

# Windows Server 2016 Public Key Infrastrukturen

# Wer bin ich?

- Marc Grote
- Seit 1989 hauptberuflich ITler / Seit 1995 Selbststaendig
- MVP Forefront (2004-2014), MVP Hyper-V (2014), MVP Cloud and Datacenter (2015-2017), 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 VMM/SCEP/DPM
  - Exchange Server seit Version 5.0
  - von \*.Forefront reden wir nicht mehr ☹

# Agenda

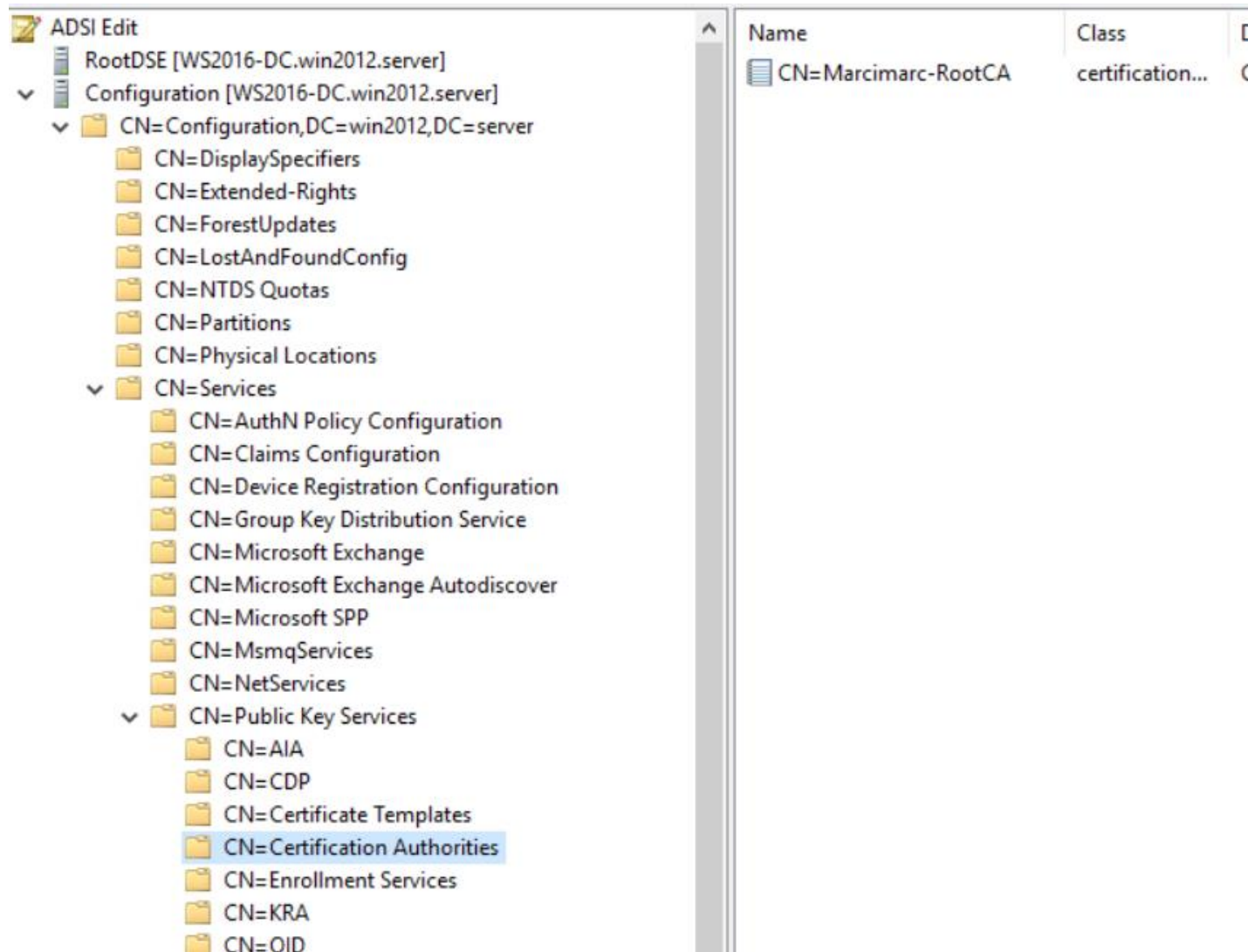
- Ueberblick ueber Public Key Infrastrukturen (PKI)
- Windows Server 2016 Zertifikatsdienste
- CA-Administration mit Rollentrennung
- CA-Hardening
- Schluesselarchivierung und -Wiederherstellung
- CA Backup und Migration

