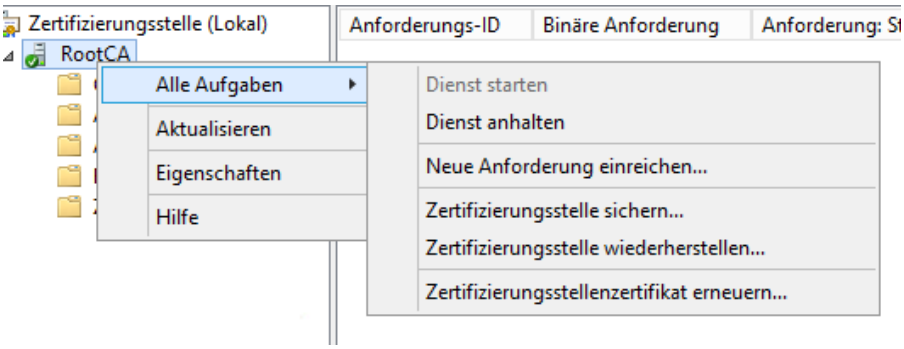
**Migration Single Tier Online Enterprise Root CA auf Two Tier Offline Standalone CA mit Online Enterprise Issuing CA mit Windows Server 2012 R2**

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

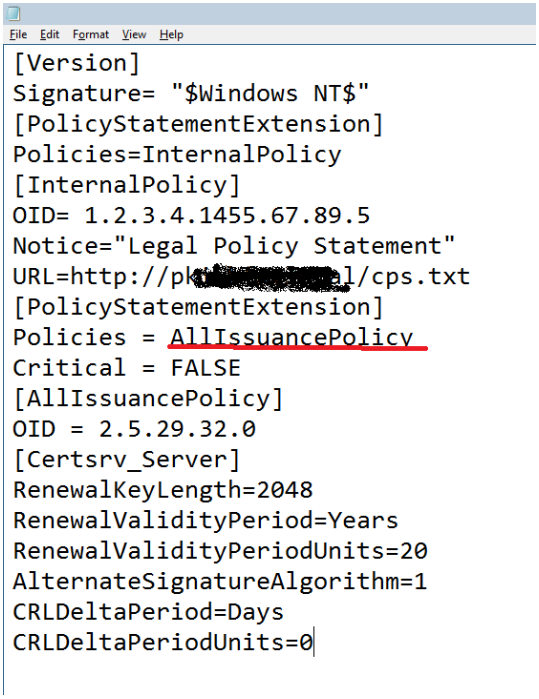
Backup IST CA




**Capolicy.inf**

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

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

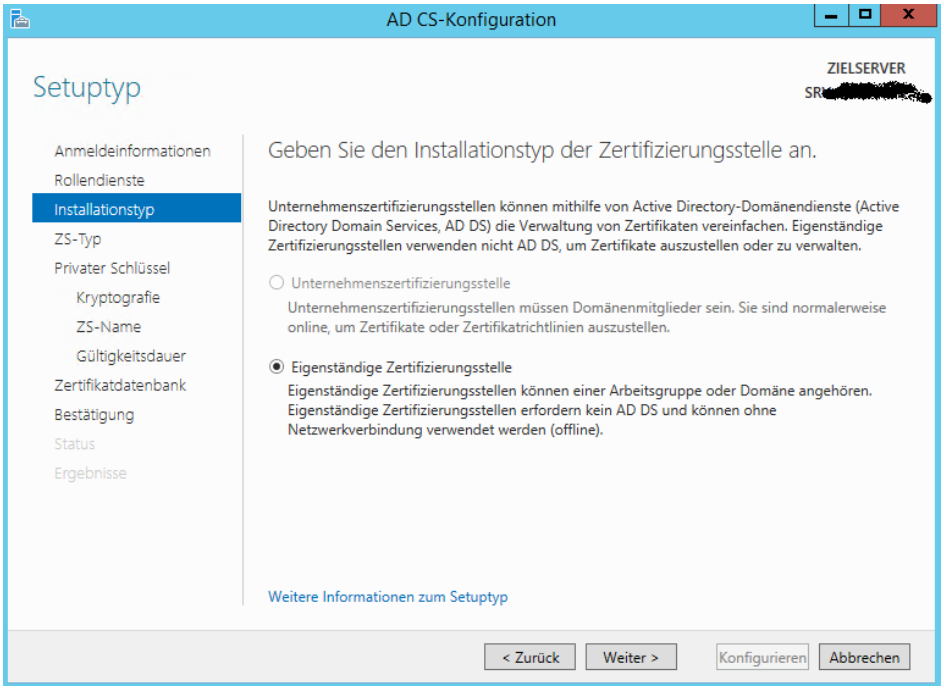



Speichern in C:\Windows\capolicy.inf

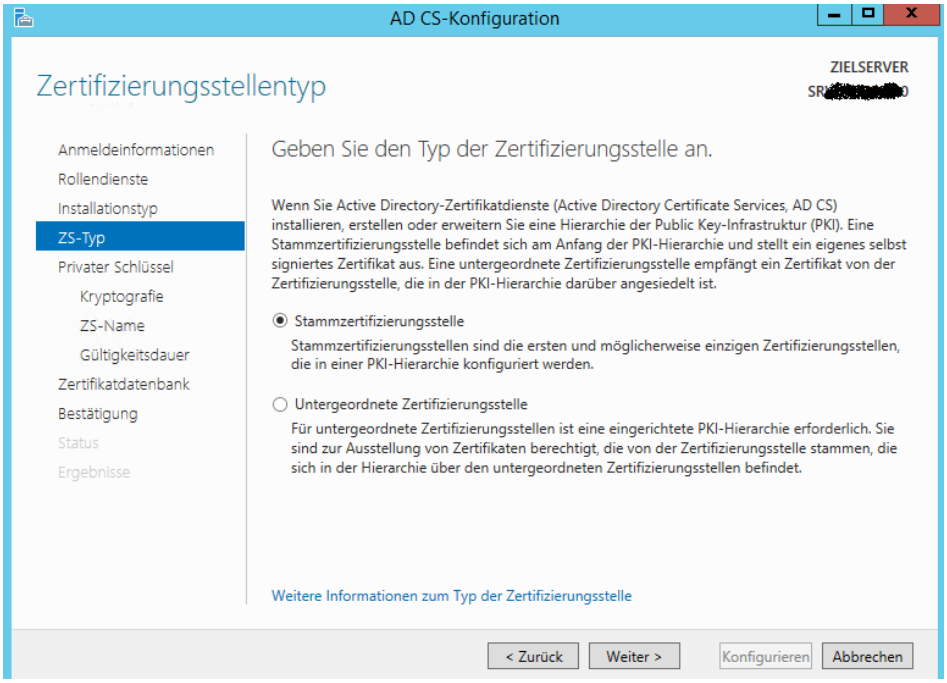
**Offline Root implementieren**

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

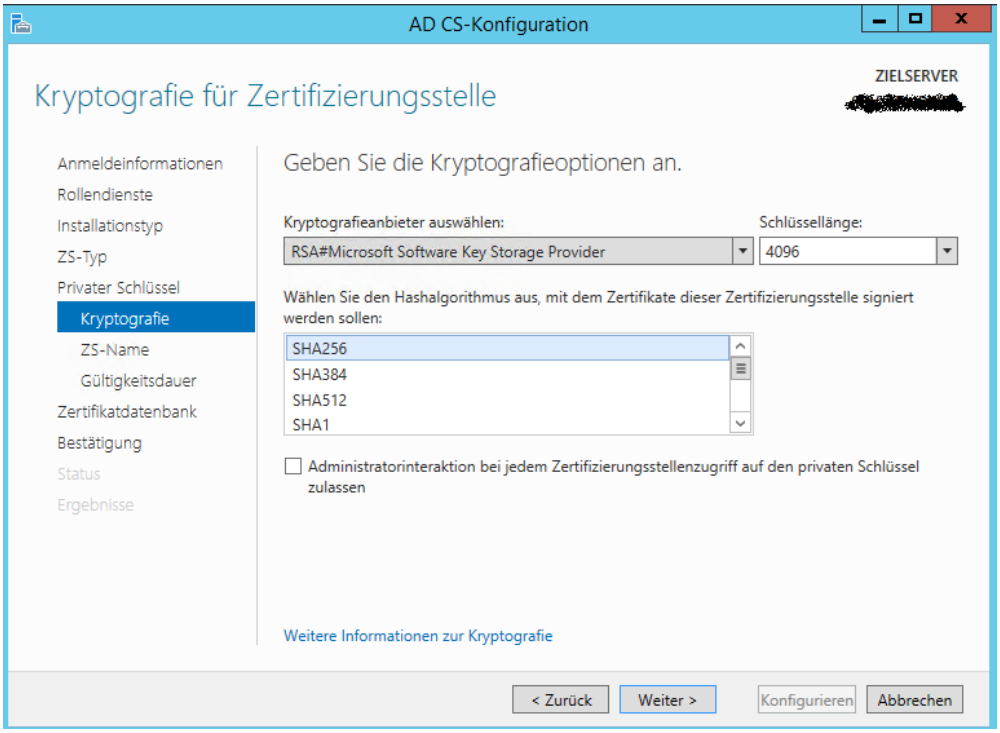
Eigenstaendige Zertifizierungsstelle



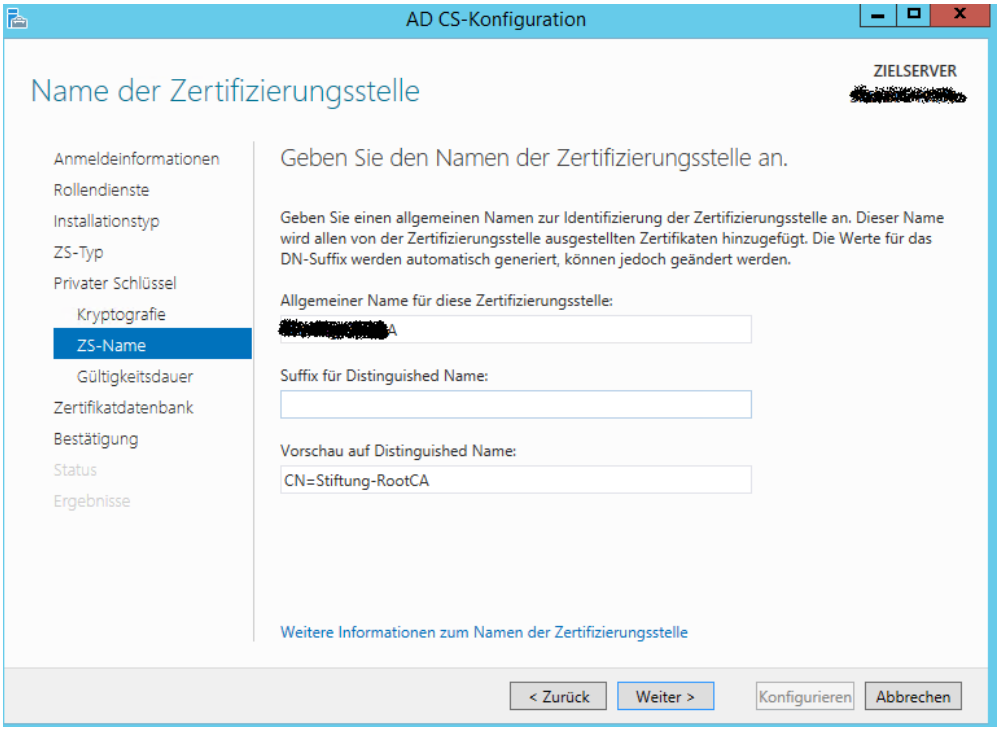

Stammzertifizierungsstelle



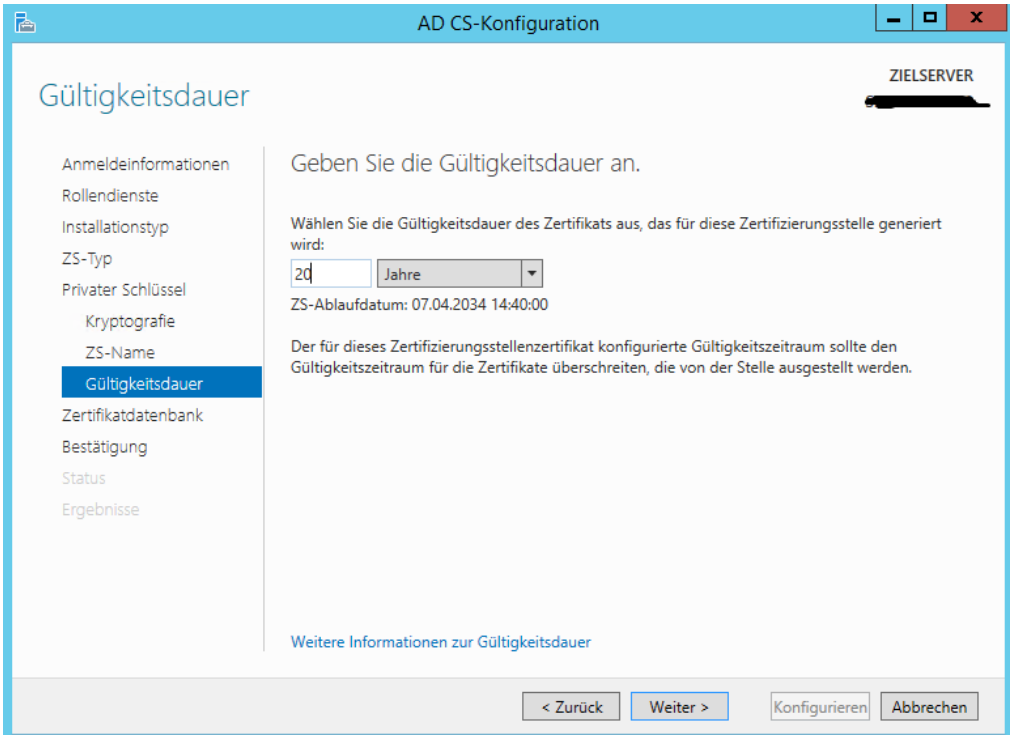
Neuen privaten Schluessel erstellen



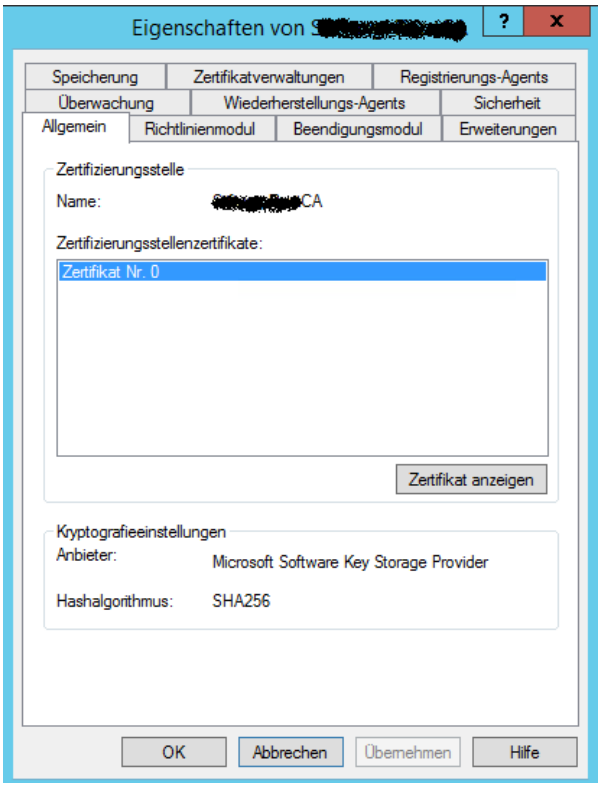

CA Name



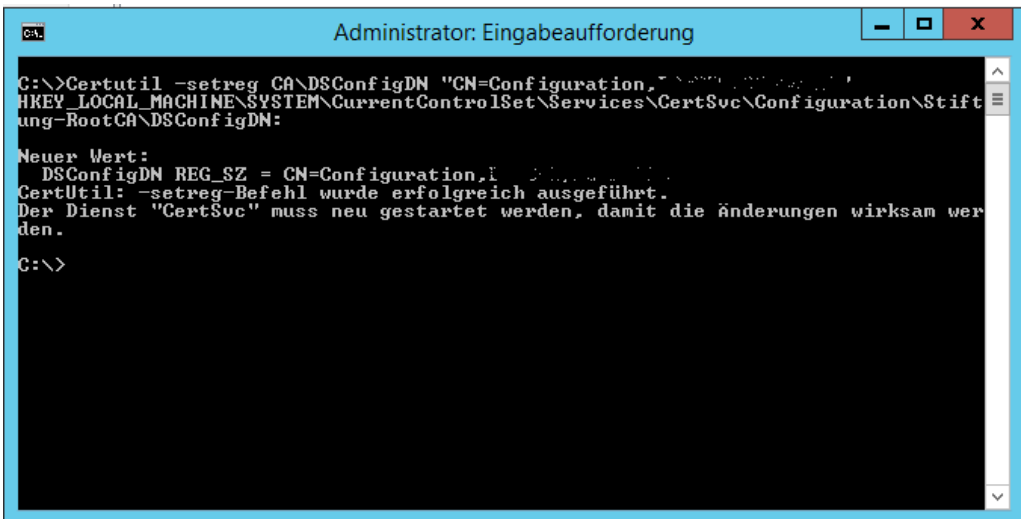
## Gueltigkeit



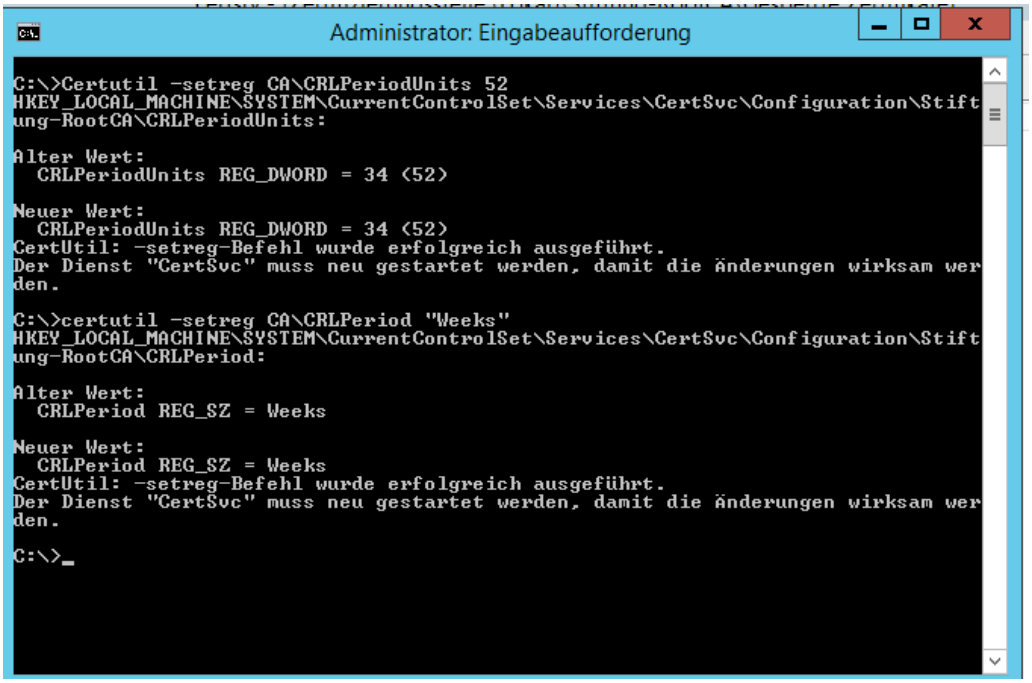

## CA Eigenschaften



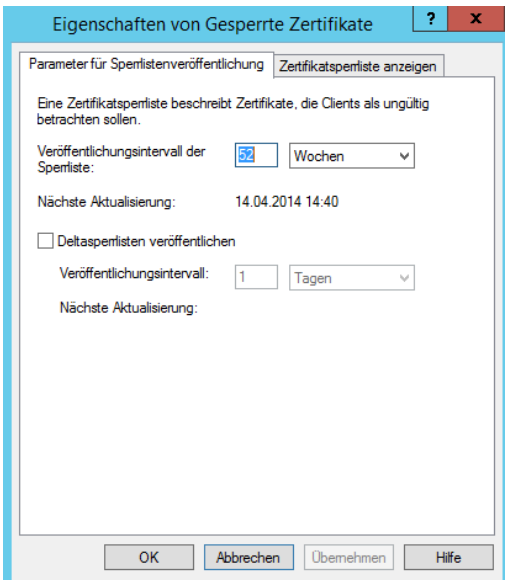
Der CA den DN zur Konfigurations Partition angeben



