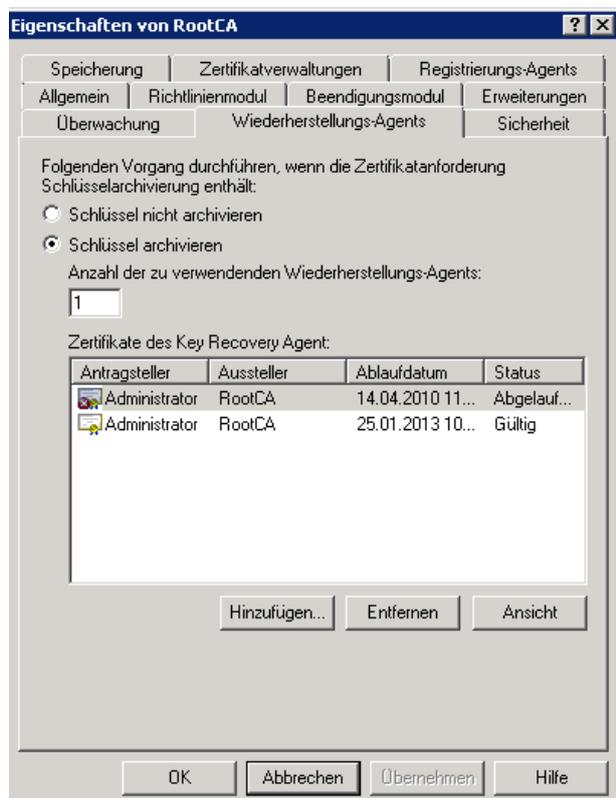


Smartcard Enrollment mit Windows Server 2008 R2 PKI und Windows 7

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.

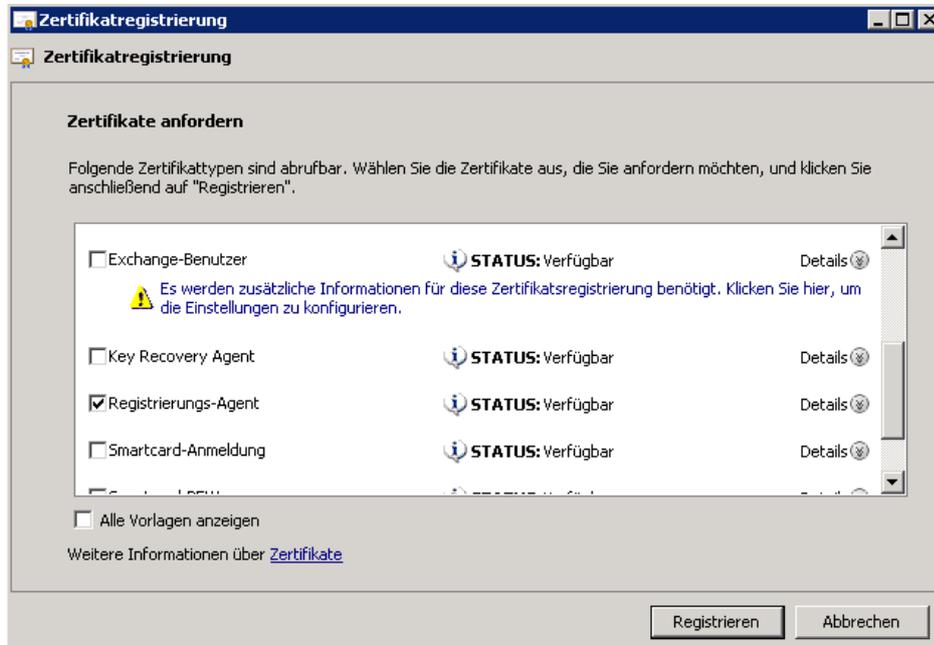


CSP des Anbieters auf dem CA Server installieren

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 Registrierungs-Agenten Zertifikats notwendig. Das Zertifikat wird fuer den Benutzer an der Smartcard Enrollment Station angefordert.



Zertifikatvorlage „Smartcard Anmeldung“ doppelnd und anpassen

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

V3 Template ist Windows Server 2003 Enterprise



Gueltigkeit 2 Jahre

Eigenschaften von Smartcard-BFW

Antragstellername | Ausstellungsvoraussetzungen

Abgelöste Vorlagen | Erweiterungen | Sicherheit | Server

Allgemein | Anforderungsverarbeitung

Vorlagenanzeigename:
Smartcard-BFW

Unterstützte Zertifizierungsstellen (Min.): Windows Server 2003 Enterprise

Vorlagenname:
Smartcard-BFW

Gültigkeitsdauer: 2 Jahre | Erneuerungszeitraum: 6 Wochen

Zertifikat in Active Directory veröffentlichen
 Nicht automatisch neu registrieren, wenn ein identisches Zertifikat bereits in Active Directory vorhanden ist

Vorhandenen Schlüssel für automatische Erneuerung von Smartcardzertifikaten verwenden, falls Erstellung eines neuen Schlüssel nicht möglich ist

OK | Abbrechen | Übernehmen | Hilfe

CSP des Smartcard Anbieters in der Anforderungsverarbeitung angeben

Kryptografiedienstanbieter auswählen

Wählen Sie die Kryptografiedienstanbieter aus, die in Anforderungen verwendet werden können:

Alle Kryptografiedienstanbieter auf dem Computer des Antragstellers

Einen der folgenden Kryptografiedienstanbieter verwenden:

Kryptografiedienstanbieter:

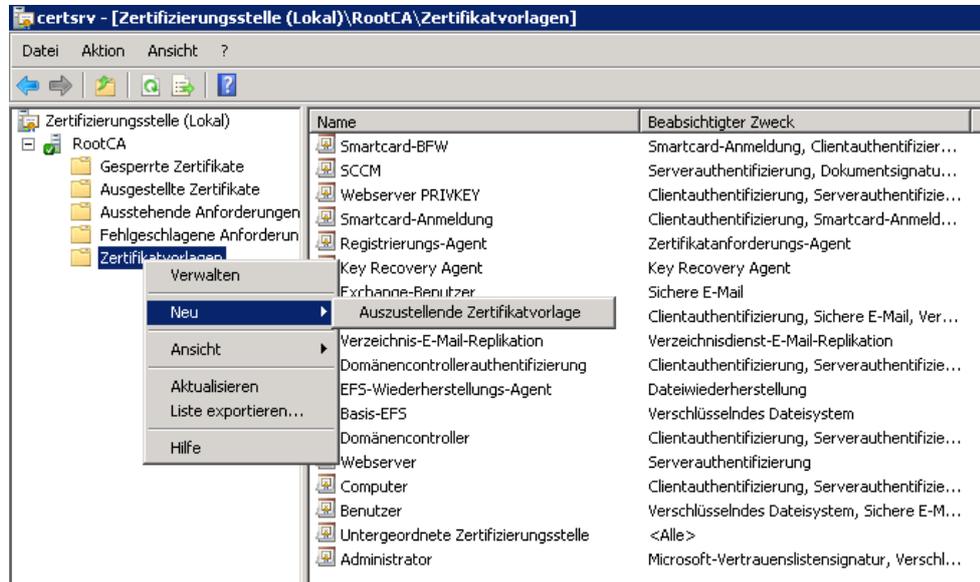
- Token Base Cryptographic Provider
- Microsoft Base Smart Card Crypto Provider
- Microsoft DH SChannel Cryptographic Provider
- Microsoft Enhanced Cryptographic Provider v1.0
- Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider
- Microsoft Enhanced RSA and AES Cryptographic Provider
- Microsoft RSA SChannel Cryptographic Provider
- Microsoft Strong Cryptographic Provider

OK | Abbrechen

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

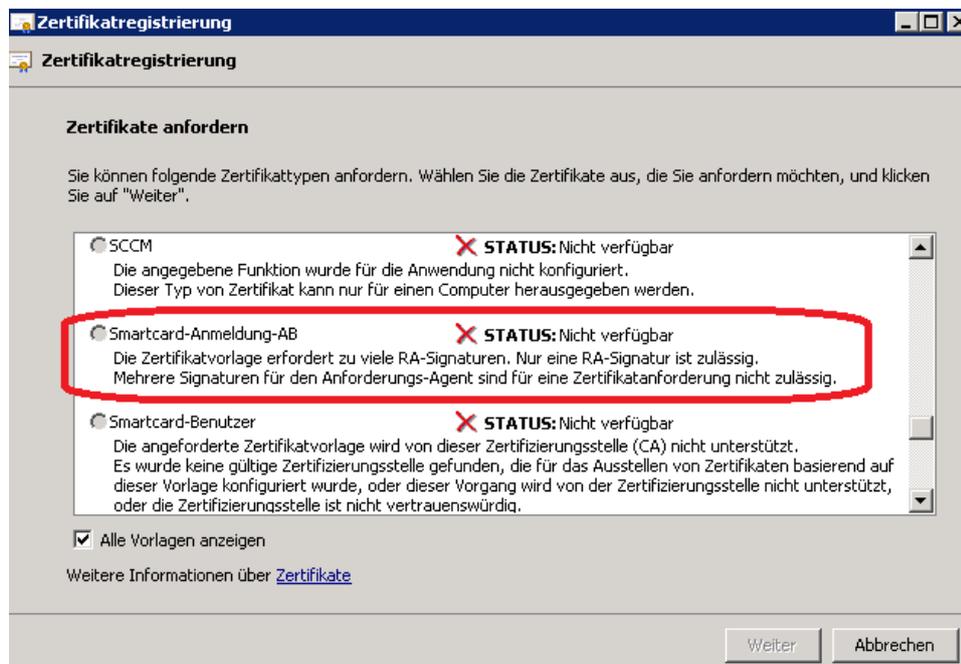
Neue Zertifikatvorlage fuer CA Verwendung aktivieren

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



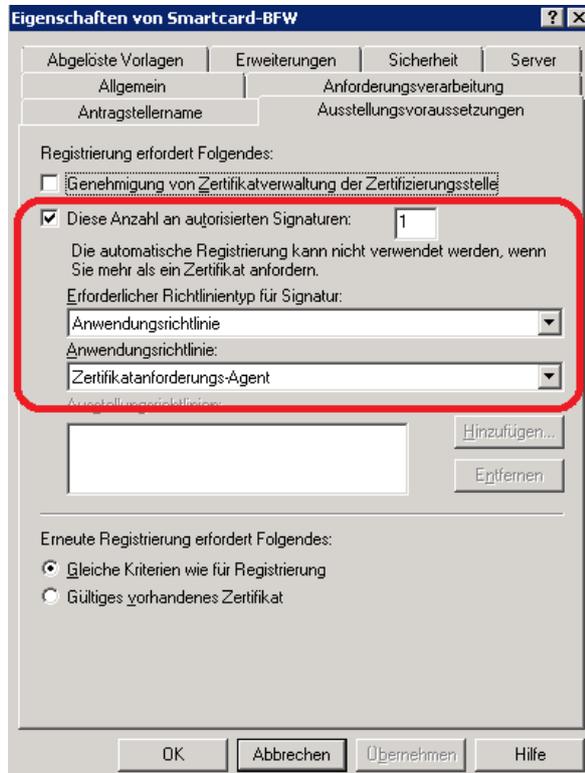
Fehlermeldung beim Anfordern des Smartcard Zertifikats

