Student Workbook

# Installation einer Enterprise PKI

**Inhalt**



FAW
Für Anwendungsorientierte Wissensverarbeitung

Tutorium

PKI

Dr. Stefan Probst
Jormannsdorf 99
7431 Bad-Tatzmannsdorf
stefan.probst@ssw-consulting.net


# Installation einer Enterprise PKI

*Dieses Tutorium erläutert anhand einer Schritt für Schritt Anleitung die Installation einer Enterprise PKI mittels Windows Server 2003 Enterprise Edition.*

Die Verwendung einer Public Key Infrastructure (PKI) gewinnt zunehmend an Bedeutung im Sicherheitsportfolio eines Unternehmens. Moderne Mechanismen zum Schutz von Dokumenten, E-Mails, Dateien oder Netzwerkkommunikation setzen auf komplexe Verschlüsselungsverfahren. Die PKI erlaubt einen Einsatz dieser Mechanismen innerhalb eines Unternehmens.

Dieses Tutorium zeigt die Installation einer PKI anhand der mit Windows Server 2003 ausgelieferten Zertifikatsdienste. Dabei wird von einem allgemeinen Verständnis zum Thema PKI sowie guten Kenntnissen des Windows Server 2003 Betriebssystems ausgegangen.

| SYMBOL-LEGENDE | |
|---|---|
| ⓘ | Informationen |
| ! | Wichtige Hinweise |
| 🖉 | Beispiele |
| ? | Verständnisfragen |

**Verwendung des Skripts:** In diesem Skriptum werden Sie immer wieder auf verschiedene Symbole und Schreibweisen stoßen.

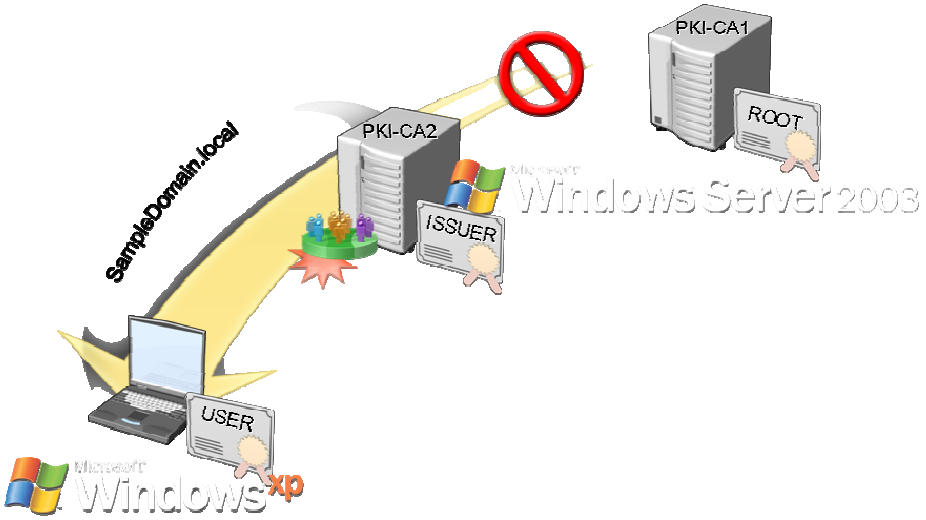
Spezielle Zeichen werden durch einfache Anführungszeichen (‚') gekennzeichnet. Kommandos werden innerhalb doppelter Anführungszeichen („") erwähnt. Variable Teile innerhalb eines Kommandos sind *kursiv* gedruckt, genauso wie betonte Wörter. Am Seitenrand werden Sie immer wieder Symbole finden, die auf spezielle Informationen hindeuten.

Als zugrunde liegende Plattform wird Windows Server 2003 Enterprise Edition benutzt.

# Voraussetzungen zur Durchführung des LABs

Die Installation einer Enterprise PKI wird anhand eines LABs demonstriert. Dabei werden sowohl die dafür notwendigen Server als auch ein Client in virtuellen Maschinen installiert.

## *Virtuelle Maschinen*




Das Lab besteht aus drei virtuellen Maschinen.