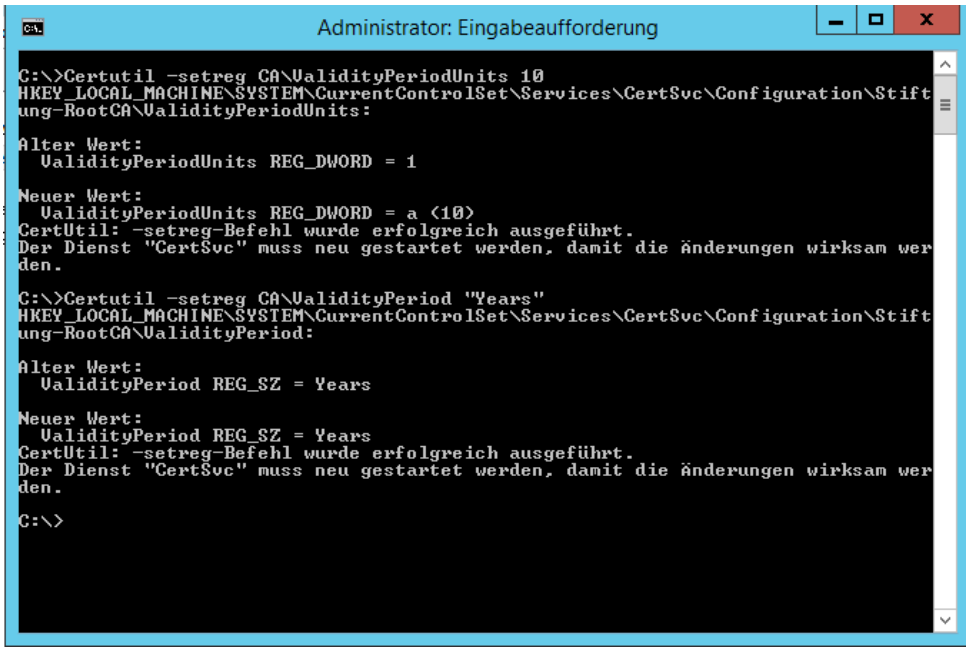

CRL Publishing auf 52 Wochen stellen



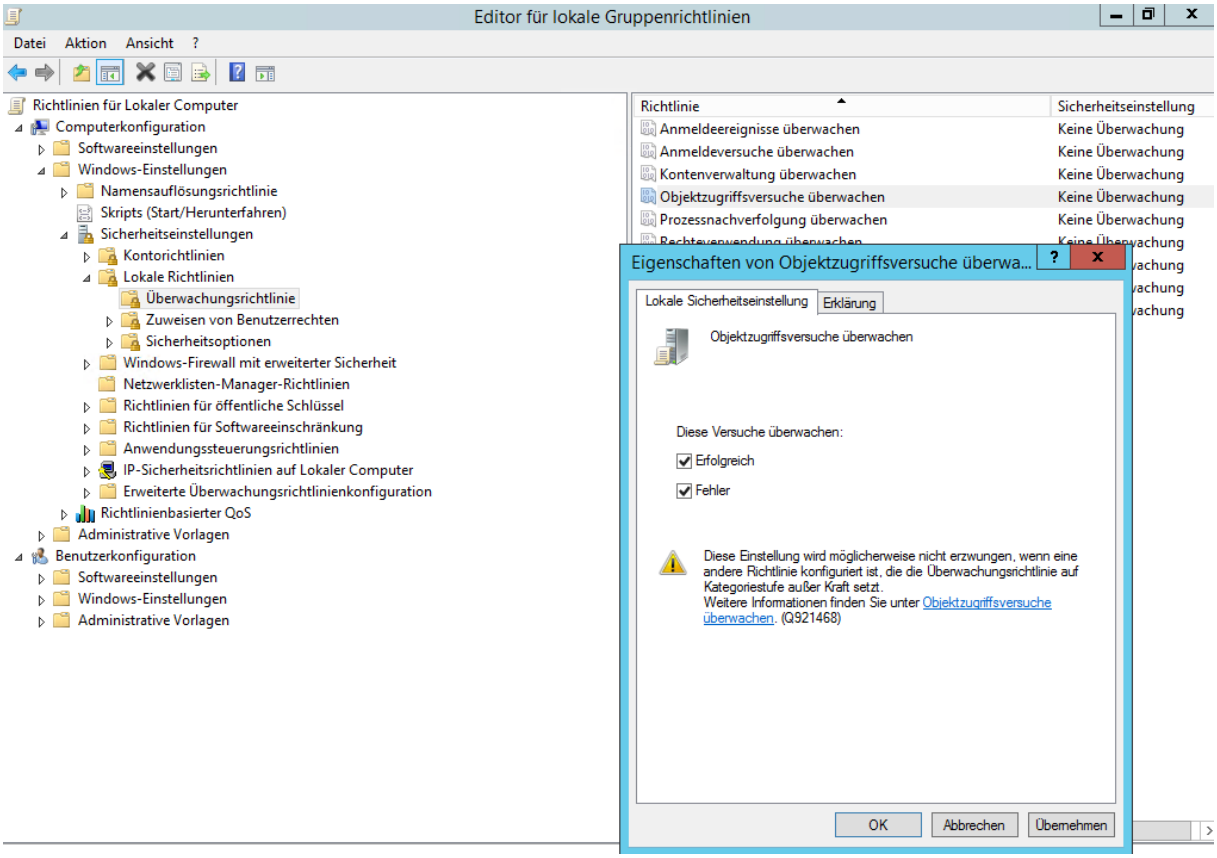
Ueberpruefung



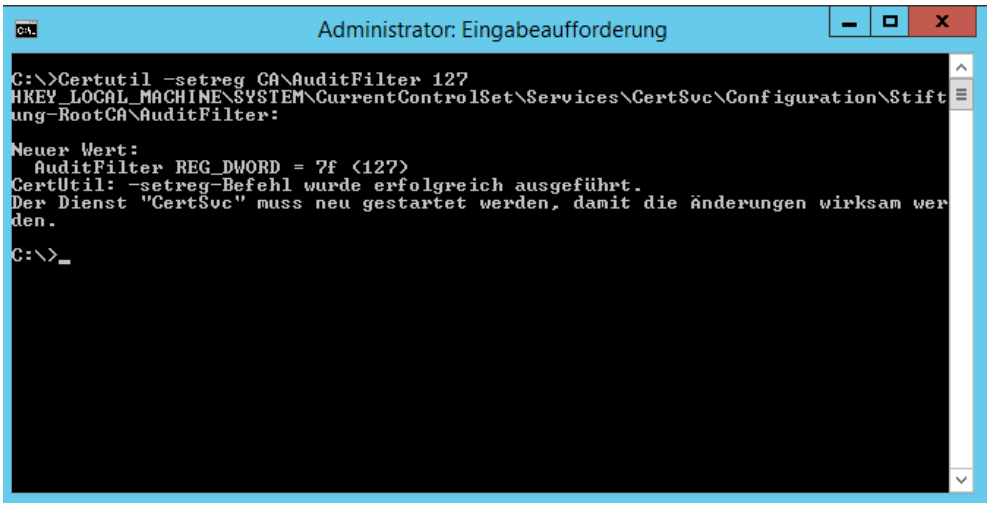

Gueltigkeit des spaeter auszustellenden Zertifikats der Issuing CA auf 10 Jahre stellen



## Objektzugriff ueberwachen

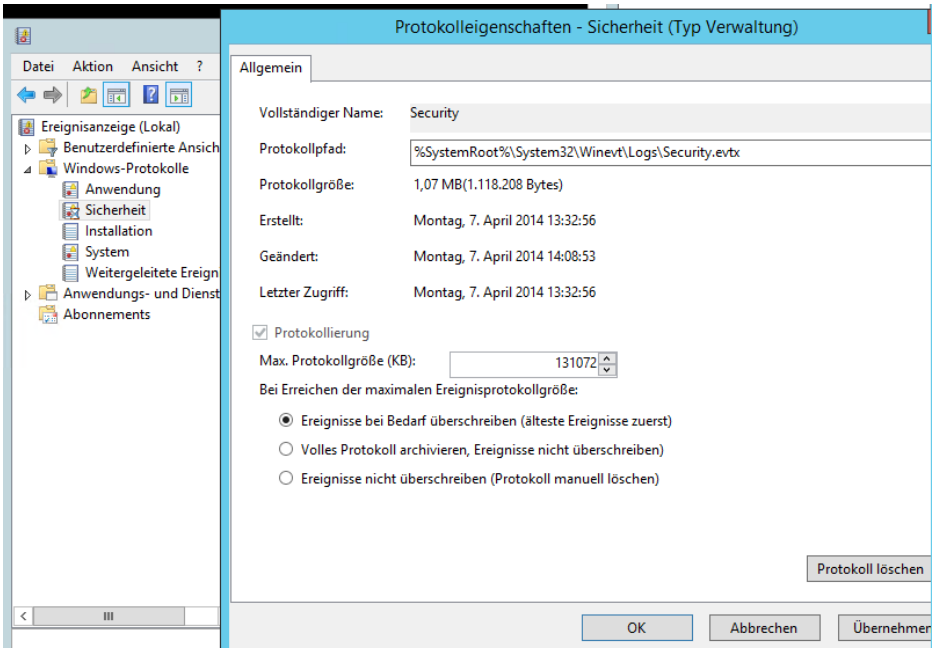



## Audit Filtering aktivieren



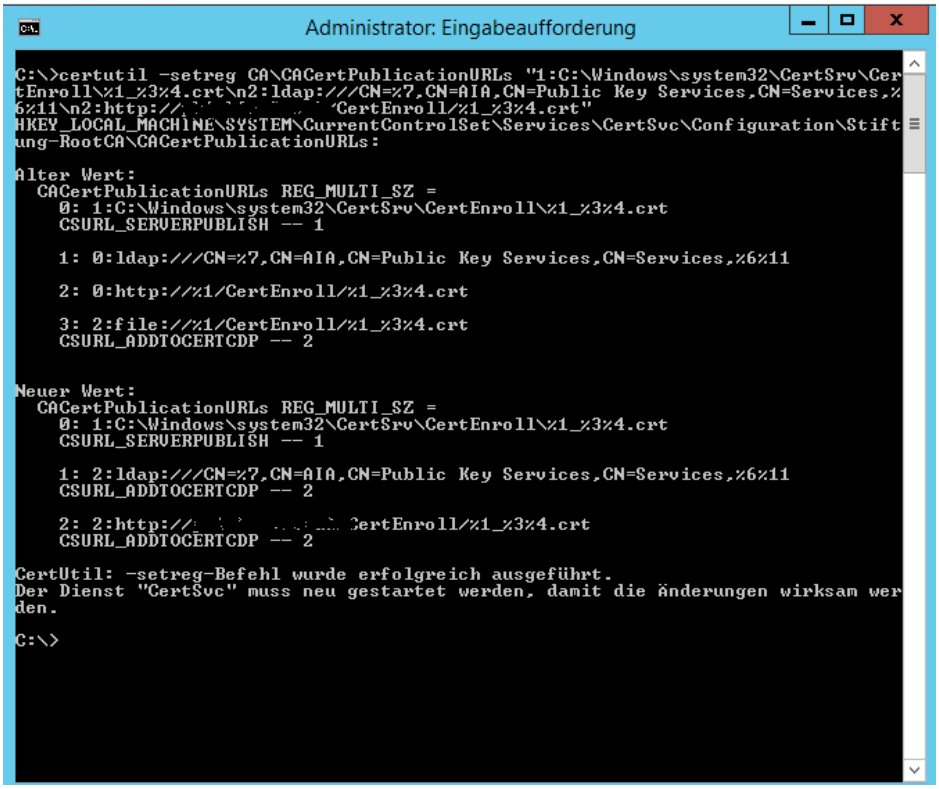

## CA Dienst neu starten

Groesse Security Event Log aendern



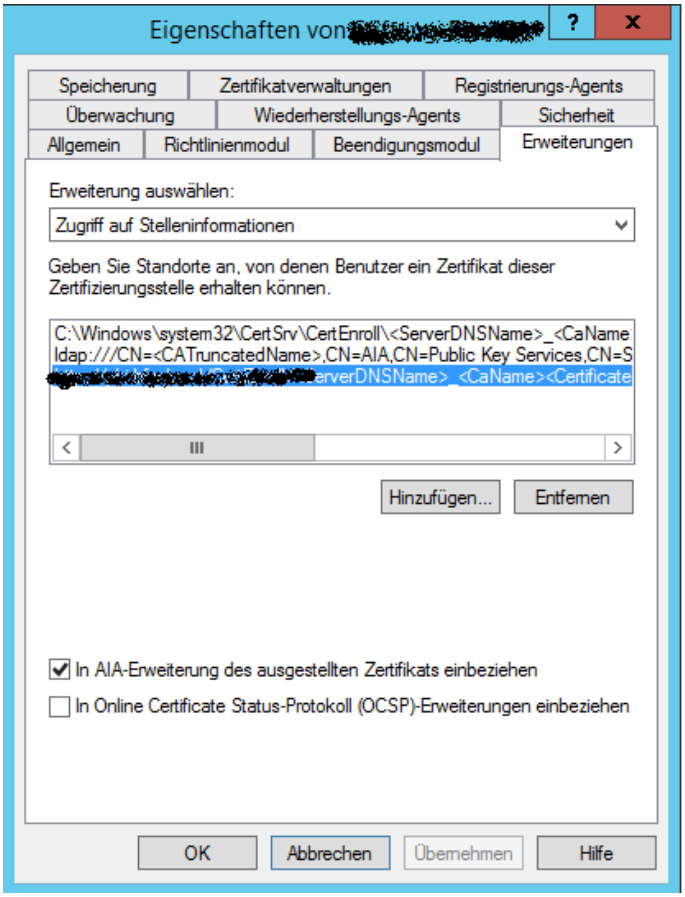

**AIA konfigurieren**

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

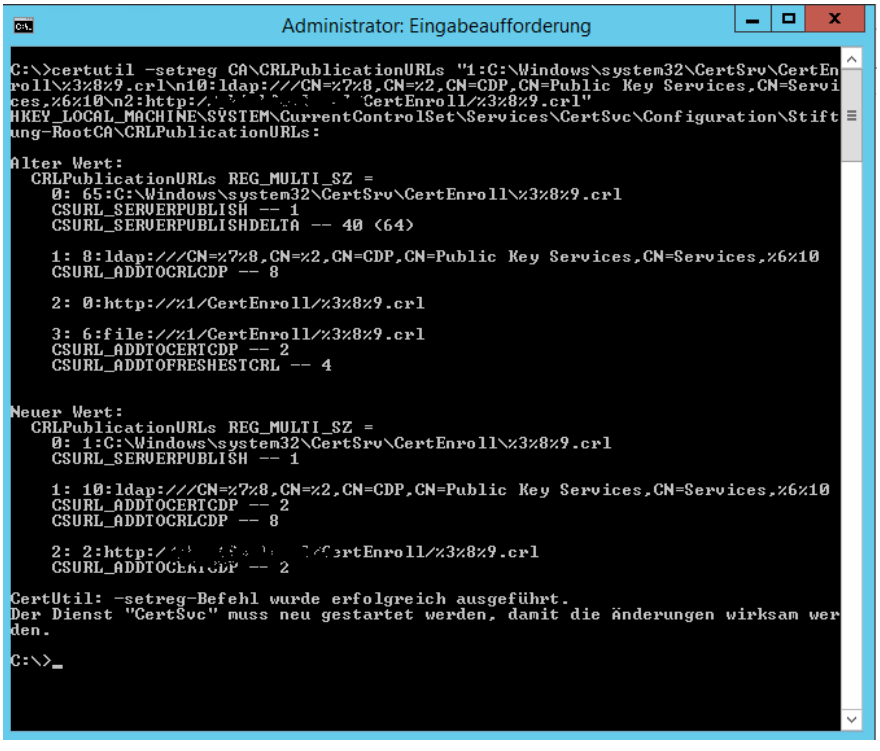



//CN=%7 wird ersetzt durch Angabe des DN zur Active Directory Konfigurations Partition. Vorher angegeben mit Certutil!

