TRAINING-GROTE
SCHULUNG&CONSULTING

Zertifikate
Exchange Server / WLAN

Referent: Marc Grote

Agenda

- Verwendungszweck von Zertifikaten
- Krytografiegrundlagen
- Symmetrische / Asymmetrische Verschluesselungsverfahren
- Windows Zertifizierungsstellen
- Zertifikatbeantragung
- Exchange und Zertifikate
- WLAN und Zertifikate

Verwendungszweck von Zertifikaten

- Code Signing
- EFS
- IPSEC
- VPN
- LDAP (Active Directory)
- Webserver
- SMTP TLS
- OWA / EAS / OA /Autodiscover
- WLAN

Zertifikatstypen

- Client Zertifikate
- Server Zertifikate
- Single Name Zertifikate
- Wildcard Zertifikate
- SAN Zertifikate
- Self Signed Zertifikate
- Zertifizierungsstellenzertifikate
- Speicherort von Zertifikaten
- Zertifikaterneuerung

Krytografiegrundlagen

- Signatur
- Verschluesselung
- Signatur und Verschluesselung
- Authentizitaet
- Integritaet

Symmetrische / Asymmetrische Verschluesselung

Alice ☺

Bob ☺

Was ist eine PKI

Als Public-Key-Infrastruktur (PKI, engl.: public key infrastructure) bezeichnet man in der Kryptologie und Kryptografie ein System, welches es ermöglicht, digitale Zertifikate auszustellen, zu verteilen und zu prüfen. Die innerhalb einer PKI ausgestellten Zertifikate sind meist auf Personen oder Maschinen festgelegt und werden zur Absicherung computergestützter Kommunikation verwendet.

Quelle: http://de.wikipedia.org/wiki/PKI

Bestandteile einer PKI

Digitale Zertifikate:

Digital signierte elektronische Daten, die sich zum Nachweis der Echtheit von Objekten verwenden lassen.

Certification Authority:

Organisation, welche die Bereitstellung von Zertifikaten übernimmt.

Registration Authority:

Organisation, bei der Personen und Maschinen Zertifikate beantragen können.

Certificate Revocation Lists:

(Sperrliste) Listen mit zurückgezogenen, abgelaufenen und für ungültig erklärten Zertifikaten.

Verzeichnisdienst:

Ein durchsuchbares Verzeichnis welches ausgestellte Zertifikate enthält, meist ein LDAP-Server, seltener ein X.500-Server.

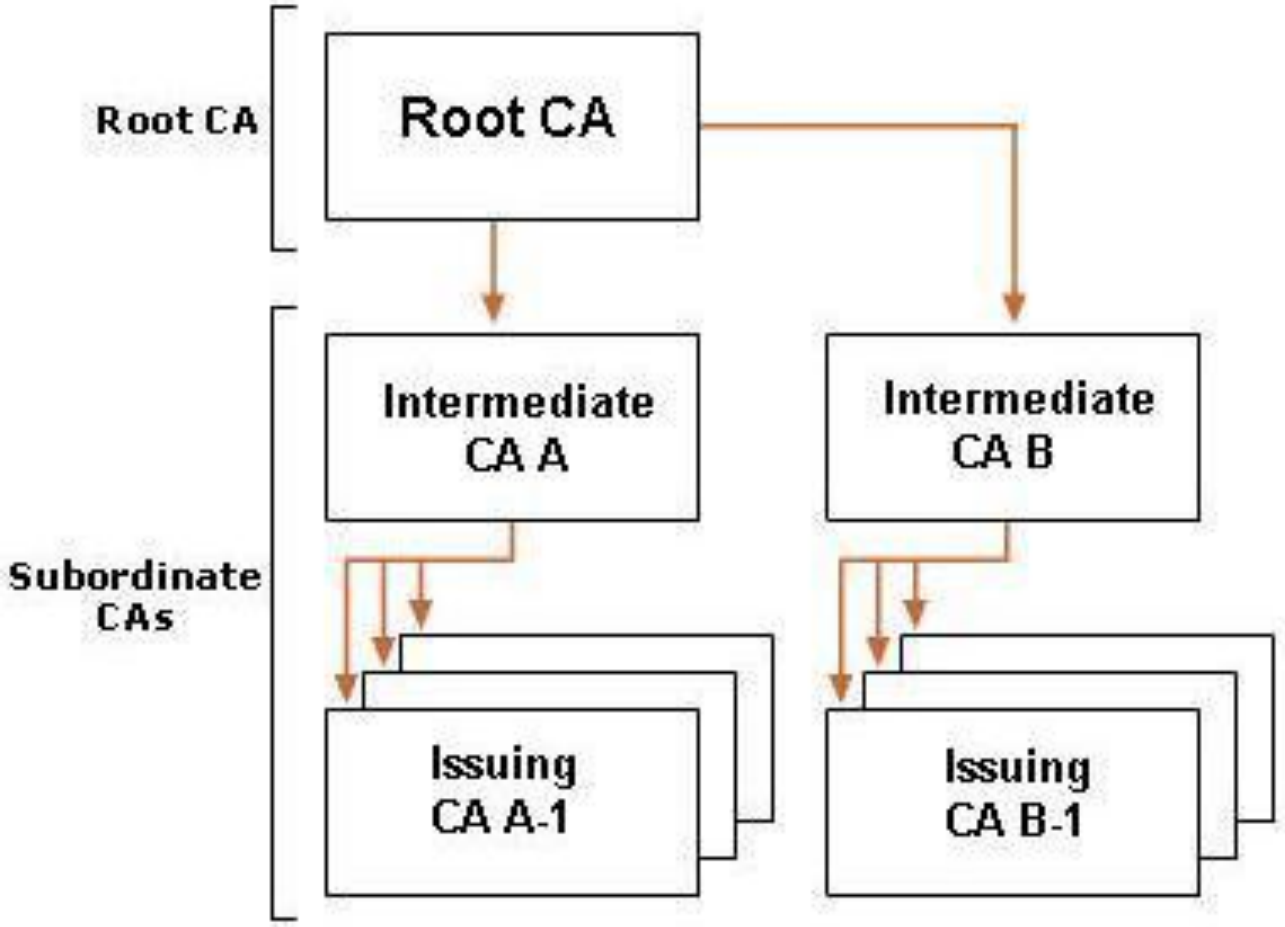
Validierungsdienst:

