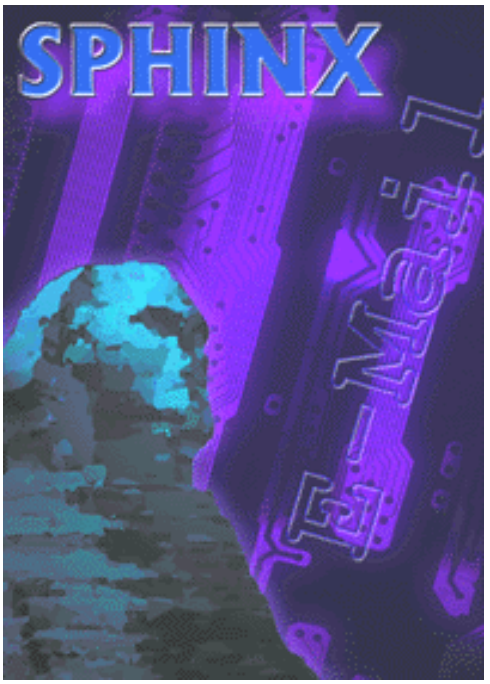
Bundesamt
für Sicherheit in der
Informationstechnik

SPHINX
Sichere E-Mail

Kurzbericht zu den Produkttests vom 10. bis 14. Mai 2004



Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

Competence Center Informatik GmbH

Theo Fischer, Thomas Beckmann
Atos Origin -
Competence Center Informatik GmbH
Lohberg 10
D-49716 Meppen

Michael Thiel
Bundesamt für Sicherheit in der Informations-
technik
Godesberger Allee 185-189
D-53175 Bonn

Inhaltsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Anh	Anhang
ASN.1	Abstract Syntax Notation 1
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority (Zertifizierungsinstanz)
CCI	Competence Center Informatik GmbH
CRL	Certificate Revocation List (Sperrliste)
DN	Distinguished Name
ISDN	Integrated Service Digital Network
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extension
MTT	MailTrust
PKI	Public Key Infrastructure
PSE	Personal Security Environment
RSA	(Rivest-Shamir-Adleman)-Verfahren
SHA	Secure Hash Algorithm
S/MIME	Secure MIME

1 Einleitung

Interoperabilität kann definiert werden als die Fähigkeit mehrerer Produkte (unterschiedlicher Hersteller) mit Partnern verlässlich zu kommunizieren, ohne dass proprietäre Schnittstellen die Daten konvertieren. Der Erzeuger einer signierten oder verschlüsselten E-Mail braucht daher die Komponenten der Kommunikationspartner nicht zu kennen, um für sie verständliche Datenformate zu erzeugen. Die Schnittstellen (Protokolle und Formate) werden von Internet-Standards (RFCs, Request for Comments) definiert, die den Programmierern zur Verfügung stehen. Die Bundesregierung formuliert diesen Zusammenhang in ihrem Beschluss vom 16.01.2002 als horizontale Interoperabilität.

Trotz umfangreicher Normenwerke treten Interoperabilitätsprobleme bei den Kommunikationspartnern auf. Nachrichten können nicht dargestellt werden und Verifikationsprozesse schlagen fehl.

Während des Pilotprojekts "SPHINX - Sichere E-Mail" wurden daher zur Qualitätssicherung Tests auf Interoperabilität durchgeführt. Durch diese Tests konnte sichergestellt werden, dass die in einem europaweit geführten Feldversuch eingesetzten PKI-Produkte und Trustcenter zueinander interoperabel waren. Nach Beendigung des Pilotprojekts im Dezember 2000 setzte das Bundesamt für Sicherheit in der Informationstechnik in Abstimmung mit den Herstellern und Trustcenterbetreibern auf die selbstregelnden Kräfte des Marktes.

Durch den Aufbau einer PKI für die öffentliche Verwaltung und der damit beginnenden großflächigen Ausstattung der Bundes- und Länderverwaltungen mit PKI-Produkten zur Absicherung der E-Mail-Kommunikation waren weitere Funktionalitäten zu implementieren und damit verbundene Interoperabilitätsprobleme zu lösen. Um sicherzustellen, dass nur interoperable Produkte zum Einsatz kommen, wurden die Interoperabilitätstests ab Dezember 2001 fortgeführt.

