ERNW Newsletter 9 / Mai 2006

Liebe Partner, liebe Kollegen,

willkommen zur neunten Ausgabe des ERNW-Newsletters mit dem Thema:

Smartcard-basiertes SSO mit STARCOS/*AET Safesign* in Active Directory-Umgebungen mit Citrix und Zertifikaten einer 3.-Party CA

(How To mit Dokumentation)

V. 1.0 vom 1. Mai 2006

von:

Friedwart Kuhn (fkuhn@ernw.de) und
Enno Rey (erey@ernw.de)

Abstract:
In diesem How To ist detailliert dargelegt, wie eine Smartcard-basierte Authentifizierung in verschiedenen Microsoft Active Directory-Umgebungen mit öffentlichen (d.h. etwa von einer M-PKI erstellten) Zertifikaten und der Verwendung von Citrix stattfinden kann. Es sind alle notwendigen Voraussetzungen und Konfigurations-Schritte beschrieben.

INHALTSVERZEICHNIS

1 EINLEITUNG

Active Directory-basierte Citrix-Umgebungen bieten durch zentralisiertes und einheitliches Desktopmanagement immer einen mittel- und langfristigen Mehrwert für die Administration und Verwaltung von Windows-Umgebungen. Smartcard-basiertes Single Sign On (SSO) ermöglicht durch eine Zweifaktor-Authentifizierung zusammen mit Zertifikaten und einer dahinter stehenden Public Key-Infrastruktur (PKI) eine nicht nur derzeit, sondern auch in den nächsten Jahren sichere Authentifizierung gegenüber den von dem Anwender benötigten Ressourcen. Darüber hinaus bietet Smartcard-basiertes SSO die Möglichkeit für größere Umgebungen, Benutzern das Merken von einem oder mehreren Passwörtern zu ersparen; statt dessen muss der Benutzer nur die PIN der Smartcard wissen. Eine lohnende Herausforderung stellt also die Implementierung von Active Directory-basierten Citrix-Umgebungen *zusammen mit* Smartcard-basiertem SSO dar.

Soll es sich bei der PKI um eine reine Windows-basierte Lösung handeln, so ist die Implementierung zwar immer noch nicht trivial, dafür aber wohl dokumentiert und oft durchgeführt. Entsprechende How To finden sich zahlreich im Web und in guter Literatur (siehe etwa [10]). Soll die Certification Authority (CA) – also die Komponente, die die Zertifikate ausstellt – keine Windows-CA sein – und das wird von manchem Unternehmen entweder aus Sicherheitsgründen oder aus Gründen der Verwaltung von Zertifikaten in einer heterogenen Betriebssystemumgebung gefordert – , dann wird die Luft schnell dünn. An dieser Stelle soll das vorliegende How To helfen, das beschreibt, wie Smartcard-basiertes SSO in Windows 2000- und Server 2003-basierten Active Directory-Umgebungen zusammen mit Citrix Presentation Server 4.0 und einer nicht-Windows-CA realisiert werden kann.

Das How To entstand aus einem Projekt für die Deutscher Sparkassen Verlag GmbH (DSV), der als eine seiner Dienstleistungen für die Sparkassen die Implementierung von SSO mit Smartcards und Zertifikaten in unterschiedlichen Umgebungen anbietet. Wir möchten uns an dieser Stelle für die Zusammenarbeit herzlich bedanken.

DSV Gruppe
Deutscher Sparkassenverlag

Das How To ist ein technisches How To, das die Definition von Rollen und Prozessen, die für den Betrieb einer PKI stets notwendig sind, nicht betrachtet.

Haben Sie Fragen zum How To selbst oder Fragen, die weitere technische Details oder Security Management-Prozesse bei der Implementierung von Zertifikaten und PKIs betreffen, wenden Sie sich bitte an die Autoren.

Wir und das Team von ERNW (Deutschland) und ERNW.PT (Portugal) stehen Ihnen jederzeit zur Verfügung.

2 Überblick über die notwendigen Schritte

Die notwendigen Schritte lassen sich überblicksartig zusammenfassen zu:

1. Prüfung der Software-Voraussetzungen auf Servern und Clients, ggf. Installation notwendiger Hotfixes:
    a. Windows Server 2003 SP1 mit aktuellen Patches als DC: keine weitere Aktion nötig
    b. Windows Server 2003 SP1 mit Citrix Presentation Server 4.0: Installation des Hotfix-Rollups PSE400W2K3R01 von Citrix notwendig (vgl. Abschnitt 6.1)
    c. Windows 2000 Server mit SP4 und aktuellen Patches: keine weitere Aktion notwendig
    d. Windows XP Professional mit SP1 oder SP2 aktuellen Patches: Installation des Hotfixes KB 891849 (vgl. Abschnitt 4.3.1) notwendig
    e. Windows 2000 Professional mit SP4 und aktuellen Patches: keine weitere Aktion nötig
2. Ausstattung der Domänencontroller mit Zertifikaten
    a. Beantragung der Zertifikate (vgl. Abschnitt 4.1.6)
    b. Import der Zertifikate (vgl. Abschnitt 4.2.2)
3. Konfiguration von Active Directory (vgl. Abschnitt 4.2.1)
4. Beantragung der Smartcard-Zertifikate für Benutzer mit definierten Spezifikationen (vgl. Abschnitt 4.1.1 und 4.1.2)
5. Installation von CSP und Kartenleser-Treiber auf den Clients (vgl. Abschnitt 4.3)
6. Überprüfung einer erfolgreichen Smartcard-Anmeldung.

3 BESCHREIBUNG DER TESTUMGEBUNGEN

Im Testlab wurden gemäß Zielsetzung zwei Umgebungen aufgebaut: ein Windows Server 2003-basiertes Active Directory und ein Windows 2000 Server basiertes. Die beiden Umgebungen sehen dabei wie folgt aus:

3.1 Windows Server 2003-basiertes Active Directory

Installierte Maschinen und Betriebsysteme
Domain Controller (Enterprise Edition)
Terminal 2003- und Citrix Presentation Server 4.0 (beides Enterprise Edition)
Windows XP Professional
Windows 2000 Professional

Installierte Serverapplikationen
Windows Server 2003 Terminaldienste
Citrix Presentation Server 4.0 Enterprise + Hotfix PSE400W2KR01

Service Pack- und Patchlevelstand
Windows Server 2003: SP 1
Windows 2000 Server: SP 4
Windows XP Professional: SP 2 + Hotfix 891849
Windows 2000 Professional: SP 4
Darüber hinaus befinden sich alle Maschinen auf dem aktuellen Patchlevelstand (Stand: 26. März 2006).

Smartcard-Hardware
Smartcard: S-TRUST Signaturkarte
Kartenleser: Reiner SCT cyber*Jack* pinpad; Firmware-Version: 2.0.5 (siehe Screenshot nächste Seite).

Smartcard-Software
Smartcard-Betriebsystem: Starcos
A. E. T. SafeSign – Standardversion (V. 2.0.2)
Verwaltungssoftware für Reiner SCT cyber*Jack* pinpad (siehe Screenshot nächste Seite).

Bemerkungen

Die Gesamtstruktur besteht aus einer Domäne. Das untersuchte Szenario ist unabhängig von der Gesamtstruktur- und Domänenfunktionsebene. Die Tests fanden sowohl unter der niedrigsten Domänenfunktionsebene als auch unter der höchsten Gesamtstrukturfunktionsebene statt.[1]

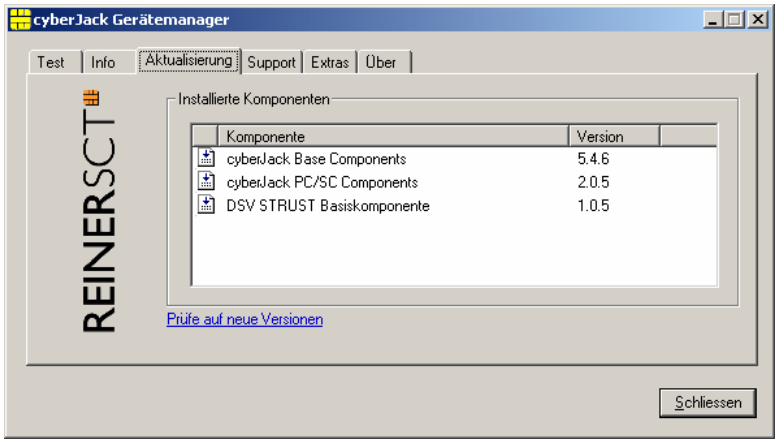
3.2 Windows 2000-basiertes Active Directory

Installierte Maschinen und Betriebsysteme
Domain Controller (Advanced Server)
Windows Server 2003-Member Server für die Zertifikatverwaltung
Windows XP Professional
Windows 2000 Professional

Service Pack- und Patchlevelstand
Windows Server 2003: SP 1
Windows 2000 Server: SP 4
Windows XP Professional: SP 2 + Hotfix 891849
Windows 2000 Professional: SP 4
Darüber hinaus befinden sich alle Maschinen auf dem aktuellen Patchlevelstand (Stand: 26. März 2006).

Smartcard-Hardware
Smartcard-Betriebsystem: Starcos
Smartcard: S-TRUST Signaturkarte
Kartenleser: Reiner SCT cyber*Jack* pinpad; Firmware-Version: 2.0.5 (siehe Screenshot)

Smartcard-Software
A. E. T. SafeSign – Standardversion (V. 2.0.2)
Verwaltungssoftware für Reiner SCT cyber*Jack* pinpad (siehe Screenshot):



[1] *Die Funktionsebene hat eine Auswirkung auf die von der Windows Server 2003-eigenen CA einsetzbaren Zertifikatsvorlagen (spielt also hier keine Rolle).*

Bemerkungen

Die Gesamtstruktur besteht aus einer Domäne. Das untersuchte Szenario ist dabei unabhängig von dem Modus, in dem die Domäne betrieben wird. Beide in einer Windows 2000-basierten Active Directory-Umgebung möglichen Modi wurden getestet.

4 How To für Smartcard-basiertes SSO in einer Windows Server 2003-basierten Active Directory-Umgebung mit 3rd. Party CA-Zertifikaten

Die erfolgreiche Konfiguration von Smartcard-basiertem SSO in einer Windows Server 2003-basierten Active Directory-Umgebung unter der ausschließlichen Verwendung von Zertifikaten, die von einer Nicht-Windows CA ausgestellt werden, impliziert die Durchführung der folgenden Schritte:

1. Erstellung geeigneter Zertifikate durch die Nicht-Windows CA
2. Konfiguration von Active Directory und Domänencontrollern
3. Installation von Kartenleser- und Cryptographic Service Provider (CSP)-Software auf dem Client sowie zusätzliche Clientkonfiguration

4.1 Erstellung geeigneter Zertifikate durch die Nicht-Windows CA

Die notwendigen Zertifikate werden von einer Test-OnSite CA von Verisign ausgestellt und sollen im Produktivbetrieb von der S-TRUST eigenen CA erstellt werden. Die Test-OnSite CA wird unter der folgenden URL erreicht:

https://onsite-test.s-trust.de/services/DSVKSSO/client/userEnrollDC.htm

Smartcard-basierte Authentifizierung in Active Directory wird über eine Erweiterung des Kerberosprotokolls möglich[2]. Dabei authentifiziert sich der Benutzer mit seinem Smartcard-Zertifikat gegenüber dem Domänencontroller, und der Domänencontroller authentifiziert sich gegenüber dem Clientrechner des Benutzers mit seinem Domänencontroller-Zertifikat. Für eine Smartcard-basierte Authentifizierung in Active Directory benötigt also jeder Benutzer ein Smartcard-Zertifikat und jeder Domänencontroller ein Domänencontroller-Zertifikat. Beide Zertifikate haben bestimmten Anforderungen zu genügen:

4.1.1 Anforderungen an das (Benutzer-) Smartcard-Zertifikat

- **Zertifikatsversion:** X.509 V.3
- Der Speicherort des CRL-Verteilungspunktes (CRL Distribution Point, CDP) muss ausgefüllt, online und verfügbar sein. Beispiel:
  [1]CRL-Verteilungspunkt
  Name des Verteilungspunktes:
  Vollständiger Name:
  URL=http://server1.name.com/CertEnroll/caname.crl (Beispiel)
- **Schlüsselverwendung** = Digitale Signatur
- **Basiseinschränkungen** [Typ des Antragstellers=Endeinheit, Einschränkung der Pfadlänge=Keine] (Basiseinschränkungen können optional angegeben werden)
- **Erweiterte Schlüsselverwendung** =
  - Clientauthentifizierung (1.3.6.1.5.5.7.3.2)
    (Die Clientauthentifizierungs-OID wird nur dann benötigt, wenn ein Zertifikat für die SSL-Authentifizierung verwendet wird.)
  - Smartcard-Anmeldung (1.3.6.1.4.1.311.20.2.2)
- **Alternativer Antragstellername** = Anderer Name: Prinzipalname = (UPN). Beispiel:
  Anderer Name:

[2] *Siehe auch Description of PKINIT Version Implemented in Kerberos in Windows 2000* (*http://support.microsoft.com/kb/248753/en-us*)

Prinzipalname=user1@name.com
Die UPN-OtherName-OID lautet: "1.3.6.1.4.1.311.20.2.3"
Der UPN-Wert "Anderer Name" muss eine ASN1-codierte UTF8-Zeichenfolge sein.