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



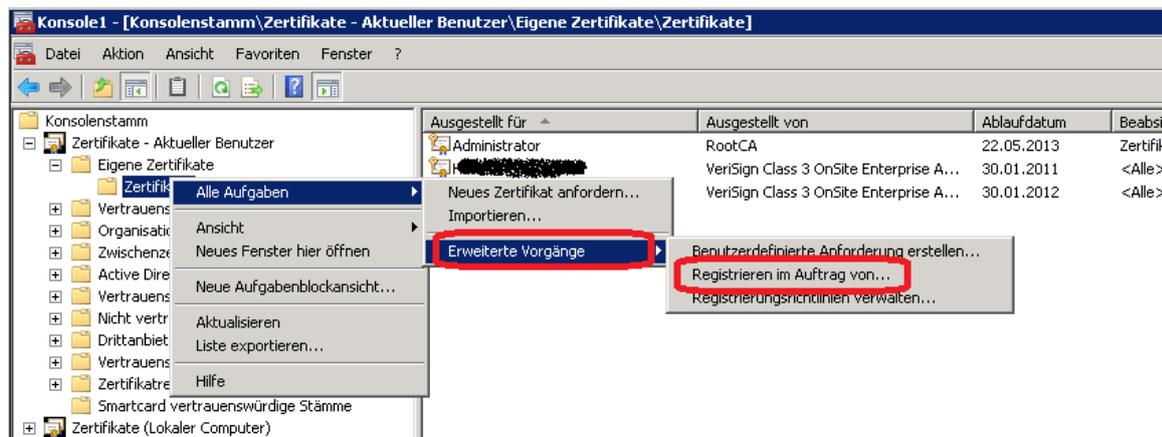
Loesung

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

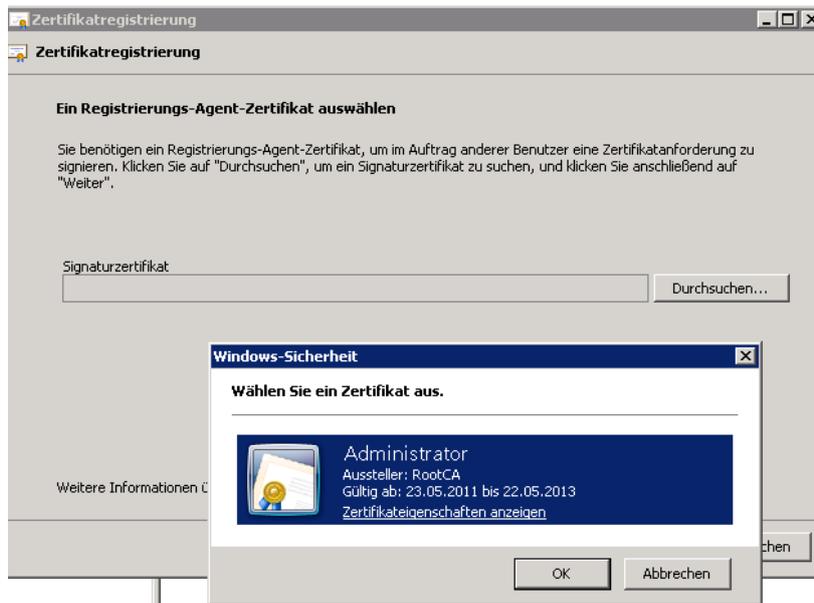


Smartcard Zertifikat Anforderung auf Enrollment Station

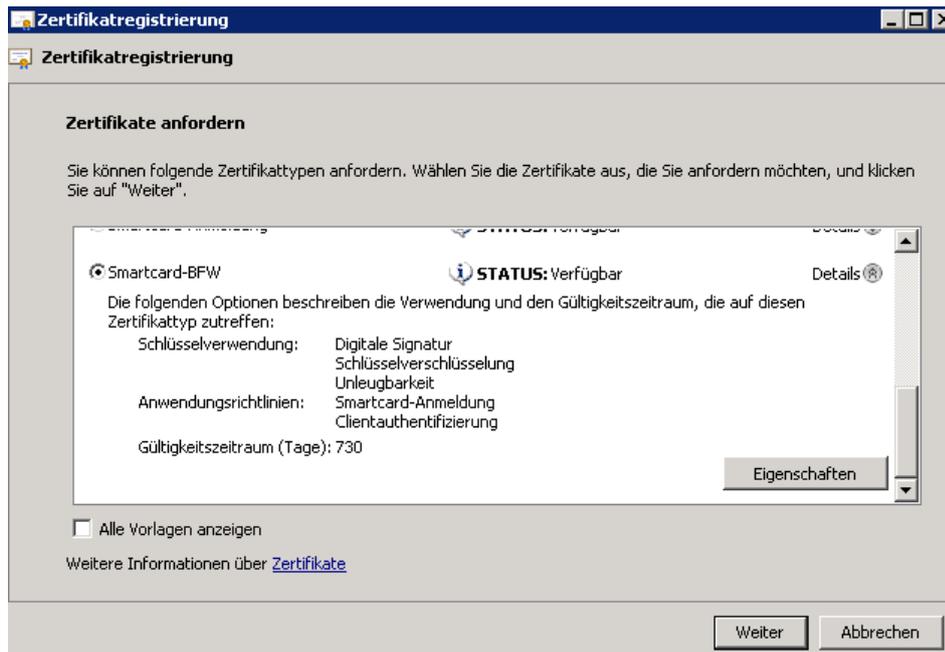
Seit Windows Server 2008 geht das Smartcardenrollment fuer andere Benutzer nicht mehr per /CERTSRV Webseite. Es muss jetzt die MMC auf dem PC verwendet werden (Seit Vista/7). Registrieren im Auftrag von ...



