



**Abschlussbericht der Machbarkeitsstudie der AG 7
„Austausch verschlüsselter E-Mail über externe Mailinglisten
unter Einsatz eines E-Mail Gateways“**

Version *1.0*
Status *Final*
Datum *09.03.2005*

TeleTrusT Deutschland e.V.
Chamissostraße 11
99096 Erfurt

© TeleTrusT Deutschland e.V.
2005



Inhaltsverzeichnis

Zusammenfassung	6
1. Einleitung "Sichere Kommunikation via Mail-Gateway"	7
1.1. Lösung 1: Jeder Teilnehmer verwaltet seine Adressliste	7
1.2. Lösung 2: Sichere Kommunikation via Gruppenschlüssel.....	8
1.3. Lösung 3: Sichere Kommunikation via Mail-Gateway	8
2. Abgrenzung	9
3. Architektur	9
4. Teilnahmevoraussetzungen	11
4.1. Organisatorische Teilnahmevoraussetzungen.....	11
4.2. Technische Teilnahmevoraussetzungen	11
5. Testlokationen	11
6. Aufbau der Testszenarien - Testspezifikation	12
7. Testablauf.....	12
8. Am Test beteiligte Produkte - Übersicht	13
8.1. Eingesetzte Gateway-Produkte	13
8.2. Eingesetzte Listen-Server	13
8.3. Eingesetzte E-Mailclients	13
8.4. Eingesetztes empfangendes Mail Gateway.....	13
8.5. Genutzte Verzeichnisdienste	14
8.6. Genutzte Validierungsdienste	14
9. Auswertung der Tests	14
9.1. Senden und Empfangen verschlüsselter E-Mails	14
9.2. Senden und Empfangen signierter E-Mails	15
9.3. Einbindung der optionalen Dienste	16
9.4. Zusammenfassung Testauswertung.....	17
10. Abkürzungsverzeichnis	18
Anhang	19
11. Beschreibungen der Tests	19
11.1. Kategorie 1	19
11.2. Kategorie 2.....	19
11.2.1. Gutfall-Tests.....	19
11.2.2. Schlechtfall-Tests	19
11.3. Kategorie 3.....	20
11.3.1. Gutfall-Tests.....	20
11.3.2. Schlechtfall-Tests	20
11.4. Kategorie 4.....	21
11.4.1. Gutfall-Tests.....	21
11.4.2. Schlechtfall-Tests	22
12. Formularvorlagen	23
12.1. Event Log	23
12.2. Rückmeldebogen Empfänger.....	24



Der vorliegende Abschlussbericht wurde im Rahmen der Machbarkeitsstudie „sicherer E-Mailaustausches unter Einbeziehung externer Mailing-Listen“ unter der Mitwirkung folgender Firmen bzw. Institutionen (alphabetische Reihenfolge) erstellt:



Applied Security GmbH

Frau Christiane Schnall
Industriestraße 16
D-63811 Stockstadt
www.apsec.de



BCC Unternehmensberatung GmbH

Herr Thomas Reich
Heinrich-Hertz-Str. 26
D-63225 Langen
www.bcc-unternehmensberatung.de



Bundesamt für Sicherheit in der Informationstechnik

Herr Michael Thiel und Herr Matthias Ryll
Godesberger Allee 185-189
D-53175 Bonn
www.bsi.bund.de



ICC InfoTeSys Computer Consulting GmbH

Herr Ralf Schnitzler
Luxemburger Str. 124-136
D-50939 Köln
www.iccgmbh.de



Information & Communication

NetSys.IT Information & Communication GbR

Herr Peter Steiert
Weimarer Str. 28
D-98693 Ilmenau
www.netsys-it.de



Nimbus Network Technologieberatung

Herr Arno Fiedler
Auf dem Grat 41a
D-14195 Berlin
www.nimbus-network.de



noventum consulting GmbH

Herr Stephan Wappler
Münsterstraße 111
D-48155 Münster
www.noventum.de



SAP AG

Herr Dr. Gunter Bitz und Herr Fritz Bauspieß
Neurottstraße 16
D-69190 Walldorf
www.sap.com



secaron AG

Herr Dr. Thomas Störckuhl
Ludwigstr. 45, Haus B
D-85399 Hallbergmoos
www.secaron.de



TC TrustCenter AG - A Cybertrust Company

Herr Thomas Blumenthal
Sonninstraße 24-28
D-20097 Hamburg
www.cybertrust.com
www.trustcenter.de



Utimaco Safeware AG

Herr Dr. Henning Seemann
Hohemarkstraße 22
D-61440 Oberursel
www.utimaco.de



Siemens AG

Herr Dr. Michael Steinacker
Otto-Hahn-Ring 6
D-81730 München
www.siemens.com



Totemo AG

Herr Marc O. Stöckli
Seestraße 134a
CH-8700 Kusnacht - Zurich
www.totemo.ch



Zertificon Solutions GmbH

Herr Dr. Burkhard Wiegel
Landsberger Allee 117
D-10407 Berlin
www.zertificon.com



Anerkennung und Dank für die Unterstützung

Beträchtliche Bemühungen sind in den Entwurf, die Planung, die erfolgreiche Durchführung und Auswertung der Tests gegangen. Fachleute von verschiedenen Organisationen, sowohl Anwender, TrustCenter Dienstleister, Consulting Firmen als auch Hersteller haben sich zusammengeschlossen, um den Rahmen zu definieren und die Voraussetzungen für den Austausch verschlüsselter E-Mail über externe Mailinglisten zu schaffen. Die AG7 und das Projektteam möchten ihre Dankbarkeit gegenüber dieser pflichtbewussten Gruppe von Personen und auf ihre unterstützenden Organisationen ausdehnen:

Projektkoordination	<i>Stephan Wappler, noventum consulting GmbH</i>
Verantwortlich für die NDA	<i>Christiane Schnall, Applied Security GmbH Fritz Bauspieß, SAP AG Kai Hartwich, TeleTrust Deutschland e.V.</i>
Entwicklung Testspezifikation	<i>Thomas Blumenthal, TC TrustCenter – A Cybertrust Company Stephan Wappler, noventum consulting GmbH</i>
Test-Koordinatoren	<i>Thomas Blumenthal, TC TrustCenter – A Cybertrust Company Stephan Wappler, noventum consulting GmbH</i>
Bereitstellung Listenzertifikate	<i>Stefan Kirch, T-Systems International GmbH Thomas Blumenthal, TC TrustCenter – A Cybertrust Company</i>
Unabhängige Test-Auditoren	<i>Michael Thiel, BSI Matthias Ryll, BSI</i>
Editor Abschlussbericht	<i>Stephan Wappler, noventum consulting GmbH</i>
AG7-Arbeitsgruppenleiter	<i>Fritz Bauspieß, SAP AG</i>

Das Projektteam möchte sich bei den folgenden Personen bedanken, die der Machbarkeitsstudie zu ihrem Erfolg verholfen haben:

<i>Dr. Gunter Bitz (SAP)</i>	<i>Dr. Henning Seemann (Utimaco)</i>
<i>René Gawanka (Zertificon)</i>	<i>Michael Silvan (secaron)</i>
<i>Olaf Grupe (noventum consulting)</i>	<i>Peter Steiert (NetSys.IT)</i>
<i>Dr. Frank Gutberlet (noventum consulting)</i>	<i>Dr. Michael Steinacker (Siemens)</i>
<i>Kai Hartwich (TeleTrust)</i>	<i>Marc O. Stöckli (Totemo)</i>
<i>Andreas Krümmel (BCC)</i>	<i>Dr. Thomas Störkuhl (secaron)</i>
<i>Franz Mülkens (noventum consulting)</i>	<i>Uwe Völkel (T-Systems)</i>
<i>Thomas Reich (BCC)</i>	<i>Dr. Burkhard Wiegel (Zertificon)</i>
<i>Prof. Helmut Reimer (TeleTrust)</i>	<i>Stephanie Willemsen (TC TrustCenter)</i>
<i>Ralf Schnitzler (ICC)</i>	



Zusammenfassung

Im Vordergrund stand die Prüfung der generellen Möglichkeit des Austausches verschlüsselter E-Mails über Mailinglisten unter Verwendung eines Mail-Gateways insbesondere in der Gegenüberstellung mit dem Szenario "Gruppenschlüssel". Der Ausgangspunkt für die Durchführung dieser Machbarkeitsstudie war, verschlüsselte und optional signierte E-Mails zwischen Mitgliedern der Arbeitsgruppe AG7, die über eine Mailingliste kommunizieren, auszutauschen. Die Mitglieder der AG7 gehören verschiedenen Organisationen und Unternehmen an und der Listenserver wird durch einen externen Dienstleister zentral im Internet betrieben.

