

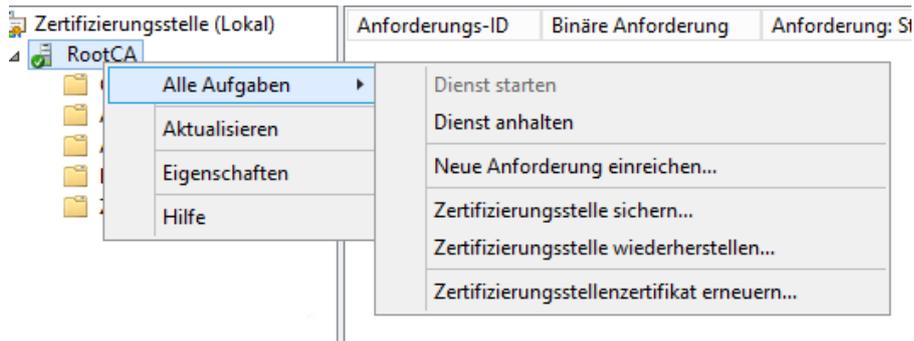
Migration Single Tier Online Enterprise Root CA auf Two Tier Offline Standalone CA mit Online Enterprise Issuing CA mit Windows Server 2012 R2

Bestandsaufnahme IST Zustand

Quellen:

<http://social.technet.microsoft.com/wiki/contents/articles/15037.ad-cs-step-by-step-guide-two-tier-pki-hierarchy-deployment.aspx>

Backup IST CA



Capolicy.inf

CAPOLICY.INF Datei erstellen. Diese wird während des CA Installationsprozesses verwendet

<http://www.it-training-grote.de/download/Issuance-Policies-SubCA.pdf>

```
File Edit Format View Help
[Version]
Signature= "$Windows NT$"
[PolicyStatementExtension]
Policies=InternalPolicy
[InternalPolicy]
OID= 1.2.3.4.1455.67.89.5
Notice="Legal Policy Statement"
URL=http://pk[REDACTED]/cps.txt
[PolicyStatementExtension]
Policies = AllIssuancePolicy
Critical = FALSE
[AllIssuancePolicy]
OID = 2.5.29.32.0
[Certsrv_Server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=20
AlternateSignatureAlgorithm=1
CRLDeltaPeriod=Days
CRLDeltaPeriodUnits=0
```

Speichern in C:\Windows\capolicy.inf

Offline Root implementieren

- Server mit MAK Key installieren weil kein Domain Member
- Administrator Kennwort aendern, um den Zugriff zu beschraenken
- RDP auslassen
- Windows Firewall aktiviert lassen

Eigenstaendige Zertifizierungsstelle

The screenshot shows the 'AD CS-Konfiguration' wizard at the 'Setuptyp' (Setup Type) step. The left sidebar lists various configuration options, with 'Installationstyp' (Installation Type) selected. The main area contains instructions and two radio button options: 'Unternehmenszertifizierungsstelle' (Enterprise Certification Authority) and 'Eigenständige Zertifizierungsstelle' (Standalone Certification Authority). The 'Eigenständige Zertifizierungsstelle' option is selected. At the bottom, there are navigation buttons: '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'.

AD CS-Konfiguration

ZIELSERVER
SR [REDACTED]

Setuptyp

Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse

Geben Sie den Installationstyp der Zertifizierungsstelle an.

Unternehmenszertifizierungsstellen können mithilfe von Active Directory-Domänendienste (Active Directory Domain Services, AD DS) die Verwaltung von Zertifikaten vereinfachen. Eigenständige Zertifizierungsstellen verwenden nicht AD DS, um Zertifikate auszustellen oder zu verwalten.

Unternehmenszertifizierungsstelle
Unternehmenszertifizierungsstellen müssen Domänenmitglieder sein. Sie sind normalerweise online, um Zertifikate oder Zertifikatrichtlinien auszustellen.

Eigenständige Zertifizierungsstelle
Eigenständige Zertifizierungsstellen können einer Arbeitsgruppe oder Domäne angehören. Eigenständige Zertifizierungsstellen erfordern kein AD DS und können ohne Netzwerkverbindung verwendet werden (offline).

[Weitere Informationen zum Setuptyp](#)

< Zurück Weiter > Konfigurieren Abbrechen

Stammzertifizierungsstelle

The screenshot shows the 'AD CS-Konfiguration' wizard at the 'Zertifizierungsstellentyp' (Certification Authority Type) step. The left sidebar lists various configuration options, with 'ZS-Typ' (CA Type) selected. The main area contains instructions and two radio button options: 'Stammzertifizierungsstelle' (Root Certification Authority) and 'Untergeordnete Zertifizierungsstelle' (Subordinate Certification Authority). The 'Stammzertifizierungsstelle' option is selected. At the bottom, there are navigation buttons: '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'.

AD CS-Konfiguration

ZIELSERVER
SR [REDACTED]

Zertifizierungsstellentyp

Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse

Geben Sie den Typ der Zertifizierungsstelle an.

Wenn Sie Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) installieren, erstellen oder erweitern Sie eine Hierarchie der Public Key-Infrastruktur (PKI). Eine Stammzertifizierungsstelle befindet sich am Anfang der PKI-Hierarchie und stellt ein eigenes selbst signiertes Zertifikat aus. Eine untergeordnete Zertifizierungsstelle empfängt ein Zertifikat von der Zertifizierungsstelle, die in der PKI-Hierarchie darüber angesiedelt ist.

Stammzertifizierungsstelle
Stammzertifizierungsstellen sind die ersten und möglicherweise einzigen Zertifizierungsstellen, die in einer PKI-Hierarchie konfiguriert werden.

Untergeordnete Zertifizierungsstelle
Für untergeordnete Zertifizierungsstellen ist eine eingerichtete PKI-Hierarchie erforderlich. Sie sind zur Ausstellung von Zertifikaten berechtigt, die von der Zertifizierungsstelle stammen, die sich in der Hierarchie über den untergeordneten Zertifizierungsstellen befindet.

[Weitere Informationen zum Typ der Zertifizierungsstelle](#)

< Zurück Weiter > Konfigurieren Abbrechen

Neuen privaten Schlüssel erstellen

AD CS-Konfiguration ZIELSERVER

Kryptografie für Zertifizierungsstelle

Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse

Geben Sie die Kryptografieoptionen an.

Kryptografieanbieter auswählen: RSA#Microsoft Software Key Storage Provider Schlüssellänge: 4096

Wählen Sie den Hashalgorithmus aus, mit dem Zertifikate dieser Zertifizierungsstelle signiert werden sollen:

- SHA256
- SHA384
- SHA512
- SHA1

Administratorinteraktion bei jedem Zertifizierungsstellenzugriff auf den privaten Schlüssel zulassen

[Weitere Informationen zur Kryptografie](#)

< Zurück Weiter > Konfigurieren Abbrechen

CA Name

AD CS-Konfiguration ZIELSERVER

Name der Zertifizierungsstelle

Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse

Geben Sie den Namen der Zertifizierungsstelle an.

Geben Sie einen allgemeinen Namen zur Identifizierung der Zertifizierungsstelle an. Dieser Name wird allen von der Zertifizierungsstelle ausgestellten Zertifikaten hinzugefügt. Die Werte für das DN-Suffix werden automatisch generiert, können jedoch geändert werden.

Allgemeiner Name für diese Zertifizierungsstelle:
[Redacted]

Suffix für Distinguished Name:
[Empty]

Vorschau auf Distinguished Name:
CN=Stiftung-RootCA

[Weitere Informationen zum Namen der Zertifizierungsstelle](#)

< Zurück Weiter > Konfigurieren Abbrechen

Gültigkeit

The screenshot shows the 'Gültigkeitsdauer' (Validity) configuration window in the AD CS console. The window title is 'AD CS-Konfiguration' and the server name is 'ZIELSERVER'. The left-hand navigation pane lists various configuration options, with 'Gültigkeitsdauer' selected. The main area contains the following text and controls:

Geben Sie die Gültigkeitsdauer an.

Wählen Sie die Gültigkeitsdauer des Zertifikats aus, das für diese Zertifizierungsstelle generiert wird:

20 Jahre

ZS-Ablaufdatum: 07.04.2034 14:40:00

Der für dieses Zertifizierungsstellenzertifikat konfigurierte Gültigkeitszeitraum sollte den Gültigkeitszeitraum für die Zertifikate überschreiten, die von der Stelle ausgestellt werden.

Weitere Informationen zur Gültigkeitsdauer

Navigation buttons: < Zurück, Weiter >, Konfigurieren, Abbrechen

CA Eigenschaften

The screenshot shows the 'Eigenschaften von' (Properties) dialog for a Certification Authority. The dialog has several tabs: 'Speicherung', 'Zertifikatverwaltungen', 'Registrierungs-Agents', 'Überwachung', 'Wiederherstellungs-Agents', 'Sicherheit', 'Allgemein', 'Richtlinienmodul', 'Beendigungsmodul', and 'Erweiterungen'. The 'Allgemein' tab is selected, showing the following information:

Zertifizierungsstelle

Name: [Redacted] CA

Zertifizierungsstellenzertifikate:

Zertifikat Nr. 0

Zertifikat anzeigen

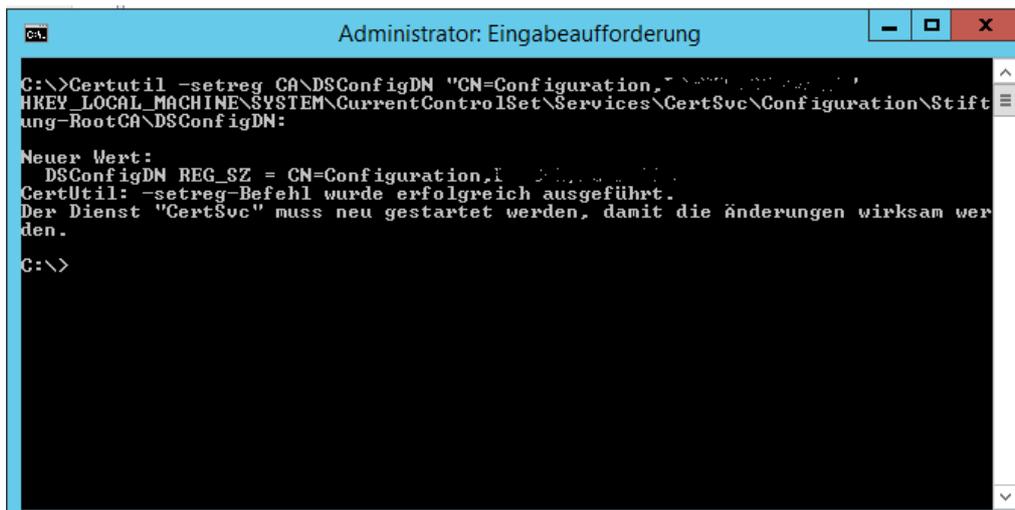
Kryptografieeinstellungen

Anbieter: Microsoft Software Key Storage Provider

Hashalgorithmus: SHA256

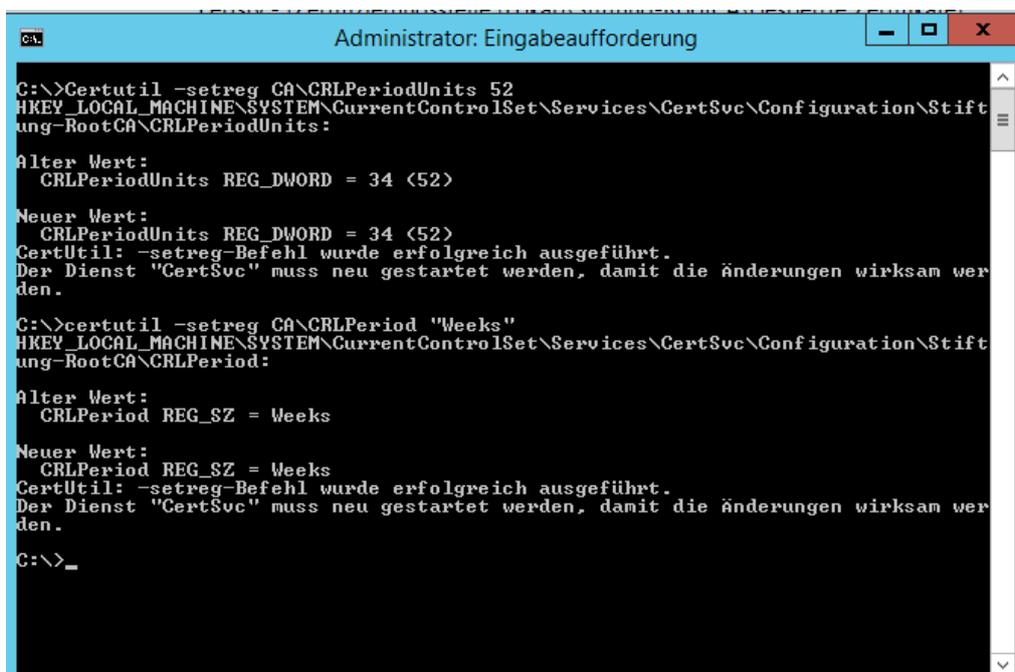
Buttons: OK, Abbrechen, Übernehmen, Hilfe

Der CA den DN zur Konfigurations Partition angeben



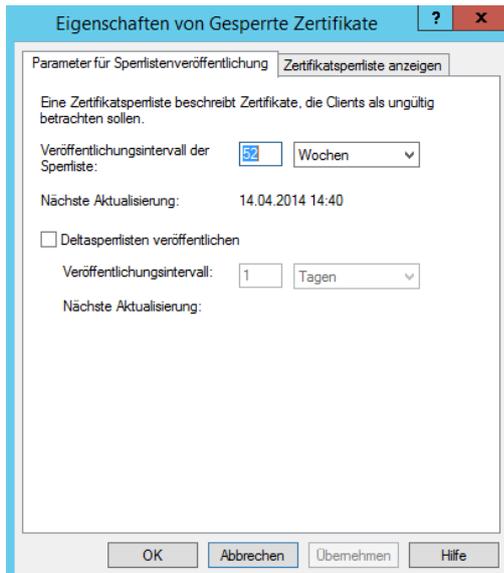
```
C:\>Certutil -setreg CA\DSConfigDN "CN=Configuration,  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Stift  
ung-RootCA\DSConfigDN:  
Neuer Wert:  
DSConfigDN REG_SZ = CN=Configuration,  
CertUtil: -setreg-Befehl wurde erfolgreich ausgeführt.  
Der Dienst "CertSvc" muss neu gestartet werden, damit die Änderungen wirksam wer  
den.  
C:\>
```