Ein Dienst, der die Überprüfung von Zertifikaten in Echtzeit ermöglicht.

Windows Zertifizierungsstellen

- Standalone CA
- Enterprise CA
- Intermediate CA
- Issuing CA
- Unterschiede Standard und Enterprise
- Zertifikatvorlagen
- CA Administration
- PKI Health Utility
- Schluesselarchivierung
- Backup und Recovery

CA Hierarchien



Unterschiede Standard / Enterprise

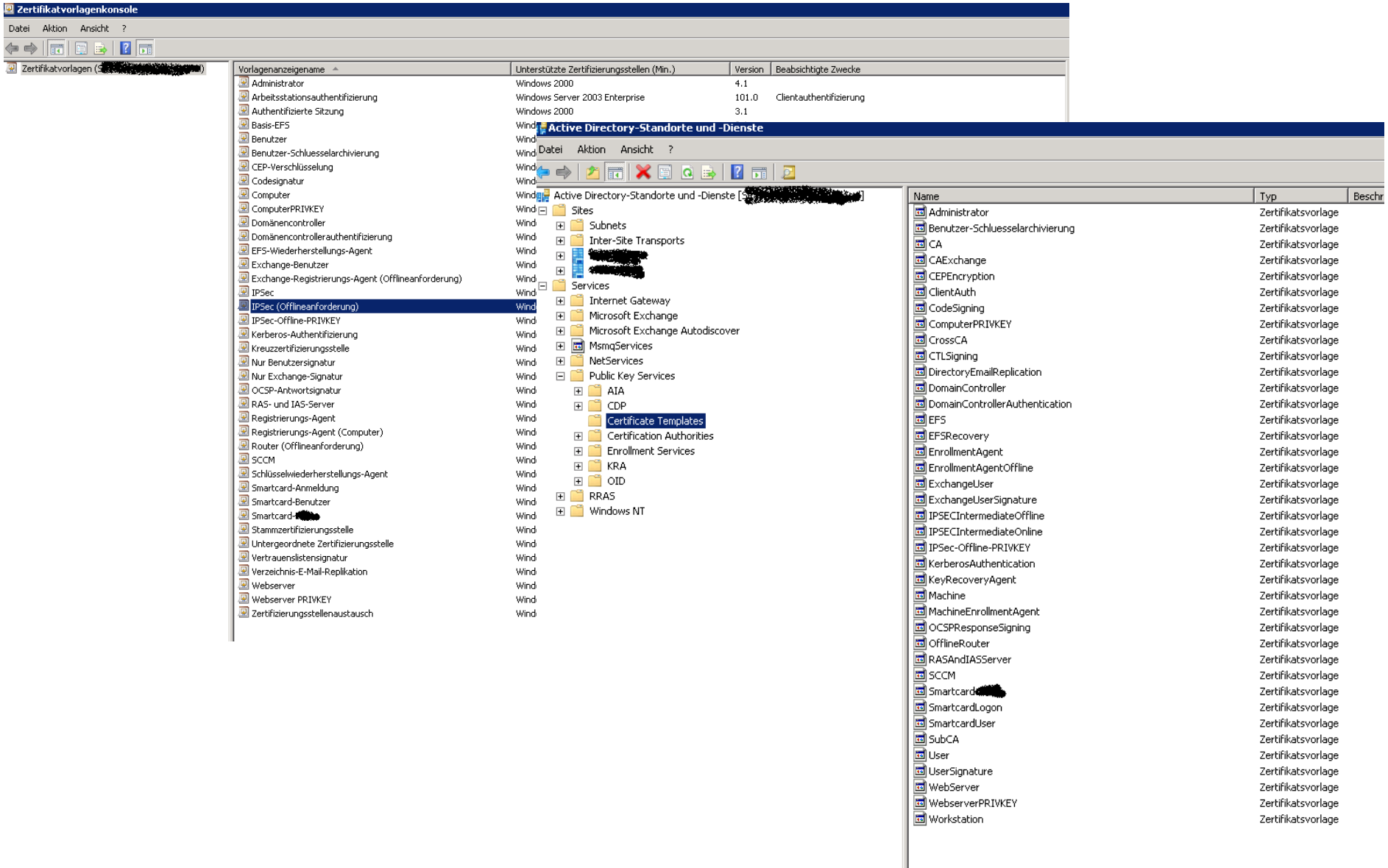
Windows Server 2008 R2 Standard

– Alle Basisfunktionen einer Windows 2000 PKI

Windows 2008 R2 Enterprise und Datacenter

– Alle Funktionen der Windows 2008 R2 Standard PKI
– NDES
– SCEP
– OCSP

Zertifikatvorlagen

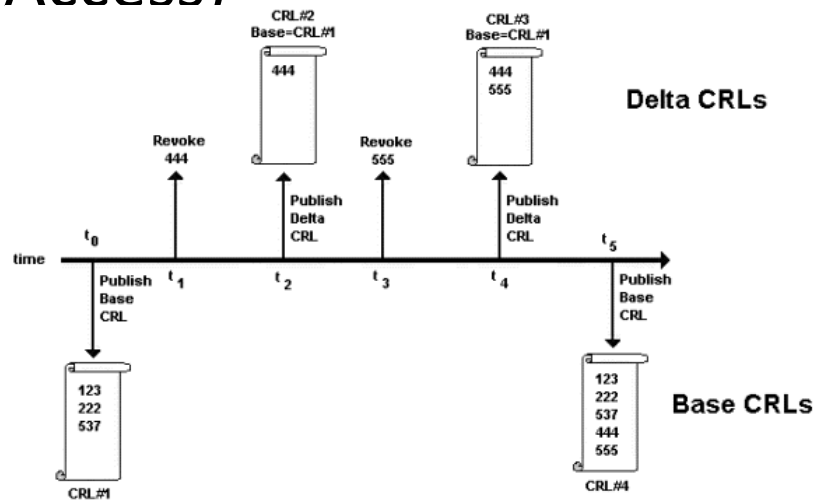


CA Administration

- Grundlegende Konfiguration
- Zertifikatvorlagenverwaltung
- Berechtigungsverwaltung
- Sperrlistenverwaltung
- Backup und Restore

