Implementierung Smartcard Aladdin E-Token pro für Domänen-Anmeldung

Hardware:

- USB Smart Card Reader und USB Token der Fa. Aladdin (E-Token Pro)

Software

- Aladdin Smart Card Runtime Environment (Version 4.0 – RTE.MSI)
- Windows 2003 Server Enterprise SP2 in Forest Root Domain mit zwei Subdomains
- Active Directory integrierte Root CA

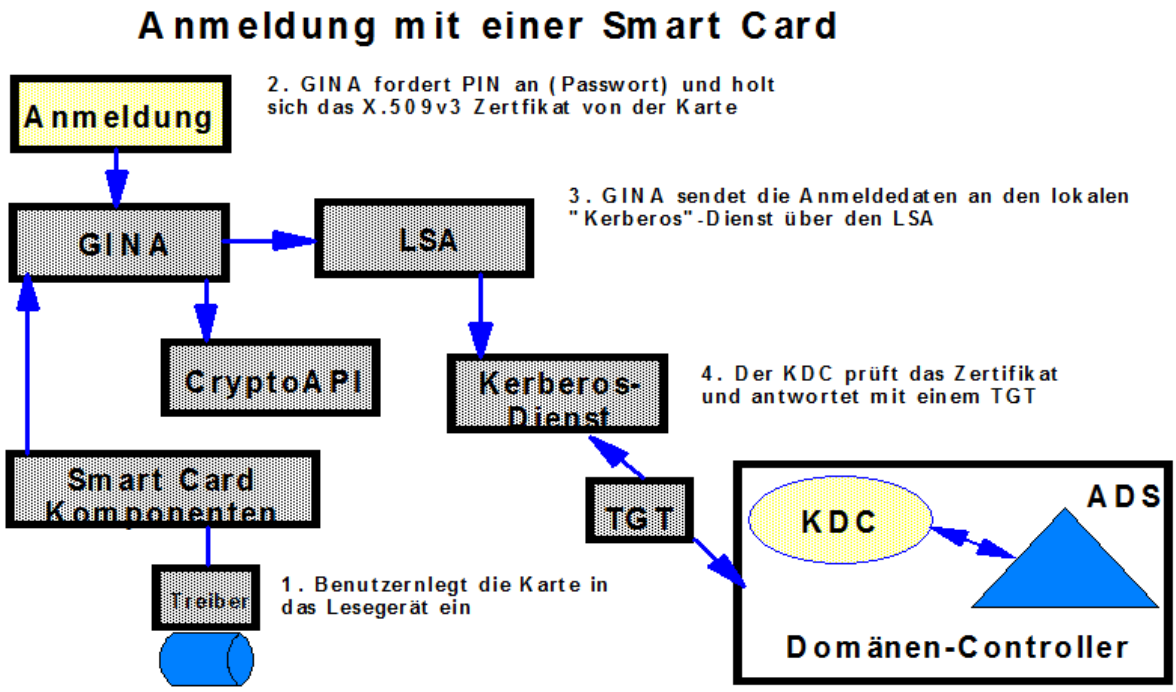
Voraussetzung:

- E-Token Runtime Environment auf dem PKI Server installieren. Die RTE 4.0 installiert auch den notwendigen CSP (Cryptographic Service Provider).
- Erstellen eine Smartcard Enrollment Workstation mit Windows XP

Ziel:

- Smartcard Anmeldung fuer einen bestimmten Benutzerkreis
- Ausschliessliches Anmelden über die Smartcard möglich
- Automatisches Abmelden bei Entfernen der Smartcard

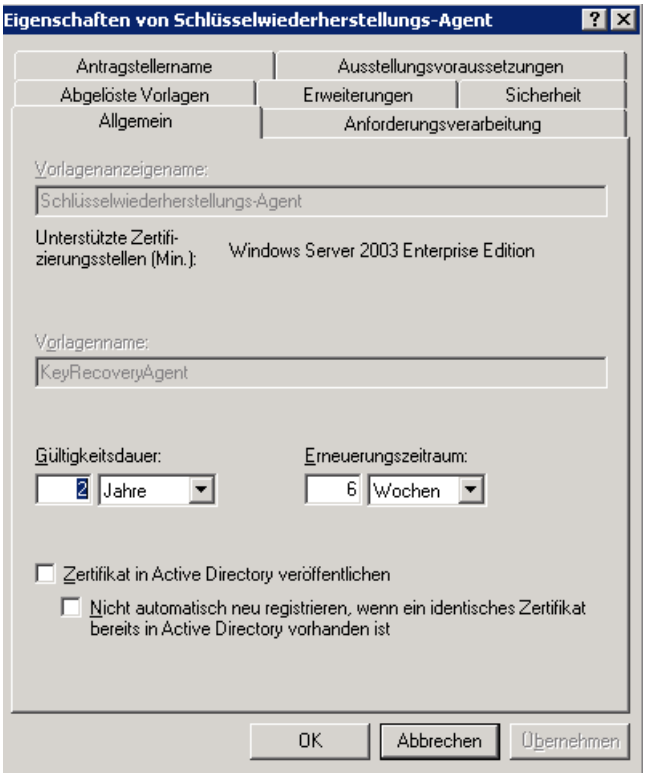
Technisches:



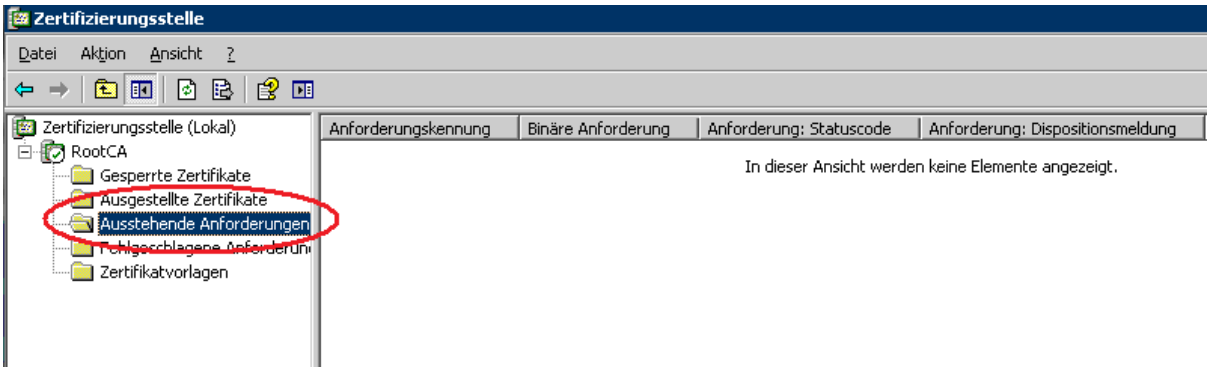
Schlüssel-Archivierung und Wiederherstellung

Der Kunde wünschte die Einrichtung einer Schlüssel-Archivierung und Wiederherstellung. Folgende High Level Steps sind zur Einrichtung erforderlich:

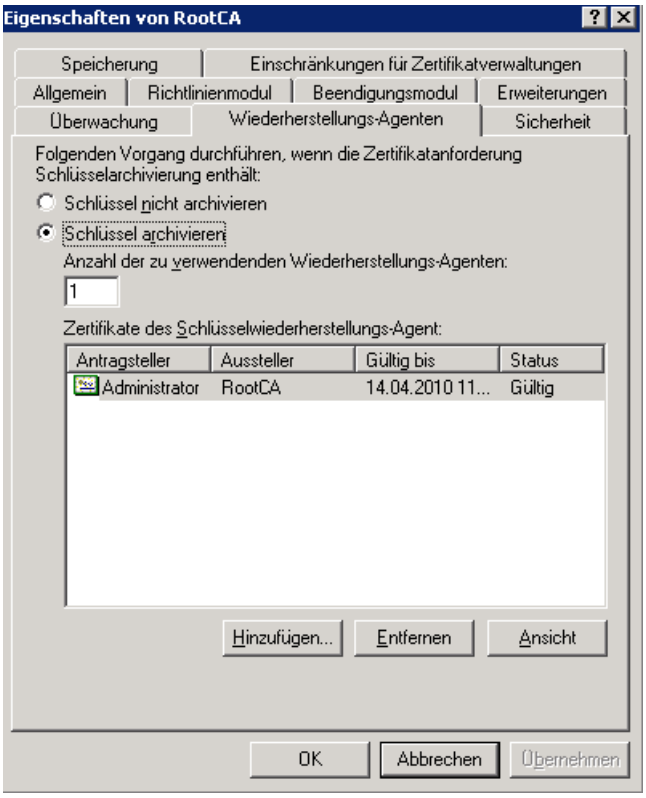
Erstellen eines Schlüsselwiederherstellungs-Agenten Zertifikats. Hierzu ist in der CA-Verwaltung die entsprechende Zertifikatvorlage zu veröffentlichen.



