



# Windows Server®

## Active Directory

Active-Directory-Zertifikatdienste (PKI)  
Installieren & konfigurieren

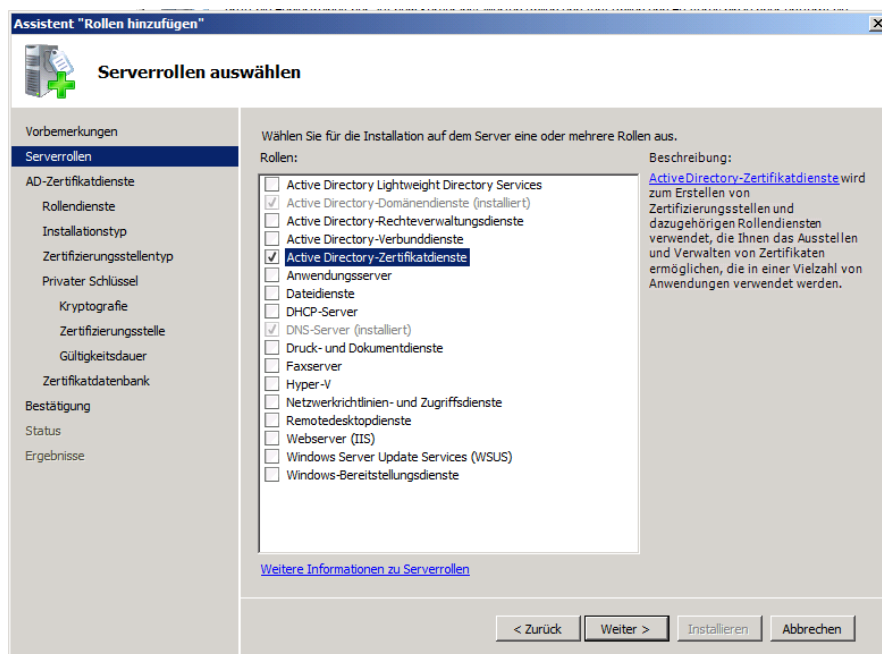
# Active-Directory-Zertifikatdienste (PKI) Installieren & konfigurieren

## Inhalt

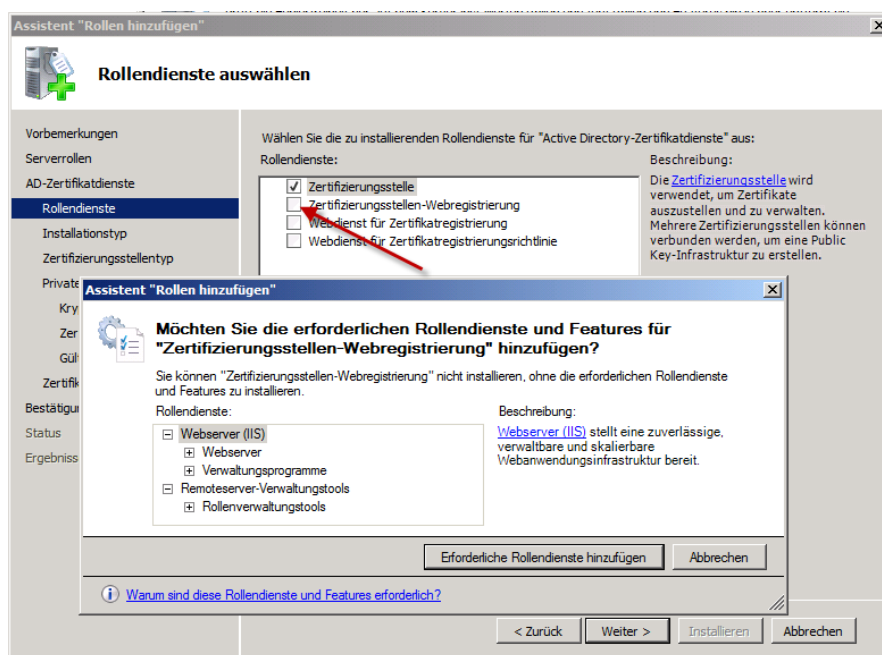
Active Directory-Zertifikatdienst Installieren .....	2
Automatische Zertifikatanforderung & Auto Enrollment konfigurieren .....	7
Sperrlisteneinträge veröffentlichen.....	12
Zertifikat und Sperrliste dem Active Directory hinzufügen.....	13

## Active Directory-Zertifikatdienst Installieren

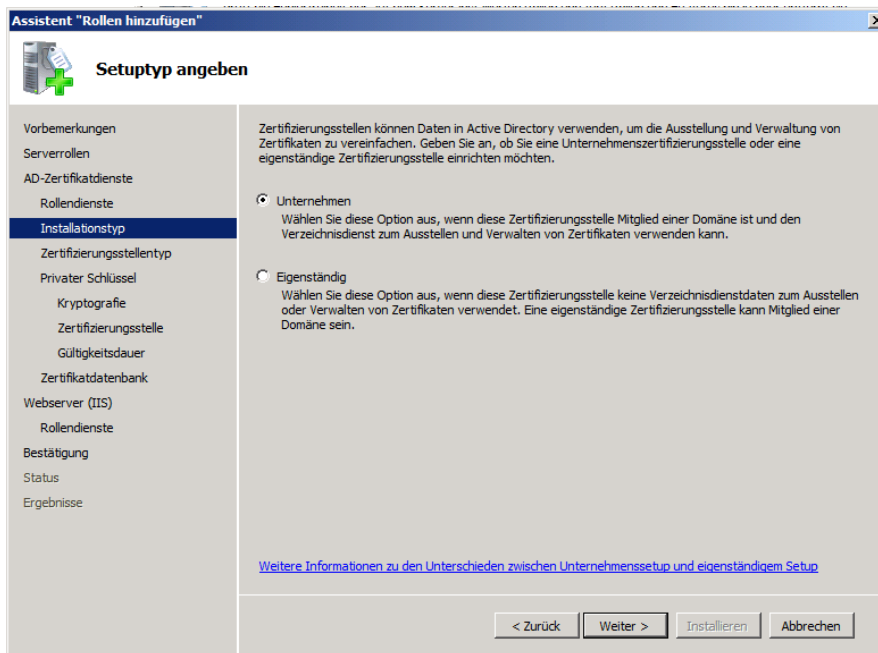
Hier in diesen Howto möchte ich euch zeigen, wie man die Active Directory-Zertifikatdienste Installiert und grundlegend konfiguriert. Das ganze wurde in einer Virtuellen Umgebung mit Oracle - VirtualBox nachgestellt. Diese Zertifikatsstelle benötige ich für Exchange 2010 und Sharepoint 2010.



