

Abschlussbericht der Machbarkeitsstudie der AG 7 „Austausch verschlüsselter E-Mail unter Einsatz eines Gruppenzertifikates“

Version *1.0*
Status *Final*
Datum *22.06.2006*

Dieses Dokument einschließlich aller Teile ist urheberrechtlich geschützt – die unveränderte Weitergabe (Vervielfältigung) des Dokuments ist ausdrücklich erlaubt. Jede weitergehende Verwertung außerhalb der engen Grenzen des Urhebergesetzes ist ohne Zustimmung der TeleTrusT unzulässig und strafbar.

© 2006 TeleTrusT Deutschland e.V.

Chamissostraße 11
99096 Erfurt

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	9
2. Abgrenzung	9
3. Architektur und Scope der Studie	9
4. Teilnahmevoraussetzungen	10
4.1. Organisatorische Teilnahmevoraussetzungen	10
4.2. Technische Teilnahmevoraussetzungen	10
5. Testlokationen	10
6. Aufbau der Testszenarien - Testspezifikation	10
7. Testablauf	11
8. Am Test beteiligte Produkte - Übersicht	11
8.1. Eingesetzter Listen-Server	11
8.2. Eingesetzte E-Mailclients	11
8.3. Eingesetztes empfangendes und sendendes Mail Gateway	11
8.4. Genutzte Verzeichnisdienste	12
9. Auswertung der Tests	12
9.1. Verteilung, Installation und Entzug des Gruppensertifikats	12
9.1.1. Verteilung des Gruppensertifikats	12
9.1.2. Installation des Gruppensertifikats	14
9.1.3. Entzug des Gruppensertifikats	15
9.2. Versand und Empfang verschlüsselter E-Mails	15
9.3. Versand und Empfang signierter E-Mails	17
9.4. Zusammenfassung Testauswertung	20
10. Referenzen	22
11. Abkürzungsverzeichnis	22
Anhang	23
12. Beschreibungen der Tests	23
12.1. Kategorie 1	23
12.1.1. Senden einer unverschlüsselten E-mail an den Koordinator	23
12.1.2. Empfang einer verschlüsselten E-Mail mit Gruppensertifikat und Schlüssel	23
12.1.3. Installation des Gruppensertifikates im eigenen E-Mail-Client	23
12.2. Kategorie 2	24
12.2.1. Senden einer verschlüsselten E-Mail an die Liste	24
12.2.2. Senden einer verschlüsselten E-Mail an die Liste	24
12.2.3. Senden einer verschlüsselten E-Mail an die Liste mit gesperrtem Gruppensertifikat	24
12.3. Kategorie 3	24
12.3.1. Senden einer signierten E-Mail an die Liste	24
12.3.2. Senden einer signierten E-Mail an die Liste	25
12.3.3. Senden einer signierten und verschlüsselten E-Mail an die Liste	25
12.3.4. Senden einer signierten und verschlüsselten E-Mail an die Liste	25
13. Formularvorlagen	26
13.1. Event Log	26
13.2. Komponenten der E-Mail-Infrastruktur	27
13.3. Testergebnisse des Mailinglistentests	28

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:



Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

Herr Michael Thiel
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



Humpert & Partner

Herr Frederik Humpert
Mendelstraße 11
D-48149 Münster
www.humpert-partner.de



INFORA GmbH

Herr Joachim Gerber
Cicerostr. 21
D-10709 Berlin
www.infora.de



Information & Communication

NetSys.IT Information & Communication GbR

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



the art of business

noventum consulting GmbH

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

.. **T** .. Systems · **totemo ag**

T-Systems GEI GmbH
Herr Jochen Gottsmann
Rabinstraße 8
D-53111 Bonn
www.t-systems.com

Totemo AG
Herr Marc O. Stöckli
Seestrasse 134a
CH-8700 Kusnacht - Zurich
www.totemo.ch

utimaco[®]
s a f e w a r e

Utimaco Safeware AG
Herr Alexander Chilinski
Hohemarkstraße 22
D-61440 Oberursel
www.utimaco.de

zertificon
solutions

Zertificon Solutions GmbH
Herr René Gawanka
Landsberger Allee 117
D-10407 Berlin
www.zertificon.com

Anerkennungen und Dank für die Unterstützung

Beträchtliche Bemühungen sind in den Entwurf, Planung, die erfolgreiche Durchführung und Auswertung der Tests gegangen. Fachleute von verschiedenen Organisationen, sowohl Anwender, Trust Center 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 AG 7 und das Projektteam möchten ihre Dankbarkeit gegenüber dieser pflichtbewussten Gruppe von Personen und auf ihre unterstützenden Organisationen ausdehnen:

Projektkoordination	<i>Stephan Wappler</i> , noventum consulting GmbH
Entwicklung Testspezifikation	<i>Michael Thiel</i> , Bundesamt für Sicherheit in der Informationstechnik
Bereitstellung Listenzertifikat	<i>Stefan Kirch</i> , T-Systems
Editor Abschlussbericht	<i>Stephan Wappler</i> , noventum consulting GmbH

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

<i>Alexander Chilinski</i> (Utimaco Safeware AG)	<i>Frederik Humpert</i> (Humpert & Partner)
<i>René Gawanka</i> (Zertificon Solutions GmbH)	<i>Mathias Schmid</i> (Deutscher Sparkassen Verlag GmbH)
<i>Joachim Gerber</i> (Infora GmbH)	<i>Ralf Schnitzler</i> (ICC InfoTeSys Computer Consulting GmbH)
<i>Jochen Gottsmann</i> (T-Systems)	<i>Holger Sesterhenn</i> (Utimaco Safeware AG)
<i>Olaf Grupe</i> (noventum consulting GmbH)	<i>Peter Steiert</i> (NetSys.IT GbR)
<i>Dr. Frank Gutberlet</i> (noventum consulting GmbH)	<i>Marc O. Stöckli</i> (Totemo AG)
<i>Kai Hartwich</i> (TeleTrust Deutschland e.V.)	<i>Uwe Völkel</i> (T-Systems)

Zusammenfassung

Im Vordergrund stand die generelle Möglichkeit des Austauschs verschlüsselter E-Mails über Mailinglisten unter Verwendung eines Gruppenschlüsselpaars insbesondere in der Gegenüberstellung mit dem Szenario "Einsatz Gateway". Der Ausgangspunkt für die Durchführung dieser Machbarkeitsstudie war, verschlüsselte und optional signierte E-Mails zwischen Mitgliedern der Arbeitsgruppe AG 7 auszutauschen, die über eine Mailingliste kommunizieren. Die Mitglieder der AG7 gehören verschiedenen Organisationen an und der Listenserver wird durch einen Dienstleister außerhalb der Mitgliederorganisationen zentral im Internet betrieben.

In der Testspezifikation wurden vier Testkategorien mit insgesamt zehn Einzeltests eingeteilt, die sich an Beispielen der Praxis orientierten und die je Teilnehmer abzuarbeiten waren. Jeder Listenteilnehmer hatte jeweils einen Rückmeldebogen auszufüllen, in dem der Status der erhaltenen E-Mails zu erfassen war.

Nach der Auswertung der Event Logs und Rückmeldebögen kann zusammenfassend festgehalten werden, dass grundsätzlich ein Austausch verschlüsselter E-Mails über eine externe Mailingliste möglich ist.

Es hat sich während der Tests gezeigt, dass die Vorbereitung und im Speziellen der Schlüsselaustausch sehr aufwändig war. Weiterhin kann festgehalten werden, dass Microsoft Outlook Native Nutzer unbedingt ein Schlüsselpaar welches auf die eigene E-Mailadresse ausgestellt ist benötigen, um verschlüsselte oder signierte E-Mails zu versenden. Bei Lotus Notes Usern muss diese Voraussetzung nicht gegeben sein.

Eine besondere Hürde organisatorischer Art hatten die Teilnehmer zu überwinden, die zentral gemanagte Verschlüsselungsgateways eingesetzt haben. Die Anpassung der Konfiguration und die Installation weiterer Root- und Sub-CA-Zertifikate haben bei einer solchen Installation weit reichende Folgen. Hierfür sind die festgelegten Regeln einzuhalten, was zu zeitlichen Verzögerungen führen kann.

