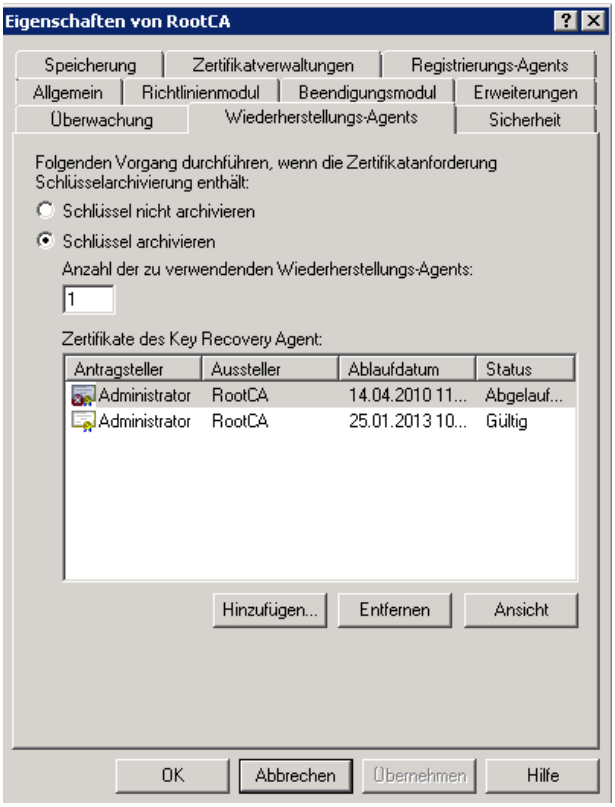
Smartcard Enrollment mit Windows Server 2008 R2 PKI und Windows 7

Ziel ist die Erstellung einer neuen Zertifikatvorlage fuer das Smartcard Enrollment mit einer Gueltigkeit von 2 Jahren. Ein Enrollment Agent soll konfiguriert werden, damit ein EDV-Mitarbeiter stellvertretend fuer alle Mitarbeiter Smartcard Zertifikate ausstellen kann.

CA fuer Schluesselarchivierung aktivieren

Sollen private Schluessel archiviert werden, ist erst die Schluesselarchivierung an der CA zu aktivieren. Im ersten Schritt muss dazu ein Key Recovery Agent Zertifikat angefordert werden und anschliessend die Schluesselarchivierung aktiviert werden.

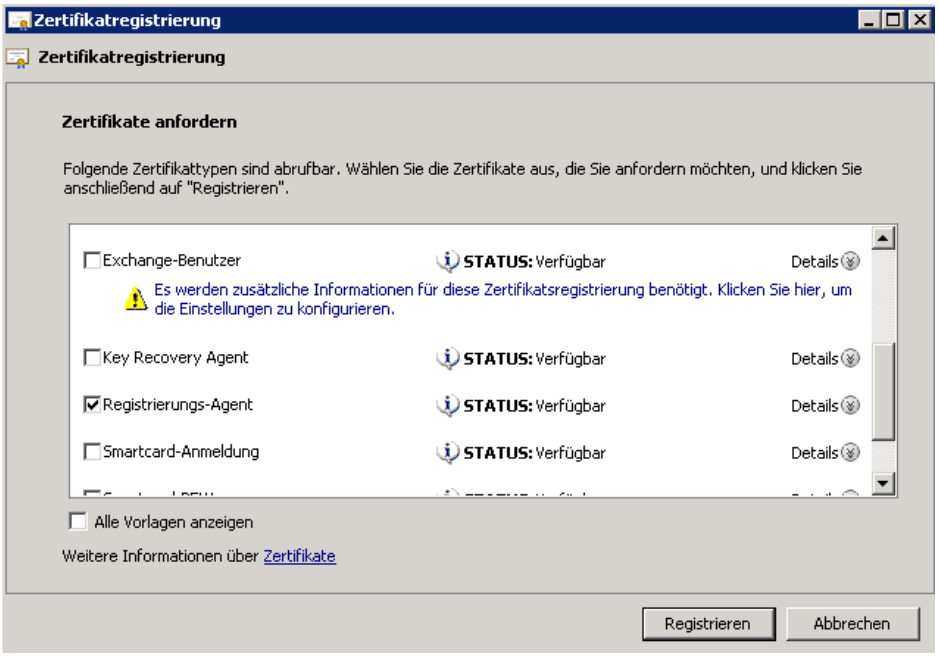


CSP des Anbieters auf dem CA Server installieren

In meinem Kundenfall werden Aladdin etoken verwendet. Die Zertifikatvorlage in der CA muss fuer den entsprechenden CSP eingerichtet werden, so dass die Installation des CSP (Smartcard Client) auf der CA erforderlich ist, damit man in der Zertifikatvorlage den CSP auswaehlen kann.

Registrierungs Agenten Zertifikat installieren

Damit ein Benutzer stellvertretend fuer andere Benutzer Smartcard Zertifikat anfordern kann, ist die Ausstellung eines Registrirungs-Agenten Zertifikats notwendig. Das Zertifikat wird fuer den Benutzer an der Smartcard Enrollment Station angefordert.