Es wurden fünf Gateway-Produkte in Verbindung mit acht verschiedenen E-MailClients getestet. Optional wurden vergleichbare Dienste der *European Bridge-CA* (Verzeichnisdienst und Validierungsdienst) in die Tests mit einbezogen. In der Testspezifikation wurden vier Testkategorien mit insgesamt 16 Einzeltests, eingeteilt in Gutfall- und in Schlechtfall-Tests, spezifiziert, die sich an Beispielen der Praxis orientierten und die je Gateway abzuarbeiten waren. Die Tests wurden je Produkt in einem der zwei zur Verfügung stehenden TestLabs unter der Aufsicht eines unabhängigen Beobachters des BSI durchgeführt. Vor Ort wurde ein Event Log über die aufgetretenen Probleme geführt, und die Listenteilnehmer hatten jeweils einen Rückmeldebogen auszufüllen, in dem der Status der erhaltenen E-Mails zu erfassen war.

Nach der Auswertung der Event Logs und der Rückmeldebögen kann zusammenfassend festgehalten werden, dass grundsätzlich ein Austausch verschlüsselter E-Mails über eine externe Mailingliste möglich ist. Die Gutfall-Tests bezüglich der Verschlüsselung, d.h. bei optimalen Bedingungen für eine verschlüsselte Weiterleitung wurden von fast allen getesteten Produkten erfolgreich bestanden. Es hat sich während der Tests jedoch gezeigt, dass bei eingehenden signierten E-Mails die Signatur nur von sehr wenigen Produkten unverändert bei der Weiterleitung an die Listenteilnehmer an der E-Mail belassen wurde. Die Mehrzahl der Gateways hat die Signatur entfernt und durch einen Footer ersetzt. Weiterhin wurde beobachtet, dass, wenn nicht alle Voraussetzungen positiv erfüllt waren, erhebliche Unterschiede zwischen den getesteten Produkten in der Behandlung der Problemsituation (Schlechtfall-Tests) aufgetreten sind. Einige der in diesem Zusammenhang aufgetretenen Fehler oder Probleme sind auf die Entwicklungsphilosophie der Hersteller zurückzuführen.

Die Philosophie besagt, dass die Gateways an der Grenze zwischen internem vertrauenswürdigen und externem nicht vertrauenswürdigen Netzwerk platziert werden. Die Testarchitektur basierte jedoch auf einer externen – externen Kommunikationsbeziehung, d.h. die eingehenden E-Mails kamen über ein externes nicht vertrauenswürdigen Netzwerk, und die ausgehenden E-Mails wurden über ein externes nicht vertrauenswürdigen Netzwerk wieder versendet.

Einige Hersteller haben nach Abschluss ihrer Tests Produktänderungen für die nächste Version angekündigt. Somit kann für die Auswahl und den Einsatz eines Gateways zur Absicherung des E-Mailverkehrs über eine externe Mailingliste nur empfohlen werden, den Fokus auf die Schlechtfall-Tests zu legen.

Zur Durchführung der Machbarkeitsstudie ist noch erwähnenswert, dass die Studie im Juli 2004 gestartet und im März 2005 beendet wurde. Während dieser Zeit hat es nicht ein persönliches Treffen der Teilnehmer (Ausnahme die Beteiligten im TestLab) gegeben. Alle Terminvereinbarungen und der Gedankenaustausch wurden per E-Mail und Telefonkonferenzen durchgeführt. Dies hat von alle Beteiligten ein hohes Maß an Disziplin und Kooperationsbereitschaft gefordert. An dieser Stelle gebührt allen Teilnehmern, Koordinatoren und den fleißigen Helfern im Hintergrund Dank und Anerkennung.

1. Einleitung "Sichere Kommunikation via Mail-Gateway"

Der Ausgangspunkt für die Machbarkeitsstudie war, verschlüsselte und optional signierte E-Mails zwischen Mitgliedern der Arbeitsgruppe AG7, die über eine Mailingliste kommunizieren, auszutauschen. In der Regel gehören die Mitglieder von solchen Mailinglisten verschiedenen Organisationen an und der Listenserver wird durch einen Dienstleister außerhalb der Mitgliederorganisationen zentral im Internet betrieben. Weiterhin ist den Mitgliedern einer solchen Liste sehr oft nicht im Detail bekannt, wer noch Mitglied der Liste ist. Dies ist sehr oft auch so gewünscht.

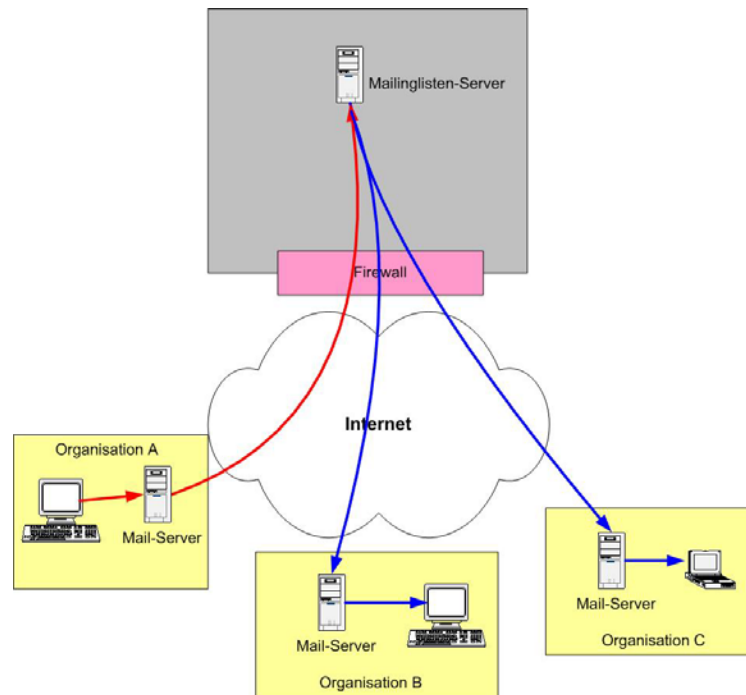


Abbildung 1: Ausgangssituation

In diesem Zusammenhang wurden drei generell verschiedene Lösungsansätze herausgearbeitet und untersucht:

- Lösung 1: **Jeder Teilnehmer verwaltet seine Adressliste**
- Lösung 2: **Machbarkeitstest "Sichere Kommunikation via Gruppenschlüssel"**
- Lösung 3: **Machbarkeitstest "Sichere Kommunikation via Mail-Gateway"**

1.1. Lösung 1: Jeder Teilnehmer verwaltet seine Adressliste

Bei der näheren Analyse der Lösung 1 wurden die folgenden Schwierigkeiten identifiziert:

- Sehr oft wissen die Teilnehmer nicht, wer auf der Liste ist.
- Das Schlüsselmanagement ist für den einzelnen Teilnehmer bei einer größeren Anzahl von Teilnehmern nicht mit vertretbarem Aufwand durchführbar.

Aus diesen Gründen wurde das Management der Listen für den Einzelnen für Lösung 1 als zu kompliziert eingestuft und diese Lösung wurde nicht weiter untersucht.

1.2. Lösung 2: Sichere Kommunikation via Gruppenschlüssel

Bei dieser Lösung wird die Liste auch weiterhin zentral geführt und bleibt in ihrer bestehenden Form erhalten. Es wird ein Gruppenschlüsselpaar auf die Mailing-Liste ausgestellt und jeder Teilnehmer der Liste erhält den öffentlichen und den privaten Gruppenschlüssel, um Nachrichten an die Gruppe verschlüsseln und entschlüsseln zu können.

Der Vorteil dieser Lösung besteht darin, dass keine Änderungen an der Architektur und am Mailinglisten-Server vorgenommen werden müssen.