- **Antragsteller** = Definierter Benutzername. Dieses Feld ist eine obligatorische Erweiterung, kann jedoch beliebig gefüllt werden.

Bemerkungen

1. Da der authentifizierende Domänencontroller die Identität eines sich authentifizierenden Benutzers aus dem Wert *Anderer Name: Prinzipal Name= (UPN)* der Erweiterung *Alternativer Antragsteller* extrahiert und mit dem im Active Directory für diesen Benutzer definierten Wert vergleicht, müssen der in dem Smartcard-Zertifikat definierte Wert und der in den Eigenschaften des Benutzerkontos definierte Wert im Active Directory sein.[3]
2. Der Speicherort des CRL-Verteilungspunktes (CRL Distribution Point, CDP) muss ausgefüllt, online und verfügbar sein, da er sowohl vom dem sich authentifizierenden Client als auch von dem authentifizierenden Domänencontroller abgefragt wird.

4.1.2 Bereitzustellende Daten für die Beantragung des Smartcard-Zertifikats

- Benutzeranmeldename im UPN-Format[4]

4.1.3 Beispiele

Beispiel für ein richtig definiertes Smartcard-Zertifikat:

-----BEGIN CERTIFICATE-----
MIIEQDCCAyigAwIBAgIQdLCkND6XWfUgpPQhIWGQUDANBgkqhkiG9w0BAQQFADBw
MRYwFAYDVQQKEw1WZXJpU2lnbiBFTUVBMSMwIQYDVQQLExpEZW1vbnN0cmF0aW9u
IFByaXZhdGUgUm9vdDExMC8GA1UEAxMoVmVyaVNpZ24gRU1FQSBEZW1vbnN0cmF0
aW9uIFByaXZhdGUgUm9vdDAeFw0wNjAzMjIwMDAwMDBaFw0wNzAzMjIyMzU5NTla
MFQxDDAKBgNVBAoUA0RTVjENMAsGA1UECxQES1NTTzEXMBUGA1UEAxMORnJpZWR3
YXJ0IEt1aG4xHDAaBgkqhkiG9w0BCQEWDWZrdWhuQGVybncuZGUwgZ8wDQYJKoZI
hvcNAQEBBQADgY0AMIGJAoGBANln46nApEtQkO0UKK/QPO6kgsUK1pAlXOQEt4KZ
OnCk3RarOA22HD/zMgRRecCqT07inBpyAqborXNj2BMQSyPtezcWja8UIFKmz8sn
HLAgzP/ZSTzz3ZMJEfc+KEG4KxEXO9bIoV5OGlhEFt3s48ieNeHY9/8w4C9Fdufv
whD7AgMBAAGjggF0MIIBcDAJBgNVHRMEAjAAMIGTBgNVHSMEgYswgYihdKRyMHAx
FjAUBgNVBAoTDVZlcmlTaWduIEVNRUExIzAhBgNVBAsTGkRlbW9uc3RyYXRpb24g
UHJpdmF0ZSBSb290MTEwLwYDVQQDEyhWZXJpU2lnbiBFTUVBIERlbW9uc3RyYXRp
b24gUHJpdmF0ZSBSb290ghBBFlGhy+GxemgESKFnXDWYMB0GA1UdDgQWBBRm53hs
pVH4cDoSqiAozHokaLm/6TBHBgNVHR8EQDA+MDygOqA4hjZodHRwOi8vb25zaXRl
Y3JsLXRlc3Qucy10cnVzdC5kZS9EU1ZLU1NPL0xhdGVzdENSTC5jcmwwCwYDVR0P
BAQDAgWgMB8GA1UdJQQYMBYGCCsGAQUFBwMCBgorBgEEAYI3FAICMDcGA1UdEQQw
MC6gHQYKKwYBBAGCNxQCA6APDA1ma3VobkBlcm53LmRlgQ1ma3VobkBlcm53LmRl
MA0GCSqGSIb3DQEBBAUAA4IBAQBD9AoM2M/nZP6/THoEndpkC8ZXHtscmNQQ2x63

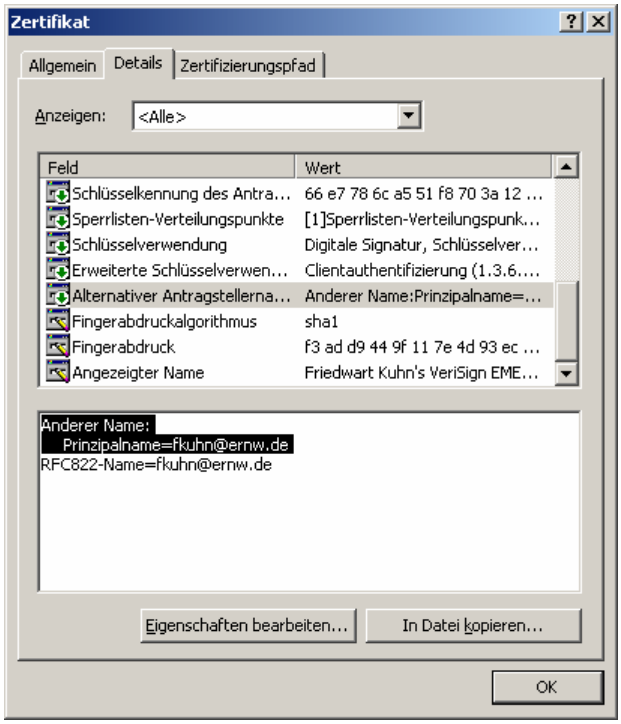
---

[3] *Bei der Verwendung einer Windows CA muss zusätzlich die E-Mail in den Eigenschaften des Benutzerkontos definiert und identisch mit der in dem Smartcard-Zertifikat verwendeten sein. Da hier jedoch keine Windows CA verwendet wird, muss kein Wert für die E-Mailadresse in den Eigenschaften des Active Directory-Benutzerkontos definiert werden.*

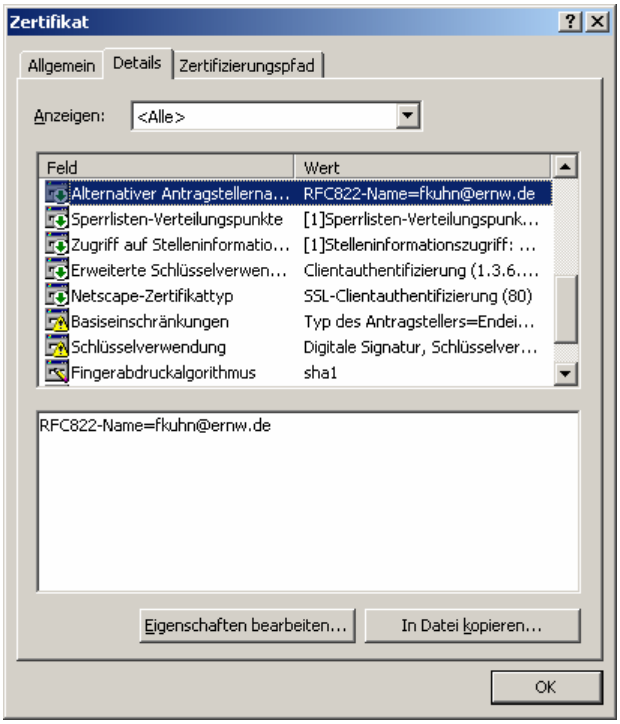
[4] *Hier wird nur die für das Testszenario relevante technische Information aufgeführt. Im Produktivbetrieb beantragen Benutzer über ein Formular nach einem definierten Verfahren eine Smartcard (und mit dieser das darauf befindliche Zertifikat).*

Uhhtur80egfImfGy5CwH5xZTF0EH0la3TVXcHIC/vMOIg9Pj0hSREKcAj410Z7Z8
H1A/aZJC8pUimGcJUZDqab7QHiiGhRS76Fk9yXjICCUw8V93NFzHipj+2F/ELg5D
ryN9nnItHwQzzamUV02ev1e+fjWAgQtvHuTBA/hgBBiq53wZaI4G6in/eXIsGg0K
LMcag5JP8ZwCfmGq+4d7kpbTg8VjGNsF1OXcP6m8ynufgqgyETWGH9Pm2EOptiTc
JythaFOpXgsKuijfGThr8tKRsv8cbEgJvg/3rYV5hLsK18NQ
-----END CERTIFICATE-----

Beispiel für einen richtig definierten Wert Anderer Name: *Prinzipalname = (UPN)* in einem Smartcard-Zertifikate:

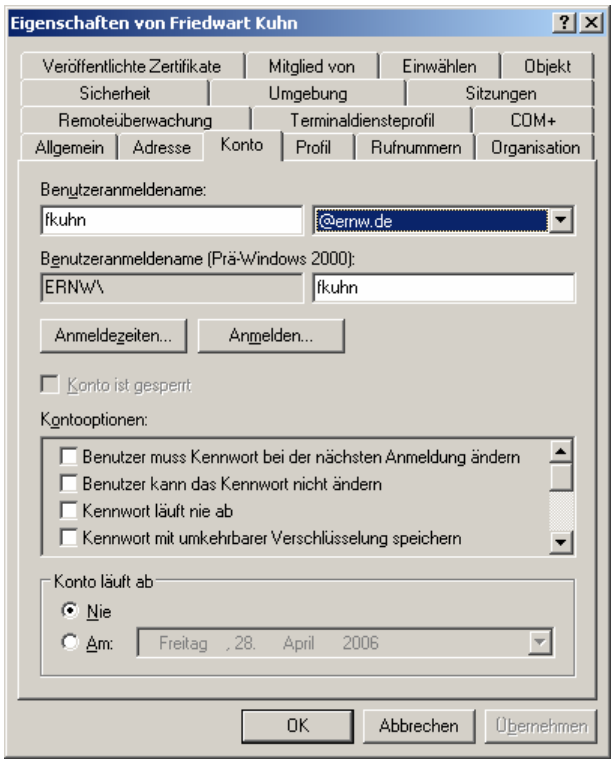


Zum Vergleich ein von der gleichen CA ausgestelltes Zertifikat, jedoch ohne den entscheidenden Wert in *Alternativer Antragsteller*:



Smartcard-Anmeldung funktioniert mit diesem Zertifikat **nicht**.

Der UPN-Wert in den Eigenschaften des Benutzerkontos im Active Directory:



4.1.4 Anforderungen an das Domänencontroller-Zertifikat

Jeder Domänencontroller der Domäne(n), in der (denen) Smartcard-basierte Authentifizierung statt finden soll benötigt ein gültiges und nach den folgenden Vorgaben formatiertes Zertifikat[5]:

- Das Zertifikat muss eine CRL-Erweiterung des CRL-Verteilungspunktes haben, die auf eine gültige Zertifikatsperrliste (CRL) verweist.
- Das Zertifikat sollte unter *Antragsteller* den Verzeichnispfad des Server-Objekts (Definierter Name) enthalten; Beispiel[6]:
  CN=s03dc.ernw.de
  OU=KSSO
  O=DSV
- Der Abschnitt Schlüsselverwendung muss enthalten:
  Digitale Signatur Schlüsselverschlüsselung
- Der Abschnitt Basiseinschränkungen kann optional enthalten:
  [Typ des Antragssteller=Endeinheit]
  [Einschränkung der Pfadlänge=keine]
- Der Abschnitt erweiterte Schlüsselverwendung muss enthalten:
  - Clientauthentifizierung (1.3.6.1.5.5.7.3.2)
  - Server-Authentifizierung (1.3.6.1.5.5.7.3.1)
- Der Alternativer Antragstellername muss die Objekt ID (OID), den Global Eindeutigen Bezeichner (GUID) für den Domänencontroller und dessen DNS-Name enthalten:
  Anderer Name: 1.3.6.1.4.1.311.25.1=06 Aa Ac-4b-d6-4f-a9 5 D 29 9 C 4 C BC D9 65 6a B0 DNS-Name=s03dc.ernw.de
- Die Zertifikatvorlage muss eine Erweiterung mit dem BMP-Datenwert "DomainController" haben.
- Das Domänencontroller-Zertifikat muss in dem (logischen) Zertifikatsspeicher: Computer Zertifikate – Eigene Zertifikate gespeichert sein.

