

PKI – wie weiter ?

*Jens Albrecht, insinova ag
SwissInfosec 2003*

Agenda

Ausgangssituation der Firma

Zertifikatsaustausch

Zertifikatserstellung

PKI-Betriebskonzept

Kosten einer PKI

PKI für interne Zwecke wurde aufgebaut

Realisierte Funktionen

- Anmelden an der Domäne
- Anmelden an Applikationen (z.B. Citrix MF, SAP R/3)
- Sicherer Zugang per VPN und RAS
- Verschlüsseln von Dateien
- Gebäudezutritt
- Zeiterfassung
- Bezahlssystem für Kantine
- Mitarbeiterausweis



Sicherheitsaspekt

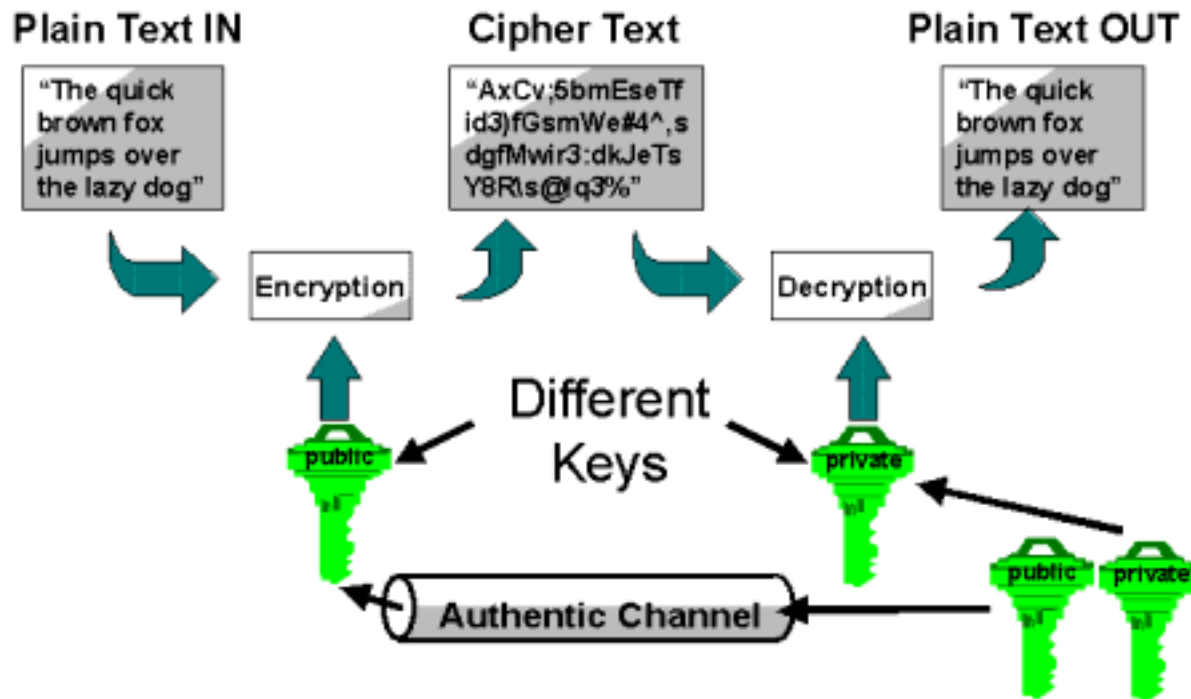
- Smart Card basierende Lösung kombiniert mit
- Gebäudezutritt, Zeiterfassung und Bezahlen
→ Gewährleistet, dass die Smart Card immer beim Benutzer ist!

Gewünschte Erweiterung

- Austausch verschlüsselter E-Mails mit Partnern und Kunden, um den Anforderungen des Datenschutzgesetzes zu entsprechen.
- Zertifikat-basierender Zugang für Partner und Kunden auf eigene Applikationen.

