Unternehmensübergreifende E-Mail-Sicherheit:

SPHINX

Norbert Pohlmann

Vorstand Utimaco Safeware AG

utimaco®
safeware

Inhalt

- Schutzbedarf
- Anforderungen an die E-Mail-Sicherheit
- Unabhängige, übergreifende Initiativen: TeleTrusT
- MailTrusT - der technische Standard
- SPHINX - die Praxis
- Open Common Bridge CA -
  die praktikable Umsetzung

Schutzbedarf (1/2)

- E-Mailversand ist die am häufigsten genutzte Anwendung im Internet.
- Inhalt und Anhang repräsentieren u.U. hohe Werte (Vertragsentwürfe, Geschäftsabschlüsse, Fusionsverhandlungen).
- Forderung: Schutz der Grundwerte der Kommunikation
  - Vertraulichkeit
  - Integrität
  - Authentizität
  - Verbindlichkeit
  - Verfügbarkeit

Schutzbedarf (2/2)

- **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.

Unabhängige, übergreifende Initiativen - TeleTrusT e.V.

- Internationale Mitglieder des TeleTrusT kommen aus den Bereichen:
  - Hersteller
  - Anwender
  - Forschungsinstitute
  - Bundesbehörden
  - Verbraucherverbände
  - Beratungsunternehmen
  - Netzbetreiber und Serviceanbieter

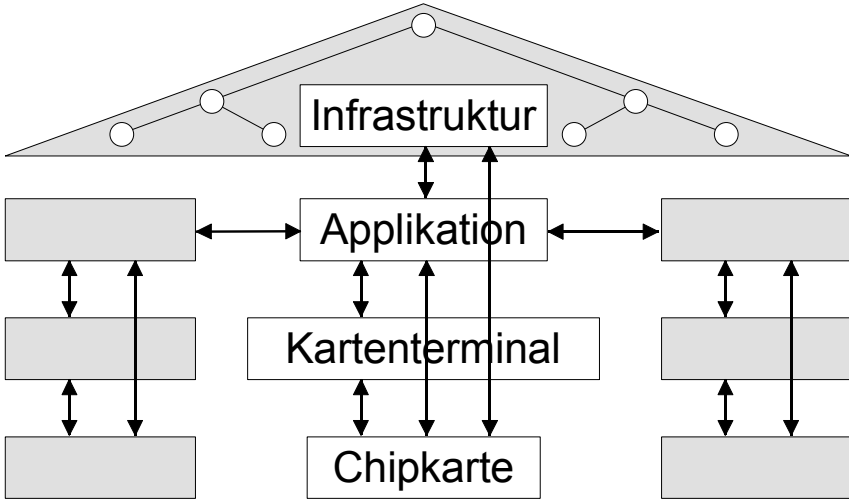
TeleTrusT e.V. - MailTrusT der Standard

- Selbstverständnis und Aufgaben:
  - Brücke zwischen Forschung und Praxis
  - Brücke zwischen Entwicklern und Anwendern
  - Schließt die Lücken zwischen theoretischer Sicherheit und marktgerechten Sicherheitslösungen
  - Zur Absicherung der Grundwerte der E-Mail-Sicherheit initiierte TeleTrusT die Entwicklung eines gemeinsamen Standards
    - MailTrusT-Standard wurde etabliert und im Projekt SPHINX einem großangelegten Praxistest unterworfen.

utimaco safeware

MailTrusT - Konzeptionelle Anforderungen

- Interoperabilität
  - herstellerunabhängige Kompatibilität
- Minimalität
  - “so wenig wie möglich, so viel wie nötig”
- Kontinuität
  - Integration von bestehenden Lösungen
- Universalität
  - keine Festlegung auf ein PKI-Modell
- Modularität - voneinander (in Grenzen) unabhängige Teile
- Standardkonformität - Berücksichtigung: ISO, IETF
- Unabhängigkeit - keine proprietären Speziallösungen