1.) **PKI-CA1**: Diese virtuelle Maschine realisiert die Enterprise ROOT CA. Da diese Maschine eine offline ROOT CA implementieren wird, ist dies ein Stand-Alone Server *ohne* Domänenzugehörigkeit!
Betriebssystem: Windows Server 2003 Enterprise Edition
LAB IP-Adresse: 192.168.0.2
Domänenzugehörigkeit: keine

2.) **PKI-CA2**: Diese virtuelle Maschine realisiert die Online Issuing CA. Hier werden die Clients ihre Zertifikate online beziehen. Die Online Issuing CA ist der ROOT CA untergeordnet.

! Im Lab fungiert diese Maschine auch als Active Directory Domänenkontroller. Bitte beachten Sie, dass dies keine empfohlene Konfiguration ist. Sie sollten aus verschiedensten Gründen niemals eine CA auf einem Domänenkontroller installieren.

Betriebssystem: Windows Server 2003 Enterprise Edition
LAB IP-Adresse: 192.168.0.1
Domänenzugehörigkeit: SampleDomain.local

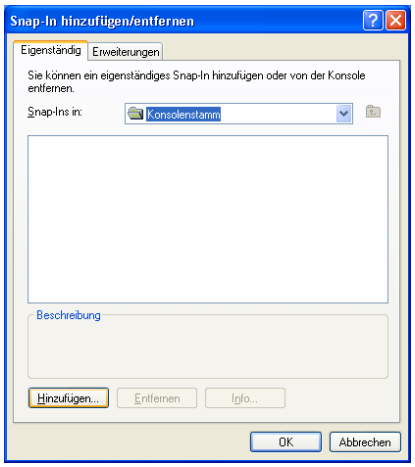
3.) **Client**: Diese virtuelle Maschine repräsentiert eine Arbeitsstation im Enterprise Netzwerk.
Betriebssystem: Windows XP Professional
LAB IP-Adresse: 192.168.0.5
Domänenzugehörigkeit: SampleDomain.local

## Zertifikate am Client

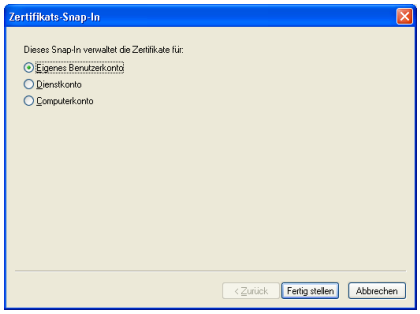
Zunächst machen wir uns am Client mit der Zertifikatskonsole vertraut. Dazu wird unter Windows XP ein entsprechendes Snap In für die Microsoft Management Console (MMC) bereitgestellt. Starten Sie diese, in dem Sie auf Start → Ausführen klicken und im Dialog „mmc“ eingeben.


In der erscheinenden Konsole müssen wir nun die entsprechenden Zertifikats-Snap-Ins hinzufügen. Wählen Sie hierzu aus dem Datei-Menü den Eintrag „Snap-In hinzufügen/entfernen“.

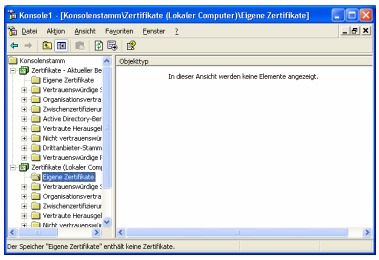
Im erscheinenden Dialog klicken Sie nun unter der Kategorie ‚Eigenständig’ auf die Schaltfläche ‚Hinzufügen…’. Wählen Sie dann das Snap In Zertifikate aus und klicken Sie dann auf die Schaltfläche ‚Hinzufügen’.








Sie können nun auswählen, für welchen Zertifikatsbereich Sie die Konsole verwenden wollen. Die Optionen ‚Dienstkonto’ und ‚Computerkonto’ stehen nur Administratoren zur Verfügung. Wählen Sie zunächst den Bereich ‚Eigenes Benutzerkonto’ und fügen Sie eine zweites Zertifikate Snap-In für den Bereich ‚Computerkonto’ hinzu.