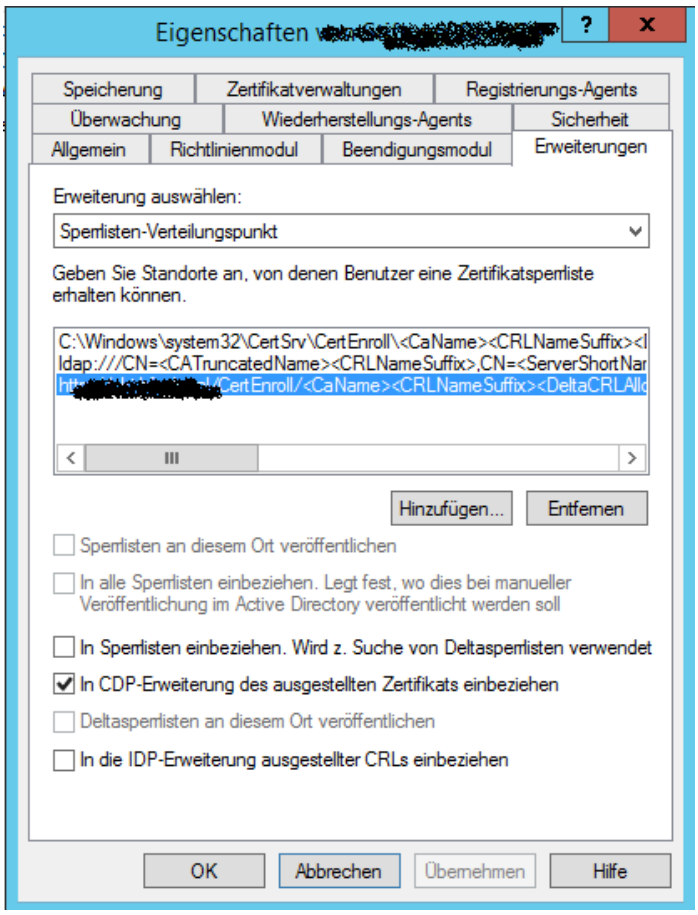
## Pruefen




CDP anpassen



Pruefen

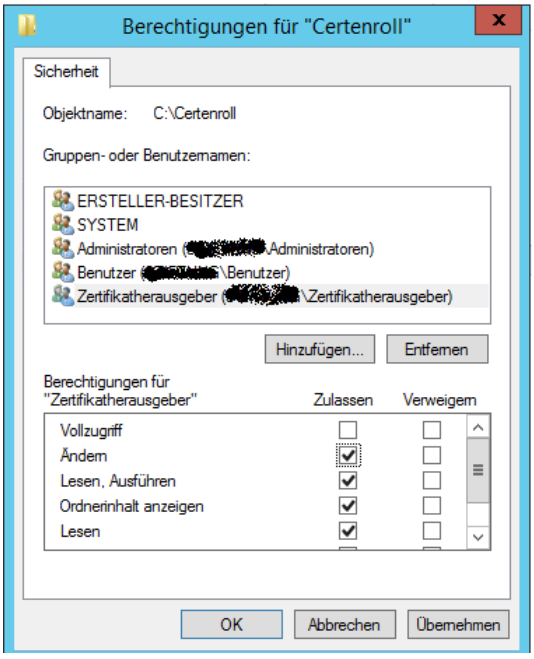



**Webserver fuer den CRL Distribution Point erstellen**

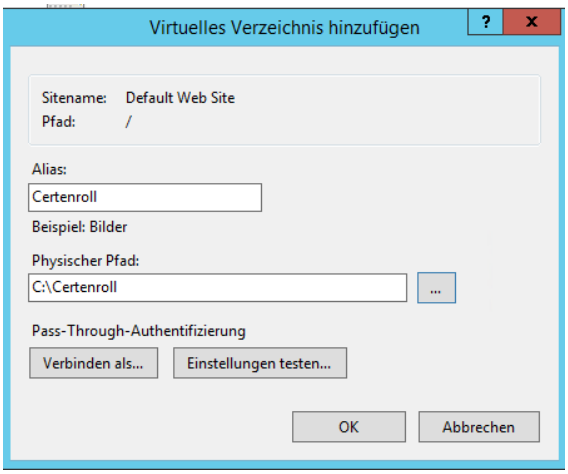
IIS auf dafuer designierten Webserver installieren

Verzeichnis C:\CERTENROLL anlegen

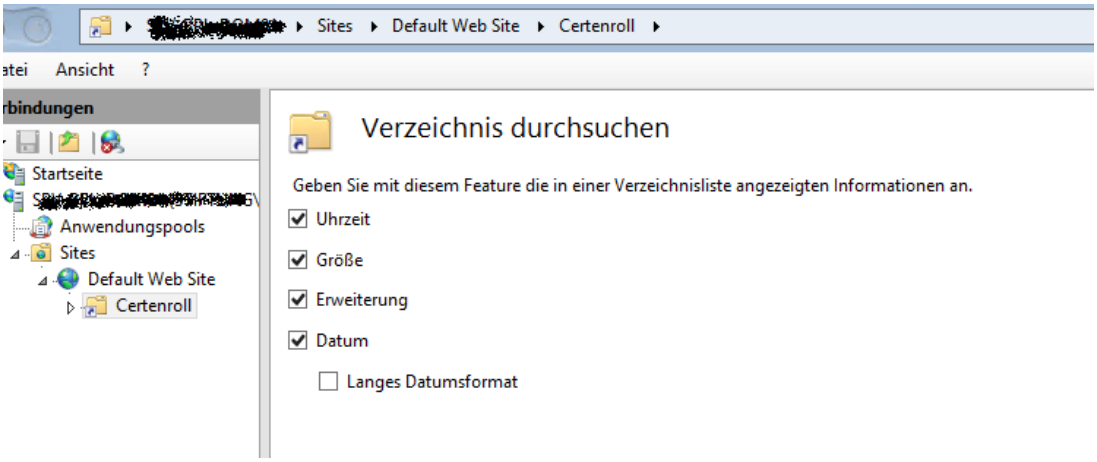
Gruppe Zertifikatherausgeber Modify Permission vergeben



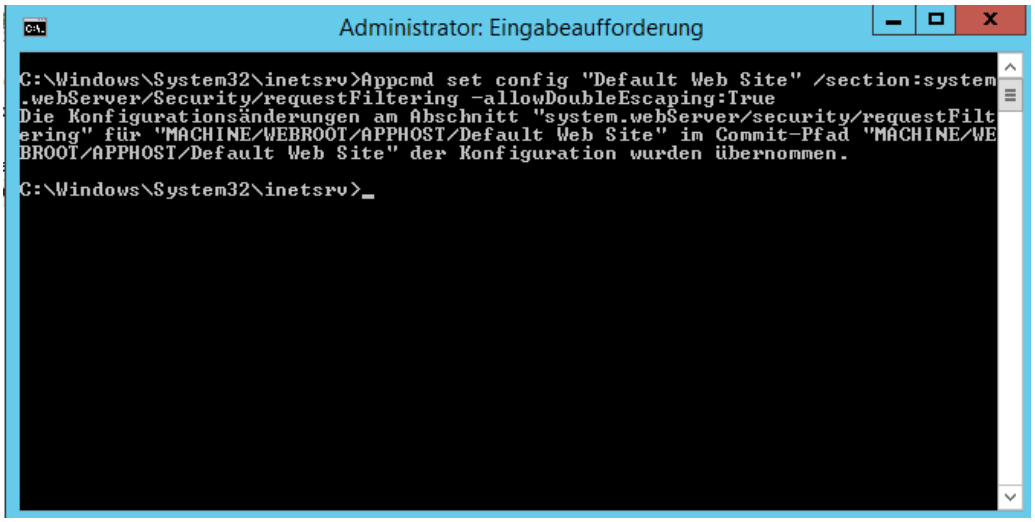
Neues virtuelles Verzeichnis CERTENROLL im IIS anlegen, Verzeichnis durchsuchen erlauben



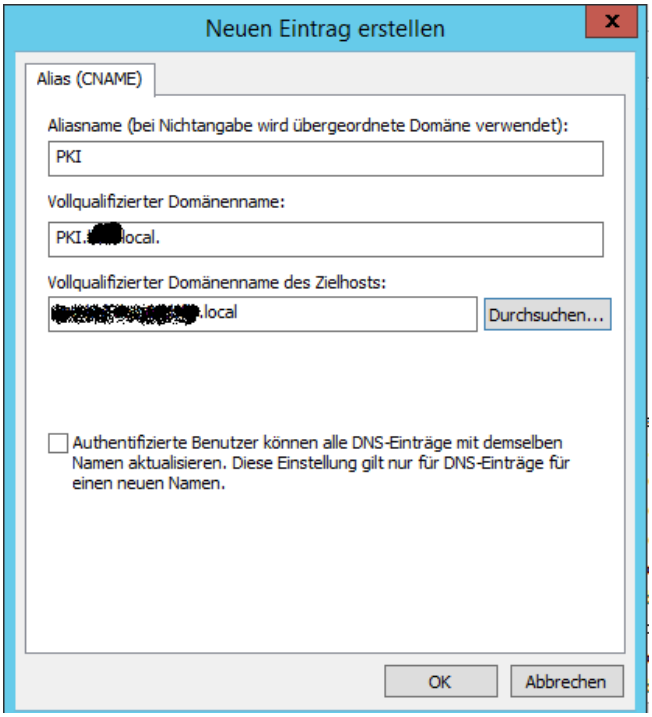

Verzeichnis freigeben mit Modify Berechtigungen fuer die Gruppe Zertifikatherausgeber



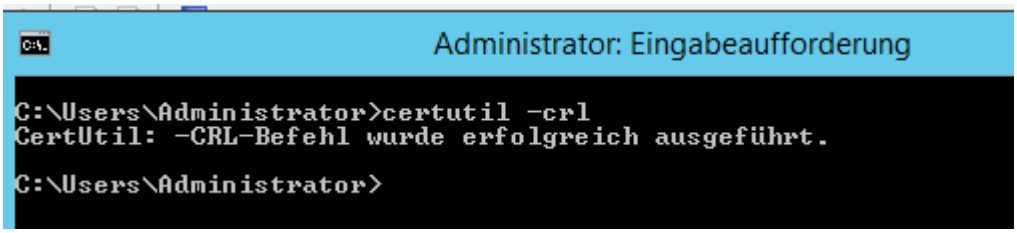

Double Escaping auf IIS Server erlauben



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




**CRL publishen**



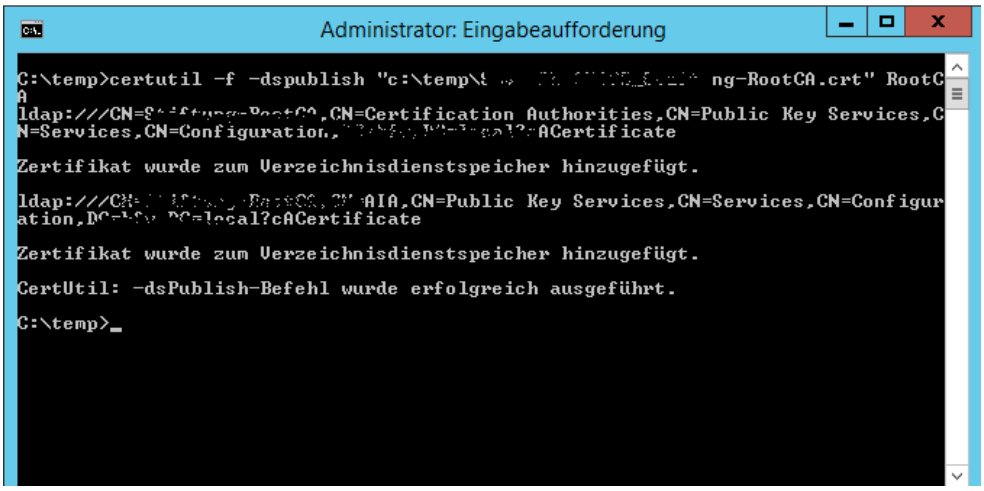

**CRL Datei auf Webserver kopieren**

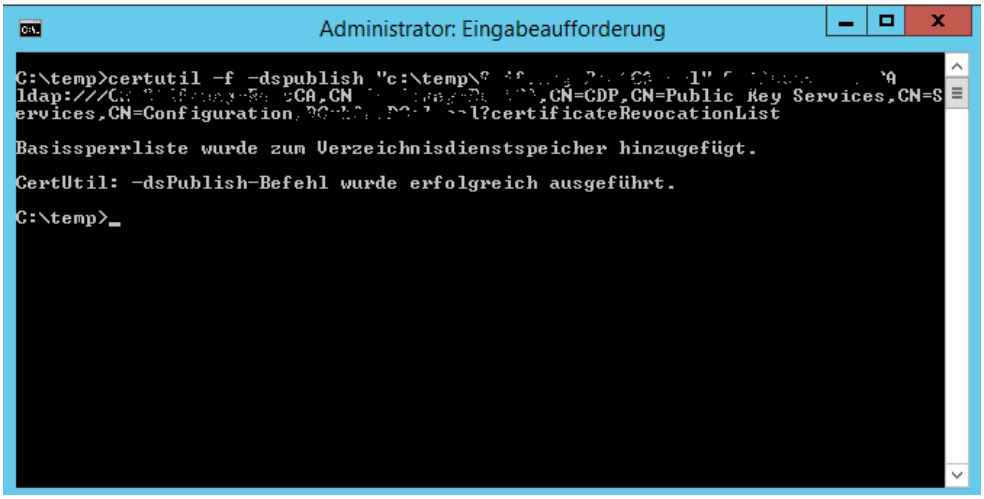
**ACHTUNG**: Dieser Prozess muss wie in diesem Beispiel alle 52 Wochen wiederholt werden und dazu die Offline CA eingeschaltet werden