Voraussetzung zur E-Mail Verschlüsselung

- Der Sender muss *im Besitz des Zertifikats des Empfängers* sein, damit mit dem öffentlichen Schlüssel des Empfängers verschlüsselt werden kann.
- Die verschlüsselte Nachricht kann nur mit dem *privaten Schlüssel des Empfängers* geöffnet werden. Der private Schlüssel sollte sich auf PIN-geschützten Smart Cards befinden.

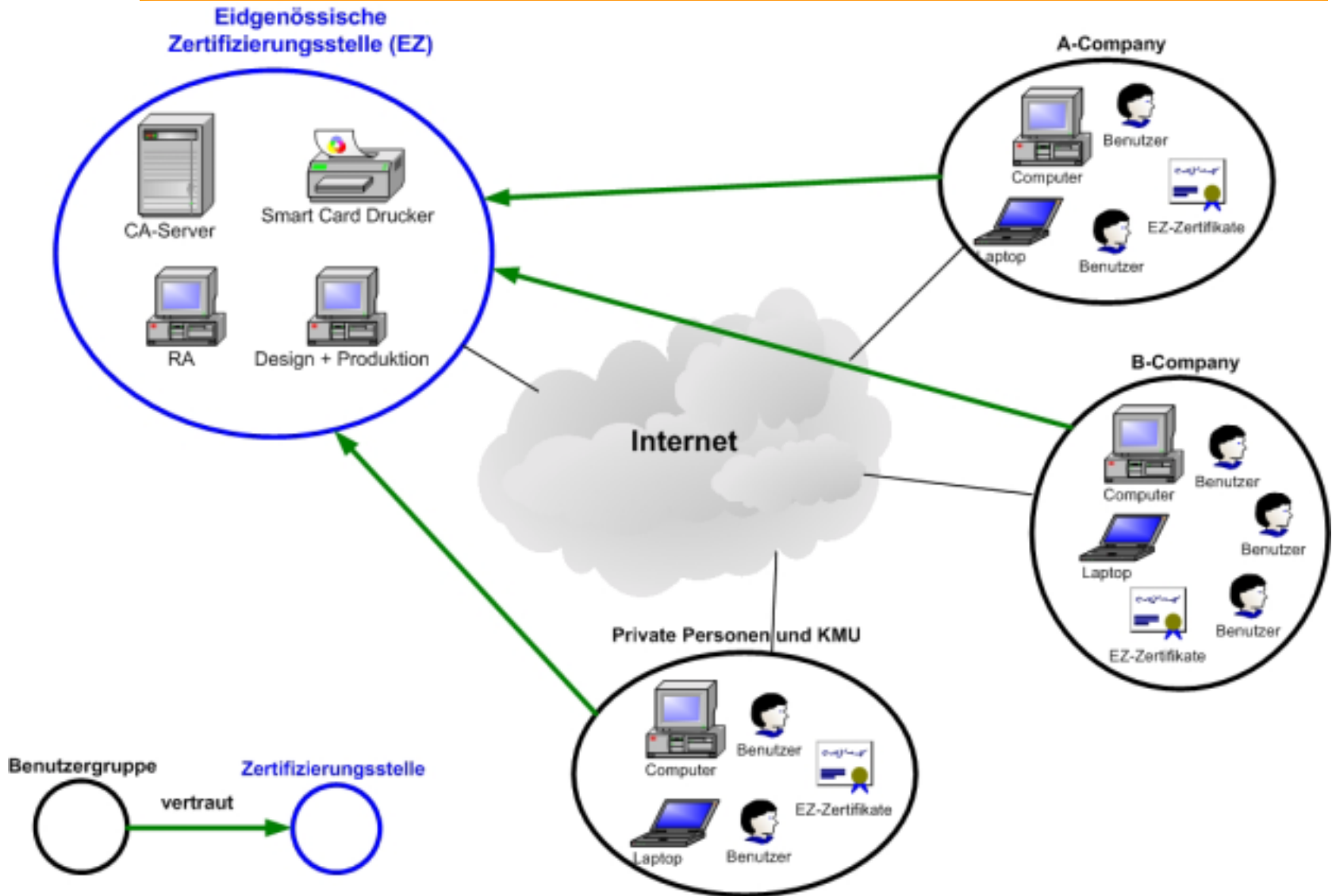


Voraussetzung zum zertifikat-basierenden Zugang

- Die Partner und Kunden müssen im Besitz eines Zertifikats sein, damit sie durch die Firma eindeutig identifiziert werden können.



