Windows Server 2016 PKI

Marc Grote

Wer bin ich?

- Marc Grote
- Seit 1989 hauptberuflich ITler / Seit 1995 Selbststaendig
- Microsoft MVP fuer Hyper-V 2014, seit 2015 MVP Cloud and Datacenter (MVP Forefront von 2004-2014)
- Microsoft MCT/MCSE Messaging/Security/Server/MCLC /MCITP*/MCTS*/MCSA*/MC*
  MCSE Private Cloud, Productivity, Cloud Platform and Infrastructure, Server Infrastructure, Exchange
  MCS Server Virtualization Hyper-V / System Center/ Azure
  MCITP Virtualization Administrator
- Buchautor und Autor fuer Fachzeitschriften
- Schwerpunkte:
  - Windows Server Clustering/Virtualisierung/PKI
  - System Center SCVMM/SCEP/DPM
  - Exchange Server seit Version 5.0
  - von *.Forefront reden wir nicht mehr ☹

Agenda

- Ueberblick Windows Server 2016 PKI
- Notwendigkeit von Public Key Infrastrukturen
- Grundlagen Kryptografie
- Anwendungen durch PKI
- Neue Features von Windows Server 2016 / Windows 10
- Windows Server 2016 Zertifikatsdienste
- PKI-Design und Implementierung einer Windows Server 2016 CA
- PKI-Administration mit Rollenseparation
- Key Archivierung und Recovery
- Auditing & Troubleshooting
- PKI Migration

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

Wesentliche Bestandteile einer (minimalen) PKI sind:

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.

Fachchinesisch I

Application Constraints
A constraint that limits what purposes a certificate can be used for in a qualified subordination configuration. A presented certificate must contain the required application constraint to be accepted by the partner organization.

Authority Information Access (AIA)
A certificate extension that contains URL locations where the issuing CAs certificate can be retrieved. The AIA extension can contain HTTP, FTP, LDAP or FILE URLs.

Authority Key Identifier (AKI)
A certificate extension used by the certificate chaining engine to determine what certificate was used to sign a presented certificate. The AKI can contain the issuer name and serial number, public key information, or no information at all. By matching the information in a certificates AKI extension to a CA certificates Subject Key Identifier (SKI) extension, a certificate chain can be built.

Fachchinesisch II

CaPolicy.inf
A configuration file stored in the %SystemRoot% folder that defines Configuration settings for CAs when they are installed and when the CAs certificate is renewed.

CRL Distribution Point (CDP)
A certificate extension that indicates where the certificate revocation list for a CA can be retrieved. This extension can contain multiple HTTP, FTP, File, or LDAP URLs for the retrieval of the CRL.

Certificate Trust List (CTL)
A method of restricting certificates chaining to a designated CA for limited time periods or usages. It is used more prevalently in a Windows 2000 network. In a Windows Server 2003 environment, qualified subordination is the preferred method for restricting certificate usage between organizations.

Fachchinesisch III

Certificate Revocation List (CRL)

A digitally signed list issued by a CA that contains a list of certificates issued by the CA that have been revoked. The listing includes the serial number of the certificate, the date that the certificate was revoked, and the revocation Reason Applications can perform CRL checking to determine a presented Certificates revocation status

.

Cross-Certification

The process of issuing subordinate CA certificates for existing CAs that link two root CAs. Cross-Certification Authority Certificate A certificate issued by one CA for another CA's signing key pair (that is, for another CA's public verification key).

Issuance Policy

Constraint A constraint that defines what issuance practices must be followed for certificates to be trusted by your organization. Issuance policy object identifiers (OIDs) in your organization are mapped to the matching object identifiers in a partner organization, so that object identifiers in presented certificates are recognized by your PKI.