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

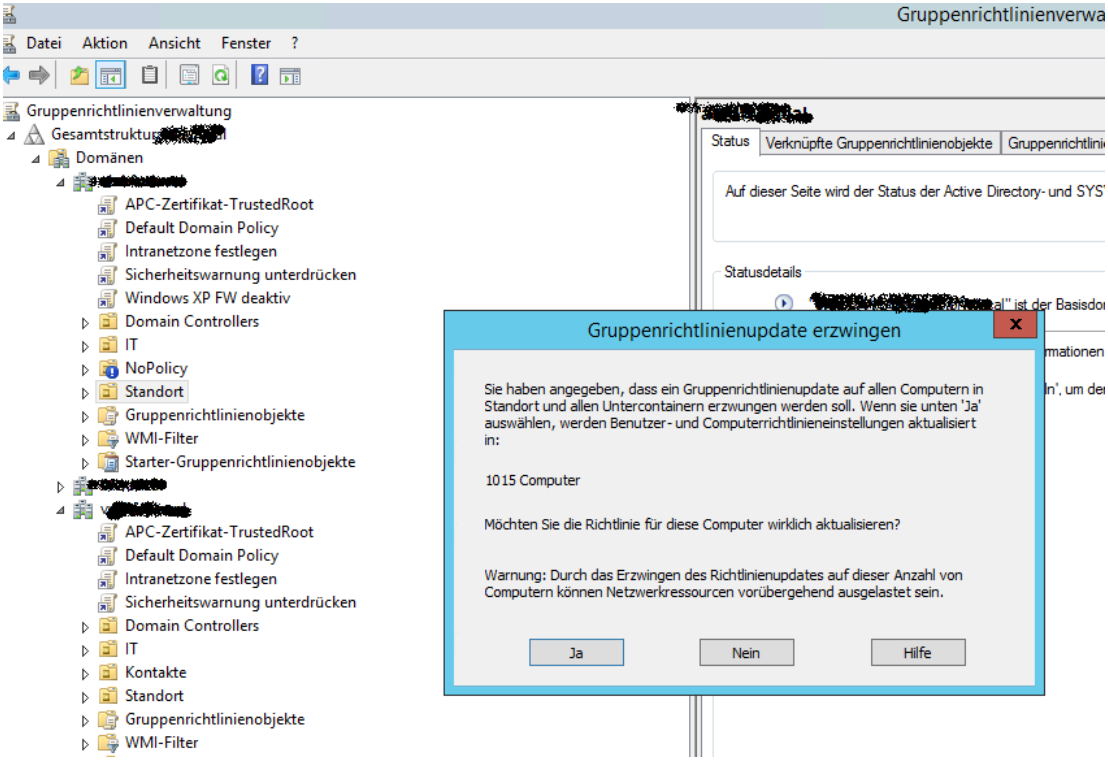
**CA Cert verteilen**

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

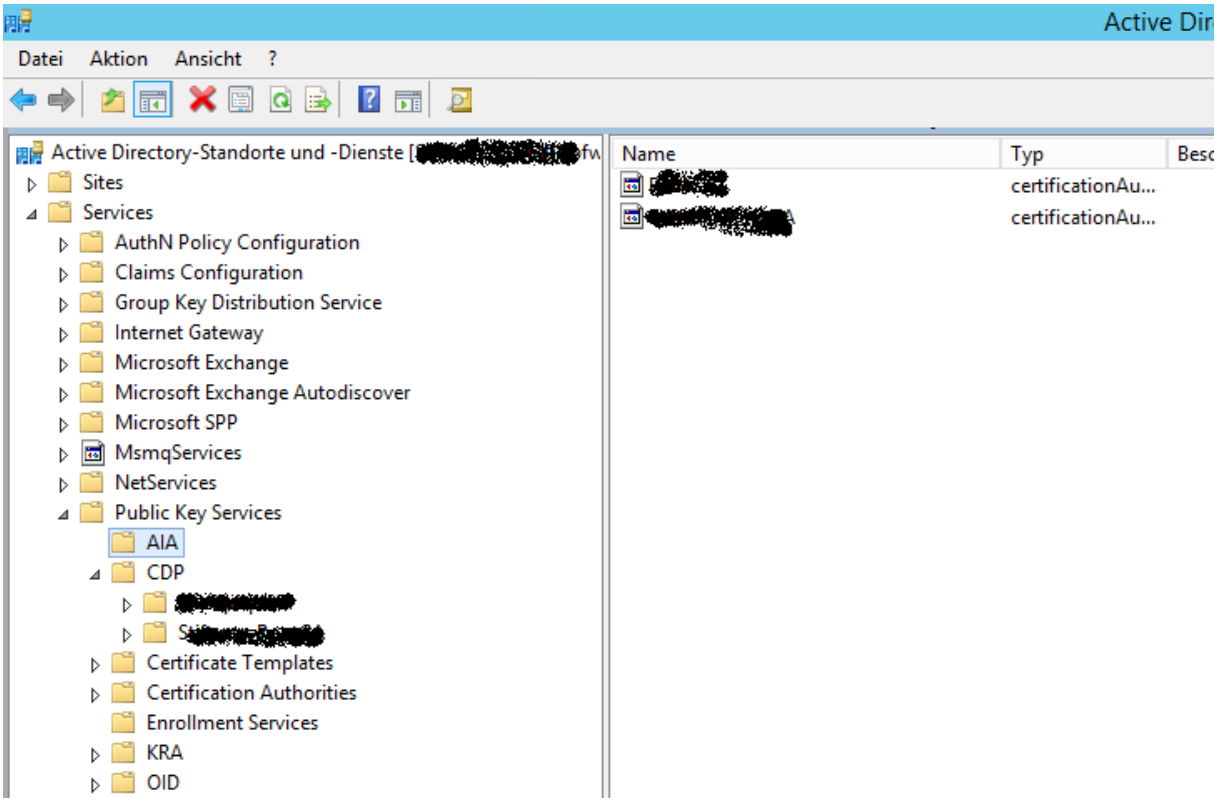


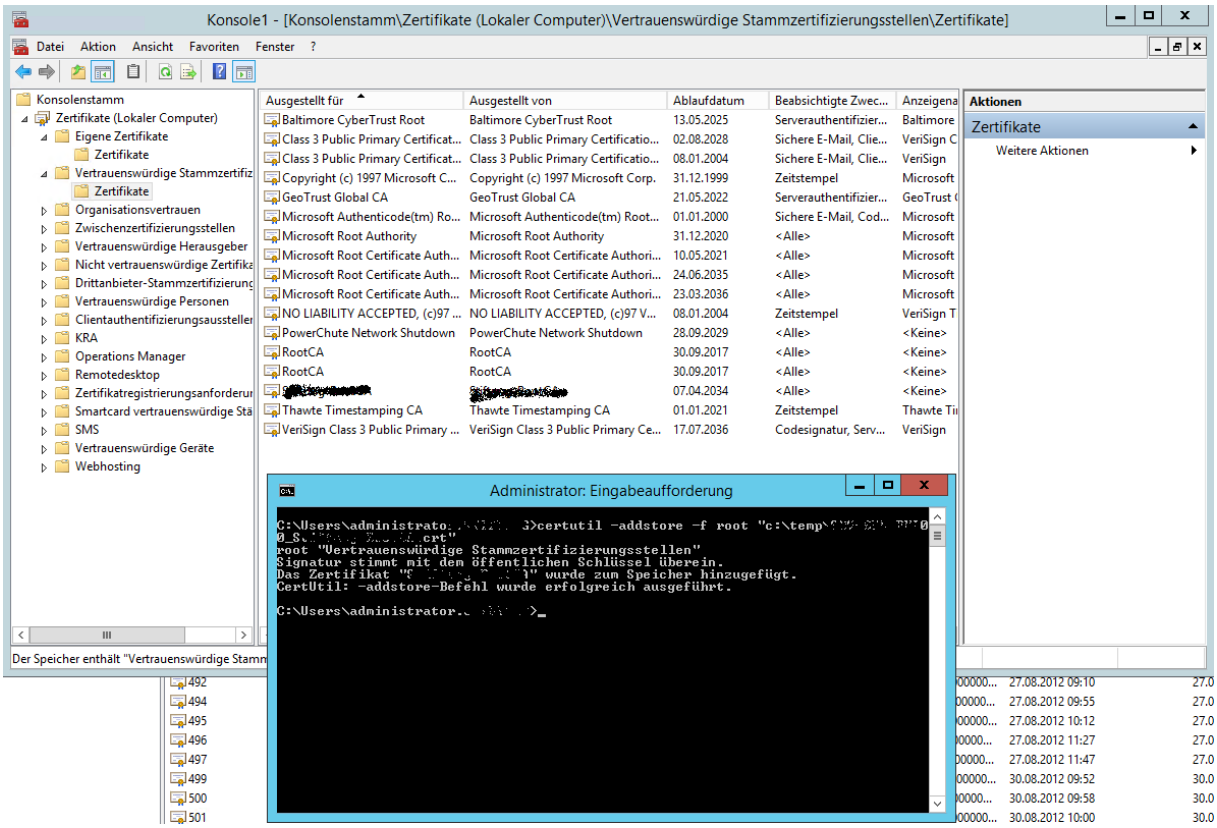

Ggfs. per Remote Group Policy Update beschleunigen

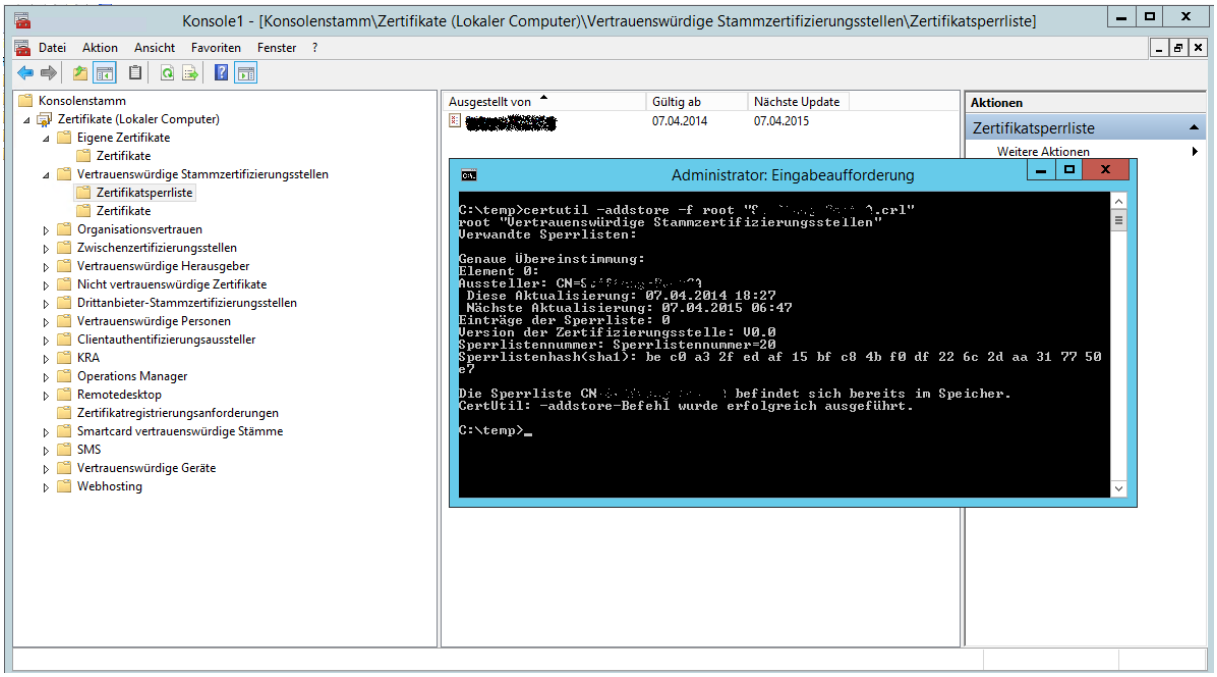


In DSSITE.MSC verifizieren

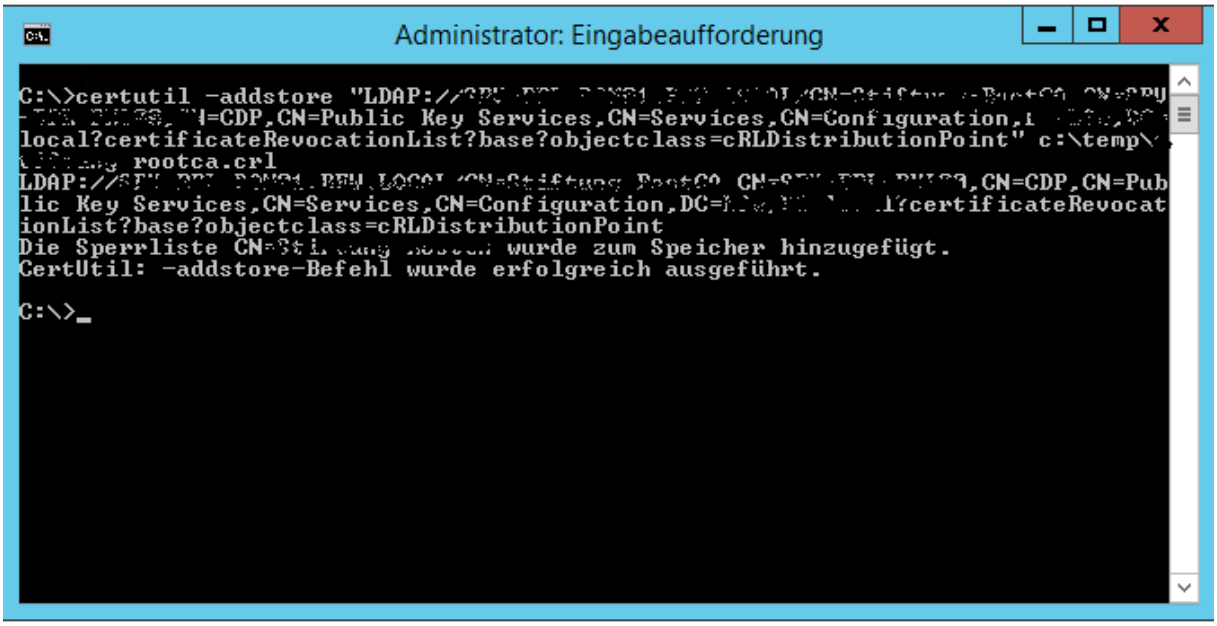



Das Offline Root CA Zertifikat in den Zertifikatspeicher der vertrauenswuerdigen Stammzertifizierungsstellen des lokalen Computers der neuen Enterprise Online Issuing CA kopieren



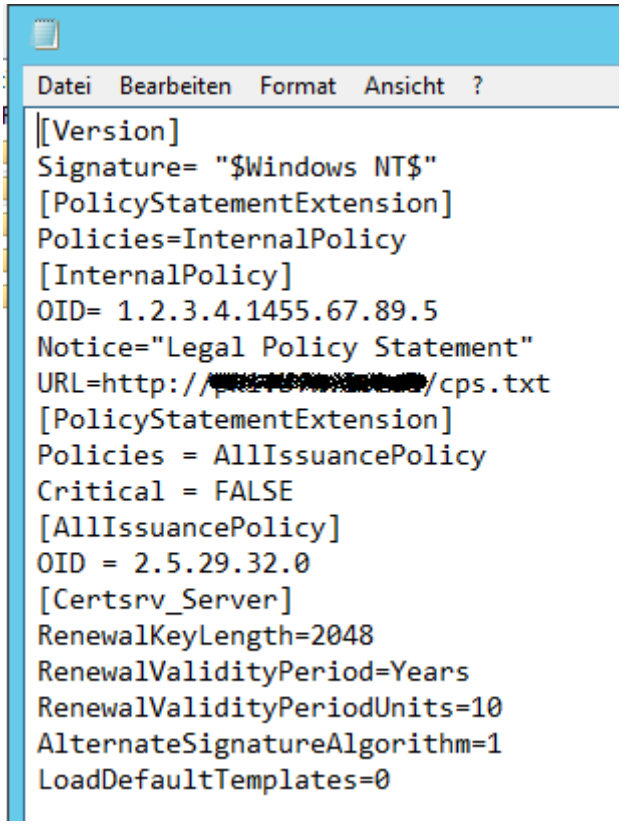



LDAP CRL publishen, da die Offline Root CA nicht Domaenenmitglied ist, kann der Prozess von einem Domaenenmitglied-PC durchgefuehrt werden