Mit den Interoperabilitätstests wird durch das Bundesministerium des Innern empfohlen, nur erfolgreich geprüfte Produkte für den Einsatz in der Bundesverwaltung zu beschaffen.

Die Tests werden je einmal pro Quartal vom Testlabor der Firma Atos Origin - Competence Center Informatik (CCI) GmbH in Meppen im Auftrag des Bundesamts für Sicherheit in der Informationstechnik durchgeführt. Die Basis des Tests bildet die “Testspezifikation Client-Produkte: Interoperabilität und Funktionalität”.

Der vorliegende Testbericht beschreibt den durchgeführten Quartalstest, der in der 20. Kalenderwoche 2004 (10. bis 14. Mai) durchgeführt wurde.

Insgesamt haben zehn Produkte am Test teilgenommen. Die Versionen von acht Produkten wurden bereits im vorigen Test geprüft. Die anderen Produkte haben neu am Test teilgenommen oder es wurden aktuellere Versionen getestet.

2 Allgemeine Angaben zum Testlabor

Im Folgenden werden Angaben zum Testlabor und den Evaluatoren aufgeführt.

Testlabor:

Atos Origin GmbH
Lohberg 10
49716 Meppen
Telefon: 05931/805-0
Telefax: 05931/805-100
WWW: http://www.atosorigin.com

Evaluatoren:

Thomas Beckmann
Telefon: 05931/805-242
E-Mail: Thomas.Beckmann@atosorigin.com

Theo Fischer
Telefon: 05931/805-219
E-Mail: Theo.Fischer@atosorigin.com

3 Hersteller und ihre Produkte im Test

In **Fehler! Verweisquelle konnte nicht gefunden werden.** sind die Produkte aufgeführt, die von Herstellern bei der Atos Origin CCI GmbH zu dem Quartalstest eingereicht beziehungsweise vom Bundesamt für Sicherheit in der Informationstechnik ins Testfeld integriert wurden.

Tabelle 1: Produkte im Test vom 10. bis 14. Mai 2004

Hersteller und Ansprechpartner	Produktname	Version	Mail-Client
SECUDE Sicherheitstechnologie Informationssysteme GmbH Dolivostraße 11 64293 Darmstadt Ansprechpartner: Frau Petra Barzin	AuthenteMail	3.0	MS Outlook 98
	AuthenteMail	2.7	Lotus Notes 5.0.10
Secartis AG Bretonischer Ring 3 85630 Grasbrunn Ansprechpartner: Herr Wolfgang Christ	GDtrust Mail	4.1.2 enterprise	MS Outlook 98
cv cryptovision GmbH Munscheidstr. 14 45886 Gelsenkirchen Ansprechpartner: Herr Carsten Pratsch	cv act s/mail	2.1.2	Groupwise 5.5
	cv act s/mail	2.1.2	MS Outlook 98
	cv act s/mail	2.1.2	Lotus Notes 5.0.10
Intevation GmbH Georgstraße 4 49074 Osnabrück Ansprechpartner: Herr Jan-Oliver Wagner	Ägypten	2.0	KMail/Linux (BSI ERPOSS 3 3.6.3 β7)
Glück & Kanja Technology AG Christian-Pless-Str. 11-13 63069 Offenbach am Main Ansprechpartner: Herr Victor Arens	CryptoEx	2.1	MS Outlook 98
GUARDEONIC SOLUTIONS AG Rosenheimer Str. 116 81669 München Ansprechpartner: Herr Ludwig Wiechers	TrustedMIME	3.3.1	Lotus Notes 5.0.10
			MS Outlook 98

Anmerkungen zu den getesteten Produkten:

Die Produkte sind sogenannte PlugIns, die während der Tests mit den angegebenen Mail-Clients unter dem Betriebssystem Microsoft WINDOWS NT 4.0 (mit Ausnahme von Ägypten) eingesetzt wurden.

Das Produkt Ägypten von Intevation ist ein PlugIn für den Linux-Mailclient Kmail.

Das Produkt cv act s/mail für Groupwise wurden in englischer Sprache eingereicht.