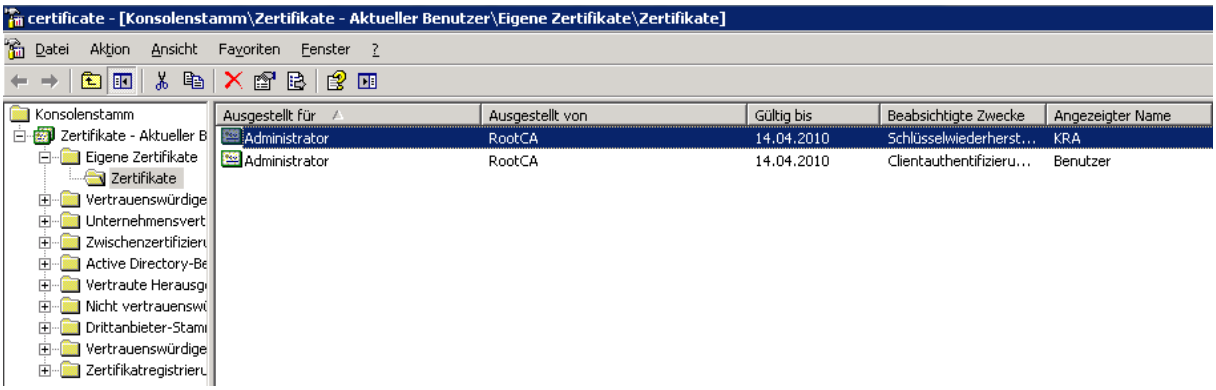
Die Gueltigkeit wurde auf zwei Jahre erhoeht. Bei der Beantragung ueber das Zertifikats SnapIn am lokalen Computer wird das Zertifikat aufgrund der Sicherheitsbrisanz nicht sofort ausgestellt, sondern muss von der CA-Verwaltung manuell ausgestellt werden (Ausstehende Anforderungen).



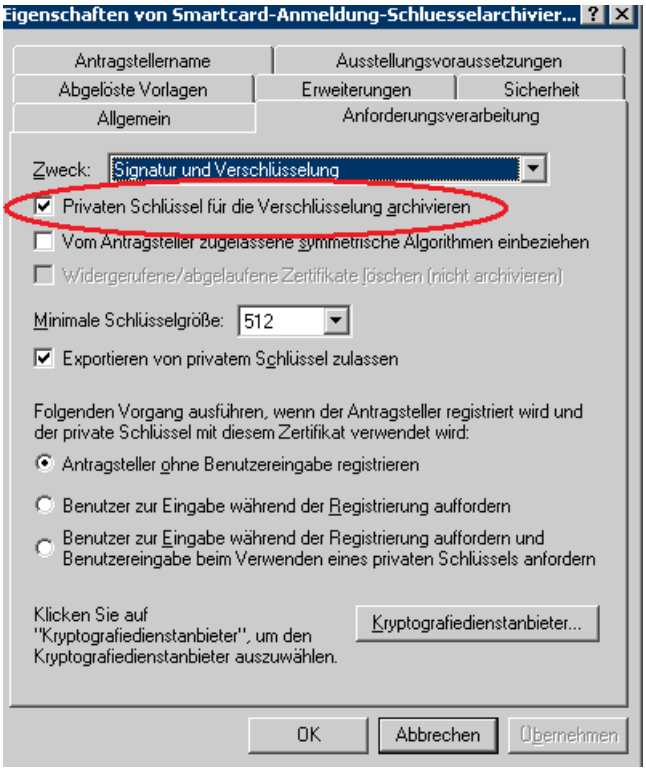
Anschließend kann in den Eigenschaften der CA, die Schlüsselwiederherstellung aktiviert werden.
Wenn das Schlüsselwiederherstellungs-Agentenzertifikat ueber die MMC beantragt wurde, muss anschliessend das Zertifikat als .CER-Datei auf dem PKI-Server exportiert und auf dem Schluesselwiederherstellungs-Agenten PC wieder importiert werden. Bei einer Bentragung ueber das Webinterface (HTTPS://Servername.tld/certsrv) waere das nicht notwendig gewesen.