Im Vergleich zu Machbarkeitsstudie „Austausch verschlüsselter E-Mail über externe Mailinglisten unter Einsatz eines E-Mail Gateways“ stellt die Lösung mit einem verteilten Gruppenschlüsselpaar eine Alternative dar. Jedoch ist der Lösung unter Einsatz eines E-Mail-Gateway im Anbetracht des Aufwandes für das Schlüsselmanagement der Vorzug zu geben.

Zur Durchführung der Machbarkeitsstudie ist noch erwähnenswert, dass diese zweite Studie im September 2005 gestartet und im März 2006 beendet wurde. Während dieser Zeit hat es, wie bereits bei der ersten Studie, nicht ein persönliches Treffen der Teilnehmer 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 erfordert. 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 AG 7 auszutauschen, die über eine Mailingliste kommunizieren. In der Regel gehören die Mitglieder solcher 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.

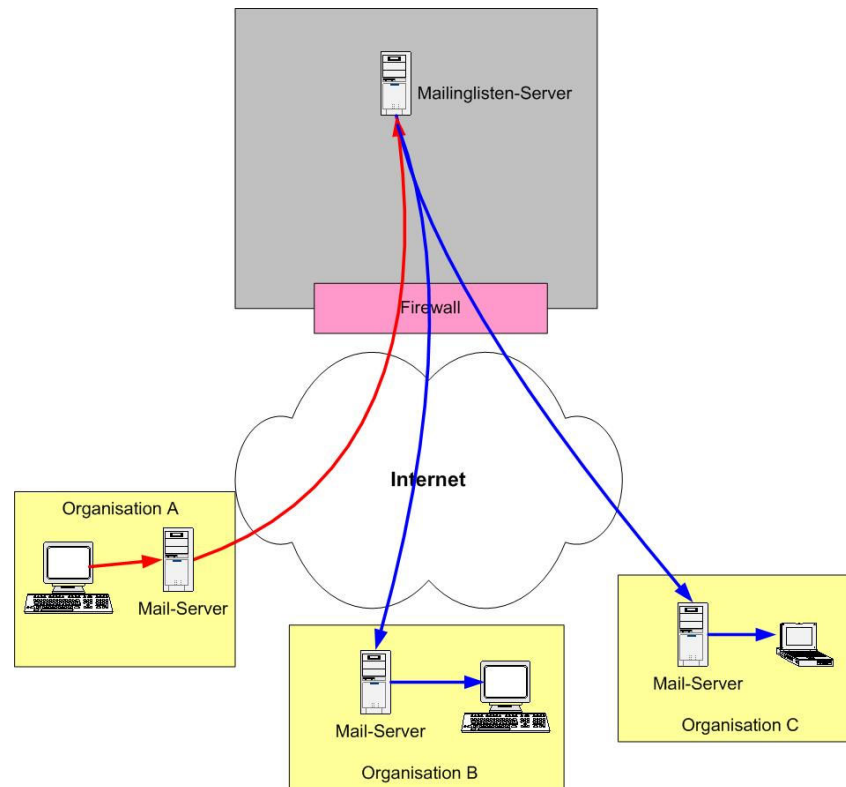


Abbildung 1: Ausgangssituation

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 managebar.

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 die Tests gezeigt haben, 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 zweijährlich 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. Nur das Löschen der Adresse von der Liste führt dazu, dass der Teilnehmer die E-Mail nicht mehr direkt zugestellt bekommt. Zusätzlich muss das Root- und die Sub-CA-Zertifikate der ausstellenden CAs für die Verwendung des öffentlichen Listenschlüssels in den entsprechenden Clients installiert werden.

Die Tests und die Auswertung werden nachfolgend beschrieben.

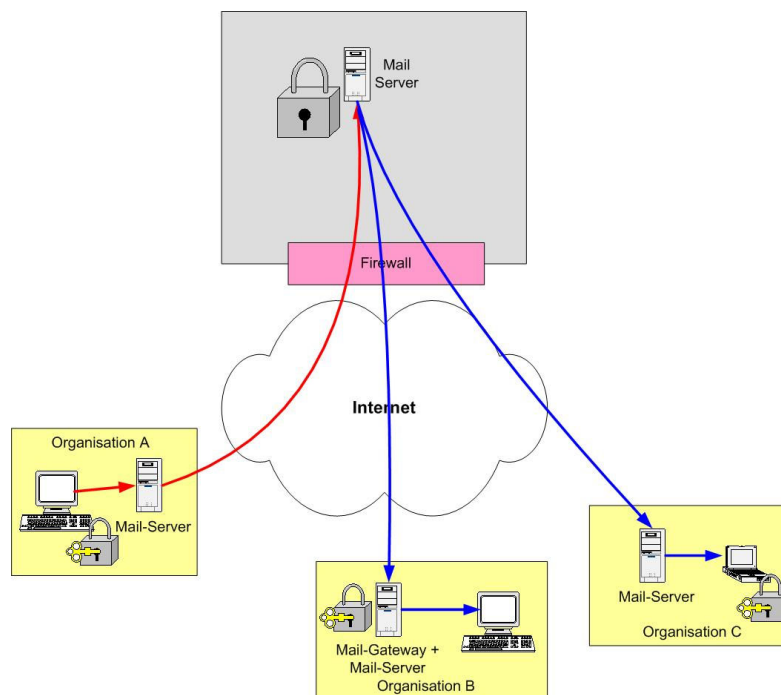


Abbildung 2: Nutzung eines Gruppenschlüssels

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 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.

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 werden muss. Weiterhin muss jeder Listenteilnehmer bzw. jede teilnehmende Organisation im Besitz eines eigenen Schlüsselpaares sein und das Root- und die Sub-CA-Zertifikate der ausstellenden CAs für die Verwendung des öffentlichen Listenschlüssels in den entsprechenden Clients installieren.

Der Abschlussbericht zu diesen Tests und die Auswertung wurden bereits zur CeBIT 2005 veröffentlicht und können von der TeleTrust Webseite unter <http://www.teletrust.de> bezogen werden.

2. Abgrenzung

Die Durchführung der Tests diente 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 AG 7 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 und Scope der Studie

Ziel der Machbarkeitsuntersuchung der Lösung 2 war es, an eine Mailingliste sichere Nachrichten zu senden, die mit dem auf die E-Mailadresse der Mailingliste ausgestellten Zertifikat verschlüsselt sind. Das Gruppenzertifikat wird auf die E-Mailadresse der Mailingliste ausgestellt.

Die verschlüsselten E-Mails werden an den Listenserver gesendet. Dieser löst dann die Liste auf, indem die Teilnehmeradressen im BCC-Feld eingefügt werden. Der Mailinglistenserver sendet die Emails un-

verändert an die Mailinglistenmitglieder weiter. Der Teilnehmer muss den Entschlüsselungsschlüssel (pkcs#12) in seinen Mailclient einbinden können, und entschlüsselt damit die Email.

Neben der Basisfunktionalität der Verschlüsselung sollen optional die Möglichkeiten der Signatur und die Einbindung von Verzeichnis- und Validierungsdiensten mit getestet werden.

Das Vorgehen beim Empfang einer signierten E-Mail sollte folgendermaßen aussehen:

Der Mailinglistenserver leitet die Email unverändert an die Teilnehmer weiter. Der Emailclient des Teilnehmers überprüft die Signatur und die Gültigkeit der verwendeten Zertifikate. Zur Signatur könnte sowohl ein persönliches Zertifikat als auch das Gruppensertifikat verwendet werden. In dieser Studie werden beide Fälle getestet.

Weiterhin werden auch der Aufwand und die Voraussetzungen zur authentischen und sicheren Verteilung des Gruppensertifikates incl. privaten Schlüssels dokumentiert.

