

# Zertifikate

## Exchange Server / WLAN

Referent: Marc Grote

# Agenda

- Verwendungszweck von Zertifikaten
- Kryptografiegrundlagen
- Symmetrische / Asymmetrische Verschlüsselungsverfahren
- 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

# Kryptografiegrundlagen

- Signatur
- Verschlüsselung
- Signatur und Verschlüsselung
- Authentizität
- Integrität

# Symmetrische / Asymmetrische Verschlüsselung

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.

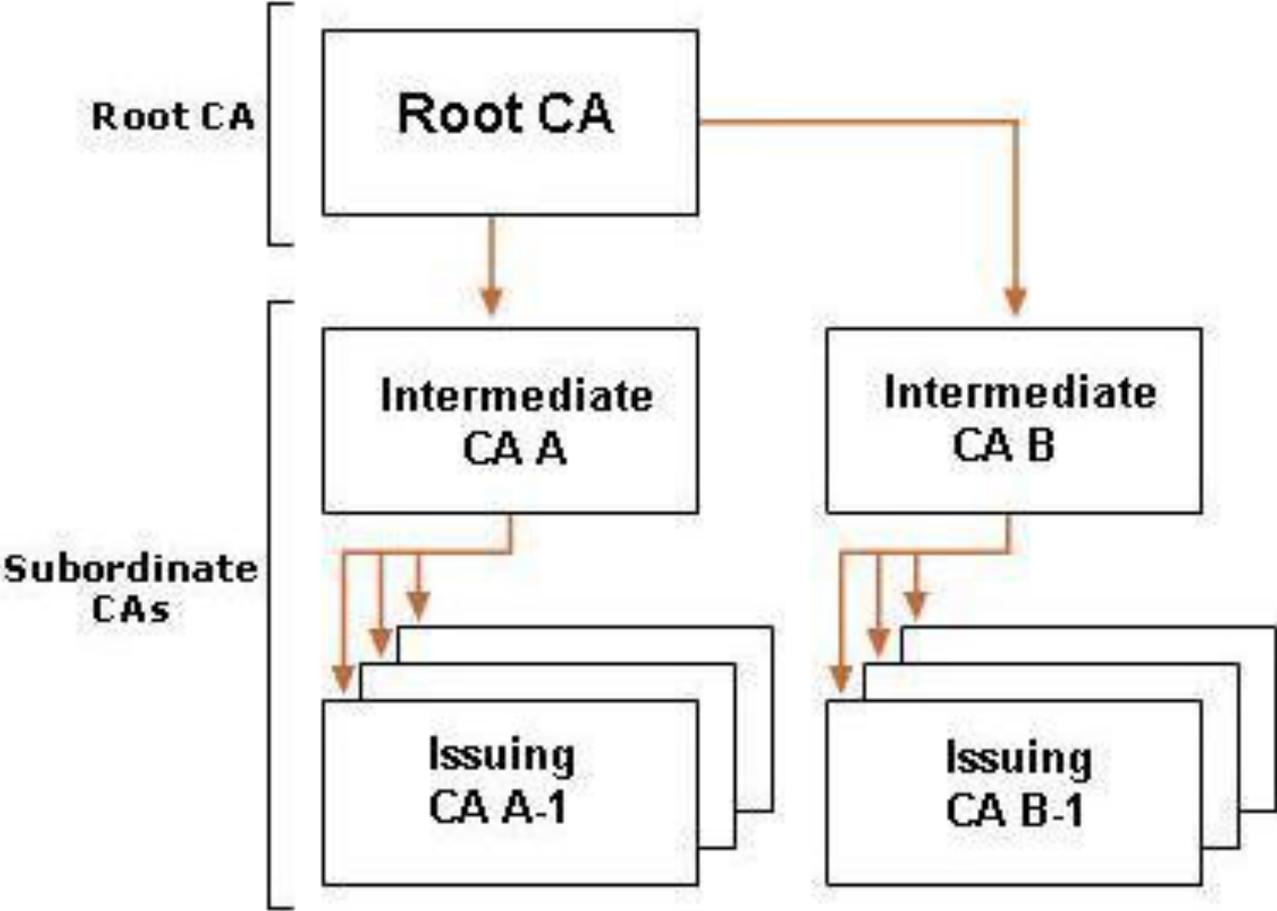
## Validierungsdienst:

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

**Zertifikatvorlagenkonsole**

Datei Aktion Ansicht ?

Zertifikatvorlagen (C:\Programme\Microsoft...)