Bemerkungen:

1. Mit dem letzten Punkt ist gemeint: Der Abschnitt *Zertifikatsvorlagenname* in dem Domänencontroller-Zertifikat muss den Wert *DomainController* aufweisen.

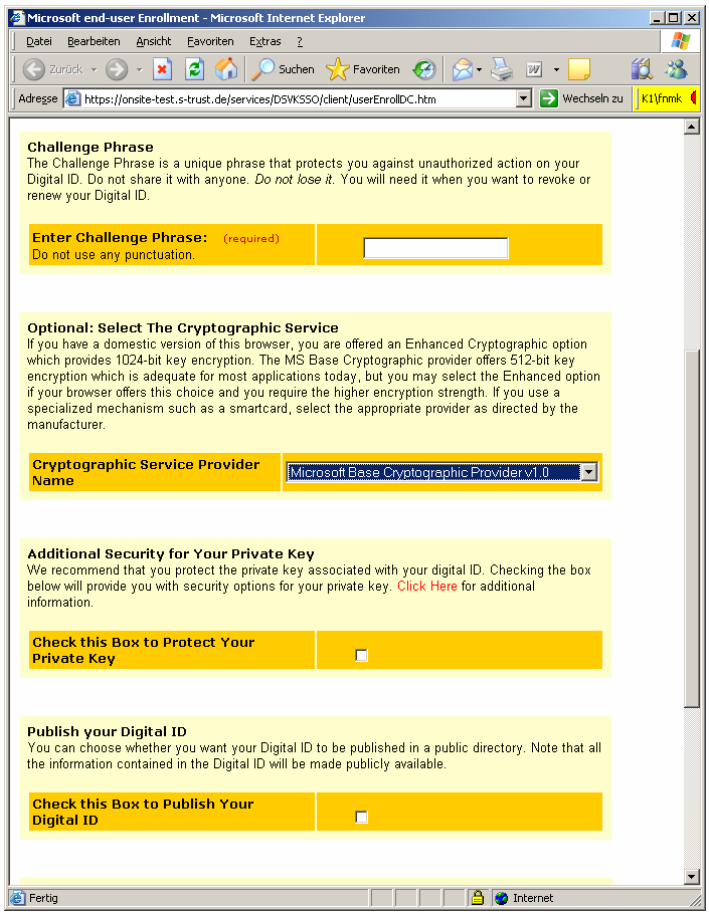
2. Microsoft weist in [3] darauf hin, dass der Secure Channel CSP für die Generierung des Schlüsselpaares für das Domänencontrollerzertifikat verwendet werden muss. Bei dem

---

[5] Vgl. auch [3]. Achtung: Da der Domänencontroller-Name Bestandteil des Domänencontroller-Zertifikats ist, dürfen Domänencontroller unter Windows Server 2003 nach dem Erhalt des Zertifikats, nur dann umbenannt werden, wenn sei ein neues Zertifikat erhalten. Das Zertifikat auf den alten Domänencontroller-Namen sollte dann widerrufen und aus dem Zertifikatsspeicher des Domänencontrollers gelöscht werden. Domänencontroller unter Windows 2000 Server sind davon nicht betroffen, weil sie nicht umbenannt werden können.

[6] Zum Vergleich: Wenn es sich um eine Windows CA handelt, dann gibt es nur die von Microsoft verwendeten LDAP-Namenskomponenten, nämlich CN, OU und DC. Dass in dem vorliegenden Szenario wegen der Nicht-Windows CA andere LDAP-konforme Namenskomponenten verwendet werden, tut der Interoperabilität von Active Directory mit einer Nicht-Windows CA keinen Abbruch.

vorliegenden Szenario stand dieser CSP auf der Seite der Test-OnSite CA nicht zur Auswahl bereit. Stattdessen wurde der Microsoft Base Cryptographic Provider v1.0 verwendet[7]:



4.1.5 Bereitzustellende Daten für die Beantragung des Domänencontroller-Zertifikats

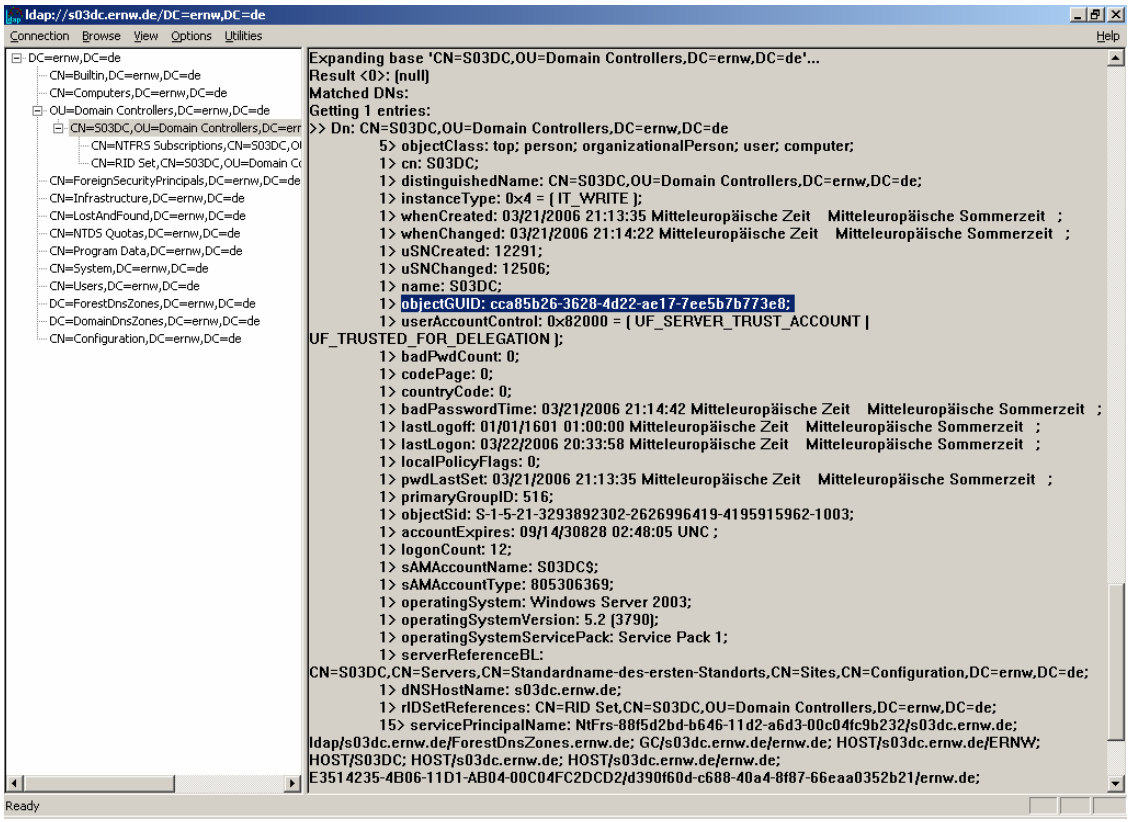
- Bereitstellung des DNS-Namens des Domänencontrollers
- Bereitstellung GUID des Domänencontrollers im Active Directory
- Bereitstellung der Information, welcher CSP für die Erzeugung des Schlüsselmaterials für das Domänencontroller-Zertifikat verwendet wird

Bestimmung der GUID des Domänencontrollers im Active Directory:

[7] *Die Unterschiede zwischen dem Microsoft Base Cryptographic Provider v1.0 und dem Microsoft Secure Channel CSP sind allerdings auch recht gering. Es ist wahrscheinlich, dass auch der Microsoft Enhanced Cryptographic Provider 1.0 sowie der Microsoft Strong Cryptographic Provider der Test-OnSite CA verwendet werden können, da sich diese CSPs im Vergleich zum Microsoft Base Cryptographic Provider v1.0 im Wesentlichen durch die verschiedenen Schlüssellängen unterscheiden. Vor der Produktivverwendung sollte jedoch ein Test erfolgen. Weitere Details hierzu entnimmt man [1].*

1. Aufruf von Ldp.exe (erst möglich nach der Installation der Support Tools auf der Installations-CD unter \i386\support\tools)
2. Klicken Sie im Menü **Connection** auf **Connect**.
3. Geben Sie in der Organisation den Servernamen eines Domänencontrollers ein, überprüfen Sie, ob **port** auf 389 eingestellt wurde, deaktivieren Sie das Kontrollkästchen **Connectionless** und klicken Sie anschließend auf **OK**. Sobald die Verbindung abgeschlossen wurde, werden die serverspezifischen Daten im rechten Fenster angezeigt.
4. Klicken Sie im Menü **Connection** auf **Bind**. Geben Sie den Benutzernamen, das Kennwort und den Domänennamen (im DNS-Format) in die jeweiligen Felder ein (möglicherweise müssen Sie das Kontrollkästchen **Domain** aktivieren), und klicken Sie anschließend auf **OK**. Wenn die Bindung erfolgreich war, wird im rechten Fenster eine Meldung angezeigt, die der folgenden ähnelt: "Authenticated as dn:'YourUserID'".
5. Gehen Sie im Menü "View" auf "Tree" und geben Sie in der Dialogbox "Tree view" unter "BaseDN" den Domänennamen-Kontext ein (Der **Base DN** ist der Ausgangspunkt in der Hierarchie des Active Directory, an dem Ihre Suche beginnt.):

6. Navigieren Sie zum CN des Domänencontrollers und klicken diesen doppelt. Dann finden Sie im rechten Fenster unter dem CN eine Reihe von Attributen aufgelistet, unter anderem die "objectGUID", das ist die GUID des Domänencontrollers:



4.1.6 Schritte für die Beantragung des Domänencontroller-Zertifikats

1. Man gehe auf die Site der ausstellenden CA (im Testszenario war diese unter der folgenden URL erreichbar:
   https://onsite-test.s-trust.de/services/DSVKSSO/client/userEnrollDC.htm
2. Dort werden die in 4.1.5 aufgeführten Daten über den Browser eingegeben.
3. Die Freigabe zur Ausstellung des Zertifikats erfolgt über den entsprechenden Verantwortlichen (in diesem Fall Herr Joachim Buck).
4. Eine E-Mail benachrichtigt die Person, die den Antrag für das Zertifikat des Domänencontrollers gestellt hat, und stellt eine PIN zur Verfügung, die zur Abholung des Zertifikats berechtigt. Die Abholung erfolgt im Testszenario auf der URL:
   https://onsite-test.s-trust.de/services/DSVKSSO/digitalidCenter.htm

Das Zertifikat muss dann noch in den lokalen Speicher des Computers importiert werden (siehe Abschnitt 4.2.2).

