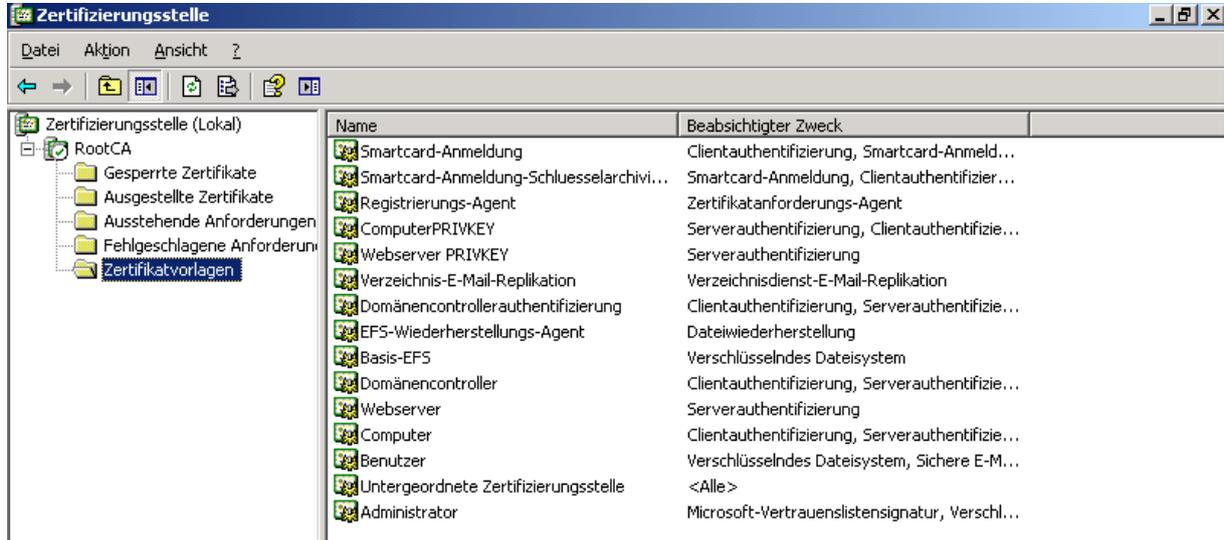


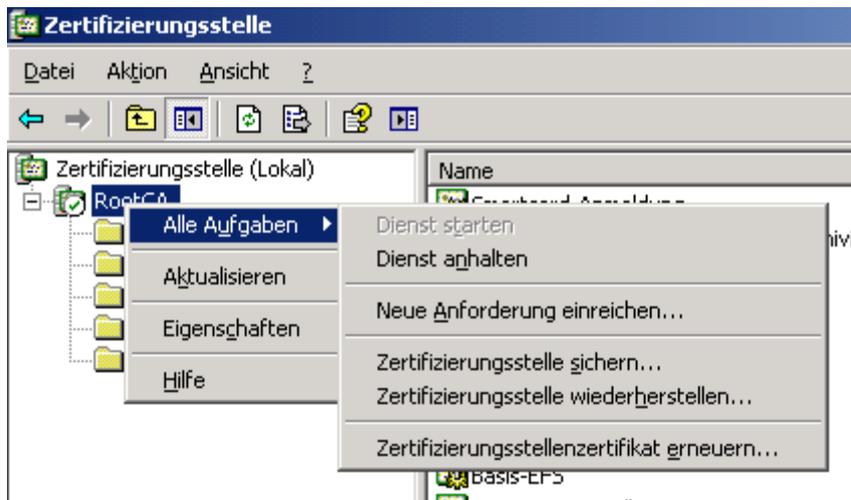
# Windows Server 2003 CA Migration auf Windows Server 2008