Das Schluesselwiederherstellungs-Agenten Zertifikat



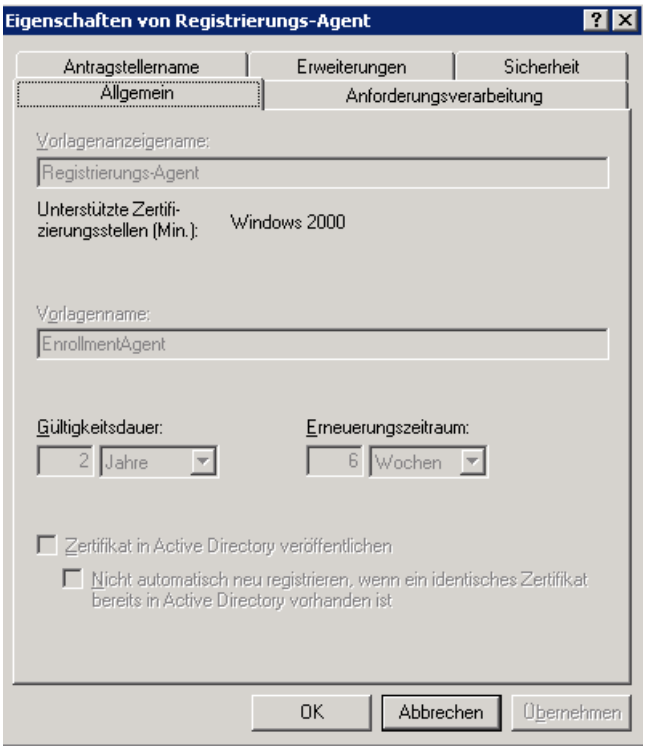
Im naechsten Schritt muss die Vorlage fuer die Smartcard Anmeldung gedoppelt werden, damit fuer die neue Vorlage eine Schluesselarchivierung aktiviert werden kann.



Smartcard Anforderung

Als erstes muss die Vorlage „Smartcard Anmeldung“ oder die neue Smartcard-Anmeldung Zertifikatvorlage mit aktivierter Schluessel-Archivierung zur Verwendung an der CA ausgestellt werden.

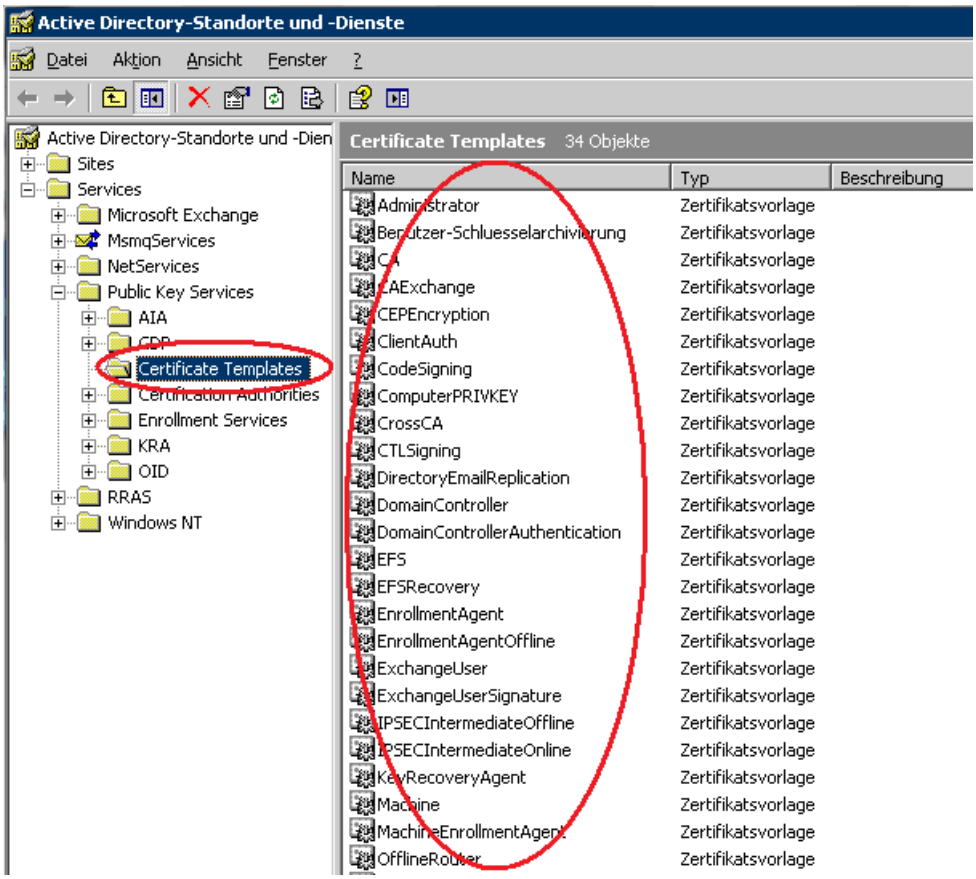
Im naechsten Schritt muss die Zertifikatvorlage „Registrierungs-Agent“ ausgestellt werden. Mit Hilfe dieser Vorlage darf spaeter ein vertrauenswuerdiger Administrator Smartcard-Zertifikat fuer andere Benutzer ausstellen.



