodytext bleibt unverändert.
PGP-Encrypt+Sign Attachment (Site2Site)	Verschlüsselung aller Attachments für Zieldomäne (Site to Site-Verbindungen) und Signieren mit dem Unternehmensschlüssel (CSA-Key). Der Bodytext bleibt unverändert.
PGP-Sign Mail (Company)	Signieren aller Bestandteile einer Mail (Body, Attachments) mit dem Unternehmensschlüssel (CSA-Key), Signierte Attachments werden in das ASC-Format konvertiert. Der Empfänger benötigt für den Zugriff auf diese Attachments geeigneter PGP-Software.



PGP-Sign Mail (User)	<i>Signieren aller Bestandteile einer Mail (Body, Attachments) im Namen des Users (mit dem Schlüssel des Absenders), Signierte Attachments werden in das ASC-Format konvertiert. Der Empfänger benötigt für den Zugriff auf diese Attachments geeigneter PGP-Software.</i>
PGP-Sign Text (Company)	<i>Signieren des Bodytextes einer Mail mit dem Unternehmensschlüssel (CSA-Key), Attachments werden nicht signiert.</i>
PGP-Sign Text (User)	<i>Signieren des Bodytextes einer Mail im Namen des Users (mit dem Schlüssel des Absenders), Attachments werden nicht signiert.</i>

S/MIME	
Szenario Name	Beschreibung
SMIME-Encrypt only	<i>Verschlüsselung für Empfängeradresse.</i>
SMIME-Encrypt only (Site2Site)	<i>Verschlüsselung für Zieldomäne (Site to Site-Verbindungen).</i>
SMIME-Encrypt+Sign Detached (Company)	<i>Verschlüsselung für Empfängeradresse und Signieren mit dem Unternehmensschlüssel (CSA-Key), Detached bedeutet, dass die Signatur als separater Container an den unveränderten Bodytext angehängt wird.</i>
SMIME-Encrypt+Sign Detached (User)	<i>Verschlüsselung und Signieren im Namen des Users (mit dem Schlüssel des Absenders), Detached bedeutet, dass die Signatur als separater Container an den unveränderten Bodytext angehängt wird.</i>
SMIME-Encrypt+Sign Opaque (Company)	<i>Verschlüsselung für Empfängeradresse und Signieren mit dem Unternehmensschlüssel (CSA-Key), Opaque bedeutet, dass die Signatur Bestandteil des ins S/MIME-Format konvertierten Bodytextes wird.</i>
SMIME-Encrypt+Sign Opaque (User)	<i>Verschlüsselung und Signieren im Namen des Users (mit dem Schlüssel des Absenders), Opaque bedeutet, dass die Signatur Bestandteil des ins S/MIME-Format konvertierten Bodytextes wird.</i>
SMIME-Encrypt+Sign (Site2Site)	<i>Verschlüsselung für Zieldomäne und Signieren mit dem Unternehmensschlüssel (CSA-Key), Die Signierung erfolgt im Opaque-Format. Opaque bedeutet, dass die Signatur Bestandteil des ins S/MIME-Format konvertierten Bodytextes wird.</i>
SMIME-Sign Detached (Company)	<i>Signieren mit dem Unternehmensschlüssel (CSA-Key), Detached bedeutet, dass die Signatur als separater Container an den unveränderten (Klartext) Bodytext angehängt wird.</i>
SMIME-Sign Detached (User)	<i>Signieren im Namen des Users (mit dem Schlüssel des Absenders), Detached bedeutet, dass die Signatur als separater Container an den unveränderten (Klartext) Bodytext angehängt wird.</i>
SMIME-Sign Opaque (Company)	<i>Signieren mit dem Unternehmensschlüssel (CSA-Key), Opaque bedeutet, dass die Signatur Bestandteil des ins S/MIME-Format konvertierten Bodytextes wird.</i>
SMIME-Sign Opaque (User)	<i>Signieren im Namen des Users (mit dem Schlüssel des Absenders), Opaque bedeutet, dass die Signatur Bestandteil des ins S/MIME-Format konvertierten Bodytextes wird.</i>
Non-RFC S/MIME	
Die folgenden sind zur Behebung bestimmter Inkompatibilitäten vorgesehen (Sonderfälle). Der Aufbau der SMTP/MIME-Header entspricht nicht mehr dem definierten RFC-Standard für S/MIME-Nachrichten. Der Einsatz dieser Szenarios ist daher nicht empfohlen und sollte nur bei Kompatibilitätsproblemen in Betracht gezogen werden.	
SMIME-NonRFC Encrypt	<i>Verschlüsselung für Empfängeradresse.</i>
SMIME-NonRFC Encrypt+Sign (Company)	<i>Verschlüsselung und Signieren mit dem Unternehmensschlüssel (CSA-Key).</i>
SMIME-NonRFC Encrypt+Sign (User)	<i>Verschlüsselung und Signieren im Namen des Users (mit dem Schlüssel des Absenders).</i>
SMIME-NonRFC Sign (Company)	<i>Signieren mit dem Unternehmensschlüssel (CSA-Key)</i>