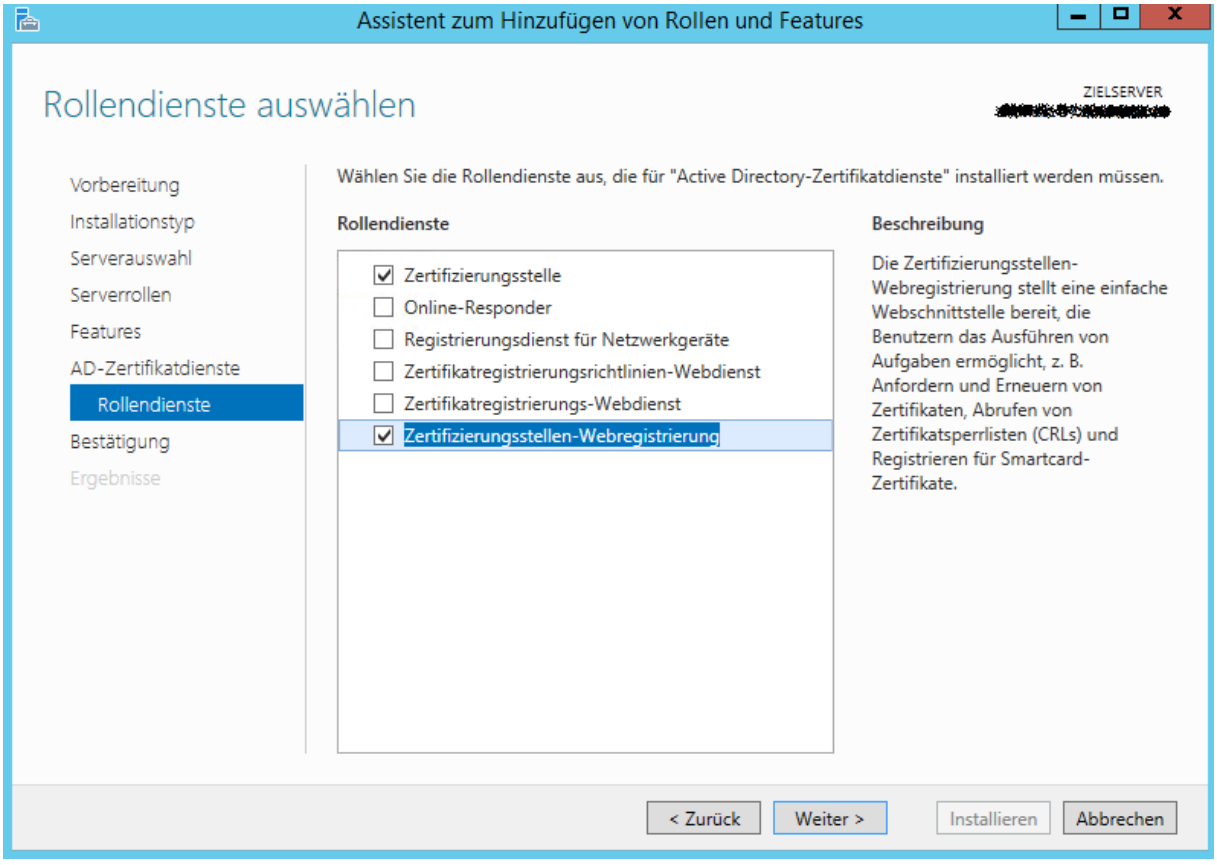


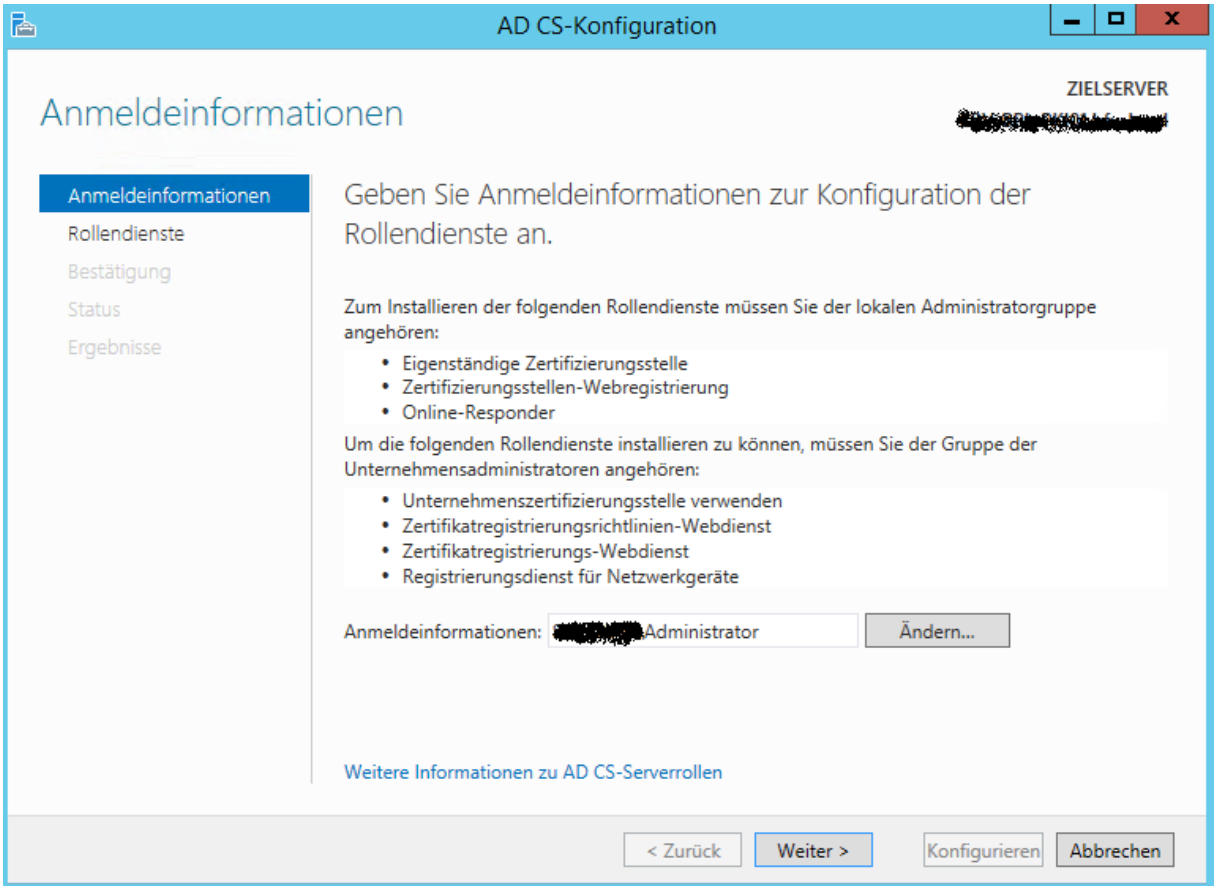
## Neue Issuing CA implementieren

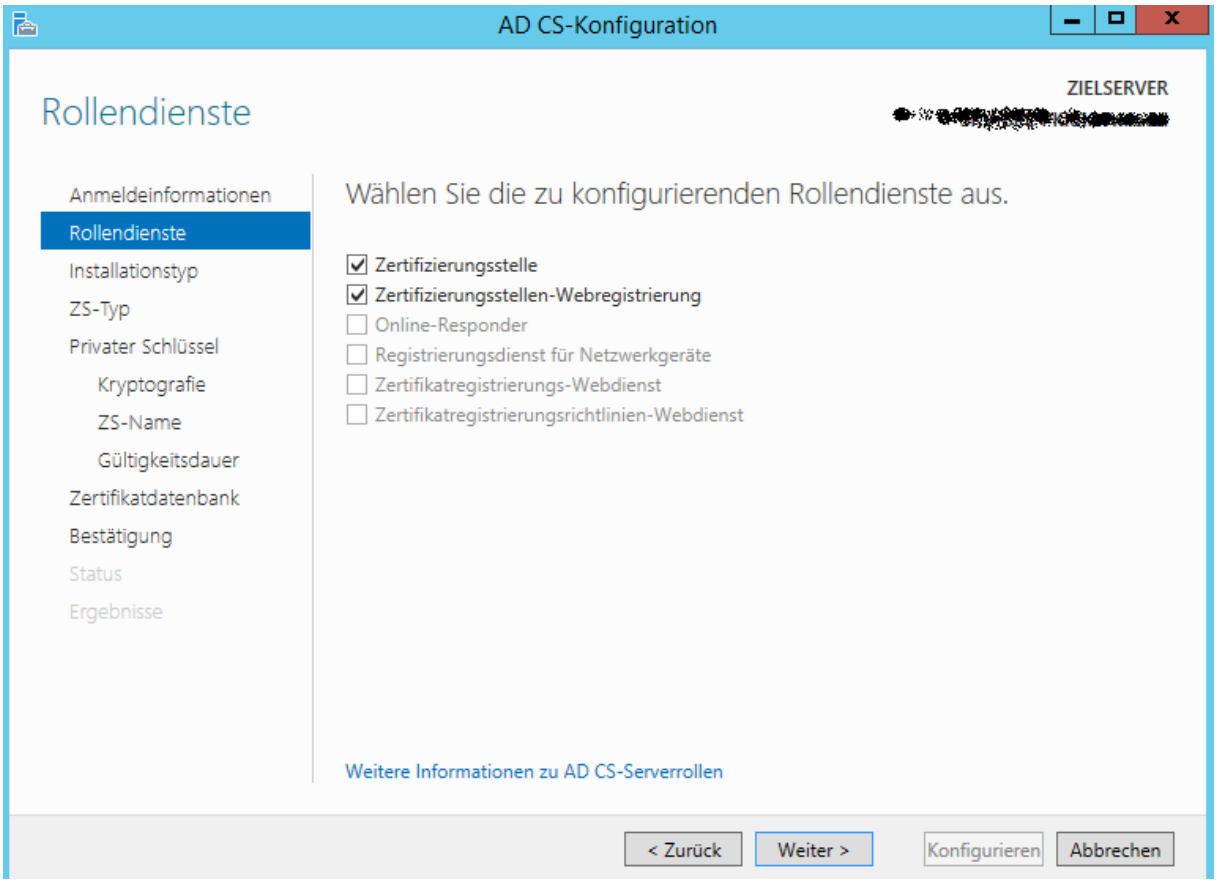
CAPolicy.inf Datei anlagen

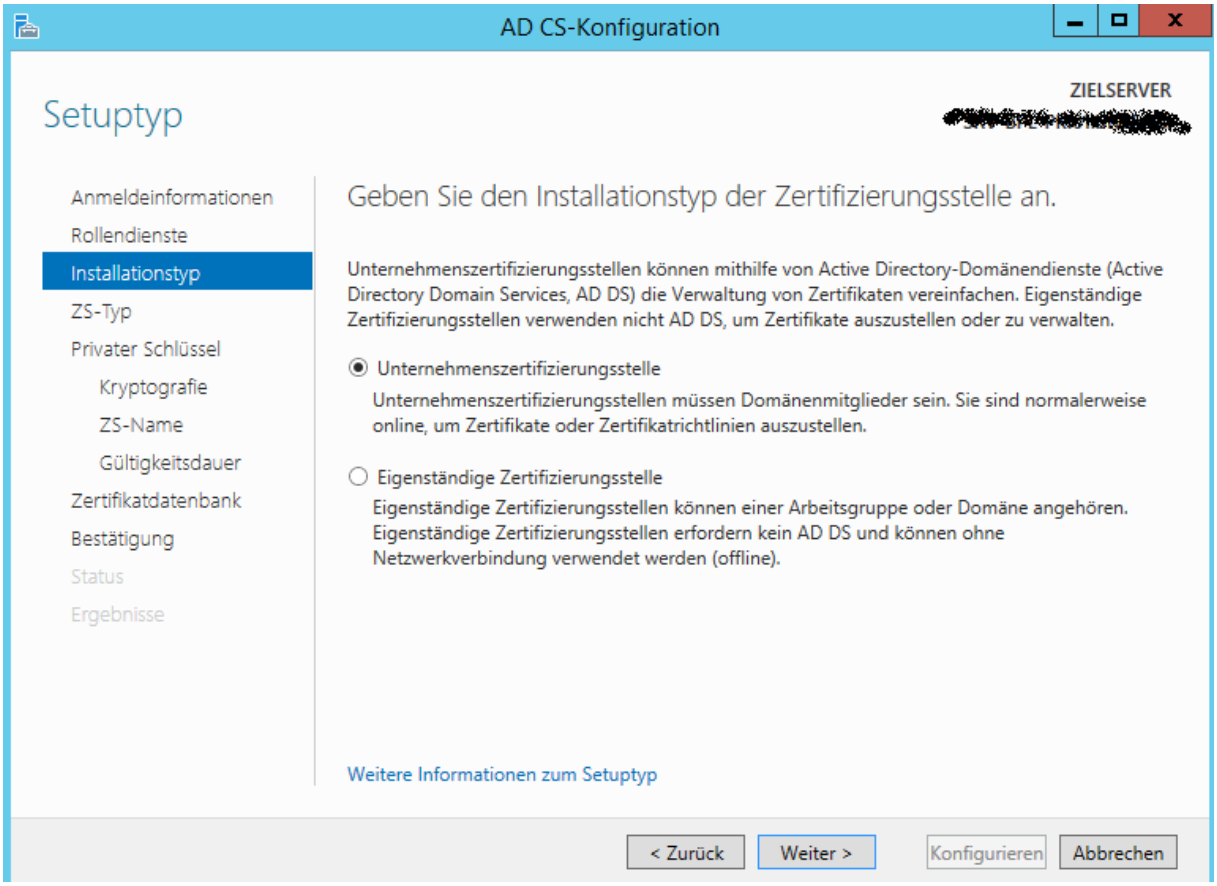


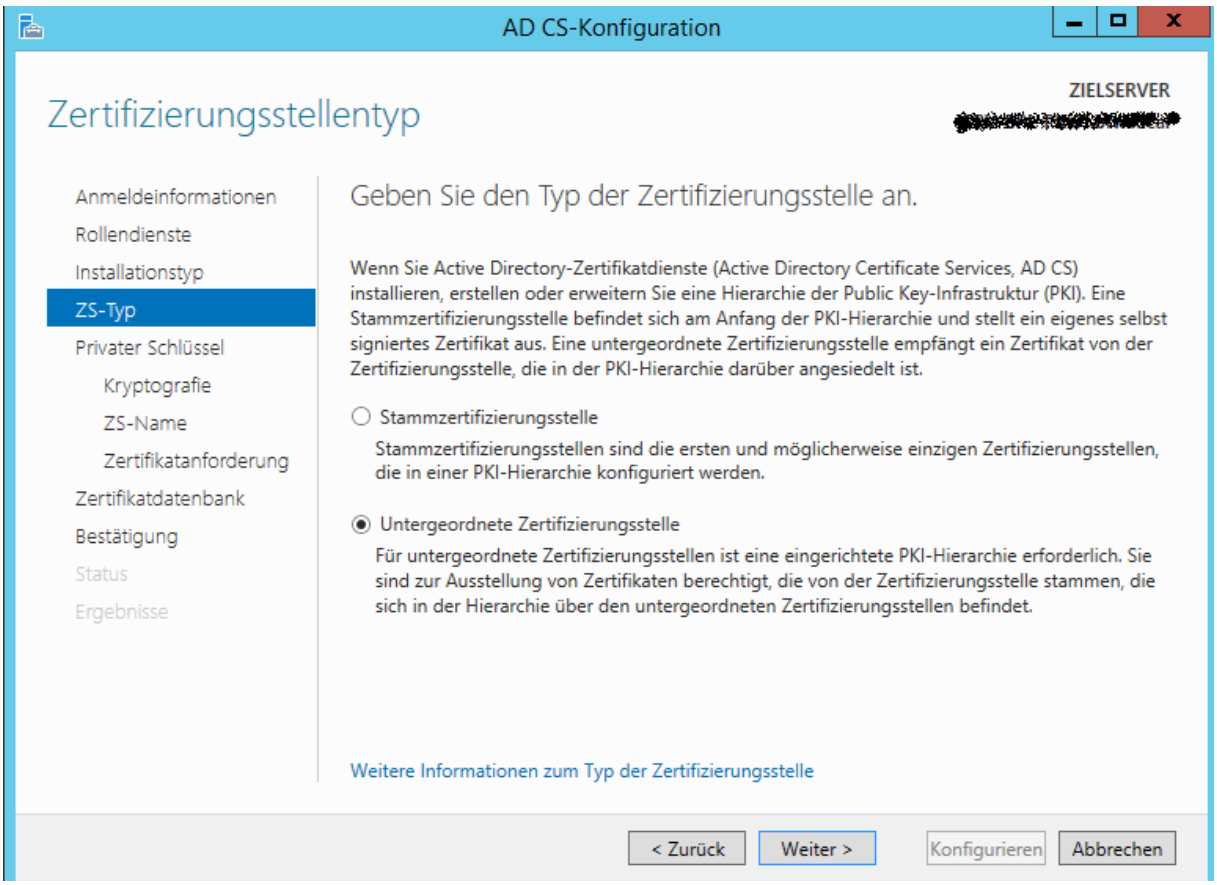

Issuing CA installieren

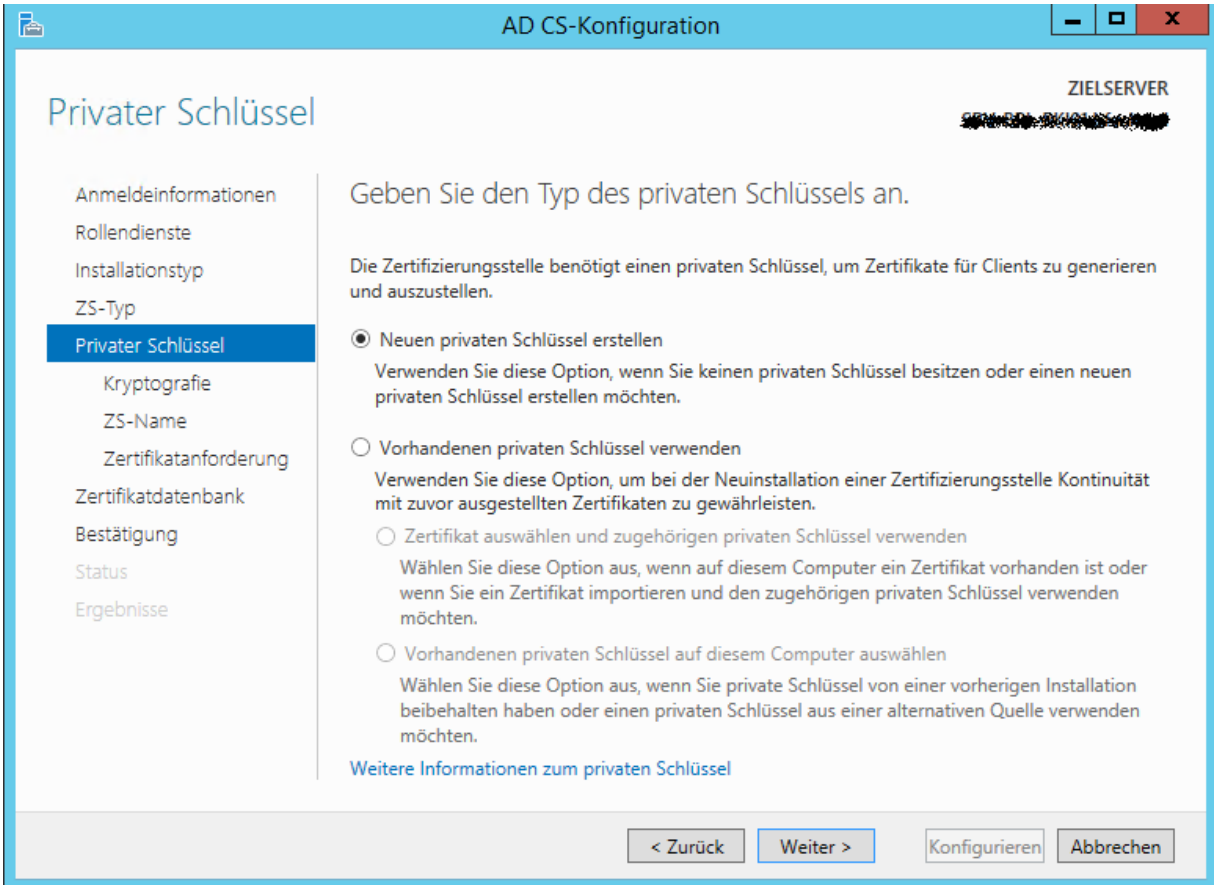


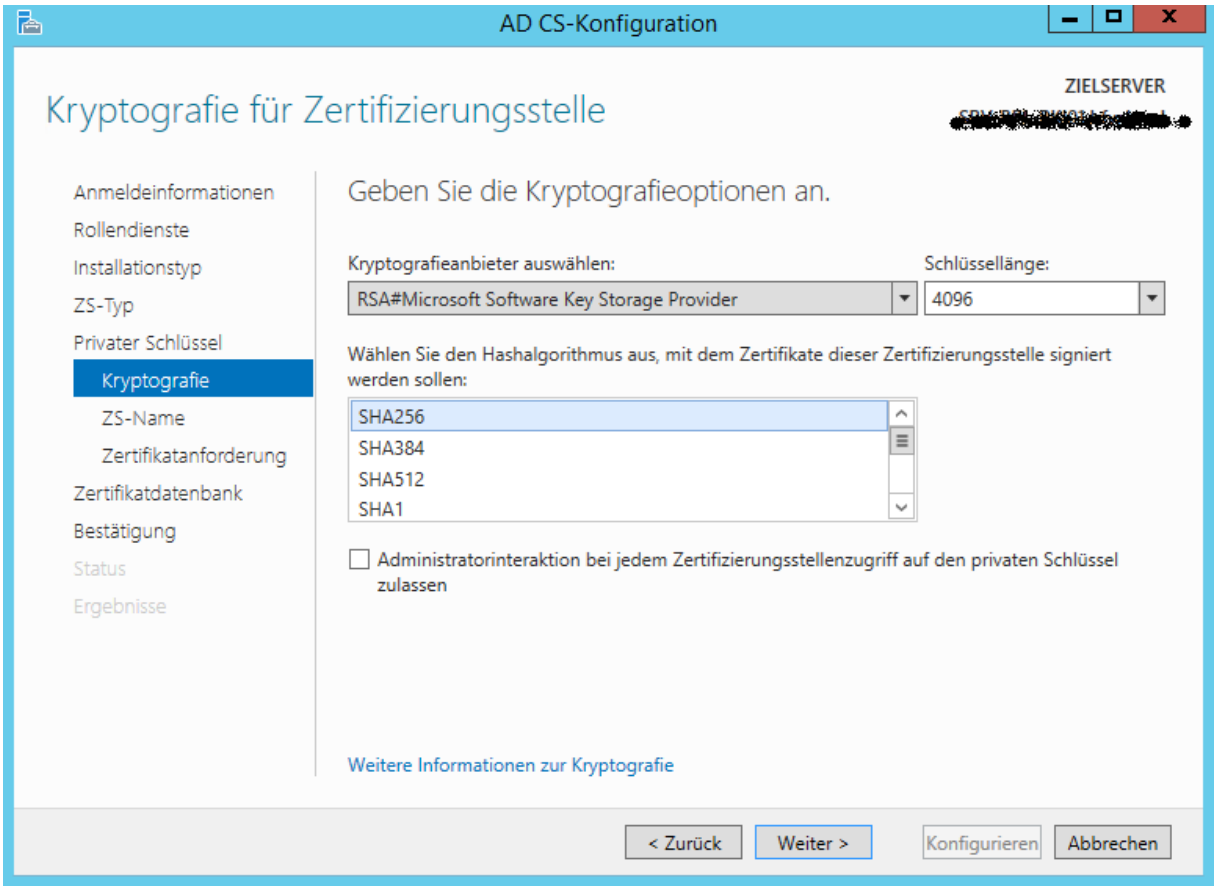

AD CS-Konfiguration
Anmeldeinformationen
ZIELSERVER
[redacted]
Anmeldeinformationen
Rollendienste
Bestätigung
Status
Ergebnisse
Geben Sie Anmeldeinformationen zur Konfiguration der Rollendienste an.
Zum Installieren der folgenden Rollendienste müssen Sie der lokalen Administratorgruppe angehören:
• Eigenständige Zertifizierungsstelle
• Zertifizierungsstellen-Webregistrierung
• Online-Responder
Um die folgenden Rollendienste installieren zu können, müssen Sie der Gruppe der Unternehmensadministratoren angehören:
• Unternehmenszertifizierungsstelle verwenden
• Zertifikatregistrierungsrichtlinien-Webdienst
• Zertifikatregistrierungs-Webdienst
• Registrierungsdienst für Netzwerkgeräte
Anmeldeinformationen: [redacted]Administrator
Ändern...
Weitere Informationen zu AD CS-Serverrollen
< Zurück
Weiter >
Konfigurieren
Abbrechen

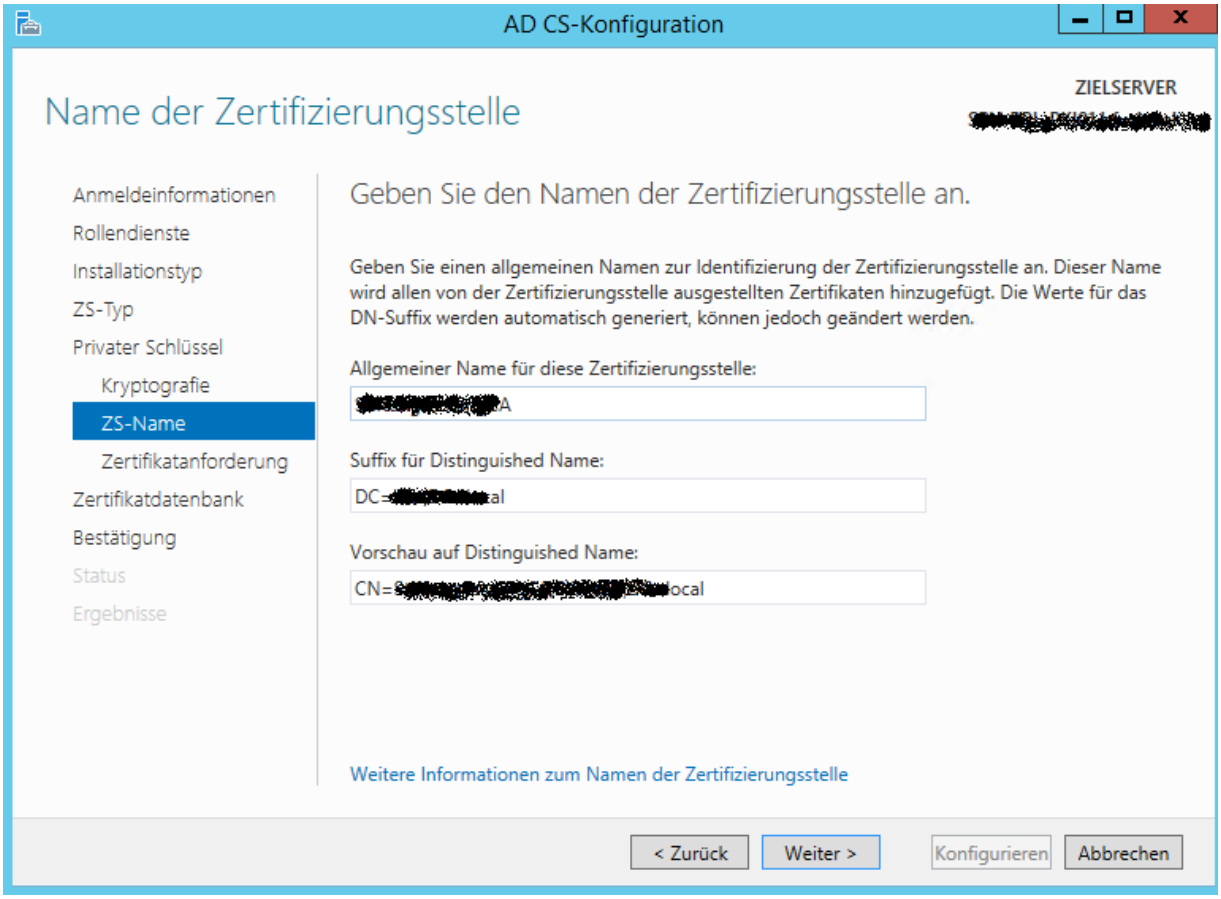

AD CS-Konfiguration
Rollendienste
ZIELSERVER
[redacted]
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Wählen Sie die zu konfigurierenden Rollendienste aus.
Zertifizierungsstelle
Zertifizierungsstellen-Webregistrierung
Online-Responder
Registrierungsdienst für Netzwerkgeräte
Zertifikatregistrierungs-Webdienst
Zertifikatregistrierungsrichtlinien-Webdienst
Weitere Informationen zu AD CS-Serverrollen
< Zurück
Weiter >
Konfigurieren
Abbrechen

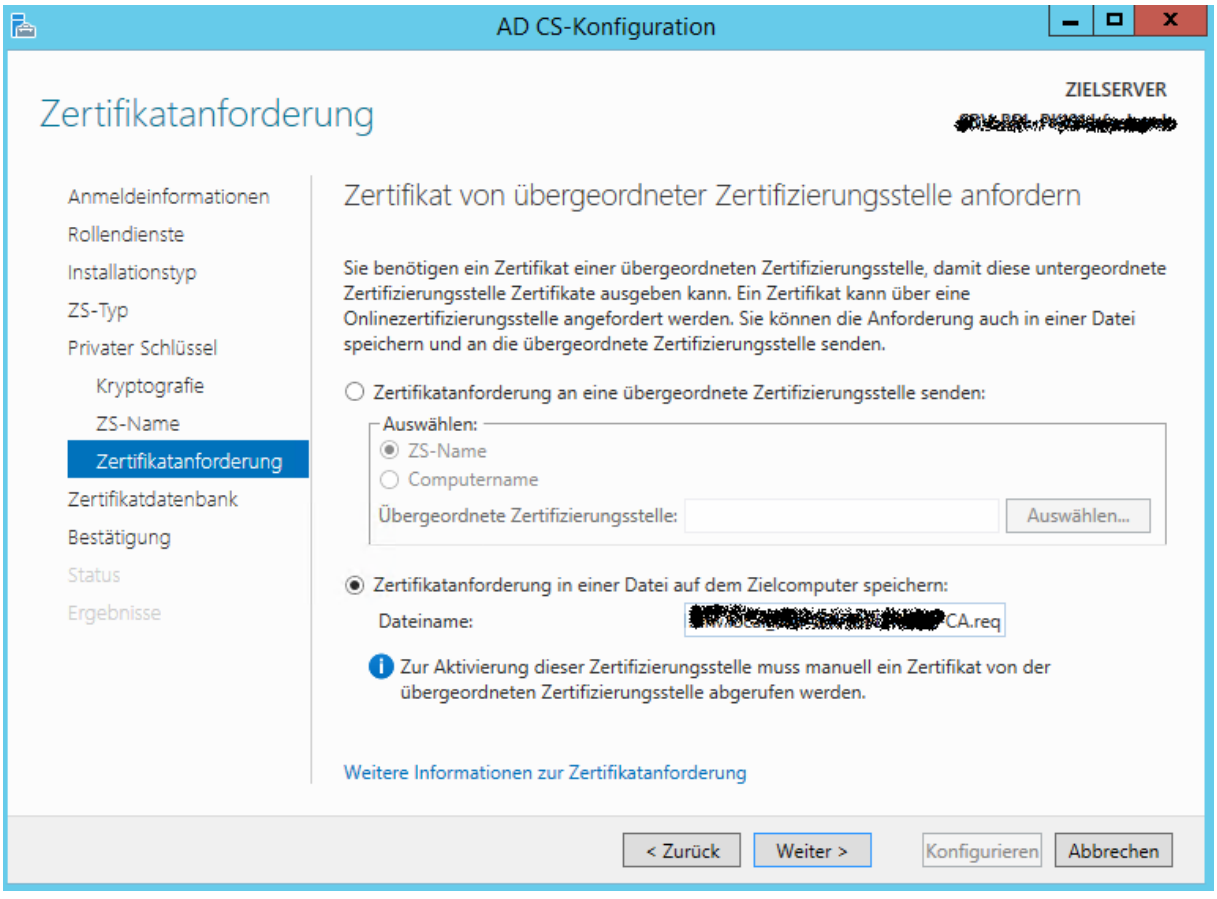

AD CS-Konfiguration
Setuptyp
ZIELSERVER
[redacted]
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Geben Sie den Installationstyp der Zertifizierungsstelle an.
Unternehmenszertifizierungsstellen 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