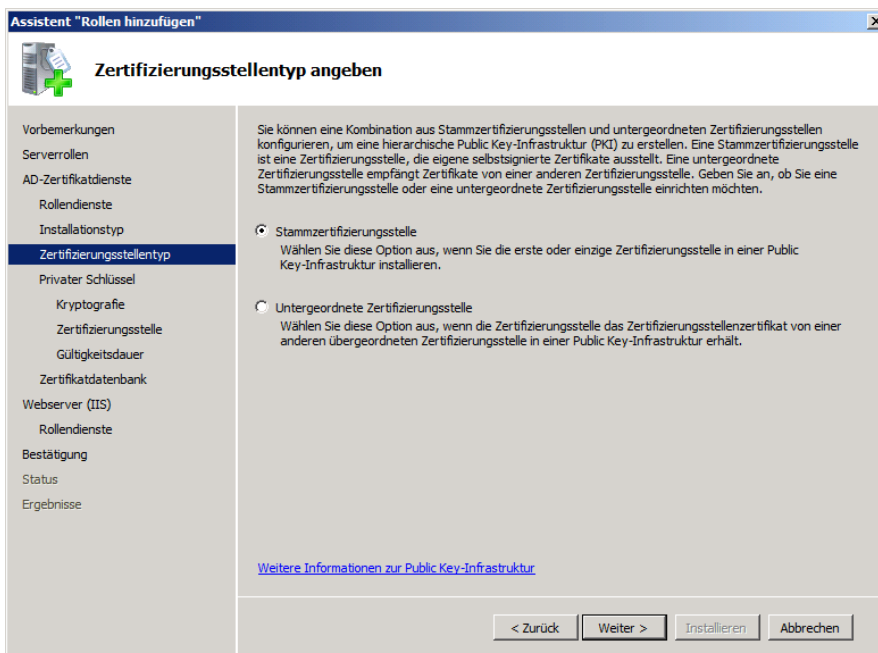
In den Serverrollen aktiviere ich die Active Directory-Zertifikatdienste und klicke auf Weiter



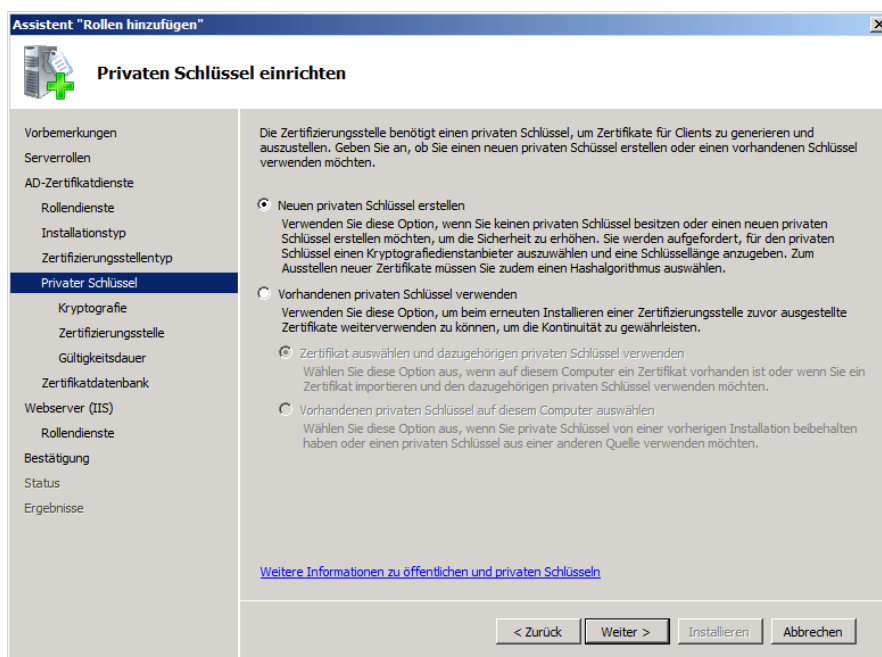
Aktiviere die Zertifizierungsstelle und die Zertifizierungsstelle-Webregistrierung, danach poppt der Rollen Assistent hoch dass noch der IIS zusätzlich Installiert werden muss.



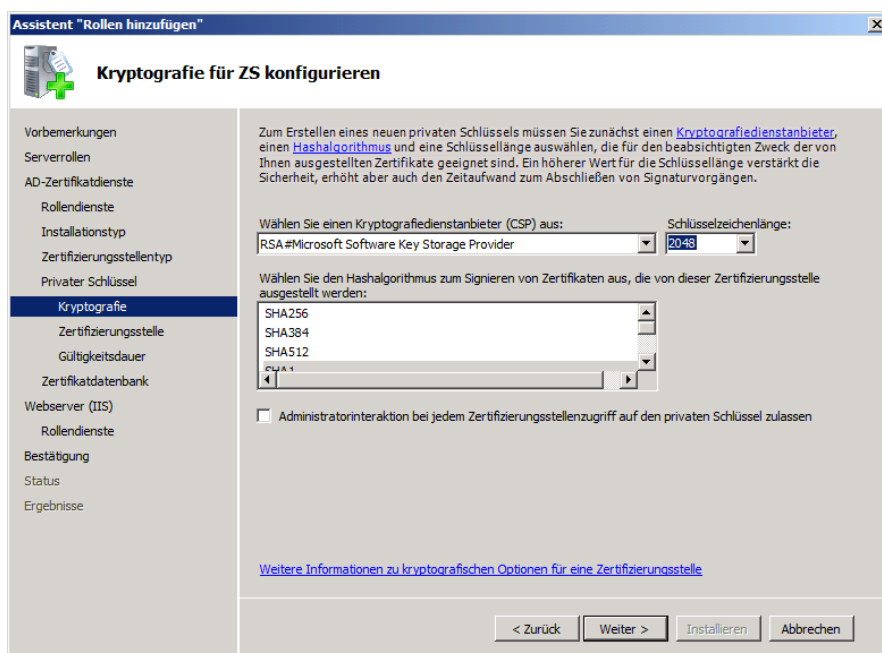
Wir wählen die Unternehmens PKI aus und klicken auf Weiter



