

Public Key Infrastrukturen

Erfahrungen aus der Praxis

Dirk Fox

fox@secorvo.de



Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-452

Fax +49 721 6105-455

E-Mail info@secorvo.de

<http://www.secorvo.de>

PKI-Aktivitäten (Auswahl)

Unternehmens-PKIs:

- ◆ Bayer
- ◆ Bertelsmann
- ◆ BMW
- ◆ Commerzbank
- ◆ DaimlerChrysler
- ◆ Deutsche Bank
- ◆ Deutsche Bundesbank
- ◆ Dresdner Bank
- ◆ HypoVereinsbank
- ◆ Mannesmann

- ◆ Siemens
- ◆ Telekom
- ◆ Thyssen
- ◆ Volkswagen
- ◆ ...

Öffentliche PKIs:

- ◆ IVBB (“Sphinx”)
- ◆ Zertifizierungsstellen (SigG)
- ◆ Zertifizierungsdienstleister (TC TrustCenter, ...)
- ◆ Identrus

Erfahrungen aus der Praxis

- ◆ **Organisatorische Schwierigkeiten**
 - Registrierungsprozess mit geringen Wegezeiten
 - Öffnung des Verzeichnisdienstes nach außen
 - CRL-Policy: Häufigkeit und Gültigkeit von CRLs
 - Festlegung eines unternehmensweit eindeutigen, langfristig stabilen “Distinguished Name” (DN)
 - Komplexe DNs erzwingen Zertifikatsrückrufe
- ◆ **Technikbedingte Schwierigkeiten**
 - Einschränkung der Zertifikatsnutzung nicht durchsetzbar
 - Policies für Cross-Zertifizierung
 - Automatische Policy-Prüfung nicht möglich

Erfahrungen aus der Praxis

- ◆ **Anforderungen an Produkte**
 - **PKI-Core-Komponenten**
 - Automatisierbare Zertifikatsverlängerung (ohne Schlüsselwechsel)
 - Trennung von Zertifizierungs- und Rückrufschlüsseln
 - “Cloning” der CA-Schlüssel
 - “Message Recovery” mit separatem Recovery-Key
 - Unterstützung von “Bulk Registration” (Roll-Out)
 - Unterstützung überlappender CRLs
 - **Client-Komponenten**
 - Eindeutige Darstellungskomponente (“See what you sign”)
 - Unterscheidung verschiedener Nutzer-Zertifikate
 - Korrekte und vollständige Prüf-Policy für digitale Signaturen
 - Möglichkeit zur Auswahl des Gültigkeitsmodells