Windows Server 2003 CA sichern

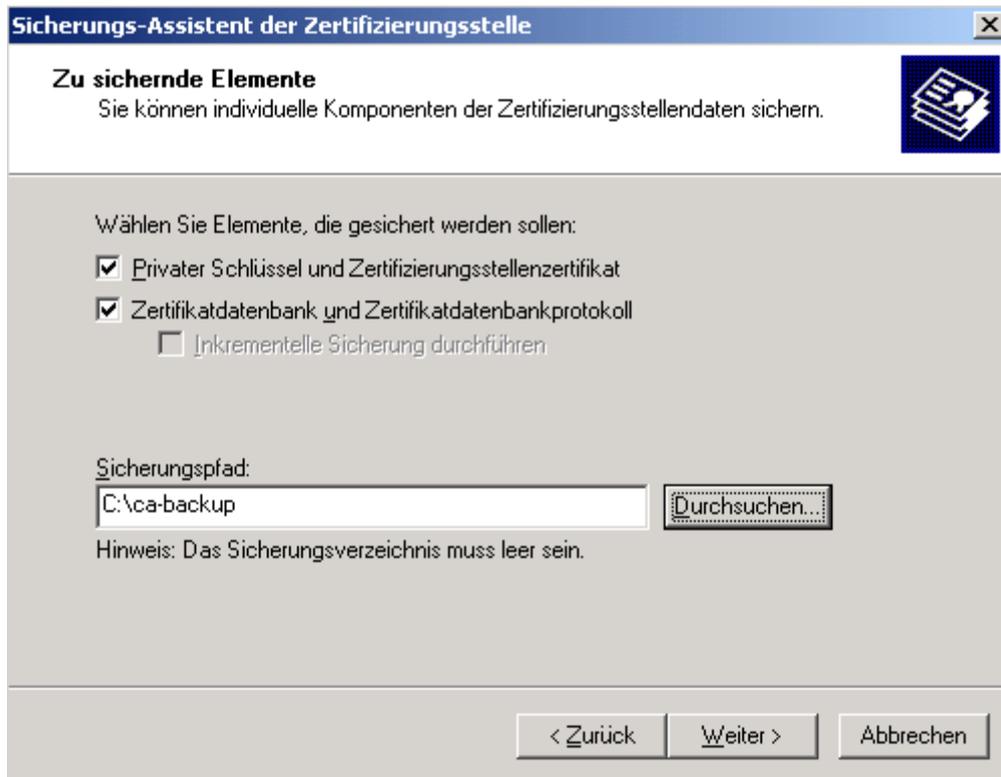
Windows Server 2003 CA



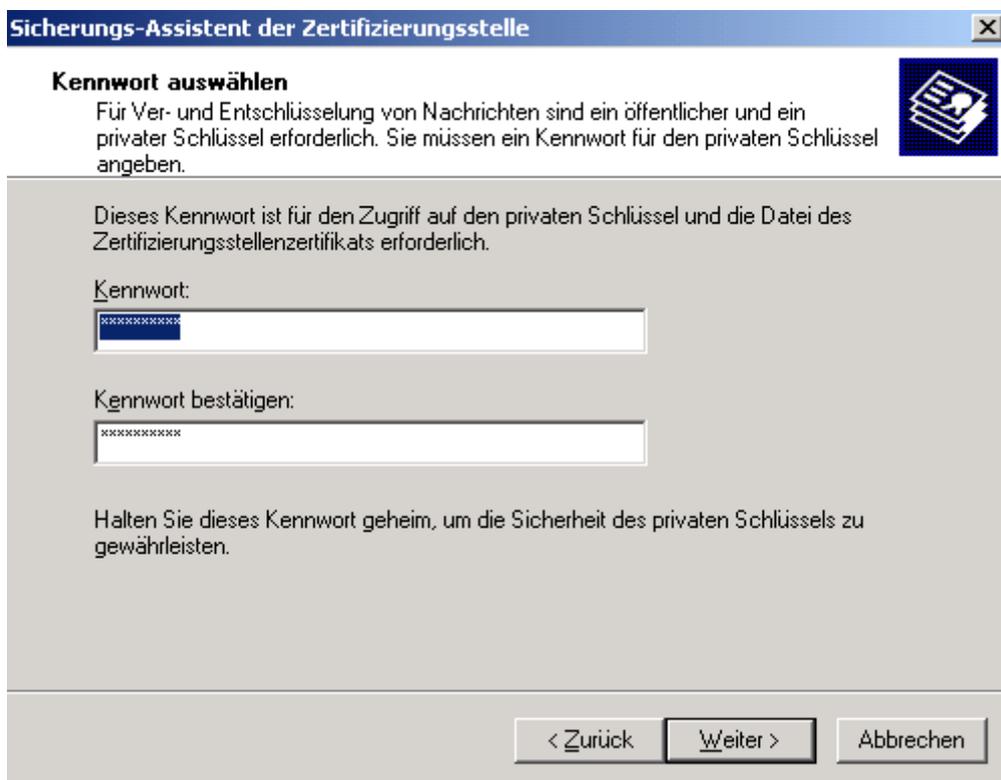
Sichern der Zertifizierungsstelle



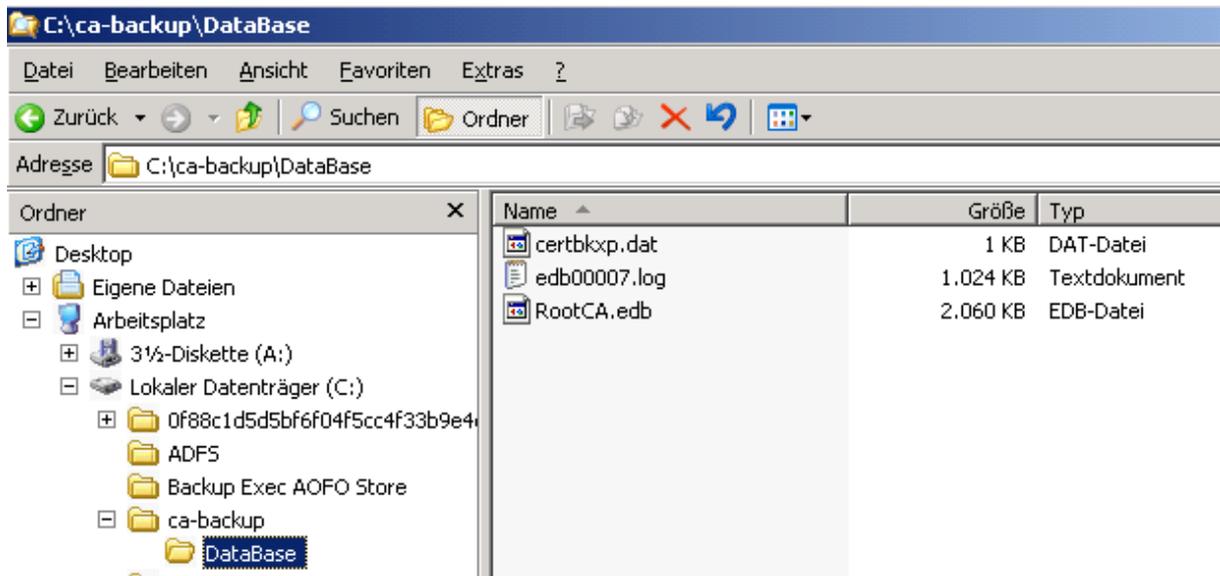
Optionen zur Sicherung



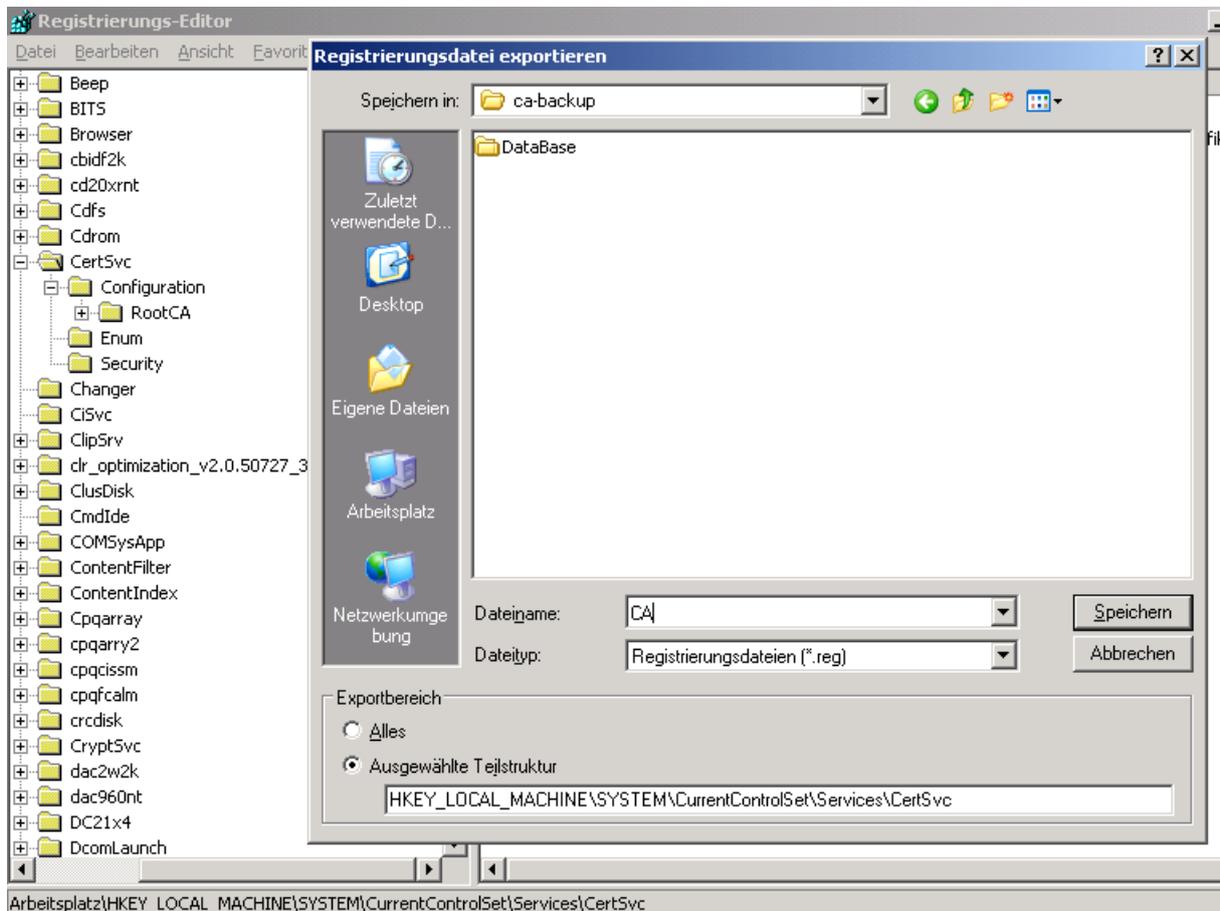
## Sicherung des Exports



## Datenbank Sicherung

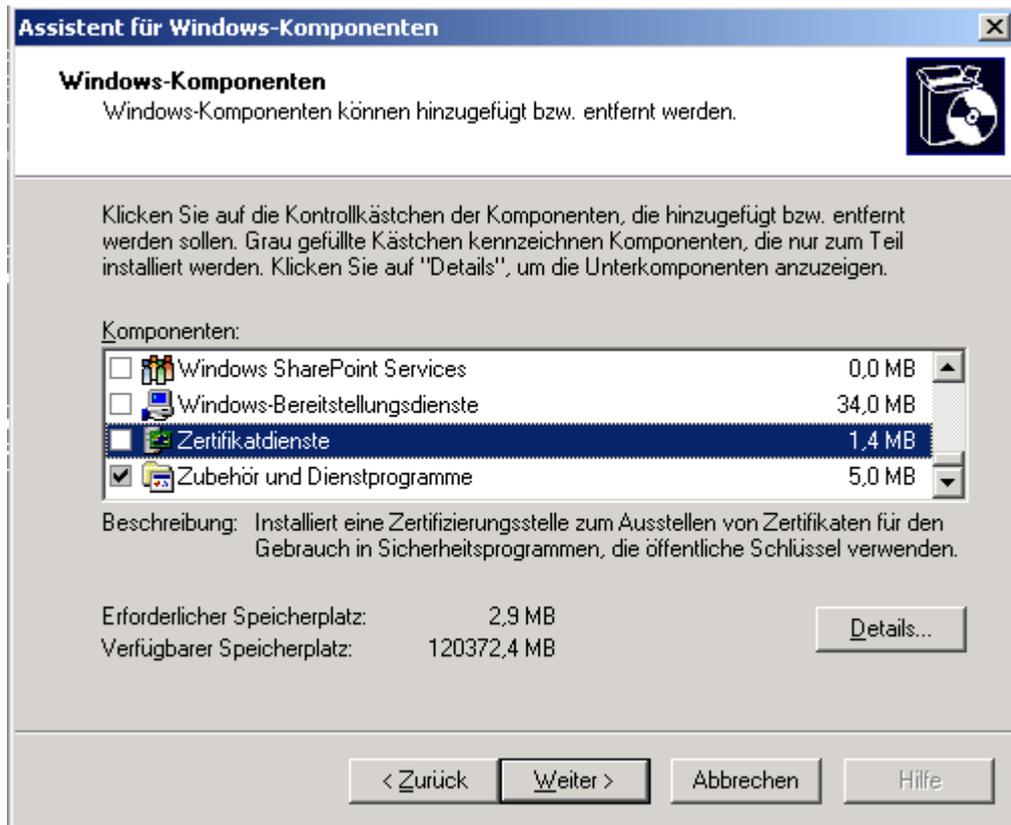


HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc exportieren



