PKI Grundlagen und Realisierungskonzepte – 1. Tag

10:00 Einleitung

10:15 PKI als Basis für sicheres E-Business
- Sicherheitsanforderungen
- PKI Nutzen
- Aufgaben einer PKI
- Motivation für PKI

10:45 Kryptographische Grundlagen
- Symmetrische Verfahren
- Asymmetrische Verfahren
- Hashfunktionen

11:30 PAUSE

11:45 Digitale Zertifikate
- Vertrauensmodelle
- Aufbau digitaler X.509-Zertifikate
- Zertifizierungsstrukturen
- Zertifikatsprofile
- Gültigkeit und Zertifikatsstatus (CRL, OCSP)
- Standardisierung

13:00 PAUSE

13:45 Elemente einer PKI
- PKI-Dienste (CA, RA, KG, Directory)
- PKI Management-Protokolle (PKCS#10,SCEP)
- Schlüsselspeicher (SmartCards, HSMs etc)
- Zertifikatsspeicher
- PKI Middleware

14:30 PKI-basierte Anwendungen (1) (mit Demonstration)
- Sichere E-Mail
- Verschlüsselung von Dateien und HDD-Volumes
- Digitale Signatur von Dokumenten
- Zeitstempel

15:45 PAUSE

16:00 Rechtliche Aspekte
- Kryptogesetze
- Signaturgesetzgebung
- Elektronische Identifizierung und Vertrauensdienste (eIDAS)

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
- Lebenszyklus von Schlüsseln und Zertifikaten
- PKI-Organisation
- PKI Rollen
- Aufgaben eines Trust-Centers
- CA-Strukturen
- Zertifikatstypen
- Zertifikatsrichtlinie und Nutzungserklärung (CP, CPS)

10:15 PAUSE

10:30 Realisierungsalternativen
- Make-or-buy
- Produkt- und Anbieterübersicht
- Managed PKI Services
- SmartCards vs. SW-Keys

11:30 Umsetzung einer internen Windows-PKI
- Features, CA-Typen
- Architektur, Komponenten, Tools
- Certificate Templates
- Rollen
- Enrollment
- Sperrmechanismen (CRL, OCSP)
- Active Directory

12:30 PAUSE

13:15 PKI-Anwendungen (2)
- Code-Signing
- Datenverschlüsselung
- Starke Authentisierung
- Kerberos & PKINIT
- SSL/TLS
- IPSec
- 802.1x

14:15 PKI-Interworking
- Unternehmensübergreifende Verschlüsselung
- Gegenseitiges Vertrauen
- PKI Bridges

15:00 PAUSE

15:15 Planung eines PKI Projektes
- Kosten- und Nutzenbewertung
- Projektphasen
- Zeitplanung
- Praktische Hinweise

16:00 PKI Status heute und morgen
- Übersicht über existierende PKIen und Projekte
- PKI-Vorfälle
- Ausblick auf künftige Entwicklungen

16:30 Diskussion

17:00 ENDE des Workshops