CRL Publishing auf 52 Wochen stellen

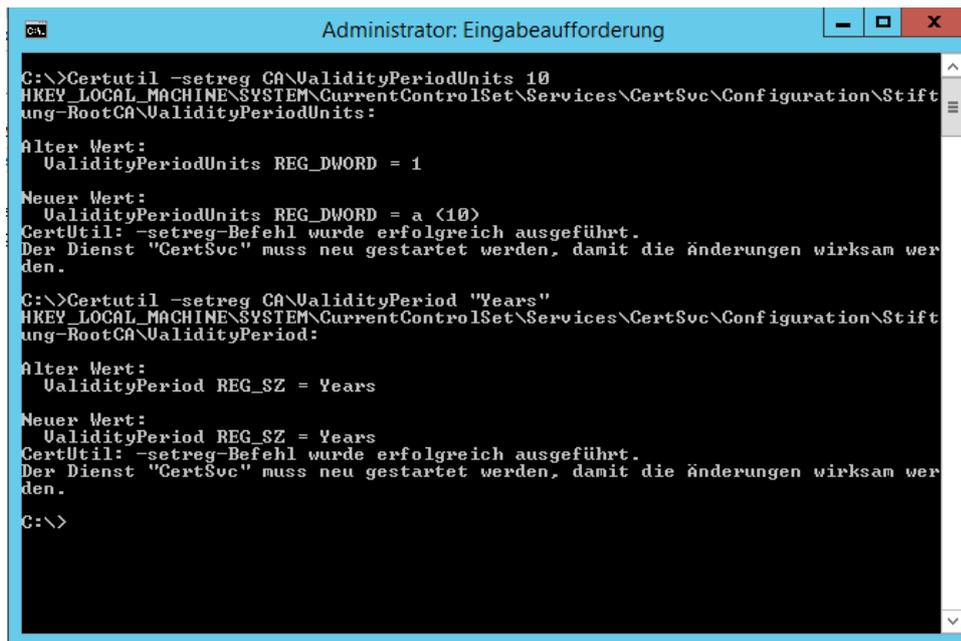


```
C:\>Certutil -setreg CA\CRLPeriodUnits 52  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Stift  
ung-RootCA\CRLPeriodUnits:  
Alter Wert:  
CRLPeriodUnits REG_DWORD = 34 (52)  
Neuer Wert:  
CRLPeriodUnits REG_DWORD = 34 (52)  
CertUtil: -setreg-Befehl wurde erfolgreich ausgeführt.  
Der Dienst "CertSvc" muss neu gestartet werden, damit die Änderungen wirksam wer  
den.  
C:\>certutil -setreg CA\CRLPeriod "Weeks"  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Stift  
ung-RootCA\CRLPeriod:  
Alter Wert:  
CRLPeriod REG_SZ = Weeks  
Neuer Wert:  
CRLPeriod REG_SZ = Weeks  
CertUtil: -setreg-Befehl wurde erfolgreich ausgeführt.  
Der Dienst "CertSvc" muss neu gestartet werden, damit die Änderungen wirksam wer  
den.  
C:\>_
```

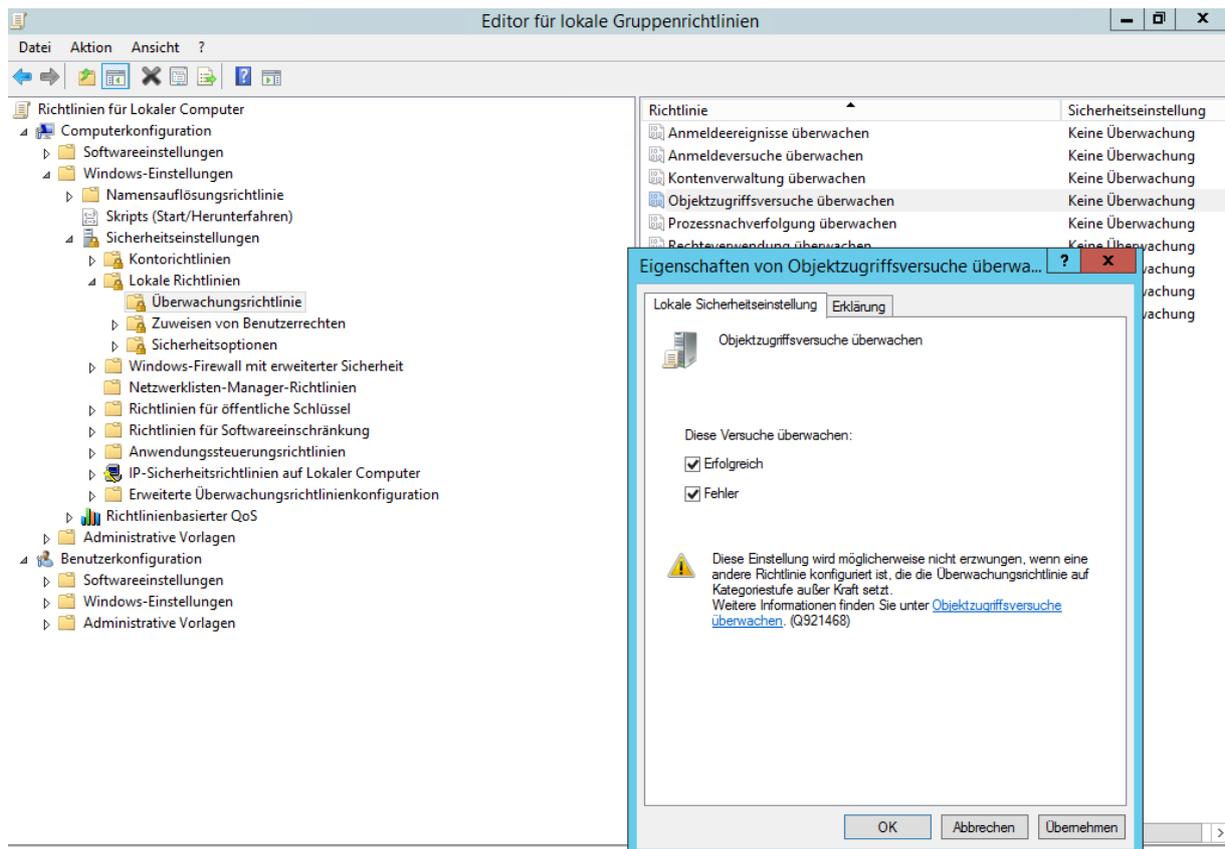
Ueberpruefung



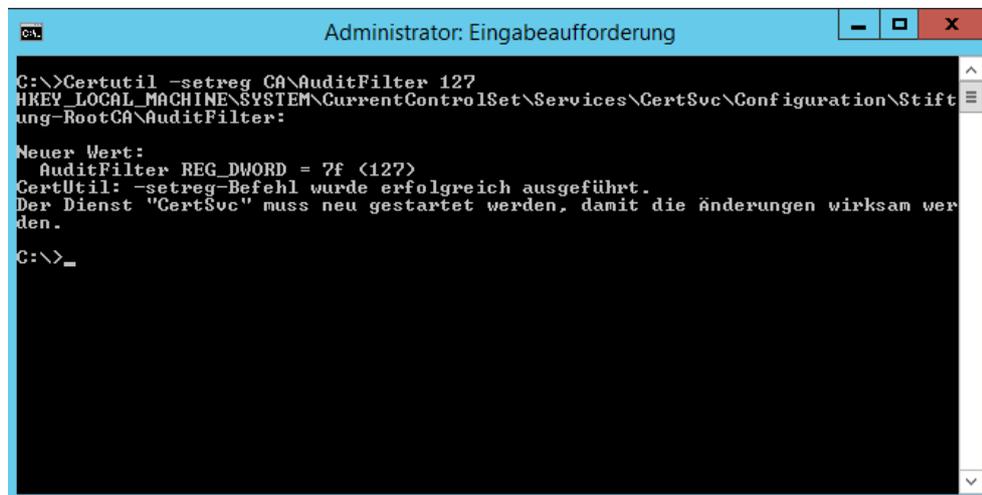
Gueltigkeit des spaeter auszustellenden Zertifikats der Issuing CA auf 10 Jahre stellen



Objektzugriff ueberwachen

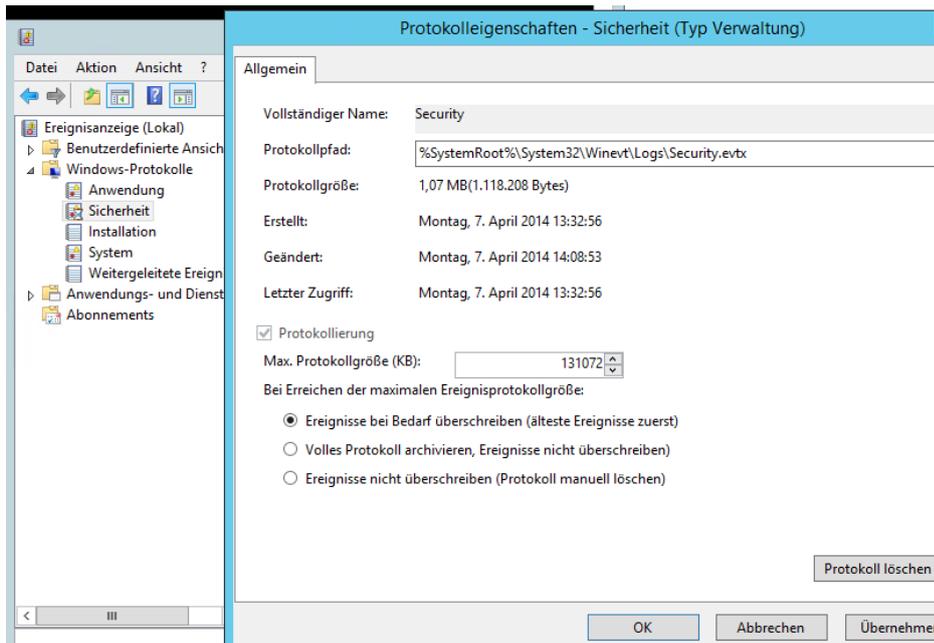


Audit Filtering aktivieren



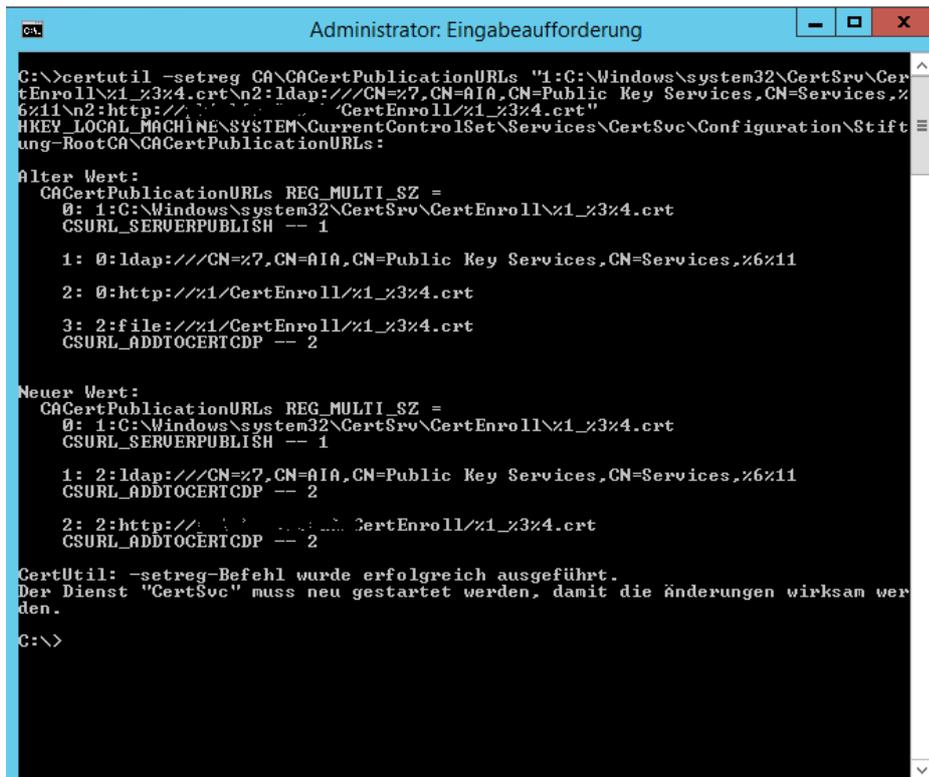
CA Dienst neu starten

Groesse Security Event Log aendern



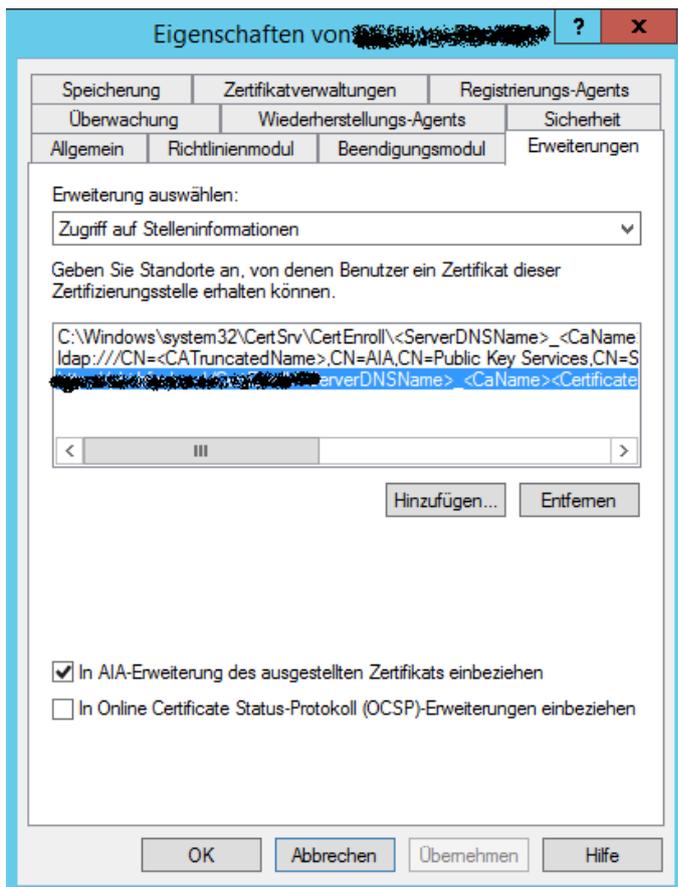
AIA konfigurieren

AIA URL auf Webserver URL setzen (wie in CAPOLICY.INF)



//CN=%7 wird ersetzt durch Angabe des DN zur Active Directory Konfigurations Partition. Vorher angegeben mit Certutil!