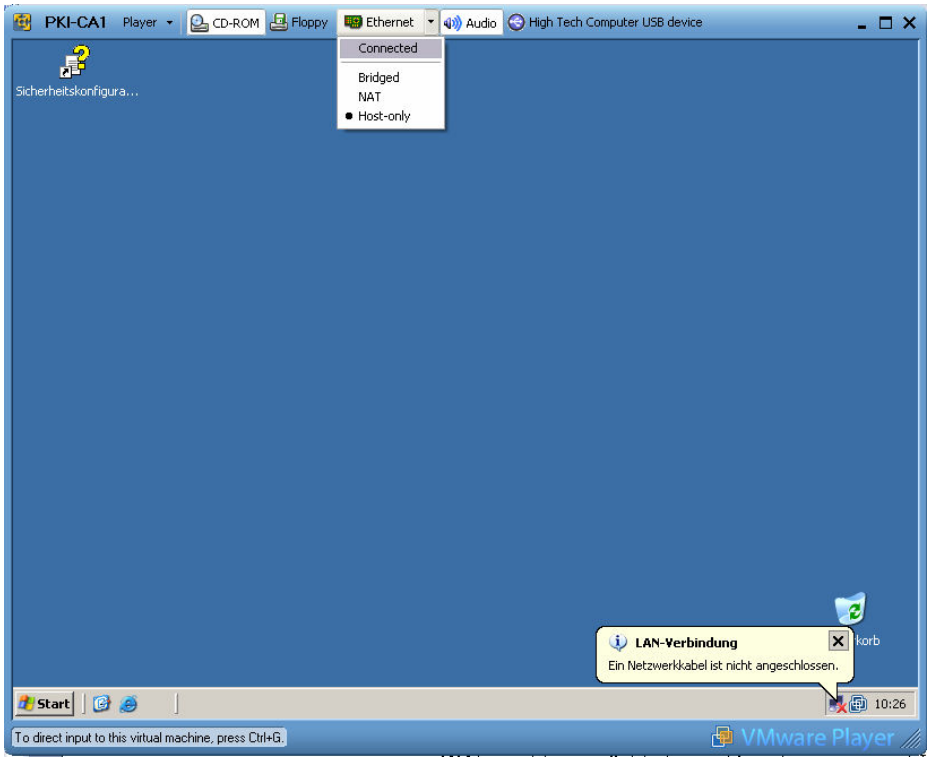

Schließen Sie alle Dialoge bis Sie wieder auf der Managementkonsole landen. Sie haben nun die Möglichkeit, die Zertifikate des aktuellen Benutzers und die Computerzertifikate einzusehen. Im ersten Schritt stellen wir fest, dass in der Kategorie „Eigene Zertifikate“ keine Zertifikate vorhanden sind. Das bedeutet, dass derzeit noch keine Zertifikate für den Benutzer oder den Computer ausgestellt wurden.

# Installation der Offline ROOT CA

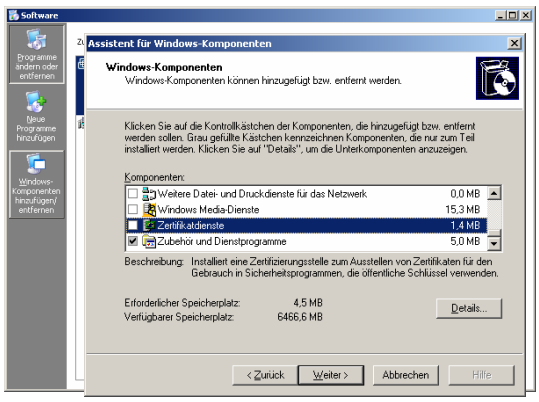
Im nächsten Schritt soll nun die Offline ROOT CA installiert werden. Da die ROOT CA das Herzstück der Infrastruktur ist, bedarf diese einen besonderen Schutz. Wird die ROOT CA kompromittiert, so ist die komplette PKI unbrauchbar. Es empfiehlt sich daher, diese Maschine vom Netz zu trennen und die Zertifikate über ein anderes Medium (z.B. Wechseldatenträger) auszutauschen.

## *Schritt 1: Offline-Schalten der ROOT CA*

Für die folgenden Schritte benötigt die ROOT CA keine Netzwerkverbindung mehr. Im Falle der virtuellen Maschine deaktivieren wir die Netzwerkverbindung über die VMWare Player Netzwerkeinstellungen.