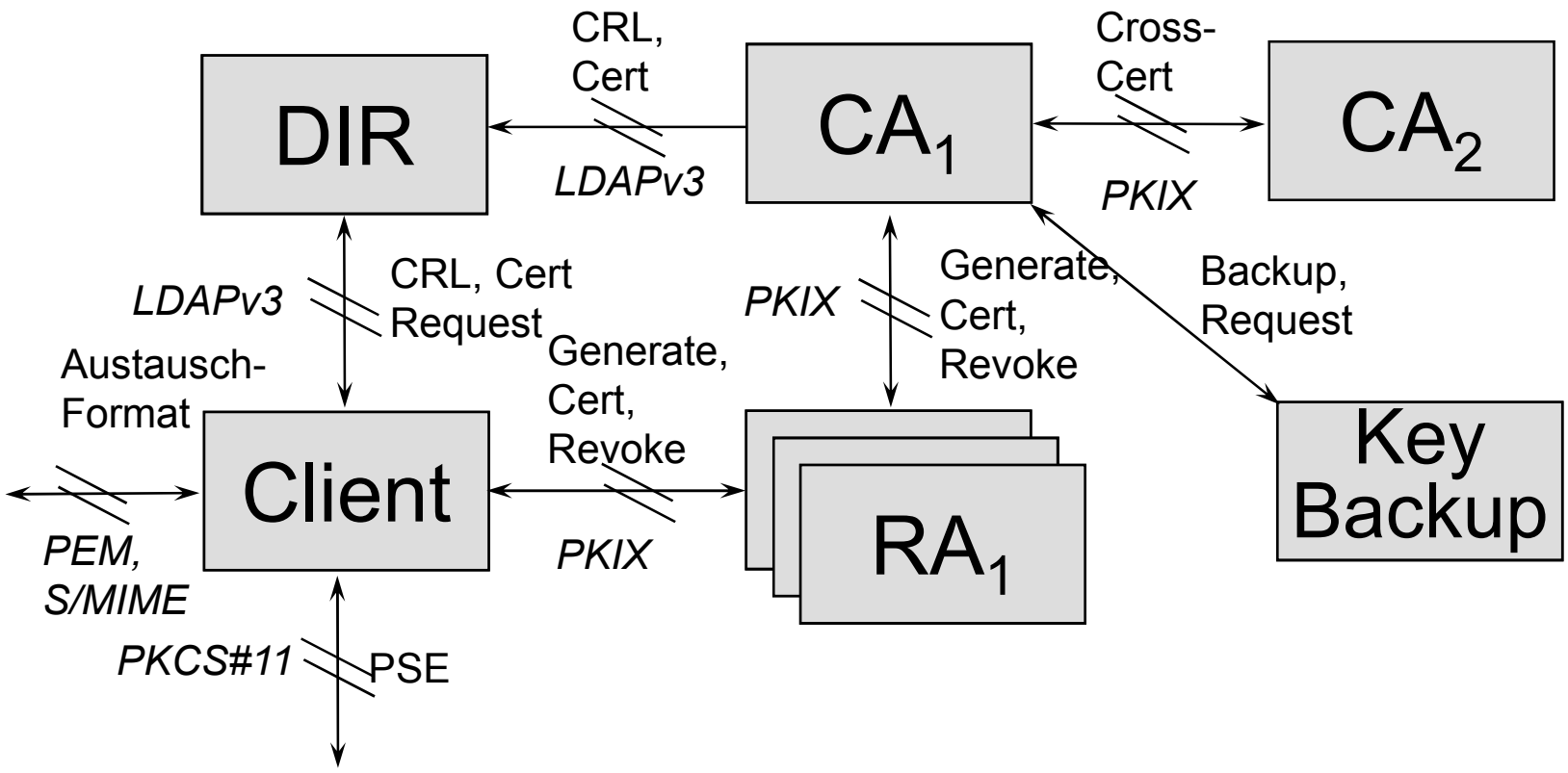
MailTrusT - Gesamtkonzept (1/2)