Pruefen

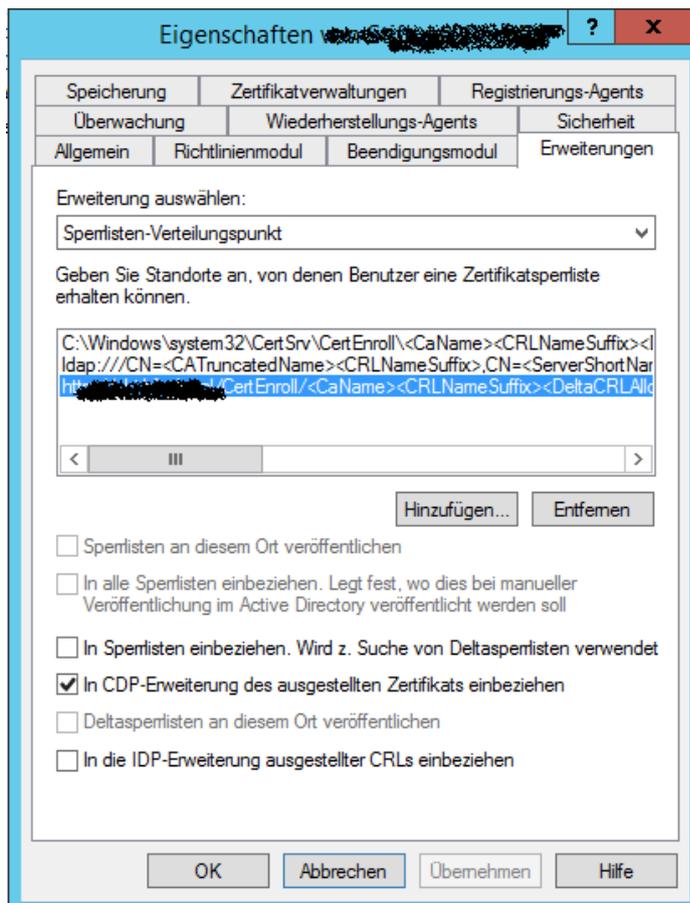


CDP anpassen

```
Administrator: Eingabeaufforderung

C:\>certutil -setreg CA\CRLPublicationURLs "1:C:\Windows\system32\CertSrv\CertEnroll\3%8%9.cr1\n10:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Stiftung-RootCA\CRLPublicationURLs:
Alter Wert:
CRLPublicationURLs REG_MULTI_SZ =
0: 65:C:\Windows\system32\CertSrv\CertEnroll\3%8%9.cr1
CSURL_SERVERPUBLISH -- 1
CSURL_SERVERPUBLISHDELTA -- 40 (64)
1: 8:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
CSURL_ADDTOCRLCDP -- 8
2: 0:http://1/CertEnroll/3%8%9.cr1
3: 6:file://1/CertEnroll/3%8%9.cr1
CSURL_ADDTOCERTCDP -- 2
CSURL_ADDTOFRESHESTCRL -- 4
Neuer Wert:
CRLPublicationURLs REG_MULTI_SZ =
0: 1:C:\Windows\system32\CertSrv\CertEnroll\3%8%9.cr1
CSURL_SERVERPUBLISH -- 1
1: 10:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
CSURL_ADDTOCERTCDP -- 2
CSURL_ADDTOCRLCDP -- 8
2: 2:http://1/CertEnroll/3%8%9.cr1
CSURL_ADDTOCERTCDP -- 2
CertUtil: -setreg-Befehl wurde erfolgreich ausgeführt.
Der Dienst "CertSvc" muss neu gestartet werden, damit die Änderungen wirksam werden.
C:\>
```

Pruefen

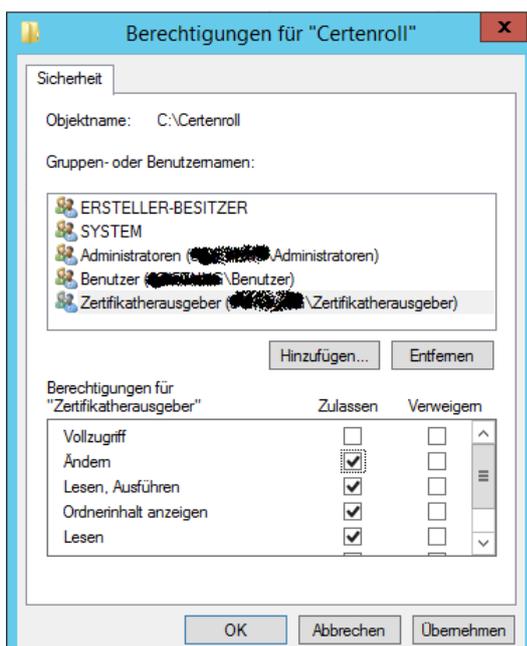


Webserver fuer den CRL Distribution Point erstellen

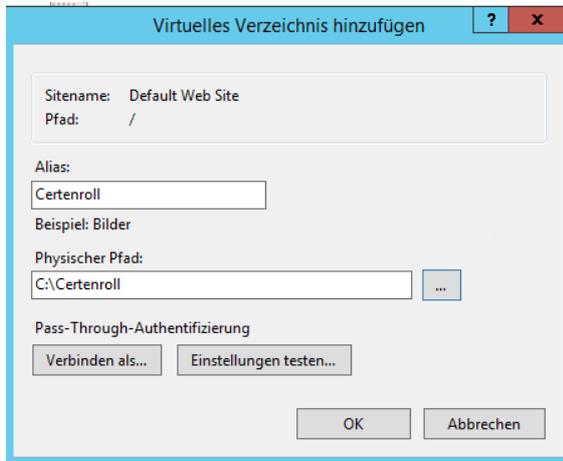
IIS auf dafuer designierten Webserver installieren

Verzeichnis C:\CERTENROLL anlegen

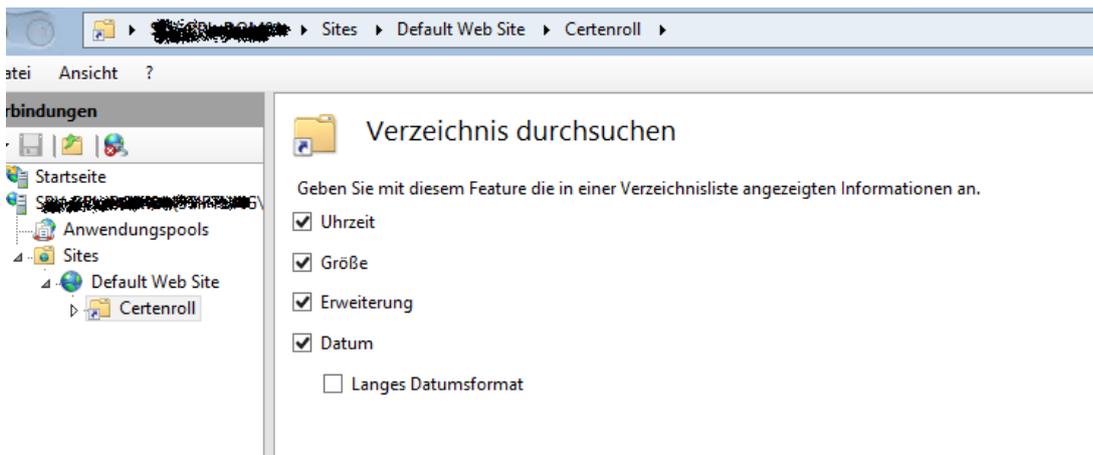
Gruppe Zertifikatherausgeber Modify Permission vergeben



Neues virtuelles Verzeichnis CERTENROLL im IIS anlegen, Verzeichnis durchsuchen erlauben



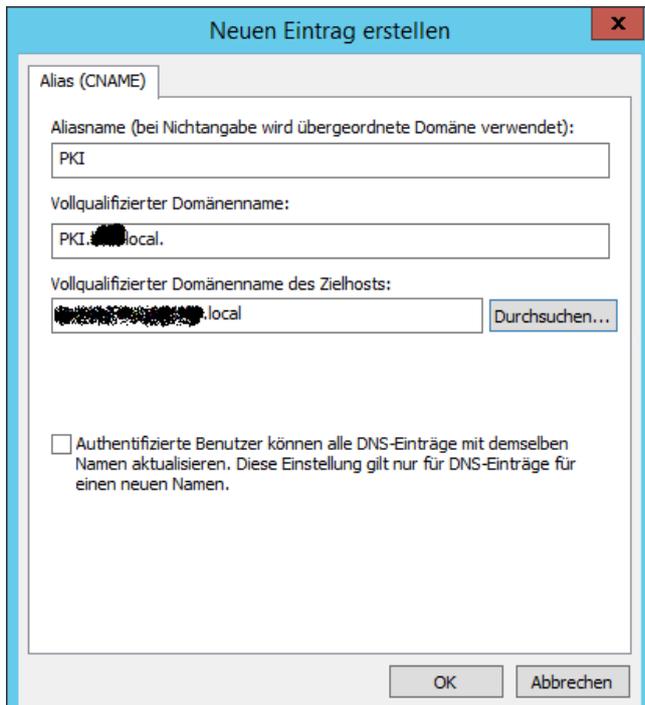
Verzeichnis freigeben mit Modify Berechtigungen fuer die Gruppe Zertifikatherausgeber



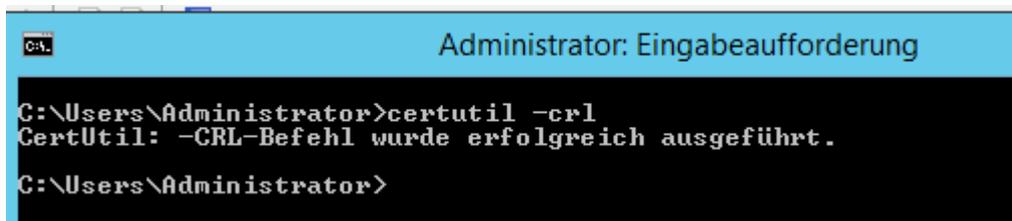
Double Escaping auf IIS Server erlauben



Alias (CNAME) im DNS anlegen mit PKI.XYZ.LOCAL und Verweis auf den Webserver



CRL publishen



```
C:\Users\Administrator>certutil -crl
CertUtil: -CRL-Befehl wurde erfolgreich ausgeführt.
C:\Users\Administrator>
```

CRL Datei auf Webserver kopieren

ACHTUNG: Dieser Prozess muss wie in diesem Beispiel alle 52 Wochen wiederholt werden und dazu die Offline CA eingeschaltet werden

Zu einem späteren Zeitpunkt kann der CRL Download getestet werden, sobald von der neuen PKI Infrastruktur ein Zertifikat verteilt wurde.

CA Cert verteilen

Die .CRT und .CRL Datei der Offline Root CA muss im Active Directory veröffentlicht werden, damit jedes Domänenmitglied das Zertifikat der Offline Root CA in den Zertifikatspeicher der vertrauenswürdigen Stammzertifizierungsstellen kopiert bekommt.

```

Administrator: Eingabeaufforderung

C:\temp>certutil -f -dsPublish "c:\temp\...ng-RootCA.crt" RootCA
ldap:///CN=...-RootCA,CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=...?cACertificate
Zertifikat wurde zum Verzeichnisdienstspeicher hinzugefügt.
ldap:///CN=...-RootCA,CN=CA,CN=Public Key Services,CN=Services,CN=Configuration,DC=...?cACertificate
Zertifikat wurde zum Verzeichnisdienstspeicher hinzugefügt.
CertUtil: -dsPublish-Befehl wurde erfolgreich ausgeführt.
C:\temp>_

```

```

Administrator: Eingabeaufforderung

C:\temp>certutil -f -dsPublish "c:\temp\...-1" ...
ldap:///CN=...-RootCA,CN=...-1,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=...?certificateRevocationList
Basissperrliste wurde zum Verzeichnisdienstspeicher hinzugefügt.
CertUtil: -dsPublish-Befehl wurde erfolgreich ausgeführt.
C:\temp>_

```

Ggfs. per Remote Group Policy Update beschleunigen

The screenshot shows the Group Policy Management console with a tree view on the left and a main pane on the right. A dialog box titled "Gruppenrichtlinienupdate erzwingen" (Force Group Policy Update) is open in the foreground. The dialog contains the following text:

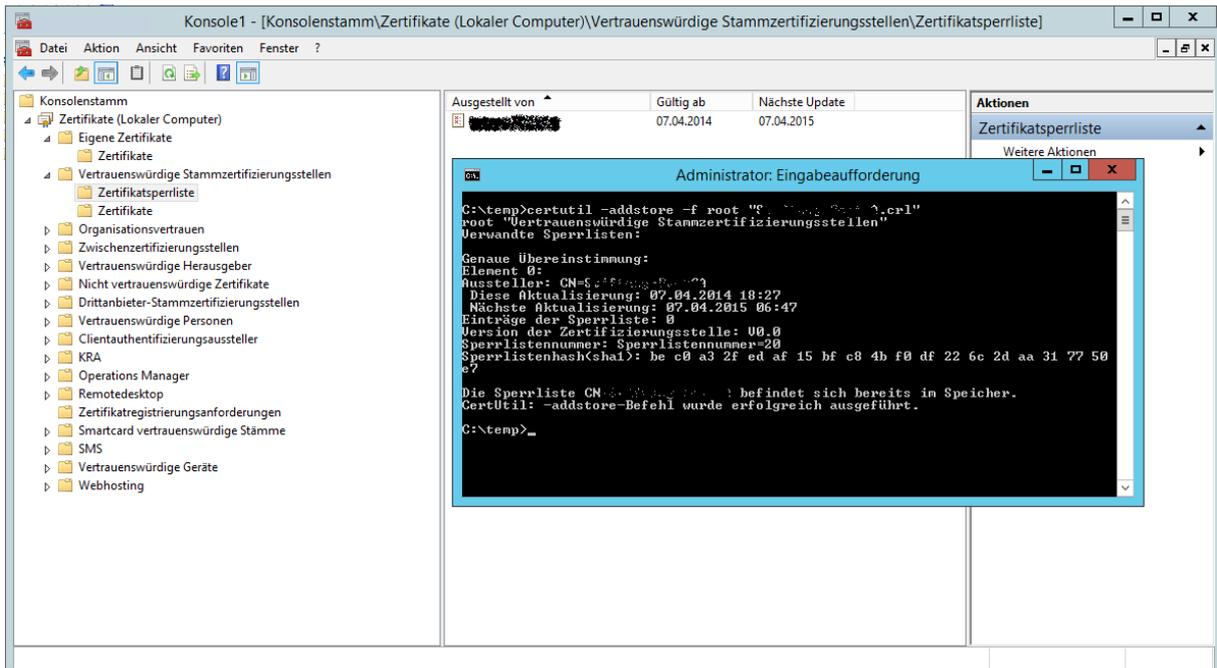
Sie haben angegeben, dass ein Gruppenrichtlinienupdate auf allen Computern in Standort und allen Untercontainern erzwungen werden soll. Wenn sie unten 'Ja' auswählen, werden Benutzer- und Computerrichtlinieneinstellungen aktualisiert in:

1015 Computer

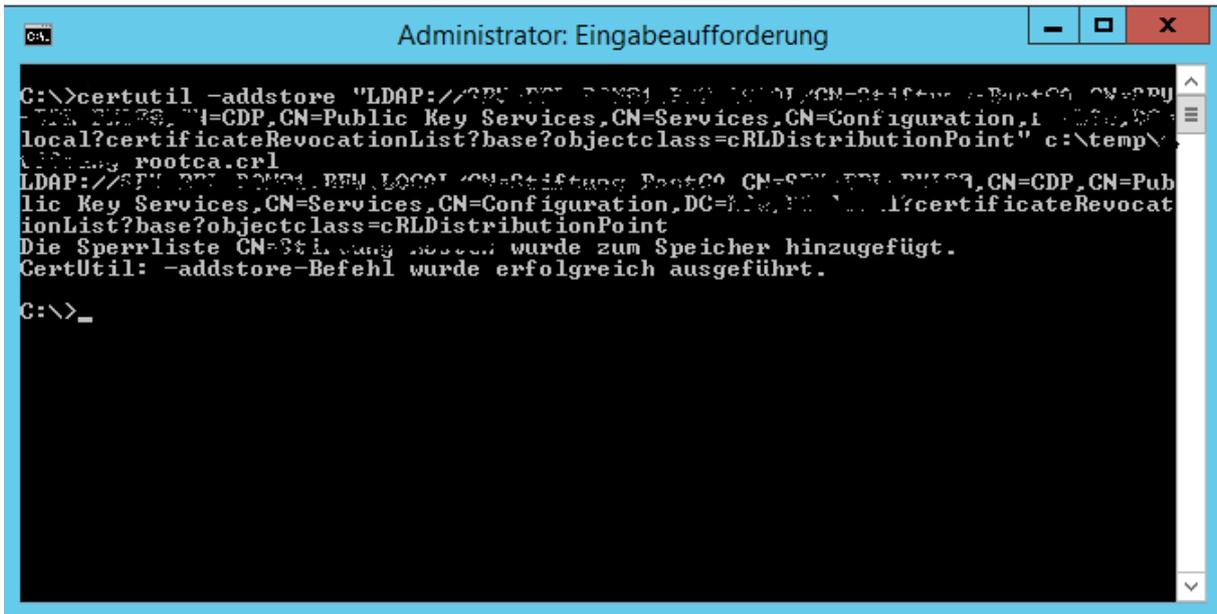
Möchten Sie die Richtlinie für diese Computer wirklich aktualisieren?