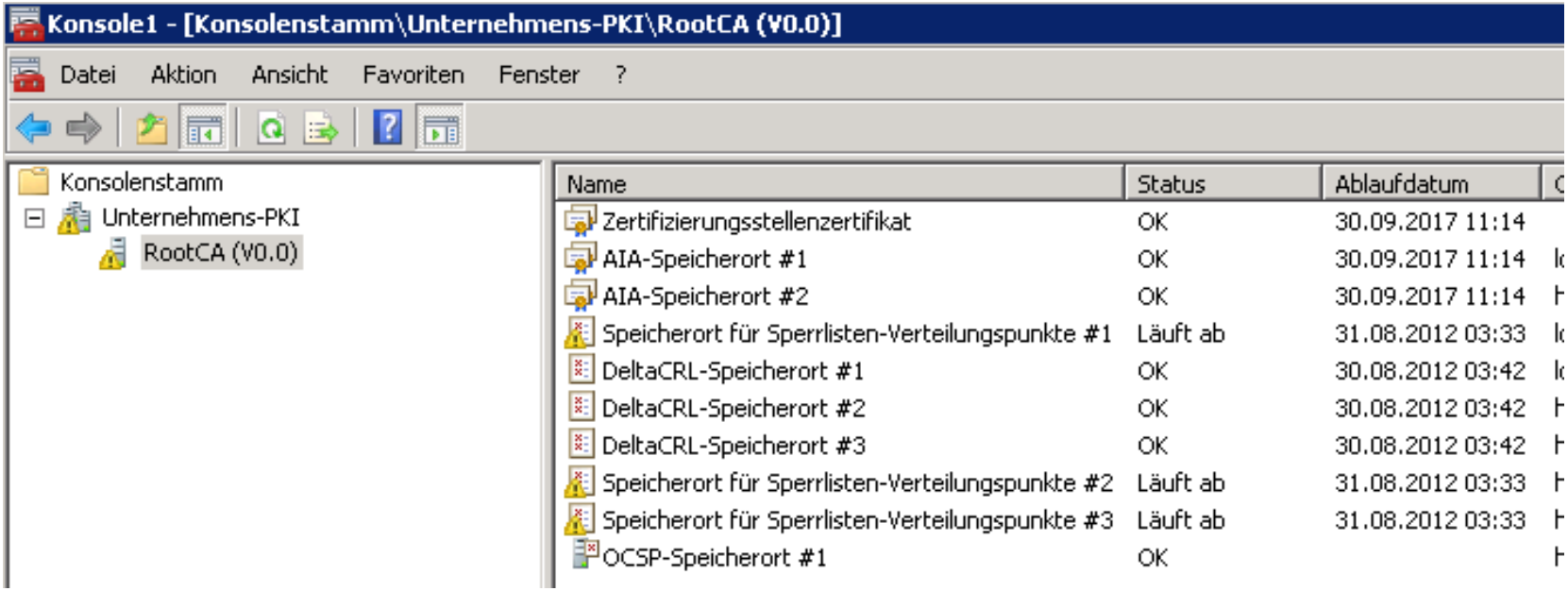
Sperlistenverwaltung

- OCSP (Online Certificate Status Protocol)
- CRL (Certificate Distribution List)
  - Base CRL
  - Delta CRL
  - AIA (Authority Information Access)
  - CDP (CRL Distribution Point
    - LDAP
    - File
    - HTTP (Internal / External)



PKI Health

Prueft den „Gesundheitszustand einer internen Public Key Infrastruktur



Zertifikatbeantragung

- Webschnittstelle
- MMC
- Certutil
- Autoenrollment

Schluesselarchivierung / Wiederherstellung

- CA fuer Schluesselarchivierung aktivieren
  - Key Recovery Agent Zertifikate
- CA Template fuer Schluesselarchivierung aktivieren
- Zertifikatwiederherstellung mit CERTUTIL
  - http://technet.microsoft.com/en-us/library/ee449489(WS.10).aspx

Exchange und Zertifikate

- Verwendungszweck
- Self signed Zertifikate
- Self Signed Zertifikate „trusted“
- Zertifizierungsstellenzertifikate
- Zertifikatbeantragung
- Zertifikaterneuerung

Exchange und Zertifikate

- Get-exchangecertificate
- https://www.digicert.com/easy-csr/exchange2007.htm
- New-ExchangeCertificate -GenerateRequest -Path c:\certificates\request.req -SubjectName "c=DE, o=IT-TRAINING-GROTE.DE, cn=Hyper. it-training-grote.de" -DomainName it-training-grote.de, autodiscover.it-training-grote.de, hyper, hyper.test.intern, autodiscover.test.intern -PrivateKeyExportable $true
- get-exchangecertificate -Thumbprint "Thumbprint" | fl
- Import-ExchangeCertificate –Path c:\certnew.cer
- Certificate aktivieren
- Enable-ExchangeCertificate –Thumbprint <thumbprint> -Services “IIS, POP, IMAP, SMTP"

Exchange und Zertifikate

- IIS Konfiguration
- Get-exchangecertificate | new-exchangecertificate
- New-Exchangecertificate
- Enable-exchangecertificate
- Export-exchangecertificate –Thumbprint 4711ABC –Password Geheim –Path cert-pfx
- Import-Exchangecertificate
- Remove-Exchangecertificate -Thumbprint

WLAN

- Kurzer Ueberblick ueber WLAN Standards
- 802.1x Planung und Implementierung
- 802.1x User Certificates - Deployment
- Was muss alles konfiguriert werden ? (DC, Client, WLAN Komponenten)
- Best Practices

WLAN Infrastruktur

- WLAN Access Point 802.1x RADIUS
  - WPA2 Enterprise
- NPS Server
  - RADIUS Client
  - Connection Request Policy
  - Network Policy – EAP Smartcard/Zertifikat
- Group Policy zur zentralen Steuerung
- Computer Zertifikat auf Client
  - Certificate Autoenrollment

Das Ende


IT TRAINING GROTE
IT Consultant & IT Trainer
Marc Grote
Suelbeckerbrand 22
31688 Nienstaedt
Mobil: 0176 / 233 802 79
E-Mail: Grotem@IT-Training-Grote.de
Web: HTTP://www.it-training-grote.de