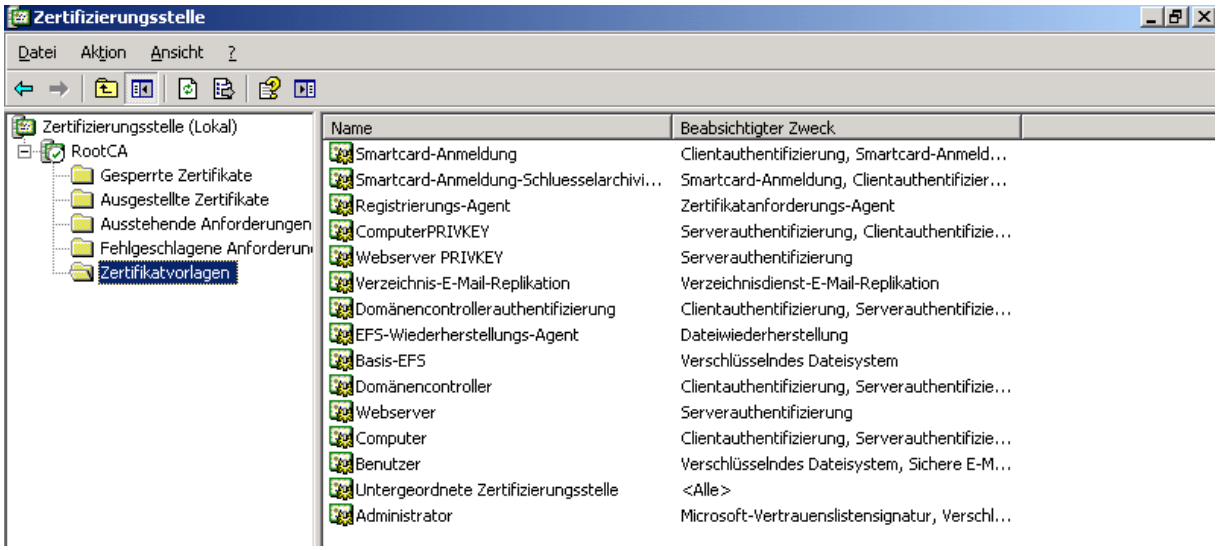
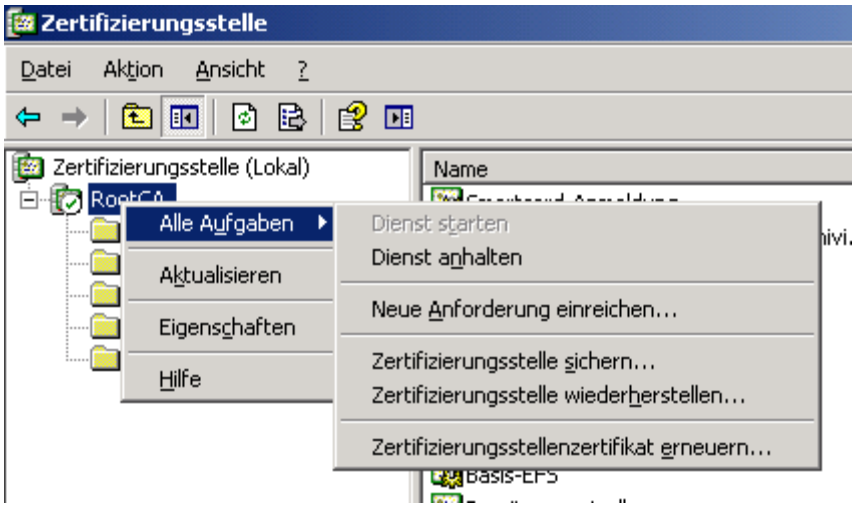
Windows Server 2003 CA Migration auf Windows Server 2008