4. Teilnahmevoraussetzungen

4.1. Organisatorische Teilnahmevoraussetzungen

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

- Die Teilnehmer mussten TTT-Mitglied sein.
- T-Systems erzeugt das für diesen Test benötigte Schlüsselmaterial und Gruppensertifikat, und stellt es der AG7 für den weiteren Testablauf zur Verfügung. T-Systems stellt außerdem ein Verzeichnis mit den zugehörigen CA-Zertifikaten und Sperrlisten für diesen Test bereit.

4.2. Technische Teilnahmevoraussetzungen

Die technischen Voraussetzungen für die allgemeinen Tests waren:

- X.509 v3 Zertifikate, eigene PKI oder von einem Trust Center zur Signatur
- Das Einbinden des X509 v3 Gruppensertifikates in den E-Mailclient
- Das Einbinden des privaten Schlüssels zum Gruppensertifikat in den E-Mailclient
- Asymmetrische Schlüssellänge mindestens 1.024 Bit
- Symmetrische Schlüssellänge 128 Bit
- S/MIME kompatible Mailsysteme

5. Testlokationen

Die Testteilnehmer führten die Tests in ihren eigenen Geschäftsräumen aus. Der Mailinglistenserver wurde von TeleTrust zur Verfügung gestellt.

6. Aufbau der Testszenarien - Testspezifikation

Die Testszenarien werden in drei verschiedene Kategorien eingeteilt. Weiterhin werden die Testfälle nach Gut- und Schlechtfalltests unterschieden. Mit den Schlechtfalltests wurden besondere Zustände erzeugt, die vom E-Mail-Client entsprechend zu interpretieren waren.

Kategorie 1

Hier wurde der Aufwand zur Verteilung und Installation des Gruppenzertifikates und der persönlichen Zertifikate der Teilnehmer ermittelt.

Kategorie 2

Diese E-Mails dienten zur Überprüfung des verschlüsselten Austauschs von E-Mails über den Mailinglistenserver.

Kategorie 3

Diese E-Mails dienten zur Überprüfung des verschlüsselten und signierten Austauschs von E-Mails über den Mailinglistenserver. Ziel war die Überprüfung des Umgangs mit der Signatur und mit Zertifikatsstatusdiensten.

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 allen Teilnehmern im Vorfeld zur Verfügung gestellt.

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. Eingesetzter Listen-Server

- Standardlösung von TeleTrust

8.2. Eingesetzte E-Mailclients

- Microsoft Outlook 2003 SP 2
- Microsoft Outlook 2000 / TrustedMime V3.3.1, Guardeon Solutions
- Microsoft Outlook 2000 SP 3, T-Telesec Signet 1.6
- Microsoft Outlook Express 6
- Lotus Notes R 6.5
- Lotus Notes R 6.5.2

8.3. Eingesetztes empfangendes und sendendes Mail Gateway

- SecurE-Mail Gateway, Utimaco Safeware AG
- Z1 SecureMail Gateway Enterprise Version 2.2, Zertificon Solutions GmbH
- Z1 SecureMail Gateway Enterprise Version 2.3, Zertificon Solutions GmbH

8.4. Genutzte Verzeichnis- und Validierungsdienste

- Öffentlicher Verzeichnisdienst von T-Systems
- In den Teilnehmerzertifikaten angegebene Sperrlistenbezugspunkte

9. Auswertung der Tests

Bei der Vorbereitung und Durchführung der Tests sind mehrere organisatorische und technische Punkte besonders aufgefallen, die die Komplexität und die aufgetretenen Schwierigkeiten sehr gut widerspiegeln. Nachfolgend werden die einzelnen Punkte detaillierter beschrieben.

9.1. Verteilung, Installation und Entzug des Gruppensertifikats

Bevor mit dem Austausch verschlüsselter und signierter E-Mails begonnen werden kann, steht das Verteilungsproblem des Gruppenschlüsselpaares an die Listenmitglieder. Dies ist eine wesentliche Herausforderung, die auf gar keinen Fall unterschätzt werden darf.

Für die nachfolgenden Betrachtungen wird von den folgenden Werten ausgegangen:

- Konstante Anzahl von ca. 40 Teilnehmern auf der Liste
- Jährlicher Tausch von ca. 5-10 Teilnehmern, d.h. Abgänge und Zugänge

9.1.1. Verteilung des Gruppensertifikats

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. Diese Verteilung an alle Teilnehmer muss in Abhängigkeit von der Gültigkeit der Zertifizierung jährlich oder zweijährlich erfolgen. Weiterhin müssen auch das Root- und die Sub-CA-Zertifikate der ausstellenden CAs für die Verwendung des öffentlichen Listenschlüssels mit an die Listenteilnehmer verteilt werden.

Für die Verteilung Listenschlüsselpaares bieten sich mehrere verschiedene Möglichkeiten an:

1. Verteilung bei einem persönlichen Treffen
2. Zustellung per Einschreiben gegen Unterschrift
3. Download von einer Web-Seite mit Zugangsschutz
4. Sichere Verteilung per verschlüsselter E-Mail

Verteilung bei einem persönlichen Treffen

Diese Möglichkeit konnte aus Mangel an einem persönlichen Treffen nicht genutzt werden. Weiterhin hat die Vergangenheit gezeigt, dass nach der Generierung eines Schlüsselpaares meist zeitnah kein Treffen für die Verteilung möglich ist und dass nie alle Listenmitglieder zu persönlichen Treffen anwesend sind. Die Verteilung über diese Möglichkeit funktioniert, wird jedoch bei größeren Listen als nicht praktikabel angesehen, da nur ein kleiner Teilnehmerkreis zeitnah erreicht wird.

Auch bei den Teilnehmern, die neu auf die Liste aufgenommen werden, funktioniert diese Verteilungsmethode nur in begrenztem Maße, da nicht jeder neue Teilnehmer bei Teilnahme an einem persönlichen Treffen ein PC oder vergleichbareres Device, z.B. einen USB-Stick bei sich führt, so dass er das Schlüsselpaar in Empfang nehmen kann. Weiterhin müssen auch Teilnehmer auf die Liste aufgenommen werden können, ohne dass sie an einem persönlichen Treffen teilgenommen haben. Sie beantragen die Aufnahme ihrer E-Mailadresse beim zuständigen Listenmanager, zum Beispiel per E-

Mail. Ein persönliches Treffen findet dann nicht statt, so dass das Problem wie diese Personen auf sicherem Weg das Schlüsselpaar erhalten nicht gelöst ist.

Zustellung per Einschreiben gegen Unterschrift

Auch diesem Verfahren kann keine Empfehlung ausgesprochen werden. Der initiale Versand des Schlüsselpaares auf einem nicht veränderbaren Medium per Einschreiben gegen Unterschrift oder gar persönliche Zustellung ist für den Koordinator sehr zeit und kostenaufwändig. Weiterhin muss der Koordinator über jede Neuaufnahme von Teilnehmern auf die Liste informiert werden und den Versand an den neuen Teilnehmer initiieren.

Download von einer Web-Seite mit Zugangsschutz

Dieses Verfahren erscheint praktikabler, da es den Zeitaufwand minimiert und einfach realisiert werden kann. Die Teilnehmer können bei Bedarf selbständig das Schlüsselpaar nach einer entsprechenden Authentifizierung beziehen. Dies ist der wesentliche Vorteil dieser Lösung. Die Voraussetzungen und Nachteile sollen hier jedoch auch nicht verschwiegen werden.

Diese Lösung setzt bei der Organisation, unter deren Namen die Mailinglisten betrieben werden, eine entsprechende Web-Seite mit Authentifizierungslösung voraus. Technisch sehen wir die Anforderung nach einer stärkeren Authentifizierung, Minimal bei jedem Teilnehmer eigener Nutzernamen + Passwort und eine mindestens 128 Bit-SSL/TLS abgesicherte Web-Seite. Dies setzt ein umfangreicheres Usermanagement und Passwortmanagement voraus.

Dies ist heute bei sehr vielen Organisationen so nicht gegeben. Weiterhin müssen die Zugangsdaten initial an die Teilnehmer auf einem sicheren Wege verteilt werden. Zusätzlich kommt noch hinzu, dass nicht jede Teilnehmerorganisation eine 128 Bit TLS Verschlüsselung ins Internet oder andere Verfahren wie Active-X-Controls oder Cookies zulässt. Für diese Organisationen müssen wiederum andere Lösungen gefunden werden.