- Die Spezifikation des Systemkonzeptes setzt kein festes Modell einer Zertifizierungsinfrastruktur voraus. (Flexibilität)
- Jede MailTrusT-Public-Key-Infrastruktur (PKI) besteht aus folgenden Grundkomponenten:
  - Teilnehmer-Komponenten (TN)
  - Zertifizierungsstellen (CA)
  - Registrierungsstellen (RA)
  - Verzeichnisdiensten (DIR)
- Keine feste Aufgabenzuweisung an die Komponenten, um möglichst flexibel an die Anforderungen der jeweiligen Public-Key-Infrastruktur angepasst werden zu können.

MailTrusT - Gesamtkonzept (2/2)

- 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:

MailTrusT—
Komponenten und Schnittstellen



MailTrusT - Facts

- Austauschformate
  - PEM
  - MTT-Varianten
  - S/MIME
- Zertifikatsformat
  - X.509 Version 3 [X.509 (97)]
- Sperrlisten
  - X.509 CRL Version 2 [X.509 (97)]
- Verzeichnisdienst
  - LDAP Version 3
- PKI-Schnittstellen
  - PKIX-Protokolle
- Token
  - PKCS#11
  - PKCS#12
  - PKCS#13

SPHINX - Die Praxis

- Das Projekt
- Die Ziele

SPHINX - Das Projekt

- **„Ende-zu-Ende-Sicherheit für den elektronischen Dokumentenaustausch”**
  - Erprobung von E-Mail-Sicherheitsprodukten in einem für die Einführung einer Zertifizierungshierarchie „idealen“ Rahmen: im Bereich oberer Bundes- und Landesbehörden
  - Beteiligt waren: u.a. Stellen in/im
    - Bundeskriminalamt, Bundesamt für Sicherheit in der Informationstechnologie, der Innenministerien von Sachsen und Schleswig-Holstein, die Bundesdruckerei.....
  - Acht europäische Technologiehersteller testeten in diesem Projekt ihre Technologien, darunter auch drei verschiedene Trust-Center-Technologien
  - Phase 1: 4/1998 bis 9/1998
  - Phase 2: 10/1998 bis 3/1999

utimaco safeware

SPHINX - Ergebnisse (1/2)
Gute Noten für MailTrusT

- MailTrusT-Konzept stellt eine tragfähige Lösung dar
  - 81 % der Befragten vergaben gute Noten für die Einsetzbarkeit der Sicherheitstechnologien
  - 90 % hielten den abverlangten Aufwand für vertretbar

- Weitere Ergebnisse:
  - Betonung der Wichtigkeit einer guten Betreuung der Nutzer
  - Wichtig: Vermittlung von Hintergrundinformationen (Besonders: die Notwendigkeit des Einsatzes von Sicherheitstechnologien.)
  - Mehr Anwenderakzeptanz durch Sensibilisierung

SPHINX - Ergebnisse (2/2)

- Ergebnis:
  - Herstellerübergreifende Sicherheit in großen Informationsverbänden funktioniert
  - Auch komplexe Systeme können kompatibel betrieben werden
  - Die Ergebnisse des Pilotprojektes erfüllten die Erwartungen und waren ermutigend für Teilnehmer und Betreiber
  - Für die Interoperabilität der Produkte sorgt die gemeinsame Orientierung am MailTrusT-Standard von TeleTrusT

SPHINX wird fortgesetzt

- Konkrete Ziele:
  - Erweiterung des Funktionsumfangs der Produkte
  - Behebung von kleineren Problemen
- SPHINX-Projekt als vielversprechender Ansatz, der sich als Keimzelle einer umfassenden Sicherheitsinfrastruktur für E-Mails erweisen könnte
- In den kommenden Jahren sind grundlegende Schritte in Richtung eines Sicherheitssystems zu erwarten, das bald zum Geschäftsalltag gehören wird

SPHINX wird fortgesetzt

- Nach dem großen Erfolg von SPHINX ist zu hoffen, dass MailTrusT auch in anderen großen Anwendungsfeldern wie
  - Banken,
  - Versicherungen,
  - Industrie und
  - Gesundheitswesen zum Einsatz kommt.