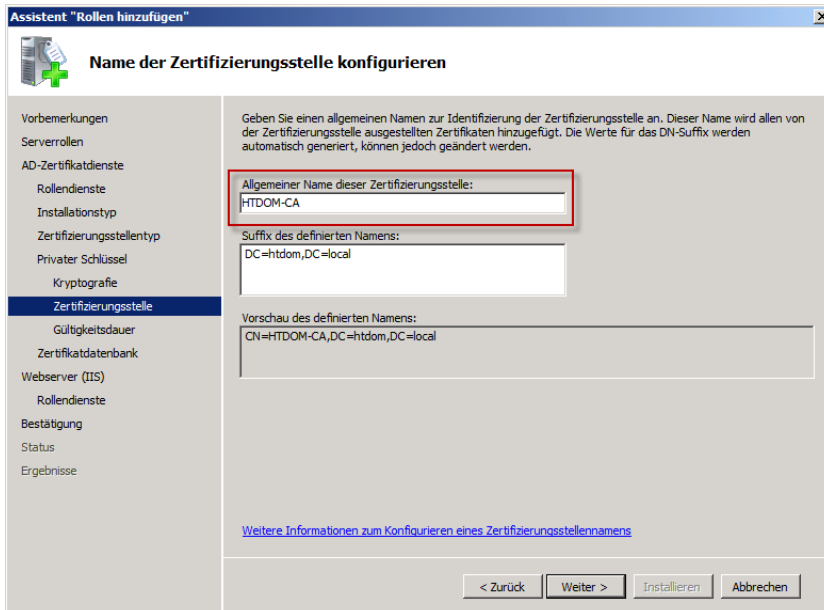
Da es unser erster Zertifikatserver ist wählen wir die Stammzertifizierungsstelle aus und klicken auf Weiter.



Wir lassen uns einen neuen Schlüssel erstellen und klicken auf Weiter



Übernehmen die Standardeinstellungen für den privaten Schlüssel und klicken auf Weiter



**Assistent "Rollen hinzufügen"**

**Name der Zertifizierungsstelle konfigurieren**

Vorbemerkungen  
Serverrollen  
AD-Zertifikatsdienste  
Rollendienste  
Installationstyp  
Zertifizierungsstellentyp  
Privater Schlüssel  
Kryptografie  
**Zertifizierungsstelle**  
Gültigkeitsdauer  
Zertifikatsdatenbank  
Webserver (IIS)  
Rollendienste  
Bestätigung  
Status  
Ergebnisse

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 dieser Zertifizierungsstelle:  
HTDOM-CA

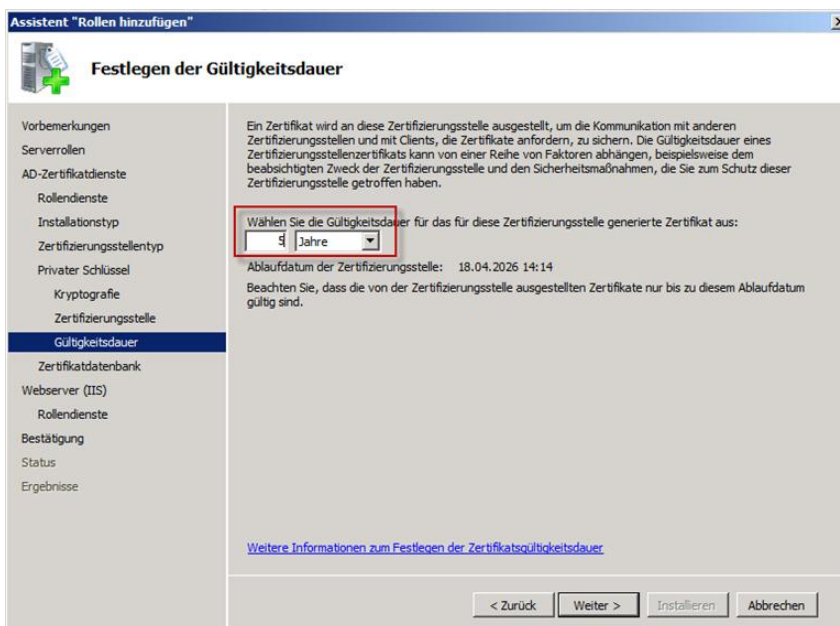
Suffix des definierten Namens:  
DC=htdom,DC=local

Vorschau des definierten Namens:  
CN=HTDOM-CA,DC=htdom,DC=local

[Weitere Informationen zum Konfigurieren eines Zertifizierungsstellennamens](#)

< Zurück Weiter > Installieren Abbrechen

Vergeben einen Aussagekräftigen Namen für die Zertifizierungsstelle und klicken auf Weiter



**Assistent "Rollen hinzufügen"**

**Festlegen der Gültigkeitsdauer**

Vorbemerkungen  
Serverrollen  
AD-Zertifikatsdienste  
Rollendienste  
Installationstyp  
Zertifizierungsstellentyp  
Privater Schlüssel  
Kryptografie  
Zertifizierungsstelle  
**Gültigkeitsdauer**  
Zertifikatsdatenbank  
Webserver (IIS)  
Rollendienste  
Bestätigung  
Status  
Ergebnisse

Ein Zertifikat wird an diese Zertifizierungsstelle ausgestellt, um die Kommunikation mit anderen Zertifizierungsstellen und mit Clients, die Zertifikate anfordern, zu sichern. Die Gültigkeitsdauer eines Zertifizierungsstellenzertifikats kann von einer Reihe von Faktoren abhängen, beispielsweise dem beabsichtigten Zweck der Zertifizierungsstelle und den Sicherheitsmaßnahmen, die Sie zum Schutz dieser Zertifizierungsstelle getroffen haben.