Sichere Verteilung per verschlüsselter E-Mail

Dieses Verfahren wurde im Rahmen der Tests genutzt. Auch bei diesem Verfahren haben sich erhebliche Schwierigkeiten gezeigt. Alle Teilnehmer waren aufgefordert ihren öffentlichen Schlüssel + zugehörige CA-Zertifikate an den Koordinator zu senden.

Einige Teilnehmer haben darauf hin eine signierte E-Mail an den Koordinator gesendet. Bei diesem ist jedoch ein Verschlüsselungsgateway im Einsatz, welches so konfiguriert ist, dass bei eingehenden signierten E-Mails die Signatur überprüft und anschließend entfernt wird. Somit hat der Koordinator nur die öffentlichen Schlüssel der Teilnehmer erhalten, die ihr Zertifikat explizit an die E-Mail angefügt haben.

Weiterhin funktioniert diese Verteilungsmethode nur bei den Listenteilnehmern, die eigene Zertifikate besitzen. Für Listenteilnehmer ohne eigenes Zertifikat müssen andere Lösungen gefunden werden.

Auf die Problematik Validierung der Zertifikate und den daraus resultierenden Problemen bei privaten Public Key Infrastrukturen ohne öffentliche Verteilungspunkte wird hier nicht näher eingegangen.

Zusätzlich sind generell auch die Root- und Sub-CA-Zertifikate der anderen Listenteilnehmer mit zu verteilen, damit die über die Liste empfangenen signierten E-Mails auch überprüft werden können. Auf die hieraus resultierenden organisatorischen und technischen Problemstellungen wird nachfolgend nicht weiter eingegangen, da dieses allgemeine Verteilungsproblem bereits hinreichend in der Literatur diskutiert worden ist bzw. Lösungen wie zum Beispiel die European Bridge-CA (<http://www.bridge-ca.org>) existieren.

9.1.2. Installation des Gruppensertifikats

Nach dem Empfang des Schlüsselpaares wartet auf die Listenteilnehmer die nächste Aufgabe. Die Installation des privaten Listenschlüssels kann gegen die Policies der Organisation des Teilnehmers verstoßen. Zusätzlich muss das Root- und die Sub-CA-Zertifikate der ausstellenden CAs für die Verwendung des öffentlichen Listenschlüssels im entsprechenden Client oder Verschlüsselungsgateway installiert werden.

Installation Gruppensertifikat im Verschlüsselungsgateway

Teilnehmer, die Verschlüsselungsgateways einsetzen, haben besondere Herausforderungen in ihrer eigenen Organisation zu überwinden. Zunächst muss der private Schlüssel + CA-Zertifikate am Gateway installiert und dem User zugeordnet werden. Dieses Vorgehen benötigt die Freigabe durch die entsprechenden Instanzen in der Organisation und setzt technisches Know-How für die Umsetzung am Gateway durch die Administratoren voraus. Dies ist keinesfalls ein leichtes Unterfangen, welches sehr schnell realisiert werden kann.

Installation Gruppensertifikat im Lotus Notes Client

Bevor ein Lotus Notes User das Gruppenschlüsselpaar zum Entschlüsseln nutzen kann, muss er den privaten Schlüssel und die zugehörigen CA-Zertifikate in seine Notes-ID einfügen. Dieses Vorgehen benötigt eventuell die Freigabe durch die entsprechenden Instanzen in der Organisation und setzt technisches Know-How für die Umsetzung am Client voraus.

Hat der User kein eigenes X.509 Zertifikat, sondern will für die Signatur das Listenschlüsselpaar verwenden, dann muss er für diesen Punkt die Konfiguration anpassen. Zusätzlich muss er verhindern, dass die Administratoren seine spezifischen Konfigurationseinstellungen mit zentralen Vorgaben überschreiben.

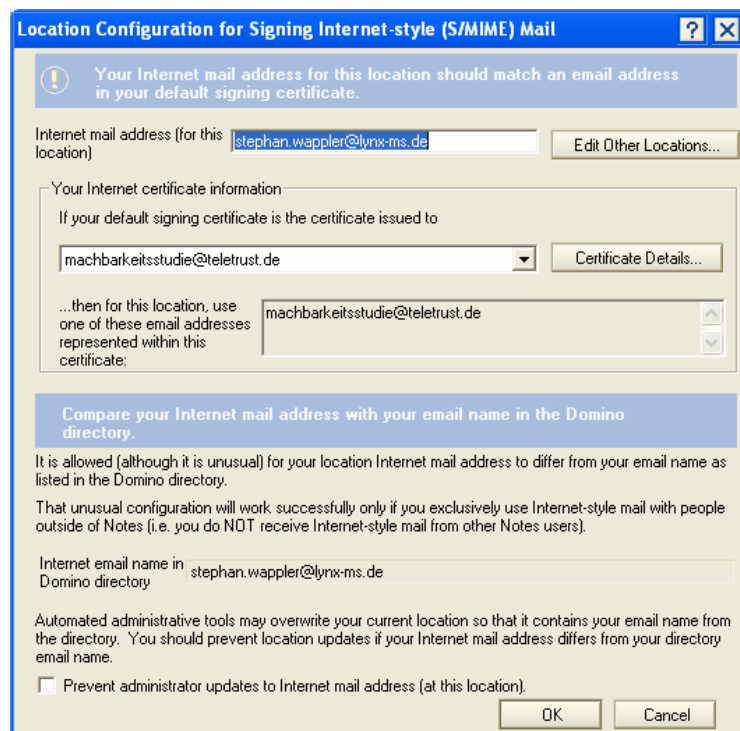


Abbildung 3: Lotus Notes Konfiguration

Installation Gruppensertifikat im Microsoft Outlook Client

Bevor ein Microsoft Outlook User das Gruppenschlüsselpaar zum Entschlüsseln nutzen kann, muss er den privaten Schlüssel und die zugehörigen CA-Zertifikate in seinem Microsoft Zertifikatsspeicher einfügen. Dieses Vorgehen benötigt eventuell die Freigabe durch die entsprechenden Instanzen in der Organisation und setzt technisches Know-How für die Umsetzung am Client voraus.

Zusätzlich muss er verhindern, dass die Administratoren seine spezifische Konfiguration mit zentralen Vorgaben überschreiben.

9.1.3. Entzug des Gruppensertifikats

Der Entzug des privaten Schlüssels bei einem ausscheidenden Teilnehmer von der Liste kann nicht durchgesetzt werden. Nur das Löschen der Adresse von der Liste führt dazu, dass der Teilnehmer die E-Mail nicht mehr direkt zugestellt bekommt. Jedoch bleibt die Person im Besitz des privaten Schlüssels und kann damit auch weiterhin gültige Signaturen ausstellen, wenn die Key Usage im Gruppensertifikat dies zulässt.

9.2. Versand und Empfang verschlüsselter E-Mails

Das Versenden und das Empfangen verschlüsselter E-Mails mit dem Gruppensertifikat haben bei vorliegen eigener Zertifikate bis auf die bereits beschriebene notwendige Konfiguration der eingesetzten Verschlüsselungsgateways keine größeren Probleme bereitet.

Ein Teilnehmer hat dabei jedoch nicht die geforderte Stärke der Verschlüsselung mit mindestens 128 Bit symmetrischer Schlüssellänge erreicht.