Registrierungs Agenten Zertifikat auswaehlen

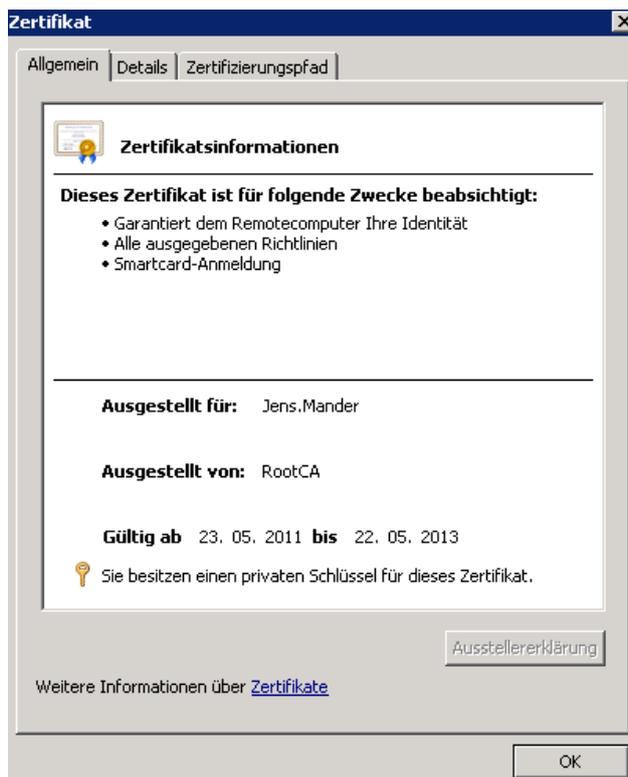


Zertifikatvorlage auswaehlen



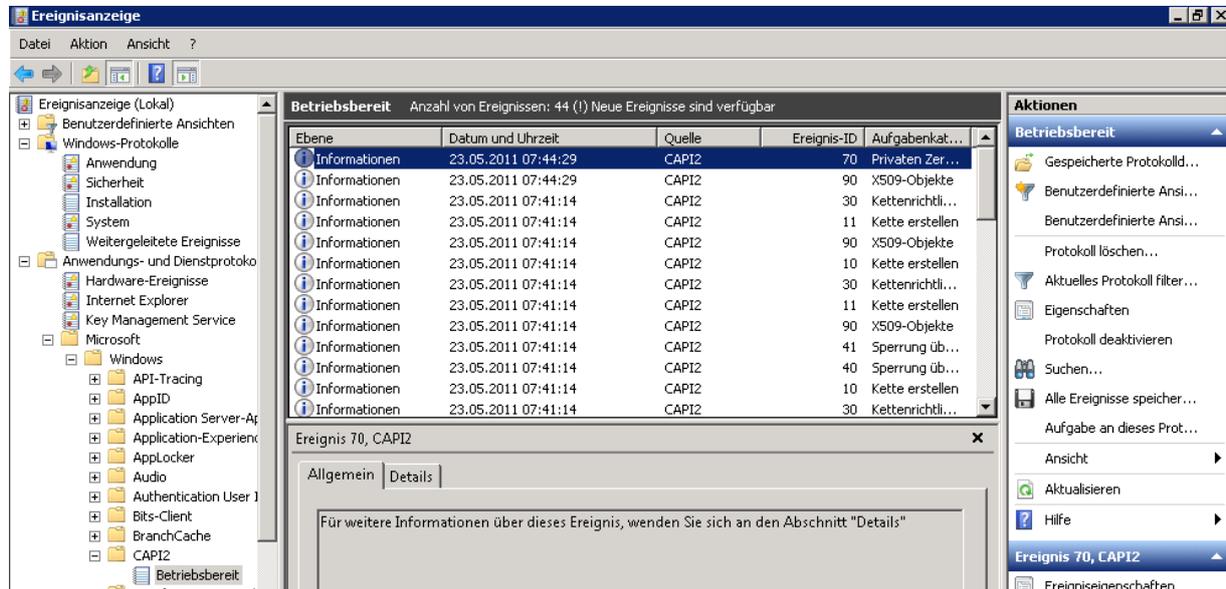


Zertifikat ist fuer zwei Jahre ausgestellt

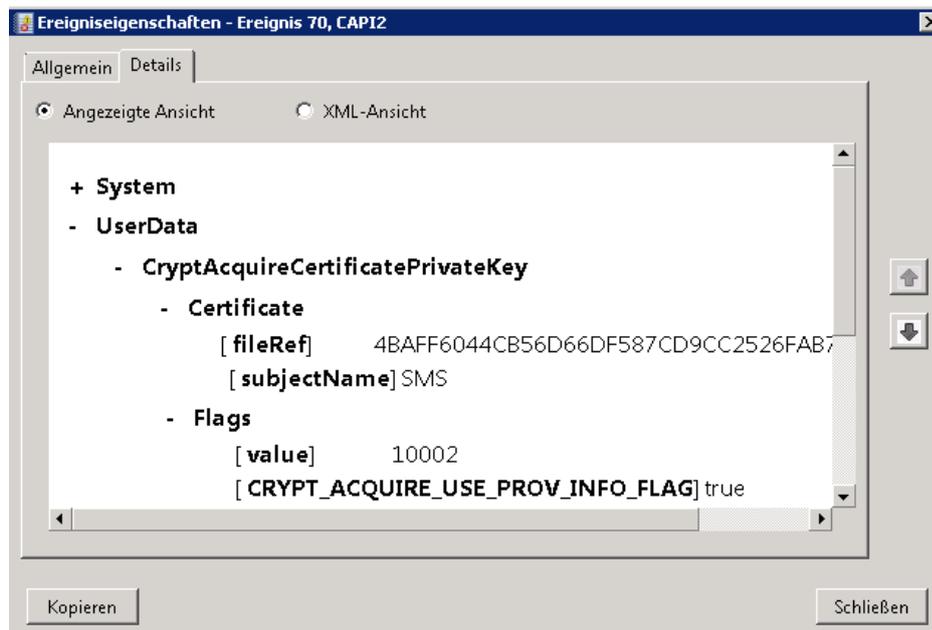


CAPI Logging

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.