Das wäre wünschenswert!



Mögliche Lösungen

Net of Trusted Private Certification Authorities

- *Die Technologie ist vorhanden → S/MIME Protokoll und X.509 Zertifikate*
- *Die Frage stellt sich, wer die Zertifikate „produziert“ und wer sich gegenseitig vertraut.*

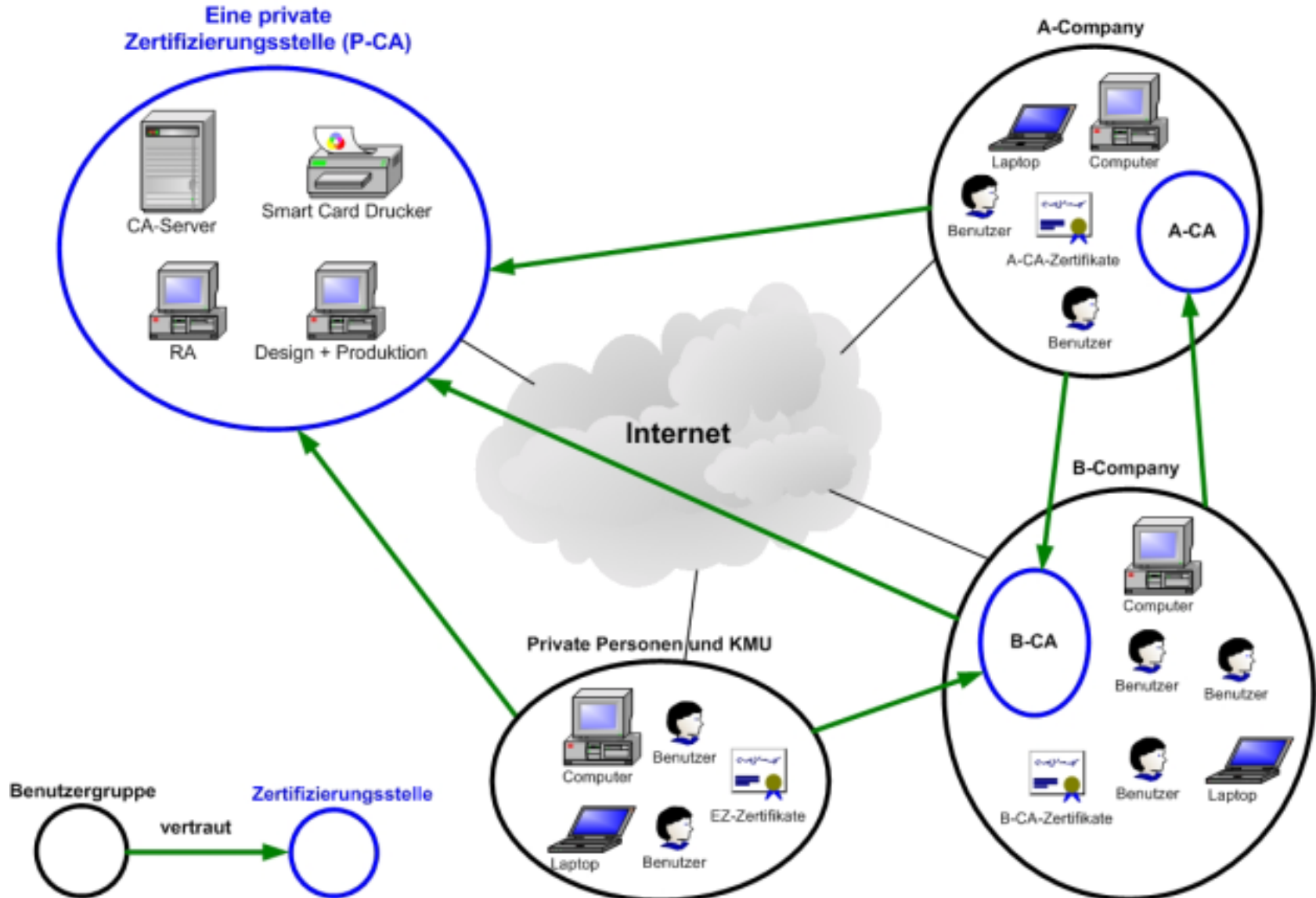
Buy

