Sichere E-Mail-Kommunikation mit Lotus Notes

Norbert Pohlmann, Vorstandsvorsitzender TeleTrusT e.V.

Abstract

Der zunehmende Austausch vertraulicher und wertvoller Informationen per E-Mail auch im Geschäftsverkehr lenkt den Blick auf die Risiken, denen im Klartext übermittelte Informationen im Internet ausgesetzt sind. Ein Security Plugin bietet die technische Möglichkeit, die Grundwerte der E-Mail-Kommunikation zuverlässig zu schützen. Über die in einem Mail-System wie Lotus Notes bereits integrierten Sicherheitsfunktionen hinaus bietet ein dem S/MIME-Standard und anderen Normen entsprechendes Security Plugin wie Sing&Crypt für Lotus Notes von Utimaco Safeware die Besonderheit, nicht nur ein dem Schutzbedarf wertvoller Geschäftsinformationen entsprechendes höheres Maß an Sicherheit zu gewährleisten, sondern auch mit anderen Mail-Systemen interoperabel zu sein. Dabei entspricht das Security Plugin der Europäischen Direktive zur Digitalen Signatur und gewährleistet ein stabiles Sicherheitsniveau, da die Schlüssellänge wählbar ist und die Security Policy nicht heruntergehandelt werden kann.

1. E-Mail: Chancen und Risiken

Der Austausch von E-Mails ist die am häufigsten genutzte Anwendung im Internet. Dabei werden mit Hilfe von E-Mails und ihren Attachments Informationen übermittelt, die hohe Werte darstellen können, zum Beispiel Vertragsentwürfe und Geschäftsabschlüsse. Bei Fusionsverhandlungen kann es unter Umständen um Milliardensummen gehen.

1. Missbrauch von Informationen

Die per E-Mail übertragenen Informationen laufen in der Regel im Klartext über das Internet. Welchen Weg eine E-Mail dabei nimmt, kann der Absender nicht beeinflussen. Die Abbildung zeigt beispielhaft den Weg, den eine E-Mail vom

Unternehmensstandort Aachen zur Rheinisch Westfälischen Technischen Hochschule in Aachen genommen hat:

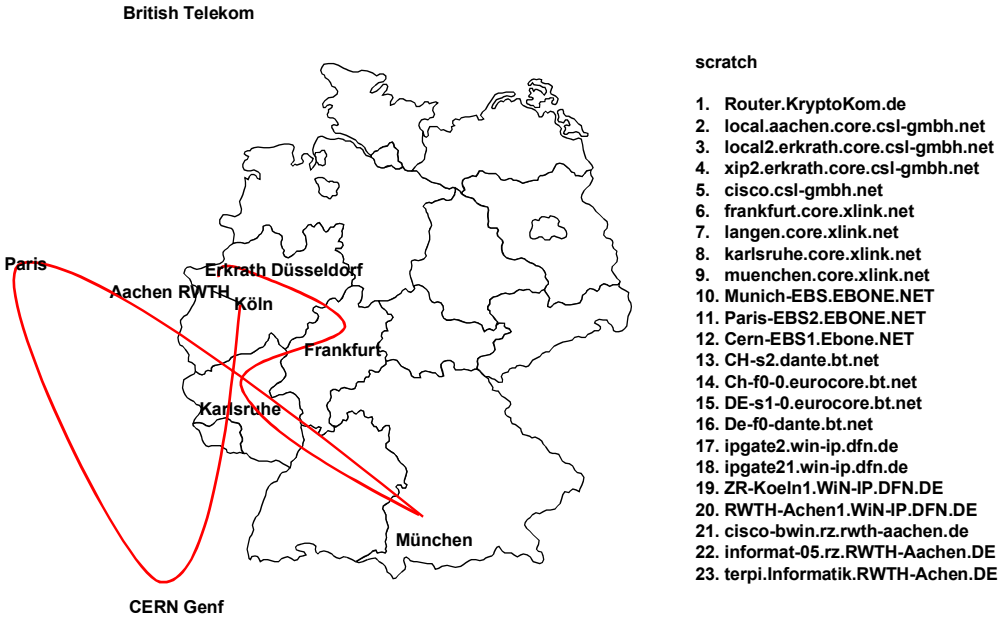

Abbildung 1: Weg einer E-Mail von Aachen nach Aachen

Das Risiko hierbei ist, dass die E-Mail an jedem Knotenpunkt abgefangen und die darin enthaltene Information zum Schaden von Absender und/oder Empfänger verwendet werden kann. Die Gefahren bei der E-Mail-Kommunikation sind:

- Mitlesen der Information im Klartext
- Einschleusen nicht-authentischer Information
- Verändern von Informationen
- Unterbinden des Nachrichtenflusses
- Wahrnehmen des Nachrichtenflusses

2. Fälschen von Absendern

Der Weg einer E-Mail vom Sender zum Empfänger hat von Beginn des Internet an bis heute eine entscheidende Schwachstelle: Das seit 1982 nahezu unverändert eingesetzte Simple Mail Transfer Protokol (SMTP) legt keinen

Authentifizierungsmechanismus fest. Dadurch ist die Identität des Absenders nicht garantiert, Fälschern und Spammern sind Tür und Tor geöffnet.

Um die SMTP-Server halbwegs sicher zu machen, nutzen die Betreiber die Passwortabfrage für E-Mail-Postfächer gemäß dem Post Office Protocol V3 (POP3) als Behelfslösung. Erst wenn sich der Nutzer mit seinem Namen und Passwort beim Postfach angemeldet hat, um die E-Mails abzuholen, wird ihm (und nur ihm) am SMTP-Server des Dienstes für eine bestimmte Zeit (meist 30 Minuten) ein kleines Türchen geöffnet, über das er seine frisch geschriebenen E-Mails loswerden kann. So soll die anonyme Nutzung des Dienstes durch nicht registrierte Personen verhindert werden.

Dieses "SMTP-after-POP" genannte Verfahren ist jedoch fehleranfällig und nicht mit allen E-Mail-Programmen kompatibel. Diverse "Workarounds" im Web bezeugen, dass sehr viele Nutzer vor diesem Problem stehen. GMX etwa stellt aus diesem Grund eigens ein kleines Tool zur Verfügung, das nur die Aufgabe hat, den SMTP-Service temporär freizuschalten.

Kennen Sie Bad Eibling?

Bad Aibling ist das älteste Moorbad Bayerns, 50 Kilometer südöstlich von München im Mangfalltal gelegen, ein hübscher Kurort mit 16.000 Einwohnern. Er bietet einen schönen Ausblick auf die Tölzer Berge und über das Inntal. (www.kur-online.de)

Abbildung 2: Bad Eibling im Mangfalltal

Bad Aibling ist der Standort eines US-Luftwaffengeländes mit Abhörstation. Unter der Leitung der National Security Agency wird hier jede Art von Kommunikation abgehört und decodiert, die für die Sicherheit der USA von Interesse sein kann. Das Budget des NSA ist sechs Mal so groß wie das der CIA. Die NSA ist der weltweit größte Arbeitgeber für Mathematiker. (www.aib.de)

Abbildung 3: Abhörstation des NSA

2. Grundwerte der E-Mail-Sicherheit

Wie bei jeder anderen Kommunikation müssen auch die Grundwerte von per E-Mail übertragenen Informationen geschützt werden. Grundwerte der Kommunikation sind Vertraulichkeit, Integrität, Authentizität, Verbindlichkeit und Verfügbarkeit. Wir verfügen heute über die Technologien, die jeden dieser Grundwerte schützen:

- Vertraulichkeit: Die Vertraulichkeit der Information kann durch Verschlüsselung und Zugriffs- bzw. Rechtekontrolle geschützt werden.
- Integrität: Digitale Signatur und Hashwert (Prüfsumme) sichern die Integrität der Information.
- Authentizität: Verschlüsselung, User Login und Zertifikate garantieren die Authentizität des Absenders.
- Verbindlichkeit: Die Digitale Signatur und Zertifikate sowie Zeitstempel machen die Information verbindlich.
- Verfügbarkeit: Die Verfügbarkeit wird durch Hardware Mirroring und Daten-Backup gewährleistet.