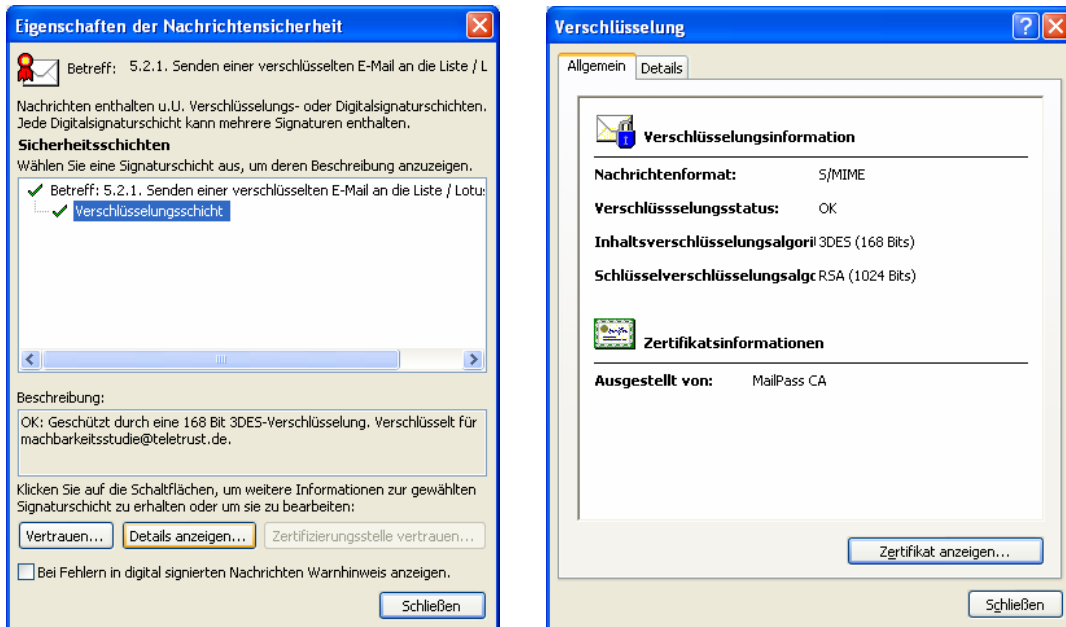


Abbildung 4: Geforderte Verschlüsselungswerte

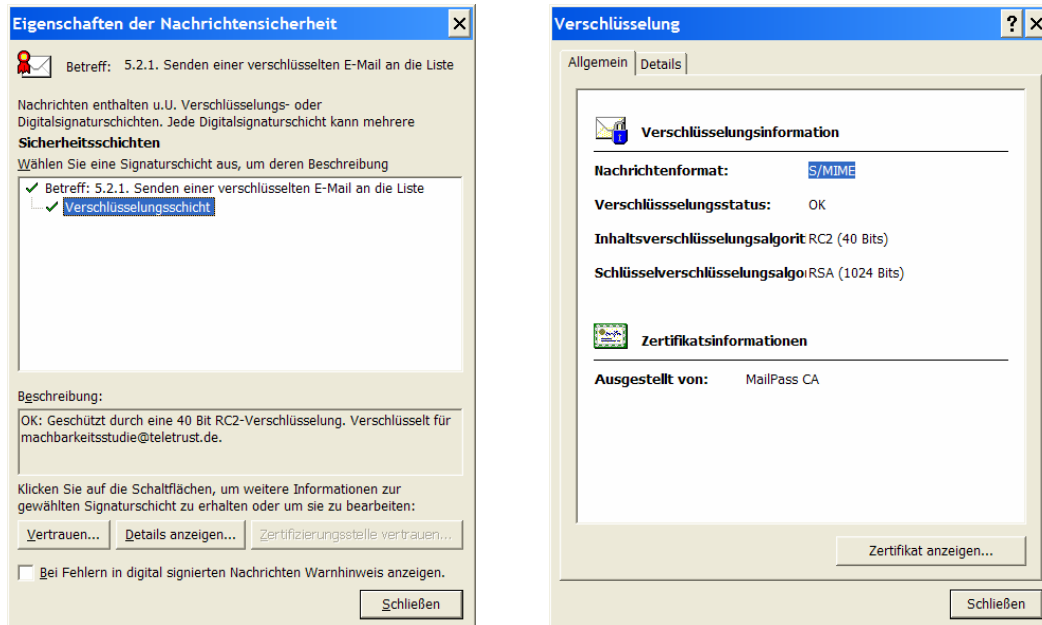


Abbildung 5: Fehlerhafte Verschlüsselungswerte (zu gering)

Microsoft Outlook Client

Das Senden verschlüsselter E-Mails an die Liste ohne, dass der Sendende einen privaten Schlüssel und ein X.509 Zertifikat für seine E-Mailadresse besitzt, war mit den getesteten Microsoft Outlook Versionen in der Standardinstallation nicht möglich. Der Standard-Microsoft-Client prüft, ob ein Schlüsselpaar für die verwendete Versand-E-Mailadresse verfügbar ist, mit dem auch eine verschlüsselte Ablage der E-Mail im eignen Postausgang möglich ist. Die Behebung der Problematik war abhängig von der Outlook-Version teilweise durch spezifische Einstellungen in der Registry möglich. Aufgrund der systemseitigen Risiken bei Eingriffen in die Registry wird an dieser Stelle auf eine Beschreibung der Vorgehensweise verzichtet.

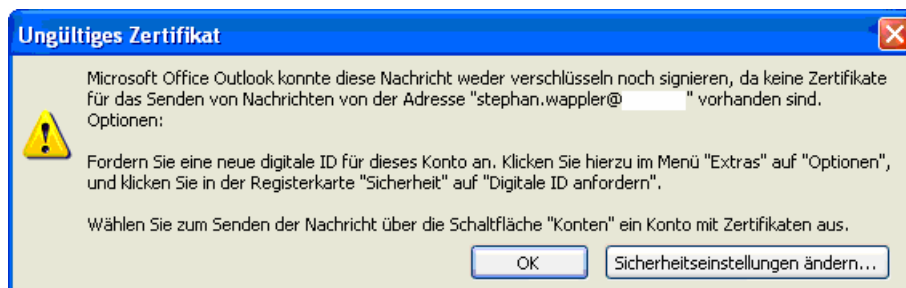


Abbildung 6: Microsoft Outlook Fehlermeldung

Ohne eigenes Zertifikat ist somit ein Versenden nur möglich, wenn ein Open Relay Server verfügbar ist. Andernfalls kann ein Teilnehmer ohne ein Schlüsselpaar ausgestellt auf die eigene E-Mailadresse mit den getesteten Standard-Microsoft Outlook Clients keine verschlüsselten E-Mails versenden.

Microsoft Outlook Express Client

Neben den unter dem Punkt Microsoft Outlook beschriebenen Schwierigkeiten kommt beim Microsoft Outlook Express noch das Problem mit der Verschlüsselungsstärke hinzu. Das Ziel von Microsoft ist es bei der Verschlüsselung kompatibel zu älteren E-Mailclients zu sein. Aus diesem Grund verschlüsselt Microsoft Outlook Express standardmäßig nur mit 40 Bit. Andere Einstellungen werden ignoriert, solange Microsoft Outlook Express nicht die Möglichkeiten des Empfängerclients kennt. Wie dies geschehen soll, wird leider nirgendwo beschrieben. Dieses Problem kann durch den Eintrag eines speziellen Registry Key behoben werden.



Abbildung 7: Fehlermeldung Microsoft Outlook Express

Lotus Notes Clients

Das oben beschriebene Problem ist nicht mit den getesteten Lotus Notes Clients aufgetreten. Diese nutzen für die verschlüsselte Ablage der versendeten E-Mails das Notes-Schlüsselpaar aus der Notes-ID.

9.3. Versand und Empfang signierter E-Mails

Der Empfang signierter E-Mails hat deutlich mehr Probleme bereitet. Diese Probleme waren teilweise unabhängig von der Nutzung des Gruppenzertifikats für Signaturzwecke und stellten zum Beispiel allgemeine Probleme beim Einsatz eines zentralen Gateways bzw. bei Lotus Notes dar.

Microsoft Outlook Client

Das Senden signierter E-Mails an die Liste ohne, dass der Sendende einen privaten Schlüssel und ein X.509 Zertifikat für seine E-Mailadresse besitzt, war mit den getesteten Microsoft Outlook Versionen in der Standardinstallation nicht möglich. Der Standard-Microsoft-Client prüft, ob ein Schlüsselpaar für die verwendete Versand-E-Mailadresse verfügbar ist. Die Nutzung des privaten Schlüssels des Listenschlüsselpaares für die Signatur war nicht möglich. Die Behebung der Problematik war abhängig von der Outlook-Version teilweise durch spezifische Einstellungen in der Registry möglich. Aufgrund der systemseitigen Risiken bei Eingriffen in die Registry wird an dieser Stelle auf eine Beschreibung der Vorgehensweise verzichtet.