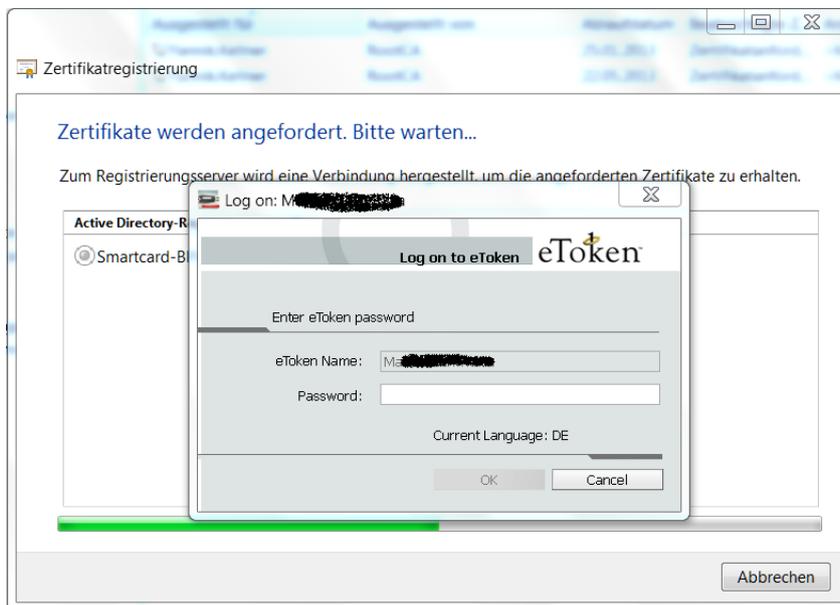
Administrative Taetigkeiten auf der Smartcard Enrollment Workstation

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

| | | | | |
|--|--|-----------|-------------|----------------|
| Remotedesktopdienste | Ermöglicht Benutzern das Herstellen einer interaktiven Verbindung mit einem Remotecomputer. Remotedesktop und Remotedesktop-Hostserve... | Gestartet | Manuell | Netzwerkdienst |
| Remoteprozaduraufwurf (RPC) | Der RPCSS-Dienst wird als Dienststeuerungs-Manager für COM- und DCOM-Server verwendet. Von ihm werden Objektivierungsanforderunge... | Gestartet | Automa... | Netzwerkdienst |
| Remoteregistrierung | Ermöglicht Remotebenutzern, Registrierungseinstellungen dieses Computers zu verändern. Wenn dieser Dienst beendet wird, kann die Registrier... | Gestartet | Automa... | Lokaler Dienst |
| Richtlinie zum Entfernen der Smartcard | Lasst eine Konfiguration des Systems zu, bei der der Benutzerdesktop bei Entfernen der Smartcard gesperrt wird. | | Manuell | Lokales System |
| Routing und RAS | Bietet Routingdienste in LAN- und WAN-Netzwerkumgebungen. | | Deaktivi... | Lokales System |
| RPC-Endpunktzuoordnung | Löst RPC-Schnittstellen-IDs für den Transport von Endpunkten auf. Wenn dieser Dienst angehalten oder deaktiviert wird, können Programme, fü... | Gestartet | Automa... | Netzwerkdienst |

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

| | |
|--|-----------------|
| Domänencontroller: Serveroperatoren das Einrichten von geplant... | Nicht definiert |
| Domänencontroller: Signaturanforderungen für LDAP-Server | Nicht definiert |
| Domänenmitglied: Änderungen von Computerkontenkennwörtern... | Nicht definiert |
| Domänenmitglied: Daten des sicheren Kanals digital signieren (we... | Nicht definiert |
| Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln... | Nicht definiert |
| Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln... | Nicht definiert |
| Domänenmitglied: Maximalalter von Computerkontenkennwörtern | Nicht definiert |
| Domänenmitglied: Starker Sitzungsschlüssel erforderlich (Window... | Nicht definiert |
| Geräte: Anwendern das Installieren von Druckertreibern nicht erl... | Nicht definiert |
| Geräte: Entfernen ohne vorherige Anmeldung erlauben | Nicht definiert |
| Geräte: Formatieren und Auswerfen von Wechselmedien zulassen | Nicht definiert |
| Geräte: Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Be... | Nicht definiert |
| Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Be... | Nicht definiert |
| Herunterfahren: Auslagerungsdatei des virtuellen Arbeitsspeicher... | Nicht definiert |
| Herunterfahren: Herunterfahren des Systems ohne Anmeldung z... | Nicht definiert |
| Interaktive Anmeldung: Anwender vor Ablauf des Kennworts zum... | Nicht definiert |
| Interaktive Anmeldung: Anzahl zwischenspeichernder vorherig... | Nicht definiert |
| Interaktive Anmeldung: Benutzerinformationen anzeigen, wenn S... | Nicht definiert |
| Interaktive Anmeldung: Domänencontrollerauthentifizierung zum ... | Nicht definiert |
| Interaktive Anmeldung: Kein STRG+ALT+ENTF erforderlich | Nicht definiert |
| Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen | Nicht definiert |
| Interaktive Anmeldung: Nachricht für Benutzer, die sich anmelde... | Nicht definiert |
| Interaktive Anmeldung: Nachrichtentitel für Benutzer, die sich an... | Nicht definiert |
| Interaktive Anmeldung: Smartcard erforderlich | Nicht definiert |
| Interaktive Anmeldung: Verhalten beim Entfernen von Smartcards | Nicht definiert |
| Konten: Administrator umbenennen | Nicht definiert |