Warnung: Durch das Erzwingen des Richtliniupdates auf dieser Anzahl von Computern können Netzwerkressourcen vorübergehend ausgelastet sein.

Buttons: Ja, Nein, Hilfe



LDAP CRL publishen, da die Offline Root CA nicht Domänenmitglied ist, kann der Prozess von einem Domänenmitglied-PC durchgeführt werden

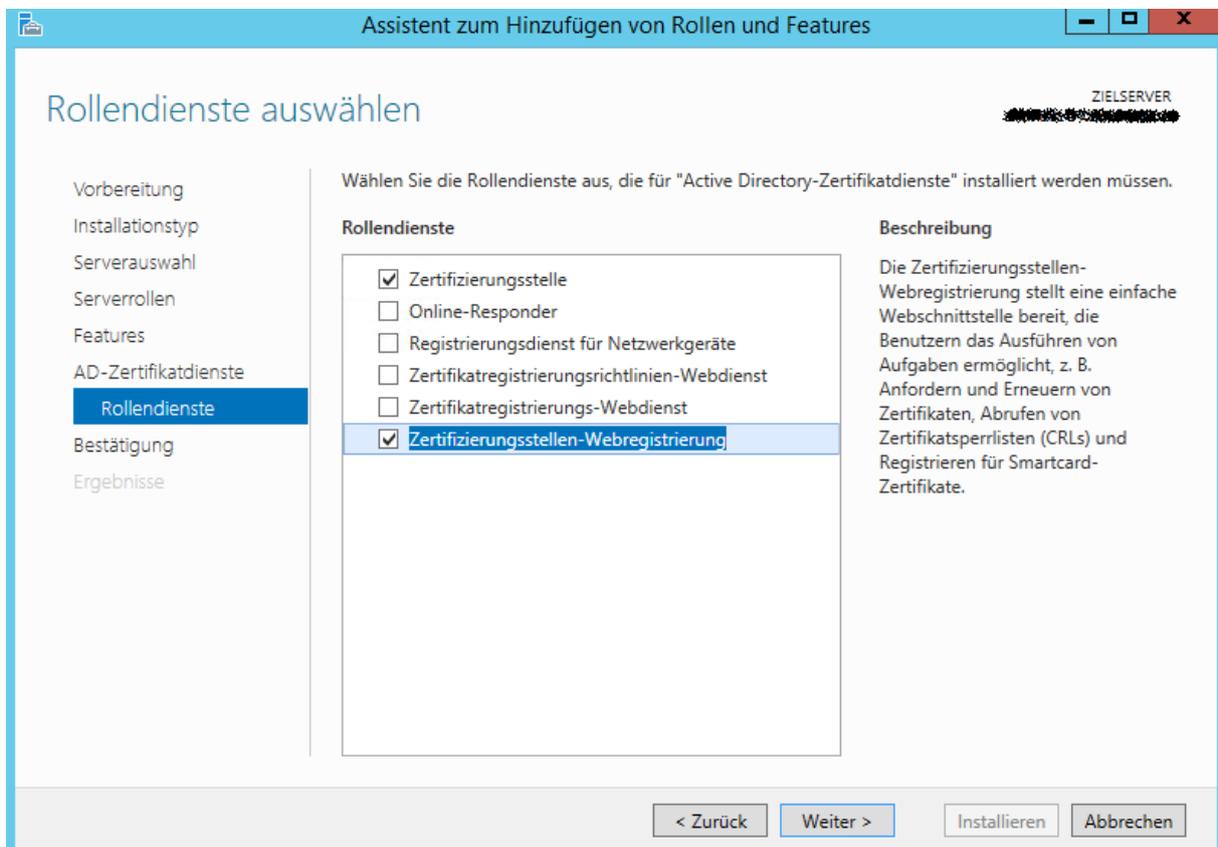


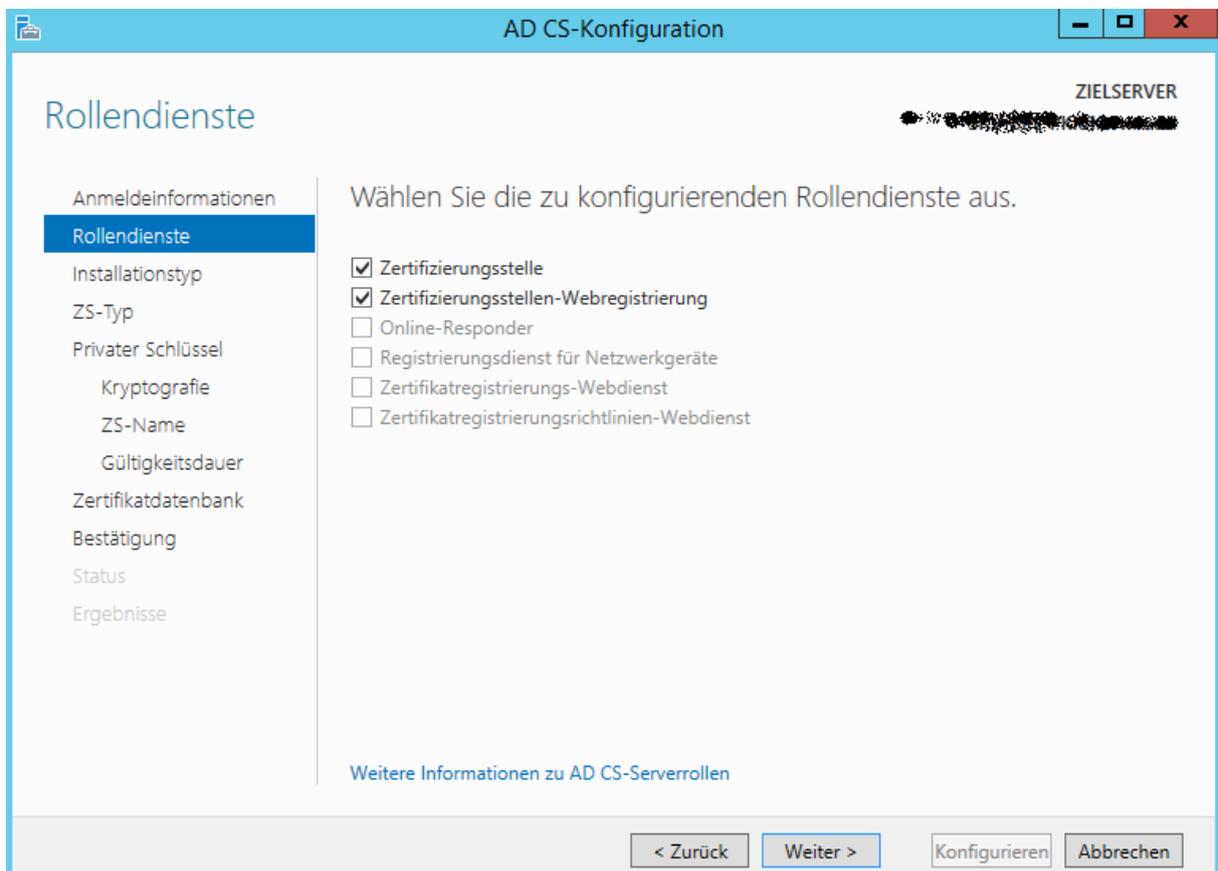
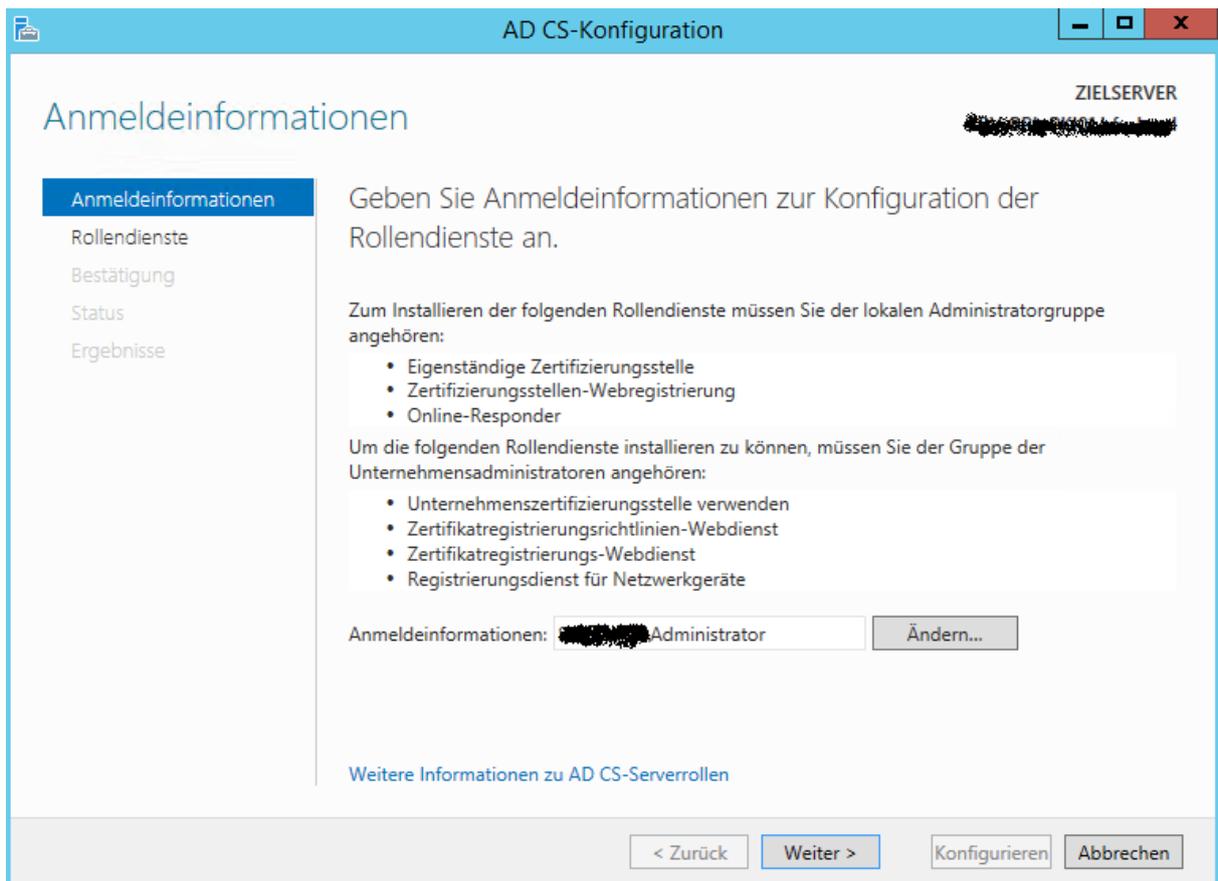
Neue Issuing CA implementieren

CAPolicy.inf Datei anlagen

```
[[Version]
Signature= "$Windows NT$"
[PolicyStatementExtension]
Policies=InternalPolicy
[InternalPolicy]
OID= 1.2.3.4.1455.67.89.5
Notice="Legal Policy Statement"
URL=http://[REDACTED]/cps.txt
[PolicyStatementExtension]
Policies = AllIssuancePolicy
Critical = FALSE
[AllIssuancePolicy]
OID = 2.5.29.32.0
[Certsrv_Server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=10
AlternateSignatureAlgorithm=1
LoadDefaultTemplates=0
```

Issuing CA installieren





AD CS-Konfiguration ZIELSERVER

Setuptyp

- Anmeldeinformationen
- Rollendienste
- Installationstyp**
- ZS-Typ
- Privater Schlüssel
 - Kryptografie
 - ZS-Name
 - Gültigkeitsdauer
- Zertifikatdatenbank
- Bestätigung
- Status
- Ergebnisse

Geben Sie den Installationstyp der Zertifizierungsstelle an.

Unternehmenszertifizierungsstellen können mithilfe von Active Directory-Domänendienste (Active Directory Domain Services, AD DS) die Verwaltung von Zertifikaten vereinfachen. Eigenständige Zertifizierungsstellen verwenden nicht AD DS, um Zertifikate auszustellen oder zu verwalten.

- Unternehmenszertifizierungsstelle**
Unternehmenszertifizierungsstellen müssen Domänenmitglieder sein. Sie sind normalerweise online, um Zertifikate oder Zertifikatrichtlinien auszustellen.
- Eigenständige Zertifizierungsstelle**
Eigenständige Zertifizierungsstellen können einer Arbeitsgruppe oder Domäne angehören. Eigenständige Zertifizierungsstellen erfordern kein AD DS und können ohne Netzwerkverbindung verwendet werden (offline).

[Weitere Informationen zum Setuptyp](#)