- *Zertifikate werden von einer Zertifizierungsstelle gekauft (z.B. TC TrustCenter, VeriSign oder Outsourcing-Partner).*
- *Kosten: gratis bis 95.- pro Zertifikat (1-3 Jahre gültig).*

Make

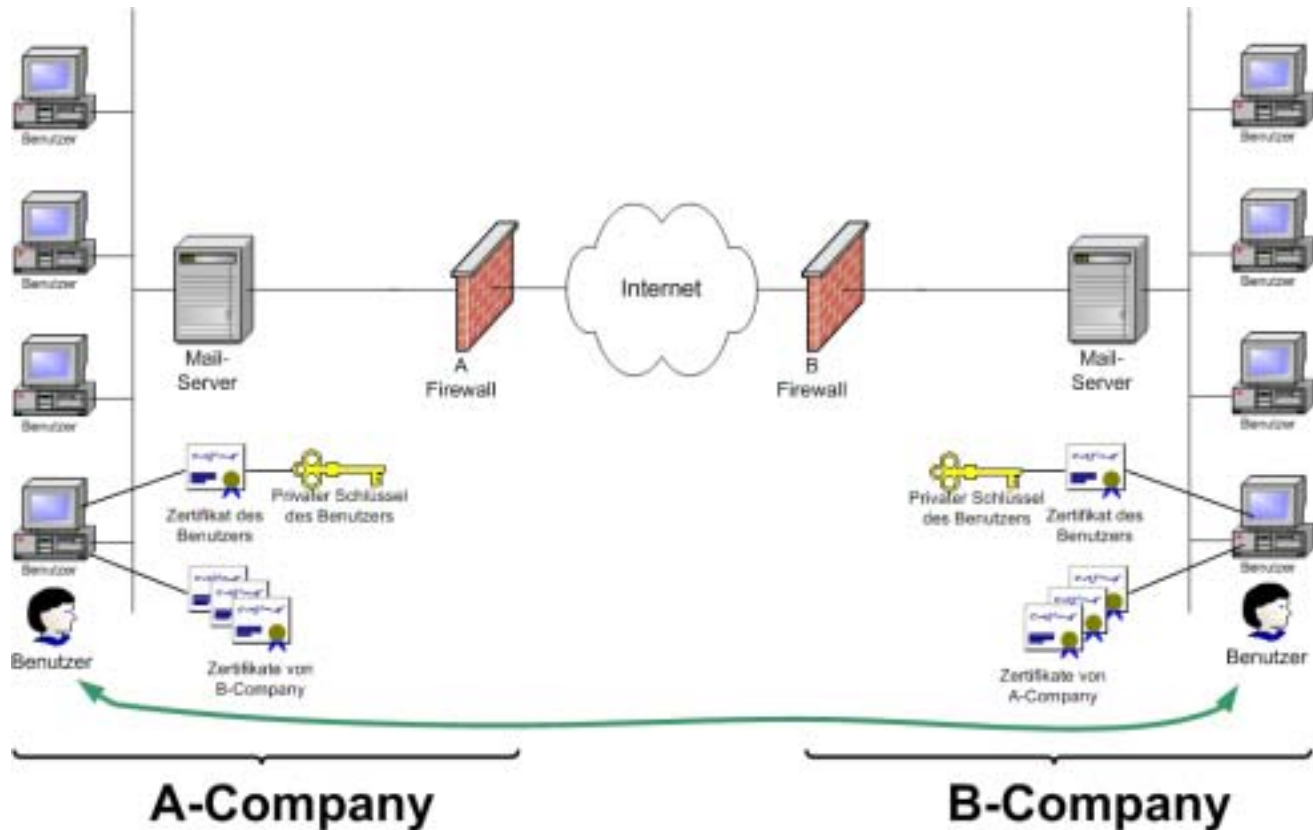
- *Die Zertifikate werden entsprechend dem Sicherheitsbedürfnis selber produziert.*
- *Kosten für eine nicht öffentliche Zertifizierungsstelle sind bezahlbar.*