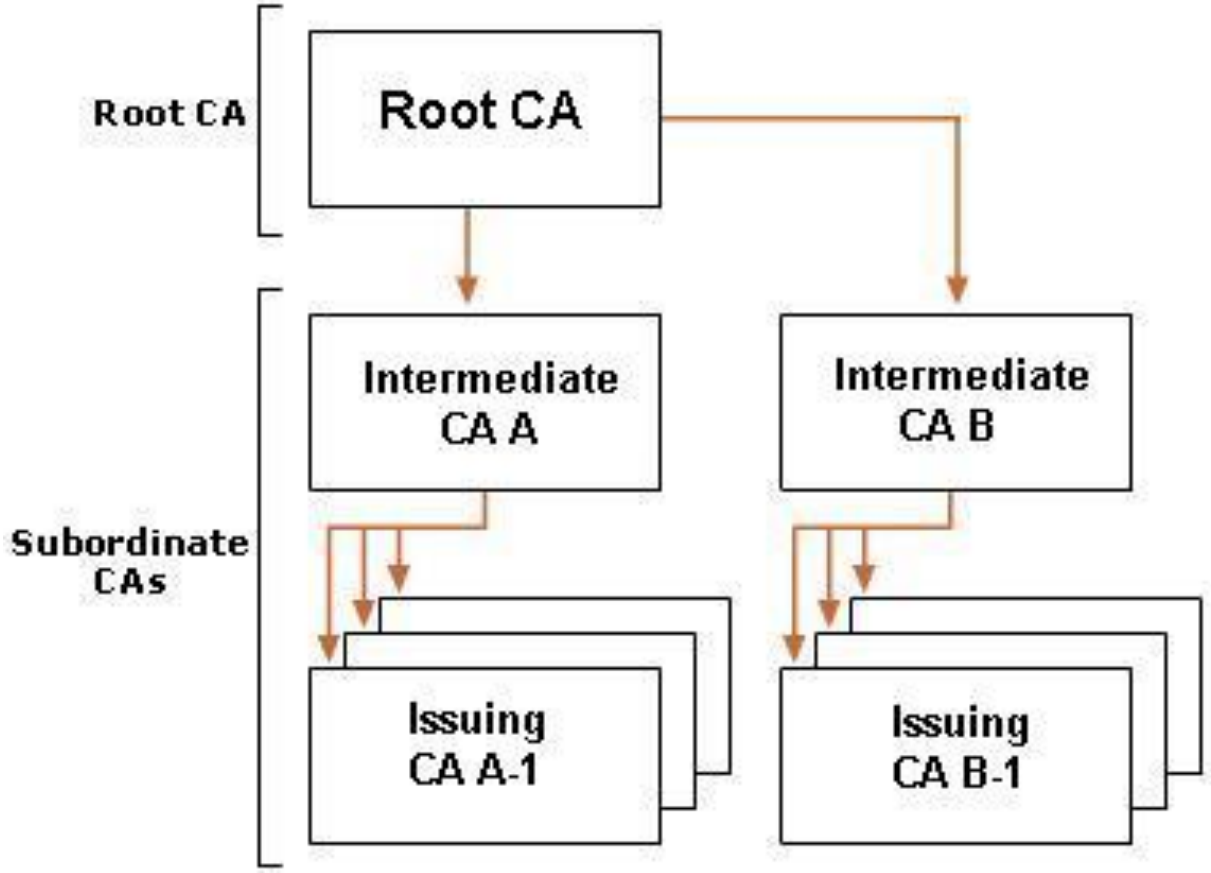
Fachchinesisch IV

Policy.inf
A configuration file that defines the constraints that are applied to a CA certificate when qualified subordination is defined.

Public Key Infrastructure (PKI)
A PKI provides an organization with the ability to securely exchange data over a public network using public-key cryptography. A PKI consists of CAs that issue digital certificates, directories that store the certificates (including Active Directory in Windows 2000 and Windows Server 2003), and X.509 certificates that are issued to security entities on the network. The PKI provides validation of certificate-based credentials and ensures that the credentials are not revoked, corrupted, or modified.

Qualified Subordination
The process of configuring cross-certification with basic constraints, name constraints, application constraints, and issuance policy constraints to govern what certificates are trusted from a partner organization.