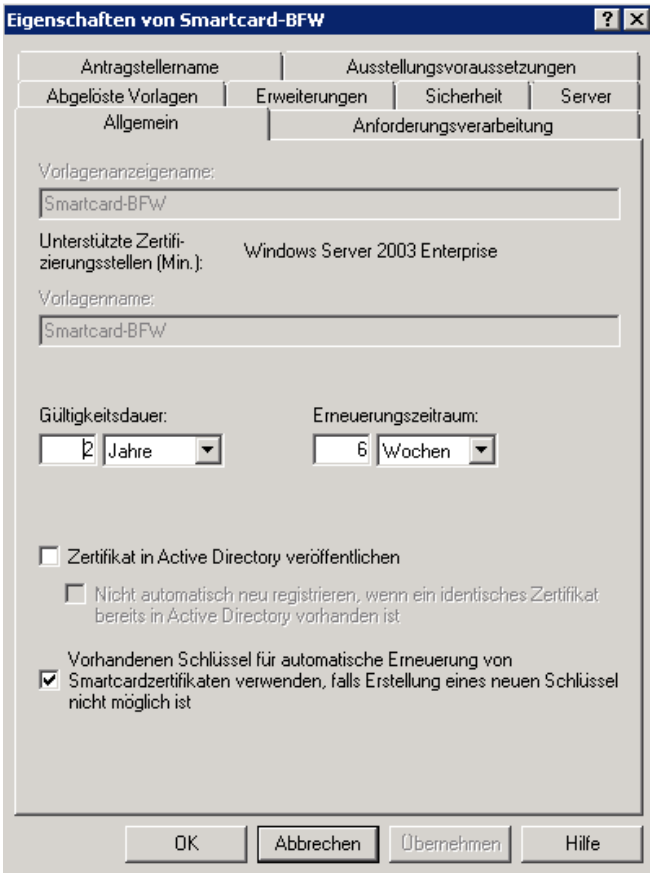


Zertifikatvorlage „Smartcard Anmeldung“ doppeln und anpassen

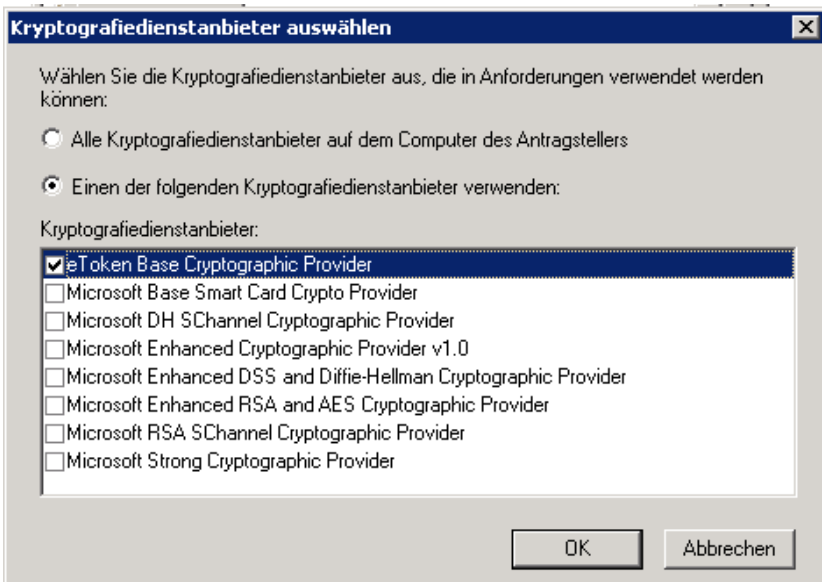
Um die Standard Zertifikatvorlage anpassen zu koennen, muss diese gedoppelt (kopiert) werden.

V3 Template ist Windows Server 2003 Enterprise

Gueltigkeit 2 Jahre



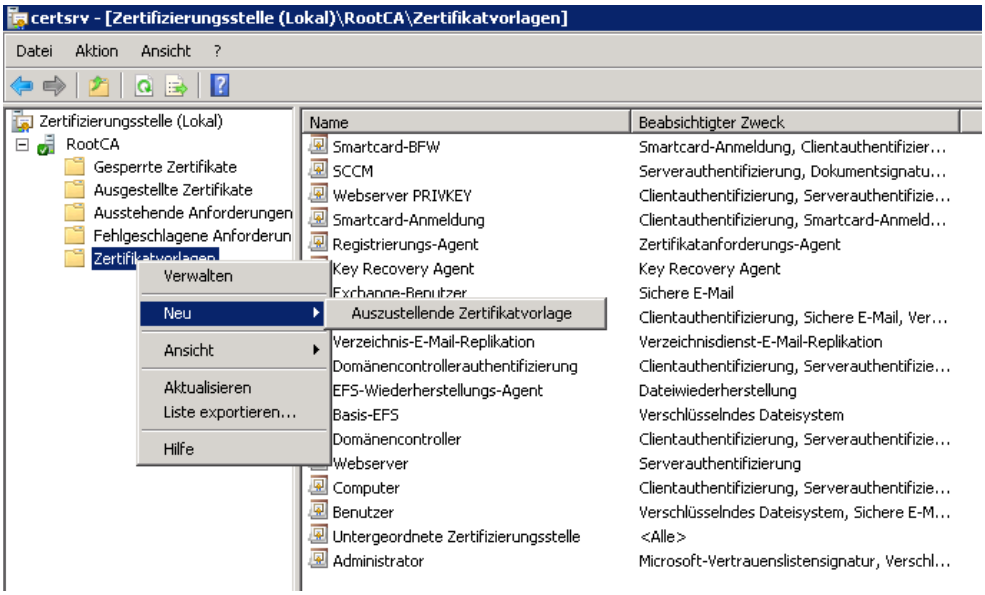
CSP des Smartcard Anbieters in der Anforderungsverarbeitung angeben



ACHTUNG: Es ist noch ein weiterer Schritt erforderlich, doch zu diesem Fehler spaeter etwas mehr ☺

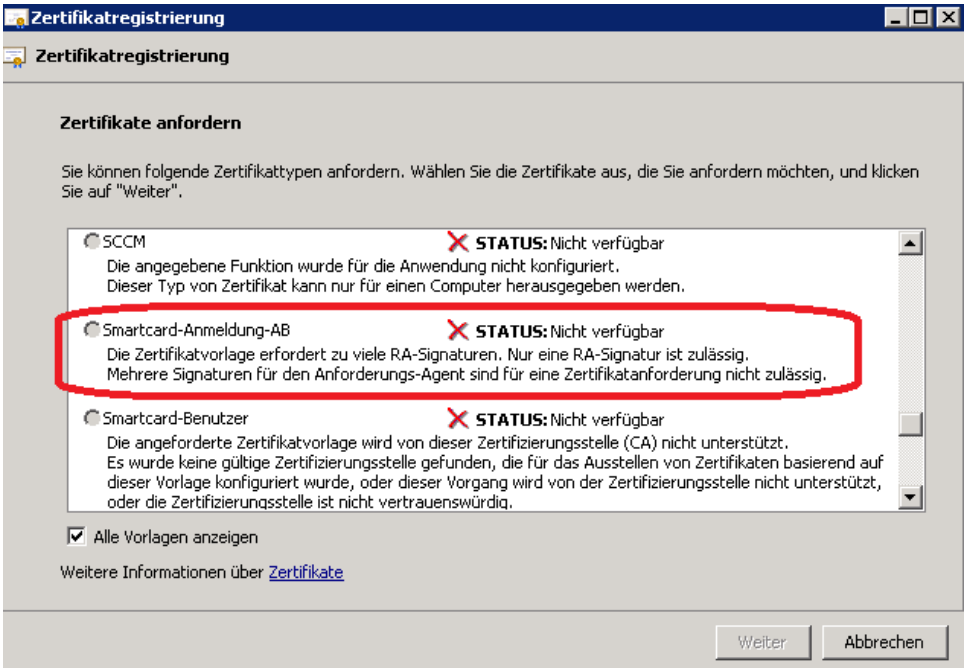
Neue Zertifikatvorlage fuer CA Verwendung aktivieren

Die neu erstellte Zertifikatvorlage muss an der CA ausgestellt werden, bevor Clients diese verwenden koennen.