Wählen Sie die Gültigkeitsdauer für das für diese Zertifizierungsstelle generierte Zertifikat aus:  
5 Jahre

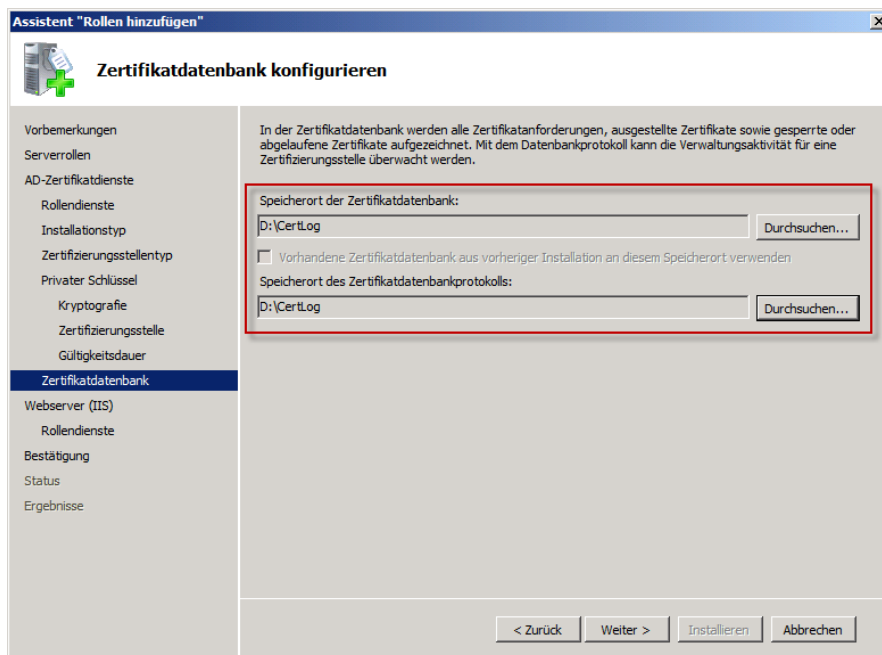
Ablaufdatum der Zertifizierungsstelle: 18.04.2026 14:14  
Beachten Sie, dass die von der Zertifizierungsstelle ausgestellten Zertifikate nur bis zu diesem Ablaufdatum gültig sind.

[Weitere Informationen zum Festlegen der Zertifikatsgültigkeitsdauer](#)

< Zurück Weiter > Installieren Abbrechen

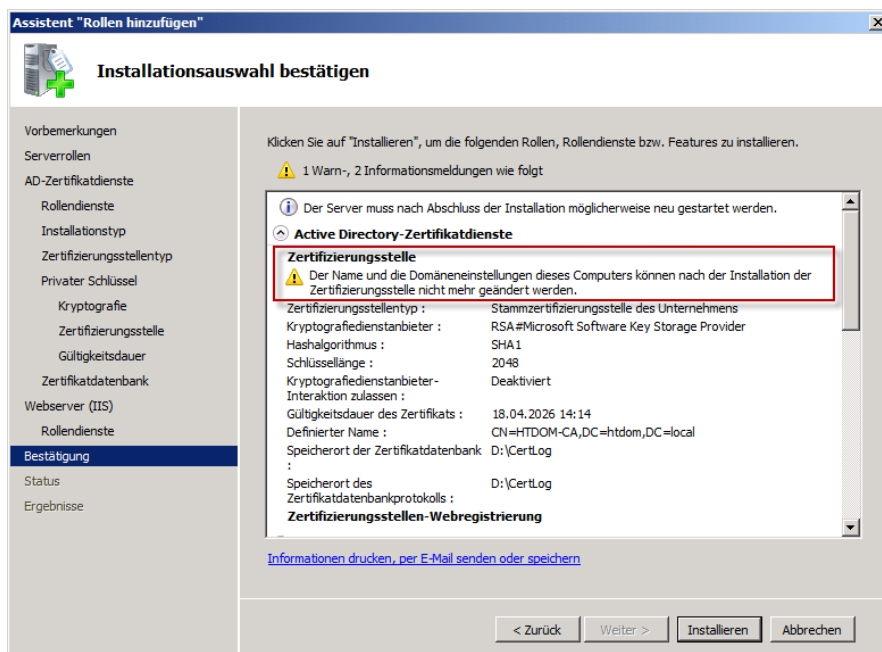
Bei der Gültigkeitsdauer belasse ich die 5 Jahre als Standardwert stehen. Entscheidung sollte jeder Administrator für sich selbst treffen.

*„Hier ist anzumerken das man oft im Internet lesen kann das ein Root CA Zertifikat so konfiguriert werden soll das die Gültigkeitsdauer 20 Jahre und länger sein soll. Persönlich Meinung ist, zum einen kommt es darauf an wie groß das jeweilige Unternehmen ist und zum zweiten wie komplex die PKI aufgebaut wird. Umso kleiner ein Unternehmen ist umso kürzer würde ich die Gültigkeitsdauer einstellen (min. 5 Jahre). Umso größer ein Unternehmen umso länger auch die Gültigkeitsdauer. Sobald sich die Serverversionen ändern, sollte man auch die PKI Updaten und neue Zertifikate ausrollen.“*



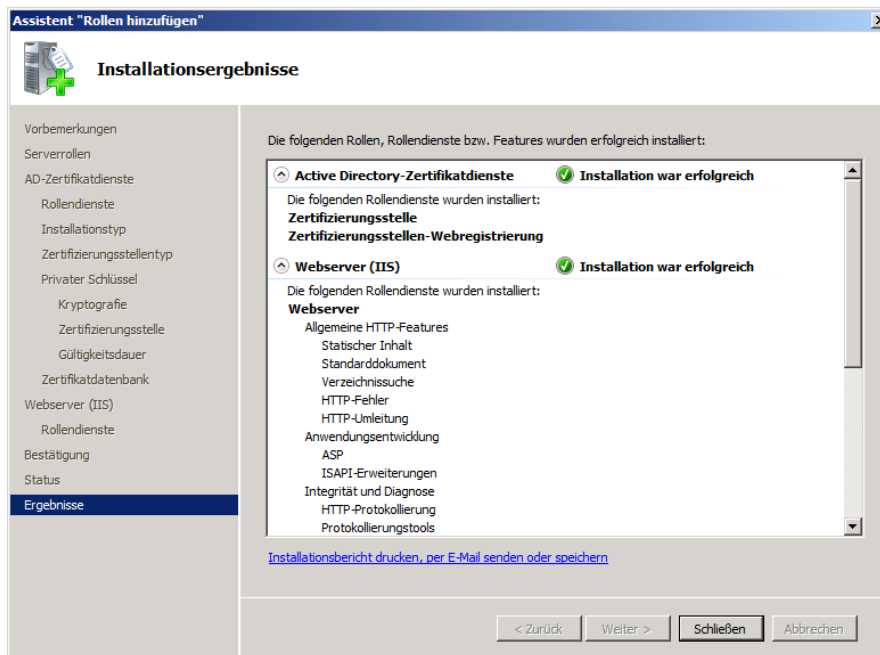
Auch im nächsten Fenster muss jeder Administrator selbst entscheiden wie er es konfiguriert, Microsoft rät bei sehr großen PKI's die Datenbank auf ein externes Laufwerk/Partition zu legen, bei kleinen PKI's kann man es im Standardpfad lassen, obwohl der Best Practice Analyzer meckert.