Die Nachteile dieser Lösung sind das Schlüsselmanagement, und wie erste Tests gezeigt haben, gibt es Probleme beim Öffnen der verschlüsselten E-Mails mit einigen E-Mailclients. Das Schlüsselmanagement ist dabei als die größere Herausforderung anzusehen. Jeder Teilnehmer muss auf einem sicheren Weg den privaten Schlüssel für die Entschlüsselung der über die Liste erhaltenen E-Mails erhalten und in seinem Client installieren. Zum einen muss diese Verteilung an alle Teilnehmer in Abhängigkeit von der Gültigkeit der Zertifizierung jährlich oder alle 2 Jahre erfolgen, und zum zweiten kann die Installation des privaten Listenschlüssels gegen die Policies der Organisation des Teilnehmers verstoßen. Weiterhin kann der Entzug des privaten Schlüssels bei einem ausscheidenden Teilnehmer nicht durchgesetzt werden. Das bloße Löschen der Adresse von der Liste führt nur dazu, dass der Teilnehmer die E-Mail nicht mehr direkt zugestellt bekommt. Zusätzlich muss das Root- und die Sub-CA-Zertifikate der ausstellenden CA's für die Verwendung des öffentlichen Listenschlüssels in den entsprechenden Clients installiert werden.

Die Tests und die Auswertung sind noch nicht endgültig abgeschlossen.

Die Koordinatorin für diese Tests ist Frau Christiane Schnall von Applied Security.

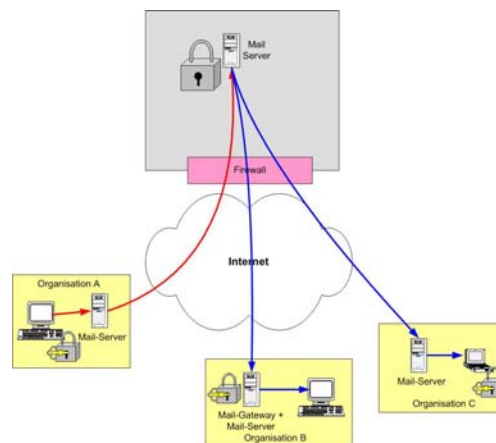


Abbildung 2: Nutzung eines Gruppenschlüssels

1.3. Lösung 3: Sichere Kommunikation via Mail-Gateway

Auch bei dieser Lösung wird die Liste weiterhin zentral geführt und bleibt in ihrer bestehenden Form erhalten. Es wird ein Gruppenschlüsselpaar auf die Mailing-Liste ausgestellt, der öffentliche Schlüssel an die Teilnehmer verteilt und im Unterschied zu Lösung 2 wird der private Schlüssel in einem speziellen Gateway gespeichert. Jeder Teilnehmer verschlüsselt seine Nachrichten an die Liste durch Benutzen des öffentlichen Schlüssels der Liste. Die verschlüsselte E-Mail wird von diesem besonderen Mail-Gateway empfangen, und die Nachricht wird durch Benutzen der privaten Schlüssel der Liste entschlüsselt. Anschließend wird die Liste durch den Listenserver exportiert und für jeden Teilnehmer eine E-Mailkopie



erzeugt. Diese Einzelmails werden dann durch das Gateway durch Benutzen des öffentlichen Schlüssels des jeweiligen Empfängers wieder verschlüsselt und an den Empfänger versandt.

Der Vorteil dieser Lösung besteht darin, dass keine Änderungen am Mailinglisten-Server vorgenommen werden müssen. Das Schlüsselmanagement stellt keine größere Herausforderung dar, da die existierenden öffentlichen Schlüssel der Teilnehmer verwendet werden. Kein Teilnehmer muss zusätzliche private Schlüssel auf seinem Client installieren. Durch das Löschen der E-Mailadresse von der Liste ist sichergestellt, dass das ausscheidende Mitglied beim Abhören des ausgehenden Mailverkehrs vom Gateway keine Zugriffschance auf den Inhalt erhält, da es nicht im Besitz eines notwendigen privaten Schlüssels ist.

Die Nachteile dieser Lösung sind, dass ein spezielles Gateway angeschafft und entweder vor dem eigentlichen Listenserver installiert oder der Listenserver durch das Gateway ersetzt wird. Weiterhin muss jeder Listenteilnehmer bzw. jede teilnehmende Organisation im Besitz eines eignen Schlüsselpaares sein und das Root- und die Sub-CA-Zertifikate der ausstellenden CA's für die Verwendung des öffentlichen Listenschlüssels in den entsprechenden Clients installieren.

2. Abgrenzung

Die Durchführung der Tests diene ausschließlich der Überprüfung der Machbarkeit des „sicheren E-Mailaustausches unter Einbeziehung externer Mailinglisten“. Die hierfür entworfene Testspezifikation richtete sich nach den Anforderungen für eine sichere E-Mailkommunikation innerhalb des Mitgliederkreises der AG7 des TeleTrust Deutschland e.V.

- Die Ergebnisse der eingesetzten Produkte haben keine Aussagekraft für den eventuellen späteren Einsatz einer solchen Lösung bei TeleTrust.
- Die detaillierten Testberichte werden nur unter Einhaltung der im NDA genannten Bedingungen veröffentlicht.

3. Architektur

Ziel der Machbarkeitsuntersuchung der Lösung 3 war es, an eine Mailingliste sichere Nachrichten zu senden, die mit dem auf die E-Mailadresse der Mailingliste ausgestellten Zertifikat verschlüsselt sind. Die verschlüsselten E-Mails werden an ein spezielles Mail-Gateway gesendet, welches die Nachrichten mit dem Listenschlüssel entschlüsselt. Anschließend wird die Liste aufgelöst, indem die Teilnehmeradressen im BCC-Feld eingefügt werden. Dies kann direkt durch das Gateway geschehen oder durch einen zusätzlichen E-Mailserver (siehe Abbildung 3). Dabei müssen die Listenserver so konfiguriert sein, dass sie keine Änderungen an den E-Mails vornehmen. Das Gateway verschlüsselt jede einzelne E-Mail für jeden Listenteilnehmer mit dessen öffentlichen Schlüssel und versendet sie über das Internet.

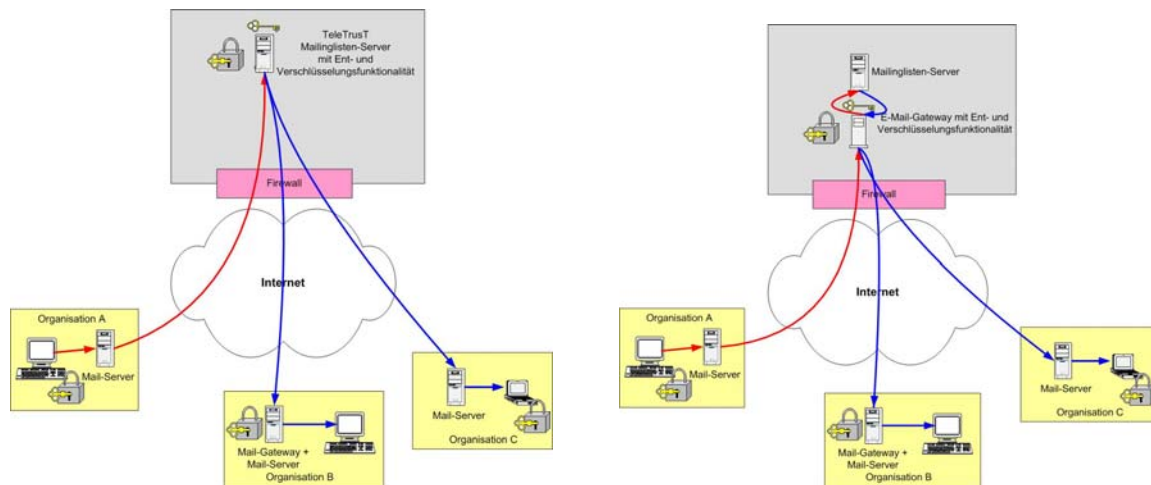


Abbildung 3: Basisarchitektur ohne und mit Trennung zwischen Gateway und Listenserver

Neben der Basisfunktionalitäten der Verschlüsselung wurden optional die Möglichkeiten der Signatur und die Einbindung von Verzeichnis- und Validierungsdiensten mit getestet. Um die Interoperabilität zu den von der *European Bridge-CA* betriebenen Diensten zu prüfen, wurden diese direkt bzw. vergleichbare Dienste mit angebunden.