CA Backup auf den neuen Server kopieren

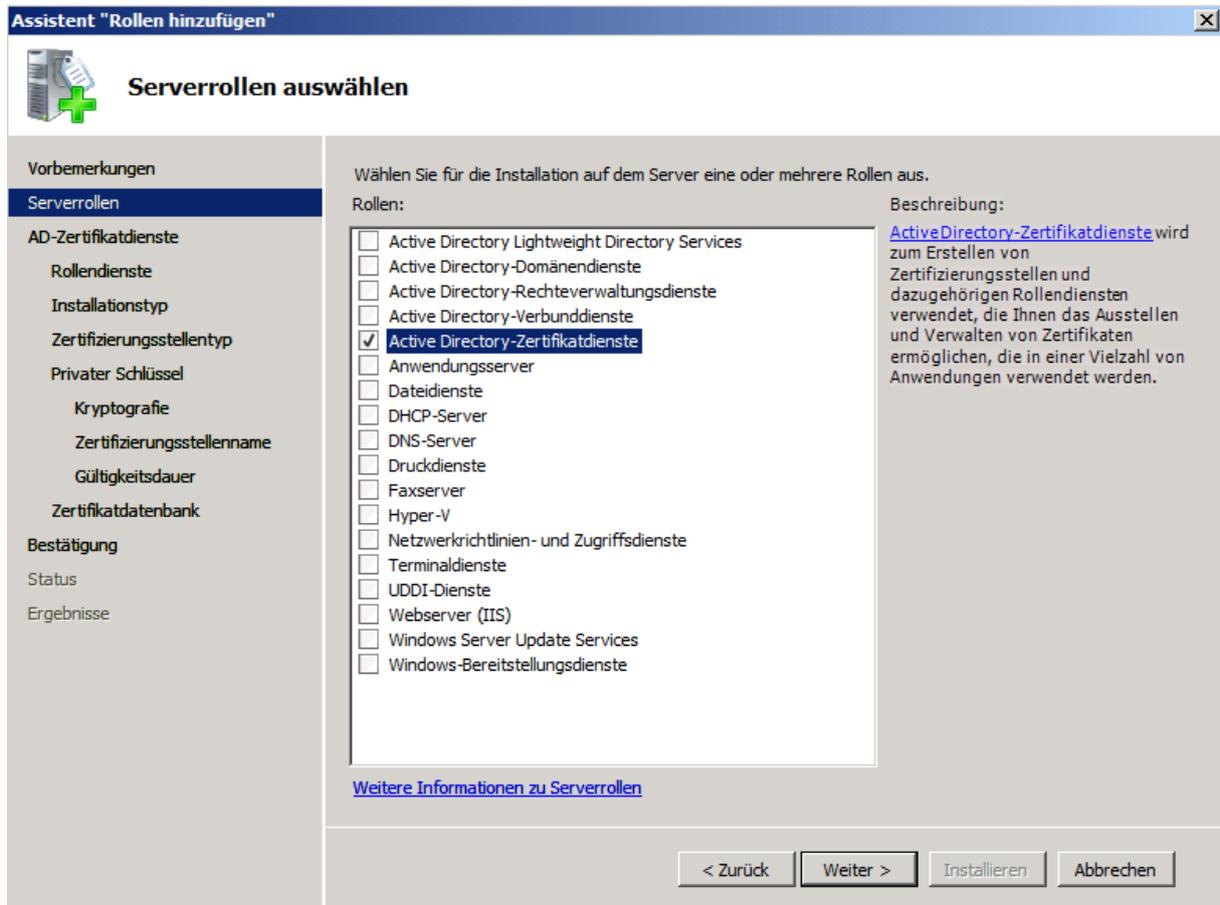
Zertifikatdienste auf dem alten Server deinstallieren



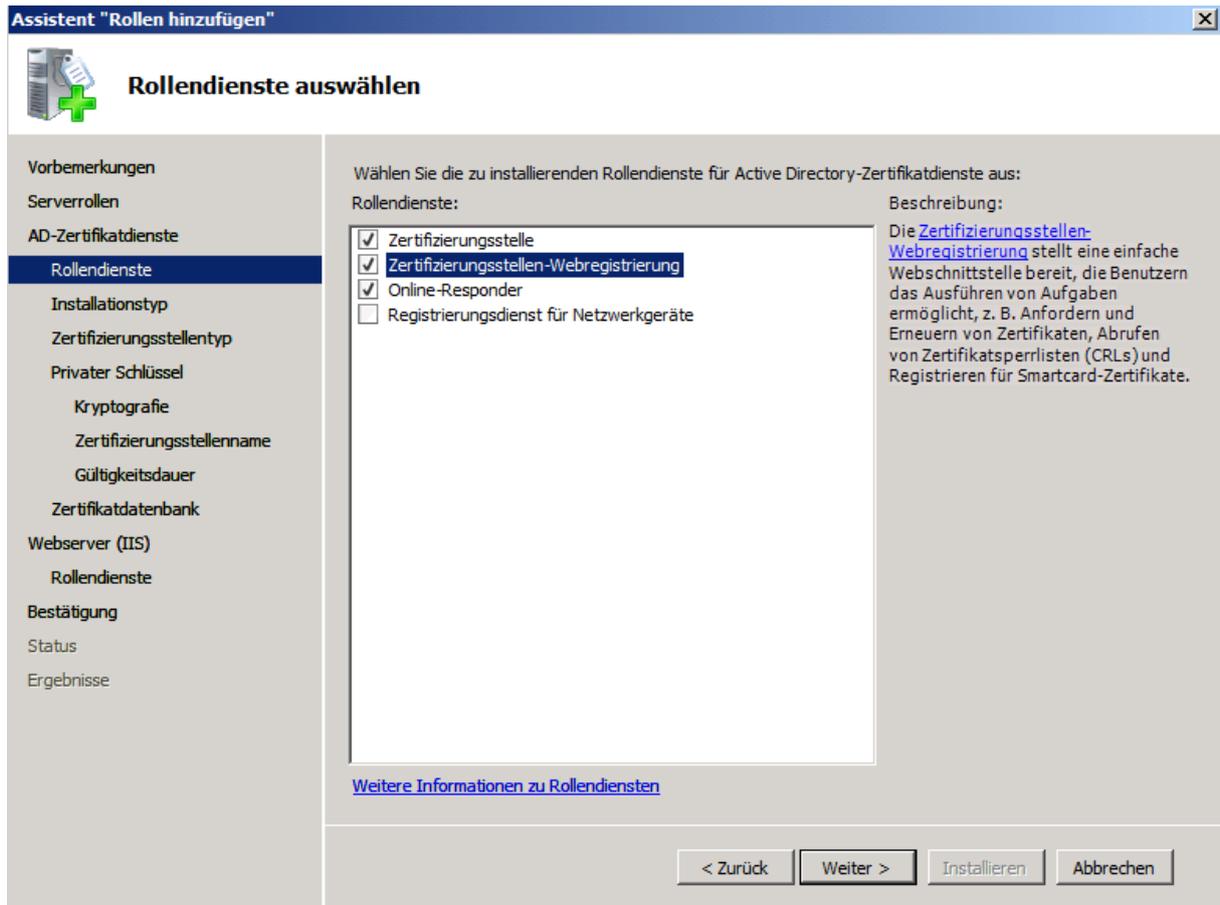
IP Adresse des alten Servers ändern, Server umbenennen, und neu starten

Dem neuen PKI Server den gleichen Namen und IP Adresse wie fuer den alten PKI Server vergeben (Nicht zwingend notwendig, wichtig ist, dass der Name der CA nicht veraendert wird).