AD CS-Konfiguration ZIELSERVER

Zertifizierungsstellentyp

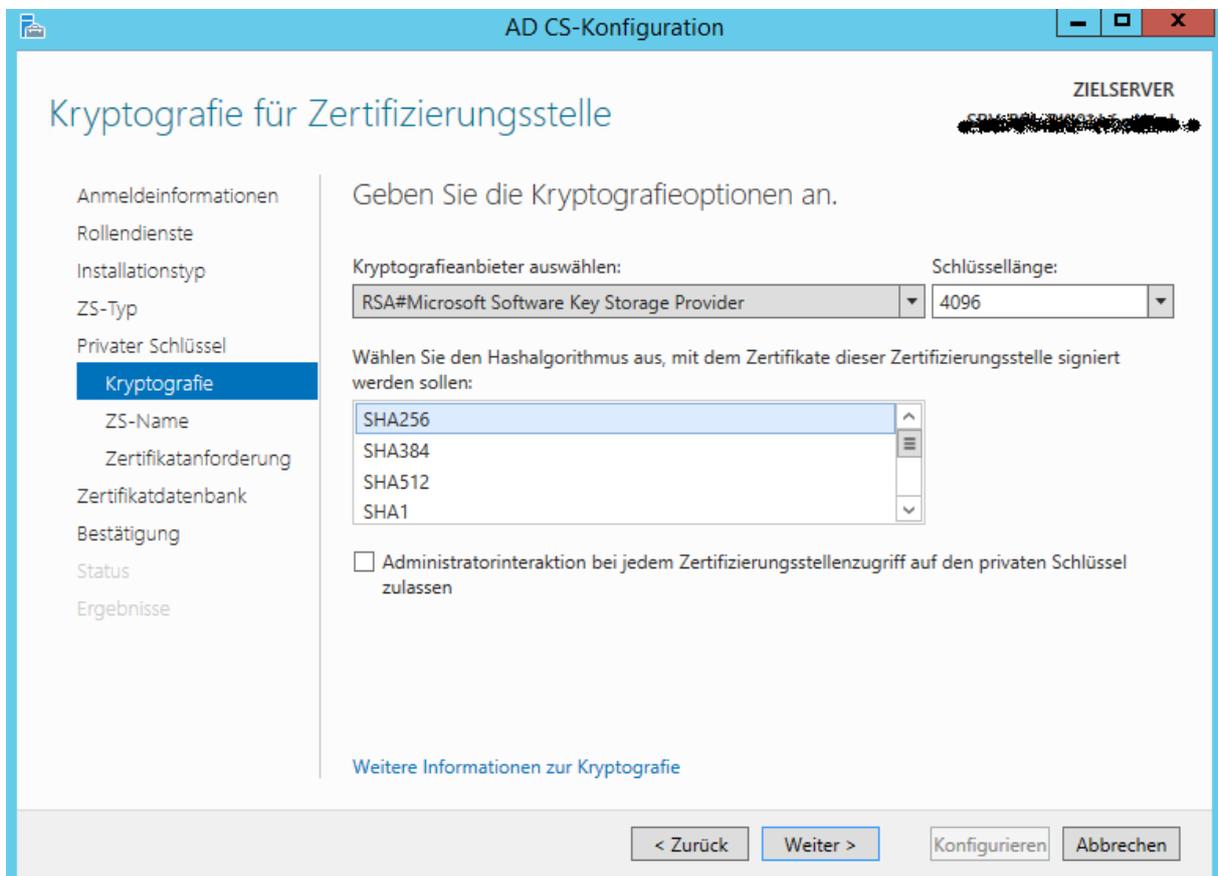
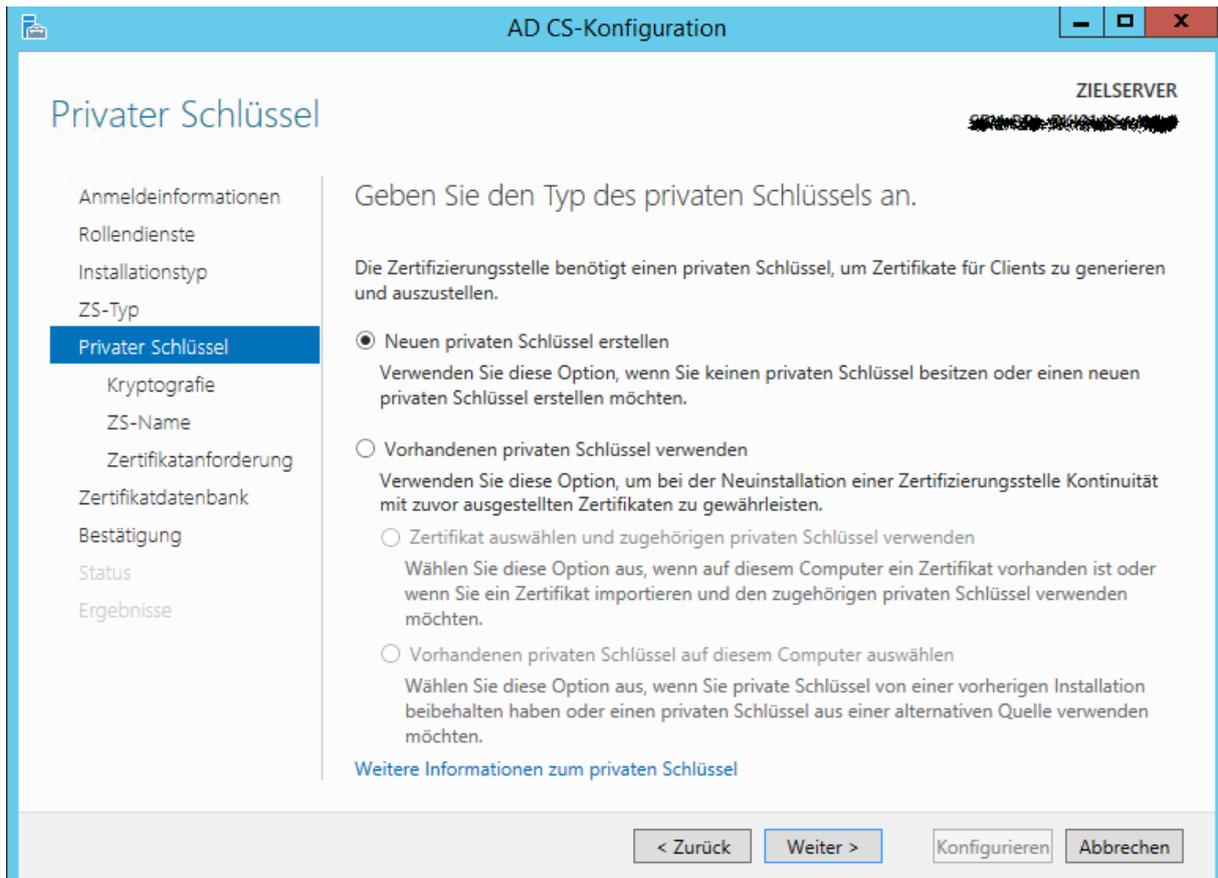
- Anmeldeinformationen
- Rollendienste
- Installationstyp
- ZS-Typ**
- Privater Schlüssel
 - Kryptografie
 - ZS-Name
 - Zertifikatanforderung
- Zertifikatdatenbank
- Bestätigung
- Status
- Ergebnisse

Geben Sie den Typ der Zertifizierungsstelle an.

Wenn Sie Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) installieren, erstellen oder erweitern Sie eine Hierarchie der Public Key-Infrastruktur (PKI). Eine Stammzertifizierungsstelle befindet sich am Anfang der PKI-Hierarchie und stellt ein eigenes selbst signiertes Zertifikat aus. Eine untergeordnete Zertifizierungsstelle empfängt ein Zertifikat von der Zertifizierungsstelle, die in der PKI-Hierarchie darüber angesiedelt ist.

- Stammzertifizierungsstelle**
Stammzertifizierungsstellen sind die ersten und möglicherweise einzigen Zertifizierungsstellen, die in einer PKI-Hierarchie konfiguriert werden.
- Untergeordnete Zertifizierungsstelle**
Für untergeordnete Zertifizierungsstellen ist eine eingerichtete PKI-Hierarchie erforderlich. Sie sind zur Ausstellung von Zertifikaten berechtigt, die von der Zertifizierungsstelle stammen, die sich in der Hierarchie über den untergeordneten Zertifizierungsstellen befindet.

[Weitere Informationen zum Typ der Zertifizierungsstelle](#)



AD CS-Konfiguration ZIELSERVER

Name der Zertifizierungsstelle

Geben Sie den Namen der Zertifizierungsstelle an.

Geben Sie einen allgemeinen Namen zur Identifizierung der Zertifizierungsstelle an. Dieser Name wird allen von der Zertifizierungsstelle ausgestellten Zertifikaten hinzugefügt. Die Werte für das DN-Suffix werden automatisch generiert, können jedoch geändert werden.

Allgemeiner Name für diese Zertifizierungsstelle:

Suffix für Distinguished Name:

Vorschau auf Distinguished Name:

[Weitere Informationen zum Namen der Zertifizierungsstelle](#)

AD CS-Konfiguration ZIELSERVER

Zertifikatanforderung

Zertifikat von übergeordneter Zertifizierungsstelle anfordern

Sie benötigen ein Zertifikat einer übergeordneten Zertifizierungsstelle, damit diese untergeordnete Zertifizierungsstelle Zertifikate ausgeben kann. Ein Zertifikat kann über eine Onlinezertifizierungsstelle angefordert werden. Sie können die Anforderung auch in einer Datei speichern und an die übergeordnete Zertifizierungsstelle senden.

Zertifikatanforderung an eine übergeordnete Zertifizierungsstelle senden:

Auswählen:

- ZS-Name
- Computername

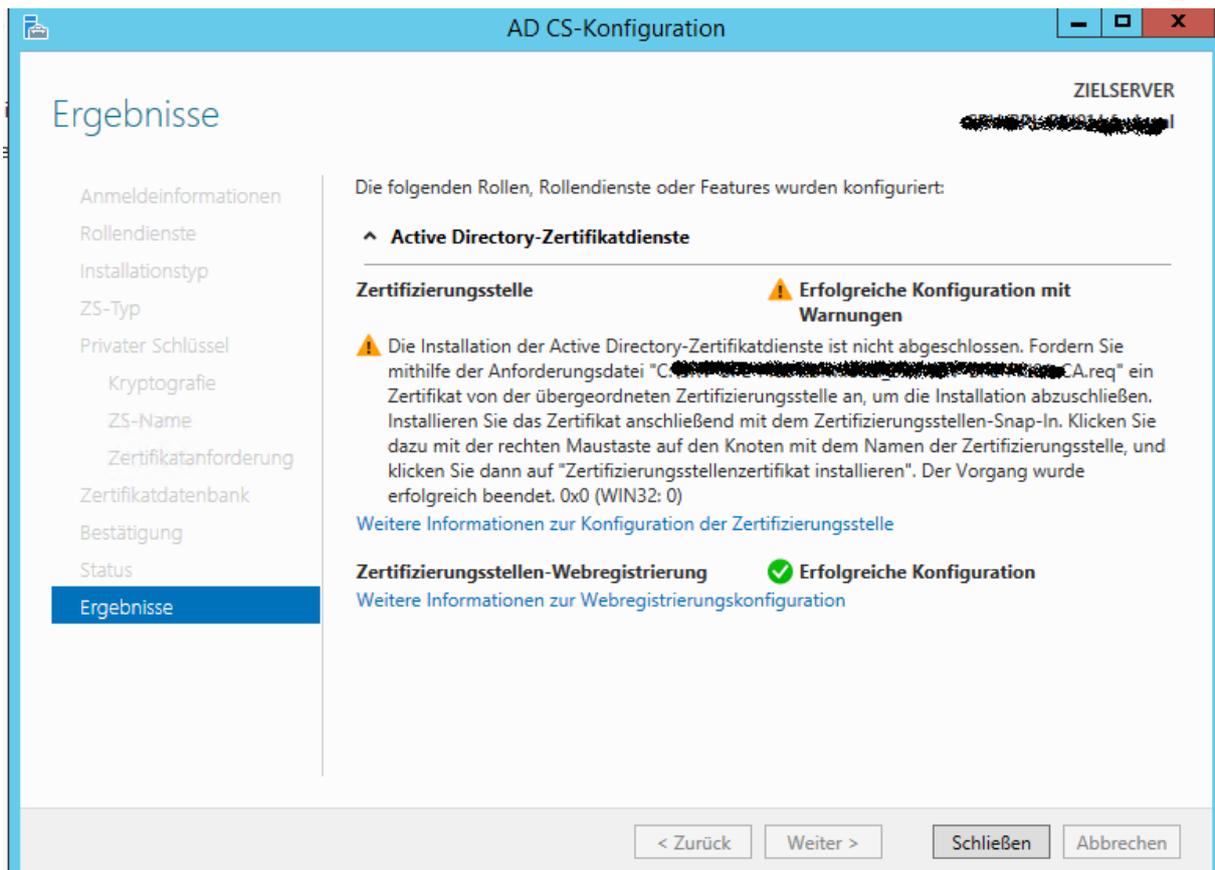
 Übergeordnete Zertifizierungsstelle:

Zertifikatanforderung in einer Datei auf dem Zielcomputer speichern:

Dateiname:

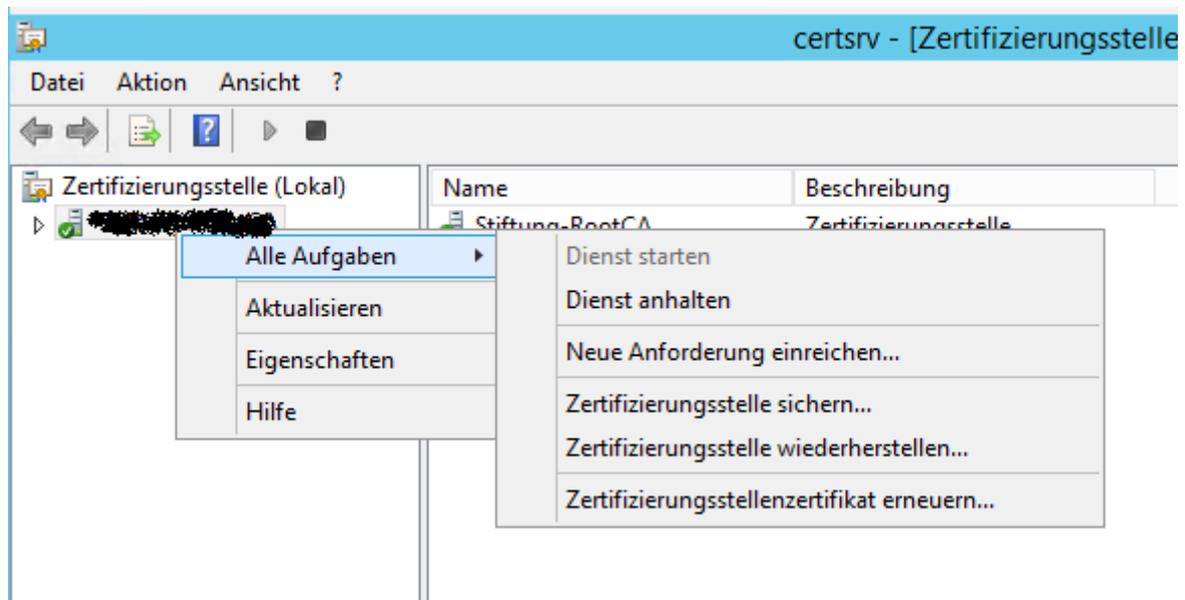
i Zur Aktivierung dieser Zertifizierungsstelle muss manuell ein Zertifikat von der übergeordneten Zertifizierungsstelle abgerufen werden.

[Weitere Informationen zur Zertifikatanforderung](#)

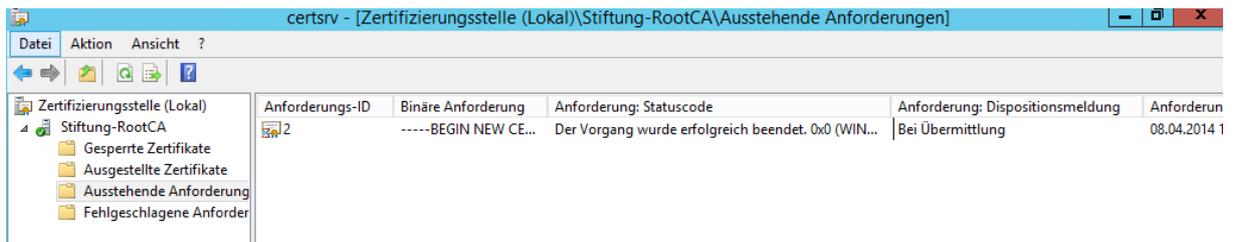


.REQ Datei zu der Offline Root CA transportieren

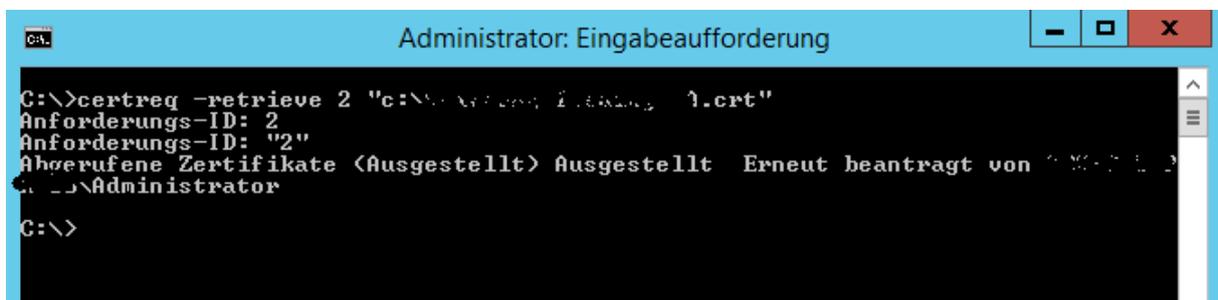
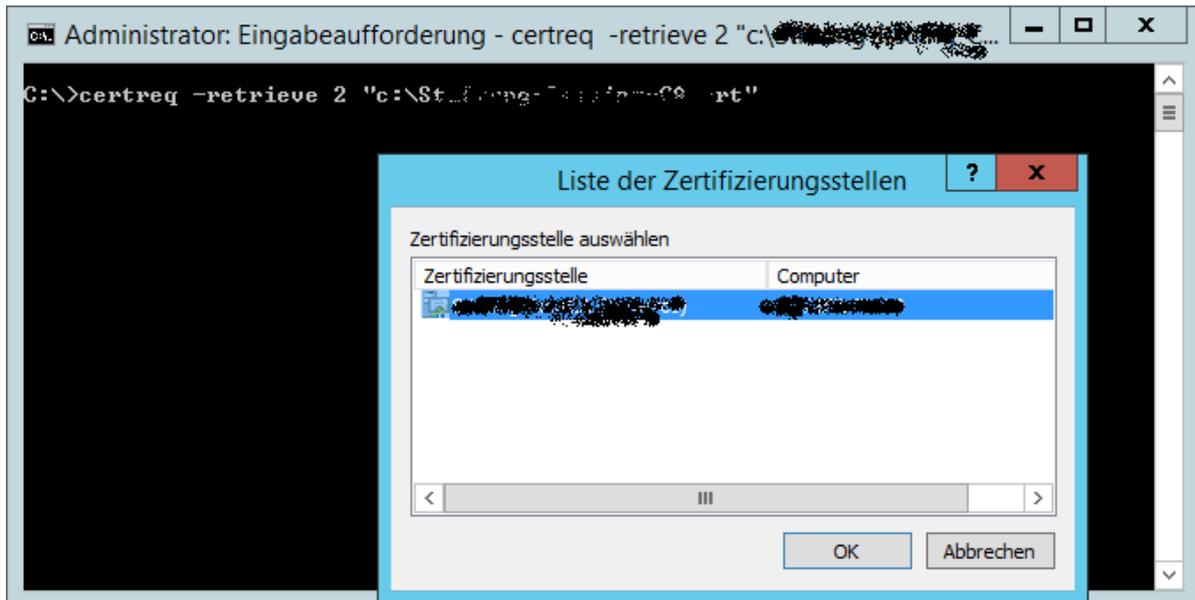
Neue Anforderung auf der Offline RootCA einreichen