Net of Trusted Private CAs



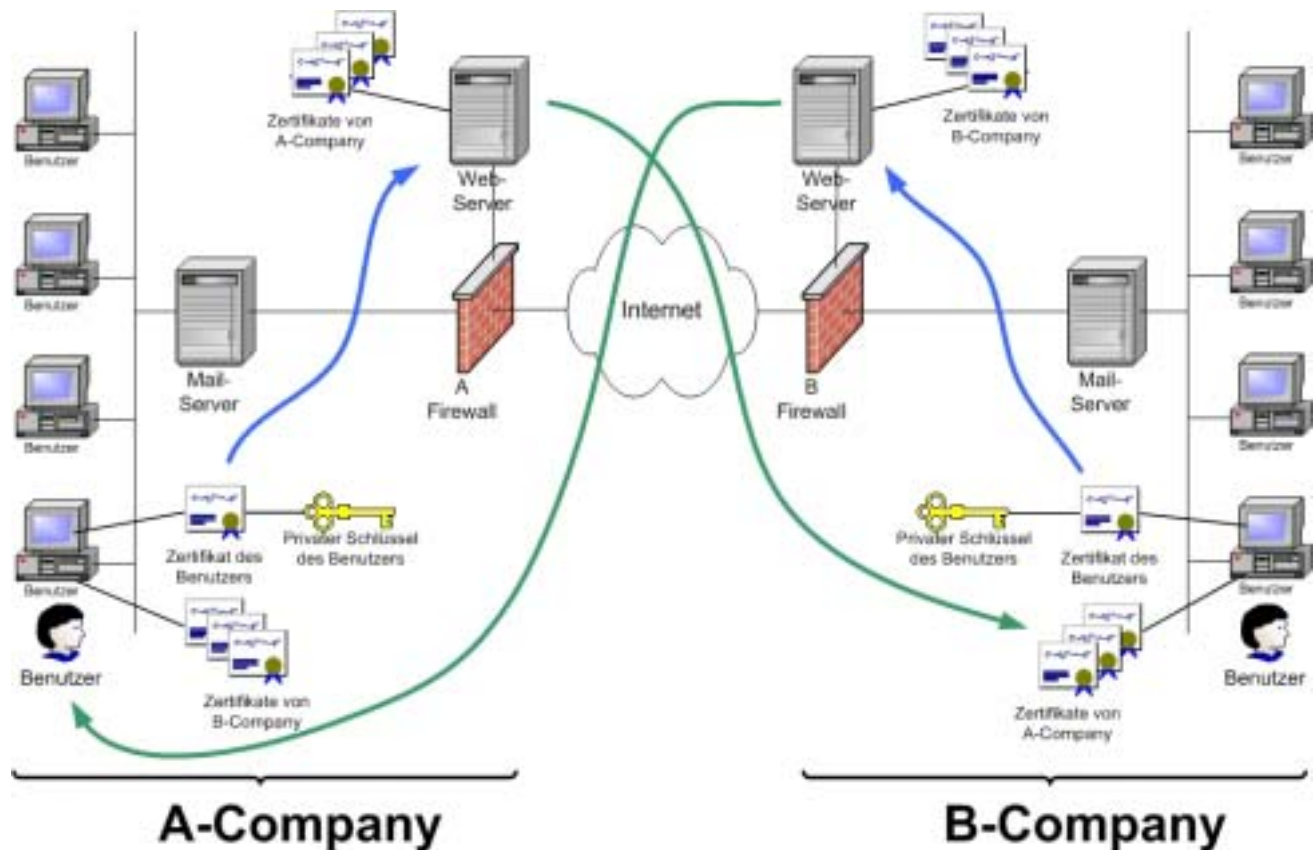
Zertifikatsaustausch manuell

- Alle Sender und Empfänger tauschen ihre Zertifikate auf eigene Initiative manuell aus.
- Entweder durch Versenden der Zertifikate oder durch signierte Mails.