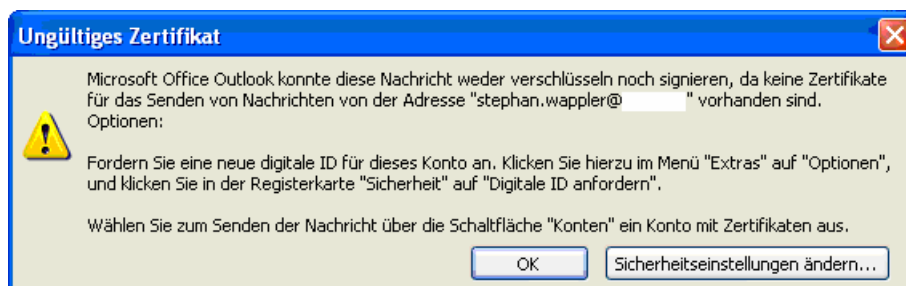


Abbildung 8: Microsoft Outlook Fehlermeldung

Der Empfang signierter E-Mails hat jedoch keine Schwierigkeiten bereitet. Auch mit dem Listenschlüsselpaar signierte E-Mails haben bei den getesteten Clients zu keinen Fehlermeldungen geführt, sondern wurden als korrekt signiert mit allen Informationen dargestellt.



Abbildung 9: Darstellung Signaturinformationen

Lotus Notes Clients

Das oben beschriebene Problem beim Versand signierter E-Mails ist nicht mit den getesteten Lotus Notes Clients aufgetreten. Diese nutzen für die Signatur der E-Mails das Listenschlüsselpaar aus der Notes-ID. Jedoch wird dem Nutzer vor dem Versenden der signierten E-Mail noch ein Warnhinweis gegeben.

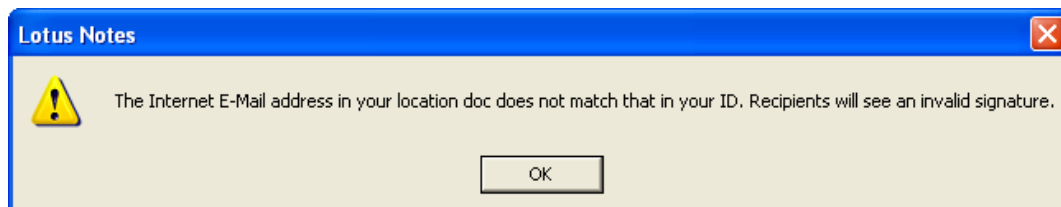


Abbildung 10: Lotus Notes Warnhinweis

Beim Empfang und Öffnen von mit dem Gruppensertifikat signierter E-Mails wurde ein Warnhinweis in der Statuszeile des Lotus Notes Clients ausgegeben. Da wie nachfolgend abgebildet, diese Meldungen nicht sehr deutlich dargestellt werden, darf davon ausgegangen werden, dass viele User diesen Warnhinweis gar nicht zur Kenntnis nehmen werden.

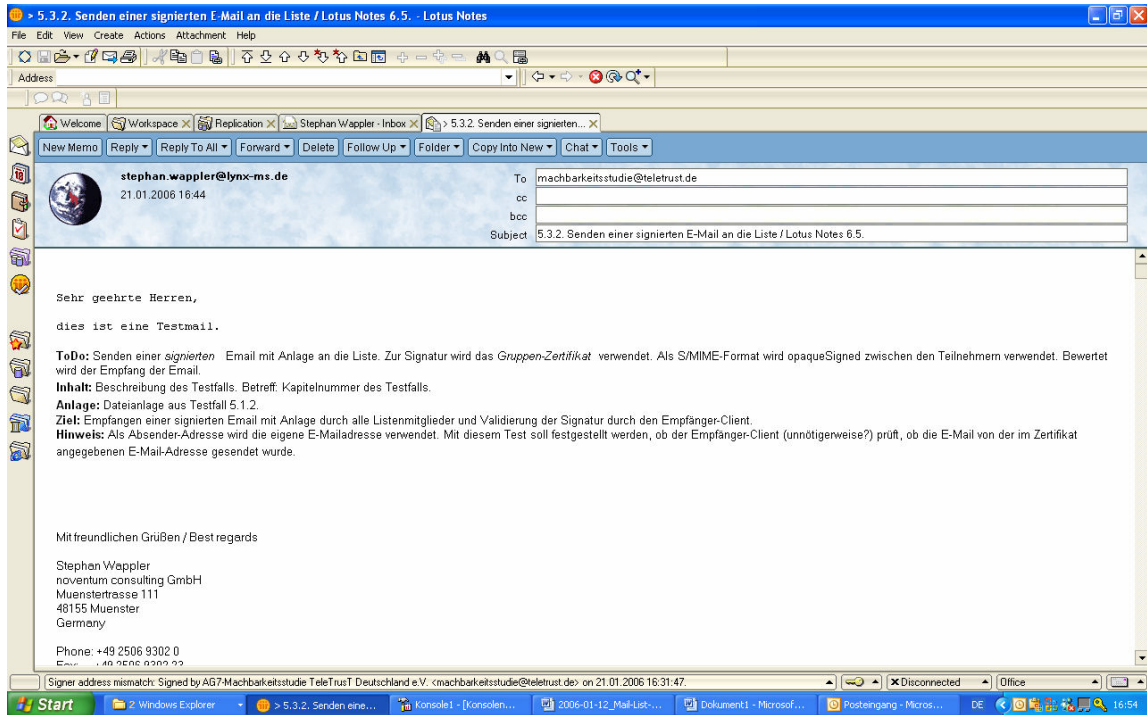


Abbildung 11: Darstellung mit Gruppenzertifikat signierte E-Mail



Abbildung 12: Vergrößerung der Meldung in der Statuszeile

Ein weiteres Problem besteht bei mit einem Outlook-Plug-In signierten E-Mails. Das Öffnen signierter oder verschlüsselter und signierter E-Mails mit diesem Plug-In hat auf den getesteten Lotus Notes Clients zu der folgenden Fehlermeldung geführt:

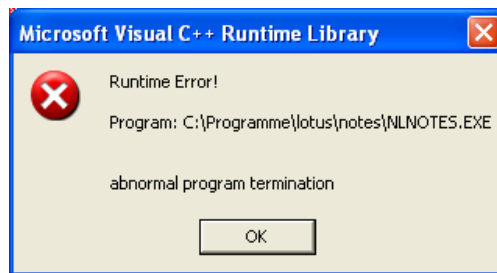


Abbildung 13: Lotus Notes Fehlermeldung

Nach dieser Fehlermeldung hat sich der Client automatisch geschlossen. Nicht gesicherte Daten sind bzw. waren verloren. Weitere Tests mit Lotus Notes R 7 Clients haben gezeigt, dass in dieser Version das beschriebene Problem nicht mehr aufgetreten ist.

Verschlüsselungsgateways

Signierte E-Mails, die von einem zentralen Verschlüsselungsgateway empfangen und nach der Überprüfung und Entfernung der Signatur an Lotus Notes Clients weitergeleitet wurden, haben den oben beschriebenen kritischen Fehler nicht ausgelöst.

Jedoch hat ein bei einem der Teilnehmer eingesetztes Gateway dazu geführt, dass ausgehende bereits auf dem Client signierte E-Mails verändert wurden, so dass die empfangenden Clients eine fehlerhafte Signatur ausgewiesen haben.

