Aufbau einer Windows PKI – 1. Tag

10:00 Begrüßung und Einleitung
10:15 Kryptografie Grundlagen
- Symmetrische & asymmetrische Algorithmen
  Hashfunktionen

11:00 Digitale Zertifikate
- Aufbau digitaler Zertifikate (X.509, PKIX)
- Standards (ASN.1, PKCS#,…)
- CA-Hierarchien
- Gültigkeit und Vertrauenswürdigkeit
- Zertifikatsstatus (CRL, Delta-CRL, OCSP)

11:45 PAUSE
12:00 Public Key Infrastruktur
- PKI-Dienste (CA, RA, Directory…)
- PKI Protokolle (PKCS#10, SCEP,…)
- Schlüsselspeicher (SmartCards, TPM, HSM,…)

13:00 PAUSE
13:45 Active Directory Certificate Services
- Architektur
- Komponenten (CA Engine, Intermediaries, Policy, Exit Module, …)
- Betriebsmodi (Offline CA, Enterprise CA)
- Erweiterungen (OCSP Responder, NDES)
- Windows Editionen und PKI Features
- Cross-Forest
- Interworking mit externe PKIen

14:30 ADCS am praktischen Beispiel
15:00 PKI Architektur und Schnittstellen in Windows (mit Demonstration)
- CryptoAPI und CNG
- Kryptografiedienste (CSP, KSP))
- DPAPI
- Windows Certificate Store
- Credential Roaming
- Windows Zertifikatsvalidierung

15:30 PAUSE
15:45 PKI Anwendungen unter Windows (mit Demonstration)
- S/MIME E-Mail (Outlook)
- Dokumentsignatur (Adobe PDF, Office XML)
- Code Signing
- Datenverschlüsselung (EFS)

16:45 Netzwerkprotokolle mit PKI
- SmartCard Logon mit Kerberos und PKINIT
- SSL/TLS
- IPsec
- 802.1x

17:30 Diskussion, offene Fragen
18:00 ENDE von Workshop-Tag 1

Aufbau einer Windows PKI – 2. Tag

09:00 Zusammenfassung vom Vortag
09:30 Windows CAs
- Root, Intermediate und Issuing CA
- Enterprise vs. Offline CA

10:00 PKI Tools
- GUI Werkzeuge
- Kommandozeilenwerkzeuge (certutil, certreq,…)
- CAPOLICY.INF

10:30 Enrollment Verfahren
- Manuelle Registrierung
- Autoenrollment
- SmartCard Enrollment
- Web Enrollment
- NDES und SCEP
- Key Backup und Recovery
- Enrollment Proxy

11:30 Validierung und Sperrung
- Prüfung der Zertifikatskette
- Sperrlisten (CRL, Delta-CRL, CDP)
- OCSP Responder

12:00 PAUSE
12:45 PKI mit Active Directory
- Certificate Templates
- Group Policies
- Veröffentlichungspunkte

13:15 PKI Rollen und Berechtigungen
- Registrierungsagenten
- Key Recovery Agents
- CA-Rollen
- Rollentrennung

13:45 PKI Planung & Vorbereitung
- Auswahl der PKI Anwendungen
- CA-Hierarchie und Parameter
- PKI-Prozesse & Organisation
- Migration Windows ADCS 2008→2012
- Installationsvorbereitung

14:30 ADCS am praktischen Beispiel
15:30 PAUSE
15:45 Betriebssicherheit
- Backup/Restore
- CA-Absicherung und Härtung
- PKI-Verfügbarkeit
- Notfall-Wiederherstellung (Disaster Recovery)

16:30 Diskussion, offene Fragen
17:00 ENDE des Workshops