4 Ergebnisse

Die Protokolle und Anmerkungen zu den einzelnen Testfällen sind umfangreich. Alle Aussagen werden zu einem Ergebnis zusammengefasst und in Tabellen über verschiedene Symbole abgebildet:

Tabelle 2: Verwendete Symbole zur Ergebnisdokumentation und ihre Bedeutung

Symbol	Bedeutung
✓	gibt an, dass zwischen den Produkten der zugehörigen Tabellenzeile und -spalte Interoperabilität nachgewiesen werden konnte.
(✓)	wird verwendet, wenn das Testergebnis dem erwarteten Ergebnis weitestgehend entspricht, so dass zwar ein positives Ergebnis, jedoch aufgrund besonderer Vorkommnisse mit Einschränkungen, ermittelt wurde.
X	wird verwendet, wenn bei den Tests Probleme aufgetreten sind und daher Interoperabilität nicht gegeben ist.
?	wird verwendet, wenn ein unklares Prüfergebnis vorliegt oder aufgrund besonderer Umstände der Testfall nicht durchgeführt und daher kein Ergebnis ermittelt werden konnte.
•	gibt an, dass die entsprechende Funktion beim Produkt nicht vorhanden ist.

Beispiel:

Sollten zwischen zwei Produkten Probleme nur bei Nachrichten des Formats “Multipart-Signed” aufgetreten sein, wird dies nicht als nicht interoperabel gewertet. Da dieses Format nicht in der zugrunde gelegten Technischen Spezifikation SPHINX als Standard definiert wurde, lautet die Beurteilung "eingeschränkte Interoperabilität" und es wird das Zeichen “(✓)” (positives Prüfergebnis mit Einschränkung) verwendet.

4.1 Ergebnis der Interoperabilitätstests

In **Fehler! Verweisquelle konnte nicht gefunden werden.** sind die Ergebnisse der Tests zur Ermittlung der Interoperabilität dargestellt. Hierbei ist die Interoperabilität von Produkt zu Produkt abgebildet.

Tabelle 3: Ergebnisse Interoperabilitätstests

Sender / **Empfänger**	AuthenteMail für Outlook	AuthenteMail für Lotus Notes	GDtrust Mail	cv act s/mail für Groupwise	cv act s/mail für Outlook	cv act s/mail für Lotus Notes	Ägypten	TrustedMIME für Outlook	TrustedMIME für Lotus Notes	CryptoEx
AuthenteMail für Outlook		✓	✓	✓	✓	✓	✓	✓	✓	✓
AuthenteMail für Lotus Notes	✓		✓	✓	✓	✓	✓	✓	✓	✓
GDtrust Mail	✓	✓		✓	✓	✓	✓	✓	✓	✓
cv act s/mail für Groupwise	✓	✓	✓		✓	✓	✓	✓	✓	✓
cv act s/mail für Outlook	✓	✓	✓	✓		✓	✓	✓	✓	✓
cv act s/mail für Lotus Notes	✓	✓	✓	✓	(✓)		✓	✓	✓	✓
Ägypten	✓	✓	✓	✓	✓	✓		✓	✓	✓
TrustedMIME für Outlook	✓	✓	✓	✓	✓	✓	✓		✓	✓
TrustedMIME für Lotus Notes	✓	✓	✓	✓	✓	✓	✓	✓		✓

CryptoEx	✓	✓	✓	✓	✓	✓	✓	✓	✓		

AuthenteMail für Lotus Notes behandelt neue Mails beim erstmaligen Öffnen korrekt. Wurden die Mails ein weiteres Mal ausgewählt und geöffnet, wurden sie nicht mehr von AuthenteMail, sondern von Lotus Notes behandelt und daher nicht mehr korrekt entschlüsselt und/oder verifiziert.

4.2 Ergebnis der Funktionalitätstests

Neben der Interoperabilität wurden für die Einsatzempfehlung noch weitere Kriterien herangezogen. Diese werden in der **Fehler! Verweisquelle konnte nicht gefunden werden.** aufgeführt und gleichzeitig die jeweiligen Ergebnisse der Produkte eingetragen.