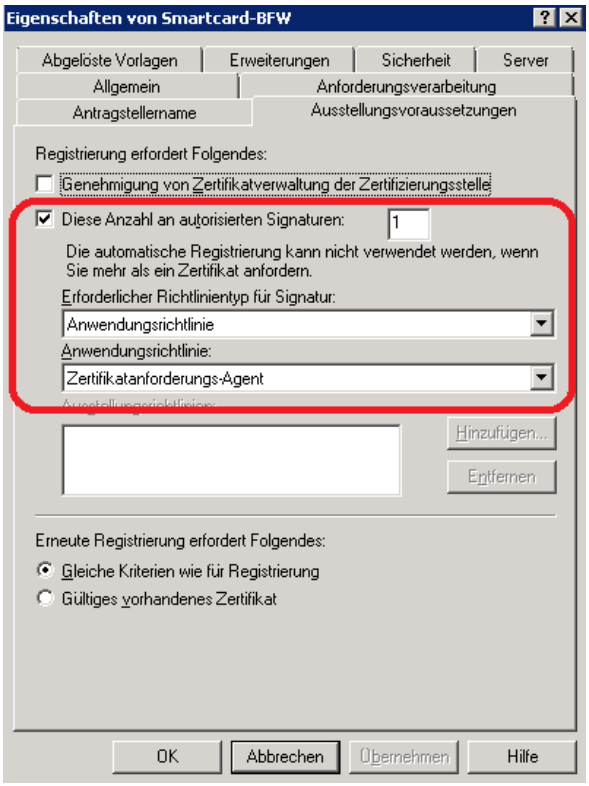
Fehlermeldung beim Anfordern des Smartcard Zertifikats

Am Client kann jetzt, nachdem das Registrierungs Agenten Zertifikat angefordert wurde, das Smartcard Zertifikat angefordert werden, es erscheint jedoch folgende Fehlermeldung:



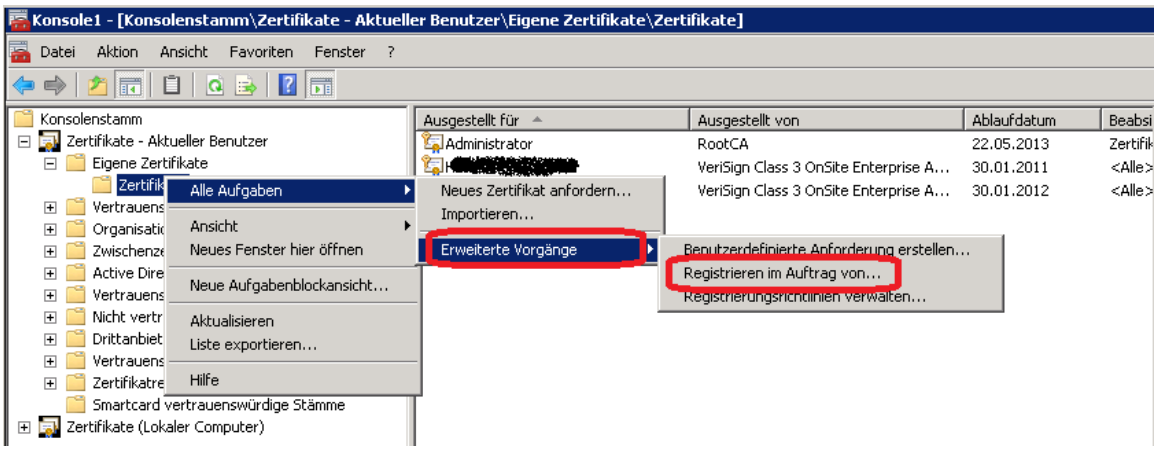
Loesung

In der CA Verwaltung muss in den Eigenschaften der neuen Zertifikatvorlage auf der Registerkarte Ausstellervoraussetzungen folgende Einstellung vorgenommen werden.

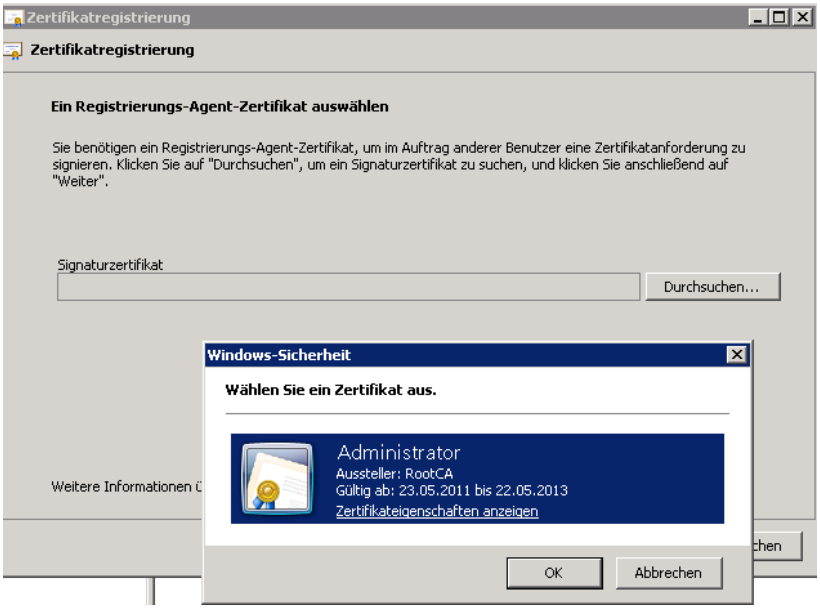


Smartcard Zertifikat Anforderung auf Enrollment Station

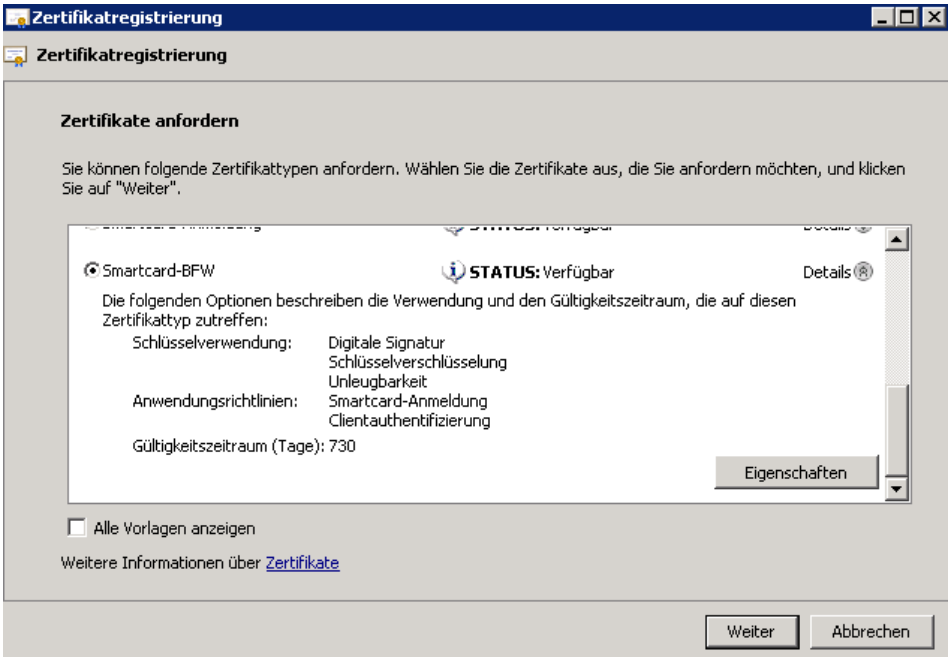
Seit Windows Server 2008 geht das Smartcardenrollment fuer andere Benutzer nicht mehr per /CERTSRV Webseite. Es muss jetzt die MMC auf dem PC verwendet werden (Seit Vista/7). Registrieren im Auftrag von ...