Windows Server 2003 CA sichern

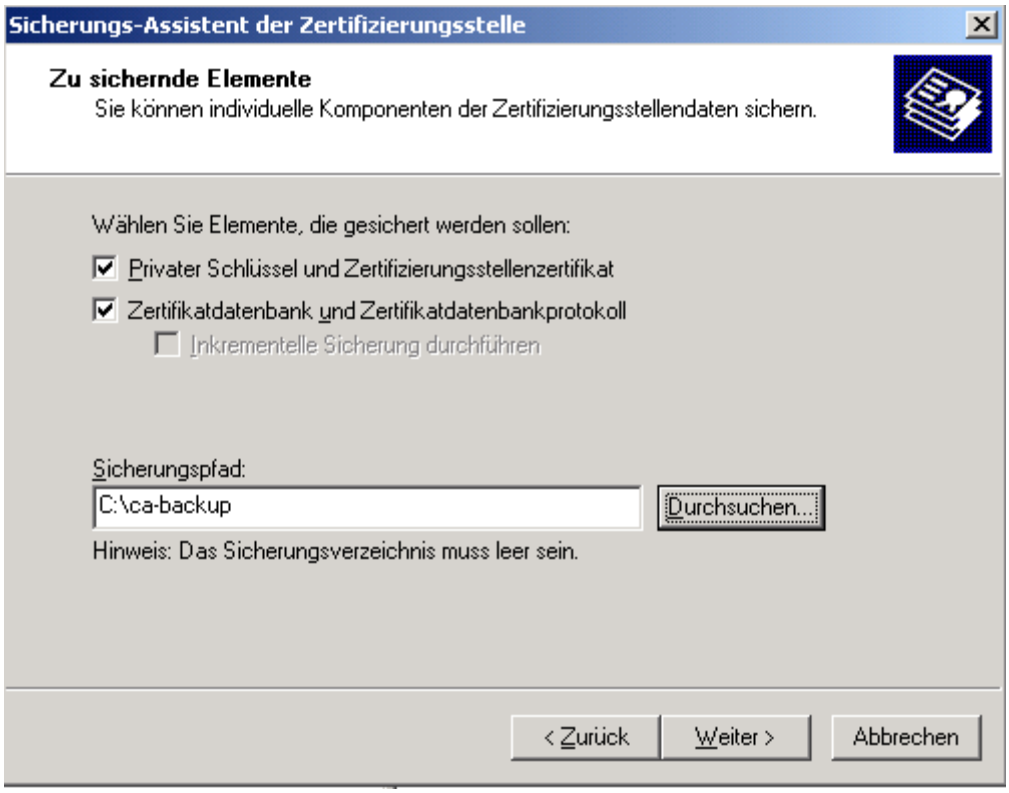
Windows Server 2003 CA



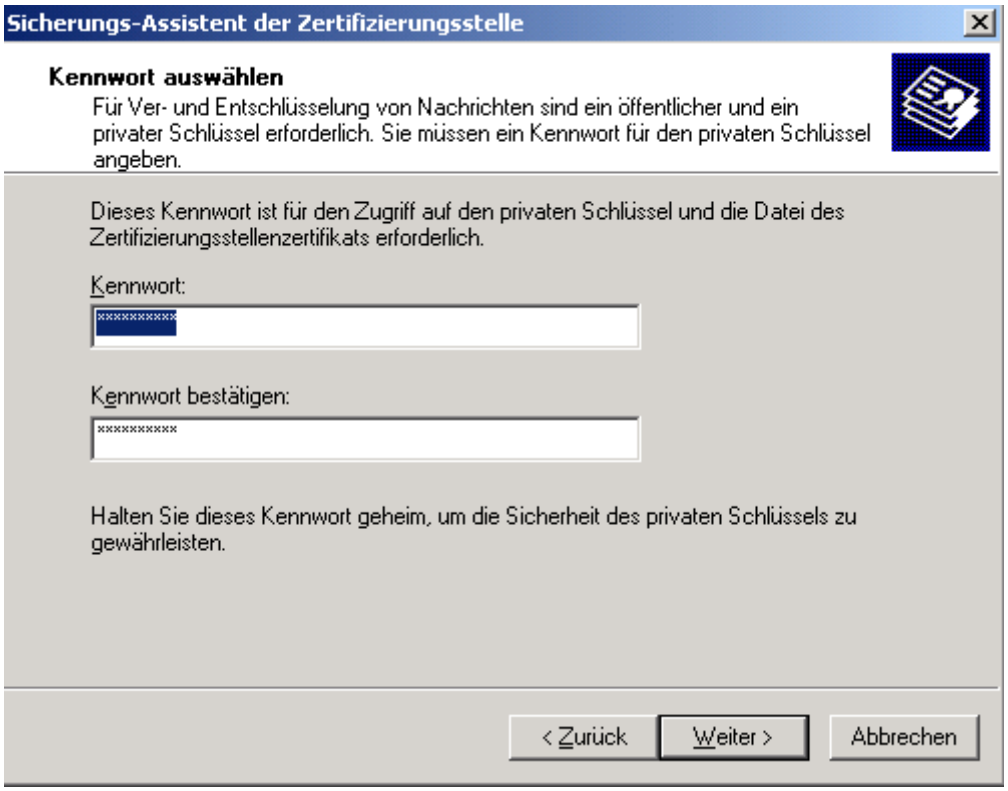
Sichern der Zertifizierungsstelle



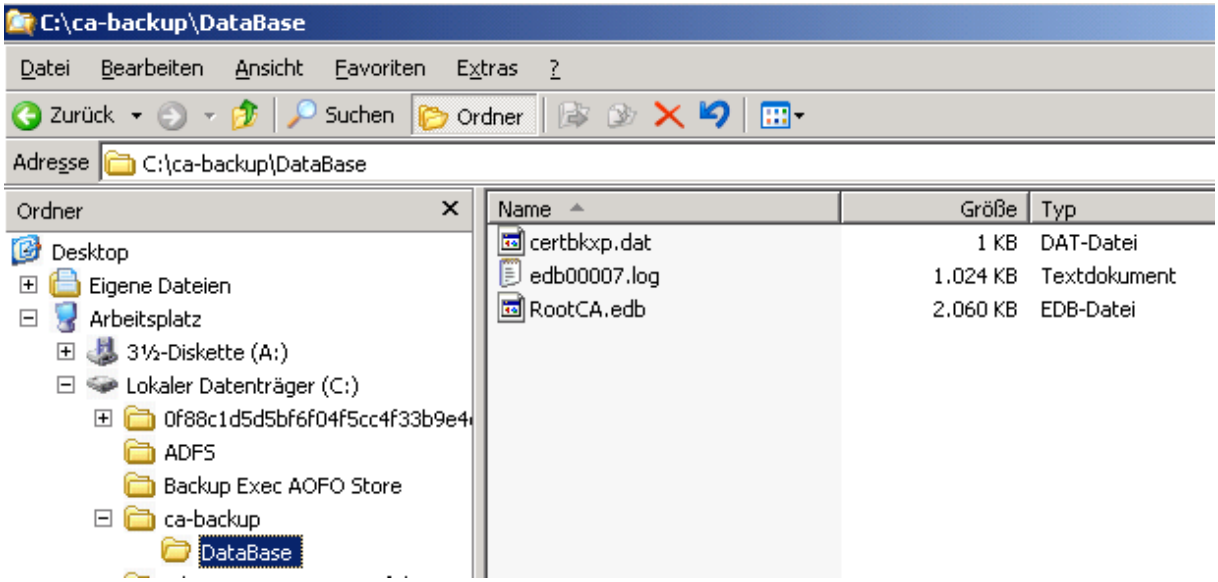
Optionen zur Sicherung



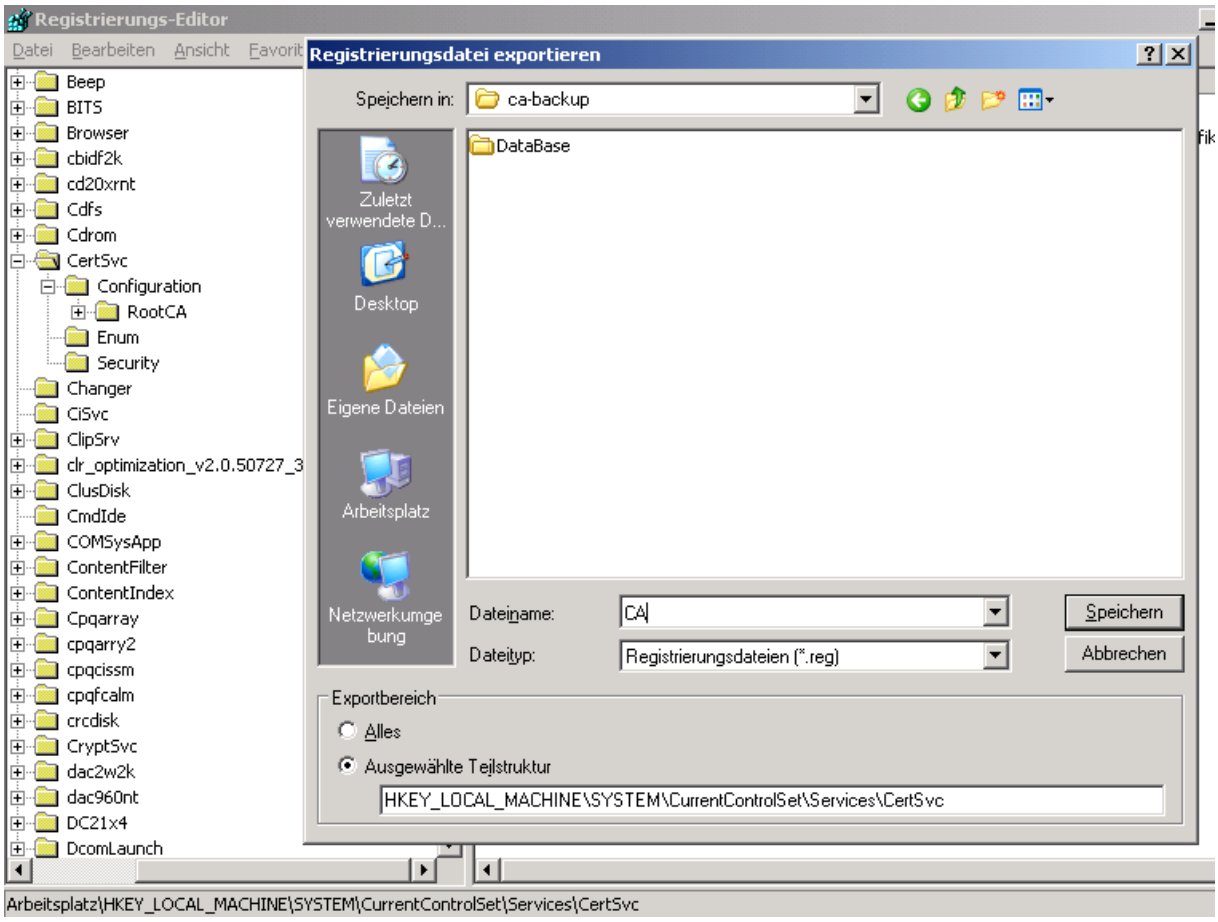