3. Interoperable Sicherheitslösung: MailTrusT (S/MIME-Standard)

In einem Sicherheitssystem, das organisationsübergreifend genutzt werden soll, ist die Infrastruktur von besonderer Bedeutung. Die folgende Grafik zeigt, dass bei der Realisierung viele unterschiedliche Schnittstellen zu berücksichtigen sind. Die gemeinsame Sicherheitsinfrastruktur geht bei virtuellen Welten wie dem Internet über alle geographischen und politischen Grenzen, Gesetze und Kulturen hinaus und stellt somit eine neue und ungewohnte Herausforderung dar.

Um eine Anwendung vertrauenswürdig realisieren zu können, muss eine Sicherheitstechnologie – ein Sicherheitsprodukt – integriert werden, die die notwendigen Sicherheitsfunktionen wie zum Beispiel Vertraulichkeit durch Verschlüsselung und Digitale Signatur zur Verfügung stellt. Typischerweise benötigt der Benutzer hierzu ein Security Token, das eine Chipkarte oder eine spezielle Diskette sein kann. Wenn es sich um eine Chipkarte handelt, muss an die Anwendung ein Chipkartenleser angeschlossen werden.

Eine Grundvoraussetzung für eine organisationsübergreifende Sicherheit ist eine gemeinsame Infrastruktur, die dafür sorgt, dass alle Personen einen eindeutigen Namen haben. Alle an dem Sicherheitssystem beteiligten Personen brauchen einen elektronischen Ausweis – in der Terminologie: Zertifikat, in dem der öffentliche Schlüssel eines Public-Key-Verfahrens beglaubigt wird. Außerdem muss die Applikation auf Verzeichnisdienste zugreifen können, die ständig darüber informieren, ob bestimmte Benutzer, mit denen eine Kommunikation durchgeführt werden soll, noch gültige Zertifikate haben oder ob sie in eine Sperrliste aufgenommen worden sind. All diese Schnittstellen müssen in einem Systemkonzept spezifiziert werden. Genau hier liegt der Ansatz von MailTrusT.

MailTrusT ist ein Systemkonzept für den vertrauenswürdigen Austausch von E-Mails und anderen elektronischen Objekten sowie der notwendigen Sicherheitsinfrastruktur in offenen Systemen. Die Leistung von MailTrusT ist es, eine Teilmenge der Möglichkeiten der einzelnen Industriestandards definiert und in Kombination unterschiedlicher Standards (zum Beispiel S/MIME) ein sinnvolles und praktisch einsetzbares Ganzes geschaffen zu haben.

Zielvorgaben des MailTrusT-Systemkonzepts

Das MailTrusT-Systemkonzept besteht aus einer Reihe von Teilspezifikationen und umfasst folgende für eine erfolgreiche Anwendung notwendigen Zielvorgaben:

Interoperabilität

Das MailTrusT-Sytemkonzept gewährleistet, dass die Produkte der unterschiedlichen Hersteller ohne Modifikationen oder weitere Abstimmungen direkt interoperabel sind.

Minimalität

Das MailTrusT-Systemkonzept ist minimal, um Produktherstellern eine maximale Gestaltungsfreiheit zu erhalten. Es ist im wesentlichen auf die für die Interoperabilität verschiedener Komponenten erforderlichen Festlegungen für einen in der Regel ausreichenden Funktionsumfang beschränkt (soviel wie nötig, so wenig wie möglich). Herstellern bleibt somit noch Spielraum, um auf Marktanforderungen einzugehen.

Kontinuität

Sowohl für die Hersteller als auch für die Kunden MailTrusT-konformer Komponenten wird durch Kontinuität Investitionssicherheit in größtmöglichem Umfang gewährleistet. Dieser Ansatz wird auch in Zukunft weiter verfolgt werden.