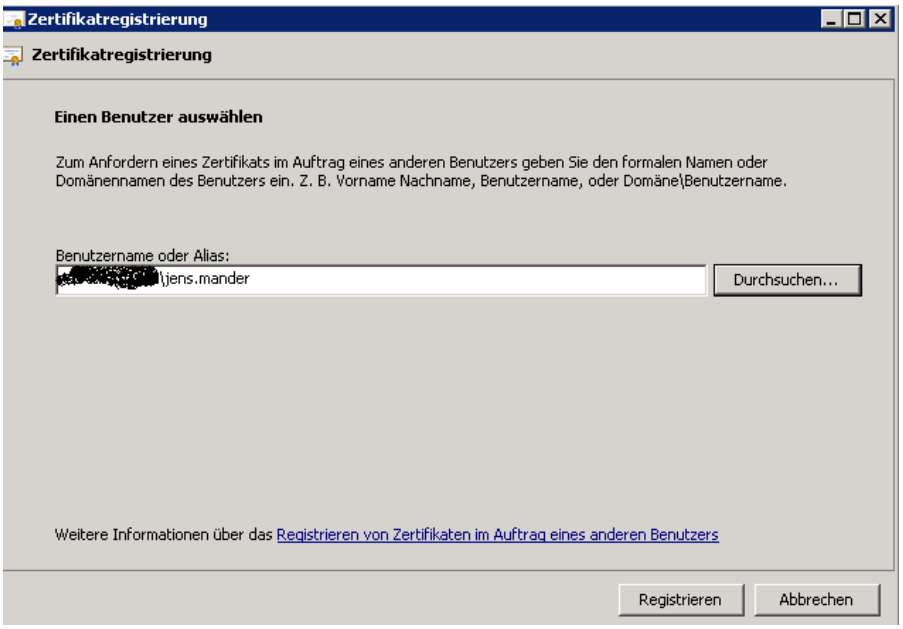


Registrierungs Agenten Zertifikat auswaehlen

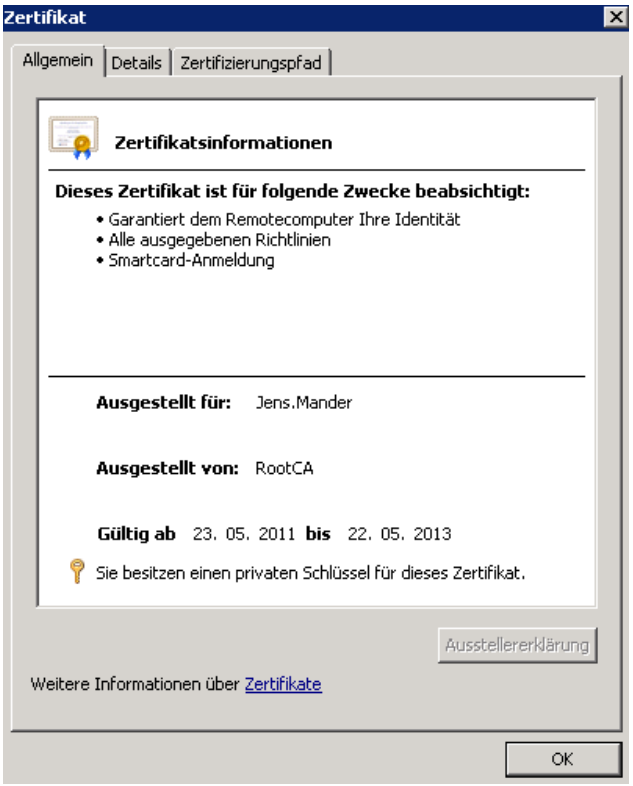


Zertifikatvorlage auswaehlen



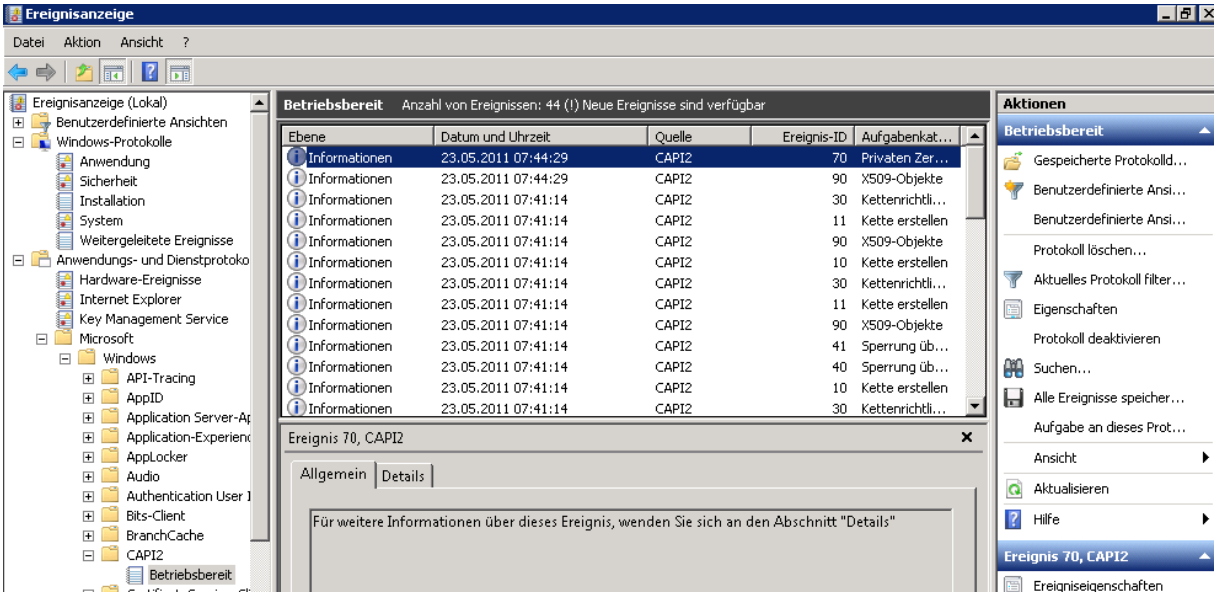


Zertifikat ist fuer zwei Jahre ausgestellt

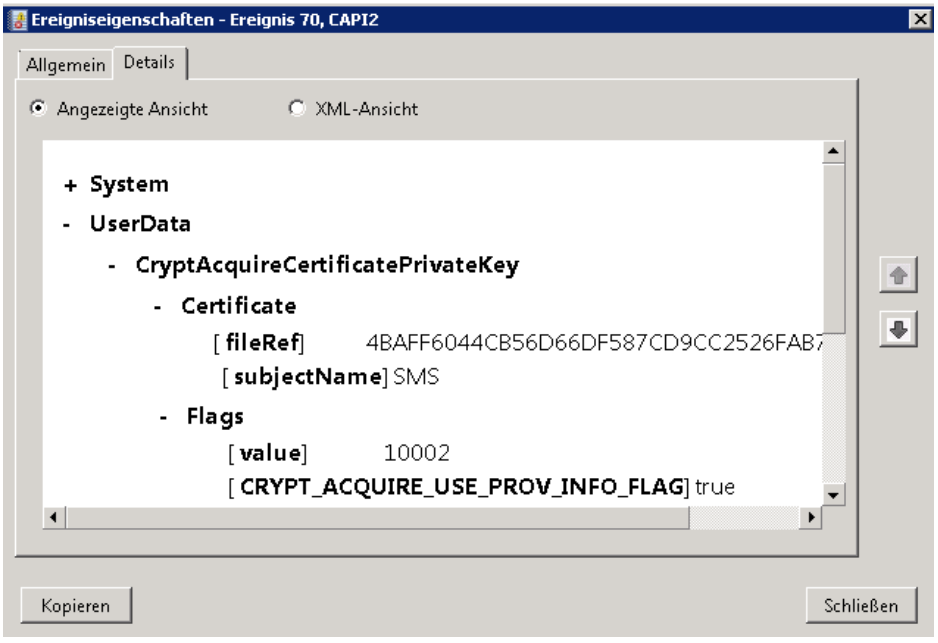


CAPI Logging

Bei Problemen mit dem Smartcard Enrollment oder allgemeinen Problemen mit der Crypto API (CAPI), kann man seit Windows Vista / 2008 das CAPI Logging in der Ereignisanzeige der CA Server oder des Clients aktivieren, um mehr Informationen zu erhalten.



XML Details



CSP auf Enrollment Station installieren