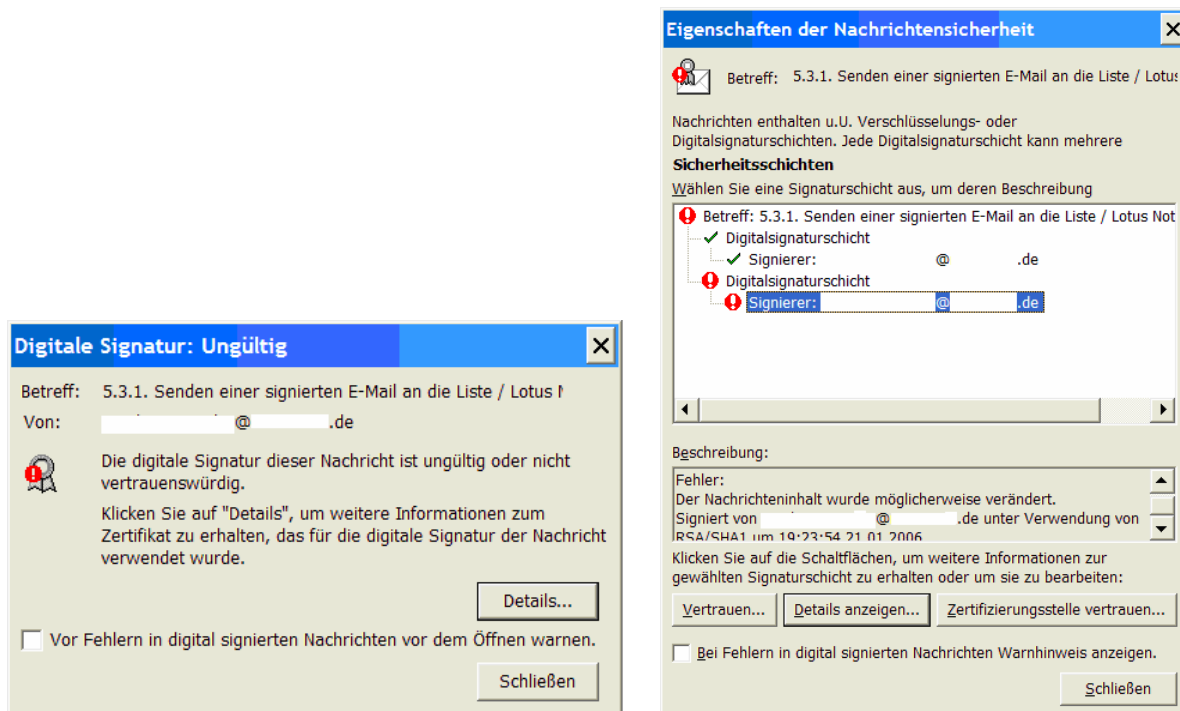


Abbildung 14: Fehlerhafte Signatur durch Gateway verursacht

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 unter Nutzung eines Gruppenzertifikats ist möglich.

Es hat sich während der Tests gezeigt, dass die Vorbereitung und im Speziellen der Schlüsselaustausch sehr aufwändig war. Weiterhin kann festgehalten werden, dass Microsoft Outlook Native Nutzer unbedingt ein Schlüsselpaar ausgestellt auf die eigene E-Mailadresse benötigen, um verschlüsselte oder signierte E-Mails zu versenden. Bei Lotus Notes Usern muss diese Voraussetzung nicht erfüllt sein. Sie können auch ohne eigenes Schlüsselpaar verschlüsselte oder signierte E-Mails versenden. Jedoch sind hier andere Schwierigkeiten aufgetreten. Besonders zu erwähnen ist hier der Absturz des Clients bei der Analyse der Signatur. Weiterhin ist die klare Empfehlung immer zeitnah die aktuellen Versionen zu installieren und zu nutzen.

Eine besondere Hürde organisatorischer Art hatten die Teilnehmer zu überwinden, die zentral gemanagte Verschlüsselungsgateways einsetzen. Die Anpassung der Konfiguration und die Installation weiterer Root- und Sub-CA-Zertifikate haben bei einer solchen Installation weit reichende Folgen. Die Installation und die Aussprache des Vertrauens erfolgt in diesem Falle für Benutzer, die derselben Benutzergruppe

im Gateway angehören. Hierfür sind die festgelegten Regeln einzuhalten, was zu zeitlichen Verzögerungen führen kann.

Weiterhin erscheint die Erstellung von Signaturen mit dem Gruppensertifikat als nicht sinnvoll. Zum einen wird nachdem Öffnen einer derart signierten E-Mail von einigen Clients ein Warnhinweis gegeben, der manchen Empfänger verwirren wird und zum anderen kann einem von der Liste ausscheidenden Teilnehmer das Schlüsselpaar nicht entzogen werden. Dieser ehemalige Listenteilnehmer behält den privaten Schlüssel und kann damit auch weiterhin ausgehende E-Mails bis zum Ablauf der Gültigkeit signieren. Deshalb wird empfohlen, die Key Usage für das Schlüsselpaar auf Data Encryption oder Key Encipherment, d.h. Verschlüsselung zu beschränken und die Key Usages Content-Comittment (früher: Non-Repudiation) und Digital Signature nicht zu zulassen.

Im Vergleich zu Machbarkeitsstudie „Austausch verschlüsselter E-Mail über externe Mailinglisten unter Einsatz eines E-Mail Gateways“ stellt die Lösung mit einem verteilten Gruppenschlüsselpaar eine Alternative dar.

Einschränkende Hinweise:

Der Gruppenschlüssel erweist sich beim Einsatz in einer größeren heterogenen Benutzergruppe als sehr schwierig, da bei den einzelnen Benutzern unterschiedliche organisatorische und technische Voraussetzungen gegeben sind. Die Installation und Nutzung des Gruppenschlüsselpaares erfordert teilweise Unterstützung durch die Administratoren in den Nutzer Organisationen und Ausnahmegenehmigungen bzw. Freigaben durch die Sicherheitsverantwortlichen, da in die Security-Policies der Organisationen eventuell eingegriffen wird.

Fazit:

In Anbetracht des Aufwandes für das Schlüsselmanagement und der Implementation der Gruppenschlüssel ist der Lösung unter Einsatz eines E-Mail-Gateways Vorzug zu geben.

10. Referenzen

1.)

Testspezifikation für „sicheren E-Mailaustausch mit externen Mailinglisten“ unter Einsatz eines Gruppenzertifikates im Rahmen einer Machbarkeitsstudie über sichere Kommunikation von Mitgliedern der AG7
TeleTrusT Deutschland e.V.

2.)

Testspezifikation für „verschlüsselte E-Mail mit externen Mailinglisten“ unter Einsatz eines E-Mail Gateways im Rahmen einer Machbarkeitsstudie über sichere Kommunikation von Mitgliedern der AG7
TeleTrusT Deutschland e.V.

3.)

Testspezifikation Interoperabilität und Funktionalität für den Austausch sicherer E-Mails mit Zertifikaten unter der European Bridge-CA
TeleTrusT Deutschland e.V.

4.)

Abschlussbericht der Machbarkeitsstudie der AG 7 „Austausch verschlüsselter E-Mail über externe Mailinglisten unter Einsatz eines E-Mail Gateways“
TeleTrusT Deutschland e.V.

11. Abkürzungsverzeichnis

AG	Arbeitsgruppe
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

12. 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.

12.1. Kategorie 1

12.1.1. Senden einer unverschlüsselten E-Mail an den Koordinator

ToDo: Senden einer *unverschlüsselten* E-Mail mit Anlage an den Koordinator. Bewertet wird der Zeitaufwand beim Versender und Empfang der E-Mail beim Koordinator.

Inhalt: Beschreibung des Testfalls. Betreff: Kapitelnummer des Testfalls.

Anlage: Die Anlage enthält das eigene Verschlüsselungszertifikat, sowie die zugehörigen CA-Zertifikate und Sperrlisten. Falls beim Senden oder Empfangen der E-Mail Fehler auftreten, sollten die Anlagen als .zip- oder .rar-Datei komprimiert werden.

Ziel: Funktion des normalen Mailtransfer testen und notwendige Vorbereitung der weiteren Tests.