Pending Requests submitten

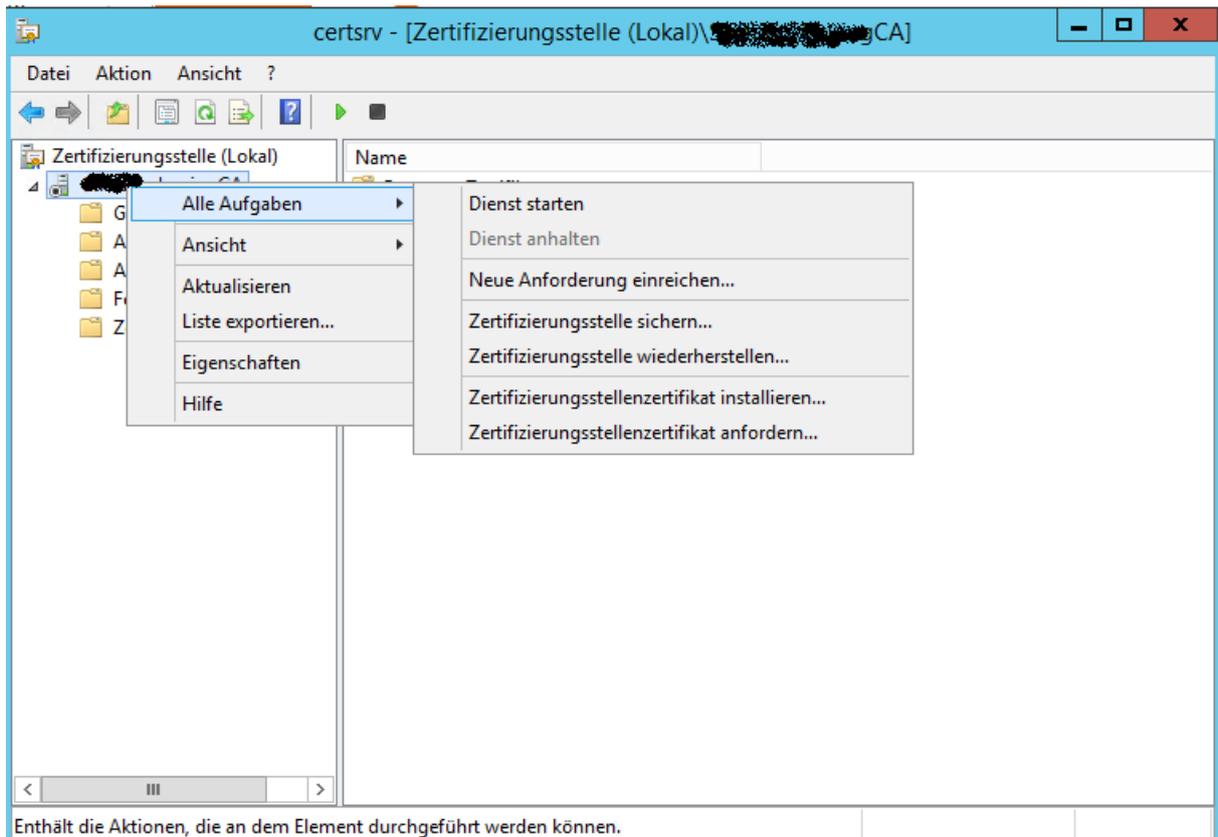


Anforderung abschliessen und .CRT Datei generieren

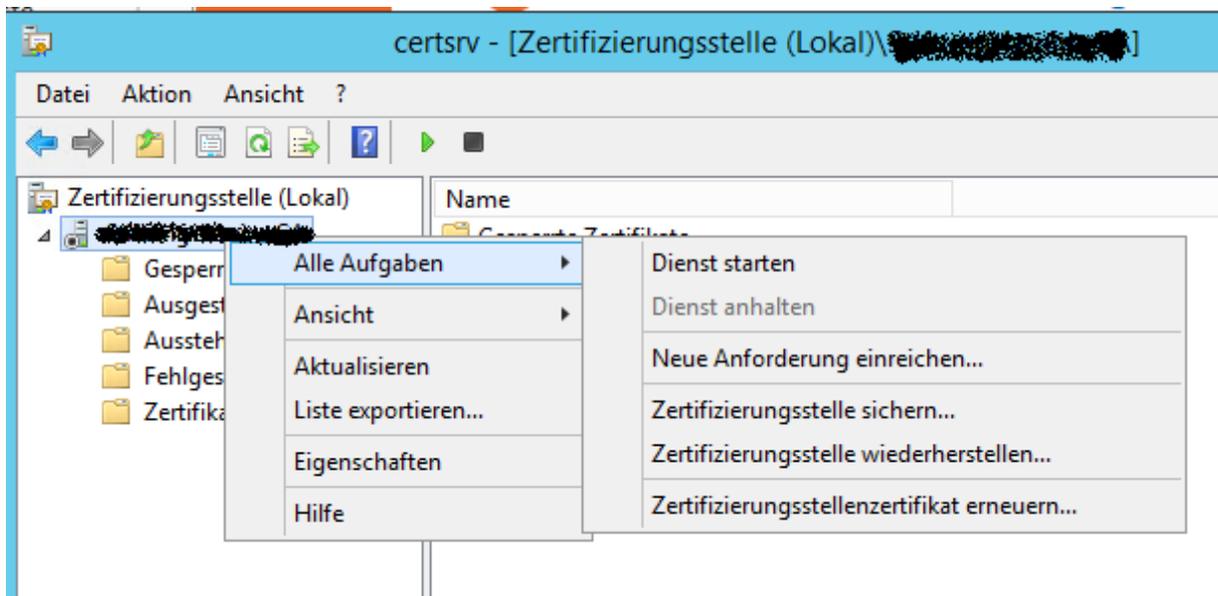


Datei zur Issuing CA transportieren

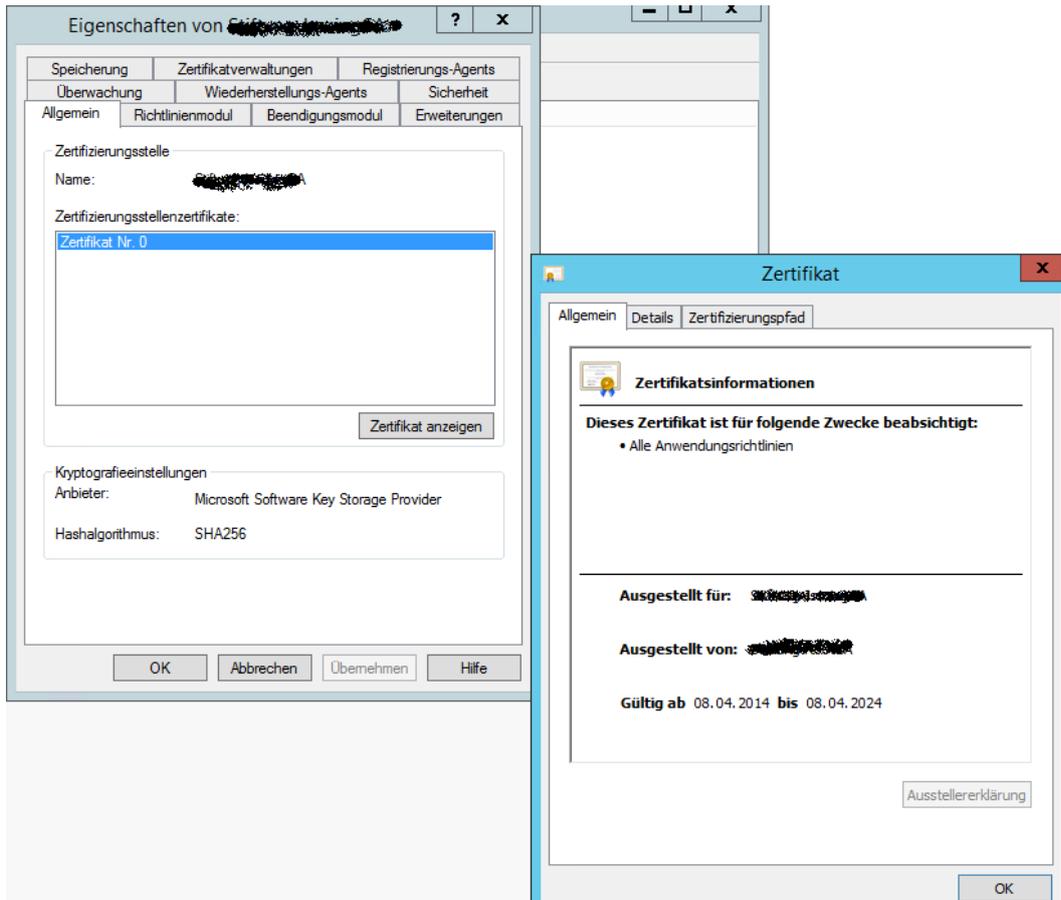
Zertifizierungsstellen Zertifikat auf Issuing CA installieren



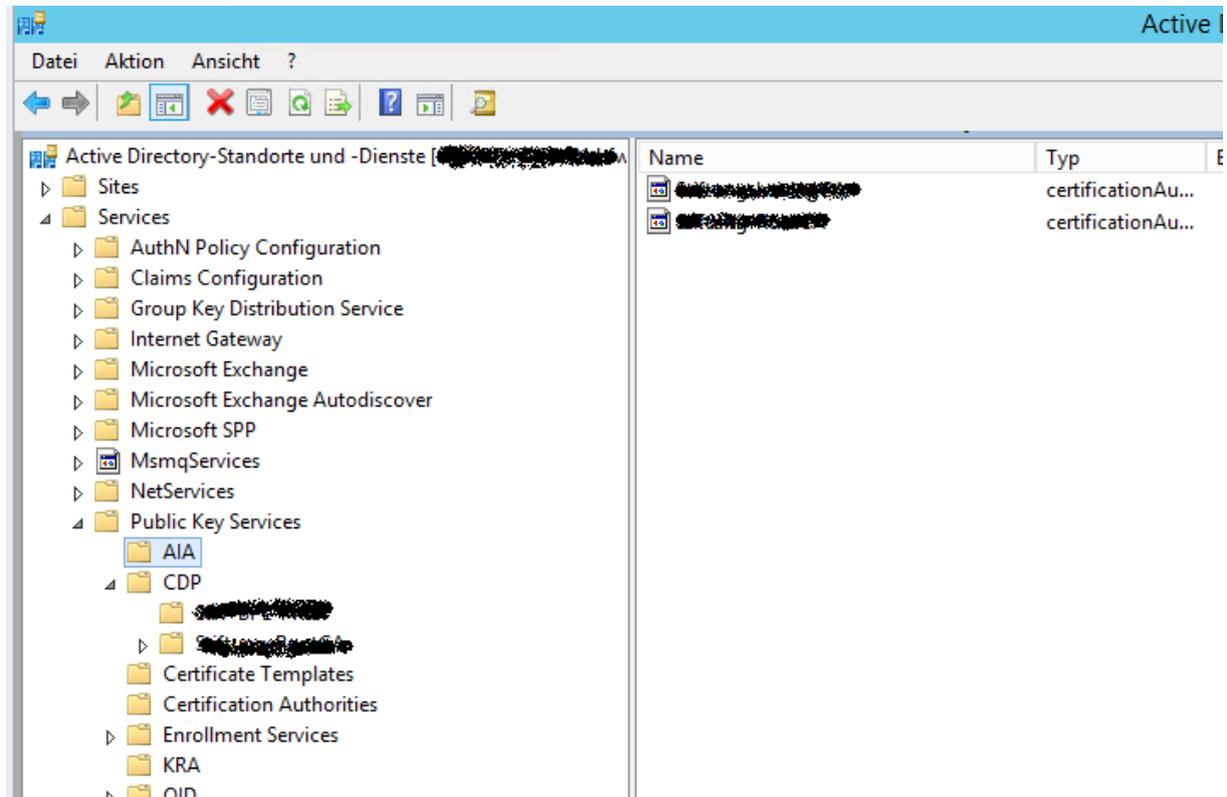
CA Dienste starten



Zertifikat prüfen ob die CA Hierarchie passt und die Gueltigkeit



Active Directory prüfen



CRL Attribut

The screenshot shows the Active Directory console on the left, with the tree view expanded to 'Public Key Services' > 'CDP'. The right pane displays the properties of a 'cRLDistributionPoint' object. A dialog box titled 'Eigenschaften von [Name]' is open, showing the 'Attribut-Editor' tab. The dialog contains a table of attributes and their values.

Attribut	Wert
certificateRevocation...	\\30\82\04\0B\30\82\01\BF\02\01\01\30\...
cn	[Redacted]
distinguishedName	CN=[Redacted], CN=Schema, CN=...
dScorePropagationD...	0x0 = ()
instance Type	0x4 = (WRITE)
name	[Redacted]
objectCategory	CN=CRL-Distribution-Point, CN=Schema, CN=...
objectClass	top; cRLDistributionPoint
objectGUID	ba126d7e-a8c5-44fa-9bd6-6622954cb711
repProperty/MetaData	AttID Ver Loc:USN Org:DSA
showInAdvancedVie...	TRUE
uSNChanged	8001959
uSNCreated	7998347
whenChanged	08.04.2014 13:50:14 Mittteleuropäische Som...