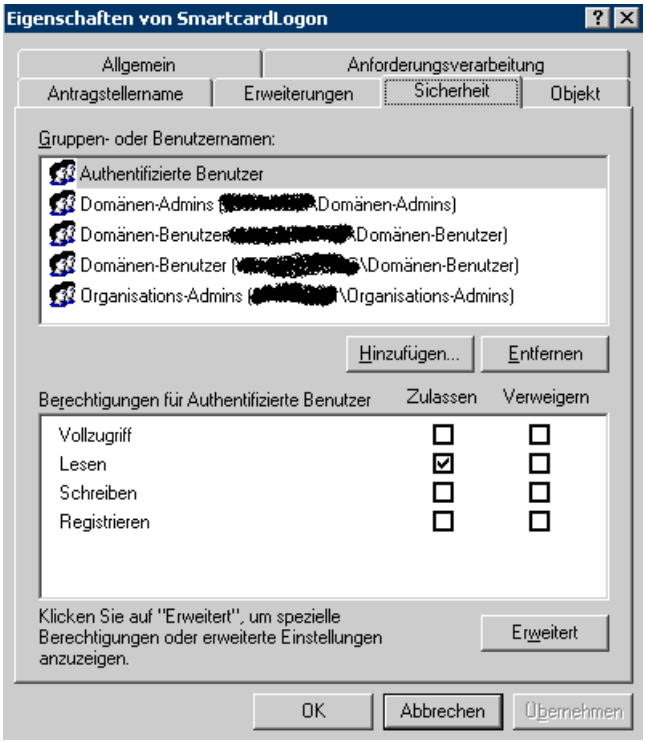
Das Registrierungs-Agenten Zertifikat wird automatisch von der Zertifizierungsstelle ausgestellt.

Damit sind die Vorbereitungen abgeschlossen, mit einer Ausnahme in diesem speziellen Szenario. Da es sich bei dem Kunden um einen Forest mit zwei Subdomains handelt, muessen die Berechtigungen fuer den Zertifikatvorlagen Container in der Konfigurations-Partition im Active Directory und fuer die notwendigen Vorlagen angepasst werden, so dass auch Benutzer in den Subdomains Zertifikate und Zertifikatvorlagen verwenden koennen.

Dazu muss zum einen dafuer gesorgt werden, dass die entsprechenden Benutzer Leseberechtigung auf den Container Zertifikatvorlagen und auf die entsprechenden einzelnen Zertifikatvorlagen haben, sonst erscheint bei dem Hinzufuegen von Zertifikaten in der Zertifikats-Management Konsole auf den Clients der Subdomaenen die Fehlermeldung, dass keine Zertifizierungsstelle und Zertifikatvorlagen installiert sind.