- Vertrauenswürdigkeit für standortübergreifende IT-Geschäftsprozesse

SPHINX B

- Deutsche Telekom + Deutsche Bank gründen Initiative zur Informationssicherheit für die elektronische Kommunikation in und zwischen Unternehmen. Die Fortführung von SPHINX

Deutsche Bank 

- Bridge CA ist das Dach für vorhandene Firmen -PKIs und löst Einschränkungen bisherigen PKI-Inseln auf
- Jetzt schon sicherer E-Mails-Austausch auf Basis des S/MIME bzw. des MailTrusT-Standards möglich
- Anwender-getrieben, standard-orientiert, neutral, branchen-übergreifend

utimaco safeware

SPHINX B

- Verbindung vorhandener Firmen-CAs: unkompliziert, pragmatisch und ökonomisch akzeptabel.
- Allen Firmen offen und nicht auf Deutschland beschränkt.
- Firmen mit PKI und ein S/MIME-fähiges Mail-System, können ohne Zusatzkosten sicher auch nach außen kommunizieren.
- Die technischen Komponenten profitier(t)en vom SPHINX-Projekt. Der Stand:
  - Deutsche Bank und Deutsche Telekom nutzen als Mail-Systeme Lotus Notes und Microsoft Outlook --
    jeweils ergänzt um ein Plug-in
  - Telekom - Mitarbeiter verfügen über eine Smartcard
  - Deutsche Bank setzt SW-Zertifikate und die Smartcard ein

Open Common Bridge-CA
Offen für Firmen + Organisationen

- Open Common Bridge-CA wird von einem neutralen Board geleitet.
- Ausdehnung der offenen Infrastruktur auf weitere Großunternehmen in Kürze
- Interoperabilitätstests laufen z.B. mit Siemens, BMW, G&D etc.
- Interesse von bisher 15 weitere Großorganisationen
- Die Bundes-PCA wird sich unter die Open Common Bridge-CA einhängen
- BSI und Industrieverbände TeleTrusT (www.teletrust.de) und BITKOM (www.bitkom.org) unterstützen diese Initiative