Rolle Zertifikatdienste auf dem Windows Server 2008 installieren



Installation zusätzlicher Rollendienste



Unternehmens CA auswählen

Stammzertifizierungsstelle

Vorhandenen Schlüssel der alten Zertifizierungsstelle auswählen

Assistent "Rollen hinzufügen"

## Privaten Schlüssel einrichten

**Vorbemerkungen**

Die Zertifizierungsstelle benötigt einen privaten Schlüssel, um Zertifikate für Clients zu generieren und auszustellen. Geben Sie an, ob Sie einen neuen privaten Schlüssel erstellen oder einen vorhandenen Schlüssel verwenden möchten.

**Serverrollen**

**AD-Zertifikatdienste**

- Rollendienste
- Installationstyp
- Zertifizierungsstellentyp
- Privater Schlüssel**
  - Vorhandenes Zertifikat**
  - Zertifikatdatenbank
  - Webserver (IIS)
  - Rollendienste
  - Bestätigung
  - Status
  - Ergebnisse

Neuen privaten Schlüssel erstellen  
Verwenden Sie diese Option, wenn Sie keinen privaten Schlüssel besitzen oder einen neuen privaten Schlüssel erstellen möchten, um die Sicherheit zu erhöhen. Sie werden aufgefordert, für den privaten Schlüssel einen Kryptografiedienstanbieter auszuwählen und eine Schlüssellänge anzugeben. Zum Ausstellen neuer Zertifikate müssen Sie zudem einen Hashalgorithmus auswählen.

Vorhandenen privaten Schlüssel verwenden  
Verwenden Sie diese Option, um beim erneuten Installieren einer Zertifizierungsstelle zuvor ausgestellte Zertifikate weiterverwenden zu können, um die Kontinuität zu gewährleisten.

Zertifikat auswählen und dazugehörigen privaten Schlüssel verwenden  
Wählen Sie diese Option, wenn auf diesem Computer ein Zertifikat vorhanden ist oder wenn Sie ein Zertifikat importieren und den dazugehörigen privaten Schlüssel verwenden möchten.

Vorhandenen privaten Schlüssel auf diesem Computer auswählen  
Wählen Sie diese Option, wenn Sie private Schlüssel von einer vorherigen Installation beibehalten haben oder einen privaten Schlüssel aus einer anderen Quelle verwenden möchten.

[Weitere Informationen zu öffentlichen und privaten Schlüsseln](#)

< Zurück   Weiter >   Installieren   Abbrechen

Angabe des Pfades und des Kennworts

Assistent "Rollen hinzufügen" X



## Auswählen eines vorhandenen Zertifikats

**Vorbemerkungen**

Serverrollen

AD-Zertifikatdienste

Rollendienste

Installationstyp

Zertifizierungsstellentyp

Privater Schlüssel

Vorhandenes Zertifikat

Zertifikatdatenbank

Webserver (IIS)

Rollendienste

Bestätigung

Status

Ergebnisse

Zum Verwenden eines privaten Schlüssels, der mit einem Zertifikat verknüpft ist, müssen Sie das Zertifikat auswählen. Möglicherweise müssen Sie ein Zertifikat importieren, wenn es nicht auf diesem Computer verfügbar ist. Das ausgewählte Zertifikat und die dazugehörigen Eigenschaften werden für diese Zertifizierungsstelle verwendet.

Zertifikate:

Antragsteller	Ausgestellt von	Ablaufdatum	

Verstärkte Sicherheitsfeatures für den privaten Schlüssel verwenden, die vom Kryptografiedienstanbieter bereitgestellt werden (dies erfordert möglicherweise eine Administratorinteraktion bei jedem Zertifizierungsstellenzugriff auf den privaten Schlüssel)

**PFX-Datei öffnen** X

Wählen Sie die "PKCS #12"-Datei aus, die Sie importieren möchten, und geben Sie das Kennwort für diese Datei an.

Dateiname:

Kennwort:

Da isser

Assistent "Rollen hinzufügen" X

 **Auswählen eines vorhandenen Zertifikats**

Zum Verwenden eines privaten Schlüssels, der mit einem Zertifikat verknüpft ist, müssen Sie das Zertifikat auswählen. Möglicherweise müssen Sie ein Zertifikat importieren, wenn es nicht auf diesem Computer verfügbar ist. Das ausgewählte Zertifikat und die dazugehörigen Eigenschaften werden für diese Zertifizierungsstelle verwendet.

**Zertifikate:**

Antragsteller	Ausgestellt von	Ablaufdatum	
 RootCA	RootCA	30.09.2017	

Verstärkte Sicherheitsfeatures für den privaten Schlüssel verwenden, die vom Kryptografiedienstanbieter bereitgestellt werden (dies erfordert möglicherweise eine Administratorinteraktion bei jedem Zertifizierungsstellenzugriff auf den privaten Schlüssel)

**Navigation:**

- Vorbemerkungen
- Serverrollen
- AD-Zertifikatsdienste
  - Rolldienste
  - Installationstyp
  - Zertifizierungsstellentyp
  - Privater Schlüssel
  - Vorhandenes Zertifikat**
  - Zertifikatsdatenbank
- Webserver (IIS)
  - Rolldienste
- Bestätigung
- Status
- Ergebnisse

Angabe des Pfades zur CA Datenbank

Assistent "Rollen hinzufügen" X

 **Zertifikatdatenbank konfigurieren**

**Vorbemerkungen**  
Serverrollen  
AD-Zertifikatdienste  
    Rollendienste  
    Installationstyp  
    Zertifizierungsstellentyp  
    Privater Schlüssel  
        Vorhandenes Zertifikat  
**Zertifikatdatenbank**  
Webserver (IIS)  
    Rollendienste  
Bestätigung  
Status  
Ergebnisse

In der Zertifikatdatenbank werden alle Zertifikatanforderungen, ausgestellte Zertifikate sowie gesperrte oder abgelaufene Zertifikate aufgezeichnet. Mit dem Datenbankprotokoll kann die Verwaltungsaktivität für eine Zertifizierungsstelle überwacht werden.

Speicherort der Zertifikatdatenbank:

Vorhandene Zertifikatdatenbank aus vorheriger Installation an diesem Speicherort verwenden

Speicherort des Zertifikatdatenbankprotokolls:

Auswahl zusätzlicher Rollendienste

Assistent "Rollen hinzufügen"

## Installationsauswahl bestätigen

Vorbemerkungen  
Serverrollen  
AD-Zertifikatdienste  
    Rollendienste  
    Installationstyp  
    Zertifizierungsstellentyp  
    Privater Schlüssel  
        Vorhandenes Zertifikat  
    Zertifikatdatenbank  
Webserver (IIS)  
    Rollendienste  
**Bestätigung**  
Status  
Ergebnisse

Klicken Sie auf "Installieren", um die folgenden Rollen, Rollendienste bzw. Features zu installieren.