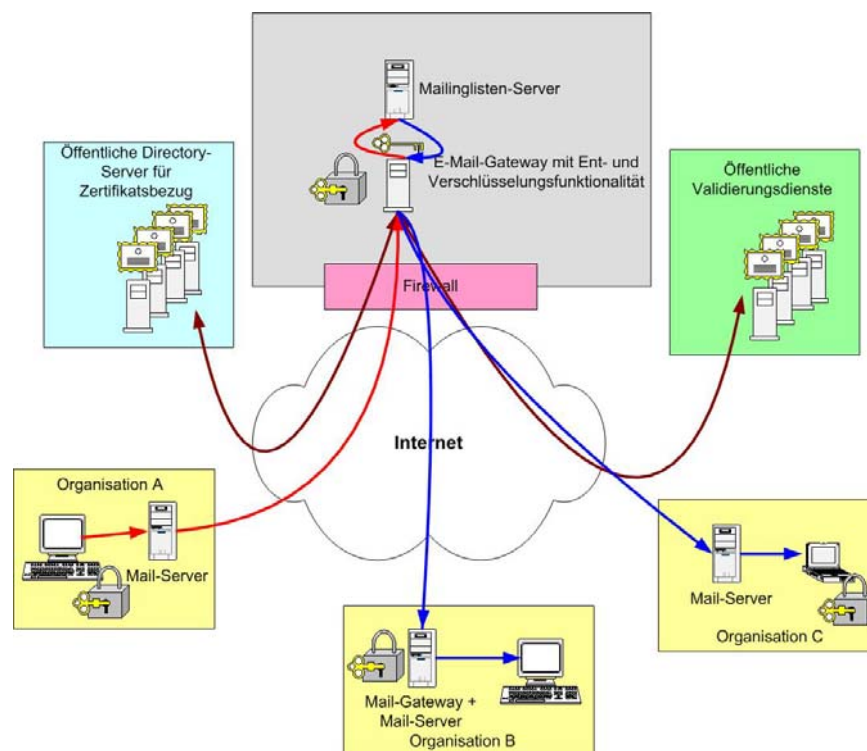


Abbildung 4: Basisarchitektur mit optionalen Diensten

Zertifikats-Validierung

Für die Validierung ausgewählter am Gateway hinterlegter Verschlüsselungszertifikate bzw. verwendeter Signaturzertifikate wurde ein vergleichbarer Validierungsdienst der *European Bridge-CA* per OCSP verwendet. Zusätzlich konnten auch CRL Listen per http direkt, per LDAP direkt oder per LDAP über den LDAP-Proxy durch das Gateway bezogen werden.



Zertifikatsbezug

Für den Bezug von Zertifikaten für neue Listenmitglieder, bei gespeicherten abgelaufenen oder gesperrten Zertifikaten wurde ein vergleichbarer Verzeichnisdienst der *European Bridge-CA* per LDAP verwendet. Die Gateways konnten auf diese Art und Weise Verschlüsselungszertifikate per LDAP Request über den Proxy oder einen anderen Verzeichnisdienst beziehen.

4. Teilnahmevoraussetzungen

4.1. Organisatorische Teilnahmevoraussetzungen

Teilnahmevoraussetzung für diese Machbarkeitsuntersuchung „Sicherer E-Mailaustausch unter Einbeziehung externer Mailinglisten“ im Rahmen der AG7 waren:

- Die Teilnehmer mussten TTT-Mitglied sein.
- Die Teilnehmer mussten die vereinbarte NDA unterschrieben haben.

4.2. Technische Teilnahmevoraussetzungen

Die technischen Voraussetzungen für die allgemeinen Tests waren:

- X.509 v3 Zertifikate, eigene PKI oder von einem Trust Center
- Asymmetrische Schlüssellänge mindestens 1.024 Bit
- S/MIME kompatible Mailsysteme
- Symmetrische Schlüssellänge 128 Bit

Für die optionalen Tests waren die folgenden Voraussetzungen zu erfüllen:

- LDAP v3 Support durch das Gateway
- OCSP Unterstützung durch das Gateway

5. Testlokationen

Für die Tests wurden Räumlichkeiten durch die nachfolgenden beiden Firmen zur Verfügung gestellt.

noventum consulting GmbH
Münsterstraße 111
D-48155 Münster
www.noventum.de

TC TrustCenter - A Cybertrust Company
Sonninstraße 24-28
D-20097 Hamburg
www.cybertrust.com
www.trustcenter.de

An beiden Lokationen war ein Testnetz mit Zugang zum Internet verfügbar. Die Auswahl der Testlokation für das jeweilige Gatewayprodukt erfolgte in Absprache mit den Beteiligten.



6. Aufbau der Testszenerien - Testspezifikation

Die Testszenerien wurden in vier verschiedene Kategorien eingeteilt. Weiterhin wurden die Testfälle nach Gut- und Schlechtfalltests unterschieden. Die Kommunikation zwischen dem E-Mailsender und dem Gateway einerseits sowie dem Gateway und dem Listenserver als auch dem Gateway und dem E-Mailempfängern wurde durch die Gutfalltests ermittelt. Mit den Schlechtfalltests wurden besondere Zustände erzeugt, die von den E-Mail Gateways entsprechend interpretiert werden mussten. Die Gateways sollte im Fehlerfall an die Betroffenen eine Benachrichtigungsmail über den Fehlerzustand schicken. In jedem Fall sollte aber der Verursacher eines Fehlers (z.B. fehlendes Zertifikat eines Listenmitgliedes) eine Benachrichtigung über den Mangel erhalten.

Kategorie 1

Diese E-Mails dienten nur der Überprüfung, dass die Kommunikation zwischen den im Test eingebundenen Systemen funktioniert.

Kategorie 2

Diese E-Mails dienten für die Überprüfung des verschlüsselten Austauschs von E-Mails über das Gateway. Die öffentlichen Schlüssel der Listenmitglieder wurden auf dem Gateway hinterlegt. Das fallweise Weiterleiten unverschlüsselter Mails war in diesen Testszenerien nicht vorgesehen und war damit auch keine Option. In realen Konfigurationen kann es aber durchaus sinnvoll sein, z.B. wenn der Vertraulichkeitsgrad einer Mail durch das Gateway sicher ermittelt werden konnte.

Kategorie 3

Diese E-Mails dienten für die Überprüfung des verschlüsselten und signierten Austauschs von E-Mails über das Gateway. Die öffentlichen Schlüssel der Listenmitglieder waren auf dem Gateway hinterlegt. Die Signatur war durch das Gateway zu validieren und der Status der Zertifikate zu ermitteln. Ziel war die Überprüfung des Umgangs mit der Signatur und mit Zertifikatsstatusdiensten. (OCSP-Requests oder CRL-Handling).

Kategorie 4

Diese E-Mails dienten für die Überprüfung des verschlüsselten und signierten Austauschs von E-Mails über das Gateway. Die öffentlichen Schlüssel der Listenmitglieder waren zum Teil auf dem Gateway hinterlegt. Bei nicht vorhandenen, abgelaufenen oder gesperrten Schlüsseln waren über den LDAP Proxy oder einen anderen Verzeichnisdienst diese zu beziehen bzw. gegen neue auszutauschen. Ziel war die Überprüfung des Umgangs mit Verzeichnisdiensten.

7. Testablauf

Der zeitliche Testablauf wurde vor Start der Tests mit allen Beteiligten abgestimmt. Die entsprechenden Informationen bzgl. des Testumfeldes, die finale Testspezifikation, die am Test beteiligten E-Mailadressen und Zertifikate wurden den Gateway-Herstellern im Vorfeld zur Verfügung gestellt.

Um die zeitlichen und finanziellen Belastungen für alle Teilnehmer so gering wie möglich zu halten, wurde je Produkt ein Testtag angesetzt. Die Tests wurden an dem vereinbarten Tag unter der Aufsicht eines unabhängigen Beobachters des BSI durchgeführt. Aufgetretene Schwierigkeiten wurden vor Ort in einem Event Log erfasst (siehe Anhang).

Die Auswertung der Tests durch die Empfänger erfolgte zeitnah zum Versand der entsprechenden Testmails. Jeder Empfänger hatte einen entsprechenden Rückmeldebogen auszufüllen (siehe Anhang).