Sicherung des Exports



Datenbank Sicherung

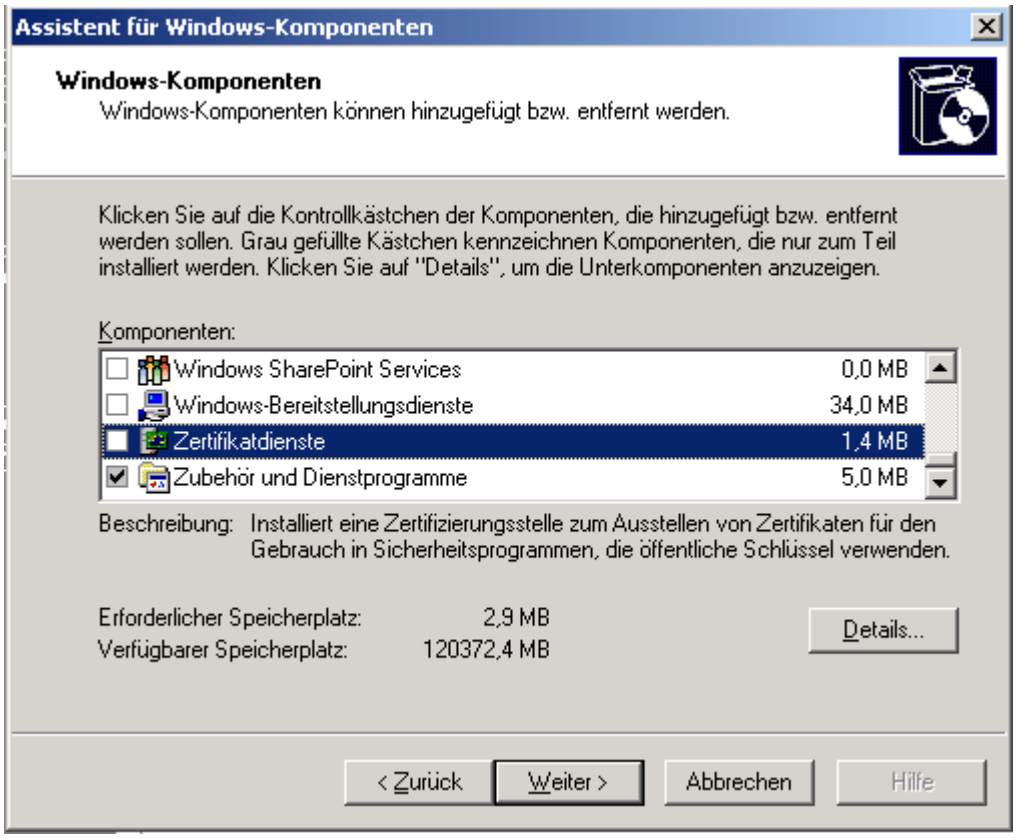


HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc exportieren



CA Backup auf den neuen Server kopieren

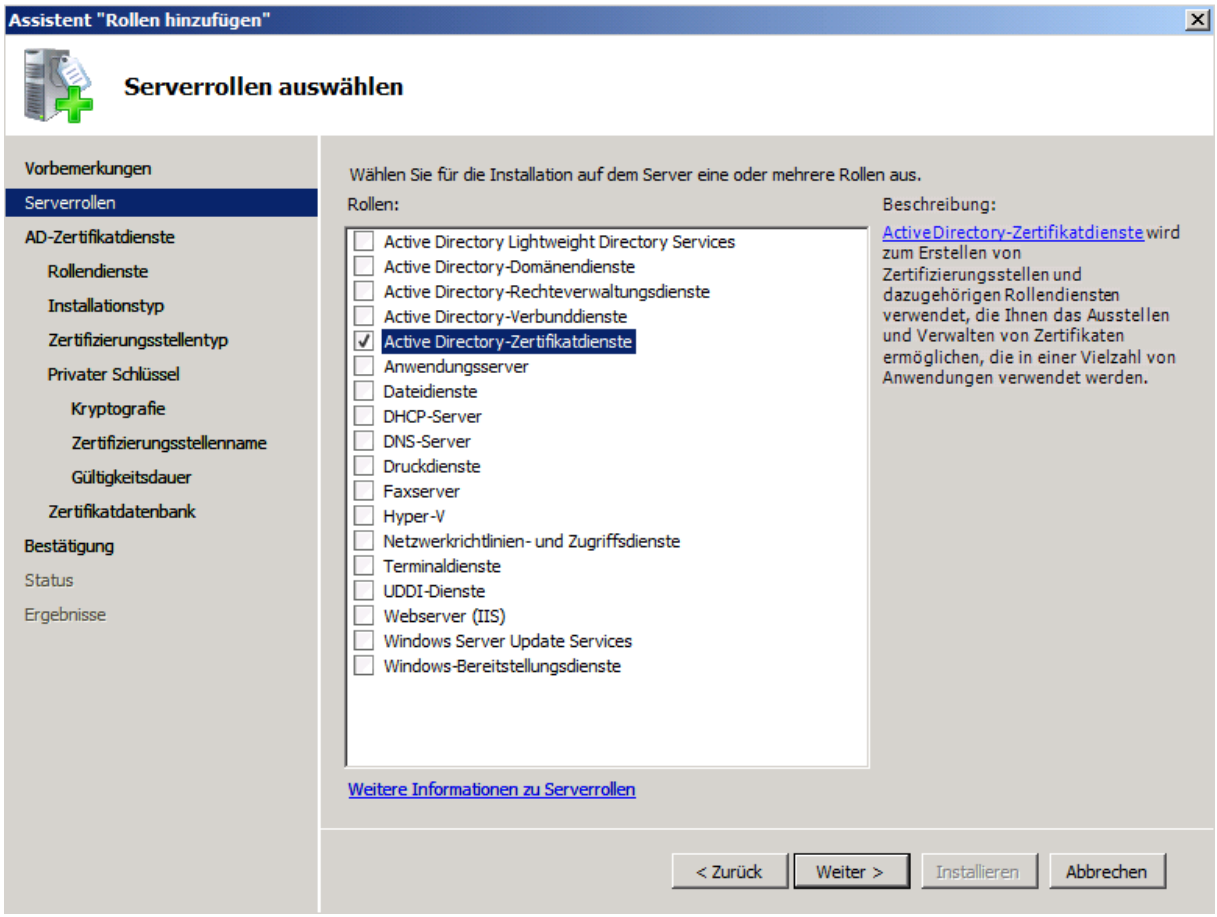
Zertifikatdienste auf dem alten Server deinstallieren