Bei dem Fenster der IIS Einstellungen lasse ich alles auf Standard und klicke auf Weiter.



Diese Warnmeldung sollte man sich wirklich zu Herzen nehmen, ansonsten verursacht eine Namensänderung zu großen Problemen im Netzwerk. Wenn man es trotzdem wagt dann viel Spaß beim Fehlerbeheben. 😊

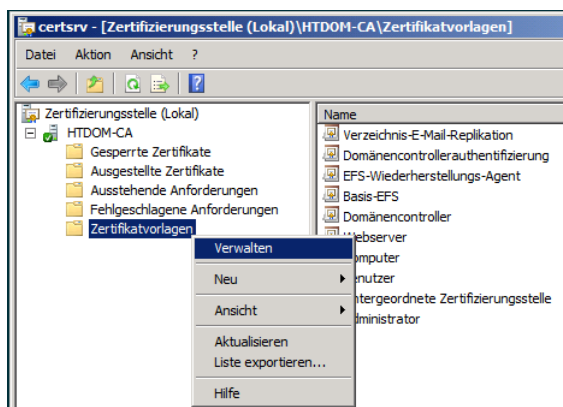




Nach kurzer Zeit ist die PKI installiert und persönlich würde ich einen Neustart vom Server durchführen.

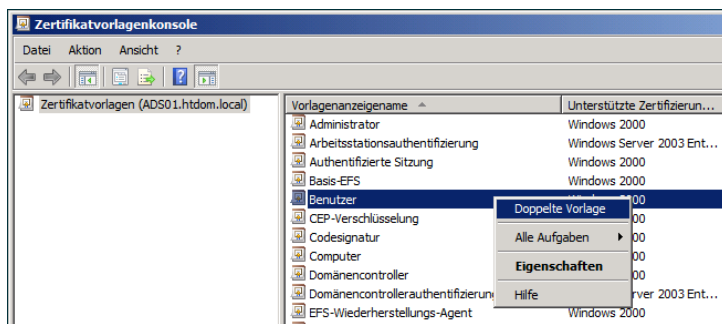
## Automatische Zertifikatanforderung & Auto Enrollment konfigurieren

Wenn wir jetzt nicht nur Computerzertifikate sondern auch Benutzerzertifikate verteilen möchten, müssen wir noch ein paar Dinge konfigurieren.



Als erstes öffnen wir die Zertifizierungsstellen-Managementkonsole → klicken mit der rechten Maustaste auf Zertifikatvorlage → Verwalten

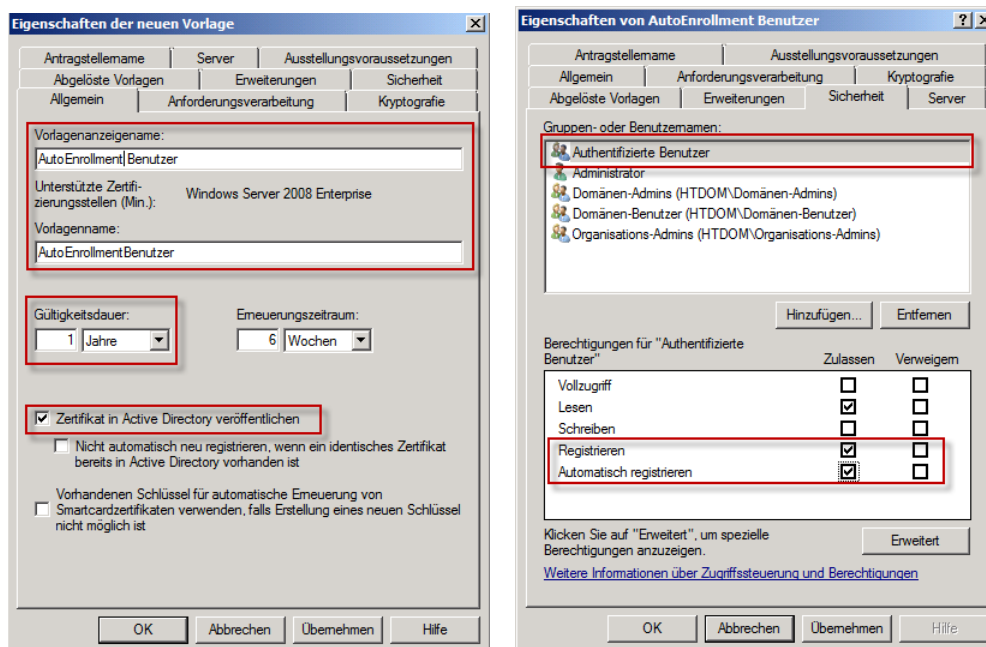




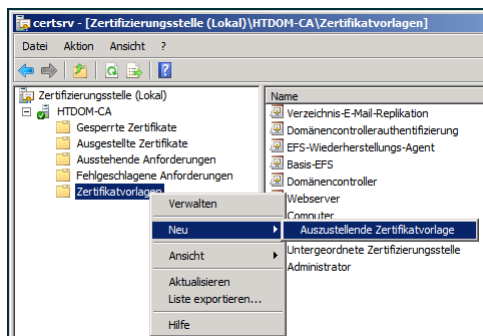
Suchen uns die Vorlage Benutzer heraus und klicken mit der rechten Maustaste auf die Vorlage und wählen den Eintrag → Doppelte Vorlage



