

**PKI Grundlagen und Realisierungskonzepte – 1. Tag**

10:00 Einleitung

10:15 PKI als Basis für sicheres E-Business

- Sicherheitsanforderungen
- Aufgaben einer PKI

10:45 Kryptographische Grundlagen

- symmetrische Verfahren
- asymmetrische Verfahren
- Hashfunktionen

11:30 PAUSE

10:45 Digitale Zertifikate

- Vertrauensmodelle
- Struktur digitaler Zertifikate (X.509)
- Zertifikatserweiterungen
- Zertifizierungsstrukturen
- Standardisierung

12:30 PAUSE

13:15 Elemente einer PKI

- Zertifizierungsinstanz (CA)
- Registrierungsstelle (RA)
- Schlüsselgenerierung (KG)
- Schlüsselverzeichnis
- SmartCards und weitere HW/SW Tokens
- Zertifikatsspeicher
- PKI Middleware

14:15 Zertifikatsstatus

- CRL, Delta-CRL
- OCSP
- Weitere Verfahren

14:45 PKI-basierte Anwendungen (1) (mit Demonstration)

- Sichere E-Mail
- Verschlüsselung von Dateien und HDD-Volumes
- Digitale Signatur von Dokumenten

15:30 PAUSE

15:45 PKI-basierte Anwendungen (2)

- Authentisierungsprotokolle
- Kerberos
- Windows Authentisierung
- Web-Authentisierung – SSL/TLS
- .

16:15 Rechtliche und organisatorische Rahmenbedingungen

- Signaturgesetz
- Qualifizierte Zertifikate
- Gültigkeitsmodelle
- Zertifikatsrichtlinie und Nutzungserklärung (CP, CPS)

17:00 Diskussion

17:30 Ende Tag 1



**PKI Grundlagen und Realisierungskonzepte – 2. Tag**

09:00 Zusammenfassung vom Vortag

09:15 Organisation und Abläufe in einer PKI

- Zertifizierungsstrukturen
- Aufgaben eines Trust-Centers
- Lebenszyklus von Schlüsseln und Zertifikaten
- Registrierungsverfahren
- Sperrungen von Zertifikaten
- CA-Backup, Key Recovery
- Absichern von Servern
- PKI Rollen

11:00 PAUSE

11:15 PKI-Interworking

- Unternehmensübergreifende Verschlüsselung
- Gegenseitiges Vertrauen
- Mechanismen und Dienste

11:45 Realisierungsalternativen

- Make-or-buy
- Produkt- und Anbieterübersicht
- Managed PKI Services
- SmartCards vs. SW-Keys

12:30 PAUSE

13:15 Umsetzung einer internen PKI

- Produkte
- Open Source
- Beispiel einer Windows PKI

14:45 Planung eines PKI Projektes

- Projektphasen
- Zeitplanung
- Kosten- und Nutzenbewertung
- Praktische Hinweise

15:45 PAUSE

16:00 PKI Status heute und morgen

- Übersicht über existierende PKI und Projekte
- Ausblick auf künftige Entwicklungen

16:30 Diskussion

17:00 ENDE des Seminars