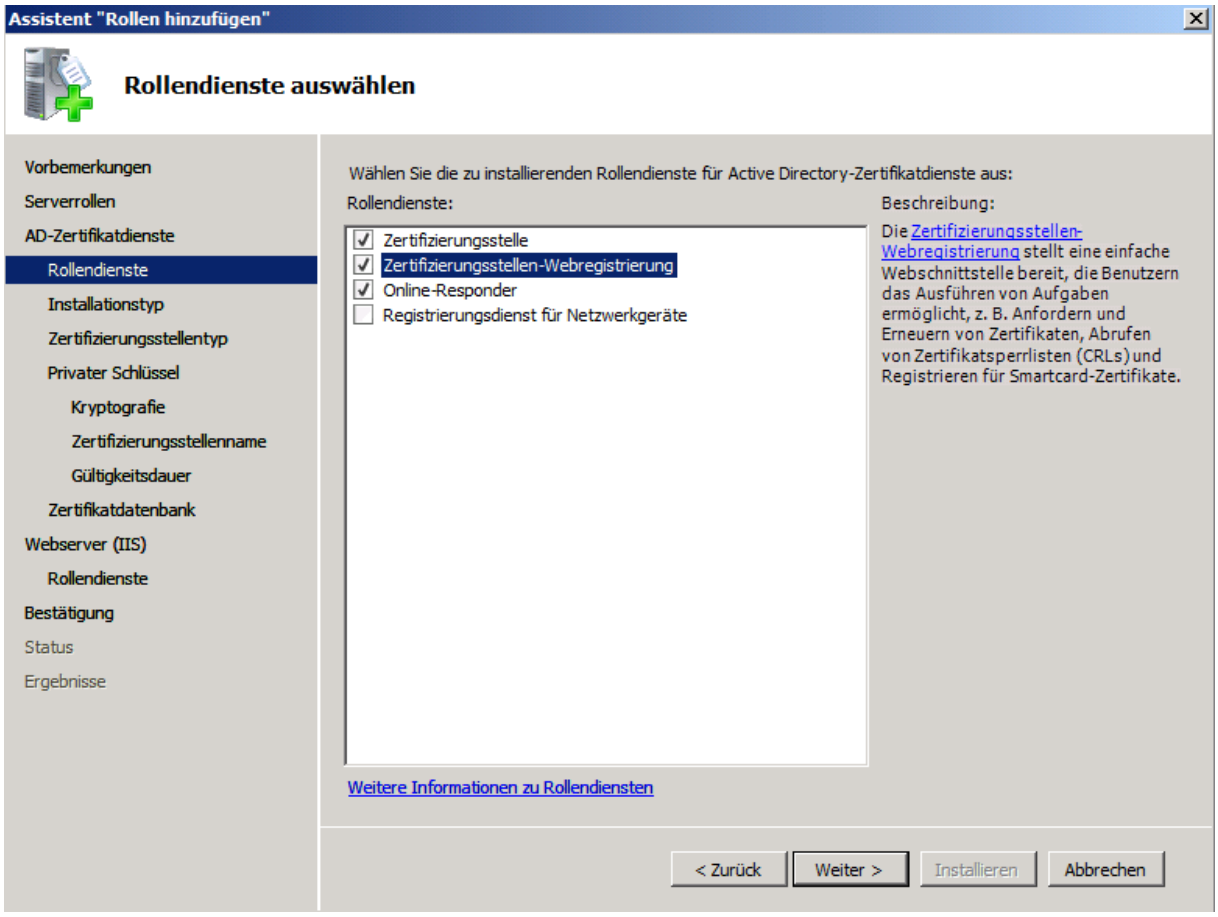
IP Adresse des alten Servers aendern, Server umbenennen, und neu starten

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



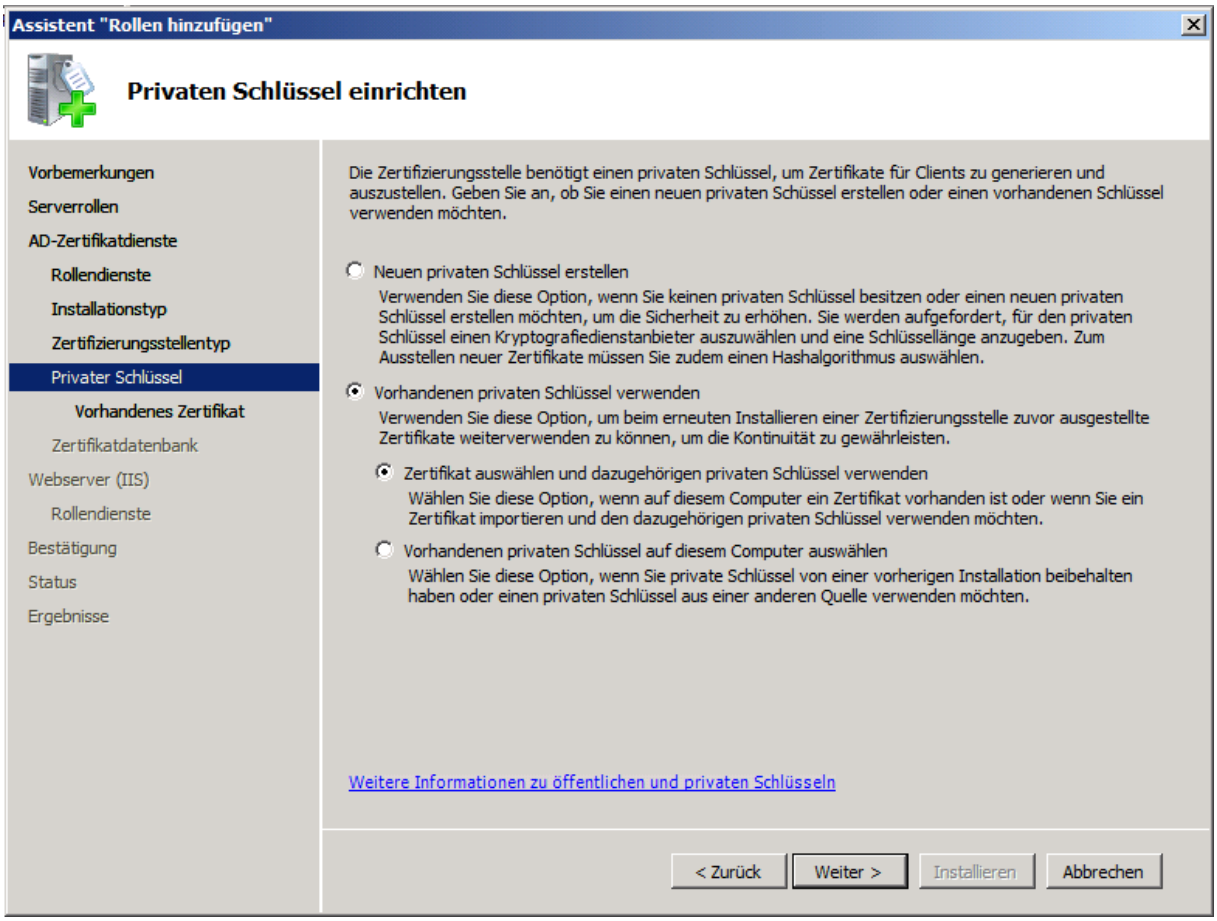
Installation zusaetzlicher Rollendienste