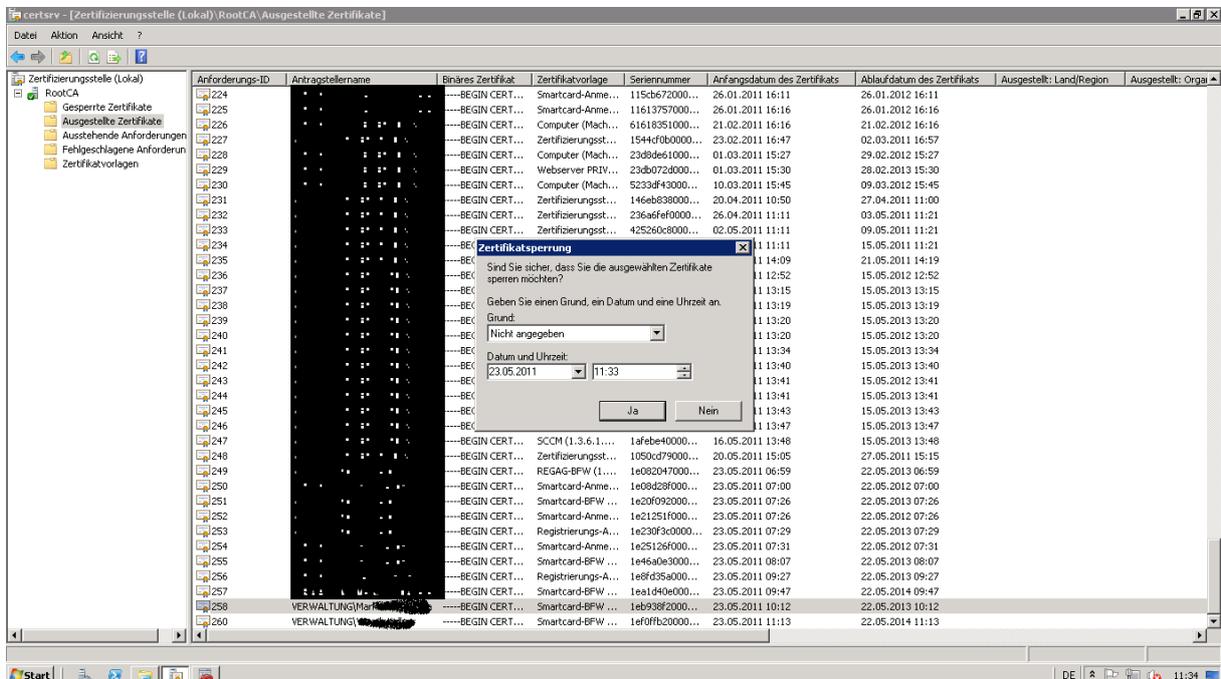
Die Einstellungen fuer den PKI Client koennen auch per Gruppenrichtlinie konfiguriert werden

| eToken PKI Client Settings/eToken PKI Client Properties Settings hide | | |
|--|-------------|-----------|
| Richtlinie | Einstellung | Kommentar |
| Advanced View | Aktiviert | |
| Advanced View | 0 | |

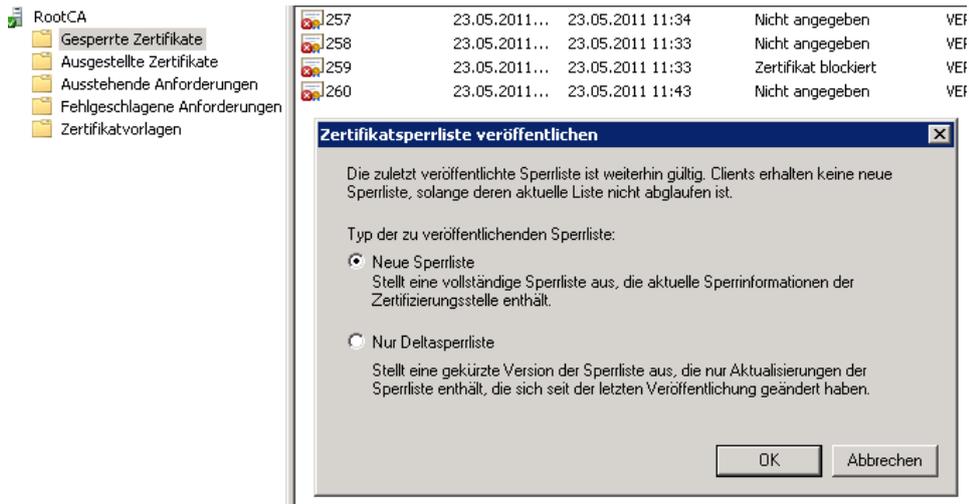
| eToken PKI Client Settings/UI Access Control List hide | | |
|---|-------------|-----------|
| Richtlinie | Einstellung | Kommentar |
| Access Control | Aktiviert | |
| ChangePassword | 1 | |
| RenameToken | 0 | |
| UnlockEToken | 0 | |
| ClearEToken | 0 | |
| ViewTokenInfo | 1 | |
| DisconnectVirtual | 1 | |
| OpenAdvancedView | 0 | |
| AddTokenVirtual | 0 | |
| ManageReaders | 1 | |
| InitializeEToken | 0 | |