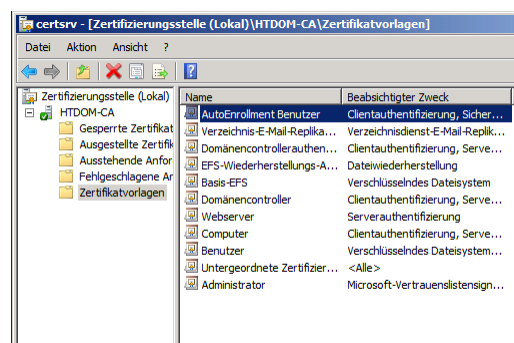
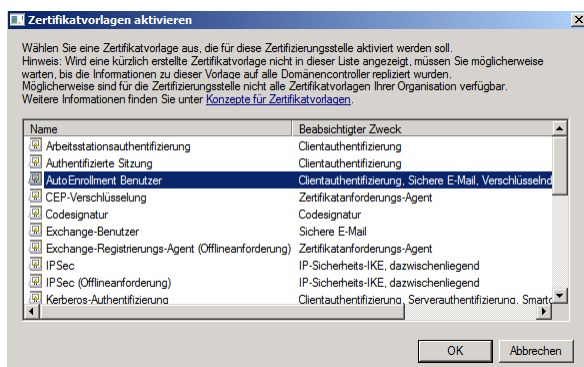
Wählen den Server Modus aus „**Windows Server 2008 Enterprise**“



Vergeben einen aussagekräftigen Namen für die Vorlage, Gültigkeitsdauer sollte das 1 Jahr nicht überschreiten und es muss im AD veröffentlicht werden. Berechtigungen für die Authentifizierten Benutzer anpassen.

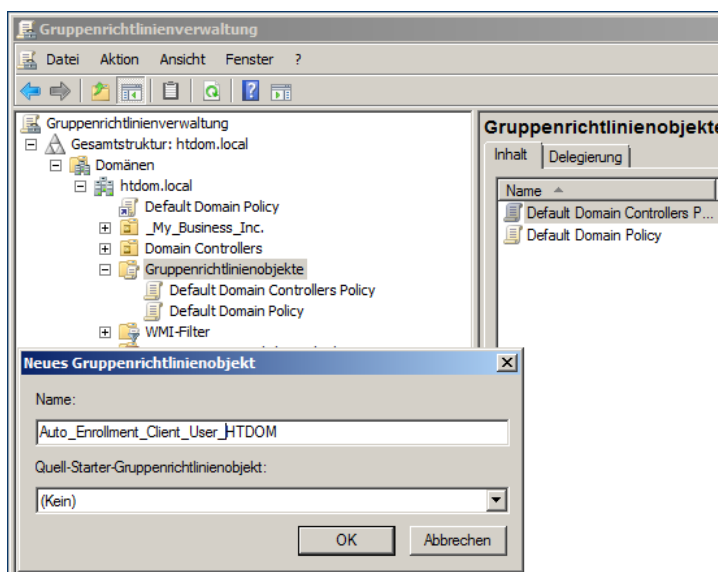


Um der Zertifizierungsstelle eine neue Vorlage hinzufügen zu können, wählen wir im Kontextmenü der Zertifikatvorlagen den Eintrag „**Auszustellende Zertifikatvorlage**“

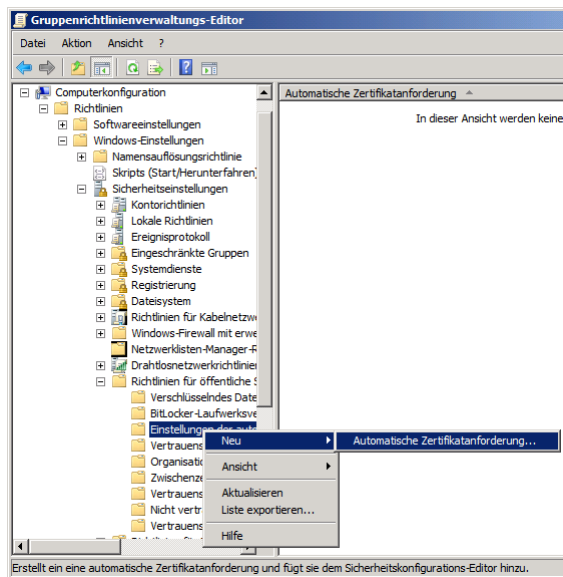


Wählen unsere bereits angelegte Vorlage aus und bestätigen das Ganze mit OK.

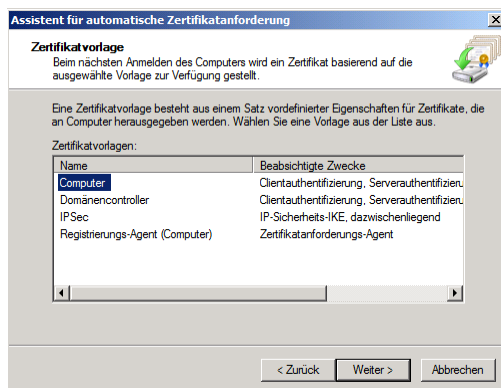
Im nächsten Schritt öffnen wir die Gruppenrichtlinienverwaltung über **Start → Alle Programme → Verwaltung → Gruppenrichtlinienverwaltung** und legen eine neue Gruppenrichtlinie unter Gruppenrichtlinienobjekte an.



Rechte Maustaste auf die neu angelegte Gruppenrichtlinie → Bearbeiten

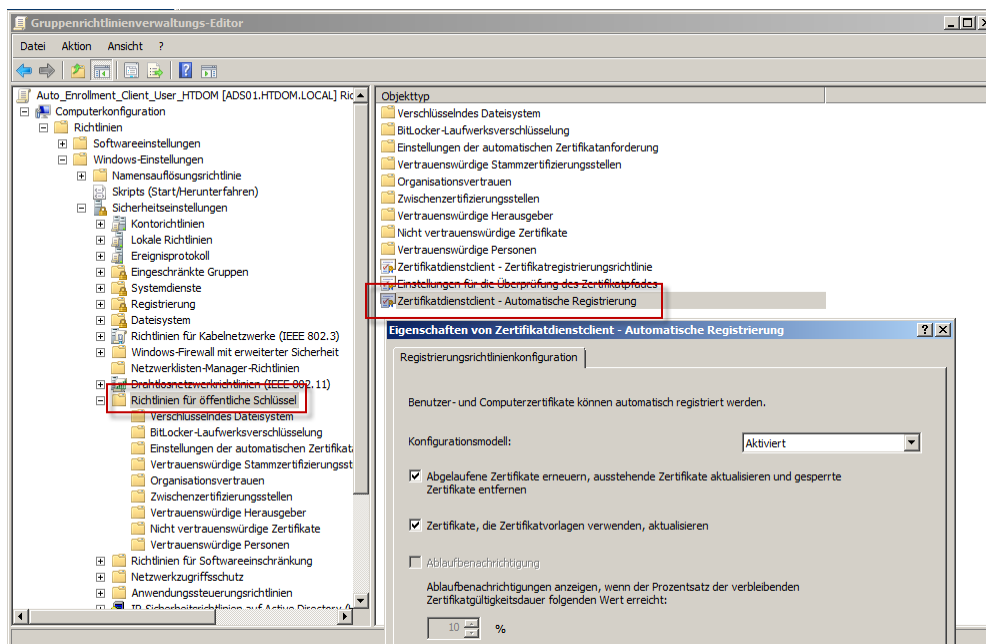


Für die Clientkonfiguration navigieren wir zu **Computerkonfiguration** → **Richtlinien** → **Windows-Einstellungen** → **Sicherheitseinstellungen** → **Richtlinien für öffentliche Schlüssel** → **Einstellungen der automatischen Zertifikatanforderung** → **Rechte Maustaste auf den Eintrag** → **Neu** → **Automatische Zertifikatanforderung**