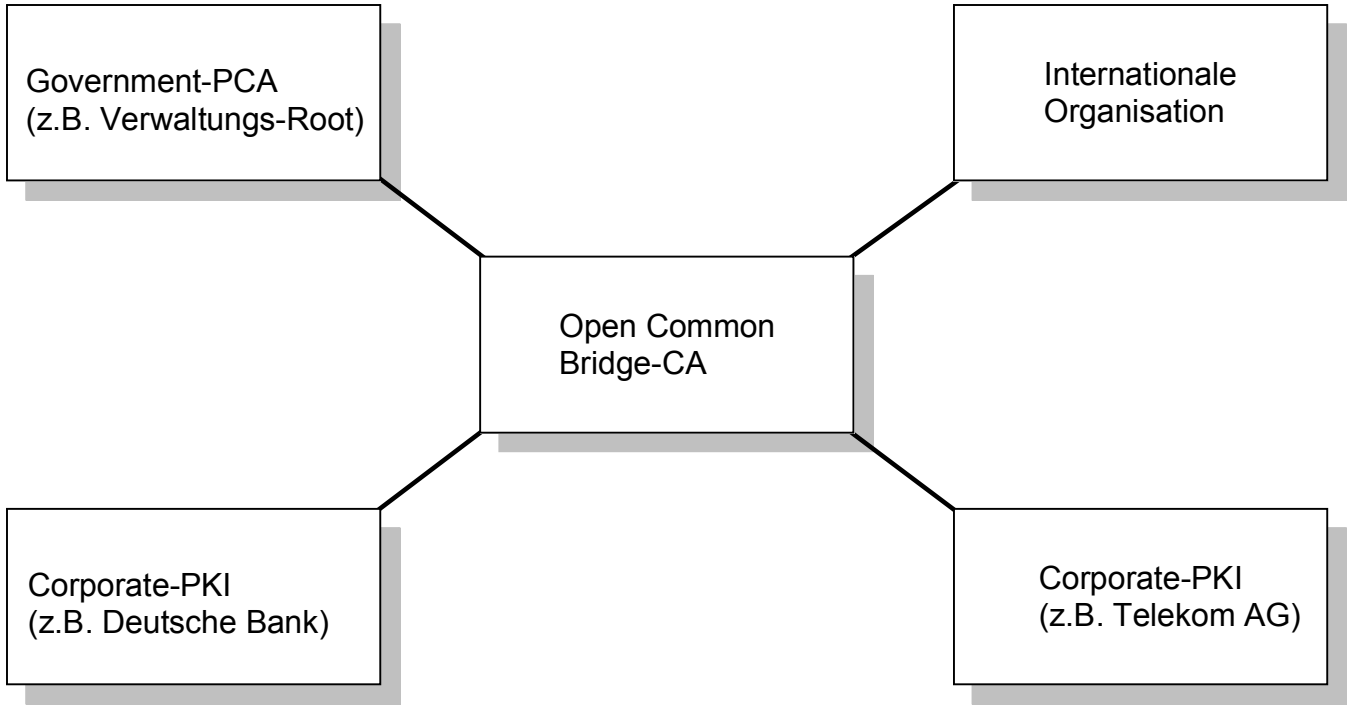
Gemeinsame PKI-Infrastruktur für Wirtschaft und Verwaltung

- Ziele / Strategie:
  - offen und international, pragmatisch, schnell
  - Investitionssicherheit schaffen
  - Barrieren beseitigen
  - Schaffung kalkulierbarer Rahmenbedingungen
  - Bündelung der Aktivitäten
  - Sichere E-Mail als erste Anwendung:
    - Beispielregion für S/MIME-Anwendung
    - erfüllt zumindest Grundschutz

Gemeinsame Infrastruktur (1/4)

- Die Migration für einen weiteren Zuwachs der Sicherheitslevel ist gegeben (elektronische Signatur, EU-Richtlinie)
- Einstieg mit Software-Zertifikaten möglich
- Smartcard-Unterstützung möglich
- Herstellerunabhängig
- Die Open Common Bridge-CA ist eine non-profit Dienstleistungs-CA, gesteuert durch ein unabhängiges Board.

Gemeinsame Infrastruktur (2/4)
Die Stern-Topologie verbindet



Gemeinsame Infrastruktur (3/4)

- Die Open Common Bridge-CA zertifiziert Root-Zertifikate der anderen CAs.
- Mindestens ein grundschutz-ähnliches Niveau
- Selbsterklärung der Teilnehmer-CAs (keine Kontrollfunktion, keine Prüfung)
- Recht auf Rückzug der erteilten Zertifikate
- Persönliche Registrierung (initial)

Gemeinsame Infrastruktur (4/4)

- BSI-Unterstützung in Richtung dieser gemeinsamen Lösung
- gemeinsames Vorgehen bei der Hilfestellung für die zukünftigen Partner-CAs, wie sie sich in diese Infrastruktur integrieren können (Whitepapers, Interoperabilität, Awareness, Schulung, Beispiele, ...)

Open Common Bridge CA - Ausblick

- Etablierung der Kultur, des Wissens und der Infrastruktur,
  - die die Internet-Sicherheit voranbringt und
  - die auch die Migration zu höchster Sicherheit unter Benutzung der Smartcard erlaubt.