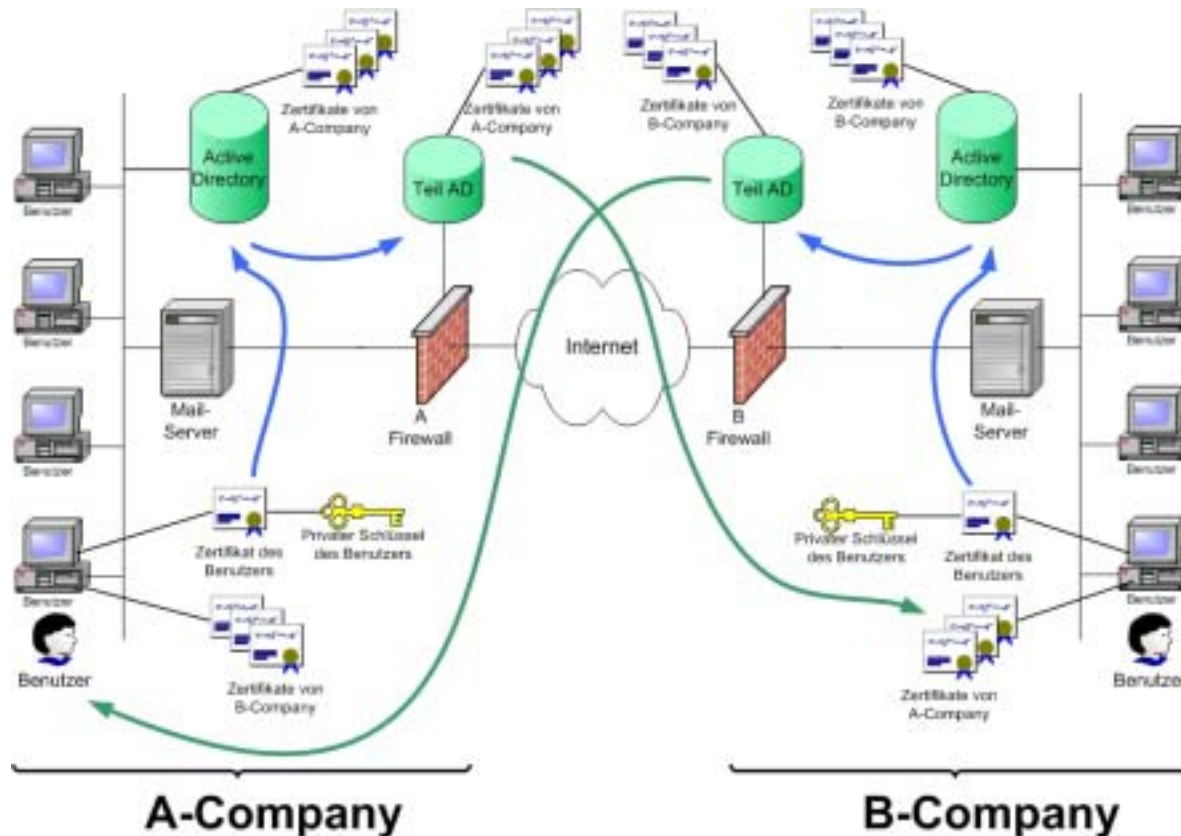
Zertifikatsaustausch halbautomatisch

- Die Sender und Empfänger haben gegenseitigen Zugriff auf einen Zertifikatsspeicherort (z.B. Web-Server).
- Benutzer kopieren sich von dort aus die Zertifikate in ihr System.