12.1.2. Empfang einer verschlüsselten E-Mail mit Gruppenzertifikat und Schlüssel

ToDo: Der Koordinator versendet an alle Teilnehmer eine *verschlüsselte* E-Mail mit dem benötigten Schlüsselmaterial. Bewertet wird der Empfang der E-Mail und der Zeitaufwand beim Versender.

Inhalt: Beschreibung des Testfalls. Betreff: Kapitelnummer des Testfalls.

Anlage: Die Anlage enthält das Gruppenzertifikat, die PSE als PKCS#12-File, das PSE-Passwort, sowie die zugehörigen CA-Zertifikate und Sperrlisten; außerdem die in den Tests der Kategorie 2 und 3 zu verwendende Dateianlage. Falls beim Senden oder Empfangen der E-Mail Fehler auftreten, sollten die Anlagen als .zip- oder .rar-Datei komprimiert werden.

Ziel: Funktion des normalen Mailtransfer testen und notwendige Vorbereitung der weiteren Tests.

12.1.3. Installation des Gruppenzertifikates im eigenen E-Mail-Client

ToDo: Das Gruppen- und die CA-Zertifikate, sowie die zugehörige PSE (PKCS#12) für diesen Test sollen in den E-Mailclient importiert werden. Sie sind als Anlage in der E-Mail Testfall 12.1.2. enthalten. Bewertet wird der Aufwand für den Import der Zertifikate.

Ziel: Der Import der Zertifikate ist notwendige Voraussetzung für die folgenden Testfälle.

12.2. Kategorie 2

12.2.1. Senden einer verschlüsselten E-Mail an die Liste

ToDo: Senden einer *verschlüsselten* E-Mail mit Anlage an die Liste. Es wird der Verschlüsselungsschlüssel des Gruppenzertifikates benutzt. Als S/MIME-Format wird enveloped data zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail.

Inhalt: Beschreibung des Testfalls. Betreff: Kapitelnummer des Testfalls.

Anlage: Dateianlage aus Testfall 12.1.2.

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

12.2.2. Senden einer verschlüsselten E-Mail an die Liste

ToDo: Senden einer *verschlüsselten* E-Mail mit Anlage an die Liste. Es wird der Verschlüsselungsschlüssel des Gruppenzertifikates benutzt. Als S/MIME-Format wird enveloped data zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail.

Hinweis: Dies ist der analoge Testfall wie 12.2.1 für Teilnehmer, die kein eigenes Zertifikat besitzen und nur das Gruppenzertifikat mit zugehöriger PKCS#12-Datei installieren.

Inhalt: Beschreibung des Testfalls. Betreff: Kapitelnummer des Testfalls.

Anlage: Dateianlage aus Testfall 12.1.2.

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

12.2.3. Senden einer verschlüsselten E-Mail an die Liste mit gesperrtem Gruppenzertifikat

ToDo: Senden einer *verschlüsselten* E-Mail mit gesperrtem Verschlüsselungs-Zertifikat (Gruppen-Zertifikat). Der Empfänger muss Zugriff auf die relevante Sperrliste haben, in der das verwendete Zertifikat eingetragen ist, vorzugsweise per LDAP- oder HTTP-Protokoll aus einem X.500-Directory. Als S/MIME-Format wird enveloped data zwischen den Teilnehmern verwendet. 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 die E-Mail trotzdem versendet, muss spätestens der empfangende E-Mail-client den Mangel bemerken. Dieser Testfall wird zeitlich als letzter ausgeführt. Den Zeitpunkt der Zertifikatssperrung gibt der Koordinator über die Mailingliste bekannt.

Inhalt: Beschreibung des Testfalls. Betreff: Kapitelnummer des Testfalls.

Anlage: Dateianlage aus Testfall 12.1.2.

Ziel: Zu erkennen, ob ein Bezug sowie die Auswertung von Sperrlisten des Gruppenzertifikates möglich ist.

12.3. Kategorie 3

12.3.1. Senden einer signierten E-Mail an die Liste

ToDo: Senden einer *signierten* E-Mail mit Anlage an die Liste. Zur Signatur wird das *eigene Zertifikat* verwendet. Als S/MIME-Format wird opaqueSigned zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail.

Inhalt: Beschreibung des Testfalls. Betreff: Kapitelnummer des Testfalls.

Anlage: Dateianlage aus Testfall 12.1.2.

Ziel: Empfangen einer signierten E-Mail mit Anlage durch alle Listenmitglieder und Validierung der Signatur durch den Empfänger-Client.

Hinweis: Teilnehmer ohne eigenes Zertifikat verwenden das Gruppenzertifikat.

12.3.2. Senden einer signierten E-Mail an die Liste

ToDo: Senden einer *signierten* E-Mail mit Anlage an die Liste. Zur Signatur wird das *Gruppenzertifikat* verwendet. Als S/MIME-Format wird opaqueSigned zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail.

Inhalt: Beschreibung des Testfalls. Betreff: Kapitelnummer des Testfalls.

Anlage: Dateianlage aus Testfall 12.1.2.

Ziel: Empfangen einer signierten E-Mail mit Anlage durch alle Listenmitglieder und Validierung der Signatur durch den Empfänger-Client.

Hinweis: Als Absender-Adresse wird die eigene E-Mailadresse verwendet. Mit diesem Test soll festgestellt werden, ob der Empfänger-Client (unnötigerweise?) prüft, ob die E-Mail von der im Zertifikat angegebenen E-Mail-Adresse gesendet wurde.

12.3.3. Senden einer signierten und verschlüsselten E-Mail an die Liste

ToDo: Senden einer *signierten und verschlüsselten* E-Mail mit Anlage an die Liste. Zur Signatur wird das *eigene Zertifikat* verwendet. Als S/MIME-Format wird SignedAndEnveloped zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail.

Inhalt: Beschreibung des Testfalls. Betreff: Kapitelnummer des Testfalls.

Anlage: Dateianlage aus Testfall 12.1.2.

Ziel: Empfangen einer signierten und verschlüsselten E-Mail mit Anlage durch alle Listenmitglieder und Entschlüsselung sowie Validierung der Signatur durch den Empfänger-Client

Hinweis: Teilnehmer ohne eigenes Zertifikat verwenden das Gruppenzertifikat.

12.3.4. Senden einer signierten und verschlüsselten E-Mail an die Liste

ToDo: Senden einer *signierten und verschlüsselten* E-Mail mit Anlage an die Liste. Zur Signatur wird das *Gruppenzertifikat* verwendet. Als S/MIME-Format wird SignedAndEnveloped zwischen den Teilnehmern verwendet. Bewertet wird der Empfang der E-Mail.

Inhalt: Beschreibung des Testfalls. Betreff: Kapitelnummer des Testfalls.

Anlage: Dateianlage aus Testfall 5.1.2.

Ziel: Empfangen einer signierten und verschlüsselten E-Mail mit Anlage durch alle Listenmitglieder und Entschlüsselung sowie Validierung der Signatur durch den Empfänger-Client.

Hinweis: Als Absender-Adresse wird die eigene E-Mailadresse verwendet. Mit diesem Test soll festgestellt werden, ob der Empfänger-Client (unnötigerweise?) prüft, ob die E-Mail von der im Zertifikat angegebenen E-Mail-Adresse gesendet wurde.

13. Formularvorlagen

13.1. Event Log

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

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.**

13.2. Komponenten der E-Mail-Infrastruktur

Organisation <ul style="list-style-type: none">- Name- Adresse- Ansprechpartner	
Testdatum	
<i>Betriebssystem</i>	
<i>E-Mailplattform</i>	
<i>E-Mailclient</i>	

<i>Kommentare zum Mailinglistentest</i>	
-----------------------------------------	--

13.3. Testergebnisse des Mailinglistentests

Sender: →	Ergebnis	Kommentare
Empfänger: ↓		
Kategorie 1		
1.1.		Zeitaufwand:
1.2.		Zeitaufwand:
1.3.		Zeitaufwand:
Kategorie 2		
2.1.		
2.2.		
2.3.		
Kategorie 3		
3.1.		
3.2.		
3.3.		
3.4.		
weitere Kommentare		

Datum, Unterschrift