4.1.7 Beispiel

Beispiel für ein den Anforderungen entsprechend ausgefülltes Domänencontroller-Zertifikat:

-----BEGIN CERTIFICATE-----
MIIDnjCCAoagAwIBAgIQOE/8raQKsAcUFHUPQw7v3zANBgkqhkiG9w0BAQQFADBw
MRYwFAYDVQQKEw1WZXJpU2lnbiBFTUVBMSMwIQYDVQQLExpEZW1vbnN0cmF0aW9u
IFByaXZhdGUgUm9vdDExMC8GA1UEAxMoVmVyaVNpZ24gRU1FQSBEZW1vbnN0cmF0

aW9uIFByaXZhdGUgUm9vdDAeFw0wNjAzMjMwMDAwMDBaFw0wNzAzMjMyMzU5NTla
MDUxDDAKBgNVBAoMA0RTVjENMAsGA1UECwwES1NTTzEWMBQGA1UEAwwNczAzZGMu
ZXJudy5kZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAzlEjHtliX8ckDDSm
4n0vnng8v08HIq7MI1pKngaryu0J9meWSAm5Nq4oSIMEkikgBGDHh4QVvkIyotQb
QhBqPVqerxCjVKmNufZ/444myffS/5Yf19IAZuzZFl+YVTo3ZfIc5XLVa6cwzUpv
LfnzkjQhLDsWjKnaZkVDJzXZyCsCAwEAAaOB8jCB7zA5BgNVHREEMjAwoB8GCSsG
AQQBgjcZAaASBBDMqFsmNihNIq4XfuW3t3Pogg1zMDNkYy5lcm53LmRlMAkGA1Ud
EwQCMAAwRwYDVR0fBEAwPjA8oDqgOIY2aHR0cDovL29uc2l0ZWNybC10ZXN0LnMt
dHJ1c3QuZGUvRFNWS1NTTy9MYXRlc3RDUkwuY3JsMA4GA1UdDwEB/wQEAwIFoDAd
BgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwLwYJKwYBBAGCNxQCBCIeIABE
AG8AbQBhAGkAbgBDAG8AbgB0AHIAbwBsAGwAZQByMA0GCSqGSIb3DQEBBAUAA4IB
AQAk/HLnUadl0stshxsuEfXi8yNnbKvIKn0kGSozw2Mk8rWCsDJZ02sB6cGNXwrU
JKWbtlZJ8Od58+F6cBZ3Px5vkAlMEnhDS7xZqxJphAfpY0i6EyyQGqw6LyrWtXRH
k7yZl4hVMSpemu9VzQIlyvmKcGHYG56CiA91SpRAHtqZ/LerYRQlIIjcqxev2SR1
RtaRdER0MzSpc9RdZTyC5Pw8y1G7UAza6y6Udf31Ejemlt3Wck4HmbhwVrIuGAal
3fWPFffrBNXZqvohY7XQDxLt8lkYDADVb8oh8lGgxeWO3NmXldLmC+HLrX4T7NyD
d2scnyuMIZsg+FQvBx7+odJ6
-----END CERTIFICATE-----

4.2 Konfiguration von Active Directory und Domänencontrollern

4.2.1 Konfiguration von Active Directory

Die Konfiguration von Active Directory beinhaltet zwei Schritte:

1. Die Bekanntmachung der Nicht-Windows CA gegenüber Active Directory
2. Import des CA-Zertifikats in den Speicher für vertrauenswürdige Stammzertifizierungsstellen auf Windows 2000- und Windows XP-Clients über ein Gruppenrichtlinienobjekt

1 Bekanntmachung der Nicht-Windows CA gegenüber Active Directory

Active Directory erkennt erst dann eine Nicht-Windows CA als CA an, wenn das Zertifikat dieser CA zum Speicher *NT-Authoriät* (*NTAuth*) hinzugefügt wird. Im Active Directory wird das Zertifikat der CA zu folgendem Objekt hinzugefügt:

```
CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=ernw,DC=de
```

In der Registrierung wird dann der Fingerabdruck der Zertifikats gespeichert und auf alle Domänencontroller repliziert. Gespeichert wird der Fingerabdruck unter:

```
HKLM\Software\Microsoft\EnterpriseCertificates\NTAuth\Certificates
```

Zum Hinzufügen des CA-Zertifikats in den Speicher *NT-Authoriät* ist der Befehl *certutil.exe* geeignet. Certutil steht auf jedem Windows Server 2003-Rechner zur Verfügung und ist in dessen adminpak.msi[8] enthalten und lässt sich damit auch auf Windows XP Professional installieren. Das CA-Zertifikat wird über den Befehl zu NTAuth hinzugefügt:

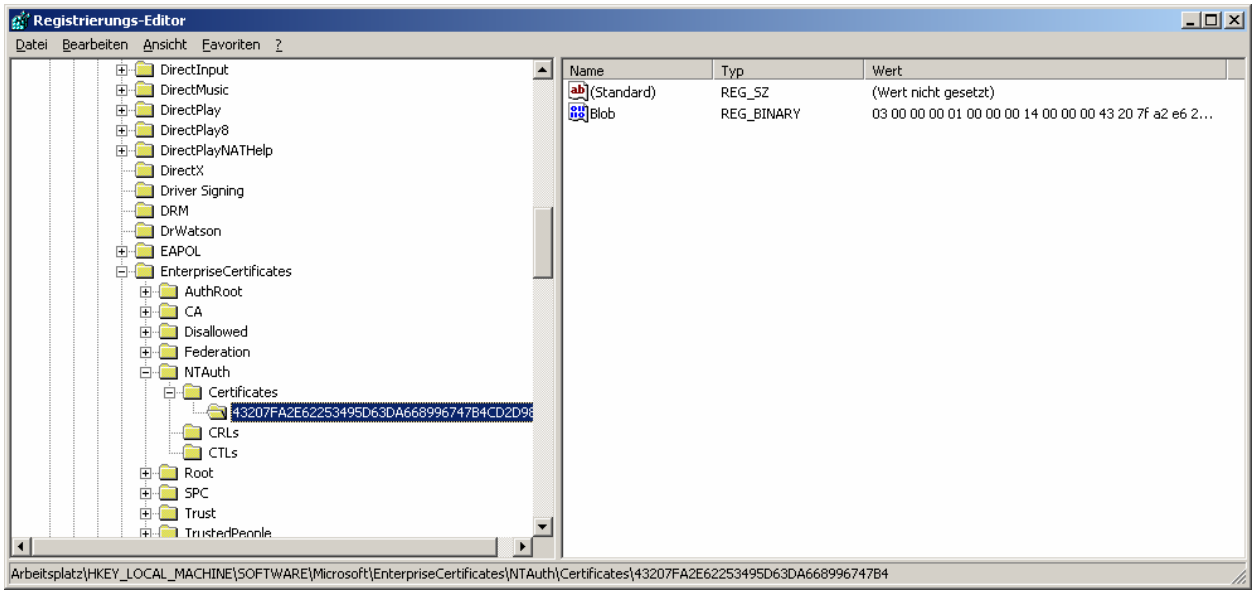
```
certutil -dspublish -f [Dateiname_des_Zertifikats_der_CA] NTAuthCA
```

Die Ausgabe nach Ausführen des Befehls sieht wie folgt aus:

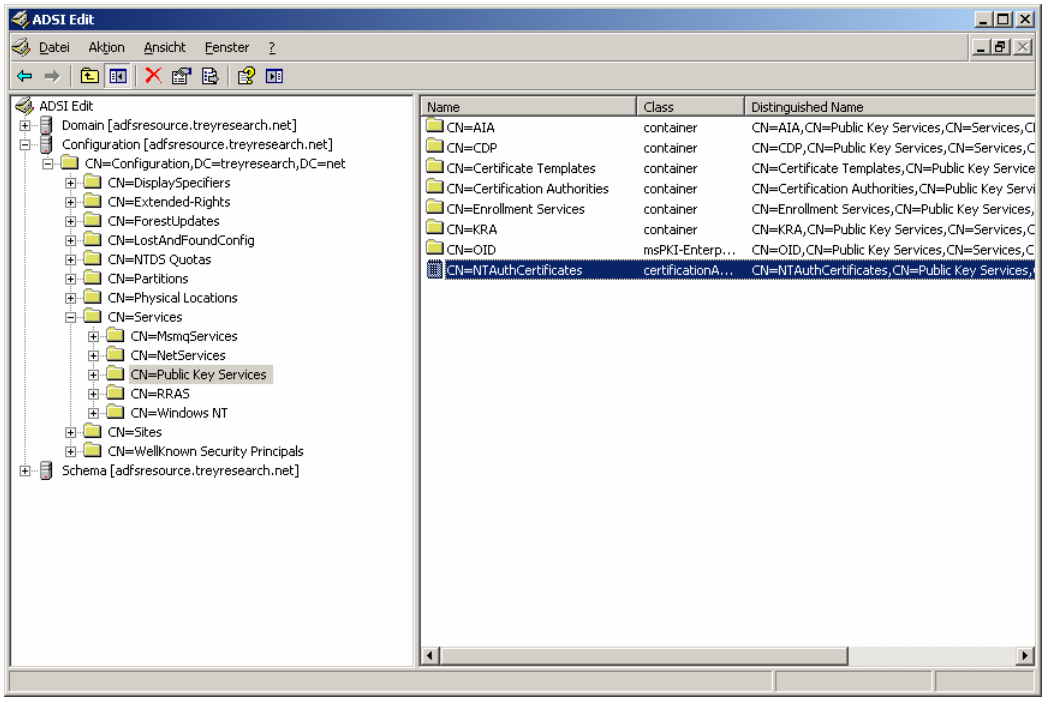
[8] *Auf der Installations-CD unter \I386.*

```
ldap:///CN=NTAuthCertificates,CN=Public
Key  Services,CN=Services,CN=Configuration,DC=ernw,DC=de?cACertificate
Zertifikat wurde zum Verzeichnisdienstspeicher hinzugefügt.
CertUtil: -dsPublish-Befehl wurde erfolgreich ausgeführt.
```

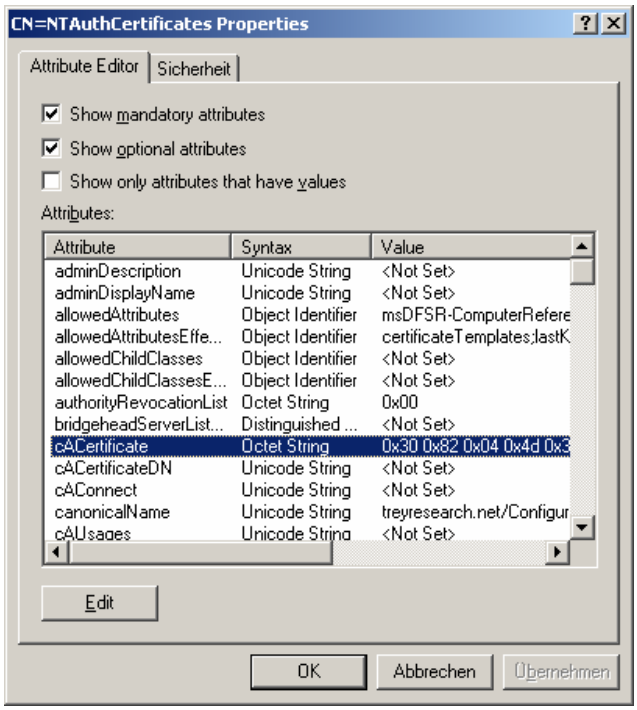
Danach ist ein Neustart des Domänencontrollers erforderlich. Nach dem Neustart findet sich der Fingerabdruck des Zertifikats in der Registrierung des Domänencontrollers:



Im Active Directory findet sich unter:



…der Wert als Attribut zu *NTAuthCertificates* mit dem Namen *CaCertificate*:



Alternativ zum beschriebenen Verfahren lässt sich ein CA-Zertifikat auch über das Snap-In *pkiview.msc* zum Speicher NTAuth hinzufügen.[9]

2. Import des CA-Zertifikats in den Speicher für vertrauenswürdige Stammzertifizierungsstellen auf Windows 2000- und Windows XP-Clients über ein Gruppenrichtlinienobjekt (GPO)

Wenn Domänenmitglieder das Zertifikat der CA über ein GPO erhalten sollen, kann ein solches für die entsprechende OU, für eine Site oder für die ganze Domäne konfiguriert werden:

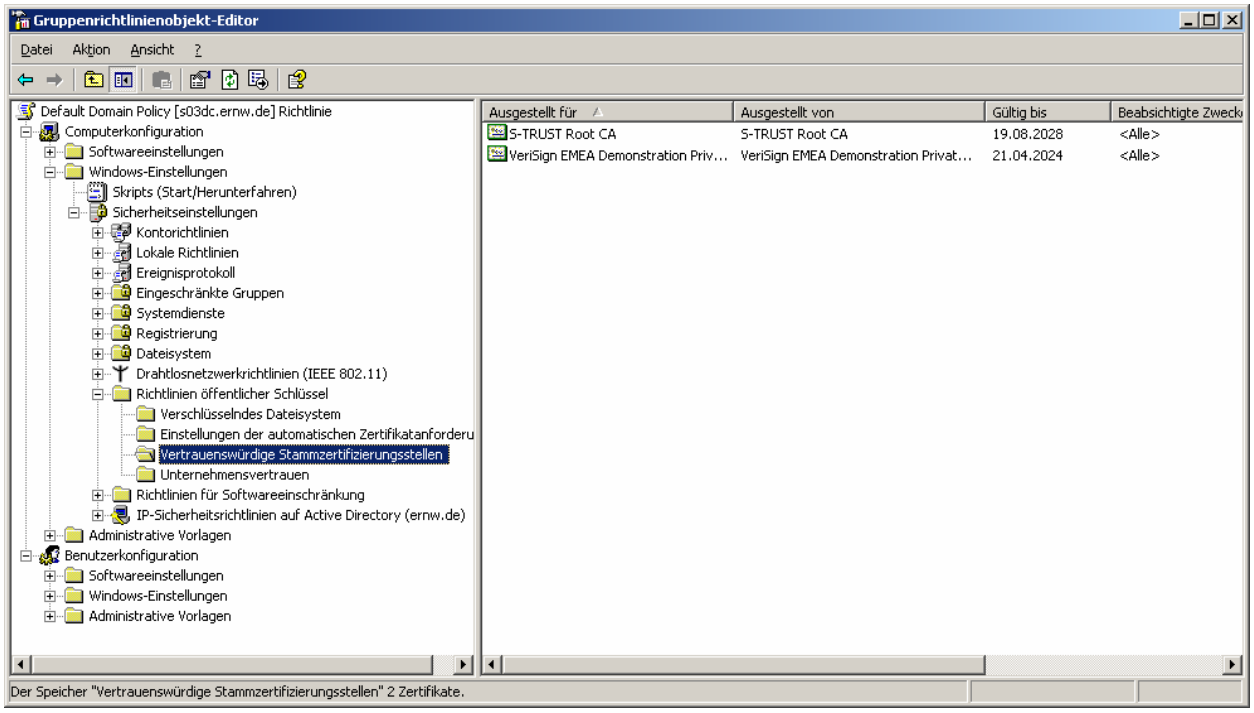
a. Klicken Sie auf **Start**, zeigen Sie auf **Programme** und anschließend auf **Verwaltung**, klicken Sie dann auf **Active Directory-Benutzer und -Computer**.
b. Suchen Sie im linken Fensterbereich die Domäne, in der die Gruppenrichtlinie angewendet wird, die Sie bearbeiten möchten.
c. Klicken Sie mit der rechten Maustaste auf die Domäne. Klicken Sie danach mit der linken Maustaste auf **Eigenschaften**.
d. Klicken Sie auf die Registerkarte **Gruppenrichtlinie**.
e. Klicken Sie auf das Gruppenrichtlinienobjekt "Default Domain Policy", und klicken Sie anschließend auf **Bearbeiten**. Ein neues Fenster wird geöffnet.
f. Erweitern Sie im linken Fensterbereich die folgenden Elemente:
   - Computerkonfiguration

[9] *Pkiview.msc ist Teil der Windows Server 2003-Resource Kit-Tools. Es funktioniert beim ersten Import eines Nicht-Windows CA-Zertifikats nicht, sondern erst nachdem bereits ein Zertifizierungsstellen-Zertifikat in NTAuth (etwa über certutil) importiert wurde. Siehe auch [4].*

- Windows-Einstellungen
- Sicherheitseinstellungen
- Richtlinien öffentlicher Schlüssel

g. Klicken Sie mit der rechten Maustaste auf die Registerkarte **Vertrauenswürdige Stammzertifizierungsstellen**.
h. Markieren Sie **Alle Tasks**, und klicken Sie anschließend auf **Importieren**.
i. Folgen Sie den Anweisungen des Assistenten, um das Zertifikat zu importieren.
j. Klicken Sie auf **OK**.
k. Schließen Sie das Fenster **Gruppenrichtlinie**.

Das fertig konfigurierte GPO sieht wie folgt aus:



Anschließend sorgt das GPO dafür, dass die dort importierten Zertifikate an alle Windows 2000- und Windows XP-Clients verteilt werden, für die dieses GPO gilt. Alternativ kann das Zertifikat auch manuell auf jedem Client installiert werden.

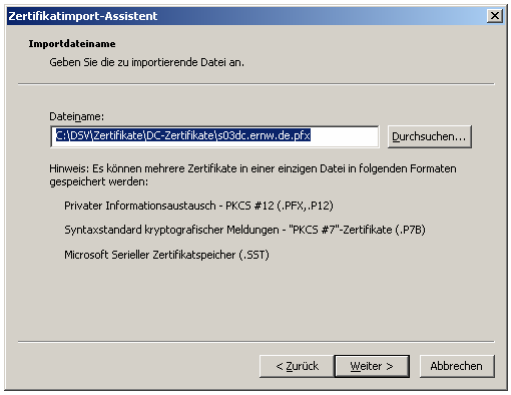
4.2.2 Konfiguration von Domänencontrollern

Achtung: Da der Domänencontroller-Name Bestandteil des Domänencontroller-Zertifikats ist, dürfen Domänencontroller unter Windows Server 2003 nach dem Erhalt des Zertifikats, nur dann umbenannt werden, wenn sei ein neues Zertifikat erhalten. Das Zertifikat auf den alten Domänencontroller-Namen sollte dann widerrufen und aus dem Zertifikatsspeicher des Domänencontrollers gelöscht werden. Domänencontroller unter Windows 2000 Server sind davon nicht betroffen, weil sie nicht umbenannt werden können.

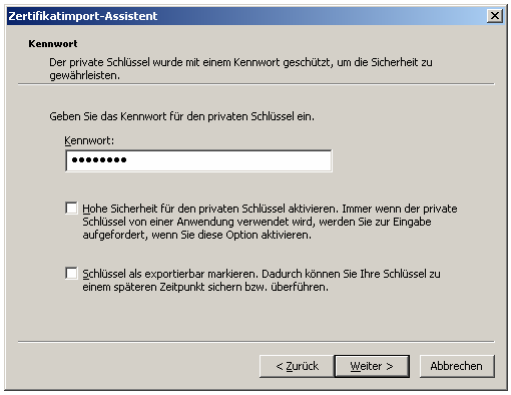
Die Konfiguration der Domänencontroller beinhaltet lediglich das Importieren des von der CA ausgestellten Domänencontroller-Zertifikats in den lokalen Speicher Zertifikatsspeicher des Domänencontrollers.

Dies geschieht durch einen Doppelklick auf die .pfx-Datei, die das Domänencontrolller-Zertifikat mit dem dazugehörigen Schlüsselpaar enthält. Dadurch wird der Zertifikatsimport-Assistent aufgerufen:

Ein Klick auf Weiter führt zur Auswahl der zu importierenden .pfx-Datei:

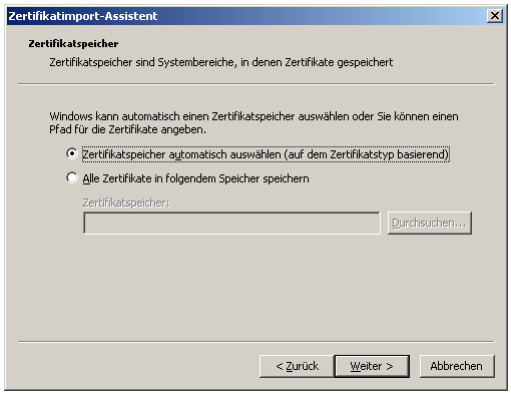


Ein Klick auf Weiter ermöglicht Konfigurationen zur Sicherheit des privaten Schlüssels[10]:

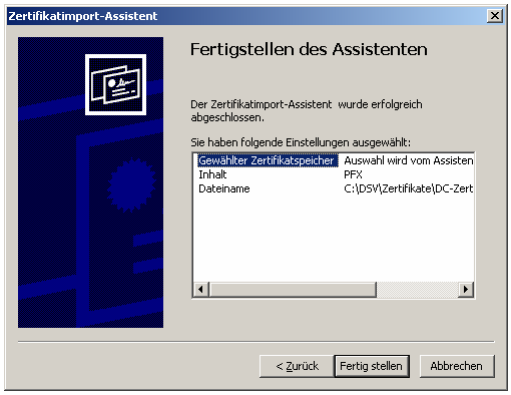


[10] *Die erste Option soll auf jeden Fall deaktiviert sein, da sonst bei jeder Verwendung des privaten Schlüssels eine Passworteingabe zu erfolgen hätte. Die zweite Option kann aktiviert werden, wenn die Möglichkeit einer Schlüsselwiederherstellung implementiert werden soll.*

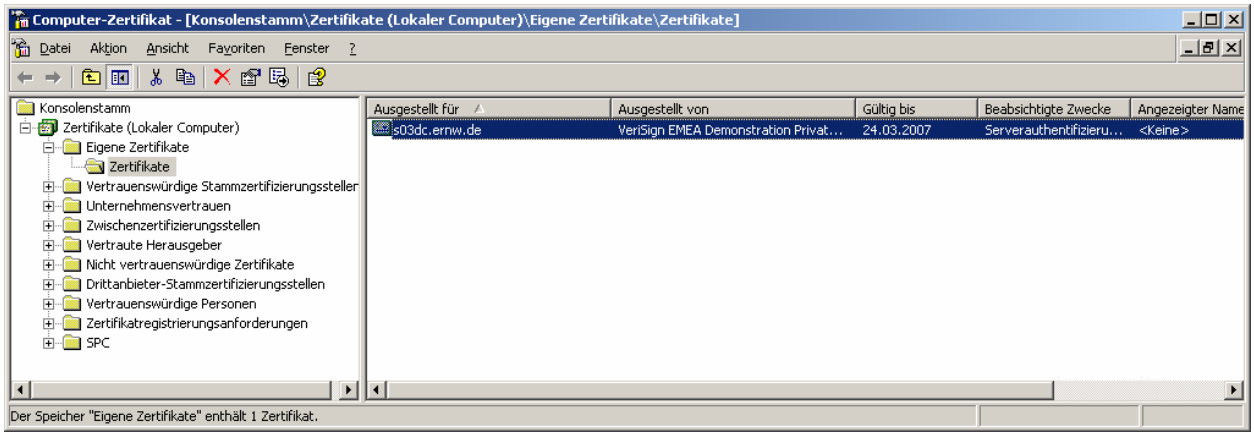
Ein anschließender Klick auf Weiter schlägt eine manuelle oder automatische Wahl des Zertifikatspeichers vor[11]:



Ein Klick auf Weiter liefert eine abschließende Zusammenfassung:



Ein Klick auf Fertig stellen importiert das Zertifikat schließlich. Der ordnungsgemäße Import wird am besten durch Aufrufen des Snap-Ins Zertifikate mit dem Fokus auf das lokale Computerkonto überprüft:



[11] *Der Zertifikatsassistent erkennt, dass es sich um ein Computer-Zertifikat handelt, so dass die vorgeschlagene Einstellung beibehalten werden kann.*

4.3 Installation und Konfiguration der Clients

4.3.1 Windows XP Professional-Clients

Installation und Konfiguration der Windows XP Professional Clients erfolgt in zwei Schritten:

1.Installation von SafeSign und des Kartenlesertreibers sowie zugehöriger Verwaltungs- und Informationssoftware von der S-TRUST CD (siehe die ausgewählten Komponenten:

2.Installation des für Windows XP Professional mit SP 1 oder SP 2 erforderlichen Hotfixes zu KB 891849. Dieser ist noch nicht frei erhältlich, sondern kann von Microsoft-Kunden oder –Partnern über den Telefonsupport erworben werden. Der Hotfix befindet sich in deutscher und in englischer Version auf der zusammen mit dem Dokument übergebenen CD.

4.3.2 Installation der Windows 2000-Clients

Wie Windows XP Professional, jedoch ohne den Hotfix.