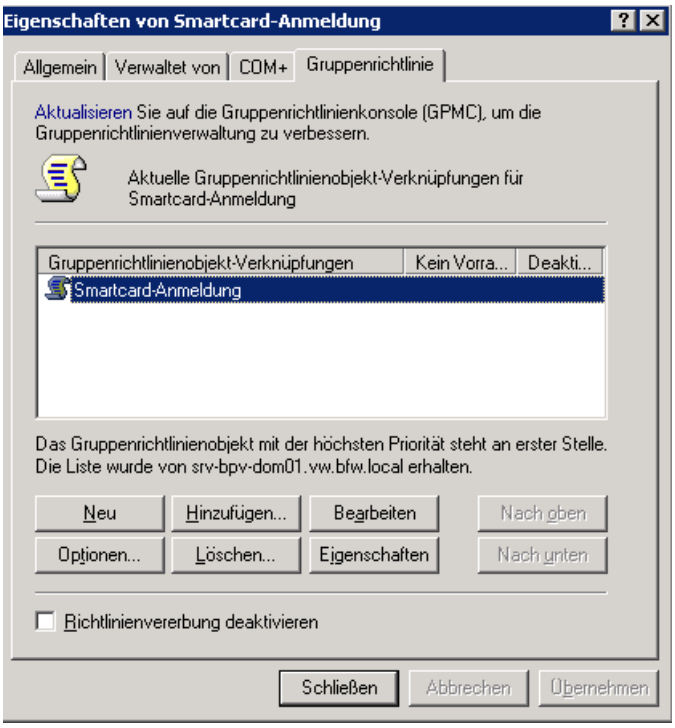


Sicherheits-Einstellungen

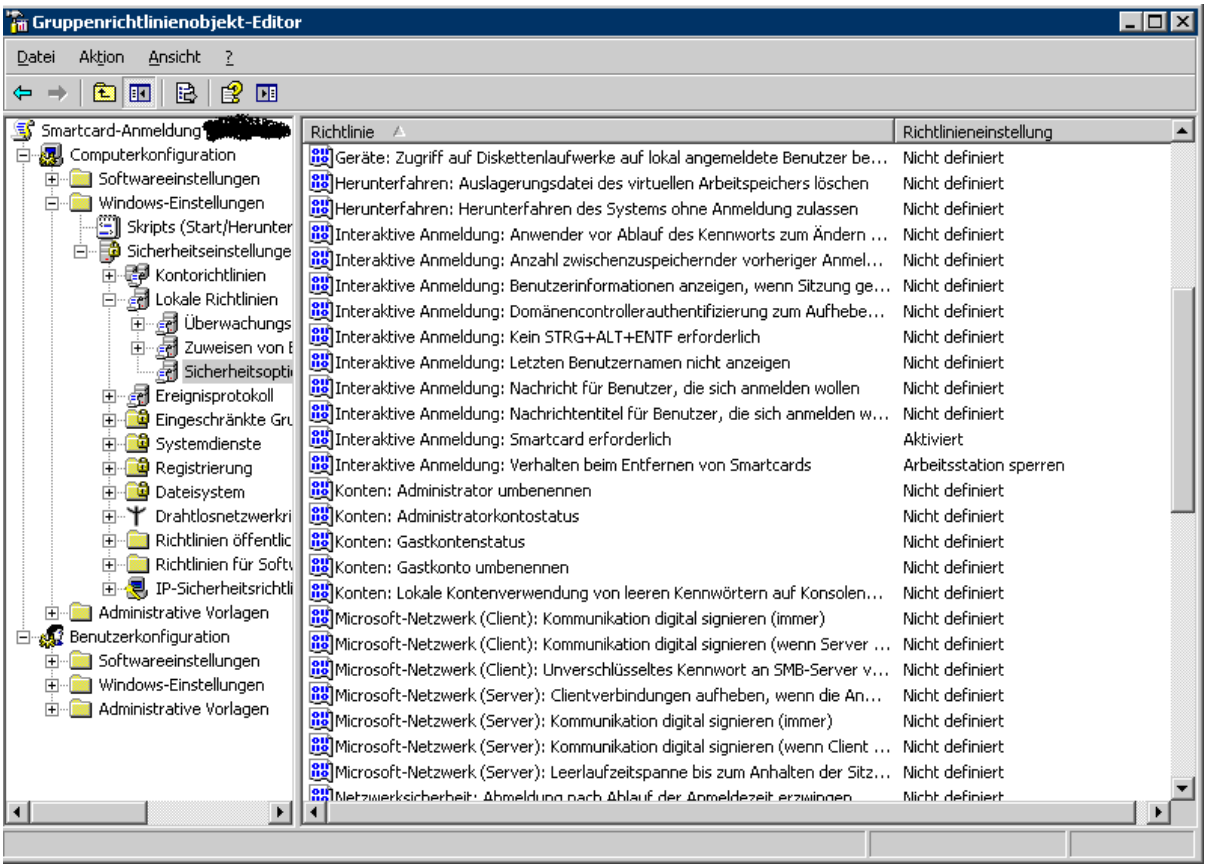


Erstellen einer Gruppenrichtlinie

Der naechste Schritt ist die Erstellung einer Gruppenrichtlinie zur Einrichtung des Verhaltens des PC bei der Verwendung von Smartcards.