Zertifikatsaustausch automatisch

- Die Sender und Empfänger haben gegenseitigen Zugriff auf ein integriertes Adressbuch (z.B. Windows Adressbuch).
- Die Adressbücher der Empfänger sind in die Mail-Applikation integriert und die Suche nach Zertifikaten und deren Installation erfolgt automatisch.



Vertrauen

- *Zertifikaten wird nur vertraut, wenn auch der Zertifizierungsstelle vertraut wird.*
- *Vertrauen wird durch Ablauforganisation, technische Umsetzung und Verpflichtungen aufgebaut.*
- *Der RFC 2527 stellt eine umfassende Themenliste zur Verfügung, mit der das Verfassen von PKI-Betriebskonzepten erleichtert wird.*
- *Das PKI-Betriebskonzept wird von der Zertifizierungsstelle für jedermann zugänglich veröffentlicht.*

Das Vertrauen in die Zertifizierungsstelle hängt vom PKI-Betriebskonzept ab.

PKI-Betriebskonzept (Ablauforganisation)

- *Wer ist für die Zertifizierungsstelle verantwortlich?*
- *Wer darf wie welche Zertifikate beantragen?*
- *Wer darf wie welche Zertifikatswiderrufsanträge stellen?*
- *Wer darf das PKI-Betriebskonzept ändern?*
- *Wie oft wird ein Review durchgeführt?*

PKI-Betriebskonzept (technisch)

- *Wie werden die privaten CA-Schlüssel verwaltet?*
→ *Einsatz von Hardware Security Modulen (HSM)*
- *Was ist der Verwendungszweck der Zertifikate?*
→ *Authentifikation, Verschlüsselung*
- *Schlüssellängen der verschiedenen Zertifikate?*
→ *1024, 2048, 4096 bits*
- *Was sind die Betriebszeiten der Zertifizierungsstelle?*
→ *6:00h – 18:00h, max. 24h Unterbruch / Jahr*

PKI-Betriebskonzept (Verpflichtungen)

- *Verpflichtungen der Zertifizierungsstelle?*
→ *Umgang mit Anträgen, Ausstellen und Revozieren von Zertifikaten*
- *Verpflichtungen der Benutzer?*
→ *Akzeptiert Konditionen und Prozeduren, macht richtige Angaben*
- *Verpflichtungen der sich verlassenden Parteien?*
→ *Akzeptiert Konditionen, zweckmässige Benutzung des Zertifikats*

Kosten einer PKI

- **Zertifizierungsstellen-Software:**
Microsoft Windows 2003 PKI ~ CHF 2'500.-
- **Schlüsselverwaltung für Zertifizierungsstelle:**
HSM von nCipher ~ CHF 25'000.-
- **Smart Card Verwaltungs-Software:**
ID Works ~ CHF 4'000.-
- **Smart Card Personalisierer:**
Datacard Select ~ CHF 10'000.-
- **Realisierung, Ablauforganisation, PKI-Betriebskonzept:**
insinova ag ~ CHF 50'000.-
- **CSP Software auf Benutzenseite:**
Kobil SmartKey ~ CHF 120.- / User
- **Smart Cards:**
Kombikarte Infineon-Chip + Legic-Chip ~ CHF 15.- / User
- **Smart Card Lesegeräte:**
Kobil KAAN Twin ~ CHF 45.- / User

Danke

insinova

Jens Albrecht

*Dipl. El.-Ing. FH
Technischer Leiter*

*jens.albrecht@insinova.ch
www.insinova.ch*

insinova