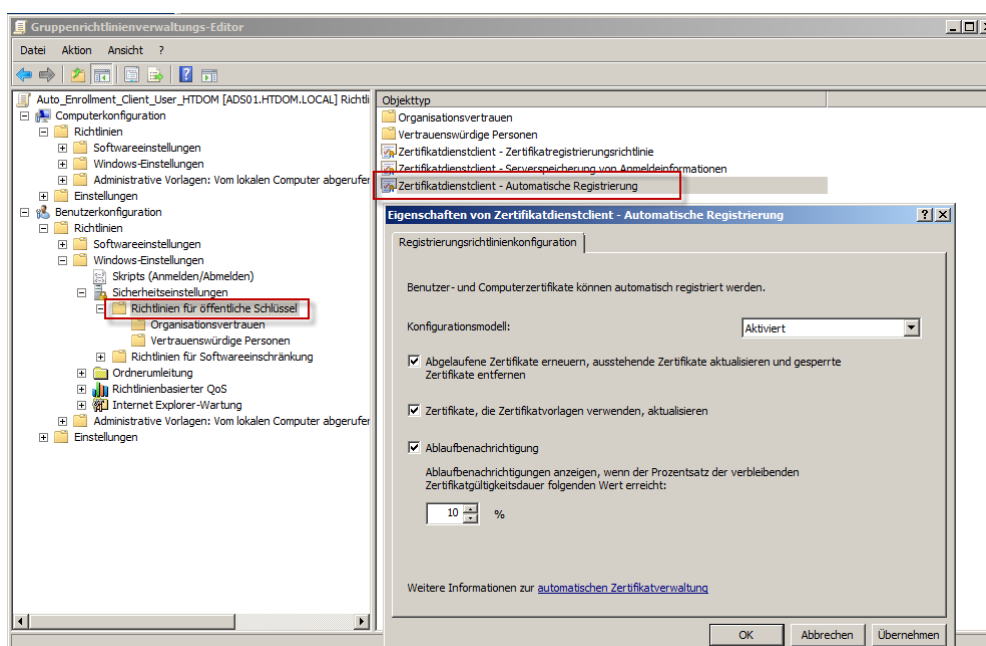


Wählen im Assistenten das „**Computer**“ Zertifikat aus und beenden den Assistenten mit Weiter und Fertigstellen.

In dem Überordner „**Richtlinien für öffentliche Schlüssel**“ liegt ein weiterer Schlüssel für die Clientkonfiguration den wir bearbeiten müssen.



**Zertifikatdienstclient – Automatische Registrierung → Hier aktivieren wir die Richtlinie und setzen beide Häkchen → Mit OK schließen wir das Fenster.**

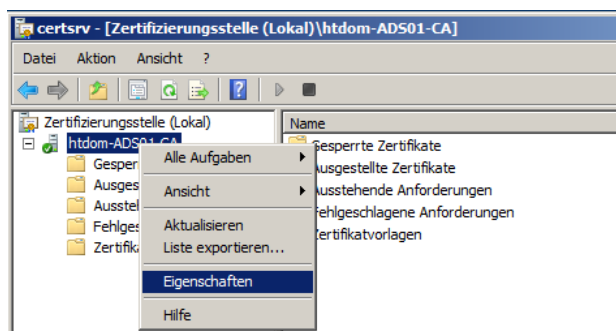


Für die Benutzer Konfiguration navigieren wir weiter zu **Benutzerkonfiguration → Windows-Einstellungen → Sicherheitseinstellungen → Richtlinien für öffentlichen Schlüssel → Zertifikatdienstclient – Automatische Registrierung → Aktivieren ebenfalls die Richtlinie und setzen hier drei Häkchen**

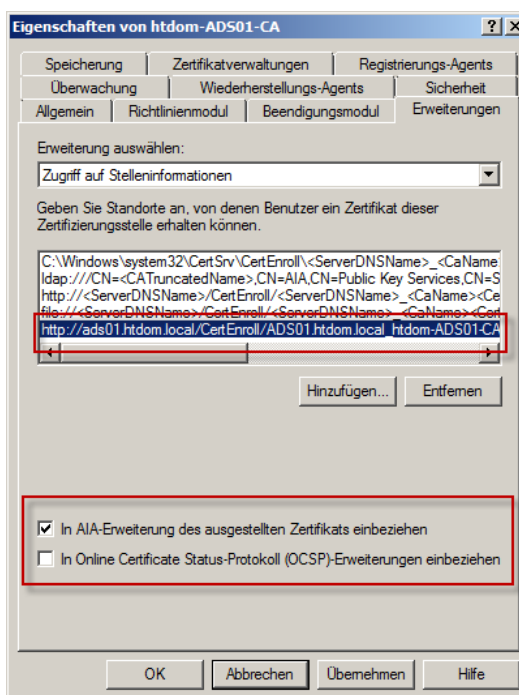
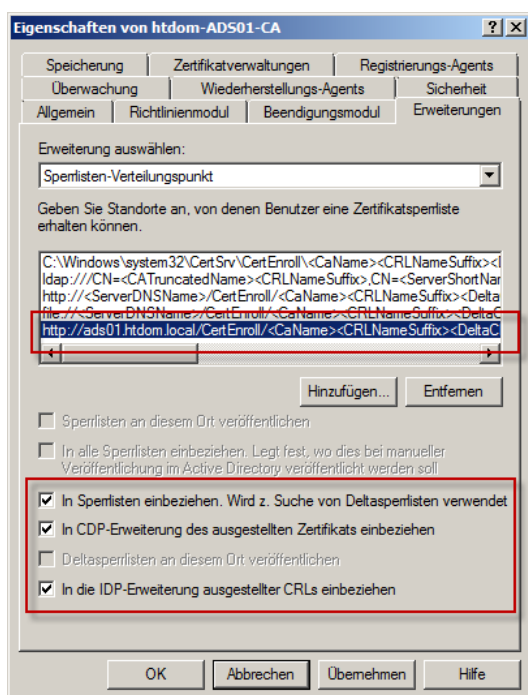
Wenn alles korrekt konfiguriert wurde, wird sich nachdem sich ein Benutzer angemeldet hat, ein Zertifikat erzeugt und Automatisch installiert.