⚠ 1 Warn-, 2 Informationsmeldungen folgen unten

ℹ Der Server muss nach Abschluss der Installation möglicherweise neu gestartet werden.

⤴ **Active Directory-Zertifikatdienste**

**Zertifizierungsstelle**

⚠ Der Name und die Domäneneinstellungen dieses Computers können nach der Installation der Zertifizierungsstelle nicht mehr geändert werden.

Zertifizierungsstellentyp:	Stammzertifizierungsstelle des Unternehmens
Kryptografiedienstanbieter:	Microsoft Strong Cryptographic Provider
Kryptografiedienstanbieter-Interaktion zulassen:	Deaktiviert
Gültigkeitsdauer des Zertifikats:	30.09.2017 10:14
Definierter Name:	CN=RootCA, DC=, DC=
Speicherort der Zertifikatdatenbank:	C:\Windows\system32\CertLog
Speicherort des Zertifikatdatenbankprotokolls:	C:\Windows\system32\CertLog

**Zertifizierungsstellen-Webregistrierung**

**Online-Responder**

⤴ **Webserver (IIS)**

ℹ Weitere Informationen zum Windows-Systemressourcen-Manager (WSRM) und zum Optimieren

[Informationen drucken, per E-Mail senden oder speichern](#)

< Zurück   Weiter >   Installieren   Abbrechen

Installation wird durchgeführt



## Installationsstatus

- Vorbemerkungen
- Serverrollen
- AD-Zertifikatdienste
  - Rollendienste
  - Installationstyp
  - Zertifizierungsstellentyp
  - Privater Schlüssel
    - Vorhandenes Zertifikat
  - Zertifikatdatenbank
- Webserver (IIS)
  - Rollendienste
- Bestätigung
- Status**
- Ergebnisse

Die folgenden Rollen, Rollendienste bzw. Features werden installiert:

<b>Active Directory-Zertifikatdienste</b>
<b>Webserver (IIS)</b>
<b>Windows-Prozessaktivierungsdienst</b>



Installation wird initialisiert...

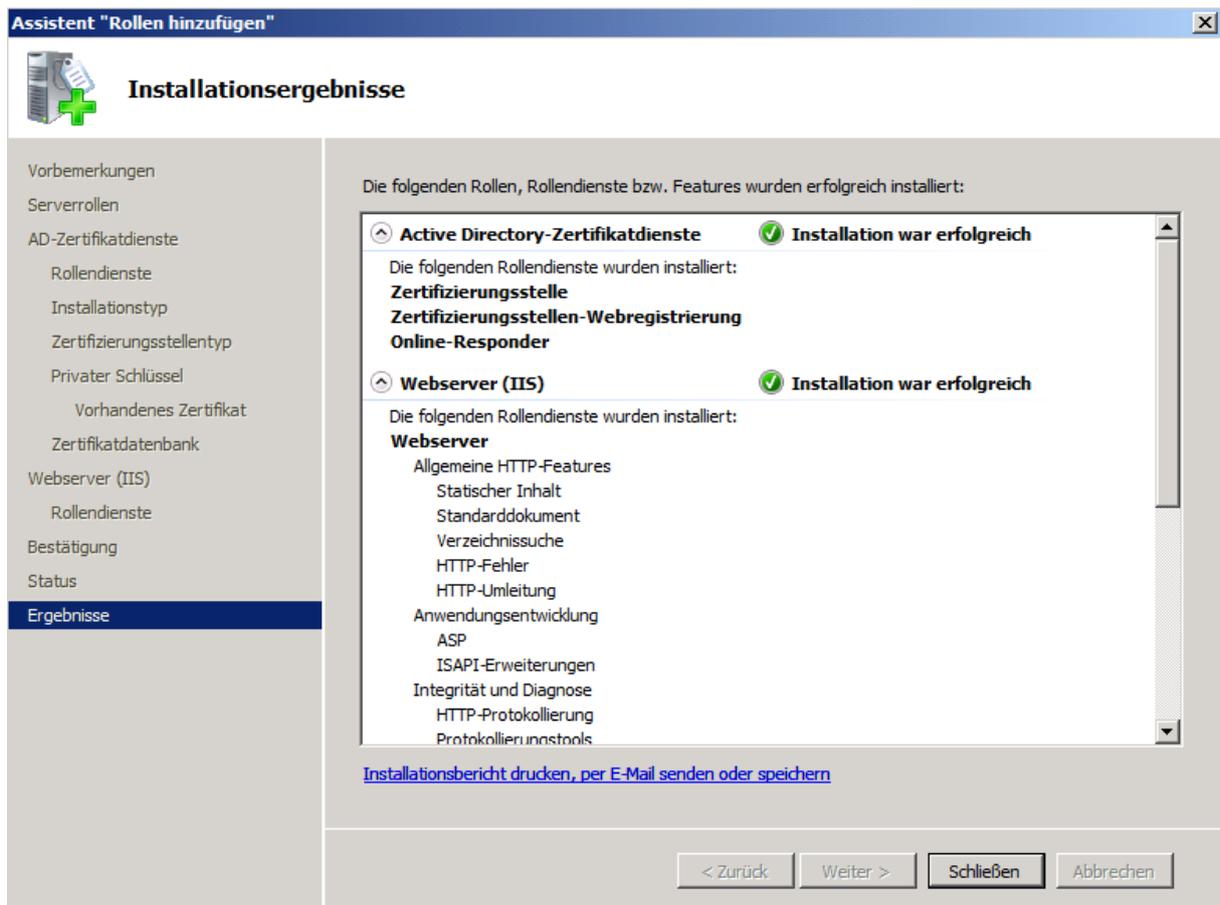
< Zurück

Weiter >

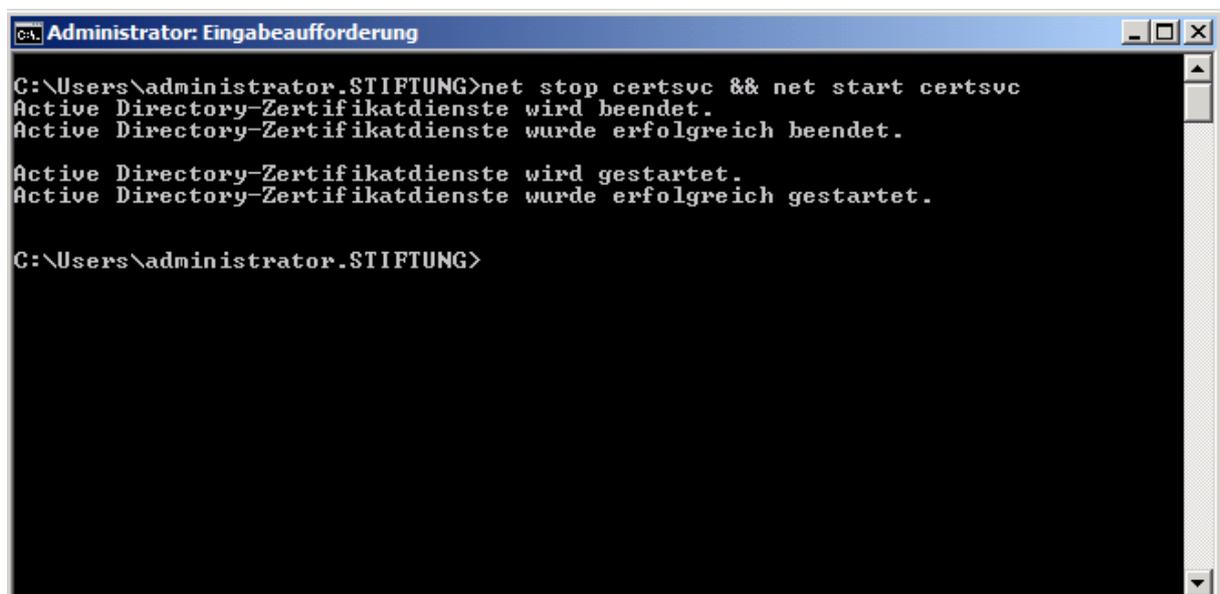
Installieren

Abbrechen

Installation wird fertig gestellt



Zertifikatdienste stoppen und starten



Import der exportierten Registry Informationen auf der neuen CA.