Die entsprechende Smartcard Client Software und der CSP muessen auf allen betroffenen PC installiert werden. Am besten wird hierzu eine entsprechende Softwareverteilungsloesung wie DSM oder SCCM verwendet.

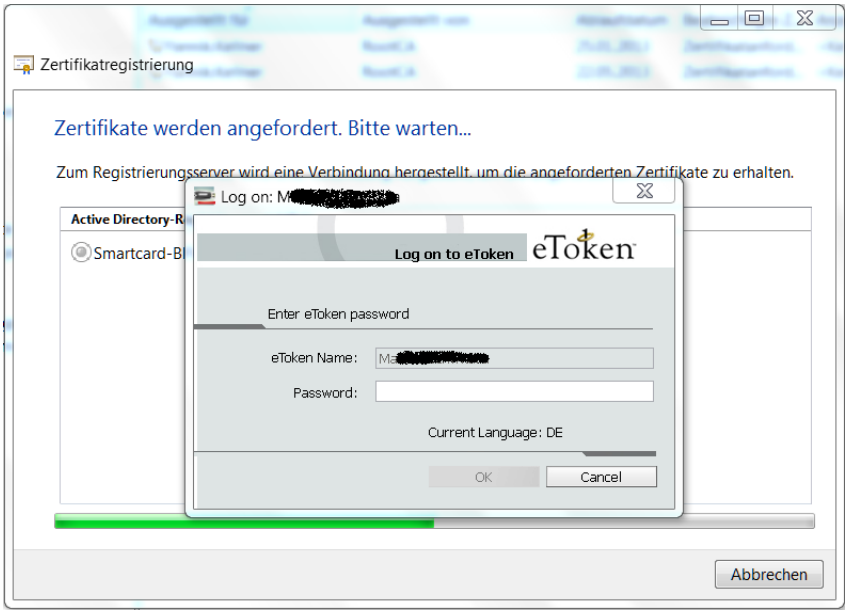
Administrative Taetigkeiten auf der Smartcard Enrollment Workstation

Smartcard initialisieren
Admin Kennwort setzen
User PIN setzen
Smartcard mit Smartcard Zertifikat ausstatten

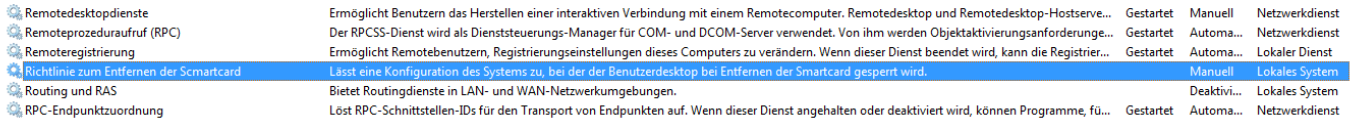
Smartcard Enrollment Workstation

Von der Smartcard Enrollment Workstation koennen jetzt durch den Enrollment Agent stellvertretend fuer die Benutzer Zertifikate angefordert werden.