Universalität

Das MailTrusT-Systemkonzept setzt kein bestimmtes Modell einer Public-Key-Infrastruktur voraus. Es unterstützt zentrale, dezentrale und kombinierte Modelle. Das MailTrusT-Systemkonzept ist auch nicht auf bestimmte Anwendungen beschränkt. Es ist vielmehr für eine breite Palette von Anwendungen entworfen.

Modularität

Das MailTrusT-Systemkonzept besteht aus mehreren aufeinander abgestimmten Modulen, die Teile eines umfassenden Systemkonzepts sind. Um ein MailTrust-konformes Produkt anbieten zu können, muss ein Hersteller nicht alle Module realisieren. Da die Module aufeinander abgestimmt sind, können Module verschiedener Hersteller miteinander kombiniert werden. Die Token-Schnittstelle ermöglicht zum Beispiel, dass Komponenten eines Herstellers mit den Chipkarten eines anderen Herstellers kooperieren.

Standardkonformität

Das MailTrusT-Systemkonzept basiert soweit wie möglich auf etablierten und verbreiteten Standards. Neben S/MIME, X.509 und PKCS#11 („Cryptoki“) werden insbesondere auch die Spezifikation der PKIX-Arbeitsgruppen der IETF und die Signatur-Interoperabilitätspezifikation zum Signaturgesetz berücksichtigt. Auf der Basis dieser Standards werden Profile definiert, die die Standards interoperabel machen und den Zielen von MailTrusT gerecht werden.

Unabhängigkeit

Das MailTrusT-Systemkonzept wurde auf der Grundlage von Praxiserfahrungen von verschiedenen Anwendern, Providern, Forschungseinrichtungen, Verbraucherverbänden und Herstellern erstellt. Proprietäre Lösungen einzelner Produkthersteller waren dabei ausdrücklich kein Maßstab für das MailTrusT-Systemkonzept.

Aufbau und Komponenten des MailTrusT-Systemkonzepts

Die vorliegende Spezifikation des Systemkonzeptes setzt kein festes Modell einer Zertifizierungsinfrastruktur voraus. Der Aufbau einer Zertifizierungsinfrastruktur kann deshalb wesentlich flexibler den jeweiligen Anforderungen angepaßt werden.

Jede MailTrusT-Public-Key-Infrastruktur (PKI) besteht aus folgenden Grundkomponenten:

- Teilnehmer-Komponenten (TN),

- Zertifizierungsstellen (CA),
- Registrierungsstellen (RA),
- Verzeichnisdiensten (DIR).

Jede dieser Komponenten hat innerhalb der Public-Key-Infrastruktur eine bestimmte Funktion und deshalb bestimmte Aufgaben zu erfüllen. Die Aufgabenzuweisung soll möglichst flexibel an die Anforderungen der jeweiligen Public-Key-Infrastruktur angepasst werden können. Deshalb erfolgt keine feste Zuweisung von Aufgaben zu Komponenten. Es werden lediglich Empfehlungen gegeben.

Zwischen den Komponenten gibt es eine Vielzahl spezifizierter online-Schnittstellen für die wesentlichen Interaktionen. Schnittstellen sind auch für die Kommunikation zwischen verschiedenen Teilen einer Grundkomponente definiert.

Die folgende Abbildung stellt exemplarisch den prinzipiellen Aufbau einer MailTrust-Public-Key-Infrastruktur mit ihren Komponenten und den Schnittstellen dar:

Systemspezifische Vorteile des MailTrusT-Standards

Für den MailTrusT-Standard sprechen zahlreiche Vorteile:

- Der Standard ist herstellerübergreifend (derzeit acht europäische Hersteller) und kann jederzeit von weiteren Herstellern weiterentwickelt werden, die eigene MTT-kompatible Produkte entwickeln.
- Kompatibilität und Interoperabilität der MTT-Produkte haben sich in verschiedenen Projekten im Gesundheitswesen und bei Bundes- und Landesbehörden (Projekt SPHINX) in Deutschland bewährt.
- Der Einsatz europäischer Technologie garantiert höchsten Sicherheitsstandard.
- Kryptographie ist in Deutschland und Europa keinen gesetzlichen Restriktionen - etwa bezüglich der Schlüssellänge – unterworfen.
- Der Aufbau auf S/MIME öffnet den MailTrusT-Standard hin zum US-amerikanischen Markt.
- Die Anlehnung an das deutsche Signaturgesetz stellt die gesetzliche Grundlage für den Einsatz der Digitalen Signatur sicher.
- Signaturgesetz-konforme Trustcenter unterstützen den Standard.

- Der Standard ist flexibel an unterschiedliche Public-Key-Infrastruktur-Modelle angebunden.
- Der MailTrusT-Standard wird regelmäßig gepflegt und weiterentwickelt: In den entsprechenden TeleTrusT-Arbeitsgemeinschaften (AG8 & SPHINX) wird offen über die Fortschreibung des MTT-Standards zwischen Herstellern, Benutzern und Mentoren, Verbraucherverbänden und Forschungseinrichtungen etc. diskutiert und die neu auftretenden Kunden- und Marktanforderungen werden in den Standard implementiert.
- Da nicht nur ein Hersteller den Standard weiter entwickelt, ist Investitionssicherheit für die Käufer garantiert.
- Durch das modulare Konzept werden verschiedene kundenspezifische Realisierungen ermöglicht.

MailTrusT-Produkte sind für viele Plattformen und Applikationen verfügbar und bieten somit plattformübergreifende und applikationsunabhängige Kommunikationssicherheit.

4. Konzeptionelle E-Mail-Sicherheit

E-Mail-Sicherheit kann nur funktionieren, wenn sie in ein Sicherheitskonzept eingebunden ist. Die Elemente des Konzeptes sind die Sicherheitspolitik des Unternehmens, eine Publik-Key-Infrastruktur, ein zuverlässiges Produkt und – last but not least – die Awareness der Anwender (Sicherheitsbewußtsein).

Sicherheitspolitik

Die Sicherheitspolitik des Unternehmens ist die Basis jeder sicheren E-Mail-Kommunikation: Das individuelle Konzept zur Realisierung von Informationsssicherheit basiert auf der Bedarfsanalyse der Kommunikationsstrukturen des Unternehmens und der Sicherheitsanforderungen und schafft somit die Grundlagen zur Implementierung und zum Betrieb von Lösungen wie Secure E-Mail.

Die Security Policy definiert, welche Partner für die E-Mail-Kommunikation einbezogen werden müssen und enthält die Bedarfsanalyse für die Sicherheit der E-Mail-Kommunikation. Dabei wird die Einwirkungsmöglichkeiten bei den Partnern berücksichtigt.

Analyse des Schutzbedarfs

Die Analyse des Schutzbedarfs beinhaltet eine Aufstellung von Sicherheitsklassen an Hand des Wertes möglicher Schäden bezüglich der Vertraulichkeit, der Integrität und der Authentizität der Kommunikation.

Beispiel für Sicherheitsklassen bzgl. Vertraulichkeit

Sicherheitsklasse	trifft zu bei	Beispiele
"geringes" Schadenpotential	• zu Dienstzwecken jedem zugänglich • kontrollierte Verbreitung im Unternehmensinteresse • kurzfristig wiederzubeschaffen bei Verlust	• interne Verzeichnisse und Regelungen • Statistiken ohne strategische und datenschutzrechtliche Relevanz • Firmendaten/-ergebnisse für die Öffentlichkeit
"mittleres" Schadenpotential	• Schaden auf Verantwortungsbereich der Organisationseinheit begrenzt (nicht unternehmensweit) • Regelfall für Kunden- und Mitarbeiterdaten	• abteilungsbezogene Sachbearbeitungsdaten (Personaldaten, Kundendaten, Teilforschungsergebnisse, ...) • Host-Daten auf PCs (File-Transfer)
"hohes" Schadenpotential	• bereichsübergreifendes Potential • Unternehmensweite Auswirkungen (Image, Geschäftsverbindungen, ...)	• strategische Informationen, Finanzdaten • vertrauliche Personal- oder Kundendaten • Verträge