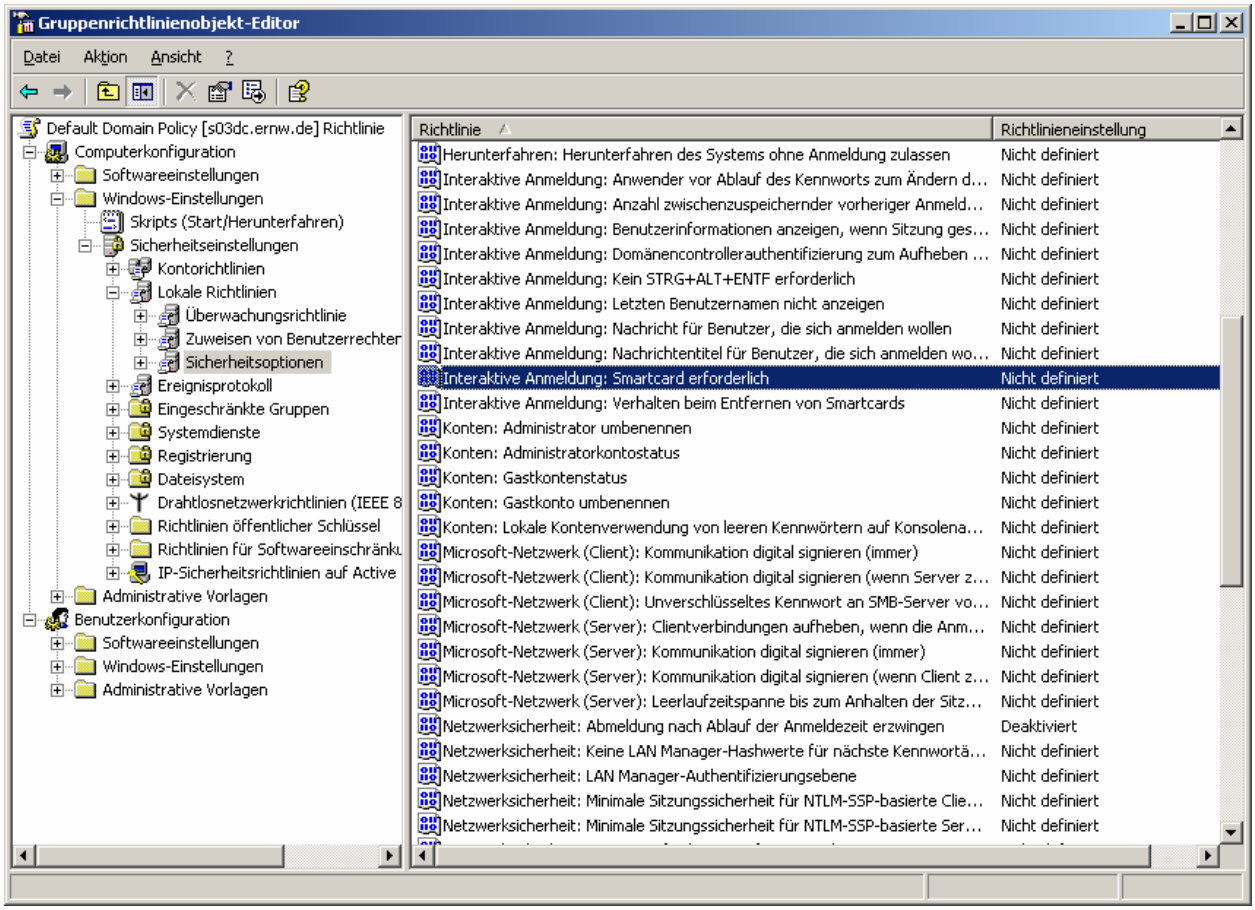
4.4 Weitere Konfigurationsmöglichkeiten im Zusammenhang mit Smartcards

Bei der Verwendung eines Smartcard-Logons gibt es noch zwei wichtige Konfigurationsmöglichkeiten, die beide in einem Gruppenrichtlinien-Objekt vorgenommen werden

4.4.1 Smartcard-Pflicht bei der interaktiven Anmeldung

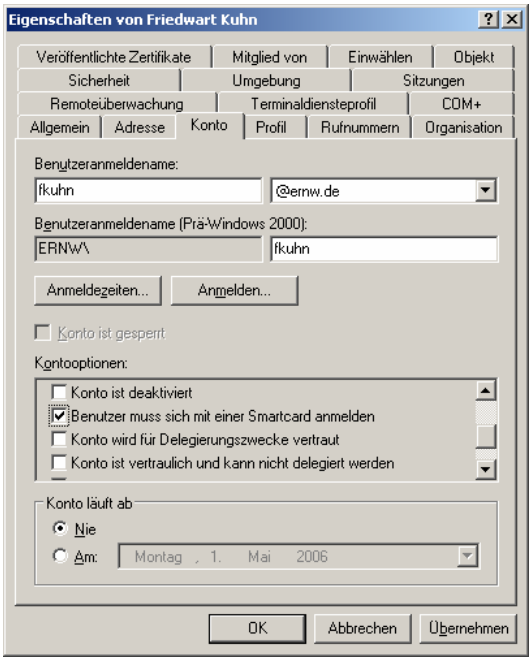
Die Verwendung der Smartcard bei der Anmeldung kann auf zweierlei Art und Weise in einer Gruppenrichtlinie vorgeschrieben werden:

Auf Computerbasis kann die Einstellung *Interaktive Anmeldung: Smartcard erforderlich* festgesetzt werden:



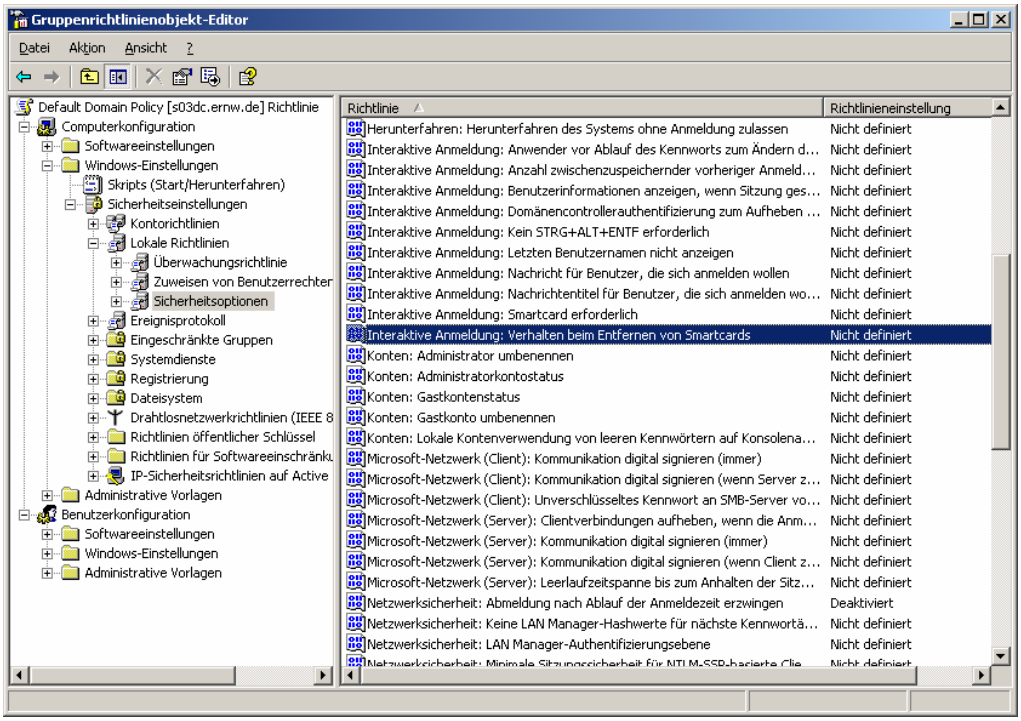
Diese Einstellung findet sich unter: *Computerkonfiguration|Windows-Einstellungen|Sicherheits-einstellungen|Lokale Richtlinien|Sicherheitsoptionen*.

Auf Benutzerbasis kann in den Eigenschaften eines Benutzerkontos im Active Directory die Smartcard-Anmeldung verlangt werden (auf Benutzerbasis ist man flexibler als auf Computerbasis):

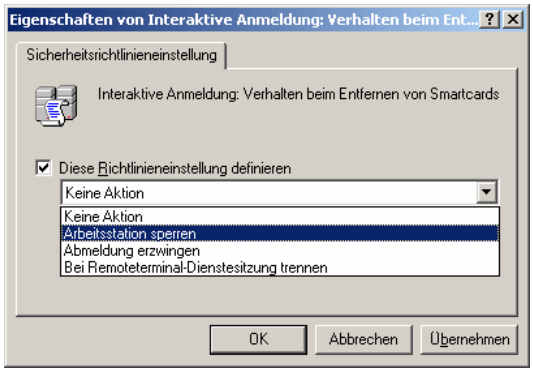


4.4.2 Verhalten bei Entfernen der Smartcard aus dem Smartcard-Leser

Zusätzlich kann das Verhalten des Computers bei Entfernen der Smartcard aus dem Reader ebenfalls über ein Gruppenrichtlinien-Objekt gesteuert werden. Unter: *Computerkonfiguration|Windows-Einstellungen|Sicherheitseinstellungen|Lokale Richtlinien|Sicherheitsoptionen* gibt es die Richtlinie *Interaktive Anmeldung: Verhalten bei Entfernen von Smartcards*:



Hier können die folgenden Aktionen definiert werden:



4.5 Ergebnis

4.5.1 Gewöhnlicher Smartcard-Logon (Domänencontroller online)

Das Ergebnis ist ein funktionierender Smartcard-Logon an der Windows Server 2003-basierten Domäne, und zwar sowohl von Windows XP- als auch Windows 2000 Professional-Clients.

Wenn der Domänencontroller online, d. h. vom Client erreichbar ist müssen zwei zusätzliche Bedingungen erfüllt sein:

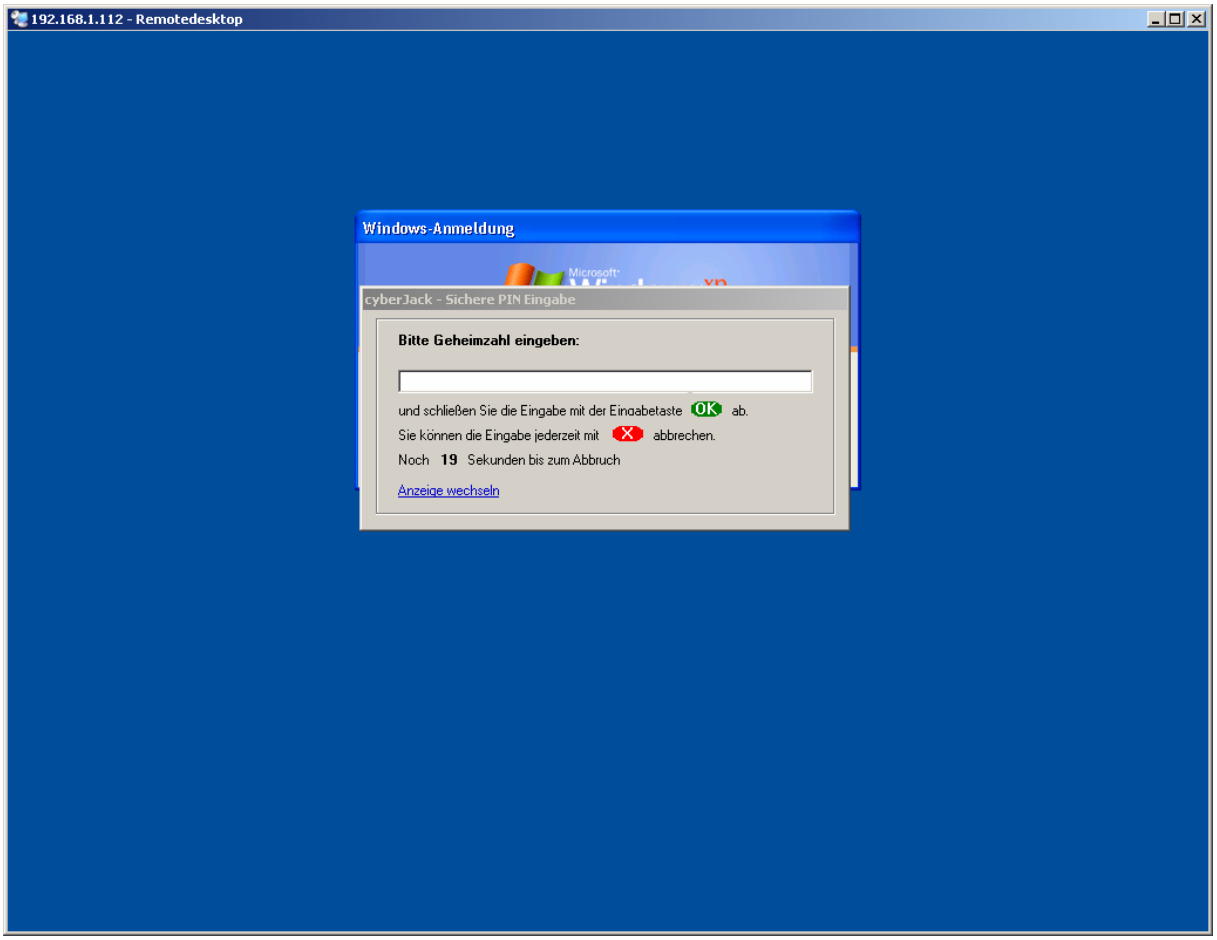
1.Der Domänencontroller muss eine Verbindung zur im CA-Zertifikat angegebenen URL des CDP (CRL-Verteilungspunkt) herstellen können

2.Der Client muss eine Verbindung zur im Smartcard-Zertifikat angegebenen URL des CDP (CRL-Verteilungspunkt) herstellen können

Sind diese Bedingungen erfüllt, so ist ein Smartcard-Logon möglich.