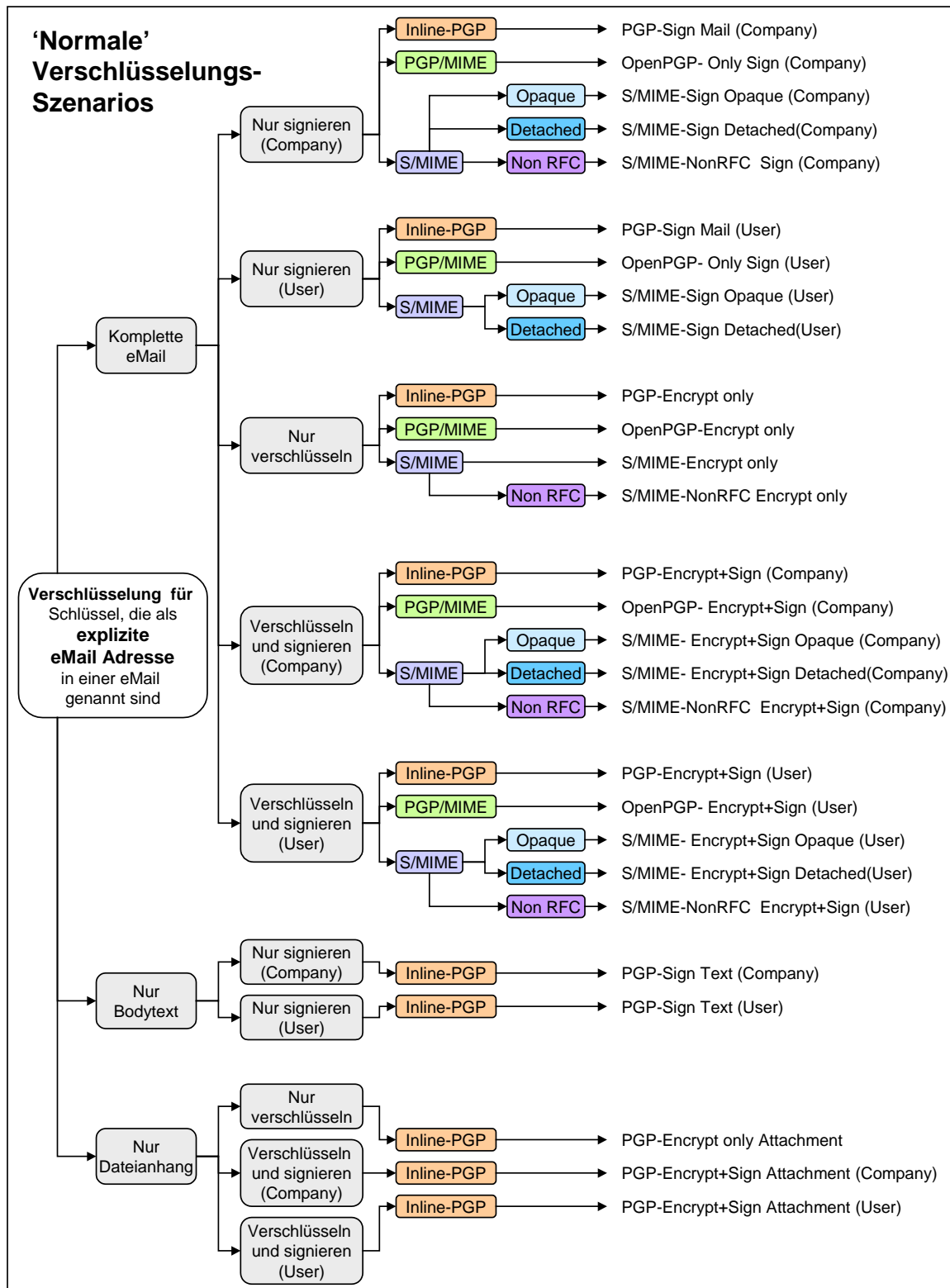
Ad Hoc Verschlüsselung (Symmetrisch)	
Szenario Name	Beschreibung
Ad Hoc Encryption	<i>Jede Nachricht wird mit der Ad Hoc Methode verschlüsselt.</i>