Sperrlistenveroeffentlichungsintervall anpassen

The screenshot shows the 'Eigenschaften von Gesperrte Zertifikate' dialog box. It has two tabs: 'Parameter für Sperrlistenveroeffentlichung' (selected) and 'Zertifikatsperrliste anzeigen'. The dialog contains the following settings:

- Veroeffentlichungsintervall der Sperrliste: [1] Wochen
- Nächste Aktualisierung: 15.04.2014 11:35
- Deltasperrlisten veroeffentlichen
- Veroeffentlichungsintervall: [1] Tagen
- Nächste Aktualisierung: 09.04.2014 11:35

CRL Verteilungspunkte setzen

AIA

```
Administrator: Eingabeaufforderung

C:\>certutil -setreg CACertPublicationURLs "1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%.crt\n2:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11\n2:http://www.example.com/CertEnroll/%1_%3%.crt"
HKKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\CertSvc\CACertPublicationURLs:

Alter Wert:
CACertPublicationURLs REG_MULTI_SZ =
0: 1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%.crt
   CSURL_SERVERPUBLISH -- 1
1: 2:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11
   CSURL_ADDTOCERTCDP -- 2
2: 2:http://www.example.com/CertEnroll/%1_%3%.crt
   CSURL_ADDTOCERTCDP -- 2

Neuer Wert:
CACertPublicationURLs REG_MULTI_SZ =
0: 1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%.crt
   CSURL_SERVERPUBLISH -- 1
1: 2:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11
   CSURL_ADDTOCERTCDP -- 2
2: 2:http://www.example.com/CertEnroll/%1_%3%.crt
   CSURL_ADDTOCERTCDP -- 2

CertUtil: -setreg-Befehl wurde erfolgreich ausgefuehrt.
Der Dienst "CertSvc" muss neu gestartet werden, damit die Aenderungen wirksam werden.

C:\>_
```

CDP

```
Administrator: Eingabeaufforderung

C:\>certutil -setreg CACRLPublicationURLs "65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%.cr1\n79:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10\n6:http://%1/CertEnroll/%3%8%.cr1\n65:file://%1/CertEnroll/%3%8%.cr1"
HKKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\CertSvc\CACRLPublicationURLs:

Alter Wert:
CRLPublicationURLs REG_MULTI_SZ =
0: 65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%.cr1
   CSURL_SERVERPUBLISH -- 1
   CSURL_SERVERPUBLISHDELTA -- 40 (64)
1: 79:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
   CSURL_SERVERPUBLISH -- 1
   CSURL_ADDTOCERTCDP -- 2
   CSURL_ADDTOFRESHSTCRL -- 4
   CSURL_ADDTOCRLCDP -- 8
   CSURL_SERVERPUBLISHDELTA -- 40 (64)
2: 0:http://%1/CertEnroll/%3%8%.cr1
3: 0:file://%1/CertEnroll/%3%8%.cr1

Neuer Wert:
CRLPublicationURLs REG_MULTI_SZ =
0: 65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%.cr1
   CSURL_SERVERPUBLISH -- 1
   CSURL_SERVERPUBLISHDELTA -- 40 (64)
1: 79:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
   CSURL_SERVERPUBLISH -- 1
   CSURL_ADDTOCERTCDP -- 2
   CSURL_ADDTOFRESHSTCRL -- 4
   CSURL_ADDTOCRLCDP -- 8
   CSURL_SERVERPUBLISHDELTA -- 40 (64)
2: 6:http://www.example.com/CertEnroll/%3%8%.cr1
   CSURL_ADDTOCERTCDP -- 2
   CSURL_ADDTOFRESHSTCRL -- 4
3: 65:file://www.example.com/CertEnroll/%3%8%.cr1
   CSURL_SERVERPUBLISH -- 1
   CSURL_SERVERPUBLISHDELTA -- 40 (64)

CertUtil: -setreg-Befehl wurde erfolgreich ausgefuehrt.
```

Die .CRT Datei fuer den AIA Punkt von der Issuing CA aus dem Verzeichnis C:\windows\system32\certsrv\certenroll in das Verzeichnis der CRLs auf dem Webserver kopieren.

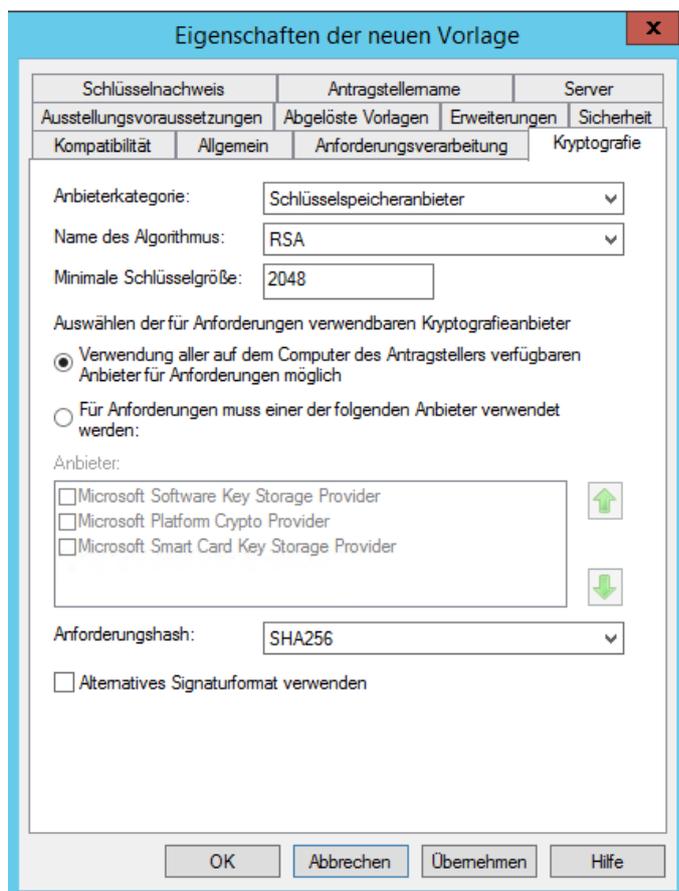
Auditing auf der CA aktivieren

Certutil -setreg CVAuditFilter 127

Certificate Templates wieder aktivieren

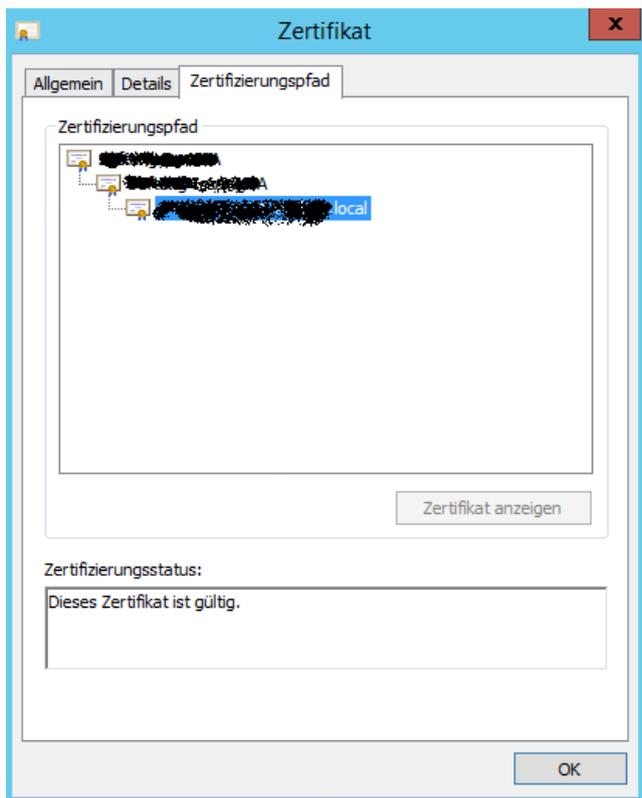
Sicherstellen, dass keine Vorlagen mehr hinzugefuegt werden, wo keine CNG Algorithmen verwendet werden. Am sinnvollsten ist es neue Zertifikat Vorlagen zu erstellen und in den Templates CNG Algorithmen festzulegen.

Achtung: Auf Abwaertskompatibilitaet zu ggfs. alten Betriebssystemen achten

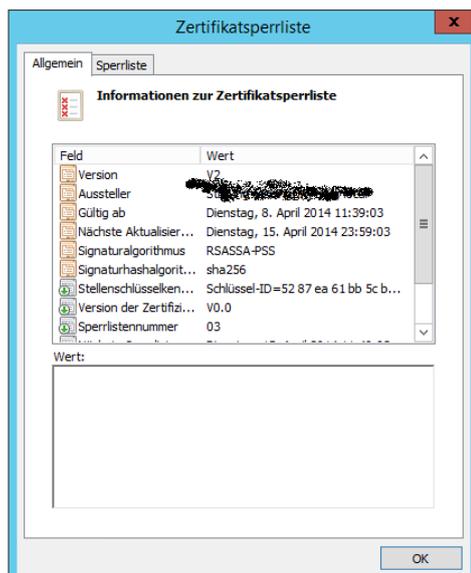
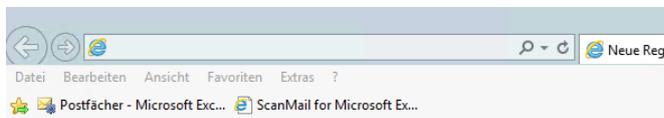


Wenn auf der Enterprise Online Issuing CA die Zertifizierungsstellen Webregistrierung installiert wurde, muss noch sichergestellt werden, dass fuer den Server ein geeignetes Webserver Zertifikat ausgestellt wird und in der IIS Verwaltungskonsole eine HTTPS-Bindung mit dem neuen Zertifikat eingerichtet wird.

Zertifikatkette prüfen

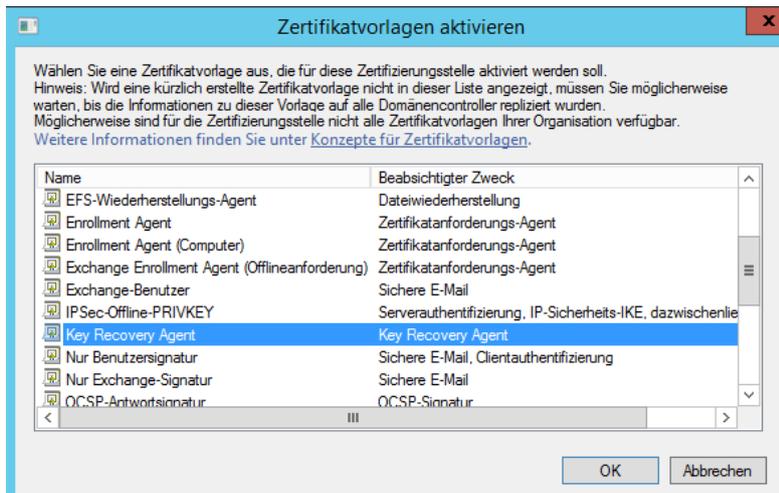


CRL Download testen



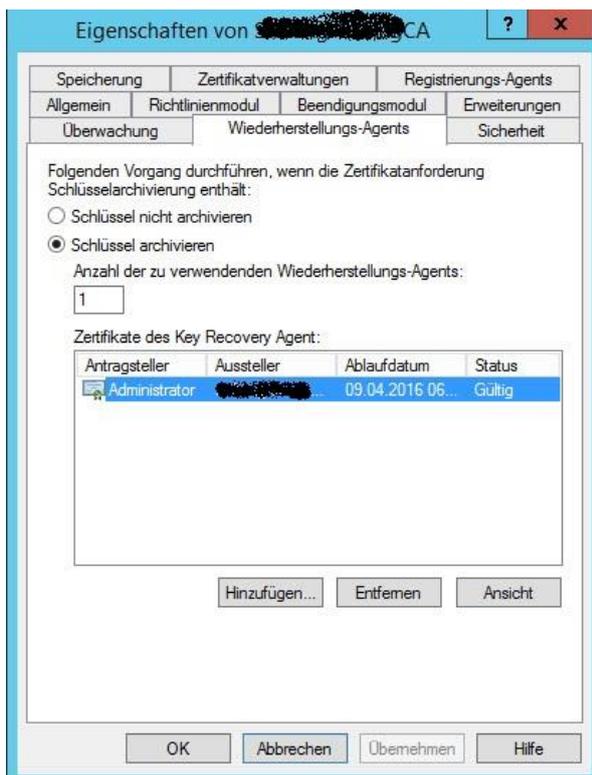
CA Schlüssellarchivierung aktivieren

KRA Vorlage aktivieren



KRA Zertifikat anfordern

CA fuer Schlüssellarchivierung aktivieren



Offline CA herunterfahren

Nach Abschluss aller Arbeiten kann die Offline CA heruntergefahren werden.

Achtung:

Alle 52 Wochen muss die Offline Root CA hochgefahren werden, die CRL mit Certutil –CRL gepublished werden und von der Offline Root CA aus dem Verzeichnis C:\windows\system32\certsrv\certenroll kopiert werden und in das Certenroll Verzeichnis auf den Webserver kopiert werden

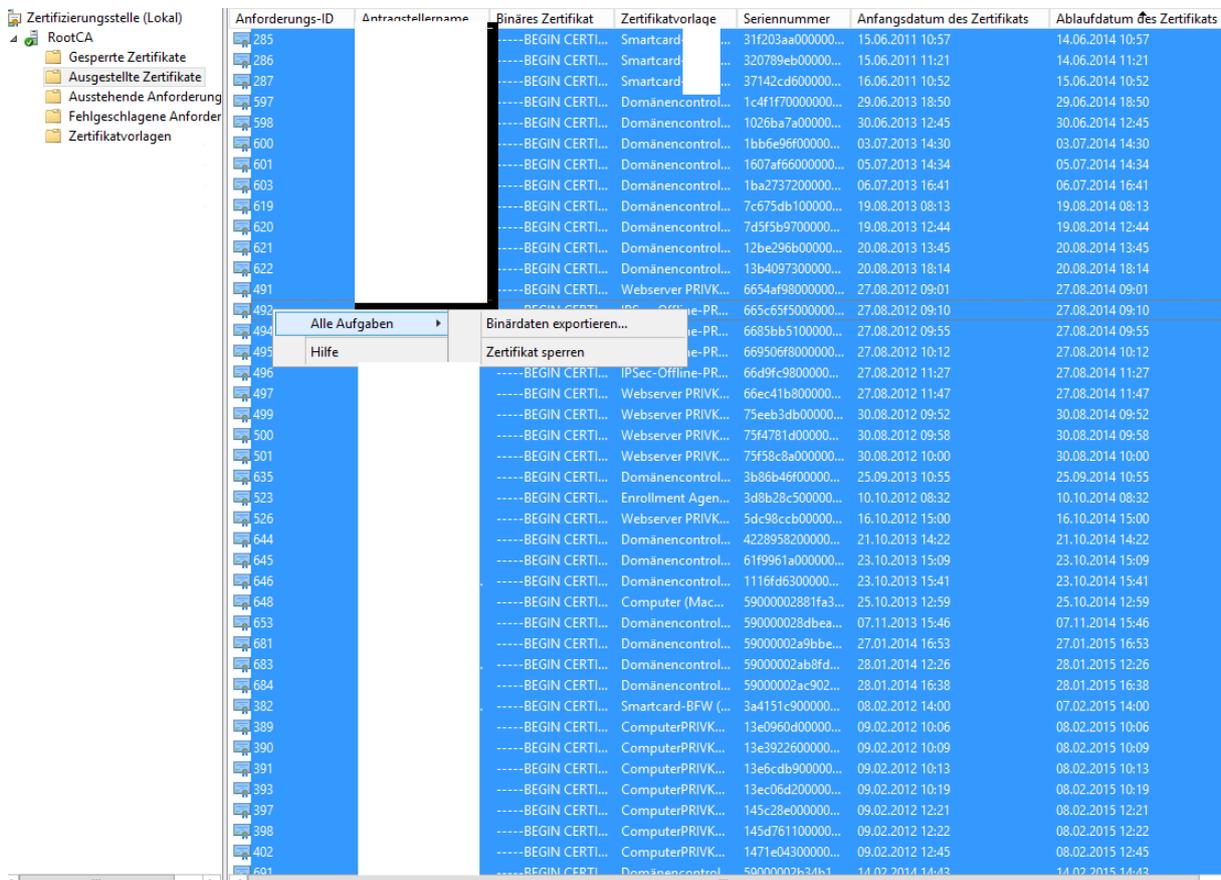
Server, Clients und Benutzer mit neuen Zertifikaten ausstatten

Nachdem die neue CA Infrastruktur in Betrieb genommen wurde, muessen auf allen Servern, Clients und Benutzer Zertifikate von der neuen CA installiert werden, bevor die alte CA dekommissioniert wird. Das ist unproblematisch in den meisten Faellen, wenn es um Webserver- oder Anwendungsserver Zertifikate geht. Viele Aufgaben koennen mit Hilfe des Autoenrollment per Gruppenrichtlinien automatisiert werden. Problematisch sind Zertifikate mit dem Zweck der Datenverschluesselung (E-Mail, Dateisystem etc.). Hier ist im **Vorfeld** mehr zu planen!!