Vor dem importieren muss der Inhalt der Registrierungs-Datei geprüfert werden und bei zum Bsp. anderen Servernamen und Datenbankpfaden eine Anpassung vorgenommen werden.

```

CA - Editor
Datei Bearbeiten Format Ansicht ?
Windows Registry Editor Version 5.00

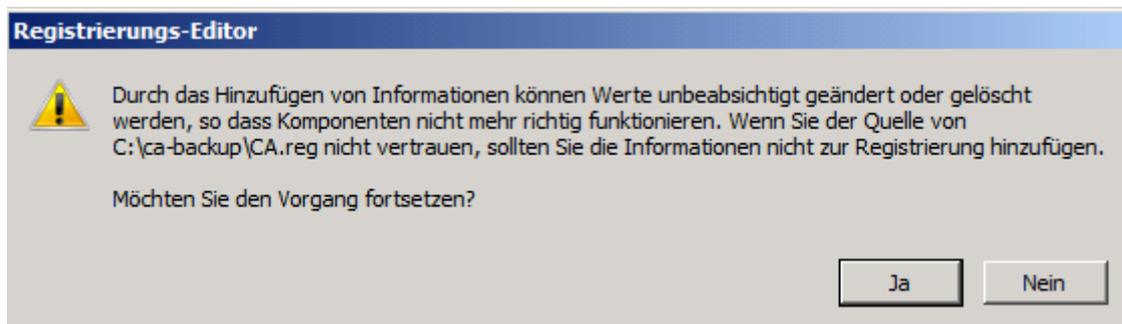
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Certsvc]
"Type"=dword:00000010
"Start"=dword:00000002
"ErrorControl"=dword:00000001
"ImagePath"=hex(2):43,00,3a,00,5c,00,57,00,49,00,4e,00,44,00,4f,00,57,00,53,00,\
5c,00,73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,63,00,65,00,72,\
00,74,00,73,00,72,00,76,00,2e,00,65,00,78,00,65,00,00,00
"DisplayName"="Zertifikatdienste"
"ObjectName"="LocalSystem"
"Description"="Erstellt, verwaltet und entfernt x.509-Zertifikate für Anwendungen wie z. B. S/MIME und SSL. v

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Certsvc\Configuration]
"SetupStatus"=dword:00002003
"Active"="RootCA"
"DBDirectory"="C:\\WINDOWS\\system32\\CertLog"
"DBLogDirectory"="C:\\WINDOWS\\system32\\CertLog"
"DBTempDirectory"="C:\\WINDOWS\\system32\\CertLog"
"DBSystemDirectory"="C:\\WINDOWS\\system32\\CertLog"
"DesessionCount"=dword:00000014
"LDAPFlags"=dword:00000000
"DBFlags"=dword:000000b8
"Version"=dword:00020002
"DBLastRecovery"=hex:32,ea,fa,b8,3e,bb,c8,01
"DBLastFullBackup"=hex:de,23,2b,41,ee,a6,c9,01

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Certsvc\Configuration\RootCA]
"SetupStatus"=dword:00000003
"DSConfigDN"="CN=Configuration,DC=,DC="
"DSDomainDN"="DC=,DC="
"ViewAgeMinutes"=dword:00000010
"ViewIdleMinutes"=dword:00000008
"CAType"=dword:00000000
"UseDS"=dword:00000001
"ForceTeletex"=dword:00000012
"SignedAttributes"=hex(7):52,00,65,00,71,00,75,00,65,00,73,00,74,00,65,00,72,\
00,4e,00,61,00,6d,00,65,00,00,00,00,00
"CommonName"="RootCA"
"Enabled"=dword:00000001
"PolicyFlags"=dword:00000000
"CertEnrollCompatible"=dword:00000000
"CRLEditFlags"=dword:00000100
"CRFlags"=dword:00000002
"InterfaceFlags"=dword:00000040
"EnforceX509NameLengths"=dword:00000001
"SubjectTemplate"=hex(7):45,00,4d,00,61,00,69,00,6c,00,00,00,43,00,6f,00,6d,00,\
6d,00,6f,00,6e,00,4e,00,61,00,6d,00,65,00,00,00,4f,00,72,00,67,00,61,00,6e,\

```

## Importieren der Konfiguration



## Die importierten Einstellungen in der Registry

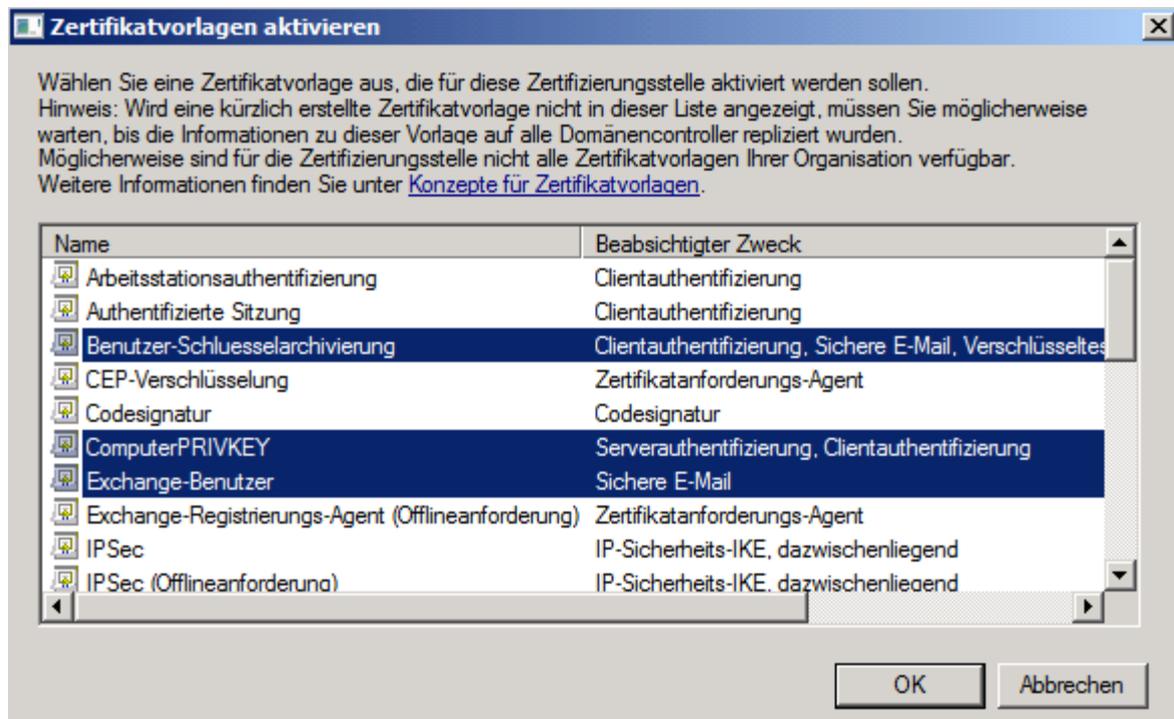
Registrierungs-Editor		
Datei Bearbeiten Ansicht Favoriten ?		
Name	Typ	Wert
(Standard)	REG_SZ	(Wert nicht gesetzt)
ACertHash	REG_MULTI_SZ	9c c6 24 bf 3e 0a 33 37 25 3c e4 c6 75 5b 49 ae bb f0 ...
ACertPublicatio...	REG_MULTI_SZ	1:C:\WINDOWS\system32\CertSrv\CertEnroll\%1_%3...
AServerName	REG_SZ	srv [REDACTED]
CAType	REG_DWORD	0x00000000 (0)
CAXchgCertHash	REG_MULTI_SZ	31 14 21 d4 c2 98 35 8f 5b 81 bb 45 f7 de 80 83 91 ae...
CAXchgOverlapP...	REG_SZ	Days
CAXchgOverlapP...	REG_DWORD	0x00000001 (1)
CAXchgValidityPe...	REG_SZ	Weeks
CAXchgValidityPe...	REG_DWORD	0x00000001 (1)
CertEnrollCompat...	REG_DWORD	0x00000000 (0)
ClockSkewMinutes	REG_DWORD	0x0000000a (10)
CommonName	REG_SZ	RootCA
CRLAttemptRepu...	REG_DWORD	0x00000001 (1)
CRLDeltaNextPu...	REG_BINARY	e8 94 52 55 c7 a7 c9 01
CRLDeltaOverlap...	REG_SZ	Minutes
CRLDeltaOverlap...	REG_DWORD	0x00000000 (0)
CRLDeltaPeriod	REG_SZ	Months
CRLDeltaPeriodU...	REG_DWORD	0x00000000 (0)
CRLEditFlags	REG_DWORD	0x00000100 (256)
CRLFlags	REG_DWORD	0x00000002 (2)
CRLNextPublish	REG_BINARY	80 b8 ad b5 5b bf c9 01
CRLOverlapPeriod	REG_SZ	Hours
CRLOverlapUnits	REG_DWORD	0x00000000 (0)
CRLPeriod	REG_SZ	Months
CRLPeriodUnits	REG_DWORD	0x00000001 (1)
CRLPublicationURLs	REG_MULTI_SZ	65:C:\WINDOWS\system32\CertSrv\CertEnroll\%3%8...
DSConfigDN	REG_SZ	CN=Configuration,DC=[REDACTED]DC=[REDACTED]
DSDomainDN	REG_SZ	DC=[REDACTED]DC=[REDACTED]
EKUIDsForPubli...	REG_MULTI_SZ	1.3.6.1.5.5.7.3.3 1.3.6.1.4.1.311.61.1.1
Enabled	REG_DWORD	0x00000001 (1)
EnforceX500Nam...	REG_DWORD	0x00000001 (1)
ForceTeletex	REG_DWORD	0x00000012 (18)
HighSerial	REG_DWORD	0x00000000 (0)
InterfaceFlags	REG_DWORD	0x00000040 (64)
KRACertCount	REG_DWORD	0x00000001 (1)
KRACertHash	REG_MULTI_SZ	37 61 46 90 e2 7c d2 ff 44 ee 31 d0 83 93 c7 1e 66 ea ...