CA-Hierarchien



Demo

Windows 2016 PKI

- Alle Basisfunktionen einer Windows PKI seit 2000
- Schluessel Archivierung und -Wiederherstellung
- v2-v4 Certificate Templates
- Role Separation (ISIS-MTT / Common PKI)
- OCSP
- TPM Key Attestation

Einsatzgebiete

- Smartcards
- X.509 Zertifikate
- Kerberos
- Token basierende Authentifizierungsmechanismen
- IPSec
- PPTP
- L2TP/IPSec
- SSL
- TLS
- EFS
- Code Signierung
- Cloud

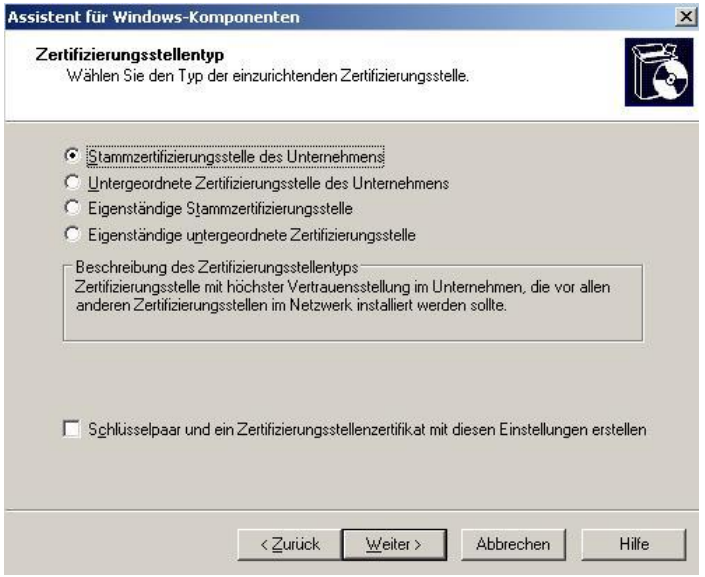
Zertifikate

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

Demo

Windows 2016 CA-Arten

- Stammzertifizierungsstelle des Unternehmens
- Untergeordnete Zertifizierungsstelle des Unternehmens
- Eigenstaendige Stammzertifizierungsstelle
- Eigenstaendige untergeordnete Zertifizierungsstelle