IST CA dekommissionieren

<http://social.technet.microsoft.com/wiki/contents/articles/how-to-decommission-a-windows-enterprise-certification-authority-and-how-to-remove-all-related-objects.aspx>

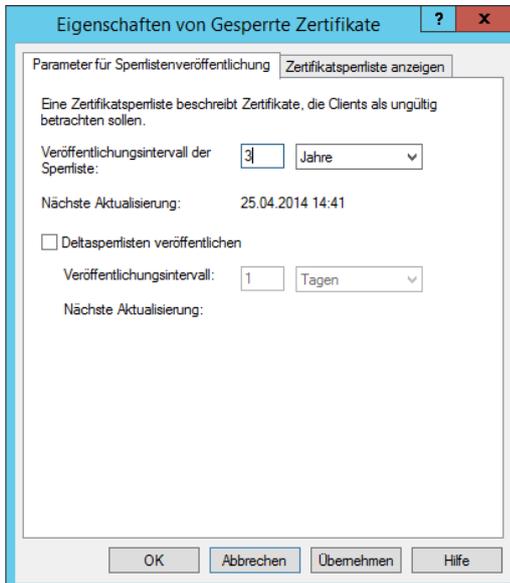
Alle aktiven Zertifikate revoke



Anforderungs-ID	Antragsstellername	Binäres Zertifikat	Zertifikatvorlage	Seriennummer	Anfangsdatum des Zertifikats	Ablaufdatum des Zertifikats
285		-----BEGIN CERTI...	Smartcard	31f203aa000000...	15.06.2011 10:57	14.06.2014 10:57
286		-----BEGIN CERTI...	Smartcard	320789eb000000...	15.06.2011 11:21	14.06.2014 11:21
287		-----BEGIN CERTI...	Smartcard	37142cd6000000...	16.06.2011 10:52	15.06.2014 10:52
597		-----BEGIN CERTI...	Domänencontrol...	1c4f1f70000000...	29.06.2013 18:50	29.06.2014 18:50
598		-----BEGIN CERTI...	Domänencontrol...	1026ba7a000000...	30.06.2013 12:45	30.06.2014 12:45
600		-----BEGIN CERTI...	Domänencontrol...	1bb6e96f000000...	03.07.2013 14:30	03.07.2014 14:30
601		-----BEGIN CERTI...	Domänencontrol...	1607af66000000...	05.07.2013 14:34	05.07.2014 14:34
603		-----BEGIN CERTI...	Domänencontrol...	1ba27372000000...	06.07.2013 16:41	06.07.2014 16:41
619		-----BEGIN CERTI...	Domänencontrol...	7c675db1000000...	19.08.2013 08:13	19.08.2014 08:13
620		-----BEGIN CERTI...	Domänencontrol...	7d5f5b97000000...	19.08.2013 12:44	19.08.2014 12:44
621		-----BEGIN CERTI...	Domänencontrol...	12be296b000000...	20.08.2013 13:45	20.08.2014 13:45
622		-----BEGIN CERTI...	Domänencontrol...	13b40973000000...	20.08.2013 18:14	20.08.2014 18:14
491		-----BEGIN CERTI...	Webserver PRIVK...	6654af98000000...	27.08.2012 09:01	27.08.2014 09:01
492		-----BEGIN CERTI...	IPSec-Offline-PR...	665c65f5000000...	27.08.2012 09:10	27.08.2014 09:10
494		-----BEGIN CERTI...	IPSec-Offline-PR...	6695bb51000000...	27.08.2012 09:55	27.08.2014 09:55
495		-----BEGIN CERTI...	IPSec-Offline-PR...	669506f8000000...	27.08.2012 10:12	27.08.2014 10:12
496		-----BEGIN CERTI...	IPSec-Offline-PR...	66d9fc98000000...	27.08.2012 11:27	27.08.2014 11:27
497		-----BEGIN CERTI...	Webserver PRIVK...	66ec41b8000000...	27.08.2012 11:47	27.08.2014 11:47
499		-----BEGIN CERTI...	Webserver PRIVK...	75eeb3db000000...	30.08.2012 09:52	30.08.2014 09:52
500		-----BEGIN CERTI...	Webserver PRIVK...	75f4781d000000...	30.08.2012 09:58	30.08.2014 09:58
501		-----BEGIN CERTI...	Webserver PRIVK...	75f58c8a000000...	30.08.2012 10:00	30.08.2014 10:00
635		-----BEGIN CERTI...	Domänencontrol...	3b86b46f000000...	25.09.2013 10:55	25.09.2014 10:55
523		-----BEGIN CERTI...	Enrollment Agen...	3d8b28c5000000...	10.10.2012 08:32	10.10.2014 08:32
526		-----BEGIN CERTI...	Webserver PRIVK...	5dc98ccb000000...	16.10.2012 15:00	16.10.2014 15:00
644		-----BEGIN CERTI...	Domänencontrol...	42289582000000...	21.10.2013 14:22	21.10.2014 14:22
645		-----BEGIN CERTI...	Domänencontrol...	61f9961a000000...	23.10.2013 15:09	23.10.2014 15:09
646		-----BEGIN CERTI...	Domänencontrol...	1116fd63000000...	23.10.2013 15:41	23.10.2014 15:41
648		-----BEGIN CERTI...	Computer (Mac...	59000002881fa3...	25.10.2013 12:59	25.10.2014 12:59
653		-----BEGIN CERTI...	Domänencontrol...	590000028dbea...	07.11.2013 15:46	07.11.2014 15:46
681		-----BEGIN CERTI...	Domänencontrol...	59000002a9bbe...	27.01.2014 16:53	27.01.2015 16:53
683		-----BEGIN CERTI...	Domänencontrol...	59000002ab9fd...	28.01.2014 12:26	28.01.2015 12:26
684		-----BEGIN CERTI...	Domänencontrol...	59000002ac902...	28.01.2014 16:38	28.01.2015 16:38
382		-----BEGIN CERTI...	Smartcard-BFW (...	3a4151c9000000...	08.02.2012 14:00	07.02.2015 14:00
389		-----BEGIN CERTI...	ComputerPRIVK...	13e09604000000...	09.02.2012 10:06	08.02.2015 10:06
390		-----BEGIN CERTI...	ComputerPRIVK...	13e39226000000...	09.02.2012 10:09	08.02.2015 10:09
391		-----BEGIN CERTI...	ComputerPRIVK...	13e6cd69000000...	09.02.2012 10:13	08.02.2015 10:13
393		-----BEGIN CERTI...	ComputerPRIVK...	13ec06d2000000...	09.02.2012 10:19	08.02.2015 10:19
397		-----BEGIN CERTI...	ComputerPRIVK...	145c28e0000000...	09.02.2012 12:21	08.02.2015 12:21
398		-----BEGIN CERTI...	ComputerPRIVK...	145d7611000000...	09.02.2012 12:22	08.02.2015 12:22
402		-----BEGIN CERTI...	ComputerPRIVK...	1471e043000000...	09.02.2012 12:45	08.02.2015 12:45
601		-----BEGIN CERTI...	Domänencontrol...	59000002b34b1...	14.02.2014 14:43	14.02.2015 14:43

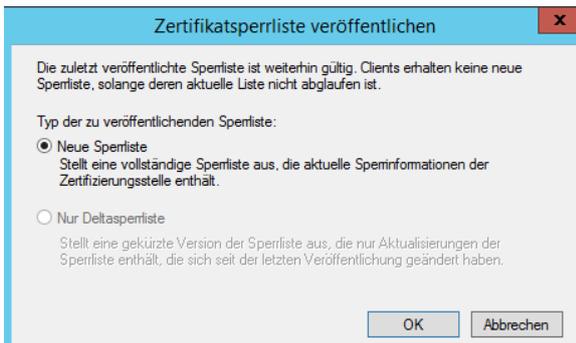
CRL anpassen

CRL Intervall verlaengern (laenger als Laufzeit der gerade revoked Zertifikate),
Publishing der Delta CRL deaktivieren



The screenshot shows a Windows dialog box titled "Eigenschaften von Gesperrte Zertifikate". It has two tabs: "Parameter für Sperlistenveröffentlichung" (selected) and "Zertifikatsperliste anzeigen". The main text reads: "Eine Zertifikatsperliste beschreibt Zertifikate, die Clients als ungültig betrachten sollen." Below this, there are two sections. The first section is for the main list, with a "Veröffentlichungsintervall der Sperliste:" set to "3" and "Jahre", and a "Nächste Aktualisierung:" of "25.04.2014 14:41". The second section is for delta lists, with a checkbox "Deltasperlisten veröffentlichen" that is unchecked, a "Veröffentlichungsintervall:" set to "1" and "Tagen", and a "Nächste Aktualisierung:" field. At the bottom, there are buttons for "OK", "Abbrechen", "Übernehmen", and "Hilfe".

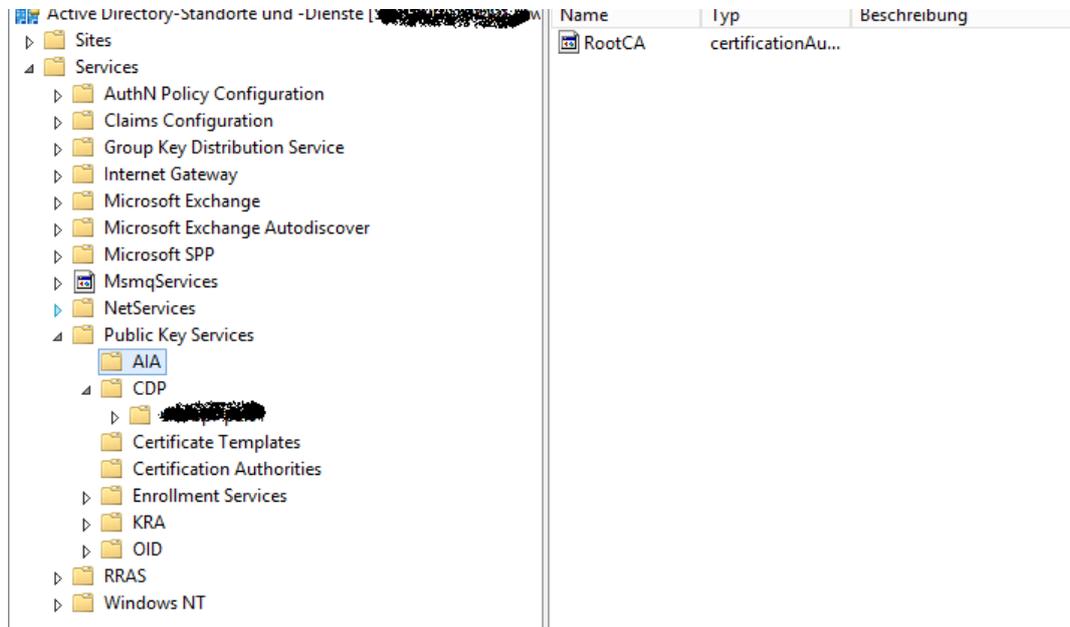
Sperlliste veroeffentlichen



The screenshot shows a Windows dialog box titled "Zertifikatsperlliste veröffentlichen". The main text reads: "Die zuletzt veröffentlichte Sperlliste ist weiterhin gültig. Clients erhalten keine neue Sperlliste, solange deren aktuelle Liste nicht abgelaufen ist." Below this, there is a section "Typ der zu veröffentlichenden Sperlliste:" with two radio button options. The first option, "Neue Sperlliste", is selected and described as: "Stellt eine vollständige Sperlliste aus, die aktuelle Sperlinformationen der Zertifizierungsstelle enthält." The second option, "Nur Deltasperlliste", is unselected and described as: "Stellt eine gekürzte Version der Sperlliste aus, die nur Aktualisierungen der Sperlliste enthält, die sich seit der letzten Veröffentlichung geändert haben." At the bottom, there are buttons for "OK" and "Abbrechen".

Zertifikatsdienste deinstallieren

CA Objekte aus der Active Directory Konfigurations Partition loeschen, wenn alle Zertifikate korrekt revoked wurden.



NTAuth Objekte loeschen

```
certutil -viewdelstore "ldap:///CN=NtAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=ForestRoot,DC=com?cACertificate?base?objectclass=certificationAuthority"
```

```
certutil -viewdelstore "ldap:///CN=NtAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=ForestRoot,DC=com?cACertificate?base?objectclass"
```

Nach der Deinstallation der CA die CA Datenbank loeschen

```
%systemroot%\System32\Certlog
```

Auf allen DC die automatisch erstellen Domaenen Controller Zertifikate loeschen

certutil -dcinfo deleteBad

```
Exclude leaf cert:
0907d8af90186095efbf55320d4b6b5eeea339da
Full chain:
6046fd03359e49ab3c92aa346316053a4a76479cb
Missing Issuer: CN=KDC, DC=corp, DC=example
Issuer: CN=KDC, DC=corp, DC=example
NotBefore: 27.01.2014 16:53
NotAfter: 27.01.2015 16:53
Subject: CN=KDC, DC=corp, DC=example
Serial: 59000002a9bbeafb9eee63e0330000000002a9
SubjectAltName: Anderer Name:DS-Objekt-Guid=04 10 43 31 d7 a7 de c6 53 45 b6 6
3 a3 99 77 7f d9 a4, DNS-Name=corp.example.com
Template: DomainController
6046fd03359e49ab3c92aa346316053a4a76479cb
Eine Zertifikatkette zu einer vertrauenswürdigen Stammzertifizierungsstelle kann
te nicht aufgebaut werden. 0x800b010a (-2146762486 CERT_E_CHAINING)
-----
Die Zertifikatkette ist unvollständig.
Folgendes Zertifikat wurde nicht gefunden:
CN=KDC, DC=corp, DC=example
1 KDC-Zertifikate für corp.example.com
CertUtil: -DCInfo-Befehl wurde erfolgreich ausgeführt.
C:\Users\Administrator>
```

Im Rahmen des naechsten Gruppenrichtlinien Aktualisierungs-Intervall werden neue DC Zertifikate angefordert