Abbildung 4: Sicherheitsklassen bzgl. Vertraulichkeit

Die Vorschriften und Arbeitsanweisungen für den Umgang mit vertraulichen Dokumenten müssen für die E-Mail-Kommunikation angepasst und erweitert werden. An Hand der Sicherheitsklassen werden Richtlinien für den Versand von Informationen erstellt, zum Beispiel:

Sicherheitsklasse (Schadenpotential)	Versand per E-Mail
gering	erlaubt, unverschlüsselt
mittel	erlaubt, aber verschlüsselt
hoch	erlaubt, aber verschlüsselt alternativ: kein Versand per E-Mail

Die Sicherheitspolitik beinhaltet ein Konzept für Information Recovery (Message Recovery, Key Recovery) und einen Notfallplan. Damit die Sicherheitspolitik greifen kann, bedarf es bestimmter Schulungsmaßnahmen für die Anwender und Arbeitsanweisungen bzw. Richtlinien für den Umgang mit Verschlüsselung und Digitaler Signatur und für die Handhabung von Schlüsseln.

Public Key Infrastructure PKI

Eine allen Teilnehmern des Systems gemeinsame Infrastruktur regelt die Verteilung und den Austausch der öffentlichen Schlüssel. Sie beruht auf dem Sicherheitskonzept, den Benutzerrichtlinien und den Organisations- und Arbeitsanweisungen des Sicherheitspolitik und beinhaltet die folgenden Elemente:

RA – Registration Authority

Die RA stellt die Identität und Registrierung der Teilnehmer sicher, der Security Policy entsprechend.

CA - Certification Authority

Die CA generiert die Schlüssel für die Zertifizierungsstelle, zertifiziert öffentliche Teilnehmerschlüssel und personalisiert das Trägermedium für Zertifikat, Schlüsselpaar etc. Sie enthält einen Zeitstempeldienst und kann optional Schlüssel für Teilnehmer generieren.

DIR - Directory Services

DIR ist der Verzeichnisdienst.

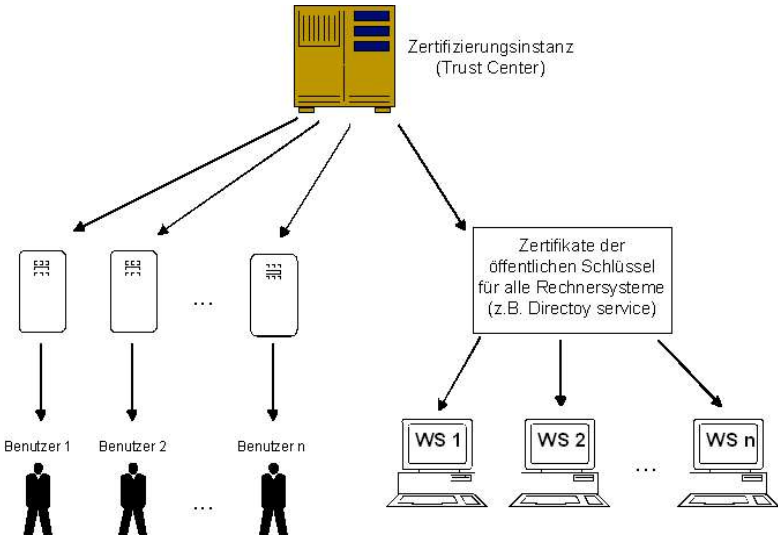

Abbildung 5: Zertifizierungsinstanz (zum Beispiel Trustcenter)

Entscheidungskriterien für die Produktauswahl

Entscheidungskriterien für die Auswahl eines geeigneten E-Mail-Security-Produktes sind die Sicherheit, Verfügbarkeit, Zuverlässigkeit, Software-Ergonomie, Schlüsselmanagement und Interoperabilität sowie der Aufwand für die Software-Wartung und die Kosten.