Zertifikat fuer andere Benutzer anfordern



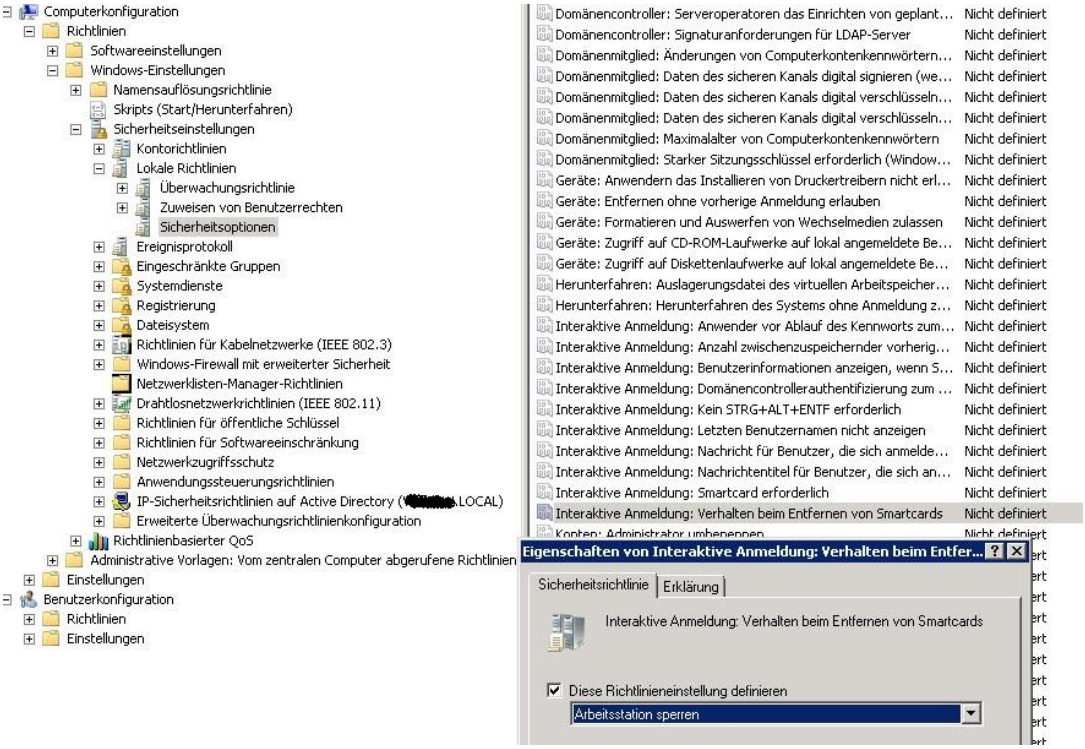
Auf dem Windows 7 Client muss folgender Dienst gestartet sein



Anmeldung des Users

Gruppenrichtlinien

Mit Hilfe von Gruppenrichtlinien kann das Smartcard Verhalten eingestellt werden. Am besten sollte per Gruppenrichtlinie auch der Windows 7 Dienst „Richtlinie zum Entfernen von Smartcards“ automatisch gestartet werden



Die Einstellungen fuer den PKI Client koennen auch per Gruppenrichtlinie konfiguriert werden

eToken PKI Client Settings/eToken PKI Client Properties Settings hide

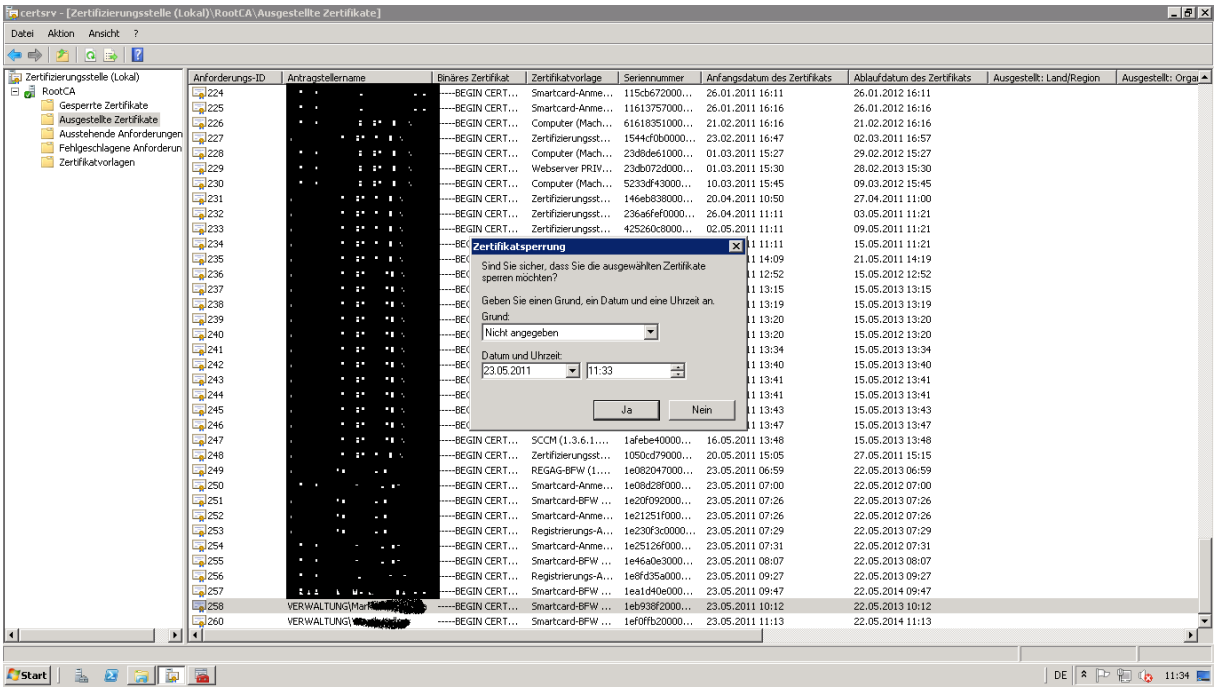
Richtlinie	Einstellung	Kommentar
Advanced View	Aktiviert	
Advanced View	0	

eToken PKI Client Settings/UI Access Control List hide

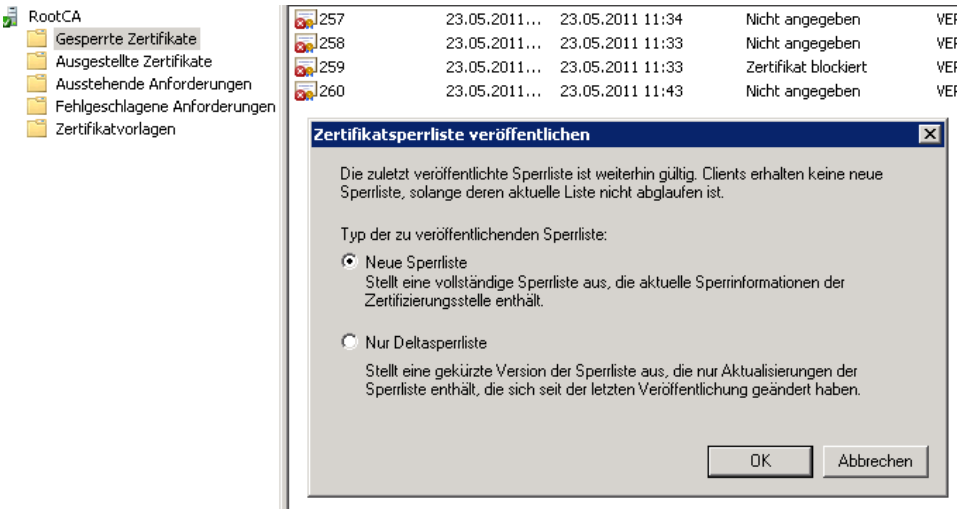
Richtlinie	Einstellung	Kommentar
Access Control	Aktiviert	
ChangePassword	1	
RenameToken	0	
UnlockEtoken	0	
ClearEToken	0	
ViewTokenInfo	1	
DisconnectVirtual	1	
OpenAdvancedView	0	
AddeTokenVirtual	0	
ManageReaders	1	
InitializeEToken	0	