Datum	Testlokation	Gateway-Hersteller	Beobachter
10.02.05	noventum consulting GmbH, Münster	Utimaco Safeware AG	BSI
10.02.05	TC TrustCenter AG, Hamburg	Zertificon Solutions GmbH	BSI



23.02.05	noventum consulting GmbH, Münster	BCC Unternehmensberatung GmbH	BSI
24.02.05	noventum consulting GmbH, Münster	ICC InfoTeSys Computer Consulting GmbH	BSI
01.03.05	TC TrustCenter AG, Hamburg	Totemo AG	BSI

Tabelle 1: Übersicht Testplan

8. Am Test beteiligte Produkte - Übersicht

Im Rahmen der Tests wurden die nachfolgenden Produkte eingesetzt und in verschiedenen Varianten miteinander kombiniert. Nicht von allen genannten E-Mail-Clients wurden auch E-Mails an die Liste versendet, jedoch wurden alle aufgeführten Clients als Empfänger eingebunden.

8.1. Eingesetzte Gateway-Produkte

- BCC_Mail Protect Gateway, BCC Unternehmensberatung GmbH
- JULIA MailOffice, ICC InfoTeSys Computer Consulting GmbH
- SecurE-Mail Gateway, Utimaco Safeware AG
- TrustMail® Secure Email Gateway, Totemo AG
- Z1 SecureMail Gateway, Zertificon Solutions GmbH

8.2. Eingesetzte Listen-Server

- Lotus Notes Domino 6.5
- Sendmail 8.13.0

8.3. Eingesetzte E-MailClients

- Groupwise 6.5.3
- Microsoft Outlook 2002 mit CryptoEx V 3.0.5.2
- Microsoft Outlook 2003 SP 1
- Microsoft Outlook Express 6 mit fideAS mail client
- Mozilla Mail 1.7
- Lotus Notes R 6.5.2
- Lotus Notes R 6.5.3
- Thunderbird 1.0

8.4. Eingesetztes empfangendes Mail Gateway

- Z1 SecureMail Gateway



8.5. Genutzte Verzeichnisdienste

- LDAP Proxy Version 3.1, The Boeing Company, betrieben durch noventum consulting GmbH
- Open LDAP Server
- Öffentliche Verzeichnisdienst von TC TrustCenter

8.6. Genutzte Validierungsdienste

- OCSP Responder, secaron AG

9. Auswertung der Tests

Im Rahmen der Tests wurde festgestellt, dass die Gateway-Produkte alle nach erfolgreichem Kategorie-1-Test umkonfiguriert wurden. Für den Kategorie-1-Test wurde eine unverschlüsselte Weiterleitung fest voreingestellt und für die nachfolgenden Tests wurde dann fest eingestellt, dass alle ausgehenden E-Mails verschlüsselt werden müssen. Eine automatische Erkennung, dass eine eingehende unverschlüsselte E-Mail auch unverschlüsselt an die Listenteilnehmer weitergeleitet und eine eingehende verschlüsselte E-Mail ausschließlich verschlüsselt an die Listenteilnehmer weitergeleitet werden muss, war in der Testspezifikation nicht enthalten und wurde somit auch nicht getestet.

Nach Aussage der meisten Hersteller kann diese automatische Erkennung jedoch realisiert bzw. konfiguriert werden.

9.1. Senden und Empfangen verschlüsselter E-Mails

Die Auswertung der Log Events und Rückmeldebögen hat ergeben, dass die Gutfalltests bzgl. der Verschlüsselung von fast allen getesteten Mail-Gateways erfolgreich bearbeitet wurden. Die Empfänger der E-Mails konnten alle empfangenen Gutfall-Mails öffnen und lesen. Weiterhin konnten die empfangenden Listenteilnehmer auch alle empfangenen Schlechtfall-Mails öffnen und lesen, bis auf eine einzige Ausnahme, d.h. eine einzige verschlüsselte E-Mail konnte nicht geöffnet – jedoch die genaueren Umstände dazu auch nicht geklärt werden. Weiterhin haben alle Gateway-Produkte gesperrte oder abgelaufene Userzertifikate erkannt und bei nicht ausdrücklichem Administratorbefehl auch nicht verwendet. User, deren Zertifikat gesperrt oder abgelaufen war, haben die E-Mail mit dem kritischen Inhalt auch nicht erhalten.

Somit kann für die empfangenden Clients festgehalten werden, dass es beim Öffnen und Lesen bis auf eine Ausnahme keine Probleme gegeben hat. Diese Ausnahme besteht darin, dass bei einer Testserie eines Gateways auch alle E-Mails problemlos entschlüsselt und geöffnet werden konnten, jedoch keine Dateianhänge in der E-Mail mehr enthalten waren. Da das Problem während des Tests nicht aufgefallen ist, konnte erst im Nachgang festgestellt werden, dass es sich um ein Konfigurationsproblem handelte.

Generell kann für die sendenden Clients festgehalten werden, dass sie alle mit den Listenzertifikaten umgehen, d.h. die ausgehenden E-Mails an die Liste mit dem zugehörigen Listenzertifikat verschlüsseln konnten. Die Auswertung auf der Seite der sendenden E-MailClients für die Schlechtfalltests hat die folgenden Fehler und Probleme offenbart:

- **Verschlüsselung mit gesperrten Listenzertifikat**

Da der Bezug von Sperrlisten entweder organisatorisch oder auch teilweise technisch nicht möglich war, d.h. manche Clients haben dies nicht unterstützt, haben die Clients auch die gesperrten Listenzertifikate verwendet. Dies hat zum einen dazu geführt, dass einige Gateway-Produkte die



E-Mails nicht öffnen konnten und sie geblockt haben, da sie nicht im Besitz des privaten Schlüssels waren oder, wenn der private Schlüssel des gesperrten Zertifikats hinterlegt war, diese E-Mail ohne Beanstandung bearbeitet haben. Eine Prüfung, ob das verwendete Listenzertifikat gesperrt wurde, wurde nur von einem der getesteten Gateway-Produkte während der Tests demonstriert. Eine Fehlermeldung wurde nach Feststellung des Mangels an den Administrator weitergeleitet und die E-Mail wurde nicht weiter bearbeitet.

Generell ist die fehlende Prüfung der Gültigkeit des Listenzertifikats den Clients anzulasten, da diese bereits den Fehler der ungeprüften Verwendung des Listenzertifikats begehen.

- **E-Mail konnte nicht allen Empfängern aus verschiedenen Gründen zugestellt werden**

Diese Fälle waren grundsätzlich Schlechtfall-Tests, bei denen bei einem Empfänger die Voraussetzung, ein gültiges Verschlüsselungszertifikat zu besitzen, nicht erfüllt war. In diesem Falle sollte das Gateway entweder den Empfänger oder den Absender über den Mangel informieren. Diese Anforderung haben nicht alle Gateways erfüllt.

- Ein Produkt hat alle Fehlermeldungen an die vom Administrator hinterlegte „Fehleradresse“ versendet. Wenn der Administrator nicht erreichbar ist oder viele Fehlermeldungen an diesen Account generiert werden, dann ist zu erwarten, dass weder der Absender noch der Empfänger zeitnah über das nicht vorliegende Zertifikat und somit der nicht Zustellung der E-Mail informiert werden.
- Ein anderes Produkt hat eine Fehlermeldung an den Absender zurück gesendet, in der es über den Mangel informierte. Unglücklicherweise wurde an diese Fehlermeldung die Originalmessage inklusive der Anlage angefügt und unverschlüsselt über das Internet zurück zum Absender übertragen. Dieser Fehler ist auf die Produktphilosophie zurückzuführen, dass so ein Gateway für eine intern-extern Kommunikationsbeziehung gedacht ist und normalerweise diese Fehlermeldung nach intern in eine vertrauenswürdige Umgebung zurück sendet. Der Hersteller hat angekündigt, dieses Problem zu lösen.

- **Bezug von Zertifikaten von einem Verzeichnisdienst-Service**

Grundsätzlich konnten alle getesteten Gateways Zertifikate von einem Verzeichnisdienst beziehen. Jedoch gab es Unterschiede im internen Zertifikatsmanagement der Gateways.