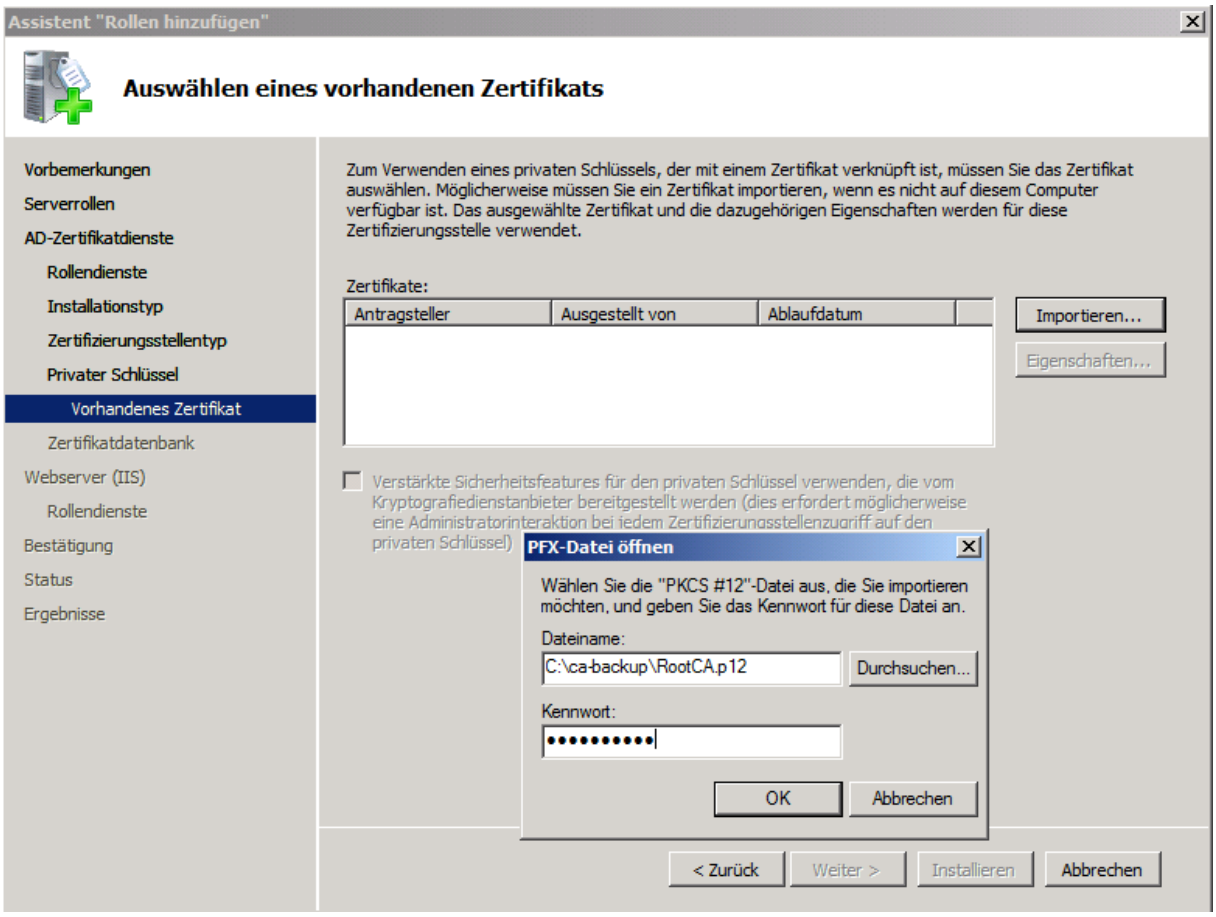
Unternehmens CA auswaehlen

Stammzertifizierungsstelle

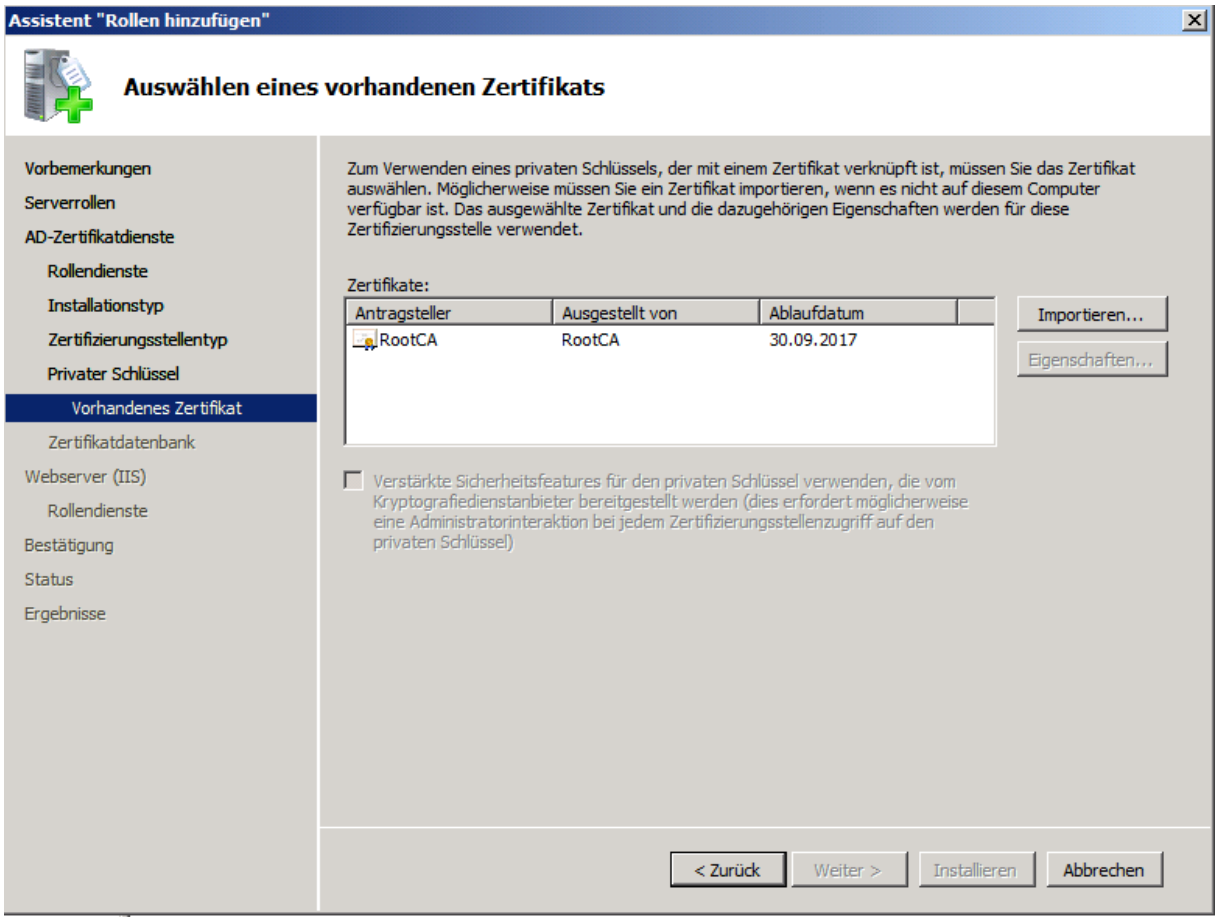
Vorhandenen Schluessel der alten Zertifizierungsstelle auswaehlen



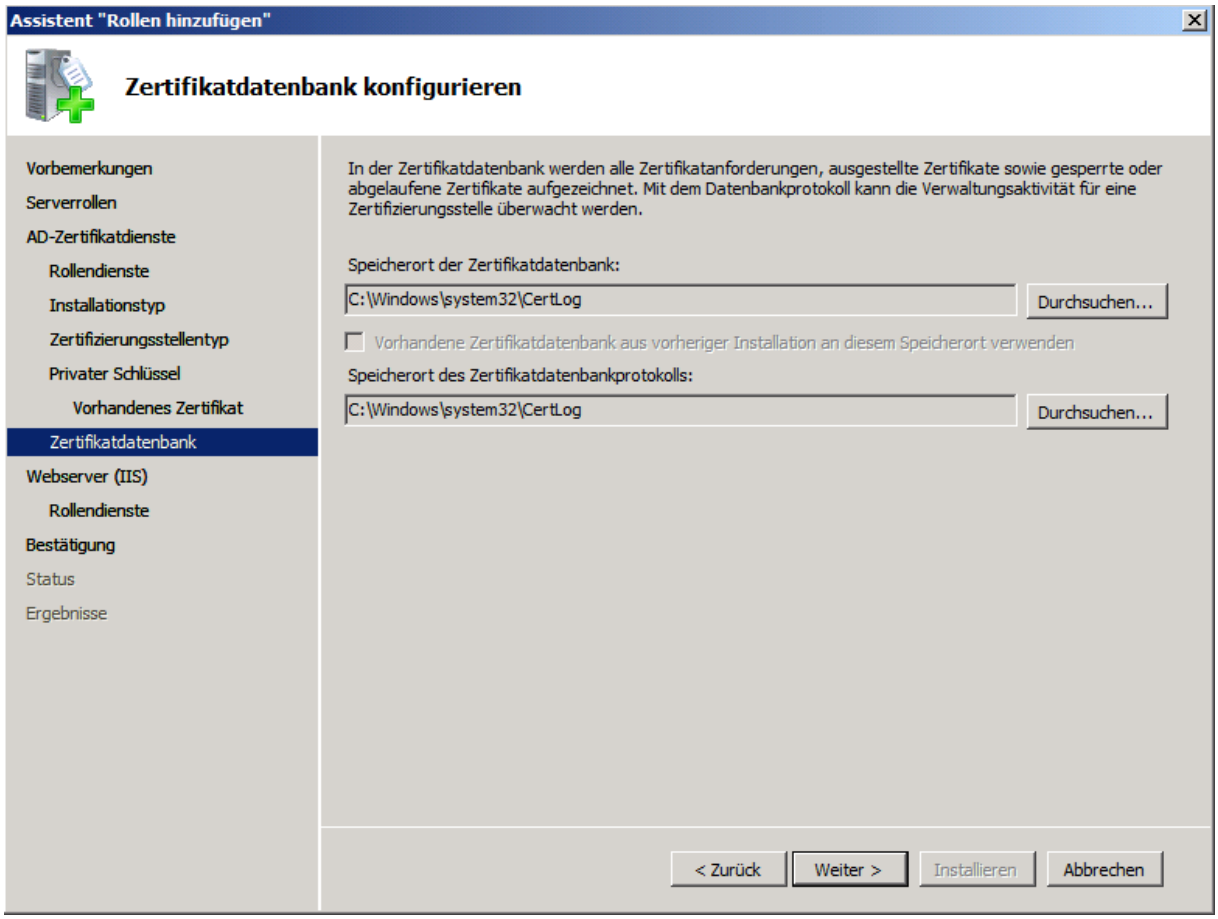
Angabe des Pfades und des Kennworts


Assistent "Rollen hinzufügen"
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
Importieren...
Eigenschaften...
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
Wählen Sie die "PKCS #12"-Datei aus, die Sie importieren möchten, und geben Sie das Kennwort für diese Datei an.
Dateiname:
C:\ca-backup\RootCA.p12
Durchsuchen...
Kennwort:
OK
Abbrechen
< Zurück
Weiter >
Installieren
Abbrechen