PKI-Design und Implementierung einer Windows Server 2016 CA

Demo

Administration

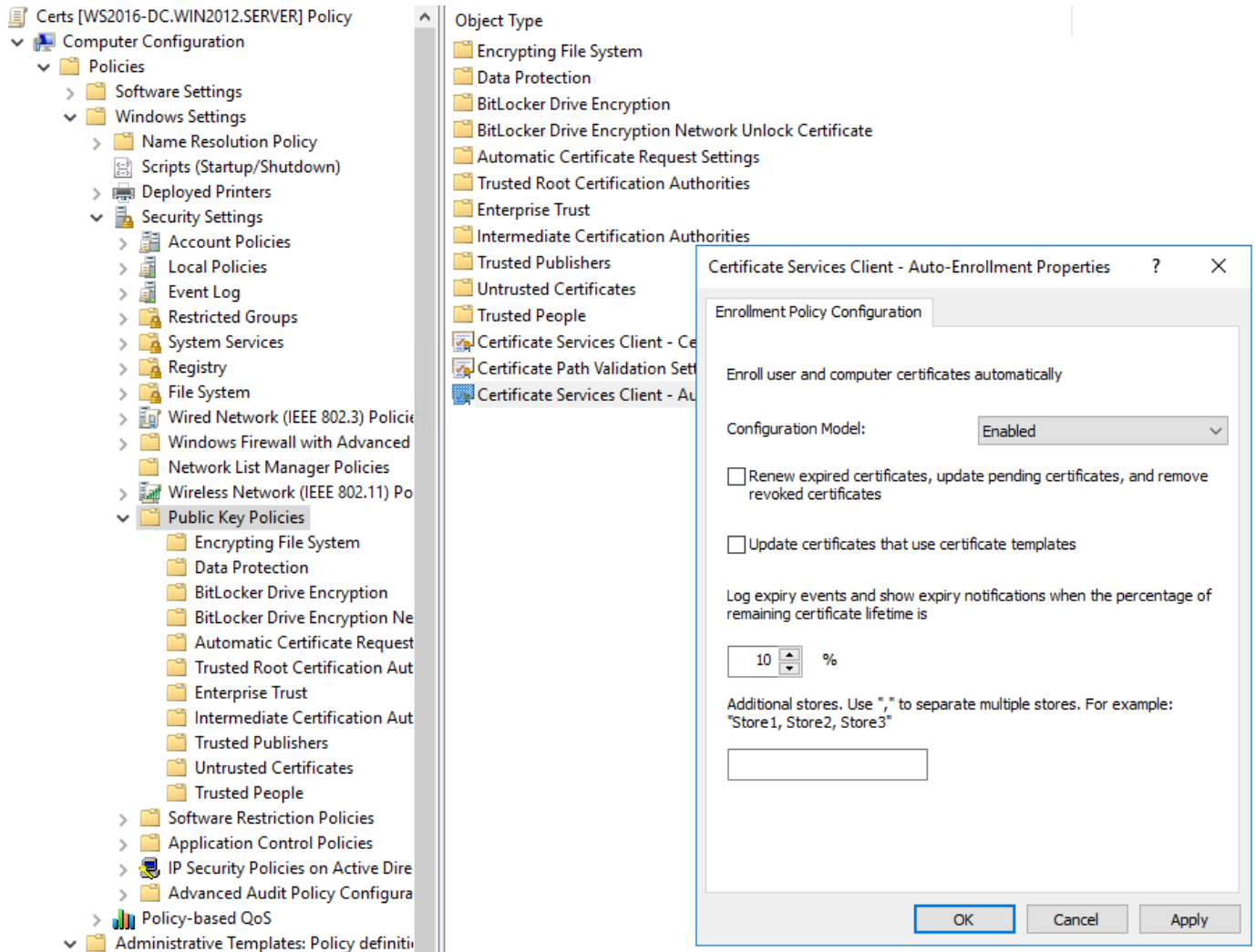
- CA-Konsole
- Certutil /? (viele viele Befehle mit schwarzem Hintergrund)
- Webkonsole (http://caserver/certsrv)
- PKIview.msc (CA Health)
- Policy.inf + CAPolicy.inf
- Powershell Module (Codeplex) https://pspki.codeplex.com/

Demo

Autoenrollment I

- Zertifikate werden automatisch mit Hilfe von Gruppenrichtlinien auf die Clients „ausgerollt“
- Anpassung der Zertifikatsvorlagen + Berechtigungen + GPO Einstellung
- Windows Server 2016 CA
  - Computer und Benutzer

Autoenrollment II



Schluessel Archivierung und -Wiederherstellung

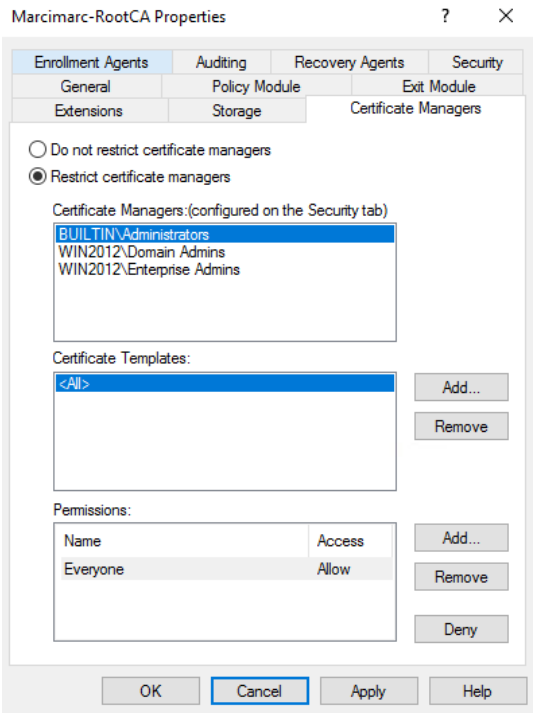
- CA muss für Schluessel Archivierung aktiviert werden
- KRA – Key Recovery Agent Certificate muss ausgerollt werden
- 4-Augen Prinzip moeglich
- Zertifikatsvorlagen muessen für Schluessel Archivierung eingerichtet sein
- Recovery mit CERTUTIL.EXE