- Einige der getesteten Gateways waren in der Lage bei mehreren Zertifikaten zu einer E-Mailadresse eine Auswahl zu treffen und die E-Mail an den Empfänger zu verschlüsseln und zu versenden.
- Andere Gateways haben zwar auch erkannt, dass gespeicherte Zertifikate inzwischen gesperrt worden oder abgelaufen waren, jedoch waren sie nicht in der Lage, dem entsprechenden Empfänger eine E-Mail aufgrund der nachfolgenden Probleme zu senden:
 - Per LDAP konnte ein gültiges Zertifikat zu der entsprechenden E-Mailadresse bezogen werden, jedoch konnte das gespeicherte Zertifikat durch das per LDAP bezogene nicht ersetzt und dann auch nicht angewendet werden, da die Schreibweise der Städtenamen verschieden war (ue statt ü) und somit beim Vergleich nicht matchten.
 - Die Suche wurde nach dem Auffinden des zur E-Mailadresse korrespondierenden, aber nicht mehr gültigen Zertifikats im internen Zertifikatsspeicher des Gateways eingestellt. Es wurde kein neues Zertifikat per LDAP abgefragt,

9.2. Senden und Empfangen signierter E-Mails

Der Umgang der Gateways mit eingehenden signierten E-Mails war für einige wenige Tests von Interesse. Generell haben alle Gateways die Gültigkeit der Absendersignatur auf Gültigkeit und die E-Mail auf Integrität überprüft. Jedoch hat sich bei der Auswertung der Tests der folgende Status über alle Gateways ergeben:

- **Signatur mit gültigem Signaturzertifikat durch sendenden E-Mailclient erstellt**



Nur einige wenige der getesteten Gateways waren in der Lage, die gültige Absendersignatur an der eingehenden E-Mail zu belassen. Wobei entweder keine Informationen an die Empfänger über den Status der Prüfung weitergegeben wurden oder der Status der Prüfung in der Subject-Line ergänzt wurde.

Alle anderen Gateways haben die Signatur entfernt und durch einen Footer in der E-Mail ersetzt, in dem sie vermerkt haben:

- Die E-Mail war signiert.
- Das Ergebnis der Signaturvalidierung war in Ordnung.
- Von wem die E-Mail signiert war.

Dieses Vorgehen war so nach Testspezifikation nicht gewünscht.

Alle Gateways hätten die ausgehenden E-Mails mit dem Listenzertifikat signieren können. Dies war jedoch nicht gewünscht und wurde auch nicht getestet, da Probleme bei einigen empfangenden Clients erwartet wurden. Einige Clients führen einen Cross-Check aus, in dem sie prüfen, ob die Absender-E-Mail-Adresse mit der im Signaturzertifikat enthaltenen Adresse übereinstimmen. Falls nicht, wird je nach Implementierung die Signatur als ungültig ausgewiesen.

- **Signatur mit ungültigem Signaturzertifikat durch sendenden E-Mailclient erstellt**

Die ungültige Absendersignatur (gesperrtes Signaturzertifikat verwendet) wurde nur von sehr wenigen Gateway an der eingehenden E-Mail belassen. Der Status der Prüfung wurde in der Subject-Line mit einem deutlichen Hinweis auf den Mangel ergänzt.

Die überwiegende Mehrzahl der Gateways hat die Signatur entfernt und durch einen Footer in der E-Mail ersetzt, in dem sie vermerkt haben:

- Die E-Mail war signiert.
- Das Ergebnis der Signaturvalidierung war nicht korrekt.
- Von wem die E-Mail signiert war.

9.3. Einbindung der optionalen Dienste

Die Möglichkeiten der Einbindung der optionalen Dienste (siehe Abbildung 4) war von Gateway Produkt zu Gateway Produkt und von Dienst zu Dienst sehr verschieden.

- **LDAP-Server und LDAP Proxy**

- Grundsätzlich konnten alle getesteten Gateways Zertifikate von einem Verzeichnisdienst-Server per LDAP-Abfrage beziehen.
- Einige Gateways konnten zusätzlich über den mit der European Bridge-CA vergleichbaren Dienst LDAP-Proxy Zertifikate beziehen.
- Nicht alle Gateway haben die technischen Voraussetzungen für die optionalen Tests erfüllt. Es konnten keine LDAP-Version-3-Abfragen sondern nur LDAP-Version-2-Abfragen generiert werden. Da der LDAP-Proxy-Dienst LDAP-Version-3-Abfragen erfordert, war ein Test gegen diesen Dienst somit nicht möglich.
- Bei einigen Gateway-Tests war dieser LDAP-Proxy-Dienst nicht verfügbar, so dass eine umfassende Aussage nicht möglich ist.

- **OCSP Responder**

- Die Validierung der Zertifikate per OCSP unter Nutzung des mit der European Bridge-CA vergleichbaren OCSP-Responder-Dienstes wurde durch die Mehrzahl der getesteten Gateways unterstützt.



- Einige wenige Gateways konnten gegen diesen Dienst aus den folgenden Gründen nicht getestet werden: Entweder haben sie in der eingesetzten Version das Protokoll OCSP nicht unterstützt oder aus Zeitgründen konnte dieser Test nicht durchlaufen werden.

9.4. Zusammenfassung Testauswertung

Zusammenfassend kann nach der Auswertung der Tests die folgende Aussage getroffen werden: Ein grundsätzlicher Austausch verschlüsselter und optional signierter E-Mails über eine externe Mailingliste ist möglich. Wenn alle Voraussetzungen positiv erfüllt sind, d.h. für alle Listenteilnehmer entweder gültige Zertifikate, jedoch keine ungültigen, im Gateway gespeichert oder auf einem erreichbaren Verzeichnisdienst hinterlegt sind, dann können E-Mails verschlüsselt an die Listenteilnehmer versendet werden. Dieser Zustand, dass alle Voraussetzungen positiv erfüllt sind, ist für eine größere Mailingliste eher die Ausnahme als die Regel.

Es hat sich während der Tests gezeigt, dass wenn nicht alle Voraussetzungen positiv erfüllt waren, dass dann erhebliche Unterschiede zwischen den getesteten Produkten in der Behandlung der Problemsituation aufgetreten sind. Einige der in diesem Zusammenhang aufgetretenen Fehler oder Probleme sind auf die Entwicklungsphilosophie der Hersteller zurückzuführen. Die Philosophie besagt, dass die Gateways an der Grenze zwischen internem vertrauenswürdigen und externem nicht vertrauenswürdigen Netzwerk platziert werden. Darauf sind Fehler wie unverschlüsselte Rücksendung der Fehlermeldung mit angehängter Originalmail an den Absender und das Abschneiden der Absendersignatur zurückzuführen.

Die Testarchitektur basierte jedoch auf einer externen – externen Kommunikationsbeziehung, d.h. die eingehenden E-Mails kamen über ein externes nicht vertrauenswürdigen Netzwerk und die ausgehenden E-Mails wurden über ein externes nicht vertrauenswürdigen Netzwerk wieder versendet.

Einige Hersteller haben bereits nach Abschluss ihrer Tests Produktänderungen für die nächste Version angekündigt.

Somit kann für die Auswahl und den Einsatz eines Gateways zur Absicherung des E-Mailverkehrs über eine externe Mailingliste nur empfohlen werden, den Fokus auf die Schlechtfall-Tests zu legen.



10. Abkürzungsverzeichnis

CA	Certification Authority
CRL	Certificate Revocation List
http	Hypertext Transfer Protocol
LDAP	Leightweight Directory Access Protocol
NDA	Non Disclosure Agreement
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure



Anhang

11. Beschreibungen der Tests

Es wurde generell davon ausgegangen, dass der sendende Client eine Verschlüsselung an die Liste mit einem abgelaufenen Zertifikat von vornherein unterbindet. Dies gilt nicht für gesperrte Zertifikate.

11.1. Kategorie 1

Aufgabe: Senden einer unverschlüsselten E-Mail mit Anlage an die Liste. Bewertet wird der Empfang der E-Mail bei den Listenmitgliedern (ebenfalls unverschlüsselt).

Inhalt: E-Mail mit beliebigem Body-Text.

Anlage: Eine beliebige Datei von ca. 20-100kB wird angehängt.

Ziel: Empfangen einer unverschlüsselten E-Mail mit Anlage von allen Listenmitgliedern um zu sehen, ob grundsätzlich die Kommunikation innerhalb der Testinfrastruktur möglich ist.

11.2. Kategorie 2

11.2.1. Gutfall-Tests

1. Aufgabe: Senden einer verschlüsselten E-Mail mit Anlage an die Liste. Als S/MIME-Format wird enveloped zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail. Jedem Listenmitglied ist ein eigener öffentlicher Schlüssel zugeordnet.

Inhalt: E-Mail mit beliebigem Body-Text.