## Sperrlisteneinträge veröffentlichen

Die Sperrlisten müssen noch als HTTP URL im Speicher veröffentlicht werden, funktioniert wie folgt:



Wir öffnen die Zertifizierungsstellen-Managementkonsole → rechte Maustaste auf die Domain-CA → Eigenschaften.



Sperrlisten-Verteilungspunkt:

***http://ads01.htdom.local/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl***

Zugriff auf Stelleninformationen:

***http://ads01.htdom.local/CertEnroll/ADS01.htdom.local\_htdom-ADS01-CA.crt***

***http://ads01.htdom.local/CertEnroll/<ServerDNSName>\_<CaName><Certificatename>.crl***

Leider funktionieren nicht alle Einstellungen über die grafische Oberfläche, sondern nur mit Certutil.

***Certutil –setreg CA\DSConfigDN CN=Configuration,DC=htdom,DC=local***

Die Konfiguration der Sperrlisten-Veröffentlichungs-Zeiträume erfolgen jetzt mit folgenden Befehlen:

***Certutil –setreg CA\CRLPeriod weeks***

***Certutil –setreg CA\CRLPeriodUnits 54***

***Certutil –setreg CA\CRLDeltaPeriod days***

***Certutil –setreg CA\CRLDeltaPeriodUnits 0***

***Certutil –setreg CA\CRLOverlapPeriod weeks***

***Certutil –setreg CA\CRLOverlapPeriodUnits 4***

Nun legen wir noch die diskreten Signaturen für ausgestellte Zertifikate fest:

***Certutil –setreg CA\csp\DiscreteSignatureAlgorithm 1***

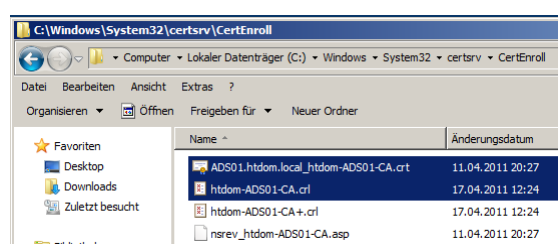
Nach Abschluss der Konfiguration müssen die Zertifikatsdienste neu gestartet werden.

***Net stop certsvc***

***Net start certsvc***

Der öffentliche Teil des Zertifikats und die Sperrliste findet man im Verzeichnis

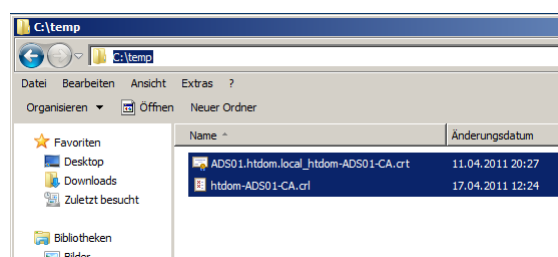
***C:\Windows\System32\CertSrv\CertEnroll***



## Zertifikat und Sperrliste dem Active Directory hinzufügen

Dieser Konfigurationsschritt ist eigentlich optional, da Zertifikate und Sperrlisten ohnehin durch das Active Directory auf den Server verteilt werden. Das manuelle Importieren in den lokalen Zertifikatsspeicher beschleunigt nur den Vorgang.

Ich kopiere mir jetzt die beiden Zertifikate in das C:\temp Verzeichnis und führe folgende Befehle aus



***certutil –addstore Root zertifikatname.crt***

```

Administrator: Eingabeaufforderung
C:\temp>certutil -addstore Root ADS01.htdon.local_htdon-ADS01-CA.crt
Root
Signatur stimmt mit dem öffentlichen Schlüssel überein.
Verwandte Zertifikate:
Genaue Übereinstimmung:
Element 1:
Seriennummer: 3f39212af02c7d8a49ea7ac25af3d563
Aussteller: CN=htdon-ADS01-CA, DC=htdon, DC=local
Nicht vor: 11.04.2011 20:17
Nicht nach: 11.04.2016 20:27
Antragsteller: CN=htdon-ADS01-CA, DC=htdon, DC=local
Version der Zertifizierungsstelle: V0.0
Signatur stimmt mit dem öffentlichen Schlüssel überein.
Stammzertifikat: Antragsteller stimmt mit Aussteller überein
Vorlage:
Zertifikathash(sha1): c9 f9 da 07 e5 0b be 79 40 00 14 22 80 63 da 30 98 8e c2 f
4
Das Zertifikat "CN=htdon-ADS01-CA, DC=htdon, DC=local" befindet sich bereits in
Speicher.
CertUtil: -addstore-Befehl wurde erfolgreich ausgeführt.
C:\temp>

```

***certutil -addstore Root zertifikatname.crl***

```

Administrator: Eingabeaufforderung
C:\temp>certutil -addstore Root htdon-ADS01-CA.crl
Root
Verwandte Sperrlisten:
Genaue Übereinstimmung:
Element 0:
Aussteller:
CN=htdon-ADS01-CA
DC=htdon
DC=local
Version der Zertifizierungsstelle: V0.0
Sperrlistennummer: Sperrlistennummer=05
Sperrlistenhash(sha1): e7 79 65 2f b8 7e cc f6 1d ab 26 99 dc 3a 55 e0 c3 1b 80
76
Die Sperrliste CN=htdon-ADS01-CA, DC=htdon, DC=local befindet sich bereits in Sp
eicher.
CertUtil: -addstore-Befehl wurde erfolgreich ausgeführt.
C:\temp>

```

Nach dem das alles konfiguriert wurde werden über das AD die Zertifikate automatisch ausgerollt, dazu genügt der Befehl lokal an den Servern oder Computer ***gpupdate /force oder der*** klassische Neustart. ☺

Viel Spaß

Helmut Thurnhofer