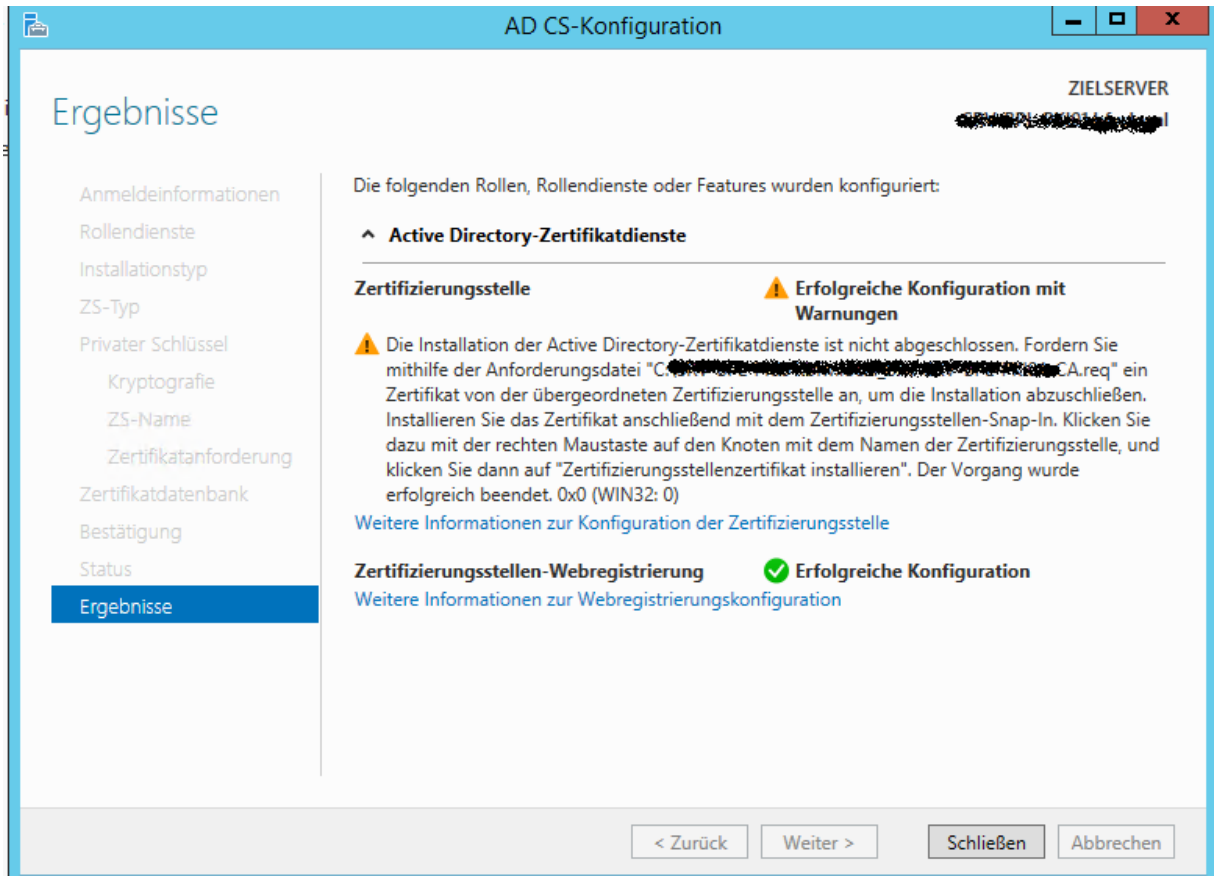

AD CS-Konfiguration
Zertifizierungsstellentyp
ZIELSERVER
[redacted]
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Zertifikatanforderung
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Geben Sie den Typ der Zertifizierungsstelle an.
Wenn Sie Active 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
< Zurück
Weiter >
Konfigurieren
Abbrechen


AD CS-Konfiguration
Privater Schlüssel
ZIELSERVER
[redacted]
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Zertifikatanforderung
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Geben Sie den Typ des privaten Schlüssels an.
Die Zertifizierungsstelle benötigt einen privaten Schlüssel, um Zertifikate für Clients zu generieren und auszustellen.
Neuen privaten Schlüssel erstellen
Verwenden Sie diese Option, wenn Sie keinen privaten Schlüssel besitzen oder einen neuen privaten Schlüssel erstellen möchten.
Vorhandenen privaten Schlüssel verwenden
Verwenden Sie diese Option, um bei der Neuinstallation einer Zertifizierungsstelle Kontinuität mit zuvor ausgestellten Zertifikaten zu gewährleisten.
Zertifikat auswählen und zugehörigen privaten Schlüssel verwenden
Wählen Sie diese Option aus, wenn auf diesem Computer ein Zertifikat vorhanden ist oder wenn Sie ein Zertifikat importieren und den zugehörigen privaten Schlüssel verwenden möchten.
Vorhandenen privaten Schlüssel auf diesem Computer auswählen
Wählen Sie diese Option aus, wenn Sie private Schlüssel von einer vorherigen Installation beibehalten haben oder einen privaten Schlüssel aus einer alternativen Quelle verwenden möchten.
Weitere Informationen zum privaten Schlüssel
< Zurück
Weiter >
Konfigurieren
Abbrechen


AD CS-Konfiguration
Kryptografie für Zertifizierungsstelle
ZIELSERVER
[redacted]
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Zertifikatanforderung
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

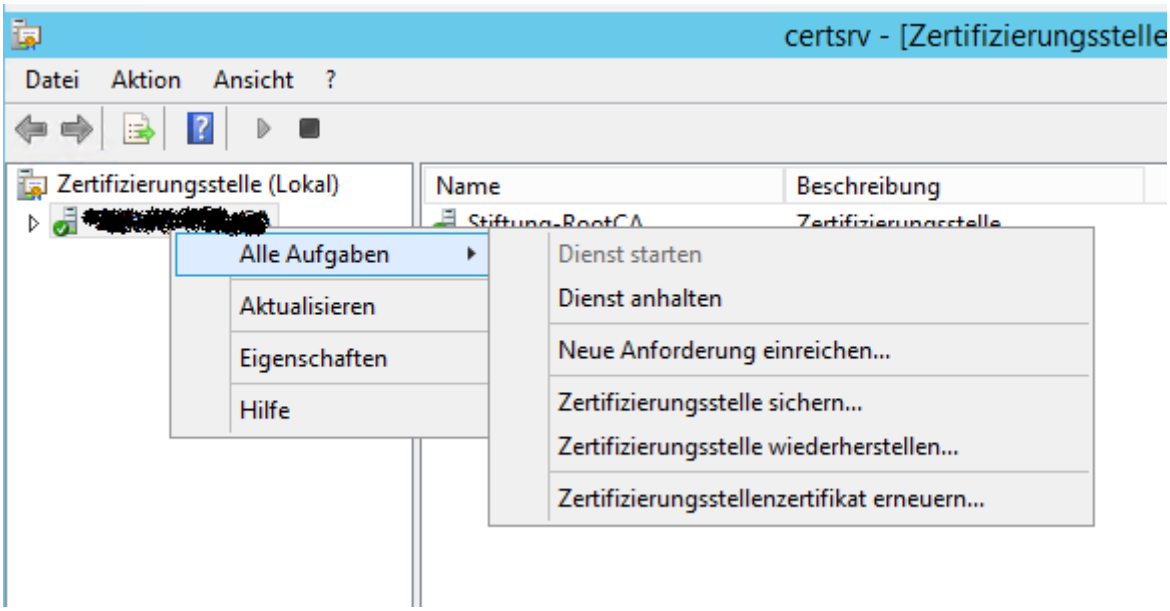

AD CS-Konfiguration
Name der Zertifizierungsstelle
ZIELSERVER
[redacted]
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Zertifikatanforderung
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Geben Sie den Namen der Zertifizierungsstelle an.
Geben Sie 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]A
Suffix für Distinguished Name:
DC=[redacted]al
Vorschau auf Distinguished Name:
CN=[redacted]ocal
Weitere Informationen zum Namen der Zertifizierungsstelle
< Zurück
Weiter >
Konfigurieren
Abbrechen


AD CS-Konfiguration
Zertifikatanforderung
ZIELSERVER
[redacted]
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Zertifikatanforderung
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
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:
Auswählen...
Zertifikatanforderung in einer Datei auf dem Zielcomputer speichern:
Dateiname:
[redacted]CA.req
Zur Aktivierung dieser Zertifizierungsstelle muss manuell ein Zertifikat von der übergeordneten Zertifizierungsstelle abgerufen werden.
Weitere Informationen zur Zertifikatanforderung
< Zurück
Weiter >
Konfigurieren
Abbrechen

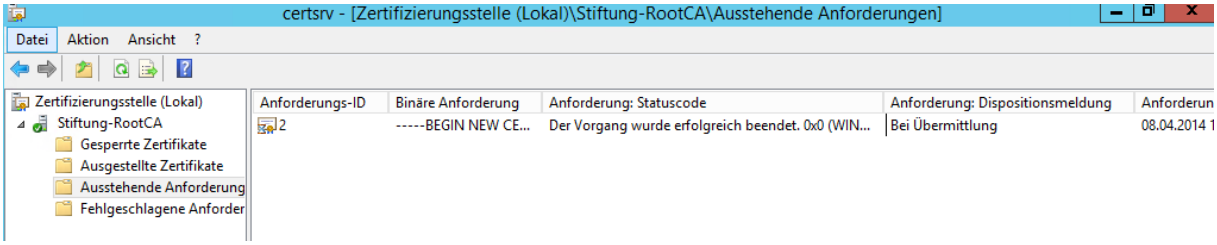



.REQ Datei zu der Offline Root CA transportieren

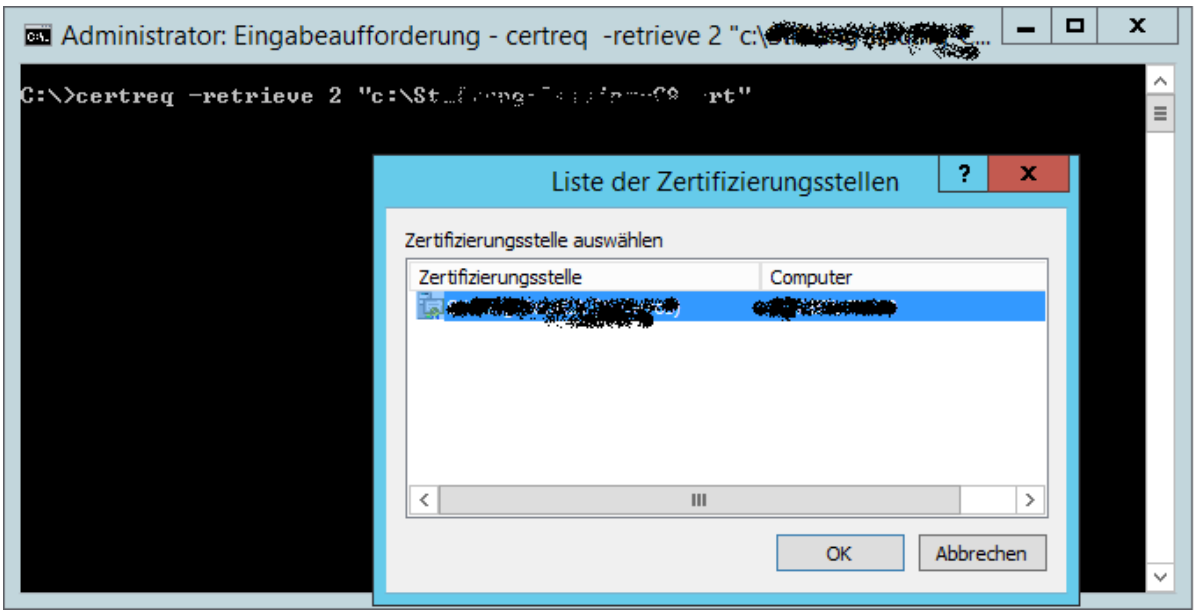
Neue Anforderung auf der Offline RootCA einreichen