Vorlagenzeigename	Unterstützte Zertifizierungsstellen (Min.)	Version	Beabsichtigte Zwecke
Administrator	Windows 2000	4.1	
Arbeitsstationsauthentifizierung	Windows Server 2003 Enterprise	101.0	Clientauthentifizierung
Authentifizierte Sitzung	Windows 2000	3.1	
Basis-EFS	Wind		
Benutzer	Wind		
Benutzer-Schlüsselarchivierung	Wind		
CEP-Verschlüsselung	Wind		
Codesignatur	Wind		
Computer	Wind		
ComputerPRIVKEY	Wind		
Domänencontroller	Wind		
Domänencontrollerauthentifizierung	Wind		
EF5-Wiederherstellungs-Agent	Wind		
Exchange-Benutzer	Wind		
Exchange-Registrierungs-Agent (Offlineanforderung)	Wind		
IPSec	Wind		
IPSec (Offlineanforderung)	Wind		
IPSec-Offline-PRIVKEY	Wind		
Kerberos-Authentifizierung	Wind		
Kreuzzertifizierungsstelle	Wind		
Nur Benutzersignatur	Wind		
Nur Exchange-Signatur	Wind		
OCSP-Antwortsignatur	Wind		
RAS- und IAS-Server	Wind		
Registrierungs-Agent	Wind		
Registrierungs-Agent (Computer)	Wind		
Router (Offlineanforderung)	Wind		
SCCM	Wind		
Schlüsselwiederherstellungs-Agent	Wind		
Smartcard-Anmeldung	Wind		
Smartcard-Benutzer	Wind		
Smartcard-...	Wind		
Stammzertifizierungsstelle	Wind		
Untergeordnete Zertifizierungsstelle	Wind		
Vertrauenslistensignatur	Wind		
Verzeichnis-E-Mail-Replikation	Wind		
Webserver	Wind		
Webserver PRIVKEY	Wind		
Zertifizierungsstellenaustausch	Wind		

Active Directory-Standorte und -Dienste

Datei Aktion Ansicht ?

Active Directory-Standorte und -Dienste (S...)

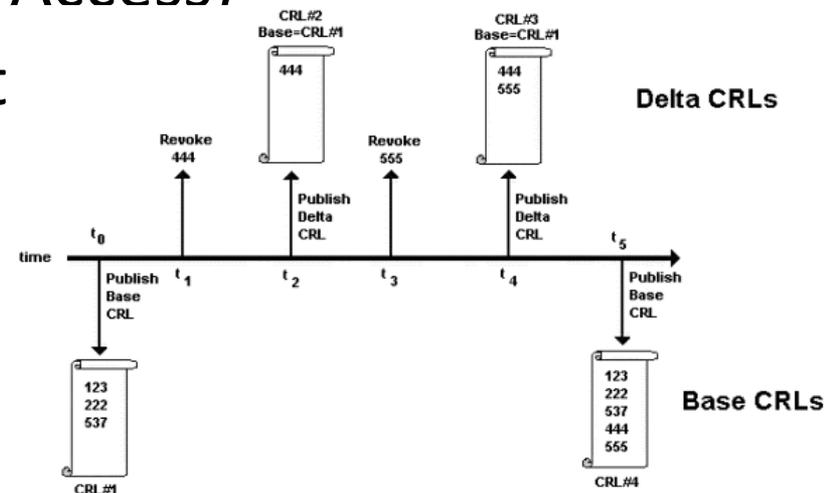
Name	Typ	Beschr
Administrator	Zertifikatsvorlage	
Benutzer-Schlüsselarchivierung	Zertifikatsvorlage	
CA	Zertifikatsvorlage	
CAExchange	Zertifikatsvorlage	
CEPEncryption	Zertifikatsvorlage	
ClientAuth	Zertifikatsvorlage	
CodeSigning	Zertifikatsvorlage	
ComputerPRIVKEY	Zertifikatsvorlage	
CrossCA	Zertifikatsvorlage	
CTLSigning	Zertifikatsvorlage	
DirectoryEmailReplication	Zertifikatsvorlage	
DomainController	Zertifikatsvorlage	
DomainControllerAuthentication	Zertifikatsvorlage	
EF5	Zertifikatsvorlage	
EF5Recovery	Zertifikatsvorlage	
EnrollmentAgent	Zertifikatsvorlage	
EnrollmentAgentOffline	Zertifikatsvorlage	
ExchangeUser	Zertifikatsvorlage	
ExchangeUserSignature	Zertifikatsvorlage	
IPSECIntermediateOffline	Zertifikatsvorlage	
IPSECIntermediateOnline	Zertifikatsvorlage	
IPSec-Offline-PRIVKEY	Zertifikatsvorlage	
KerberosAuthentication	Zertifikatsvorlage	
KeyRecoveryAgent	Zertifikatsvorlage	
Machine	Zertifikatsvorlage	
MachineEnrollmentAgent	Zertifikatsvorlage	
OCSPResponseSigning	Zertifikatsvorlage	
OfflineRouter	Zertifikatsvorlage	
RASAndIASServer	Zertifikatsvorlage	
SCCM	Zertifikatsvorlage	
Smartcard...	Zertifikatsvorlage	
SmartcardLogon	Zertifikatsvorlage	
SmartcardUser	Zertifikatsvorlage	
SubCA	Zertifikatsvorlage	
User	Zertifikatsvorlage	
UserSignature	Zertifikatsvorlage	
WebServer	Zertifikatsvorlage	
WebserverPRIVKEY	Zertifikatsvorlage	
Workstation	Zertifikatsvorlage	