Zertifikat revoke

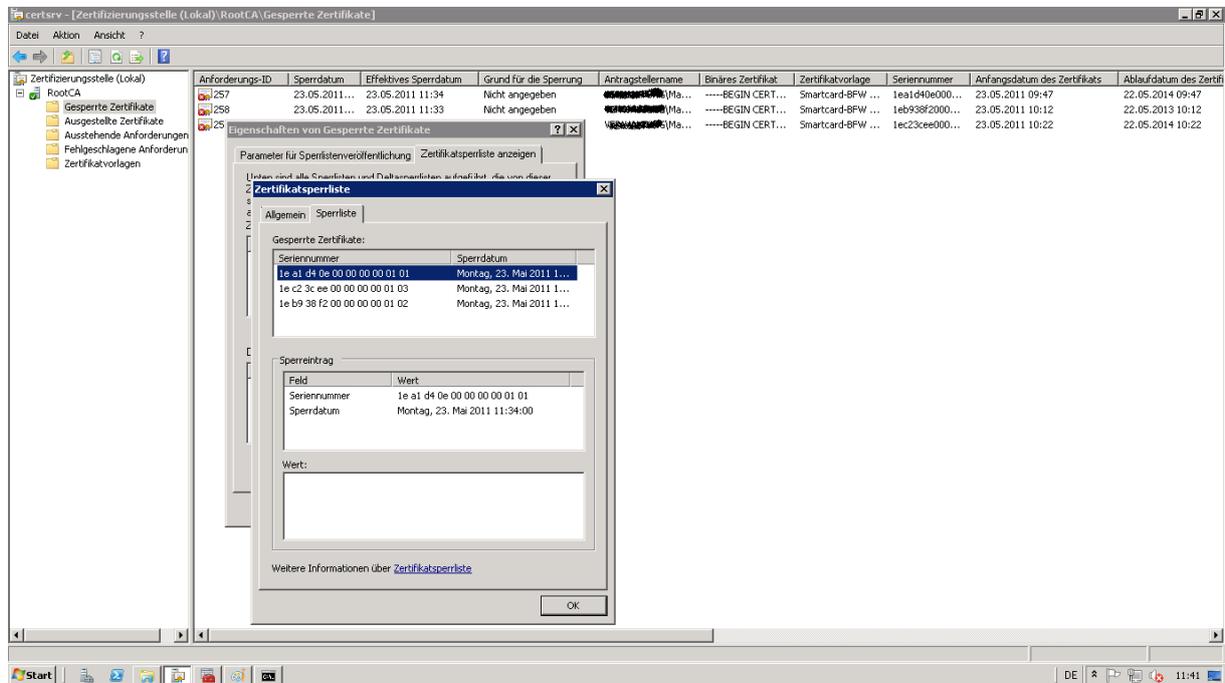
Wenn der Benutzer das Smartcard Zertifikat nicht mehr verwenden darf (z. B. Bei Verlust der Smartcard), muss das ausgestellte Zertifikat an der CA revokiert werden



Danach kann die Base- oder Delta CRL manuell veröffentlicht werden



Anzeige der Sperrliste



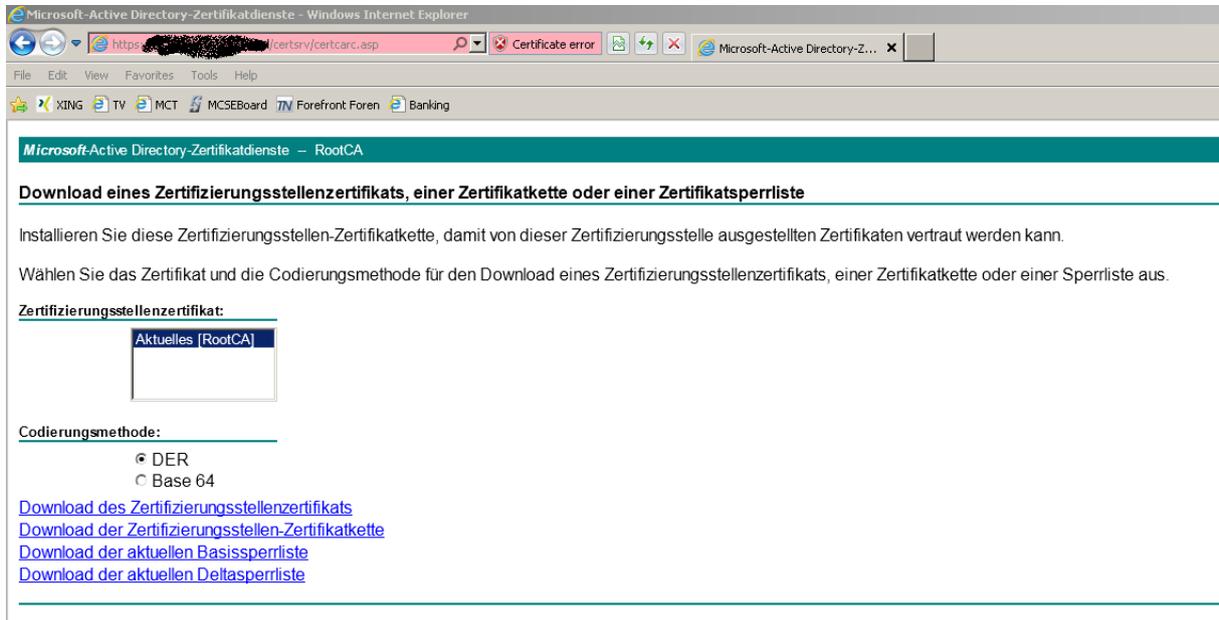
Lokalen CRL Cache anzeigen

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.

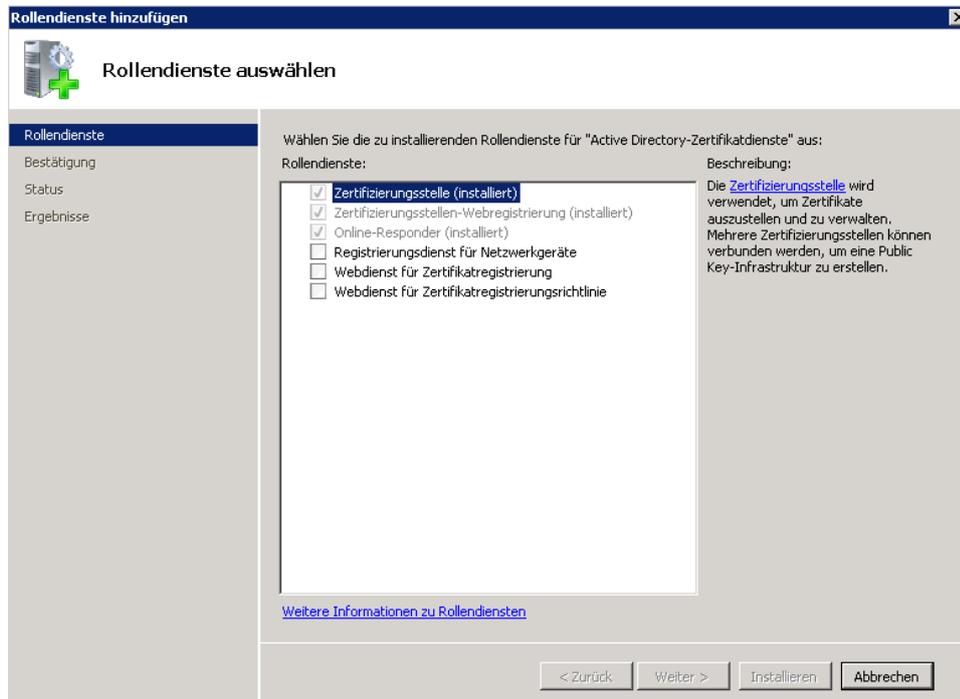


Wenn die CRL aktuell ist, passiert bei dem Versuch der Anmeldung des Clients mit Smartcard folgendes:

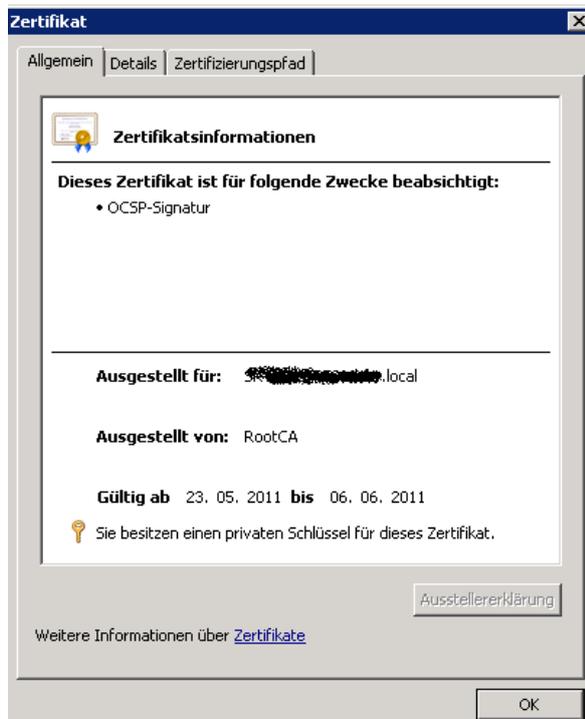


Optional: OCSP Responder Einrichtung

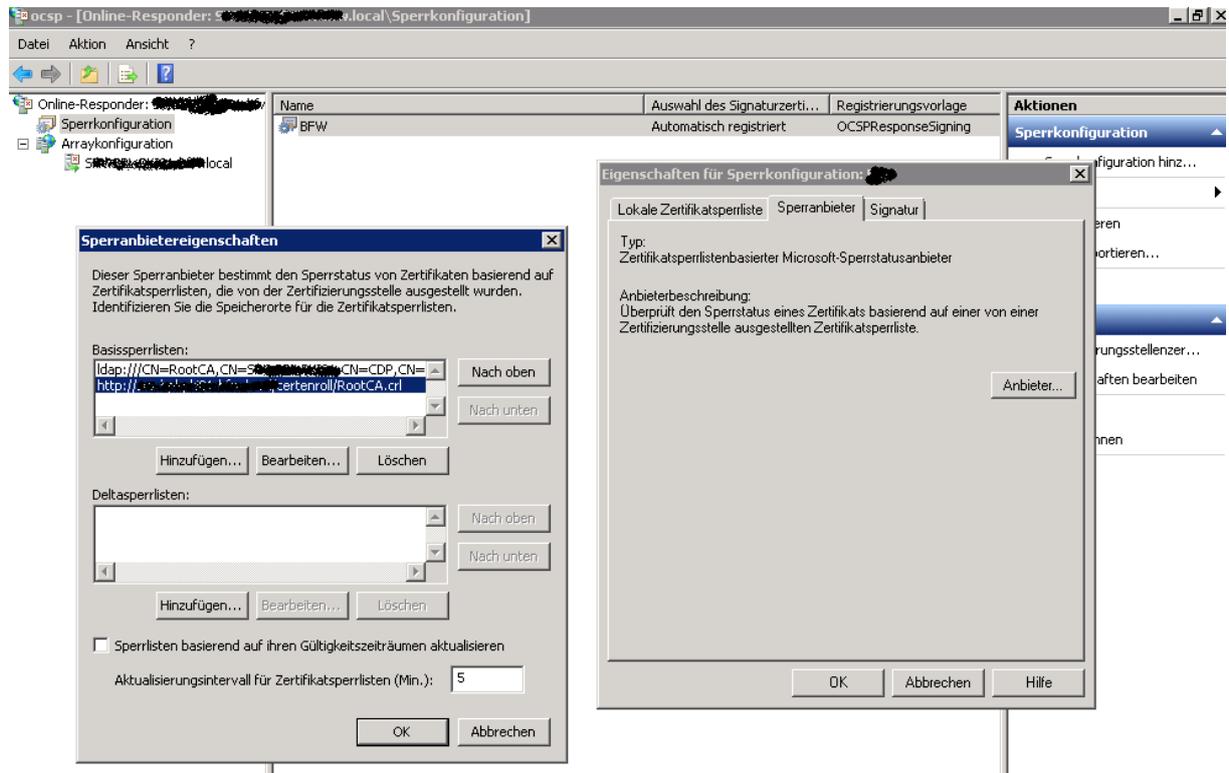
OCSP Responder installieren



OCSP Signing Zertifikat anfordern



Sperranbieter konfigurieren



Dem Zeitablauf der Sperrlisten folgen oder manuell ueberschreiben



Sperrkonfigurationsstatus OK

Sperrkonfigurationsstatus

 Signaturzertifikat... OK

[Signaturzertifikat anzeigen](#)

Sperranbieterstatus:

Typ: Zertifikatsperrlistenbasierter Microsoft-Sperrstatusanbieter
Der Sperranbieter verwendet erfolgreich die aktuelle Konfiguration.