Tabelle 4: Herangezogene Testfälle für die Einsatzempfehlung

Testfall	Beschreibung	AuthenteMail für Outlook	AuthenteMail für Lotus Notes	GDtrust Mail	cv act s/mail für Groupwise	cv act s/mail für Outlook	cv act s/mail für Lotus Notes	Ägypten	TrustedMIME für Outlook	TrustedMIME für Lotus Notes	CryptoEx
5	PKI-Management-Nachrichten im Request-Format PKCS#10	✓	✓	✓	(✓)	(✓)	(✓)	✓	✓	✓	✓
10 a	Korrekte Anzeige des Zertifikats im Format X.509v3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
10 b	Korrekte Prüfung der Erweiterungen (Extensions in X.509v3-Zertifikaten)	✓	X	X	✓	✓	✓	✓	✓	✓	X
22 b	Verzeichnisabfrage via LDAP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
27 a	Gültigkeitsmodell (Schalenmodell)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
28	Prüfung des Zertifizierungspfades	✓	✓	✓	(✓)	(✓)	(✓)	✓	✓	✓	?
30	Abgelaufene Zertifikate	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
31	Interpretation von Sperrlisten	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
35	Prüfung der Aktualität und Eignung von Sperrlisten	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

5 Einsatzempfehlung des Testlabors

Die Einsatzempfehlungen des Testlabors für die einzelnen Produkte werden aus den Ergebnissen von Interoperabilitätstests und Funktionalitätstests abgeleitet.

Entsprechend den Ergebnissen der Produkttests vom 10. bis 14. Mai wurden zwei Kategorien für die Einsatzempfehlung vergeben:

- empfehlenswert
  Das Produkt hat die Tests auf Interoperabilität und Funktionalität, die als Minimalanforderungen für eine Empfehlung festgelegt wurden (siehe **Fehler! Verweisquelle konnte nicht gefunden werden.**), erfolgreich bestanden. Es wird daher für den Einsatz empfohlen.
- bedingt empfehlenswert
  Das Produkt hat die Tests auf Interoperabilität und Funktionalität, die als Minimalanforderungen für eine Empfehlung festgelegt wurden (siehe **Fehler! Verweisquelle konnte nicht gefunden werden.**), bedingt bestanden. Es traten einzelne Probleme bei dem Produkt selbst oder im Zusammenwirken mit anderen Produkten auf. Daher wird das Produkt nur bedingt für einen Einsatz empfohlen.

5.1 Empfohlene Produkte

Die in **Fehler! Verweisquelle konnte nicht gefunden werden.** genannten Produkte haben die Minimalanforderungen der Tests auf Inter-operabilität und Funktionalität erfolgreich bestanden. Sie werden daher vom Testlabor für den Einsatz empfohlen.

Tabelle 5: Empfohlene Produkte

Hersteller	Produktname	Version	Mail-Client
Secude	AuthenteMail	3.0	MS Outlook 98
Secartis	GDTrust Mail	4.1.2 enterprise	MS Outlook 98
cv cryptovision	cv act s/mail	2.1.2	MS Outlook 98
cv cryptovision	cv act s/mail	2.1.2	Groupwise 5.5
cv cryptovision	cv act s/mail	2.1.2	Lotus Notes 5.0.10
Glück & Kanja	CryptoEx	2.1	MS Outlook 98
guaerdeonic	TrustedMIME	3.3.1	MS Outlook 98
guaerdeonic	TrustedMIME	3.3.1	Lotus Notes 5.0.10
Intevation	Ägypten	2.0	Kmail für Linux

Die Produkte AuthenteMail für Lotus Notes und CryptoEx zeigen nicht alle Zertifikatsextensions an. Die Hersteller sollten ihre Produkte verbessern, so dass alle Zertifikatserweiterungen korrekt angezeigt werden.

Bei dem Produkt CryptoEx konnte zu dem Testfall 28 (Prüfung des Zertifizierungspfades) kein Ergebnis ermittelt werden. Der Hersteller sollte den bei der Prüfung der Nachricht entstehenden Effekt “Keine Rückmeldung” von Outlook beheben.

5.2 Bedingt empfohlene Produkte

Das in **Fehler! Verweisquelle konnte nicht gefunden werden.** aufgeführte Produkt hat die Minimalanforderungen der Tests auf Interoperabilität und Funktionalität bestanden. Es traten einzelne Probleme bei dem Produkt selbst oder im Zusammenwirken mit anderen Produkten auf. Daher wird dieses Produkt für einen Einsatz bedingt empfohlen.