Sicherheit

Für hohe Sicherheit sorgt die starke Verschlüsselung (symmetrisch mindestens 112 Bit, asymmetrisch 768, 1024, 2048, ... Bit), die auf anerkannten Standards beruhen sollte und so nicht von einem Hersteller abhängt. US-amerikanische Software birgt die Gefahr von „Hintertüren“, die für staatliche Ermittlungsorgane eingebaut sind, aber auch der Wirtschaftsspionage dienen können.

Verfügbarkeit

Die rechtliche Zulässigkeit des lokalen Einsatzes (Export- bzw. Importbestimmungen) bestimmt die Verfügbarkeit des Produktes.

Zuverlässigkeit

UnabhängigeTests und etablierte, kommerzielle Produkte sind die besten Garanten der Zuverlässigkeit des Sicherheitsproduktes.

Software-Ergonomie

Besonders wichtig für den Einsatz in Unternehmen und Behörden sind die leichte Erlernbarkeit und die einfache, intuitive Bedienung. Außerdem wünscht der Benutzer die nahtlose Einbindung des Sicherheitsproduktes in E-Mail-Programme (z.B. MS Outlook, Lotus Notes, Groupwise, ...) und keine Beeinträchtigung der Geschwindigkeit bei der Verschlüsselung / Signatur.

Schlüssel-/Zertifikat-Management

Das Management von Schlüsseln und Zertifikaten beruht auf X.509-Zertifikaten, die den Einsatz von SmartCards und die LDAP-Anbindung ermöglichen.

Interoperabilität

Die „Inhomogenität“ der Kommunikationspartner, die mit verschiedenen Mail-Systemen arbeiten, setzt die Interoperabilität von eingesetzten Produkte voraus.

Software-Wartungskonzept

Wichtige Beurteilungskriterien für Sicherheitsprodukte sind die Fragen, ob Updates gemacht werden müssen, die Zusatzkosten bedeuten, und wie hoch der Aufwand für den Update der Clients (remote, silent ?) ist.

Kosten

Die Beschaffungskosten (Hardware, Software, Installation, Schulung) und die Kosten für den laufenden Betrieb (Administration, Wartung) sind einzukalkulieren.

Awareness der Anwender

Tatsache ist, dass: ca. 45 % aller Computerpannen von Anwendern durch Bedienfehler oder Nachlässigkeit verursacht werden (Quelle: KES-Studie 2000). Der Awareness der Anwender muss daher besondere Aufmerksamkeit geschenkt werden.

Schulungsmaßnahmen für Anwender umfassen die Produktschulung und die Umsetzung der Sicherheitspolitik. Anwender mit Awareness für die Sensibilität des Wirtschaftsgutes Daten behandeln Informationen und IT-Systeme als zu schützendes Gut und begreifen IT-Sicherheit als Teil der zu erfüllenden Aufgabe, und damit als Qualitätsmerkmal ihrer Arbeit.

5. Gemeinsame PKI-Struktur für Wirtschaft und Verwaltung

Die Ziele einer gemeinsamen Publik-Key-Infrastruktur liegen auf der Hand:

- Die offene Kommunikation muss international schnell und pragmatisch realisierbar sein.
- Investitionssicherheit ist ein Muss für Wirtschaft und Verwaltung, daher müssen kalkulierbare Rahmenbedingungen geschaffen werden.
- Die erste Anwendung soll der sichere E-Mail-Austausch sein, da dies die häufigste Internet-Anwendung ist.

Die auf dem S/MIME-Standard beruhende MailTrusT-Spezifizierung bietet alle Voraussetzungen der Migration für einen weiteren Zuwachs der Sicherheitslevel: die Rechtsverbindlichkeit der elektronischen Signatur ist gewährleistet und sie entspricht der EU-Richtlinie für die Digitale Signatur. Ein Einstieg mit Software-Zertifikaten ist möglich, optional mit Smartcard-Unterstützung. Dabei ist die Bridge-CA eine herstellerunabhängige, nicht-profitorientierte Dienstleistungs-CA, gesteuert durch ein unabhängiges Board.