Anwender-gesteuerte Verschlüsselung	
Szenario Name	Beschreibung
User Controlled Encryption	<i>Betreff-gesteuerte Verarbeitung der Nachricht. Wenn Schlüssel für alle Empfänger für PGP oder S/MIME verfügbar sind, wird die jeweilige Methode angewendet. Die Signierung findet in Abhängigkeit der Konfiguration und/oder Betreffzeilensteuerung statt. Sind nicht alle Schlüssel verfügbar wird die Ad Hoc Verschlüsselung angewendet.</i>

AUtomatische Verschlüsselung	
Szenario Name	Beschreibung
Best Effort	<i>Wenn Schlüssel für alle Empfänger für PGP oder S/MIME verfügbar sind, wird die jeweilige Methode angewendet. Die Signierung findet in Abhängigkeit der Konfiguration statt. Sind nicht alle Schlüssel verfügbar erhalten diese Empfänger die Mailunverschlüsselt.</i>
Automatic Encryption	<i>Kombination auf Best Effort und User Controlled Encryption.</i>

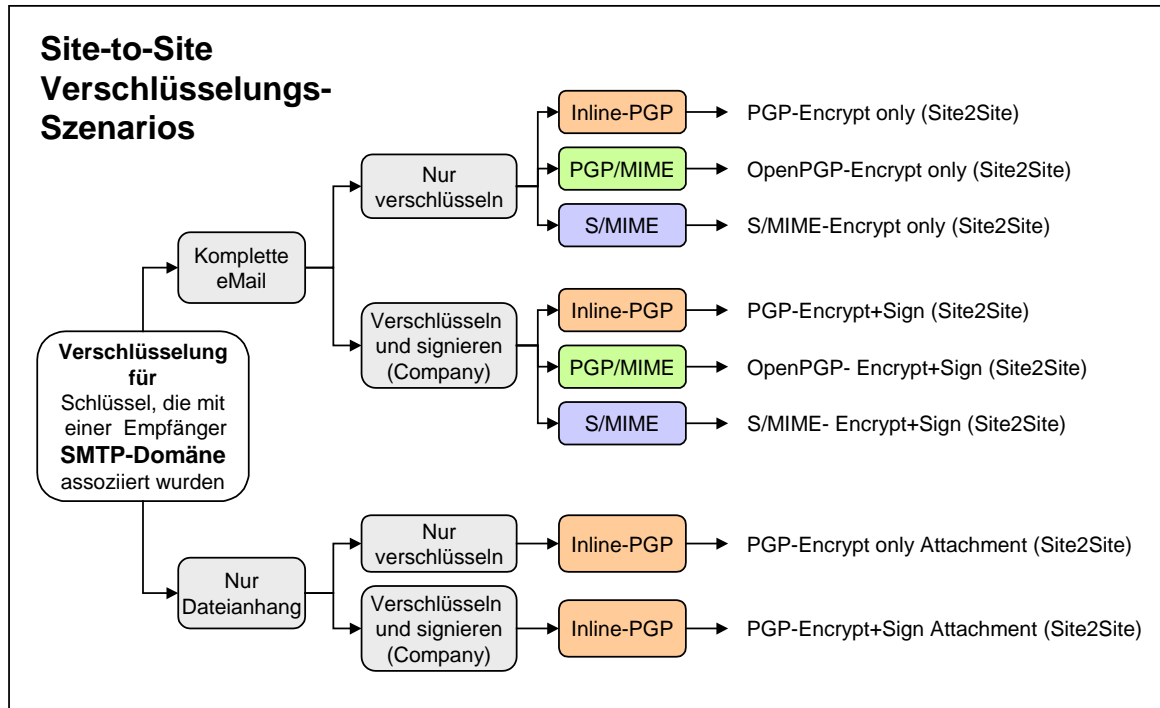


5.2.2. Verschlüsselung – Wahl des passenden Jobs





5.2.3. Site-to-Site/Gruppen Verschlüsselung – Wahl des passenden Jobs



Standard Verschlüsselung vs. Site-to-Site Verschlüsselung (Gruppen-Schlüssel)

Standard Verschlüsselung

Bei einer Verschlüsselung startet der Prozess normalerweise, indem alle eMail Empfänger Adressen extrahiert werden. Für jede Adresse, für die ein gültiger öffentlicher Schlüssel vorliegt, wird verschlüsselt. Dies ist allerdings nur dann möglich, wenn in dem Schlüssel selbst eine gültige Adresse angegeben ist.

Site-to-Site Verschlüsselung (Gruppen-Schlüssel)

Die sogenannte Site-to-Site Verschlüsselung wird immer dann benötigt, wenn:

1. Alle eMails, die an eine bestimmte SMTP Domäne geschickt werden, mit einem Schlüssel verschlüsselt werden sollen.
2. Alle eMails, die an eine begrenzte Anzahl Adressen innerhalb einer SMTP-Domäne geschickt werden mit einem Schlüssel verschlüsselt werden sollen.
3. Der Schlüssel eines externen Partners keine gültige (explizite) eMail Adresse trägt.

Die in 2. und 3. genutzten Schlüssel werden auch Gruppen-Schlüssel genannt und tragen typischerweise eine eMail Adresse, die etwa so aufgebaut ist: '@domain.com'. Für alle drei Fälle wird ein anderer Ansatz zur Schlüsselfindung benötigt, da die Empfängeradressen alleine hierfür nicht mehr genügend Informationen liefern.

Solche Gruppen/Site-to-Site Schlüssel können in CompanyCRYPT verwendet werden. Im ersten Schritt stellt der CompanyCRYPT Administrator eine Beziehung zwischen dem Schlüssel und einer SMTP Domäne her. (Nähere Angaben hierzu finden Sie im Kapitel 3.8.9 Site to Site-Verschlüsselung). Im zweiten Schritt wählen man im MIMESweeper sogenannte Site-to-Site Verschlüsselungs-Szenarios. Deren Verarbeitungslogik ist dahingehend anders, dass anstatt der expliziten eMail-Adressen, die einzelnen SMTP-Ziel-Domänen extrahiert werden, und dann die dazu assoziierten Schlüssel verwendet werden.

Eine besondere Anforderung stellen die Fälle 2. und 3. dar, da hier nur für eine bestimmte Anzahl Empfänger innerhalb der SMTP Domäne Verschlüsselung angewendet werden soll. Dies lässt sich erreichen, indem man die Sender/Empfänger-Eigenschaften des Szenarios, welches die Site-to-Site Verschlüsselung triggert, auf jene Adressgruppe limitiert.