Tabelle 6: Bedingt empfohlene Produkte

Hersteller	Produktname	Version	Mail-Client
Secude	AuthenteMail	2.7	Lotus Notes 5.0.10

Grundsätzlich konnten mit Authentemail 2.7 für Lotus Notes alle eingehenden Mails bearbeitet, d. h. entschlüsselt und/oder verifiziert werden. Auch die Prüfung der Funktionalitäten lieferte die gewünschten Ergebnisse (siehe oben). Aufgrund der in Abschnitt **Fehler! Verweisquelle konnte nicht gefunden werden.** beschriebenen Problematik konnte in dieser Testreihe nur eine Bewertung als bedingt empfohlen erfolgen. Dies, obwohl das Produkt sich zu den vorhergehenden Test nicht verändert hat.

Es wird durch den Hersteller geprüft, unter welchen Umständen diese Phänomen auftreten kann.

5.3 Erläuterungen zu den gegebenen Empfehlungen

Ein wesentlicher Schwerpunkt für die Empfehlung stellt die Interoperabilität dar. Untereinander interoperabel sind alle getesteten Produkte, die nachstehend aufgeführt sind:

Tabelle 7: Interoberable Produkte

Hersteller	Produktname	Version	Mail-Client
Secude	AuthenteMail	3.0	MS Outlook 98
Secude	AuthenteMail	2.7	Lotus Notes 5.0.10
Secartis	GDTrust Mail	4.1.2 enterprise	MS Outlook 98
cv cryptovision	cv act s/mail	2.1.2	Groupwise 5.5
cv cryptovision	cv act s/mail	2.1.2	MS Outlook 98
cv cryptovision	cv act s/mail	2.1.2	Lotus Notes 5.0.10
Glück & Kanja	CryptoEx	2.1	MS Outlook 98
Intevation	Ägypten	2.0	Kmail für Linux
TrustedMIME	guaerdeonic	3.3.1	MS Outlook 98
TrustedMIME	guaerdeonic	3.3.1	Lotus Notes 5.0.10

6 Zusammenfassung

In diesen Tests konnte hinsichtlich der vereinbarten Standardformate für gesicherte Nachrichten Interoperabilität zwischen allen Produkten nachgewiesen werden. Lediglich bei den Multipart-Formaten gab es zwischen den Produkten cv act s/mail für GroupWise und Outlook einseitig Verständigungsschwierigkeiten.

Die Interoperabilität zwischen den Produkten AuthenteMail für Outlook, AuthenteMail für Lotus Notes und CryptoEx sowie GDTrust Mail wurde erwartet, da die hier getesteten Produktversionen bereits in vorigen Tests interoperabel bewertet werden konnten.

Alle Produkte erfüllen die festgelegten Anforderungen an die Funktionalität. Folgende Produkte werden daher für den Einsatz empfohlen:

- AuthenteMail Version 3.0 für MS Outlook 98,
- GDTrust Mail Version 4.1.2 enterprise für MS Outlook 98,
- cv act s/mail Version 2.1.2 für MS Outlook 98
- cv act s/mail Version 2.1.2 für Groupwise 5.5,
- cv act s/mail Version 2.1.2 für Lotus Notes 5.0.10,
- CryptoEx Version 2.1 für MS Outlook 98,
- Ägypten Version 2.0,
- TrustedMIME Version 3.3.1 für MS Outlook 98 und
- TrustedMIME Version 3.3.1 für Lotus Notes 5.0.10.

Das Produkt AuthenteMail Version 2.7 für Lotus Notes 5.0.10 erfüllte zwar alle Interoperabilitäts- und Funktionalitätsanforderungen. Aufgrund der in Abschnitt **Fehler! Verweisquelle konnte nicht gefunden werden.** beschriebenen Probleme beim neuerlichen Öffnen von Mails konnte in dieser Testreihe nur eine bedingte Empfehlung ausgesprochen werden.

Alles in allem ist die positive Tendenz sehr erfreulich. Insbesondere bei der Interoperabilität gab es kein Produkt, das negativ herausfiel.