# 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>

# Verwendet Ihr eine Windows PKI?



ADSI Edit

- RootDSE [WS2016-DC.win2012.server]
- Configuration [WS2016-DC.win2012.server]
  - CN= Configuration,DC=win2012,DC=server
    - CN=DisplaySpecifiers
    - CN=Extended-Rights
    - CN=ForestUpdates
    - CN=LostAndFoundConfig
    - CN=NTDS Quotas
    - CN=Partitions
    - CN=Physical Locations
    - CN=Services
      - CN=AuthN Policy Configuration
      - CN=Claims Configuration
      - CN=Device Registration Configuration
      - CN=Group Key Distribution Service
      - CN=Microsoft Exchange
      - CN=Microsoft Exchange Autodiscover
      - CN=Microsoft SPP
      - CN=MsmqServices
      - CN=NetServices
      - CN=Public Key Services
        - CN=AIA
        - CN=CDP
        - CN=Certificate Templates
        - CN=Certification Authorities
        - CN=Enrollment Services
        - CN=KRA
        - CN=OID

Name	Class	ID
CN=Marcimarc-RootCA	certification...	C

# 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 uebernimmt.

## Registration Authority:

Organisation, bei der Zertifikate beantragt werden koennen.

## Certificate Revocation Lists:

Listen (Sperrlisten) mit zurueckgezogenen, abgelaufenen und für ungueltig erklarten Zertifikaten.

## Verzeichnisdienst:

Ein durchsuchbares Verzeichnis welches ausgestellte Zertifikate enthaelt

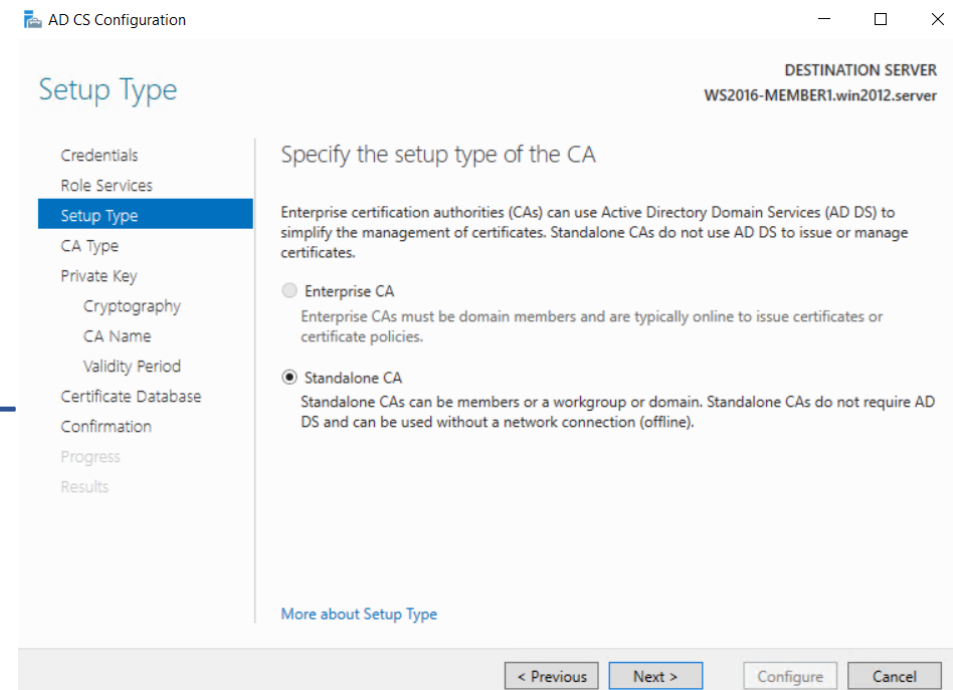
## Validierungsdienst:

Ein Dienst, der die Ueberpruefung von Zertifikaten in Echtzeit ermoeglicht (OCSP)

# Ansehen

# Windows Server 2016 CA- Arten

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





# CA Unterschiede

Standalone CA	Enterprise CA
Erfordert kein AD-DS	Erfordert AD-DS
Erfordert keine Zertifikatvorlagen	Stellt Zertifikate basierend auf Zertifikatvorlagen aus
Zertifikatverteilung ist ein manueller Prozess	User Zertifikate und Sperrlisten koennen in AD-DS veroeffentlicht werden
Alle Zertifikatsbeantragungen muessen manuell genehmigt werden	Zertifikate koennen basierend auf Zertifikatvorlagen und Gruppenrichtlinien automatisch ausgestellt werden

# CA Rollendienste

- Certificate Authority
- Certificate Authority Web Enrollment
- Online Certificate Status Protocol (OCSP)
- Network Device Enrollment Service (NDES)
- Certificate Enrollment Web Service (CEWS)

# CA-Administration/Zugriff

- CA-Konsole / MMC
- Certutil.exe /? (viele Befehle mit schwarzem Hintergrund und weisser Schrift 😊)
- Webkonsole  
(<https://caserver.domain.tld/certsrv>)
- PKIview.msc (CA Health)
- Policy.inf + CAPolicy.inf
- Powershell Module (Codeplex)  
<https://pspki.codeplex.com/>

# Ansehen

# Zertifikats-Vorlagen

Template Version	CA Betriebssystem	Crypto Provider
V1	Windows 2000	Crypto API CSP only
V2	Windows 2003	Crypto API CSP only
V3	Windows 2008 Windows 2008 R2	Nur CNG CSP
V4	Windows 2012 Windows 2012 R2 Windows 2016 Windows 2019	Crypto API CSP oder CNG CSP bei Template Kopie- Erstellung

# Ansehen

# Autoenrollment von Zertifikaten

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

# Sperrung von Zertifikaten

- CRL – Certificate Revocation List
- CDP – Certificate Distribution Point
- OCSP – Online Certificate Status Protocol
- Zertifikatssperrung
- Intern und extern verfügbare CRL
- CRL Cache



# Schlüssel Archivierung und - Wiederherstellung

- CA muss fuer die Schlüssel-Archivierung aktiviert werden
- KRA – Key Recovery Agent Zertifikat muss ausgerollt werden
- 4-Augen Prinzip moeglich
- Zertifikatvorlagen muessen fuer die Schlüssel-Archivierung eingerichtet sein
- Recovery mit CERTUTIL.EXE

# Schlüssel 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
- Schlüsselarchivierung aktivieren
- Zertifikatvorlage duplizieren - Schlüsselarchivierung aktivieren
- Zertifikat fuer Benutzer ausstellen
- Liste der ausgestellten Zertifikate um die Schlüsselarchivierung erweitern
- Ausgestellte Zertifikate Seriennummer notieren (Clipboard)
- Certutil -getkey <serialnumber> outputblob
- dir outputblob
- Certutil -recoverkey outputblob <filename>.pfx
- Zertifikat importieren mit .PFX

# CA Hardening

- CA Rollentrennung
- CA Auditing aktivieren
- Security Event Log Size erhoehen / Archivierung planen
- Einsatz von Bitlocker auf den CA-Maschinen mit TPM / Virtual TPM
- Bei Betrieb der CA auf einem Hypervisor, Zugriffsschutz-Konzepte der Hersteller umsetzen
- Aktivierung und Konfiguration der Windows Firewall
- Ausfuehrung nur fuer den Betrieb notwendiger Anwendungen / Diensten
- Zertifikatsvorlagen-Verwaltung (Berechtigungen, nur notwendige Vorlagen, minimale Schluessellaenge beachten)
- Verwendung von Autoenrollment nur wo notwendig
- Einsatz des Security Configuration Wizard (SCW bis Server 2012 R2)
- Verwendung eines HSM-Moduls
- Sichere Aufbewahrung einer Offline CA