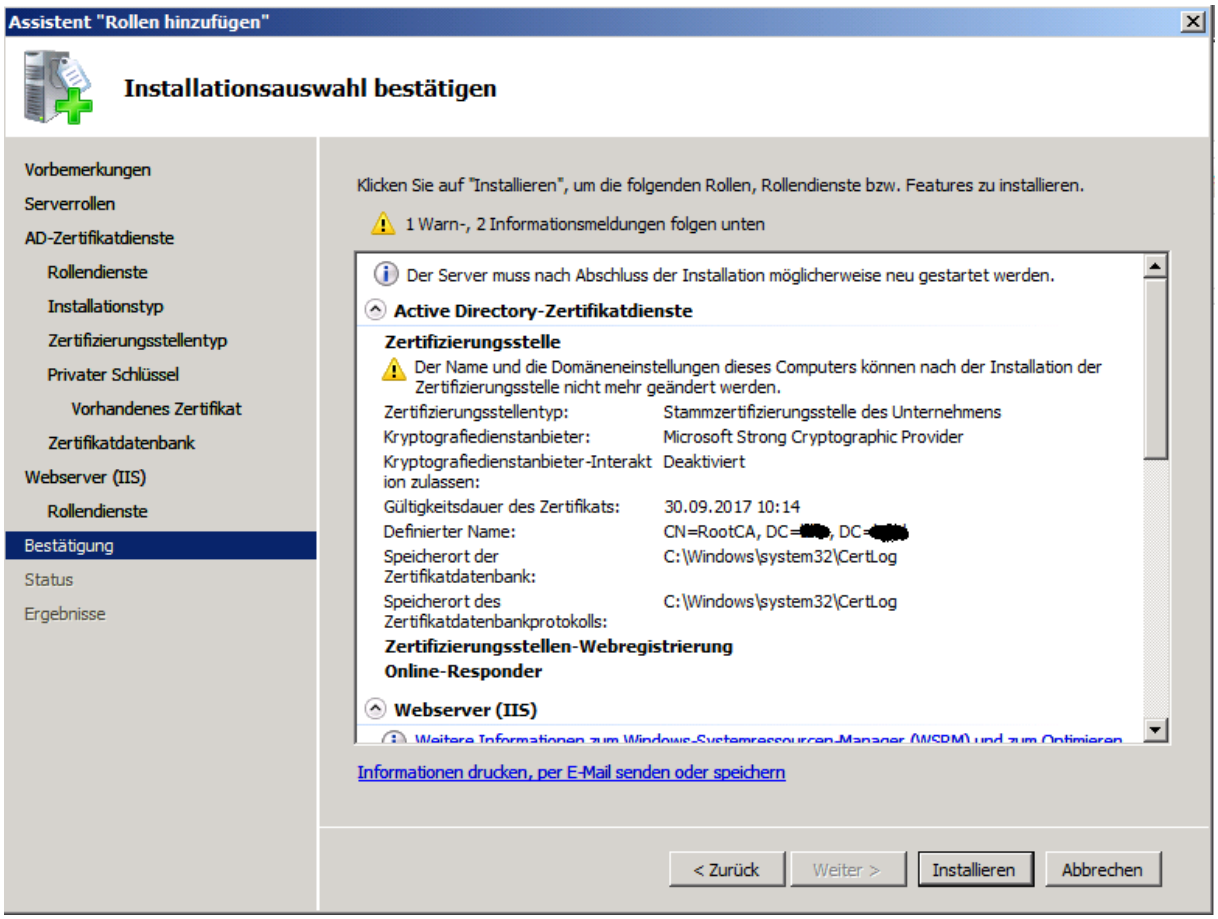
Da isser



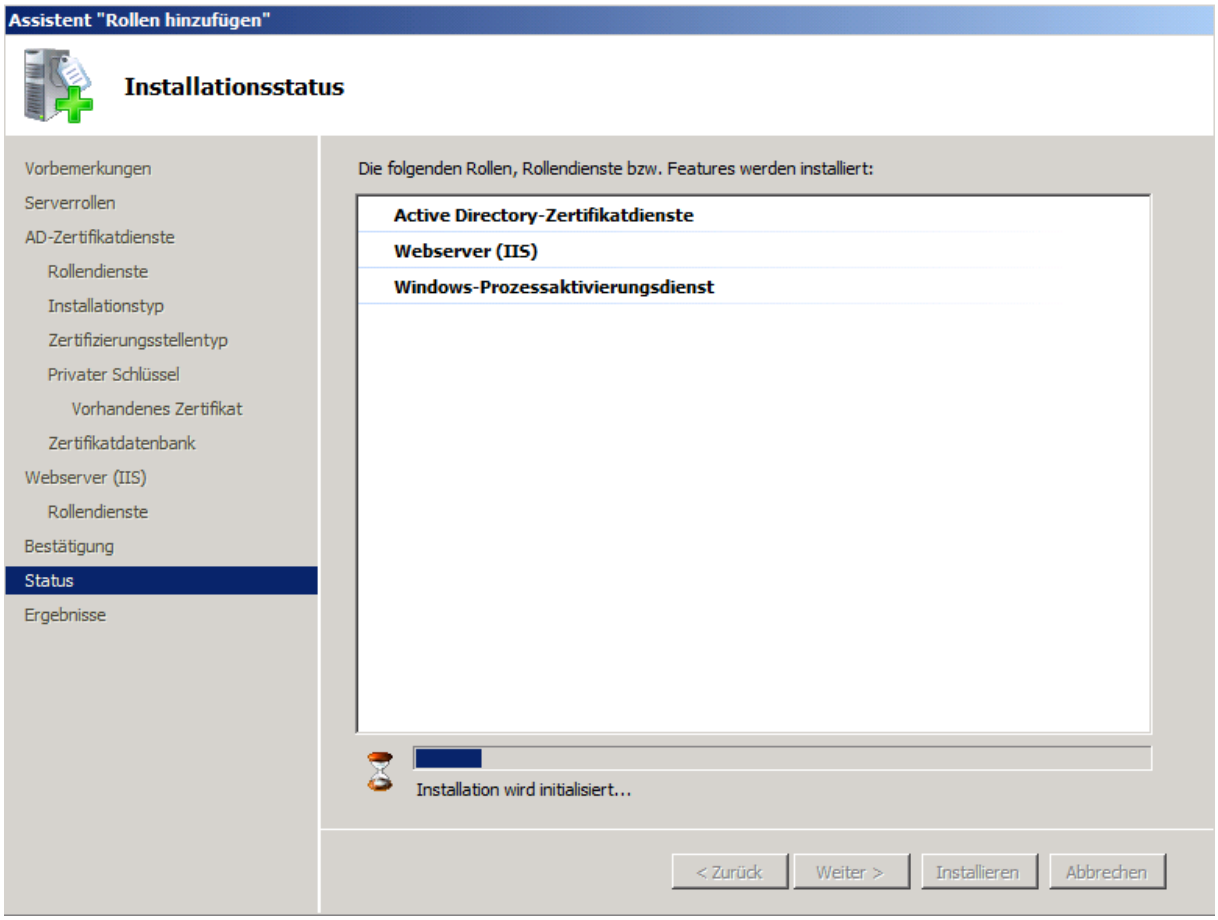
Angabe des Pfades zur CA Datenbank



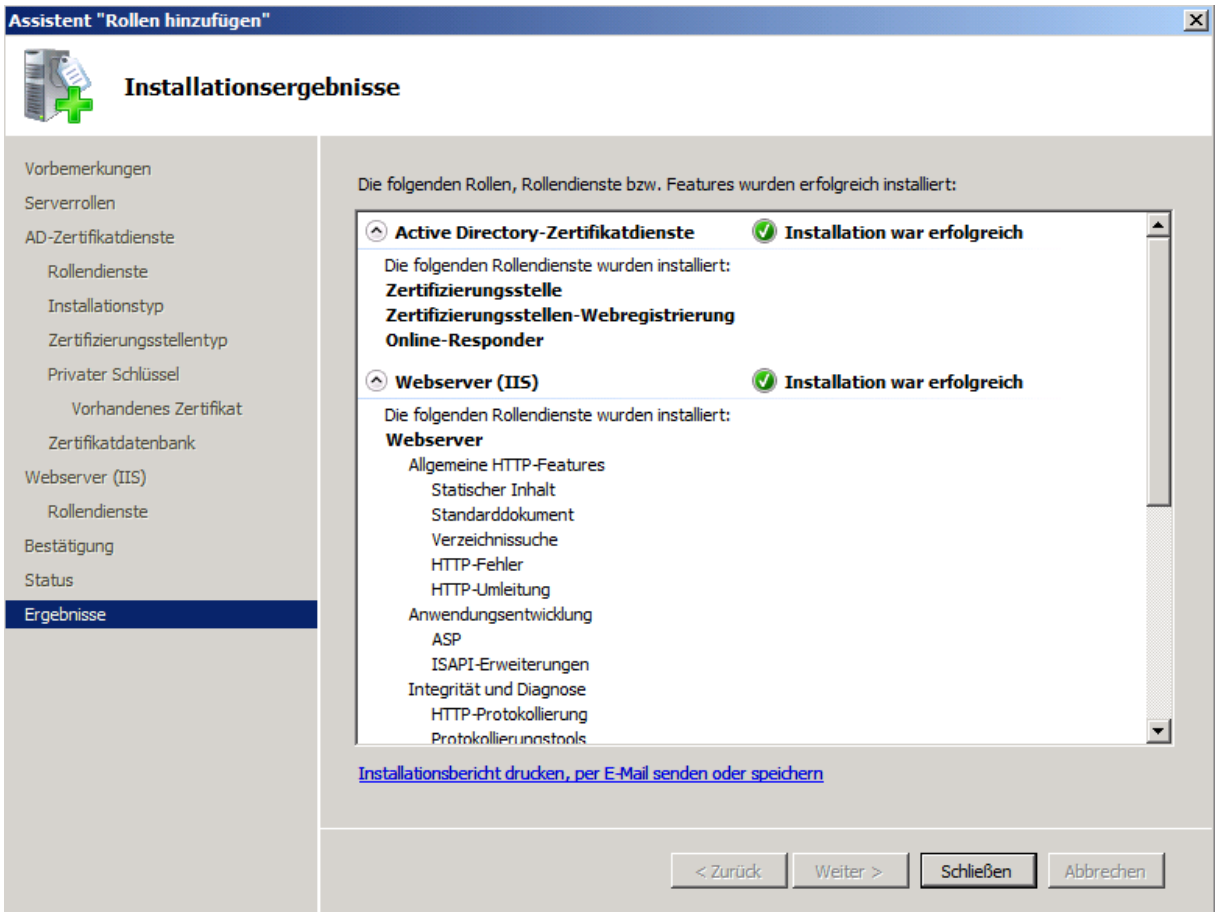
Auswahl zusaetzlicher Rollendienste



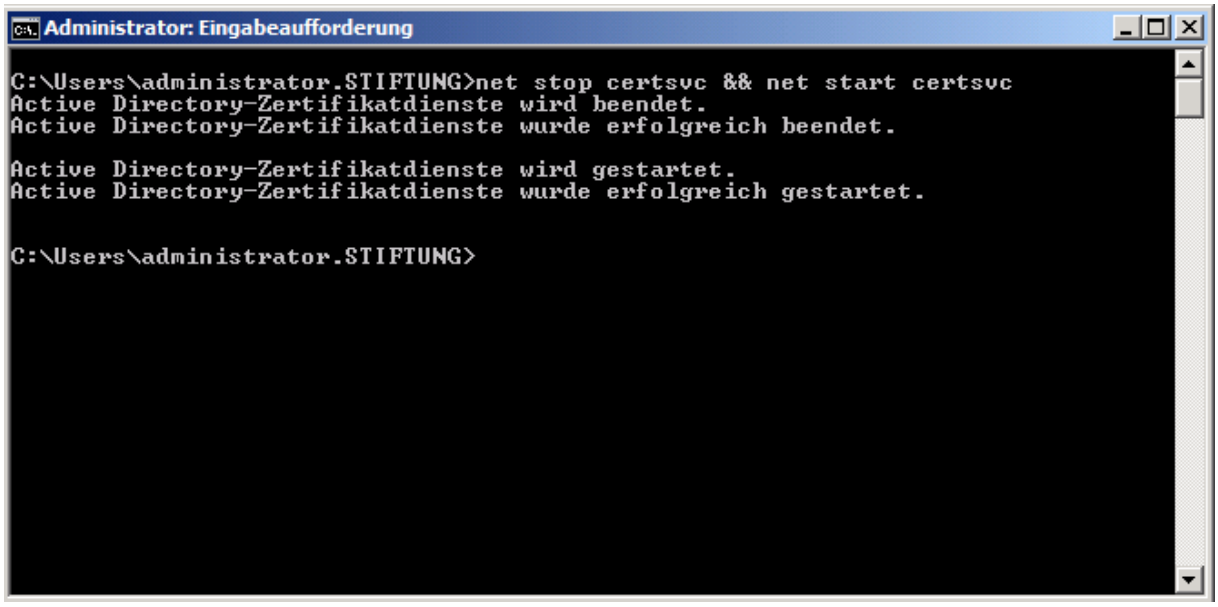
Installation wird durchgefuehrt



Installation wird fertig gestellt



Zertifikatdienste stoppen und starten



Import der exportierten Registry Informationen auf der neuen CA.

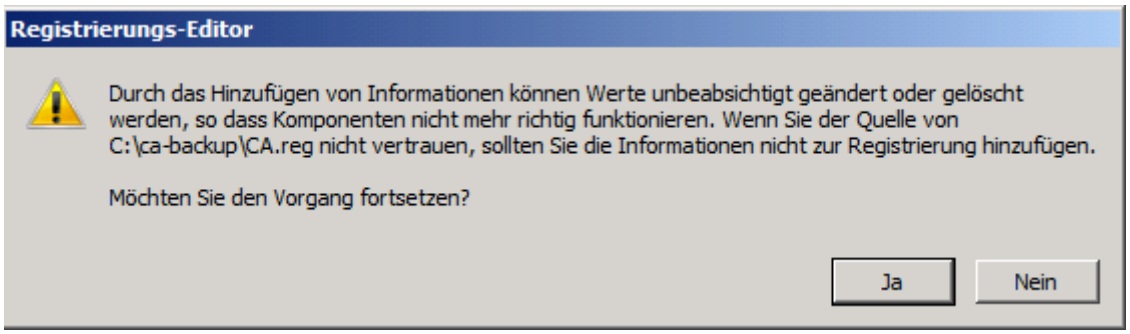
Vor dem importieren muss der Inhalt der Registrierungs-Datei geprueft werden und bei zum Bsp. anderen Servernamen und Datenbankpfaden eine Anpassung vorgenommen werden.