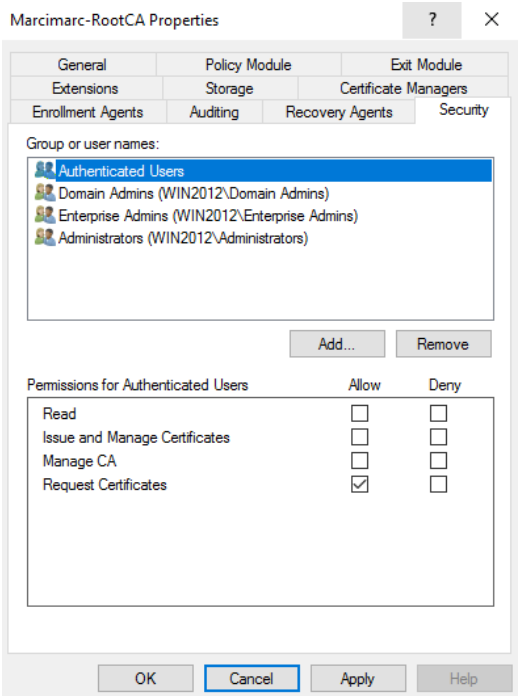
Schluessel Archivierung und -Wiederherstellung

- Key Recovery Agent Template an CA bereitstellen
- Erstellen eines Zertifikat fuer den Recovery Benutzer
- Anmelden als Recovery Benutzer
- Zertifikat fuer KRA anfordern
- CA Eigenschaften - Registerkarte Wiederherstellungs-Agents
- Schluesselarchivierung aktivieren
- Zertifikatvorlage duplizieren - Schluesselarchivierung aktivieren
- Zertifikat fuer Benutzer ausstellen
- Liste der ausgestellten Zertifikate um die Schluesselarchivierung erweitern
- Ausgestellte Zertifikate Seriennummer notieren (Clipboard)
- Certutil -getkey <serialnumber> outputblob
- dir outputblob
- Certutil -recoverkey outputblob <filename>.pfx
- Zertifikat importieren mit .PFX

Demo

Role Separation





Common PKI:

http://support.microsoft.com/default.aspx?scid=kb;en-us;890772

```
C:\Documents and Settings\Administrator>certutil -setreg ca\setroleseparartionenabled 1
SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Northwind Traders CA\setroleseparartionen

New Value:
  setroleseparartionenabled REG_DWORD = 1
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.

C:\Documents and Settings\Administrator>
```

PKI Backup und Recovery

- Systemstate (moeglich)
- CA Backup ueber GUI oder Certutil.exe
- Datenbank/Logfiles / CA Zertifikat und Private Key werden gesichert
- Backup Registry (HKLM\System\CCS\Services\CertSvc)
- Wiederherstellung auf der gleichen oder einer anderen Maschine

PKI Migration

- Migration auf einen anderen Server mit gleichem Namen
- Migration auf einen anderen Server mit anderem Namen
- Migration der CA von SHA1 auf SHA2
  - Wenn OS aktuell ist mit einem Befehl (https://blogs.technet.microsoft.com/pki/2013/09/19/upgrade-certification-authority-to-sha256/) sonst …
  - https://blogs.technet.microsoft.com/askds/2015/10/26/sha1-key-migration-to-sha256-for-a-two-tier-pki-hierarchy/


Fragen?

Kontakt

- **Marc Grote**

- E-Mail: marc.grote@it-consulting-grote.de
- Web: http://www.it-consulting-grote.de
- Blog: http://blog.it-consulting-grote.de
- XING: https://www.xing.com/profile/Marc_Grote2
- Mobile: +4917623380279