Die Zertifikatdienste neu starten

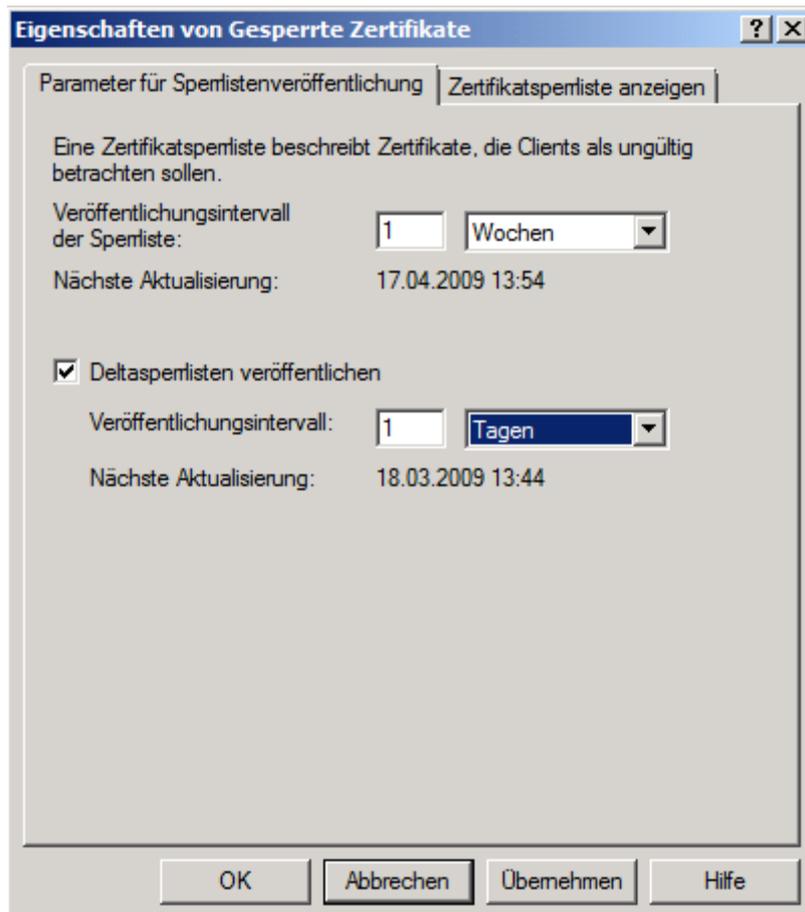
Die CA wurde komplett wiederhergestellt

Anforderungs-ID	Name des Antragstellers	Binäres Zertifikat	Zertifikatvorlage	Seriennummer	Anfangsdatum des Zertifikats	Ablaufdatum des Zertifikats
2	...	-----BEGIN CERT...	Computer (Mach...	1471f3a9000...	30.09.2007 10:15	29.09.2008 11
3	...	-----BEGIN CERT...	Domänencontroll...	1482734b000...	30.09.2007 10:33	29.09.2008 11
4	...	-----BEGIN CERT...	Domänencontroll...	14891933000...	30.09.2007 10:40	29.09.2008 11
5	...	-----BEGIN CERT...	Domänencontroll...	14d6b2cc000...	30.09.2007 12:05	29.09.2008 11
6	...	-----BEGIN CERT...	Zertifizierungsst...	6102f18a000...	30.09.2007 14:56	07.10.2007 11
7	...	-----BEGIN CERT...	Webserver (We...	6103ef14000...	30.09.2007 14:57	29.09.2009 11
8	...	-----BEGIN CERT...	Computer (Mach...	610c17e2000...	30.09.2007 15:06	29.09.2008 11
9	...	-----BEGIN CERT...	Computer-PRIVK...	610f87a5000...	30.09.2007 15:10	30.09.2009 11
10	...	-----BEGIN CERT...	ComputerPRIVK...	6110ac30000...	30.09.2007 15:11	30.09.2009 11
11	...	-----BEGIN CERT...	Domänencontroll...	618a8f31000...	01.10.2007 13:30	30.09.2008 11
12	...	-----BEGIN CERT...	Domänencontroll...	61eea4d5000...	01.10.2007 15:20	30.09.2008 11
13	...	-----BEGIN CERT...	Domänencontroll...	111edded000...	01.10.2007 16:12	30.09.2008 11
14	...	-----BEGIN CERT...	Domänencontroll...	17be6cda000...	27.11.2007 07:17	26.11.2008 01
15	...	-----BEGIN CERT...	Domänencontroll...	494a936b000...	20.12.2007 19:46	19.12.2008 11
16	...	-----BEGIN CERT...	Domänencontroll...	4a8cc981000...	21.12.2007 01:38	20.12.2008 01
17	...	-----BEGIN CERT...	Computer (Mach...	3c7d7d47000...	12.02.2008 08:39	11.02.2009 01
18	...	-----BEGIN CERT...	Zertifizierungsst...	17c39a1c000...	14.04.2008 09:42	21.04.2008 01
19	...	-----BEGIN CERT...	Schlüsselwieder...	17f30a75000...	14.04.2008 10:34	14.04.2010 11
21	...	-----BEGIN CERT...	Benutzer-Schlu...	17f92c48000...	14.04.2008 10:41	14.04.2010 11
22	...	-----BEGIN CERT...	Registrierungs-A...	18528499000...	14.04.2008 12:18	14.04.2010 11
23	...	-----BEGIN CERT...	Registrierungs-A...	1860dd92000...	14.04.2008 12:34	14.04.2010 11
24	...	-----BEGIN CERT...	Smartcard-Anme...	1861786a000...	14.04.2008 12:35	14.04.2009 11
25	...	-----BEGIN CERT...	Registrierungs-A...	188d5d5b000...	14.04.2008 13:23	14.04.2010 11
26	...	-----BEGIN CERT...	Registrierungs-A...	13e52efd000...	15.04.2008 08:06	15.04.2010 01
27	...	-----BEGIN CERT...	Benutzer (User)	141b2c19000...	15.04.2008 09:05	15.04.2009 01
28	...	-----BEGIN CERT...	Registrierungs-A...	141bd662000...	15.04.2008 09:05	15.04.2010 01
29	...	-----BEGIN CERT...	Registrierungs-A...	1434e8d7000...	15.04.2008 09:33	15.04.2010 01
30	...	-----BEGIN CERT...	Smartcard-Anme...	1435fce7000...	15.04.2008 09:34	15.04.2009 01
31	...	-----BEGIN CERT...	Smartcard-Anme...	146c51f6000...	15.04.2008 10:33	15.04.2009 11
32	...	-----BEGIN CERT...	Smartcard-Anme...	1474c5c7000...	15.04.2008 10:43	15.04.2009 11
33	...	-----BEGIN CERT...	Untergeordnete ...	155981a0000...	15.04.2008 14:52	15.04.2010 11
34	...	-----BEGIN CERT...	Smartcard-Anme...	1574391b000...	15.04.2008 15:22	15.04.2009 11
35	...	-----BEGIN CERT...	Registrierungs-A...	18c30ff0000...	16.04.2008 06:47	16.04.2010 01
36	...	-----BEGIN CERT...	Benutzer (User)	1568b0fa000...	16.05.2008 12:23	16.05.2009 11
37	...	-----BEGIN CERT...	Smartcard-Anme...	2459c2b0000...	19.05.2008 10:01	19.05.2009 11
41	...	-----BEGIN CERT...	Domänencontroll...	613fae8d000...	19.05.2008 12:04	19.05.2009 11