CA - Editor

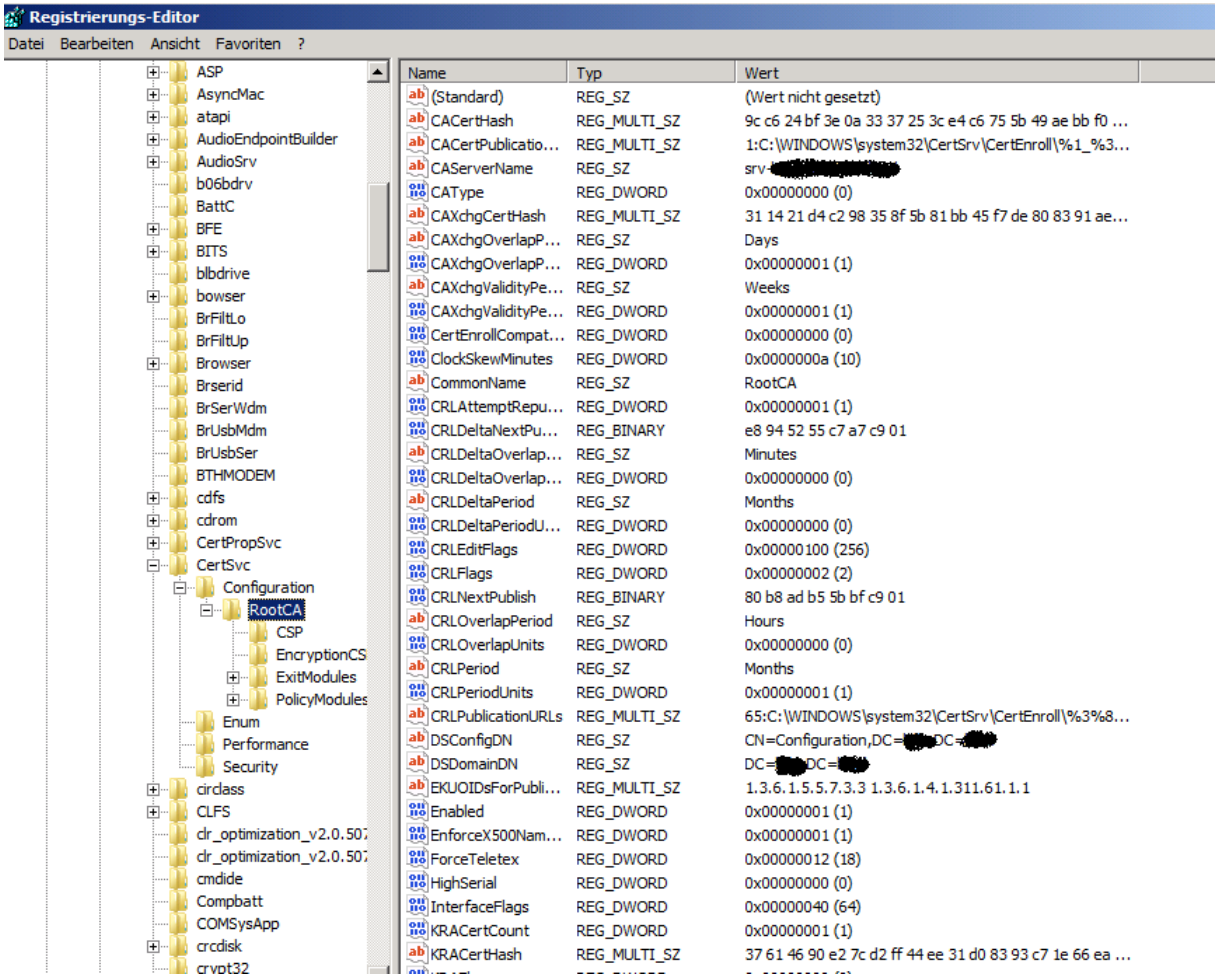
Datei Bearbeiten Format Ansicht ?

```
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. W

[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"
"DBSessionCount"=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=[redacted],DC=[redacted]"
"DSDomainDN"="DC=[redacted],DC=[redacted]"
"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
"CRLFlags"=dword:00000002
"InterfaceFlags"=dword:00000040
"EnforceX500NameLengths"=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

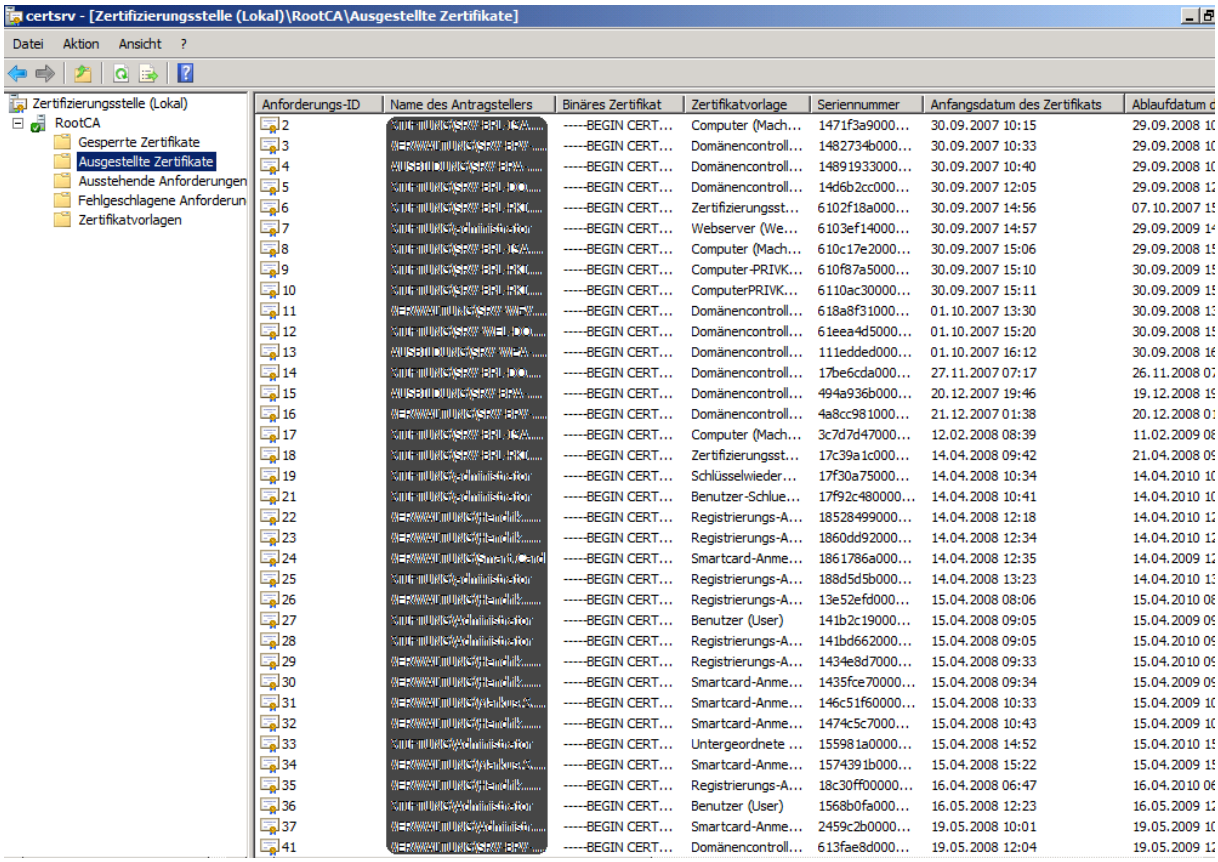


Die importierten Einstellungen in der Registry

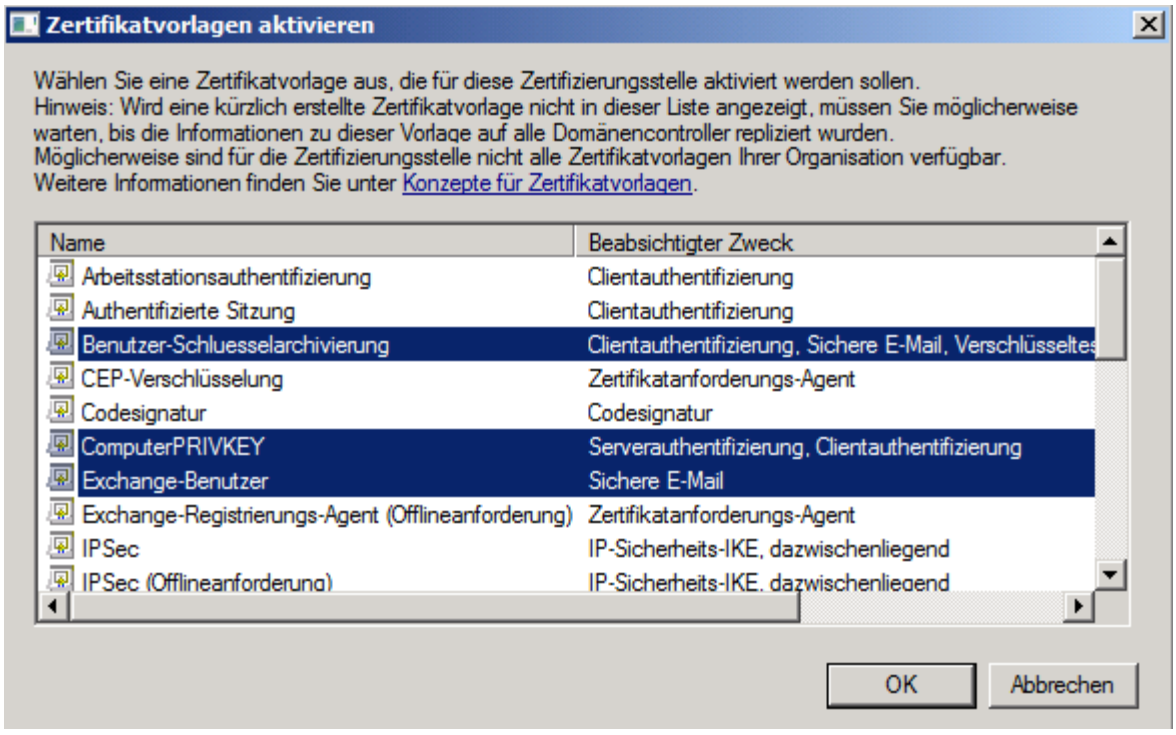


Die Zertifikatdienste neu starten

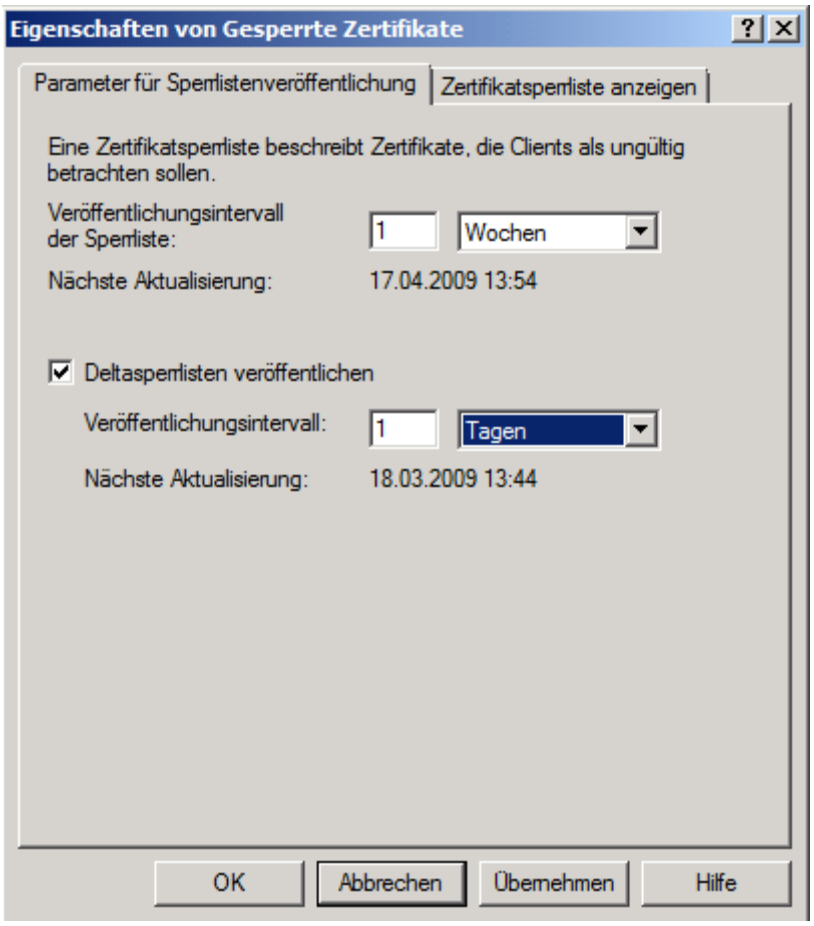
Die CA wurde komplett wiederhergestellt



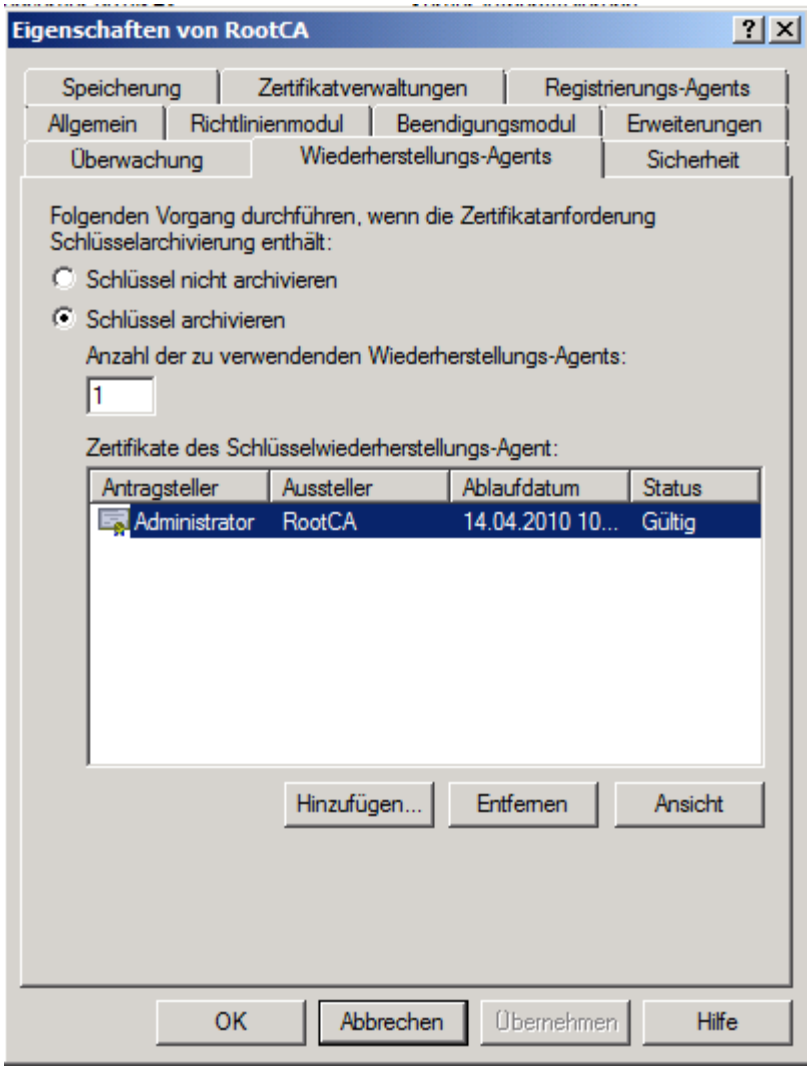
Die selbst erstellten V2 Templates muessen neu ausgestellt werden



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

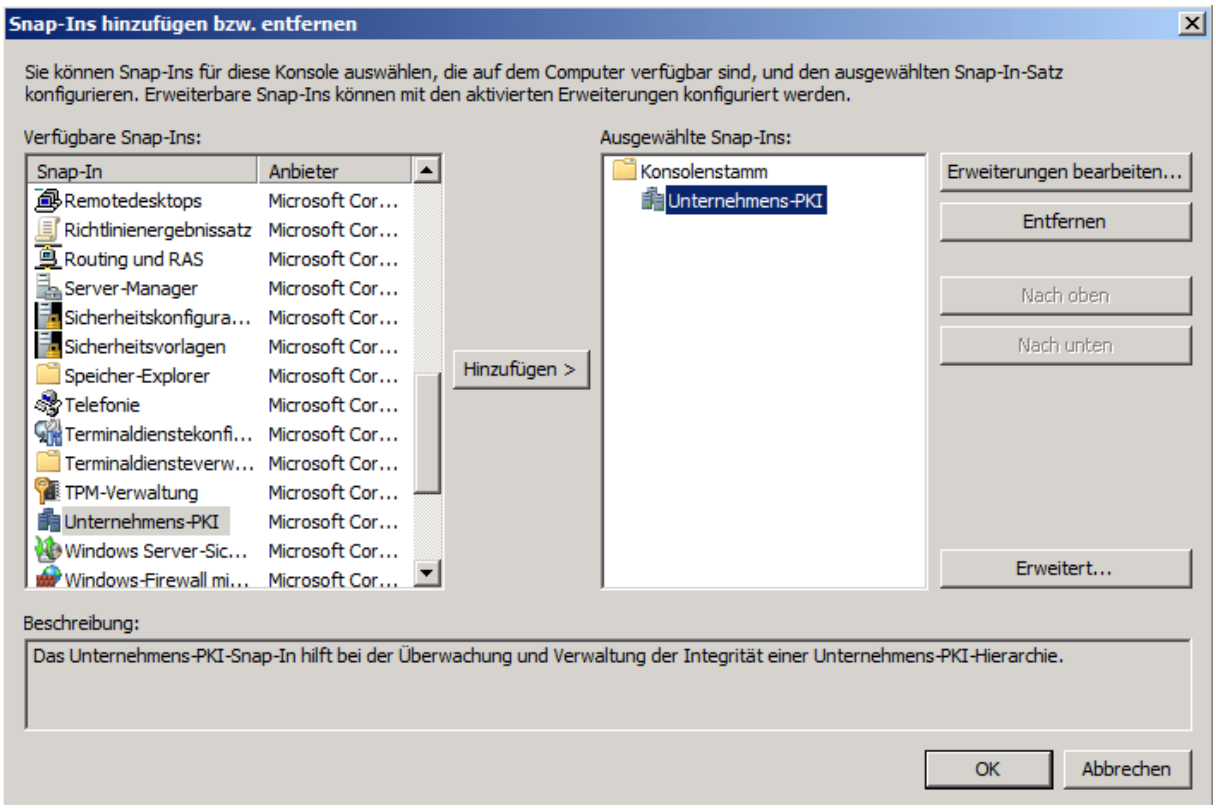


Das KRA Zertifikat wurde auch wiederhergestellt.

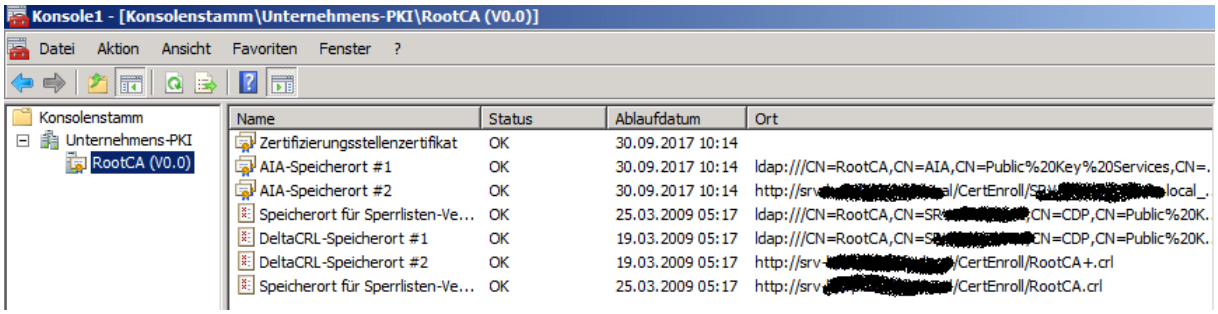


Fertig

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


Snap-Ins hinzufügen bzw. entfernen
Sie können Snap-Ins für diese Konsole auswählen, die auf dem Computer verfügbar sind, und den ausgewählten Snap-In-Satz konfigurieren. Erweiterbare Snap-Ins können mit den aktivierten Erweiterungen konfiguriert werden.
Verfügbare Snap-Ins:
Snap-In
Anbieter
Remotedesktops Microsoft Cor...
Richtlinienergebnissatz Microsoft Cor...