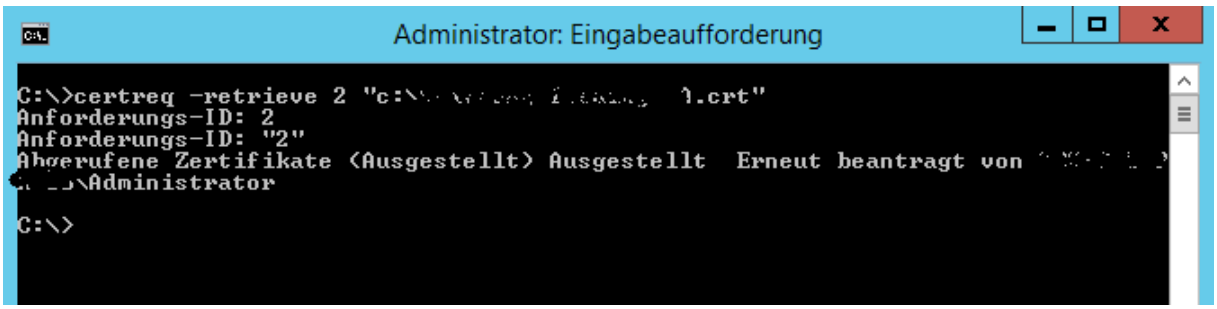


Pending Requests submitten



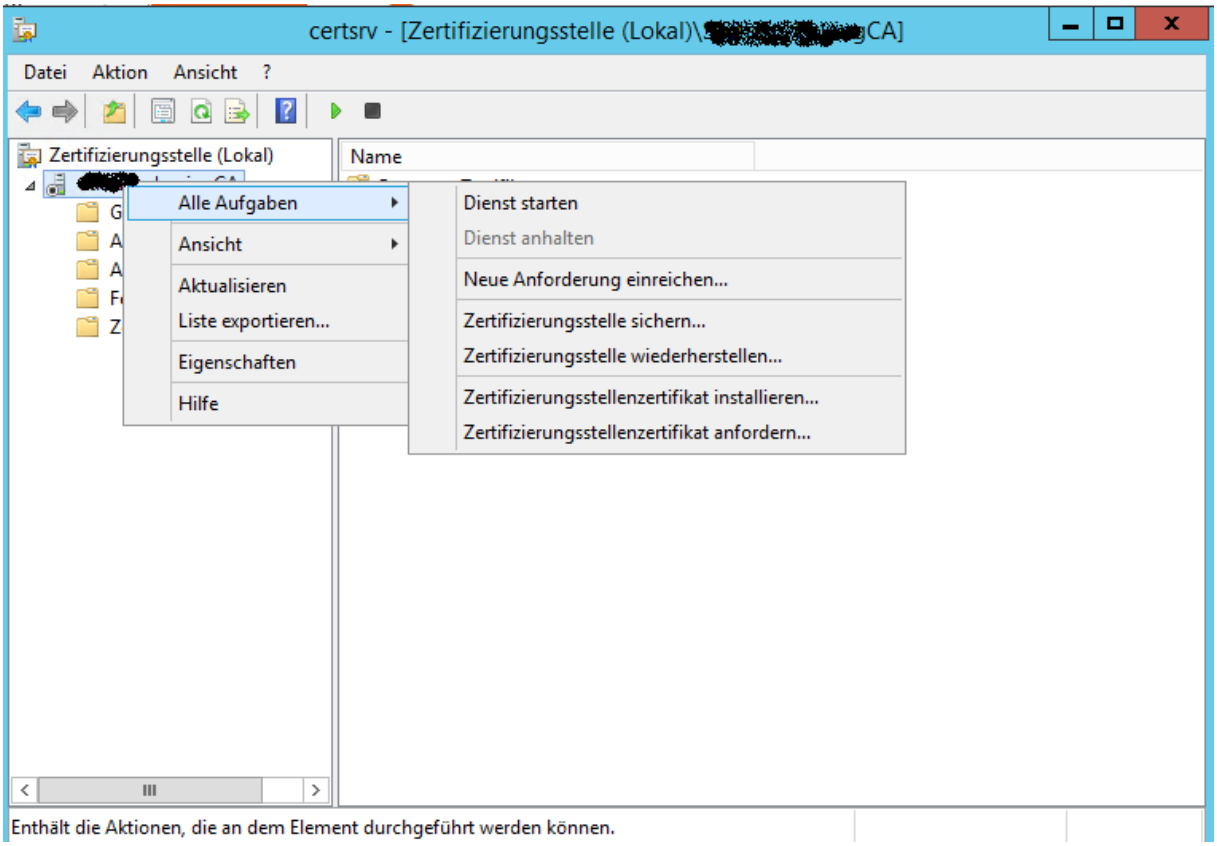

Anforderung abschliessen und .CRT Datei generieren



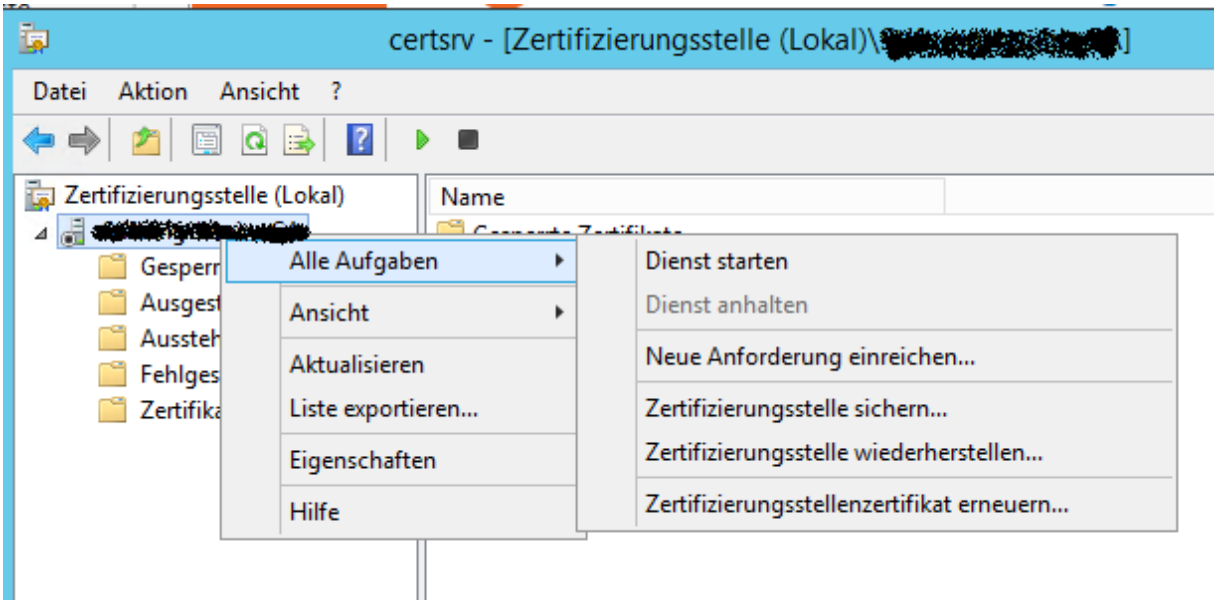




Datei zur Issuing CA transportieren

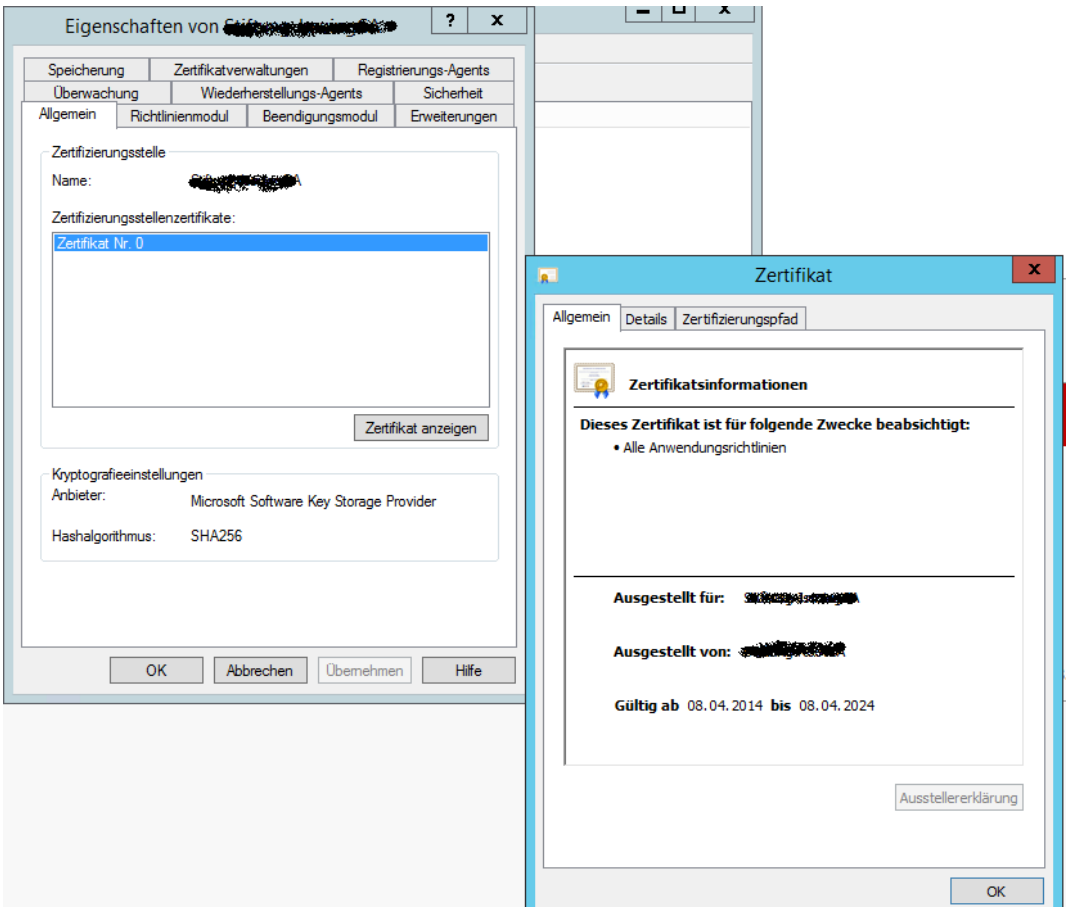
Zertifizierungsstellen Zertifikat auf Issuing CA installieren



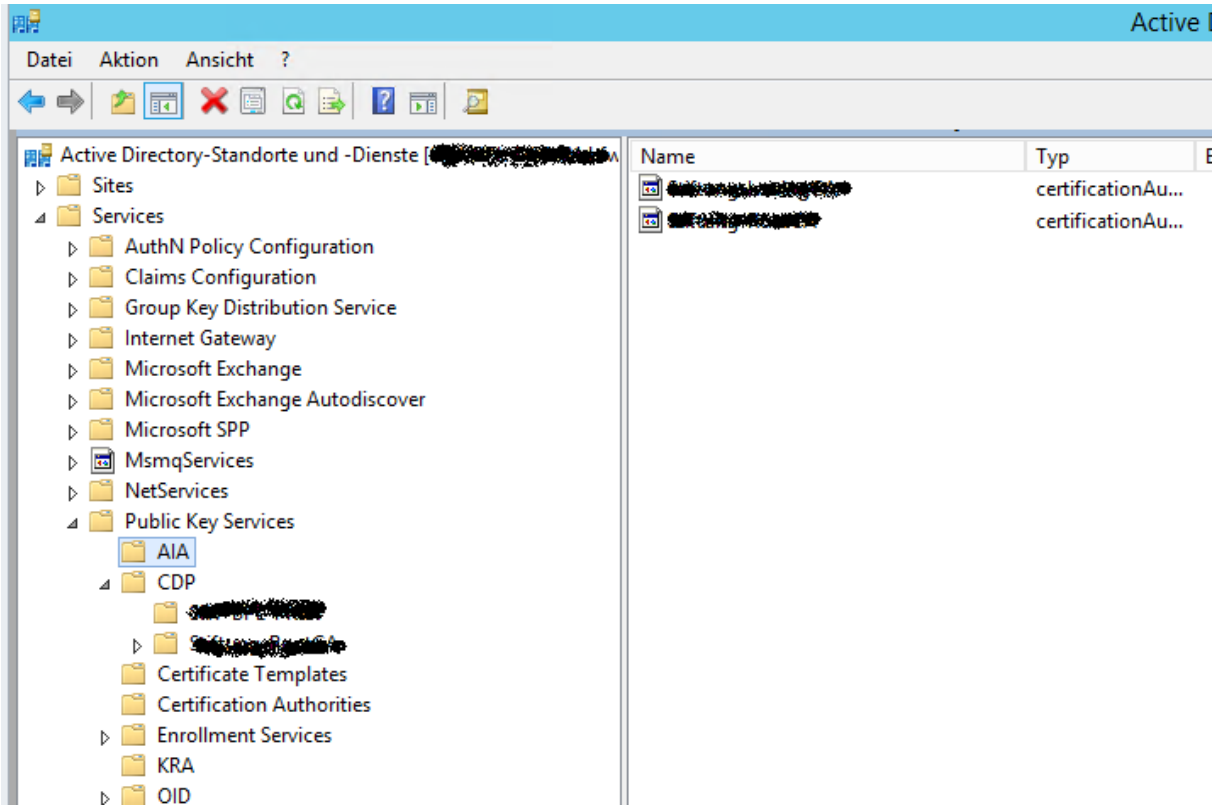

CA Dienste starten



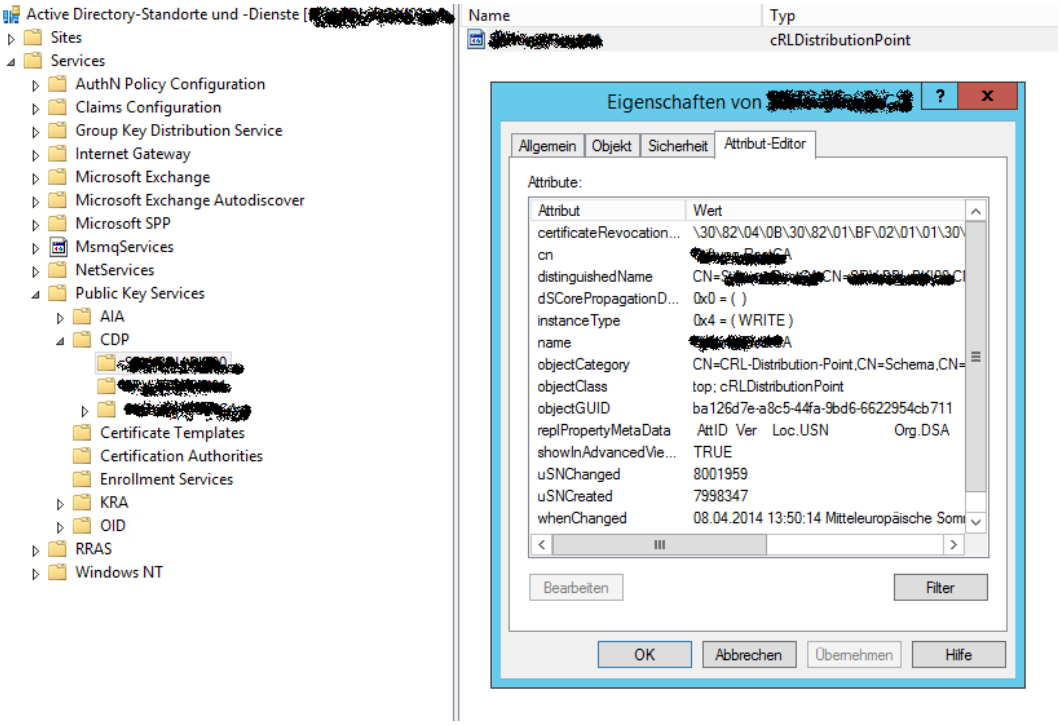
Zertifikat pruefen ob die CA Hierarchie passt und die Gueltigkeit



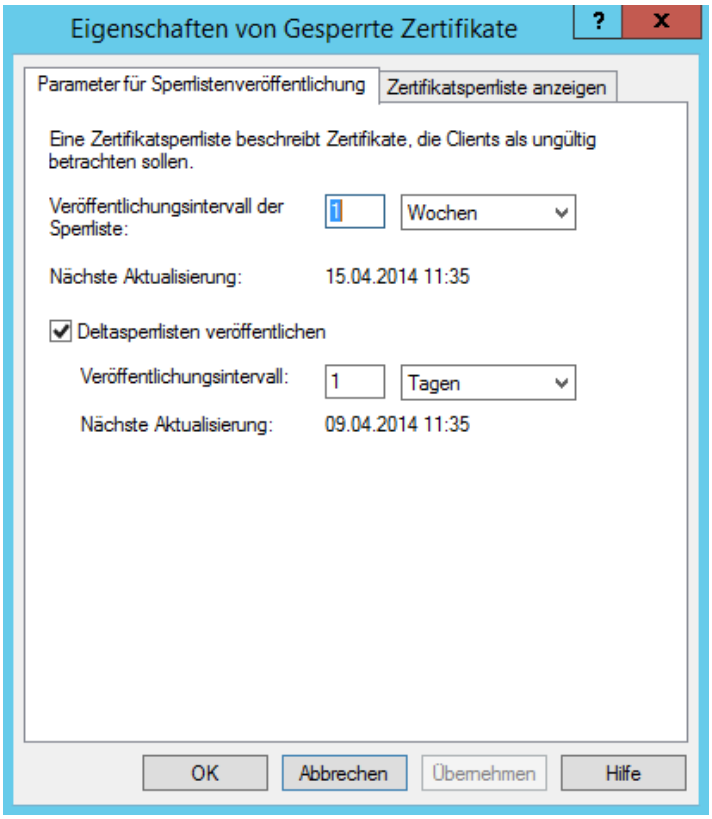

Active Directory pruefen



## CRL Attribut

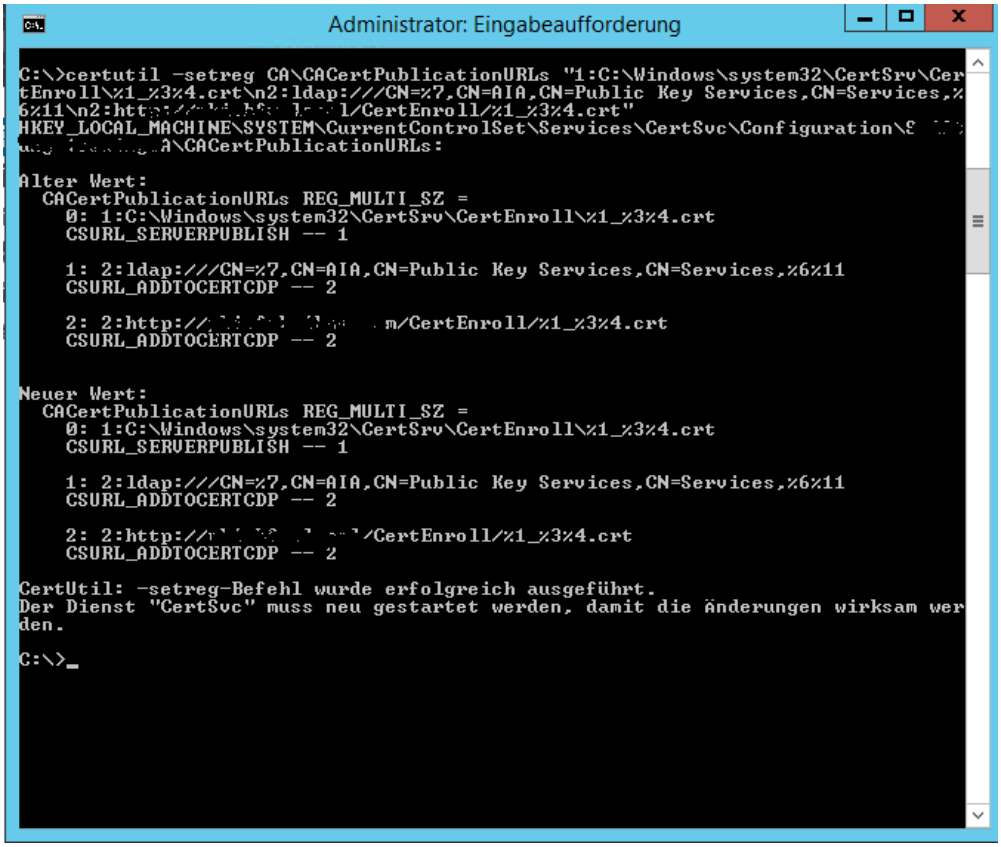



## Sperrlistenveroeffentlichungsintervall anpassen

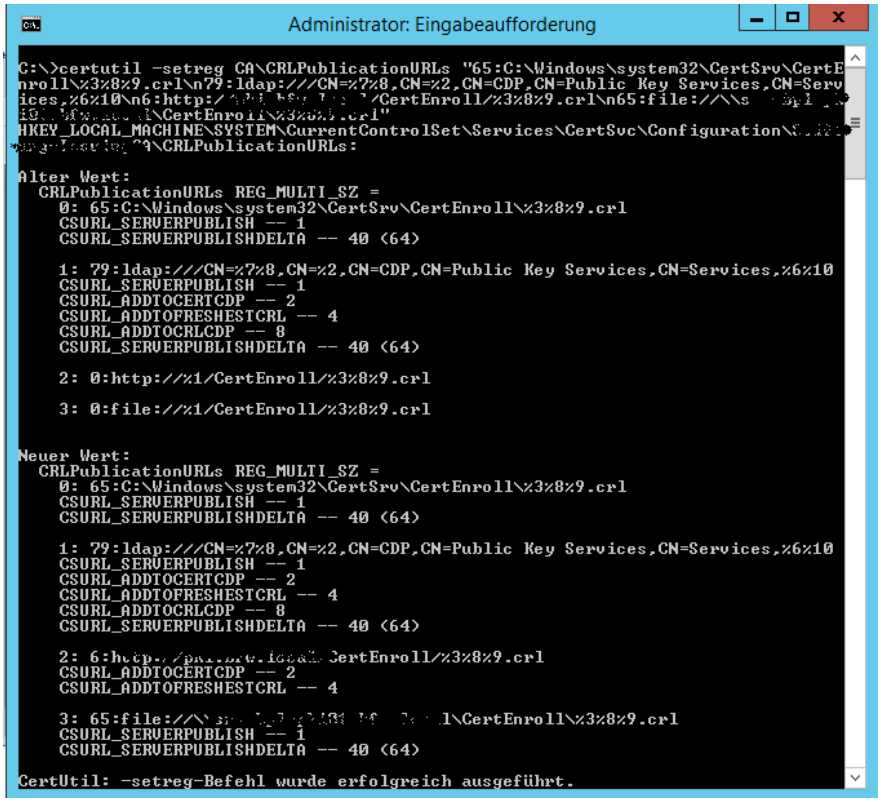


## CRL Verteilungspunkte setzen

AIA




CDP



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.

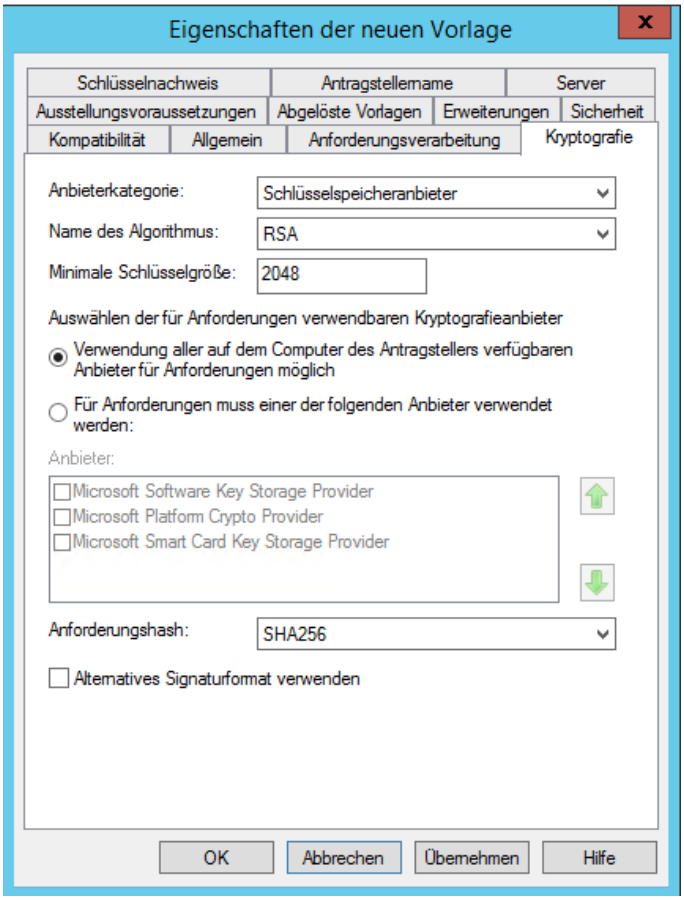
**Auditing auf der CA aktivieren**

*Certutil -setreg CA\AuditFilter 127*

**Certificate Templates wieder aktivieren**

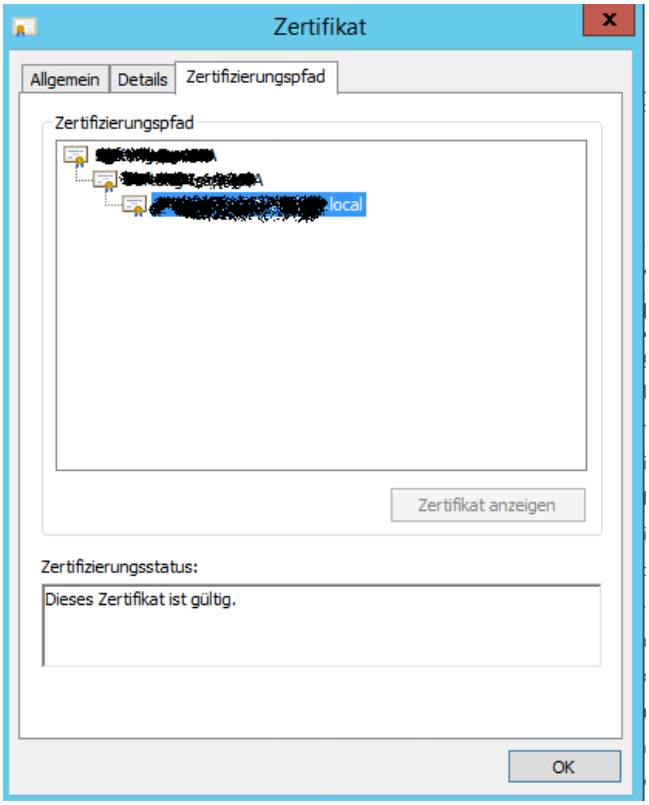
Sicherstellen, dass keine Vorlagen mehr hinzugefuegt werden, wo keine CNG Algorithmen verwendet werden. Am sinnvollsten ist es neue Zertifikat Vorlagen zu erstellen und in den Templates CNG Algorithmen festzulegen.