Der Screenshot auf der nächsten Seite zeigt das Smartcard-basierte Logon (hier sogar noch von einem Windows XP-Client aus über den Remotedesktop ausgeführt[12]):

[12] *Damit wird noch eine weitere Möglichkeit des Smartcard-Logons gezeigt, die nicht unmittelbar etwas mit der Aufgabenstellung zu tun hat: Smartcard-basiertes Logon ist über RDP möglich. Voraussetzung dafür ist die Verwendung der in Windows XP SP2 und Server 2003 SP1 basierten RDP-Version (Version 5.2). Wichtigstes Einsatzszenario des Smartcard-Logon via Remotedesktop ist die sichere Administration von Active Directory oder Windows Server 2003-Servern. Ein ansonsten – wenigsten theoretisch möglicher Angriff auf das RDP-Protokoll – wird damit ausgeschlossen.*



4.5.2 Offline-Szenario (Domänencontroller offline)

Da die Credentials sowohl von Windows 2000 als auch von Windows XP Professional zwischengespeichert werden, ist ein Smartcard-basierter Logon von beiden Betriebsystem aus an Active Directory auch dann möglich, wenn (gerade) kein Domänencontroller zur Verfügung steht. Der einzige Effekt ist eine etwas langsamere Anmeldung.[13]

[13] *Windows XP Professional und Windows 2000 speichern per Default die Credentials von 10 Benutzeranmeldungen zwischen. Danach ist kein Logon ohne Domänencontroller mehr möglich.*

5 How To für Smartcard-basiertes SSO in einer Windows 2000 Server-basierten Active Directory-Umgebung mit 3rd. Party CA-Zertifikaten – Abweichung gegenüber einer Server 2003-basierten Active Directory-Umgebung

Mit einer Abweichung sind die Schritte für eine Windows 2000-basierte Active Directory-Umgebung identisch zu denen in einer Server 2003-basierten Active Directory-Umgebung. Die Abweichung liegt hier in der fehlenden Option *–dspublish* des Befehls *certutil* unter Windows 2000 begründet.

Erläuterung: Grundsätzlich gibt es zwei Möglichkeiten, Active Directory eine nicht-Windows CA bekanntzumachen: Eine ist die Verwendung des Snap-Ins *pkiview.msc* (das Bestandteil der Support-Tools ist), die zweite Möglichkeit besteht in der Verwendung des Befehls *certutil* –mit dem Parameter *–dspublish*. Allerdings gibt es bei Windows 2000 Server, bzw. bei Windows 2000-basiertem Active Directory ein Problem: Auch in Windows 2000 Server steht der Befehl certutil.exe zur Verfügung, allerdings ohne die Option *–dspublish*. P*kiview.msc* lässt sich unter Windows 2000-Server genau dann nicht verwenden, wenn die erste CA, die zu *NTAuth* hinzugefügt werden soll, eine nicht-Windows CA ist. Also müssen in Windows 2000-basiertem Active Directory auf einem Windows XP-Mitgliedsrechner entweder die Windows Server 2003-Administrations Tools (adminpak.msi) installiert werden, oder ein Windows Server 2003 muss Mitglied der Domäne sein, da er von sich aus den Befehl *certutil –dspublish* mitbringt. In dem vorliegenden Szenario wurde letztere Option realisiert. Auf diesem Mitgliedsserver wurde der Befehl *certutil –dspublish* ausgeführt und das CA-Zertifikat wie in Abschnitt 4.2.1 beschrieben zu *NTAuth* auf dem Windows 2000-Domänencontroller hinzugefügt. In dem vorliegenden Szenario, ist die einzige Funktion des Server 2003-basierten Member-Servers also das Ausführen des Befehls *certutil -dspublish*.

6 How To für Smartcard-basiertes Logon in einer Server 2003-basierten Active Directory-Umgebung gegen Citrix Presentation Server 4.0

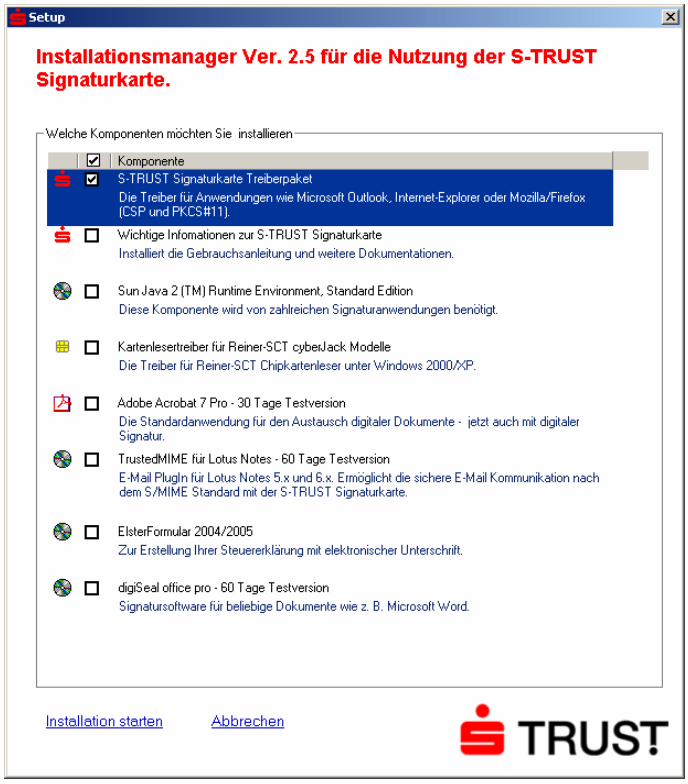
Die Testumgebung ist die gleiche wie die in Abschnitt 3.1 beschriebene. Die notwendige 'Vorarbeit' für ein Smartcard-Logon gegen Presentation Server 4.0 ist in Abschnitt 4 beschrieben.

6.1 Konfigurationsschritte

Für ein erfolgreiches Smartcard-Logon von Windows 2000- und Windows XP Professional-Clients an Citrix Presentation Server 4.0 sind folgende gegenüber Abschnitt 4 zusätzliche Schritte durchzuführen:

1. Installation des Hotfix-Rollups PSE400W2K3R01 von Citrix auf dem Presentation Server 4.0. Eine Fehlerbeschreibung und ein Link zum Download des Hotfix-Rollups sind unter folgender URL erhältlich:
http://support.citrix.com/article/CTX106053&searchID=17482155
Voraussetzung für die Installation des Hotfix-Rollups ist Windows Server 2003.

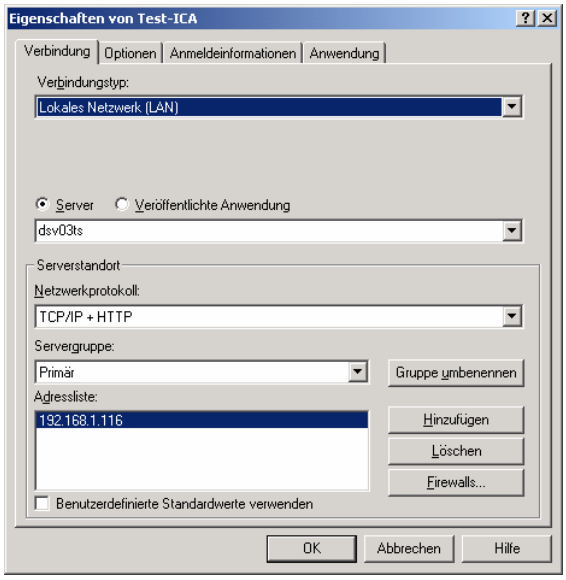
2. Installation des Cryptographic Service Provider (CSP) in Form von SafeSign von der S-TRUST CD auf dem Presentation Server[14]:



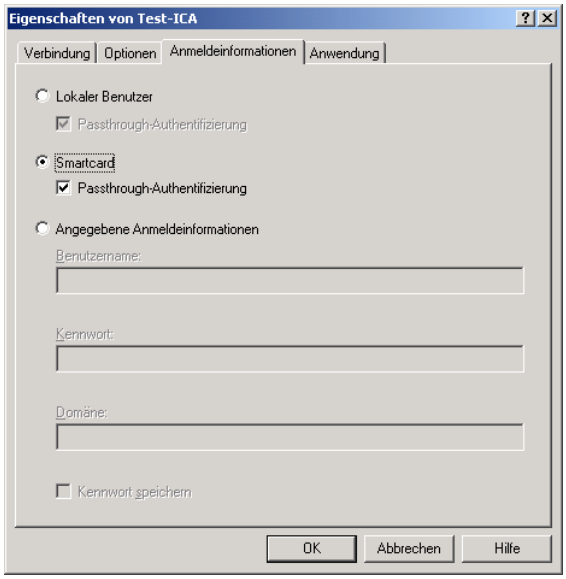
[14] *Erst die Installation des CSP auf dem Presentation/Terminal Server ermöglicht diesem das ausführen der von dem Client angeforderten kryptografischen Operationen.*

3. Installation eines aktuellen ICA-Clients, downloadbar als Client-Packager für die meisten Windows-Versionen unter:
http://www.citrix.com/English/SS/downloads/downloads.asp?dID=2755
Im vorliegenden Szenario wurde die Version 9.150 vom 16. 12. 2005 verwendet.

4. Konfiguration des ICA-Clients
Der ICA-Client soll folgendermaßen konfiguriert werden. Unter *Verbindung* sind die selbsterklärenden Eingaben zu tätigen:



Unter *Anmeldeinformationen* ist die Standardeinstellung *Lokaler Benutzer* zu deaktivieren und statt dessen die Smartcard-Anmeldung mit *Passthrough-Authentifizierung* zu aktivieren:



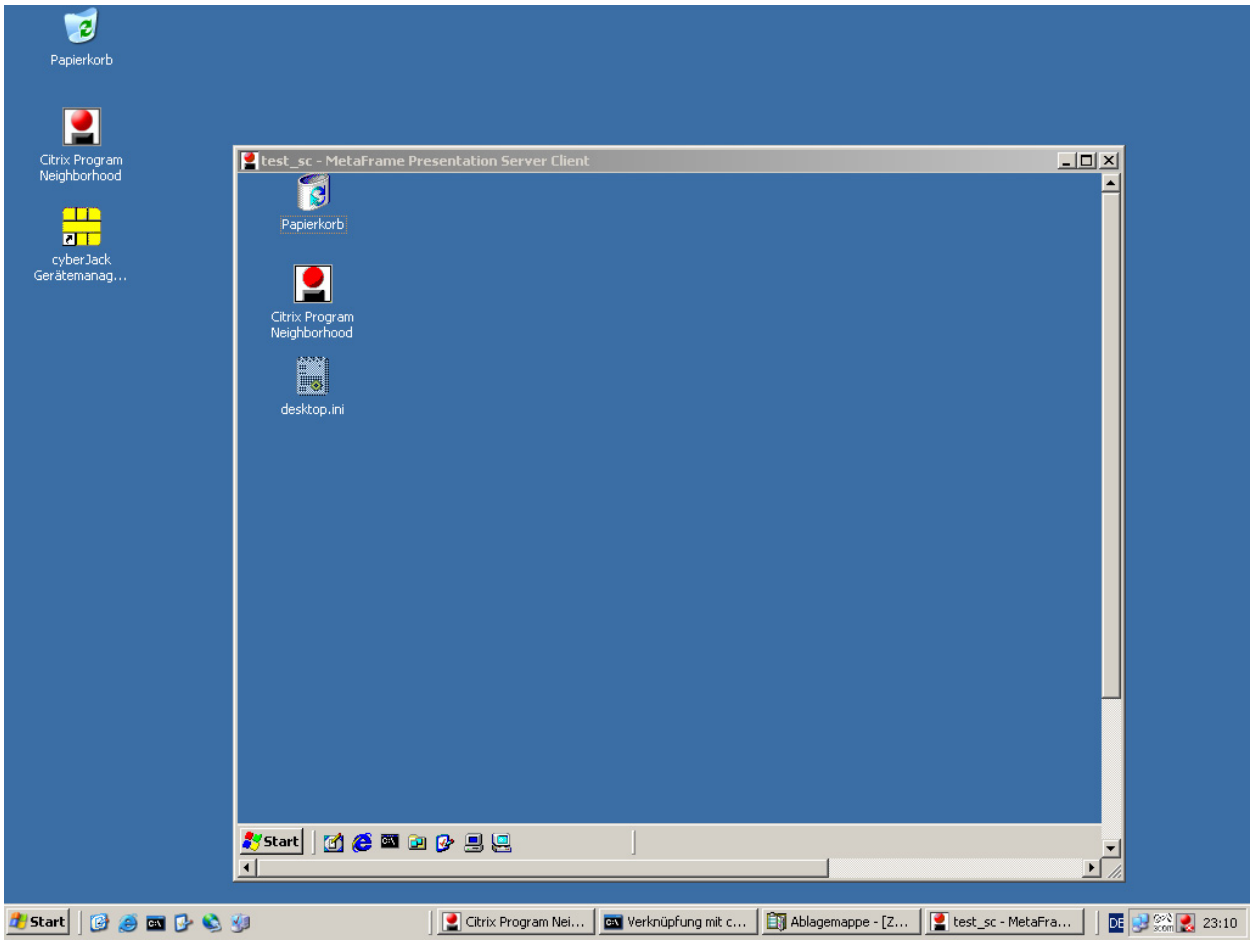
5. Im Fehlerfall manuelles Editieren der Datei *appsrv.ini* unter:
\Dokumente und Einstellungen\%username%\Anwendungsdaten\ICAClient
Es können – im Fehlerfall – die beiden folgenden Einträge gesetzt werden:
   a. EnableSSOnThruICAFile=On
   b. SSOnUserSetting=On