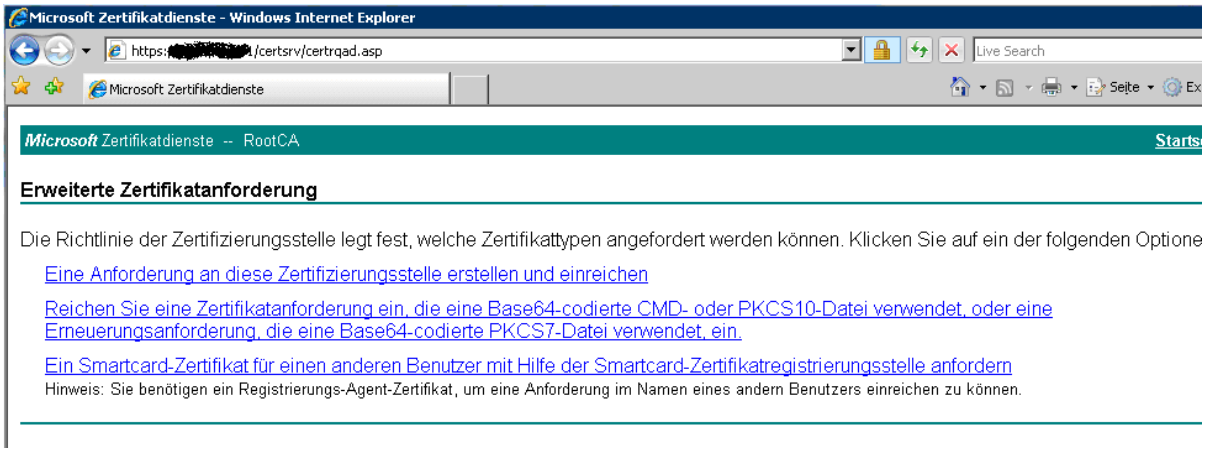
Das gewuenschte Verhalten ist hier, dass Smartcards erforderlich sind und das beim Abziehen der Smartcard der Computer gesperrt wird.



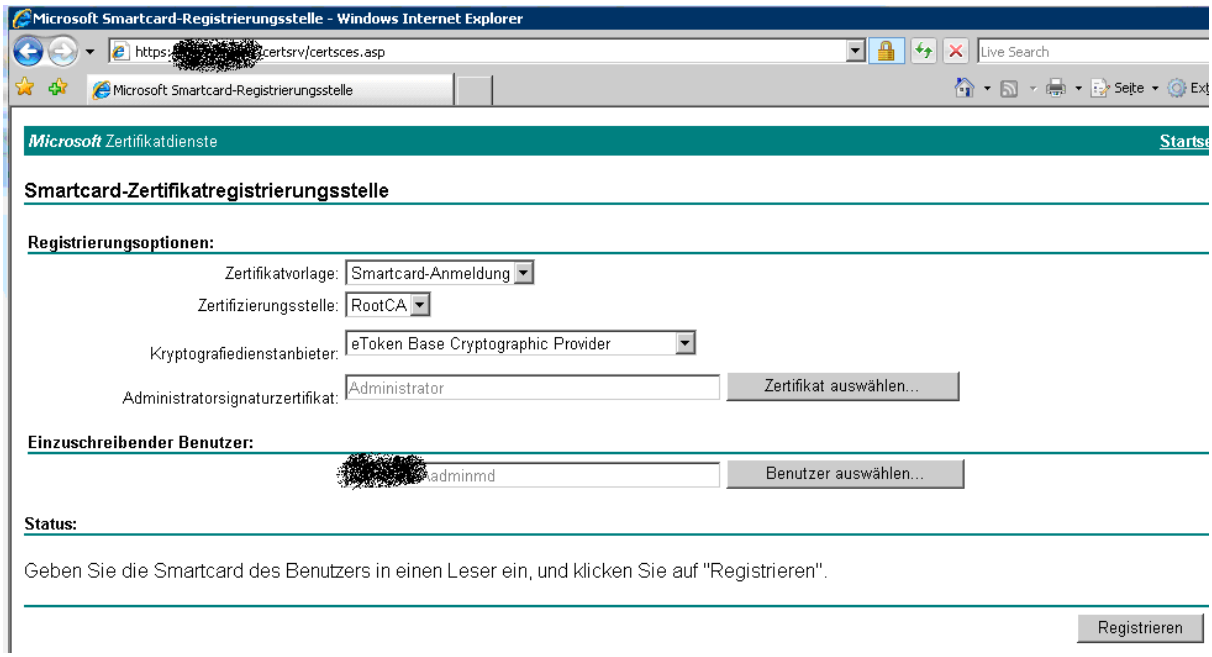
Alternativ kann auch pro Benutzerobjekt (DSA.MSC) festgelegt werden, dass eine Anmeldung ueber Smartcards zwingend erforderlich ist.