# Ansehen

# CA Sicherung und - Wiederherstellung

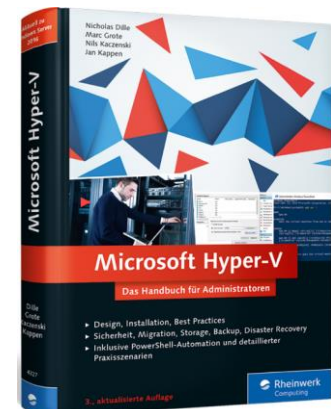
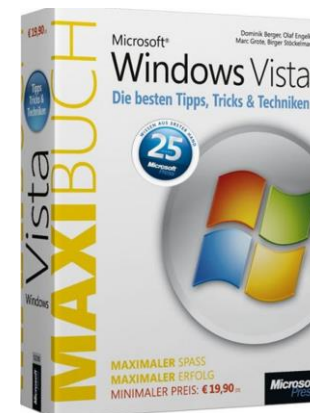
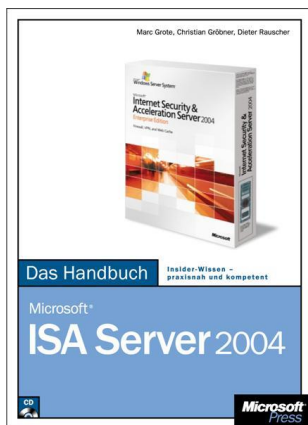
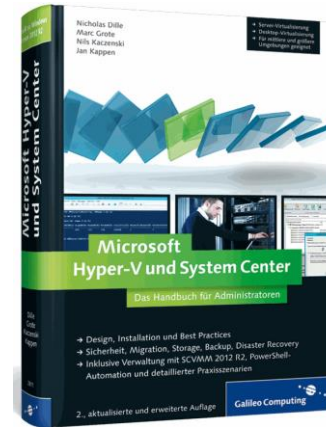
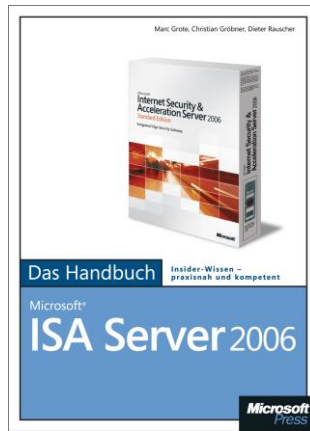
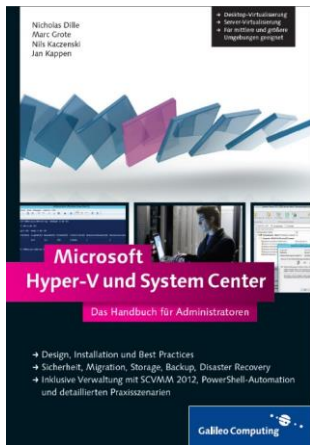
- Systemstate (moeglich)
- CA Sicherung ueber GUI oder Certutil.exe
- Datenbank / Logfiles / CA Zertifikat und Private Key werden gesichert
- Backup Registry  
(HKLM\System\CCS\Services\CertSvc)
- Wiederherstellung auf der gleichen oder einer anderen Maschine

# CA Migration

- Migration auf einen anderen Server mit gleichen Namen
- Migration auf einen anderen Server mit anderen 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?

# Werbung





# Kontakt

- E-Mail: [marc.grote@it-consulting-grote.de](mailto:marc.grote@it-consulting-grote.de)
- Web: <https://www.it-consulting-grote.de>
- Blog: <https://blog.it-consulting-grote.de>
- XING: [https://www.xing.com/profile/Marc\\_Grote2](https://www.xing.com/profile/Marc_Grote2)
- Mobile: +4917623380279