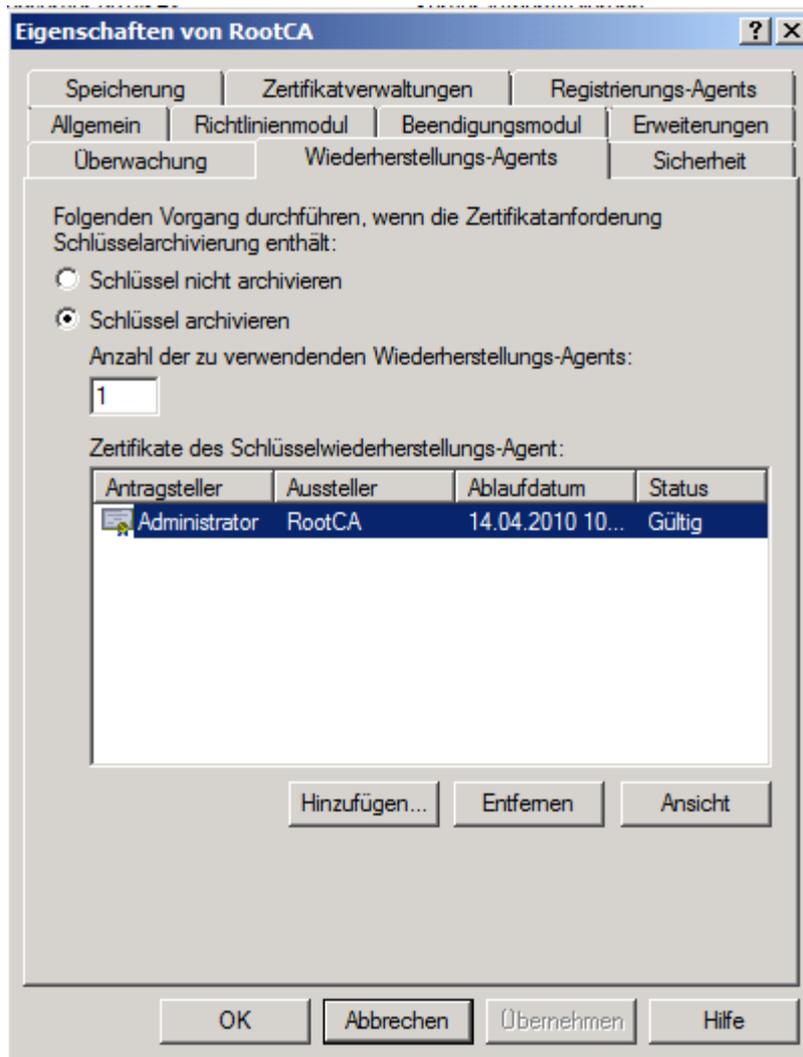
Die selbst erstellten V2 Templates muessen neu ausgestellt werden



Die hochgesetzten Zeiten fuer die Base und Delta CRL Veroeffentlichung zurueck setzen

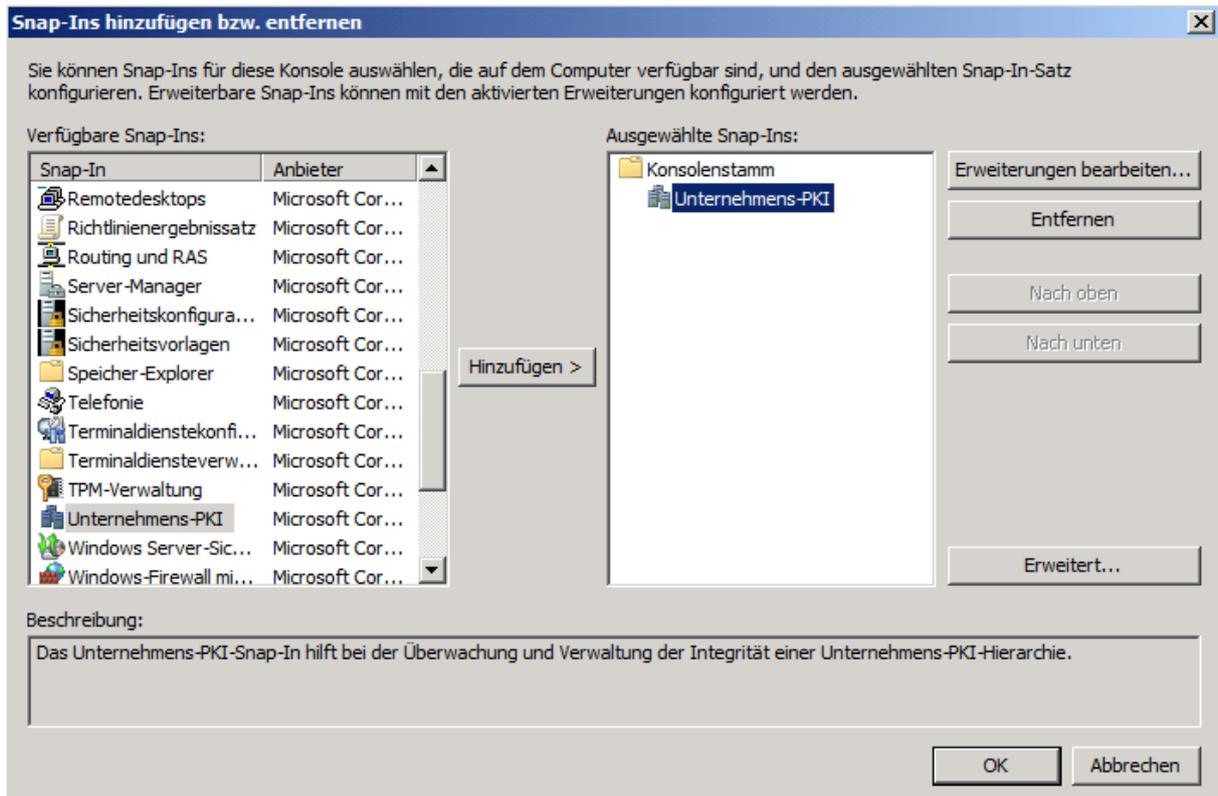


Das KRA Zertifikat wurde auch wiederhergestellt.



Fertig

Der Zustand der CA kann jetzt noch mit dem in Windows Server 2008 integrierten PKI Health Utility gecheckt werden.



Alles roger

