

Aufbau einer Windows PKI – 1. Tag

- 10:00 Begrüßung und Einleitung
- 10:15 Einführung in die kryptographischen Grundlagen
- Symmetrische & asymmetrische Algorithmen
 - Hashfunktionen
 - Smartcards, Crypto-Tokens
- 11:00 Digitale Zertifikate
- Vertrauensmodelle
 - Struktur digitaler Zertifikate (X.509)
 - Zertifikatserweiterungen
- 11:30 PAUSE
- 11:45 Public Key Infrastruktur
- Aufgaben und Elemente einer PKI (CA, RA, ...)
 - Zertifizierungsstrukturen
 - Registrierungsverfahren
- 12:15 Zertifikatsstatus
- CRL, Delta-CRL
 - OCSP
 - Weitere Verfahren
- 12:45 PAUSE
- 13:30 Rechtliche und organisatorische Rahmenbedingungen
- Signaturgesetz
 - Qualifizierte Zertifikate
 - Gültigkeitsmodelle
 - Zertifikatsrichtlinie und Nutzungserklärung (CP, CPS)
- 14:15 PKI Schnittstellen und Formate
- PKCS# Standards
 - ASN.1, PEM Kodierung
 - PKIX
- 15:00 PAUSE
- 15:15 PKI Architektur und Schnittstellen in Windows
- CryptoAPI und CNG
 - Kryptografiedienste (CSP)
 - SmartCards und Crypto-USB Tokens
 - Zertifikatsspeicher
 - Liste vertrauter Zertifikate (CTL)
- 16:00 PKI-basierte Anwendungen unter Windows
- Sichere E-Mail (z.B. Outlook)
 - Digitale Signatur von Dokumenten (z.B. Adobe PDF, Office XML)
 - Authentisierungsprotokolle (z.B. SmartCard Logon, SSL)
 - Datenverschlüsselung (z.B. EFS)
 - Sichere Netze, VPNs (z.B. IPsec)
- 16:45 Diskussion, offene Fragen
- 17:30 ENDE des 1. Seminartages

Aufbau einer Windows PKI – 2. Tag

09:00 Zusammenfassung vom Vortag

09:15 Windows Certificate Services

- Übersicht
- Architektur
- Policy- und Exit-Module
- Intermediaries
- Zertifikatsvorlagen (Templates)
- OCSP Responder (2008)
- Administrationswerkzeuge

10:30 PAUSE

10:45 Zertifizierungsstellen (CAs)

- Root, Intermediate und Issuing CA
- Enterprise vs. Offline CA

11:15 Enrollment Strategien

- Manuelle Registrierung
- Autoenrollment
- SmartCard Enrollment
- Key Backup und Recovery

12:00 PAUSE

12:45 Nutzung des AD

- Zertifikate, Templates und CRLs im AD
- Group Policies
- Veröffentlichungspunkte

13:30 PKI Rollen und Berechtigungen

- Registrierungsagenten
- Key Recovery Agents
- CA-Rollen
- Rollentrennung

14:15 PAUSE

14:30 Betriebssicherheit

- CA-Absicherung
- PKI-Verfügbarkeit
- Notfall-Wiederherstellung

15:15 PAUSE

15:30 PKI Planung, Realisierung, Betrieb

- Vorgehensweise
- Beispiele und Hinweise
- Literatur

16:15 PKI-Projektbeispiele

- Existierende PKI Lösungen
- Beispiele

16:45 Diskussion, offene Fragen

17:30 ENDE des 2. Seminartages

Aufbau einer Windows PKI – 3. Tag

09:00 Zusammenfassung vom Vortag

09:15 Aufbau einer 2-stufigen CA

- CA-Policy.inf
- Exit-Module (SMTP-Benachrichtigung)
- Anpassen der CRL-Lifetime (certutil)

10:45 PAUSE

11:00 Manuelle Zertifikatsanforderung

- Anforderung über das Webinterface
- Anforderung mit certreq.exe
- Bearbeiten der ausstehenden Zertifikatsanforderung mit certutil

11:45 CTL

- Vertrauenswürdigen CAs im AD veröffentlichen

12:00 PAUSE

12:45 Autoenrollment und Zertifikatsvorlagen

- Gruppenrichtlinien anpassen
- Autoenrollment Szenario durchspielen

13:45 Smartcards und Token

- Typen + Treiber (Aladdin, Siemens)

14:15 Smartcard Enrollment

14:45 Smartcard Anmeldung konfigurieren

- Voraussetzungen + Konfiguration

15:00 Key Recovery

- Certutil
- Krt

15:30 Backup + Recovery einer Microsoft PKI

16:00 Upgrade auf Server 2008 + OCSP Responder

16:30 Diskussion, offene Fragen

17:15 ENDE des 3. Seminartages