# CA Administration

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

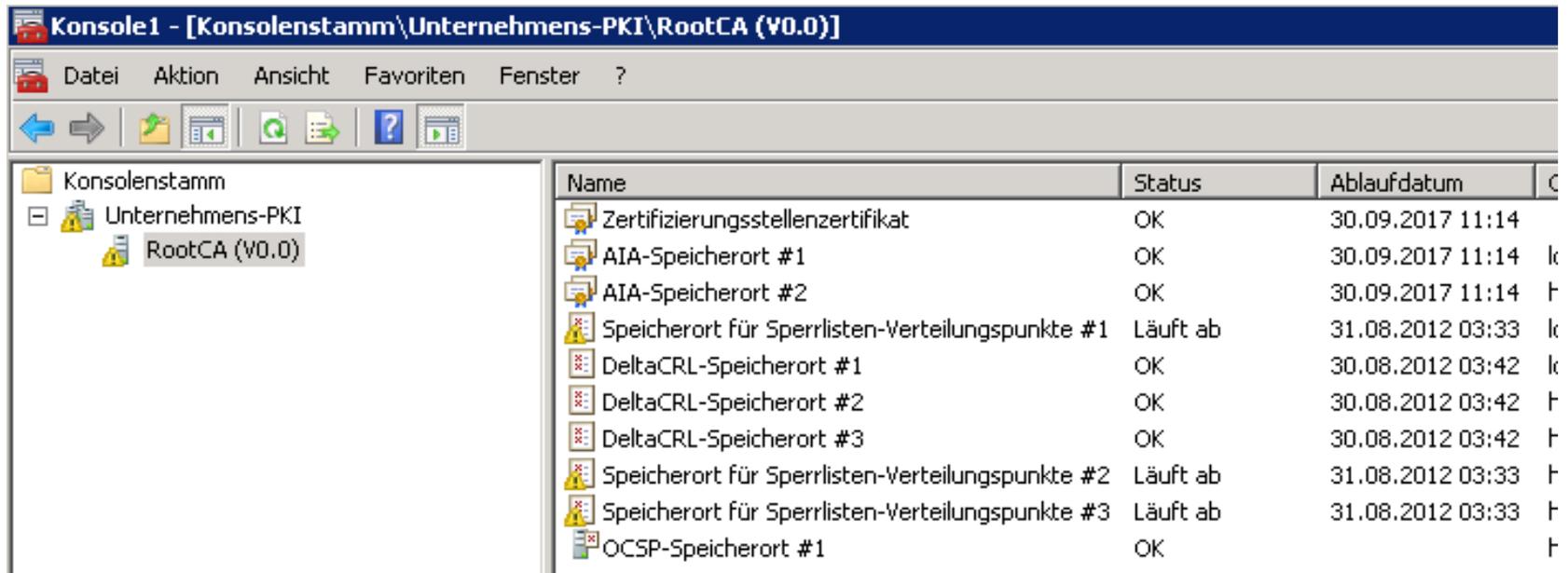
# Sperlistenverwaltung

- 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



Name	Status	Ablaufdatum	
Zertifizierungsstellenzertifikat	OK	30.09.2017 11:14	
AIA-Speicherort #1	OK	30.09.2017 11:14	k
AIA-Speicherort #2	OK	30.09.2017 11:14	f
Speicherort für Sperrlisten-Verteilungspunkte #1	Läuft ab	31.08.2012 03:33	k
DeltaCRL-Speicherort #1	OK	30.08.2012 03:42	k
DeltaCRL-Speicherort #2	OK	30.08.2012 03:42	f
DeltaCRL-Speicherort #3	OK	30.08.2012 03:42	f
Speicherort für Sperrlisten-Verteilungspunkte #2	Läuft ab	31.08.2012 03:33	f
Speicherort für Sperrlisten-Verteilungspunkte #3	Läuft ab	31.08.2012 03:33	f
OCSP-Speicherort #1	OK		f

# Zertifikatbeantragung

- Webschnittstelle
- MMC
- Certutil
- Autoenrollment

# Schlüsselarchivierung / Wiederherstellung

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