Anlage: Eine beliebige Datei von ca. 20-100kB wird angehängt.

Ziel: Empfangen einer verschlüsselten E-Mail mit Anlage durch alle Listenmitglieder und Entschlüsselung der E-Mail durch die Empfänger-Clients.

2. Aufgabe: Senden einer verschlüsselten E-Mail mit Anlage an die Liste. Als S/MIME-Format wird enveloped zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail. Einem Listenmitglied ist kein eigener öffentlicher Schlüssel zugeordnet. Es existiert aber ein Gruppenzertifikat der Zieldomäne des empfangenden E-Mailgateways (Voraussetzung ist ein Gateway auf Empfängerseite, das über ein Gruppenzertifikat verfügt).

Inhalt: E-Mail mit beliebigem Body-Text.

Anlage: Eine beliebige Datei von ca. 20-100kB wird angehängt.

Ziel: Empfangen einer verschlüsselten E-Mail mit Anlage durch alle Listenmitglieder und Entschlüsselung der E-Mail durch die Empfänger-Clients. Dem vorgesehenen E-Mailempfänger ohne User-bezogenen Verschlüsselungsschlüssel wurde seine E-Mail von seinem Gateway entschlüsselt und unverschlüsselt (intern) zugestellt.

11.2.2. Schlechtfall-Tests

1. Aufgabe: Senden einer *verschlüsselten* E-Mail mit Anlage an die Liste. Als S/MIME-Format wird enveloped zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail. Einem Listenmitglied ist kein eigener öffentlicher Schlüssel zugeordnet.

Inhalt: E-Mail mit beliebigem Body-Text.

Anlage: Eine beliebige Datei von ca. 20-100kB wird angehängt.

Ziel: Empfangen einer verschlüsselten E-Mail mit Anlage durch alle Listenmitglieder bis auf einen und Entschlüsselung dieser durch den Empfänger-Client. Dem vorgesehenen E-Mailempfänger ohne Verschlüsselungsschlüssel oder dem Absender wird eine Benachrichtigungsmail über diesen Mangel zugeschickt.

2. Aufgabe: Senden einer *verschlüsselten* E-Mail mit Anlage an die Liste. Als S/MIME-Format wird enveloped zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail. Von einem Listenmitglied ist der öffentliche Schlüssel zeitlich abgelaufen.



Inhalt: E-Mail mit beliebigem Body-Text.
Anlage: Eine beliebige Datei von ca. 20-100kB wird angehängt.
Ziel: Empfangen einer verschlüsselten E-Mail mit Anlage durch alle Listenmitglieder bis auf einen und Entschlüsselung dieser durch den Empfänger-Client. Dem vorgesehenen E-Mailempfänger ohne Verschlüsselungsschlüssel oder dem Absender wird eine Benachrichtigungsmail über diesen Mangel zugeschickt.

11.3. Kategorie 3

11.3.1. Gutfall-Tests

1. Aufgabe: Senden einer *signierten und verschlüsselten* E-Mail mit Anlage an die Liste. Als S/MIME-Format wird SignedAndEnveloped zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail. Jedem Listenmitglied ist ein eigener öffentlicher Schlüssel zugeordnet. Alle Schlüssel sind gültig (nicht abgelaufen und nicht gesperrt).

Inhalt: E-Mail mit beliebigem Body-Text.

Anlage: Eine beliebige Datei von ca. 20-100kB wird angehängt.

Ziel: Empfangen einer signierten und verschlüsselten E-Mail mit Anlage durch alle Listenmitglieder und Entschlüsselung dieser durch den Empfänger-Client. Die Signatur ist erfolgreich zu validieren (Verifikation und Statusprüfung erfolgreich).

11.3.2. Schlechtfall-Tests

1. Aufgabe: Senden einer *verschlüsselten* E-Mail mit Anlage an die Liste. Als S/MIME-Format wird enveloped zwischen den Teilnehmern verwendet. Von einem Listenmitglied ist der öffentliche Schlüssel gesperrt worden. Das Gateway muss Zugriff auf die relevanten Sperrlisten haben, in der das verwendete Zertifikat eingetragen ist, vorzugsweise per LDAP- oder HTTP-Protokoll aus einem X.500-Directory. Optional kann eine Validierung bei einem OCSP-Responder erfolgen vorausgesetzt in den betreffenden Zertifikaten ist im RFC822Name die OCSP URI eingetragen. Bewertet wird der Empfang der E-Mail.

Inhalt: E-Mail mit beliebigem Body-Text.

Anlage: Eine beliebige Datei von ca. 20-100kB wird angehängt.

Ziel: Empfangen einer verschlüsselten E-Mail mit Anlage durch alle Listenmitglieder bis auf einen und Entschlüsselung dieser durch den Empfänger-Client.

Optional: Dem vorgesehenen E-Mailempfänger mit gesperrtem Verschlüsselungsschlüssel wird eine Benachrichtigungsmail über diesen Mangel zugeschickt und/oder der Absender wird über den Mangel informiert.

2. Aufgabe: Senden einer *signierten und verschlüsselten* E-Mail mit einem gesperrten Signatur-Zertifikat. Das Gateway muss Zugriff auf die relevanten Sperrlisten haben, in der das verwendete Zertifikat eingetragen ist, vorzugsweise per LDAP- oder HTTP-Protokoll aus einem X.500-Directory. Optional kann eine Validierung bei einem OCSP-Responder erfolgen vorausgesetzt in den betreffenden Zertifikaten ist im RFC822Name die OCSP URI eingetragen. Bewertet wird der Empfang der E-Mail.

Inhalt: E-Mail mit beliebigem Body-Text.

Anlage: Eine beliebige Datei von ca. 20-100kB wird angehängt.

Ziel: Zu erkennen, ob ein Bezug sowie die Auswertung von Sperrlisten möglich ist, zu erkennen, ob das Gateway das Zertifikat als gesperrt ausweist.

Optional: Die E-Mail wird, entsprechend gekennzeichnet, an die Liste weiterleitet und/oder dem E-Mailsender wird eine E-Mail mit der Information über den Mangel seines Signaturzertifikates (gesperrt) gesendet. In jedem Fall sollte eine praktikable Reaktion auf das gesperrte Signatur-Zertifikat erfolgen.

Hinweis: Abhängig von der Konfiguration des Mailinglistenservers ist der Absender selbst Empfänger der Liste. Damit könnte er ggf. eine Kopie der versandten E-Mail bekommen. Diese enthält dann den Hinweis auf die ungültige Signatur (siehe „Ziel“). Der Empfang der versendeten E-



Mail an den originalen Absender kann auch im Gutfall als Bestätigung für die erfolgreiche Bearbeitung sinnvoll sein. Deswegen wird hier von einer derartigen Konfiguration ausgegangen. Dennoch sollte eine extra E-Mail an den E-Mailsender die Aufmerksamkeit gezielt auf diesen Mangel hinweisen.

- 3. Aufgabe:** Senden einer *verschlüsselten* E-Mail mit einem gesperrten Verschlüsselungs-Zertifikat (Listen-Zertifikat). Das Gateway muss Zugriff auf die relevanten Sperrlisten haben, in der das verwendete Zertifikat eingetragen ist, vorzugsweise per LDAP- oder HTTP-Protokoll aus einem X.500-Directory. Es kann auch eine Validierung bei einem OCSP-Responder erfolgen vorausgesetzt in den betreffenden Zertifikaten ist im RFC822Name die OCSP URI eingetragen. Bewertet wird der Empfang der E-Mail.
- Hinweis:** Es ist normalerweise Aufgabe des sendenden E-Mail-Clients für die Statusprüfung zu sorgen. Im Falle eines gesperrten Zertifikates sollte eine E-Mail dann nicht verschlüsselt werden können. Falls ein Client dies aber doch macht, muss spätestens das E-Mail-Gateway den Mangel bemerken und den Absender darüber informieren, das seine E-Mail nicht weitergeleitet wurde. Der neue Listenschlüssel sollte vom E-Mail-Gateway idealerweise gleich mitgeschickt werden.
- Inhalt:** E-Mail mit beliebigem Body-Text.
- Anlage:** Eine beliebige Datei von ca. 20-100kB wird angehängt.
- Ziel:** Zu erkennen, ob ein Bezug sowie die Auswertung von Sperrlisten auch des Listenzertifikates möglich ist, daran anschließend zu erkennen, ob das Gateway das Zertifikat als gesperrt ausweist.
- Optional:** Der Inhalt der E-Mail sollte nicht an die Liste weitergeleitet werden. Dem E-Mailsender sollte eine E-Mail über die nicht erfolgte Weiterleitung unter Angabe des Grundes (gesperrtes Zertifikat) zugesendet werden. Wird die E-Mailadresse in der Liste vorgefunden, sollte das aktuelle (gültige) Zertifikat mit der Benachrichtigungsmail mitgeschickt werden.