Anfordern eines Smartcard Zertifikat fuer einen anderen Benutzer

Im naechsten Schritt kann ein Smartcard Zertifikat fuer einen beliebigen Benutzer angefordert werden. Dazu ist die Webkonsole zu starten und ein Smartcard Zertifikat fuer einen anderen Benutzer anzufordern.

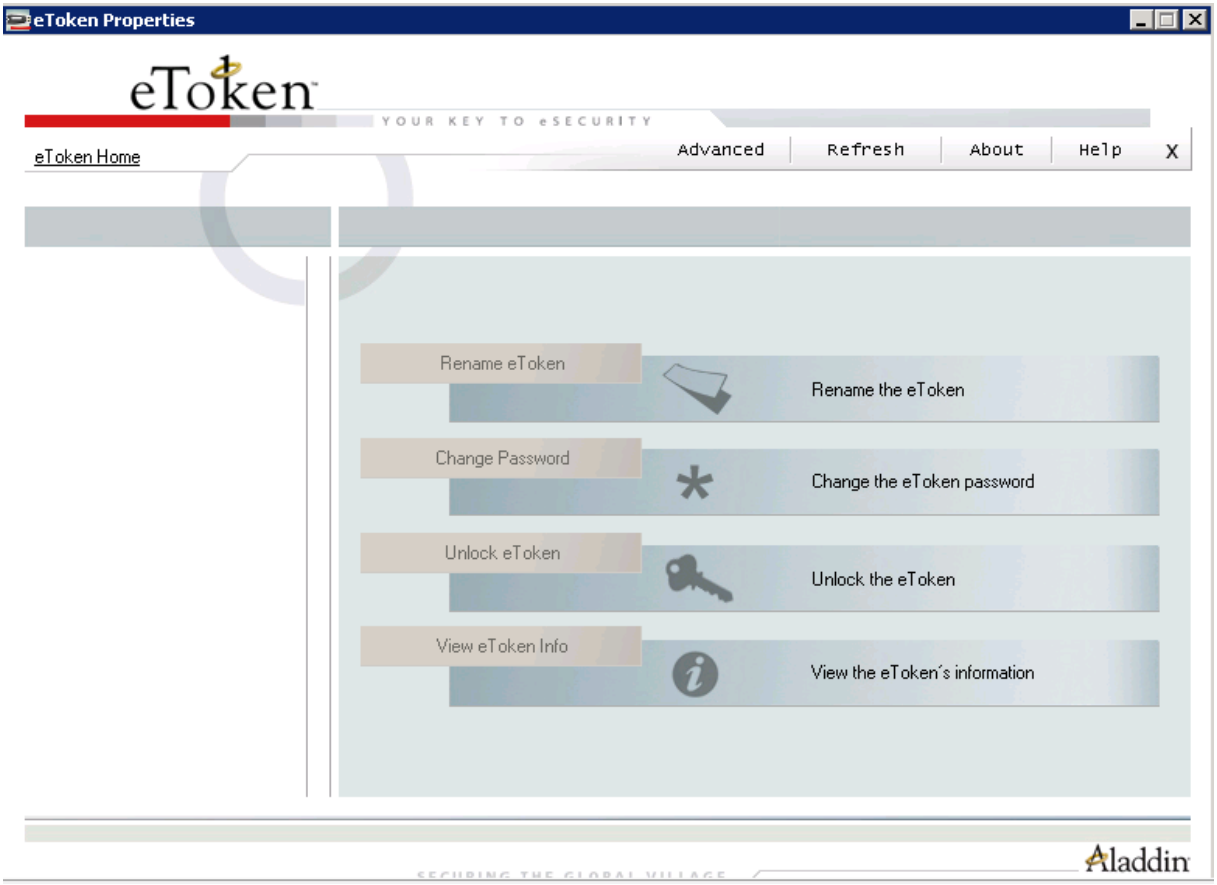


Die Zertifikatvorlage ist „Smartcard-Anmeldung“, der Kryptografiedienstanbieter ist der eToken Base Cryptographic Provider (CSP), welcher durch die RTE Installation installiert wurde.



Der Benutzer kann nun die Smartcard verwenden.

Smartcard Verwaltung mit der E-Token Software



Software-Verteilung der RTE

Die RTE kann per Microsoft Active Directory Gruppenrichtlinien verteilt werden, da die RTE als MSI-Paket vorliegt. Weitere Informationen zum Beispiel auf www.gruppenrichtlinien.de.