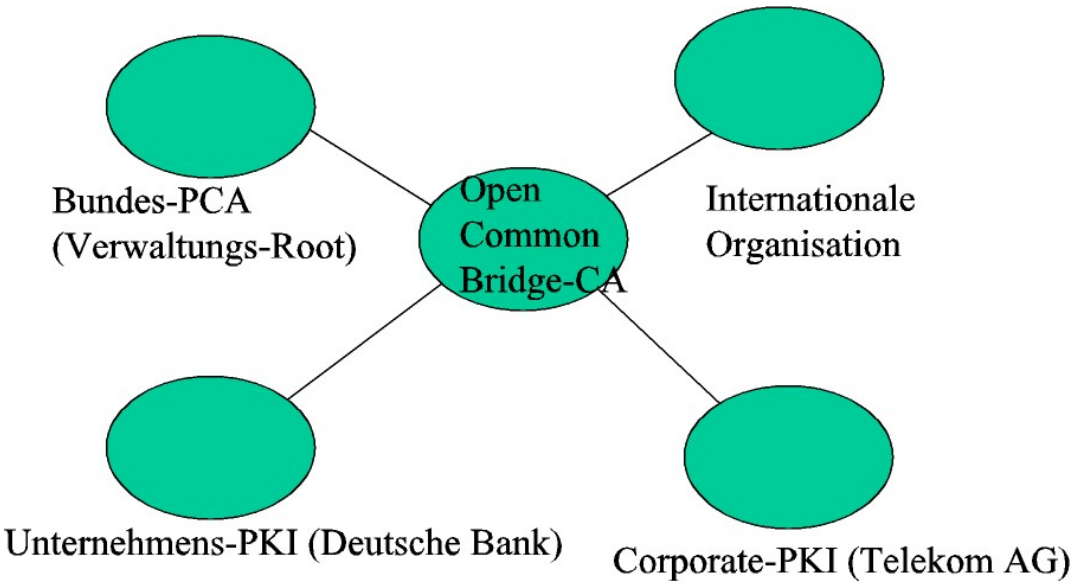

Abbildung 6: Stern-Topologie der Bridge-CA

Die Bridge-CA zertifiziert als Root die anderen CAs. Dadurch erhält sie ein grundschutzähnliches Niveau. Die Teilnehmer-CAs integrieren sich selbst in die Infrastruktur, es gibt keine Kontrollfunktion und keine Prüfung. Die erteilten Zertifikate können zurückgezogen werden. Die persönliche Registrierung geschieht initial.

Die einfach zu bedienende PKI-Lösung SafeGuard Sign&Crypt erlaubt den Import von Adressen aus Lotus Notes.

6. Fazit

Wertvolle geschäftliche Informationen sollten ebenso wenig im Klartext per E-Mail verschickt werden wie auf einer offenen Postkarte. SafeGuard Sign&Crypt für Lotus Notes von Utimaco Safeware bietet zuverlässigen Schutz der wertvollen Informationen und sichert so die Vertraulichkeit, Integrität, Authentizität, Verbindlichkeit und Verfügbarkeit der Daten – damit der digitale Geschäftsverkehr genau so gut und sicher funktioniert wie die früher eingesetzten schriftlichen Medien. Auf Standards wie S/MIME und dem Zertifikatsformat X.509 beruhend, ist Sign&Crypt mit den Produkten verschiedener anderer Hersteller aus dem MailTrusT-Verbund kompatibel und eine sichere Investition in die Zukunft, wie der Einsatz in einem großen Projekt mit bis zu 100 Tausend Clients gezeigt hat. Die Bridge-CA ermöglicht, die E-Mail-Sicherheitslösung europaweit zur Verfügung zu stellen.