11.4. Kategorie 4

11.4.1. Gutfall-Tests.

- 1. Aufgabe:** Senden einer *verschlüsselten* E-Mail mit Anlage an die Liste. Als S/MIME-Format wird enveloped zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail. Einem Listenmitglied ist kein eigener öffentlicher Schlüssel zugeordnet. Dieser ist aber gültig und befindet sich in einem erreichbaren LDAP-Verzeichnis.
- Inhalt:** E-Mail mit beliebigem Body-Text.
- Anlage:** Eine beliebige Datei von ca. 20-100kB wird angehängt.
- Ziel:** Empfangen einer verschlüsselten E-Mail mit Anlage durch alle Listenmitglieder und Entschlüsselung dieser durch den Empfänger-Client. Das Gateway hat somit den fehlenden Schlüssel gefunden und für die Verschlüsselung genutzt. Es wurden keine Benachrichtigungs-E-Mails verschickt.
- 2. Aufgabe:** Senden einer *verschlüsselten* E-Mail mit Anlage an die Liste. Als S/MIME-Format wird enveloped zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail. Einem Listenmitglied ist kein eigener öffentlicher Schlüssel zugeordnet. Dieser ist aber gültig und befindet sich in einem erreichbaren LDAP-Verzeichnis. Dort hinterlegt sind 1 Signatur- und 1 Verschlüsselungsschlüssel für den Mailempfänger.
- Inhalt:** E-Mail mit beliebigem Body-Text.
- Anlage:** Eine beliebige Datei von ca. 20-100kB wird angehängt.
- Ziel:** Empfangen einer verschlüsselten E-Mail mit Anlage durch alle Listenmitglieder und Entschlüsselung dieser durch den Empfänger-Client. Das Gateway hat somit den fehlenden Schlüssel gefunden und den Schlüssel mit der Keyextension „key/data encipherment“ für die Verschlüsselung genutzt. Es wurden keine Benachrichtigungs-E-Mails verschickt.
- 3. Aufgabe:** Senden einer *verschlüsselten* E-Mail mit Anlage an die Liste. Als S/MIME-Format wird enveloped zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail. Von ei-



nem Listenmitglied ist der öffentliche Schlüssel zeitlich abgelaufen. Ein neuer Schlüssel ist gültig und über LDAP erreichbar.

Inhalt: E-Mail mit beliebigem Body-Text.

Anlage: Eine beliebige Datei von ca. 20-100kB wird angehängt.

Ziel: Empfangen einer verschlüsselten E-Mail mit Anlage durch alle Listenmitglieder und Entschlüsselung dieser durch den Empfänger-Client. Das Gateway hat den abgelaufenen Schlüssel durch den neuen ersetzt und diesen für die Verschlüsselung genutzt. Es wurden keine Benachrichtigungs-E-Mails verschickt.

4. Aufgabe: Senden einer *verschlüsselten* E-Mail mit Anlage an die Liste. Als S/MIME-Format wird enveloped zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail. Von einem Listenmitglied ist der öffentliche Schlüssel gesperrt worden. Ein neuer Schlüssel ist gültig und über LDAP erreichbar.

Inhalt: E-Mail mit beliebigem Body-Text.

Anlage: Eine beliebige Datei von ca. 20-100kB wird angehängt.

Ziel: Empfangen einer verschlüsselten E-Mail mit Anlage durch alle Listenmitglieder und Entschlüsselung dieser durch den Empfänger-Client. Das Gateway hat den gesperrten Schlüssel durch den neuen ersetzt und diesen für die Verschlüsselung genutzt. Es wurden keine Benachrichtigungs-E-Mails verschickt.

11.4.2. Schlechtfall-Tests

1. Aufgabe: Senden einer *verschlüsselten* E-Mail mit Anlage an die Liste. Als S/MIME-Format wird enveloped zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail. Einem Listenmitglied ist kein eigener öffentlicher Schlüssel zugeordnet. Dieser existiert auch in keinem erreichbaren LDAP-Verzeichnis.

Inhalt: E-Mail mit beliebigem Body-Text.

Anlage: Eine beliebige Datei von ca. 20-100kB wird angehängt.

Ziel: Empfangen einer verschlüsselten E-Mail mit Anlage durch alle Listenmitglieder bis auf einen und Entschlüsselung dieser durch den Empfänger-Client. Dem vorgesehenen E-Malempfänger ohne Verschlüsselungsschlüssel wird eine Benachrichtigungsmail über diesen Mangel zugeschickt.

2. Aufgabe: Senden einer *verschlüsselten* E-Mail mit Anlage an die Liste. Als S/MIME-Format wird enveloped zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail. Von einem Listenmitglied ist der öffentliche Schlüssel zeitlich abgelaufen. Ein neuer Schlüssel existiert in keinem erreichbaren LDAP-Verzeichnis.

Inhalt: E-Mail mit beliebigem Body-Text.

Anlage: Eine beliebige Datei von ca. 20-100kB wird angehängt.

Ziel: Empfangen einer verschlüsselten E-Mail mit Anlage durch alle Listenmitglieder bis auf einen und Entschlüsselung dieser durch den Empfänger-Client. Dem vorgesehenen E-Malempfänger ohne Verschlüsselungsschlüssel wird eine Benachrichtigungsmail über diesen Mangel zugeschickt.

3. Aufgabe: Senden einer *verschlüsselten* E-Mail mit Anlage an die Liste. Als S/MIME-Format wird enveloped zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail. Von einem Listenmitglied ist der öffentliche Schlüssel gesperrt worden. Ein neuer Schlüssel existiert in keinem erreichbaren LDAP-Verzeichnis.

Inhalt: E-Mail mit beliebigem Body-Text.

Anlage: Eine beliebige Datei von ca. 20-100kB wird angehängt.

Ziel: Empfangen einer verschlüsselten E-Mail mit Anlage durch alle Listenmitglieder bis auf einen und Entschlüsselung dieser durch den Empfänger-Client. Dem vorgesehenen E-Malempfänger, dessen Verschlüsselungsschlüssel gesperrt wurde, wird eine Benachrichtigungsmail über diesen Mangel zugeschickt. Aus dieser Mail muss auch hervorgehen, dass versucht wurde, einen neuen Schlüssel über LDAP-Verzeichnisdienste zu finden.



12. Formularvorlagen

12.1. Event Log

AG 7 Machbarkeitstest „verschlüsselte E-Mail mit externen Mailinglisten“ unter Einsatz eines E-Mail Gateways

Event-Log

Benutzen Sie diese Seite, um ungewöhnliche Handlungen oder Ereignisse aufzuzeichnen, die während der Tests stattfinden. Sie können auch diese Seite benutzen, um etwas zu dokumentieren, das Sie für zukünftige Tests für wissenswert halten.

<i>Datum (MM/DD/ YY)</i>	<i>Zeit (HH:MM:)</i>	<i>Ereignisbeschreibung</i>	<i>Durchgeführte Handlung</i>	<i>Ihr Name</i>

**INFORMATIONEN, DIE AUF DIESER SEITE AUFGEZEICHNET WERDEN, BLEIBEN VERTRAULICH.
SIE DÜRFEN AUSSERHALB DER NDA-TEILNEHMER NICHT DISKUTIERT WERDEN.**



12.2. Rückmeldebogen Empfänger

Test-Rückmeldebogen

Teilnehmer:

E-Mailadresse:

Eingesetzter Client:

Listen-E-Mail-Adresse:

Kategorie	Test	Nummer	sendende E-Mailadresse	E-Mail O.K., d.h. das erwartete Ergebnis auf der Seite des Clients ist eingetreten?		Bemerkung
				Ja	Nein	
1	Gut	1				
2	Gut	1				
		2				
	Schlecht	1				
		2				
3	Gut	1				
		Schlecht	1			
			2			
		3				
4	Gut	1				
			2			
			3			
			4			
	Schlecht	1				
			2			
			3			