Im vorliegenden Szenario war der erste Eintrag nicht notwendig, der zweite Eintrag war automatisch gesetzt.
Weitere Informationen entnimmt man Kapitel 4 aus [11] und dem Artikel [12].

6.2 Ergebnis

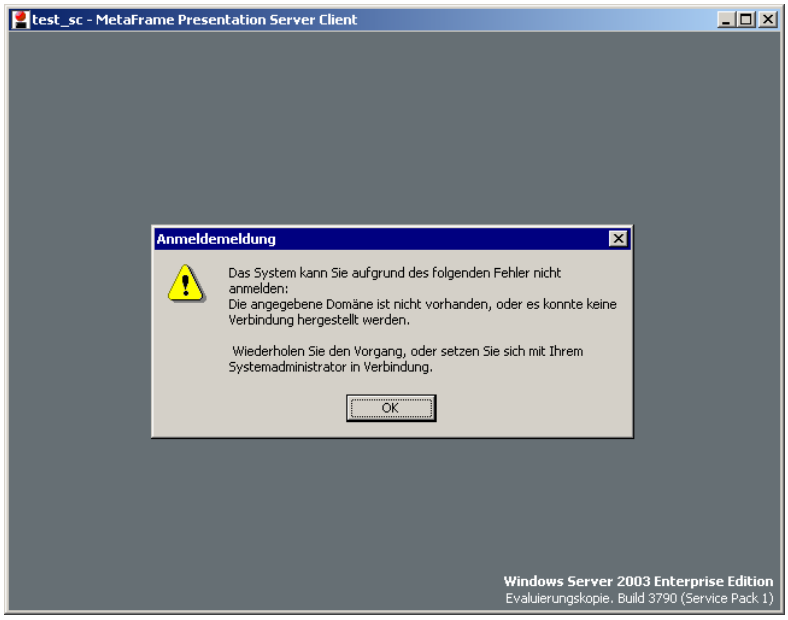
6.2.1 Gewöhnlicher Smartcard-Logon an Citrix (Domänencontroller online)

Das Ergebnis ist ein funktionierender Smartcard-Logon am Presentation Server 4.0, und zwar sowohl von Windows XP- als auch Windows 2000 Professional-Clients. Die unter Abschnitt 4.5.1 genannten Bedingungen gelten hier ebenfalls.
Erfolgreiche Smartcard-Anmeldung am Presentation Server:



6.2.2 Offline-Szenario

Eine erfolgreiche Smartcard-Anmeldung am Presentation Server 4.0 ohne verfügbaren Domänencontroller war sowohl unter Windows 2000 Professional als auch unter Windows XP Professional nicht möglich. Bei Windows 2000 fror die ICA-Verbindung zum Presentation Server ein, bei Windows XP Professional führte das Fehlen des Domänencontrollers (ebenfalls) reproduzierbar zu folgender Fehlermeldung:



7 Auswahl möglicher Fehler und Fehlermeldungen

7.1 Grundsätzliches

Die Ereignisprotokollierung ist bei allen getesteten Betriebsystemversionen nicht immer ergiebig. Das hängt vor allem damit zusammen, dass Windows 2000 und Server 2003 nur dann über eine ausführliche Protokollierung von Zertifikatsereignissen verfügen, wenn eine Windows CA installiert ist. Grundsätzlich gilt jedoch, dass Windows XP und Server 2003 ausführlicher als Windows 2000 protokollieren.

Erfolgreiche Smartcard-Anmeldungen sind im Ereignisprotokoll nicht besonders gegenüber erfolgreichen interaktiven Anmeldungen gekennzeichnet.

Fehlerhafte Smartcard-Anmeldungen finden sich im Anwendungsprotokoll von Windows XP-Professional Clients und dem Terminal /Presentation Server unter der Quelle *Smartcard-Logon*.

7.2 SafeSign

In zwei Fällen wurden fehlerhafte Logons durch die Neuinstallation von SafeSign behoben (siehe unten). Die Software zeigt beim Anmelden kein dediziertes Fenster zur Eingabe der PIN und auch die ablaufende Zeit (5 Sekunden pro Ziffer aus der PIN) entnimmt man nur dem Blinken der orangenen Lampe des Kartenlesers. Die PIN kann nur über den Kartenleser eingegeben werden. Wenn ein Konto auf dem Presentation Server vom Benutzer gesperrt wurde, öffnete sich dagegen ein extra Fenster zur Eingabe der PIN. Dabei muss die PIN dann über die Computer-Tastatur eingegeben werden.

7.2.1 SafeSign-Version

Die geteste Version 2.0.2 lief – bis auf die zwei notwendigen Reinstallationen – fehlerfrei.

7.2.2 Neuinstallation von Safesign

In der Windows 2000-basierten Active Directory-Umgebung erschien an einem Windows XP-Rechner auch nach dem Aufspielen des u. g. Hotfixes bei der Anmeldung mit der Smartcard trotz Eingabe der korrekten PIN die auch auf einem zweiten Rechner reproduzierbare Fehlermeldung:

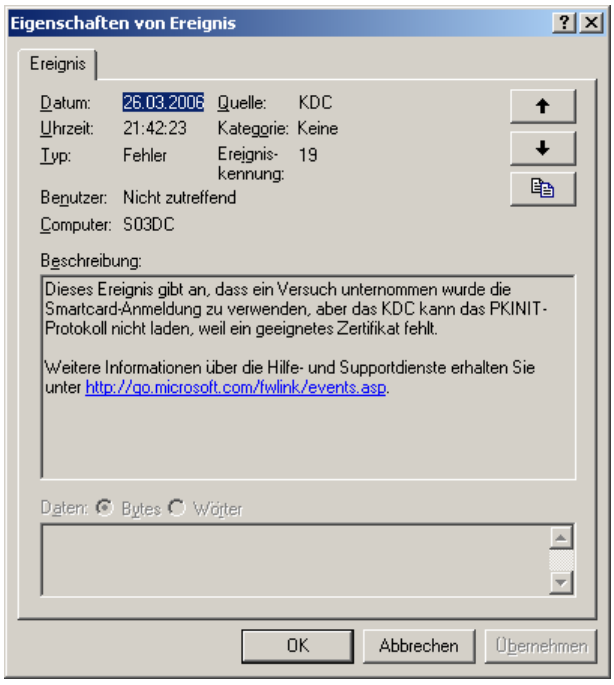
Sie konnten nicht angemeldet werden, da eine ungültige PIN-Nummer für die Smartcard eingegeben wurde.

Dem entspricht die folgende Ereignismeldung im Anwendungsprotokoll des Clients:

Auf dem Domänencontroller fanden sich keine Einträge im Ereignisprotokoll. Die Reinstallation von SafeSign führte auf beiden Computern zur Fehlerbeseitigung.

7.3 Fehlender Hotfix KB 891841 auf Windows XP mit SP1 oder SP2

Der Hotfix ist auf Windows XP Professional mit SP 1 oder SP 2 notwendig für eine funktionierende Smartcard-Anmeldung. Befindet sich der Hotfix nicht auf dem System, dann findet sich im Systemprotokoll des authentifizierenden Domänencontrollers der folgende Eintrag:



7.4 Fehler wegen falscher UPN-Definition

Wenn der UPN nicht richtig in dem Smartcard-Zertifikat definiert ist, dann erscheint während des Anmeldeversuchs mit der Smartcard die *Anmeldemeldung: Sie können aufgrund folgenden Fehlers nicht angemeldet werden:*

Falscher Parameter.

Wiederholen Sie den Vorgang, oder wenden Sie sich an den Systemadministrator.

7.5 Generelle Konfigurationen, bei denen die Zeit eine Rolle spielt

Es gilt für eine synchrone Zeit aller beteiligter Komponenten zu sorgen (Datum, Uhrzeit, Zeitzone). Zertifikate enthalten ein Zeitfenster, das ihre Gültigkeit definiert. Ist die Zeit des Systems vor oder nach dieser Periode, werden die Zertifikate zurückgewiesen. Im Übrigen spielt eine korrekte Systemzeit auch bei den beteiligten Komponenten der Kerberos-Authentifizierung eine wichtige Rolle.

8 LITERATUR

[1] How Certificates Work (http://technet2.microsoft.com/WindowsServer/en/Library/3f5fdc52-8623-4336-840d-e90b2399c8541033.mspx)

[2] Guidelines for enabling smart card logon with third-party certification authorities (http://support.microsoft.com/default.aspx?scid=kb;en-us;Q281245)

[3] Requirements for Domain Controller Certificates from a Third-Party CA (http://support.microsoft.com/kb/291010/EN-US/)

[4] How to import third-party certification authority (CA) certificates into the Enterprise NTAuth store (http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q295663)

[5] Object IDs associated with Microsoft cryptography (http://support.microsoft.com/kb/287547/EN-US/)

[6] Certificate Templates Troubleshooting (http://technet2.microsoft.com/WindowsServer/en/Library/43881ad5-aa6b-4527-ad59-cd2218bd99341033.mspx)

[7] Mapping certificates to user accounts (http://technet2.microsoft.com/WindowsServer/en/Library/66d38725-713f-494a-b4c5-0b5040bb98721033.mspx)

[8] You receive "The system could not log you on" error message when you use a smart card to log on to a Windows XP Professional-based computer (http://support.microsoft.com/kb/891849/en-us)

[9] Troubleshooting Windows 2000 PKI Deployment and Smart Card Logon (http://www.microsoft.com/technet/prodtechnol/windows2000serv/support/smrtcrdtrbl.mspx)

[10] Brian Komar et al.: Microsoft Windows Server 2003 PKI and Certificate Security, Redmond: Microsoft Press, 2004

[11] Metaframe Presentation Server Administrator´s Guide (bes. Kap. 4) (http://support.citrix.com/servlet/KbServlet/download/6338-102-14087/Administrators_Guide.pdf

[12] Configuring Smart Card authentication for Citrix Presentation Server (http://brianmadden.com/content/content.asp?id=569)

Mit freundlichen Grüßen,

Friedwart Kuhn ERNW GmbH Friedwart Kuhn Senior Security Consultant ERNW Enno Rey Netzwerke GmbH Breslauer Str. 28 69124 Heidelberg Tel. +49 6221 480390 Fax +49 6221 419008 Mobil +49 174 3278727 www.ernw.de	Enno Rey ERNW GmbH Enno Rey Geschäftsführer ERNW Enno Rey Netzwerke GmbH Breslauer Str. 28 69124 Heidelberg Tel. +49 6221 480390 Fax +49 6221 419008 Mobil +49 173 6745902 www.ernw.de