**Achtung**: Auf Abwaertskompatibilitaet zu ggfs. alten Betriebssystemen achten

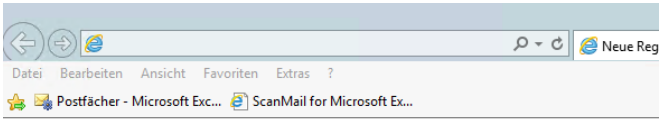


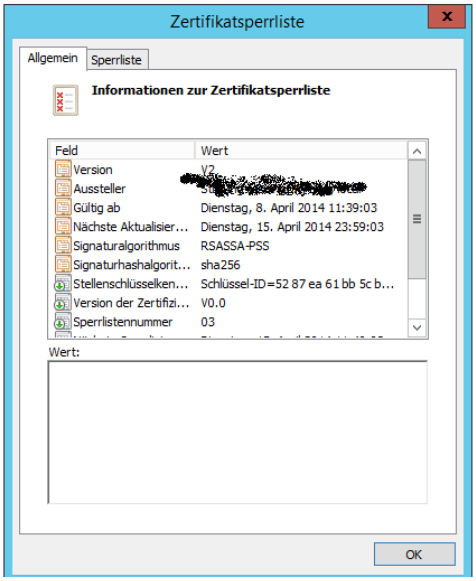

Wenn auf der Enterprise Online Issuing CA die Zertifizierungsstellen Webregistrierung installiert wurde, muss noch sichergestellt werden, dass fuer den Server ein geeignetes Webserver Zertifikat ausgestellt wird und in der IIS Verwaltungskonsole eine HTTPS-Bindung mit dem neuen Zertifikat eingerichtet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

## Zertifikatkette pruefen



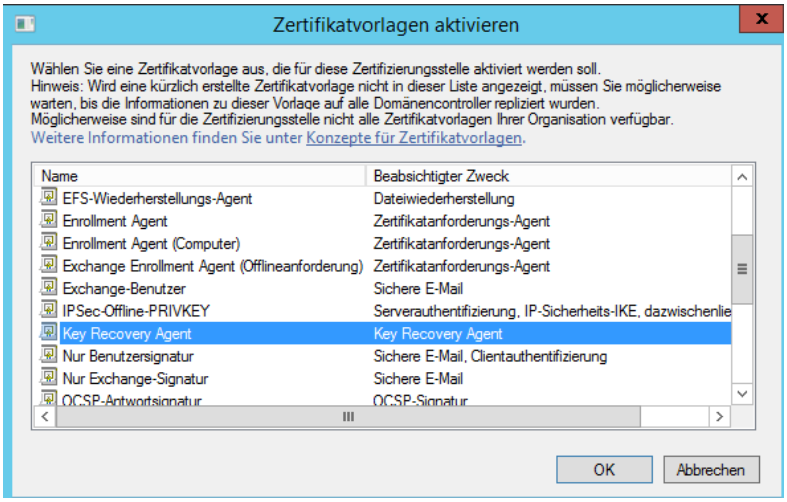

## CRL Download testen



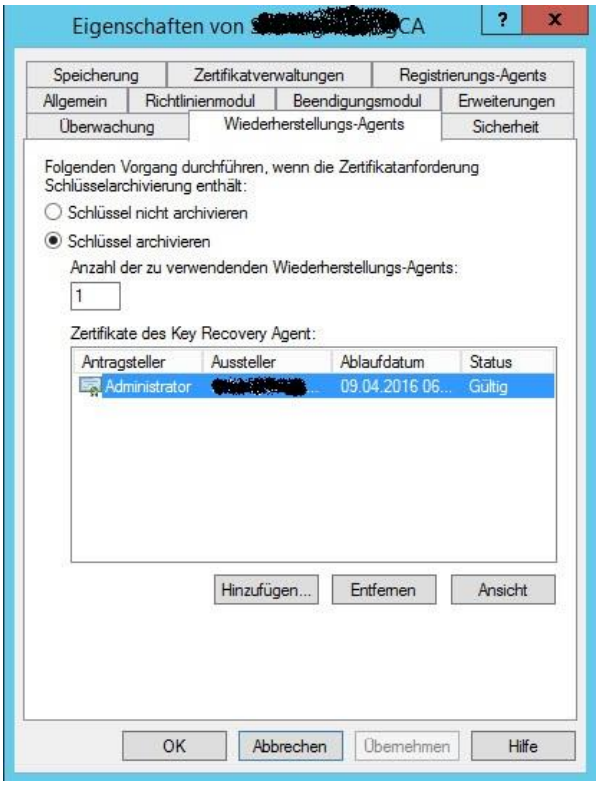
CA Schluesselarchivierung aktivieren

KRA Vorlage aktivieren

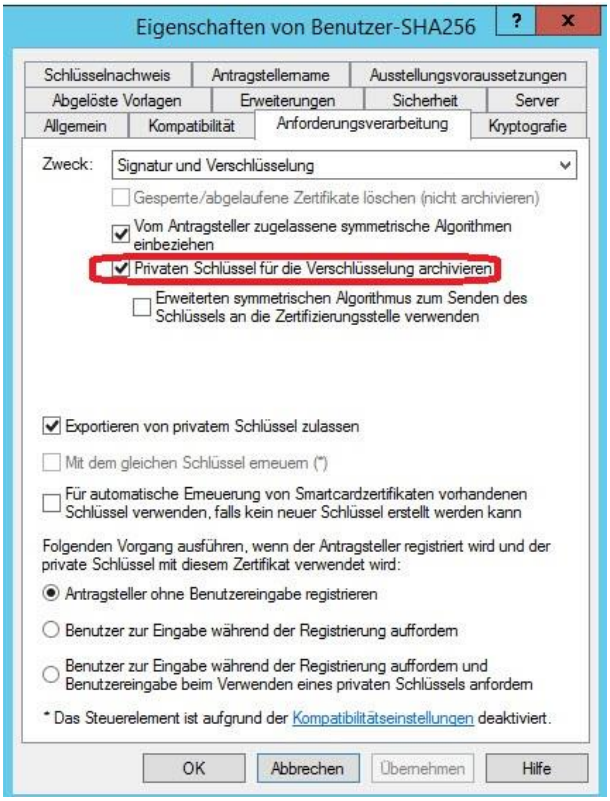



KRA Zertifikat anfordern

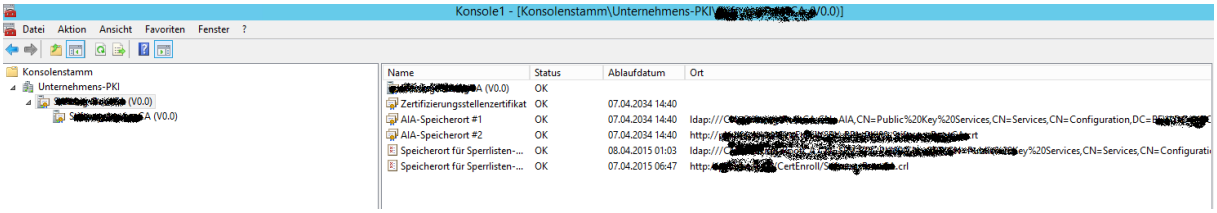
CA fuer Schluesselarchivierung aktivieren



Zertifikatvorlagen zur Schluesselarchivierung aktivieren

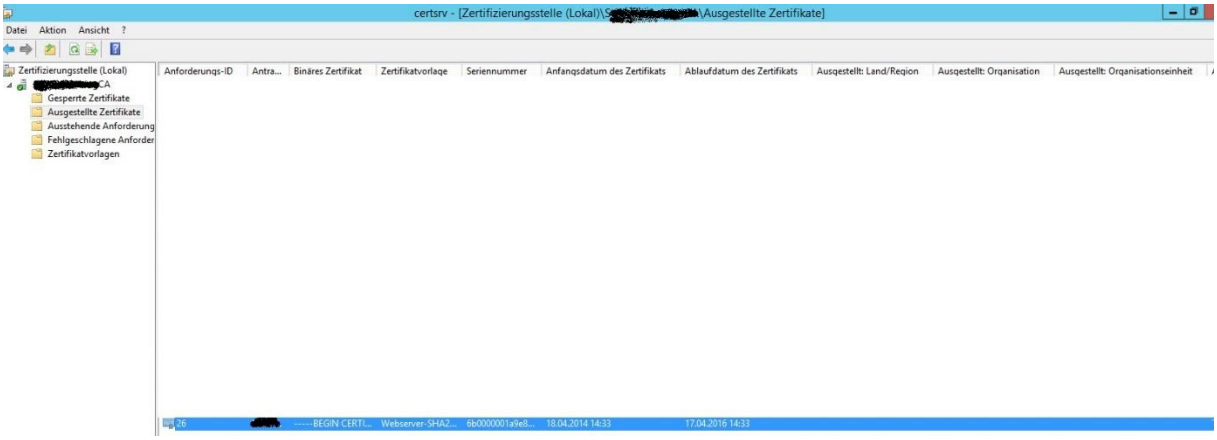



PKI Health




## Ausstellung von Zertifikaten testen

Testen, ob Computer, Benutzer, Domaenencontroller ordnungsgemaess Zertifikate anfordern koennen



## 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

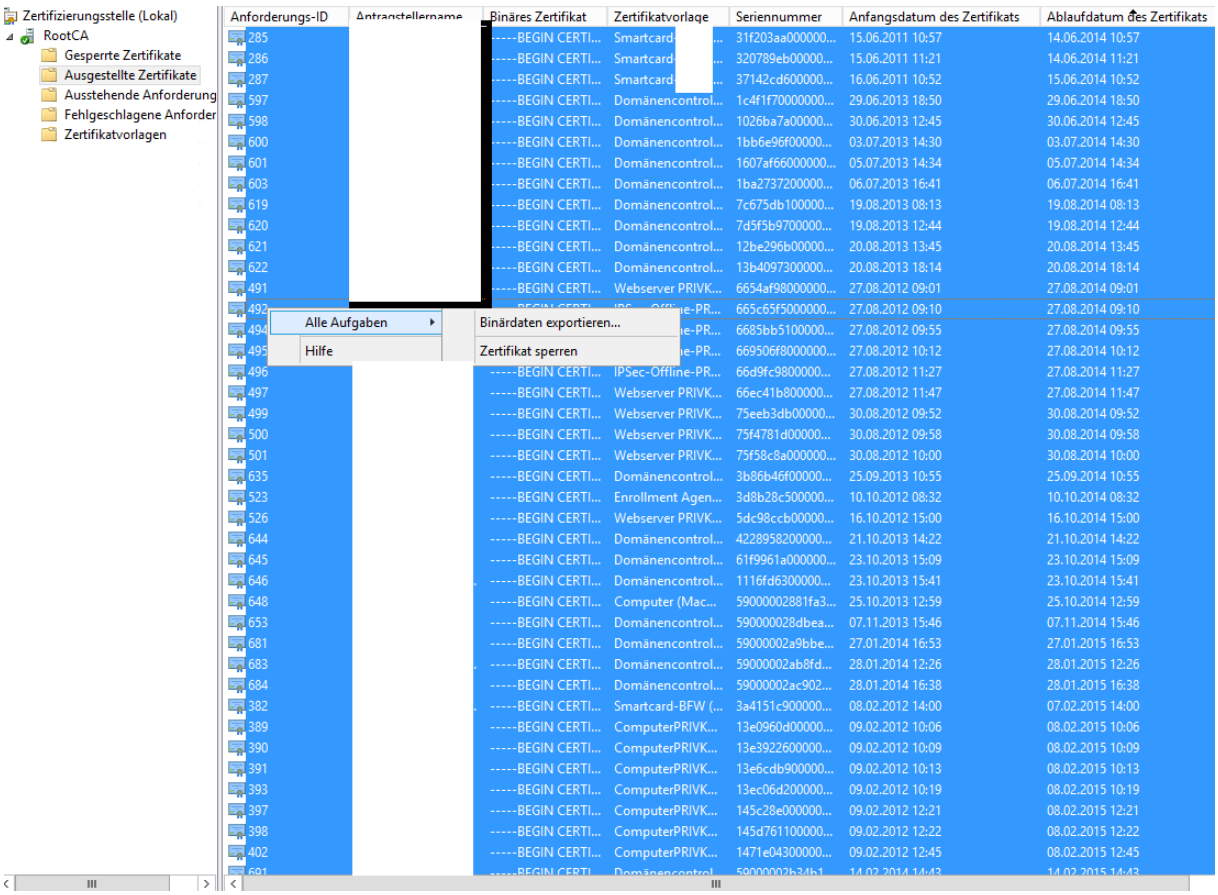
## Server, Clients und Benutzer mit neuen Zertifikaten ausstatten

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

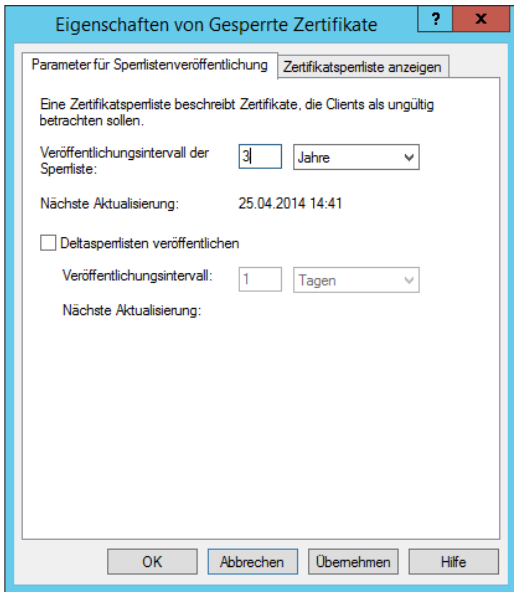
http://social.technet.microsoft.com/wiki/contents/articles/how-to-decommission-a-windows-enterprise-certification-authority-and-how-to-remove-all-related-objects.aspx

Alle aktiven Zertifikate revoken

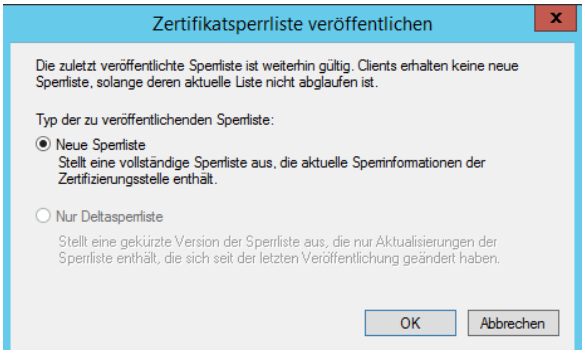


## CRL anpassen

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

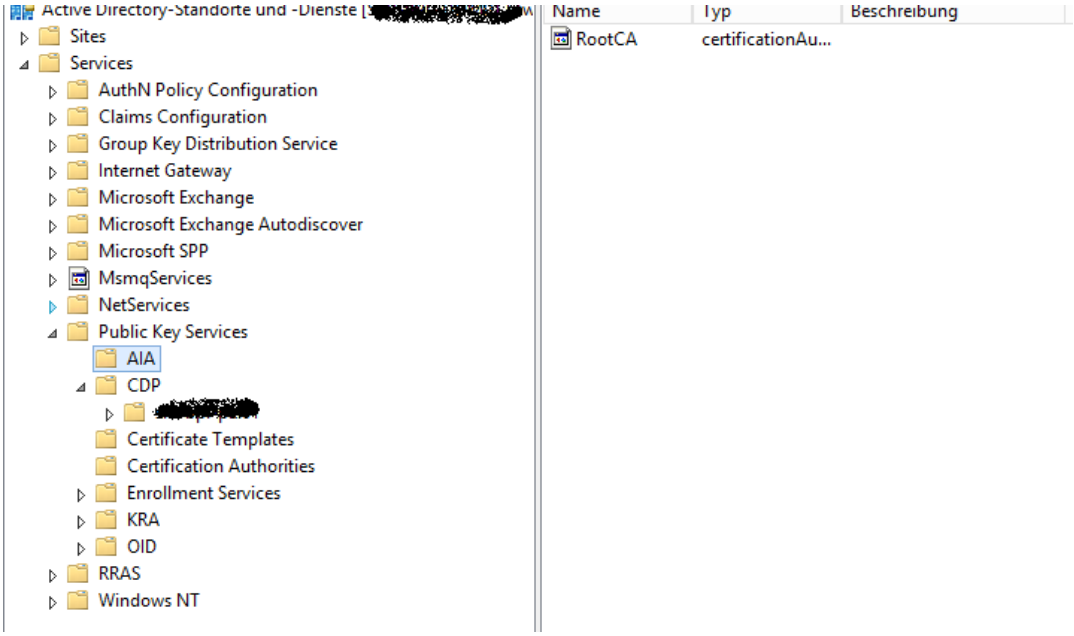



## Sperrliste veroeffentlichen



## 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*

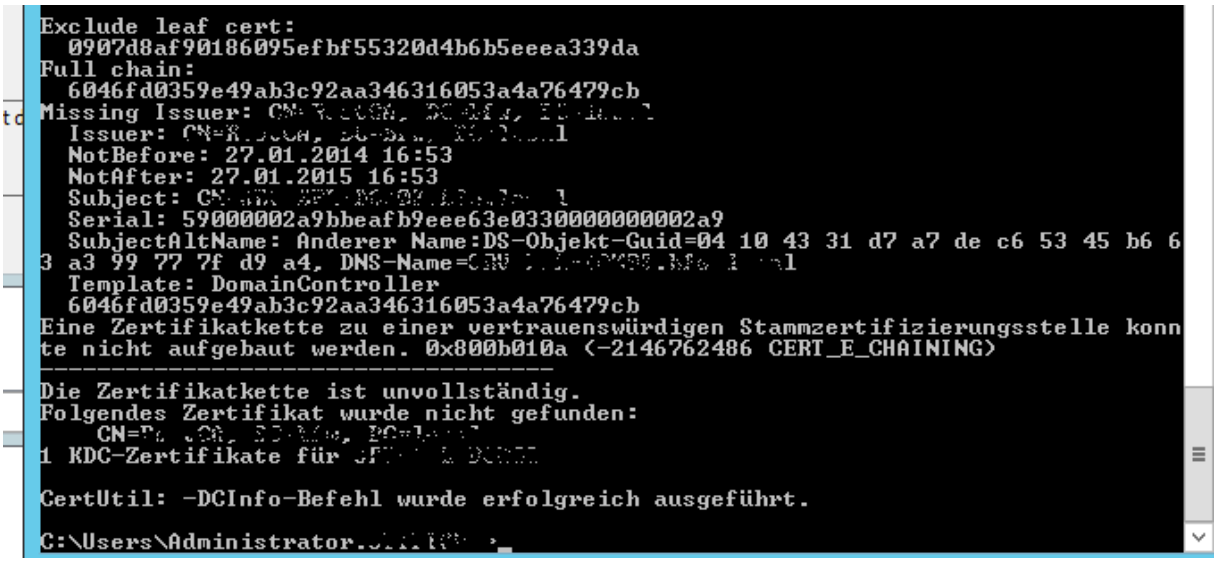
*Services,CN=Services,CN=Configuration,DC=ForestRoot,DC=com?cACertificate?base?objectclass*

## 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




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