Zertifikat revoken

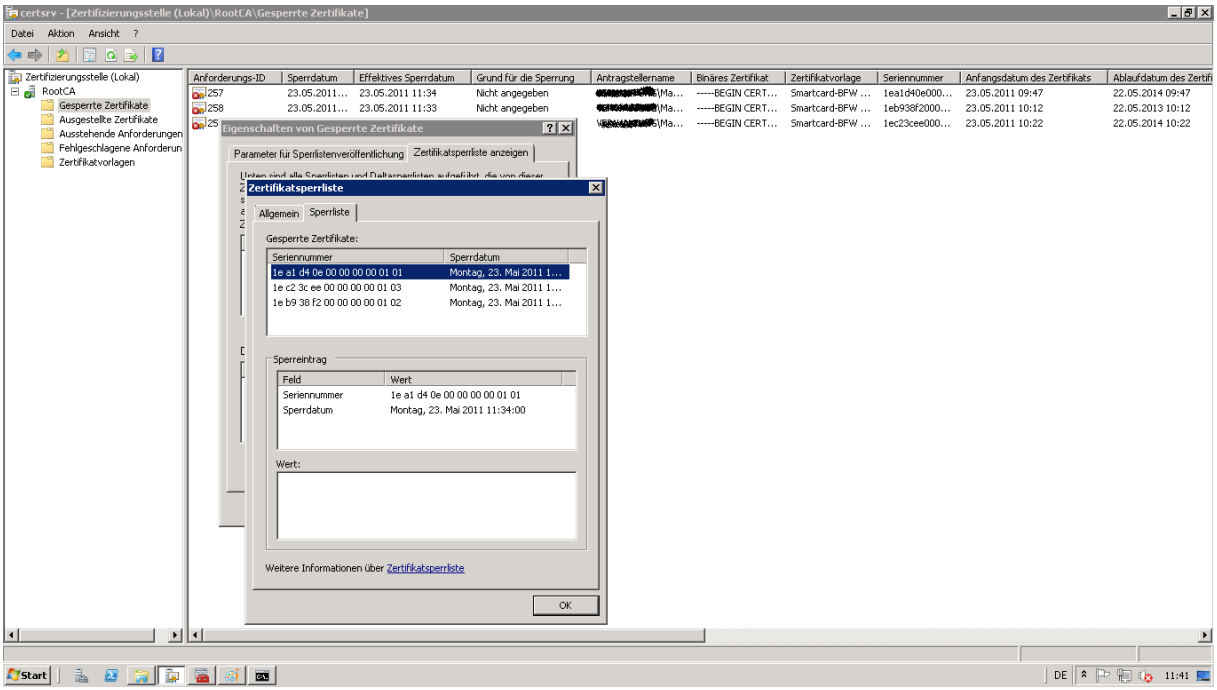
Wenn der Benutzer das Smartcard Zertifikat nicht mehr verwenden darf (z. B. Bei Verlust der Smartcard), muss das ausgestellte Zertifikat an der CA revokiert werden



Danach kann die Base- oder Delta CRL manuell veroeffentlicht werden



Anzeige der Sperrliste



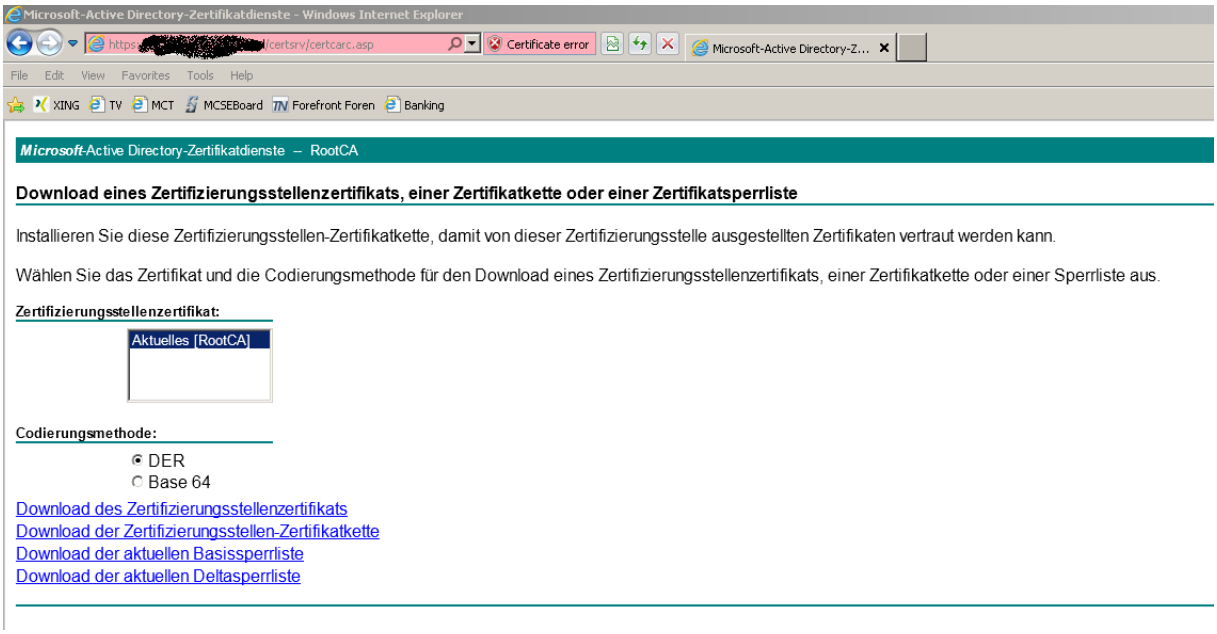
Lokalen CRL Cache anzeigen

C:\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\
C:\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\