Routing und RAS Microsoft Cor...
Server-Manager Microsoft Cor...
Sicherheitskonfigura... Microsoft Cor...
Sicherheitsvorlagen Microsoft Cor...
Speicher-Explorer Microsoft Cor...
Telefonie Microsoft Cor...
Terminaldienstekonfi... Microsoft Cor...
Terminaldiensteverw... Microsoft Cor...
TPM-Verwaltung Microsoft Cor...
Unternehmens-PKI Microsoft Cor...
Windows Server-Sic... Microsoft Cor...
Windows-Firewall mi... Microsoft Cor...
Hinzufügen >
Ausgewählte Snap-Ins:
Konsolenstamm
Unternehmens-PKI
Erweiterungen bearbeiten...
Entfernen
Nach oben
Nach unten
Erweitert...
Beschreibung:
Das Unternehmens-PKI-Snap-In hilft bei der Überwachung und Verwaltung der Integrität einer Unternehmens-PKI-Hierarchie.
OK
Abbrechen

Alles roger


Konsole1 - [Konsolenstamm\Unternehmens-PKI\RootCA (V0.0)]
Datei Aktion Ansicht Favoriten Fenster ?
Konsolenstamm
Unternehmens-PKI
RootCA (V0.0)
Name Status Ablaufdatum Ort
Zertifizierungsstellenzertifikat OK 30.09.2017 10:14
AIA-Speicherort #1 OK 30.09.2017 10:14 ldap:///CN=RootCA,CN=AIA,CN=Public%20Key%20Services,CN=.
AIA-Speicherort #2 OK 30.09.2017 10:14 http://srv[redacted]/CertEnroll/[redacted]local_.
Speicherort für Sperrlisten-Ve... OK 25.03.2009 05:17 ldap:///CN=RootCA,CN=SR[redacted],CN=CDP,CN=Public%20K.
DeltaCRL-Speicherort #1 OK 19.03.2009 05:17 ldap:///CN=RootCA,CN=S[redacted],CN=CDP,CN=Public%20K.
DeltaCRL-Speicherort #2 OK 19.03.2009 05:17 http://srv-[redacted]/CertEnroll/RootCA+.crl
Speicherort für Sperrlisten-Ve... OK 25.03.2009 05:17 http://srv[redacted]/CertEnroll/RootCA.crl