6. Empfehlungen / Praxis

Die folgende Liste erhebt keinen Anspruch auf Vollständigkeit. Sie soll helfen einiger der typischen Probleme und Fehl-Konfigurationen zu umgehen bzw. zu vermeiden. Sie kann aber auch Hilfestellung leisten, die richtige Strategie im Umgang mit Emailverschlüsselung zu finden:

PGP oder S/MIME	Beide Verfahren haben einen vergleichbar hohes Sicherheitslevel und haben sich inzwischen nebeneinander fest etabliert. Wir empfehlen ihnen sich auf den Verschlüsselungsstandard ihres Kommunikationspartners einzustellen, da CompanyCRYPT flexibel mit beiden Standards umgehen kann. OpenPGP bietet jedoch zusätzlich noch den Charme mit einem einzigen zentralen PGP-Schlüssel E-Mails für unterschiedlichste E-Mail-Adressen verschlüsseln zu lassen. Das erspart es Ihnen für jeden internen User ein Schlüsselpaar zu generieren.
MIMESweeper Config	Die Erfahrung zeigt, dass es am günstigsten ist, Adressliste, Classifications und Scenarios erst dann einzurichten, wenn Sie tatsächlich benötigt werden. Das Vorkonfigurieren für die bloße Möglichkeit hat sich in den meisten Fällen nicht ausgezahlt, da es zu mehr Aufwand bei Konfigurationsänderungen, die durch den täglichen Betrieb auftreten, kommen kann.
Entschlüsselung	Bei einer leistungsfähigen Hardwareausstattung des MIMESweeper-Gateways kann der 'Decrypt-Expect decrypt only OK' Job ohne weiteres auf alle eingehenden eMails angewendet werden. Dadurch werden spezielle Adresslisten überflüssig und der administrative Aufwand reduziert sich.
Schlüsselerzeugung	Erzeugen Sie nur die (internen) Schlüssel, die Sie wirklich benötigen. Der administrative Mehraufwand kann sehr schnell ansteigen, da sie einmal in Verkehr gebrachte Schlüssel mindestens bis zum Ende der Gültigkeit verwalten müssen. Lassen Sie ihre Schlüssel am besten „on demand“ von CompanyCRYPT erstellen, wenn der externe Partner erstmal einen Schlüssel anfordert.
Persönliche Signaturen	Da es sehr einfach ist auch persönliche (User) Signaturen auf breiter Basis anzuwenden, empfehlen wir dies, speziell bei sensiblen Anwendungen, ihren E-Mails einen eindeutigen Herkunftsnachweis beizufügen.
Massen-Signaturen	Eine beliebte Signaturmethode ist, alle ausgehenden eMails mit einem Domain- oder Firmenschlüssel zu signieren, da nur ein einziger Signierschlüssel für das gesamte Unternehmen genutzt wird. Jedoch sollten hierbei die unterschiedlichen Eigenarten der Signiermethoden berücksichtigt werden. Bei Inline-PGP führen Zitat-Antworten zu erheblichen Nebeneffekten. Zudem ist diese Methode gänzlich ungeeignet für HTML Nachrichten. Bei S/MIME treten irritierende Meldungen bei allen Empfängern auf, die MS Outlook Express benutzen. Ursache hierfür ist, dass die Absenderadresse nicht mit der im Signierschlüssel (Firmenschlüssel) eingetragenen Adresse übereinstimmt.
CA/CSA auf Homepage	Alle PGP-Anwender-Schlüssel in CompanyCRYPT sind durch den CSA-Schlüssel signiert. Alle S/MIME-Schlüssel sind entweder durch die OnBoard-CA oder durch ein Trustcenter signiert. Es ist für den Schlüsselaustausch sehr hilfreich, wenn die Schlüsseldetails dieser beiden „vertrauenswürdigen“ Schlüssel (Name, eMail, Fingerprint) auf einer Seite innerhalb der Firmen-Internet-Präsenz/Homepage angezeigt würden. Damit könnte der externe Partner einen Schlüssel, den er per MIKE abgerufen hat, über die Homepage verifizieren und sofort zur Verschlüsselung nutzen. Und das ohne Beteiligung eines Administrators.