CRL Cache loeschen
certutil -urlcache crl delete

Aktuelle Base oder Delta CRL downloaden

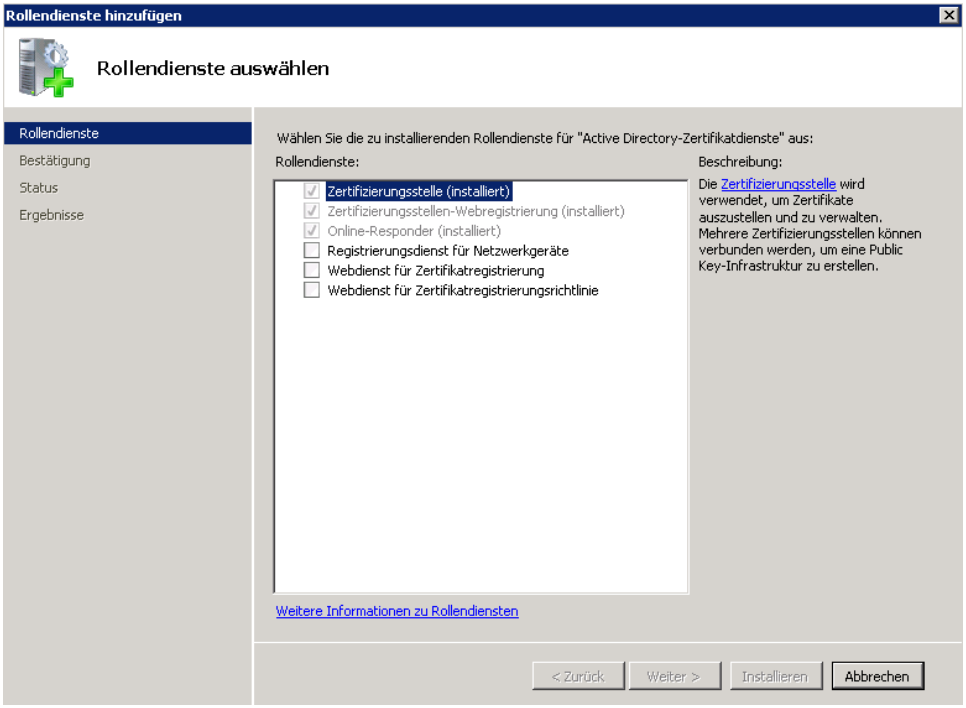
Um das Update des Base- oder Delta CRL Downloads zu beschleunigen, kann die Base oder Delta CRL manuell auf dem Client heruntergeladen werden.



Wenn die CRL aktuell ist, passiert bei dem Versuch der Anmeldung des Clients mit Smartcard folgendes:

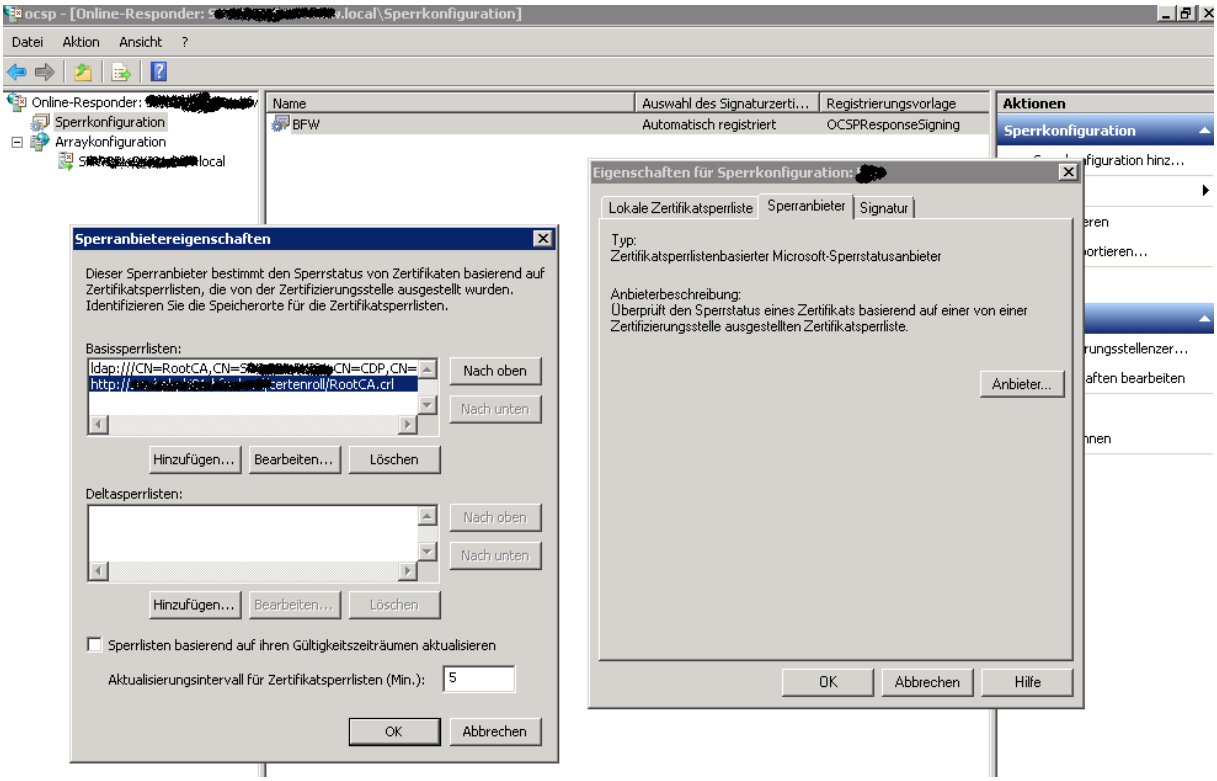
Optional: OCSP Responder Einrichtung

OCSP Responder installieren

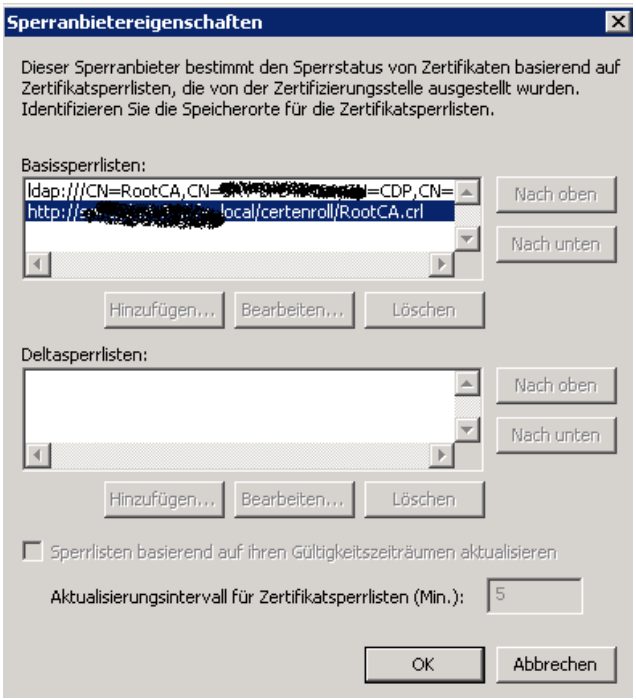


OCSP Signing Zertifikat anfordern

Sperranbieter konfigurieren



Dem Zeitablauf der Sperrlisten folgen oder manuell ueberschreiben



Sperrkonfigurationsstatus OK