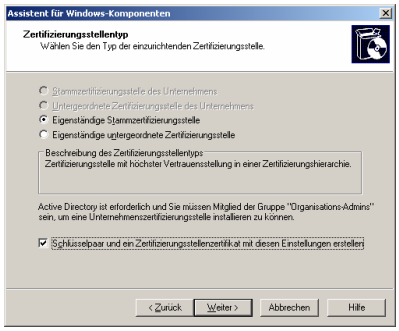

## *Schritt 2: Installation der Zertifikatsdienste*




Im nächsten Schritt installieren wir die Windows Server Zertifikatsdienste. Diese können über die Softwarekonsole in der Systemsteuerung (Start → Systemsteuerung → Software) im Menüpunkt „Windows Komponenten hinzufügen / entfernen“ installiert werden.

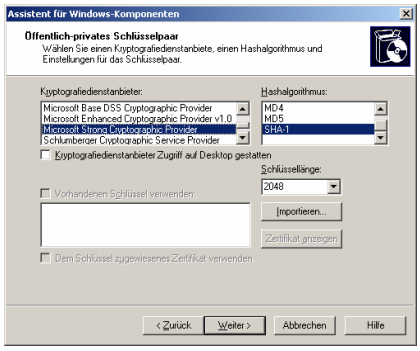
Im erscheinenden Dialog dann die Zertifikatsdienste zur Installation auswählen. Es wird nun ein Warnhinweis eingeblendet, der darauf

aufmerksam macht, dass nach der Installation der Zertifikatsdienste der Rechnername und dessen Domänenzugehörigkeit nicht mehr geändert werden kann. Diesen Hinweis bestätigen wir und setzen die Installation durch Klicken auf die Schaltfläche „Weiter >“ fort.



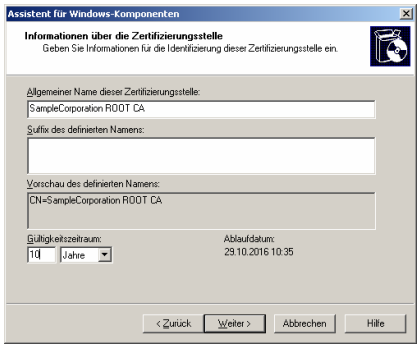

Es wird nun der Assistent zur Konfiguration der Zertifizierungsstelle gestartet. Zunächst müssen wir den Zertifizierungsstellentyp angeben.

Offline CAs sollten nicht im Active Directory integriert werden, deshalb sollten alle Offline CAs als ‚Eigenständige Zertifizierungsstelle’ realisiert werden. Im Falle der ROOT CA wählen wir deshalb die Option „Eigenständige Stammzertifizierungsstelle“ und lassen uns durch Anwählen der Option „Schlüsselpaar und ein Zertifizierungsstellenzertifikat mit diesen Einstellungen erstellen“ ein Zertifikat für die CA erstellen.




Im nächsten Dialog können wir die Parameter des Schlüsselpaars einstellen. Hier ist es mitunter möglich, bestehende Zertifikate (z.B. von einer Smartcard oder einer öffentlichen Zertifizierungsstelle) zu importieren.

In unserem Fall möchten wir uns selbst ein Zertifikat ausstellen und fahren mit den Standardeinstellungen fort.




Im nächsten Schritt werden wir aufgefordert, Informationen über die Zertifizierungsstelle bekannt zu geben. Die hier eingegebenen Informationen scheinen dann in den Zertifikaten und den untergeordneten CAs auf, deshalb sollten hier sprechende Namen vergeben werden!

Zudem wird uns die Möglichkeit gegeben, die Gültigkeitsdauer des Zertifikats der CA anzugeben. Da es sich hier um eine Offline CA handelt, die weniger Bedrohungen ausgesetzt ist als Online CAs oder Desktop-Maschinen, kann hier durchaus ein höherer Gültigkeitszeitraum angegeben werden. Da das Erneuern des Zertifikats einer Offline CA mitunter ein komplexer Prozess ist, empfiehlt sich hier die Einstellung auf 10 Jahre.

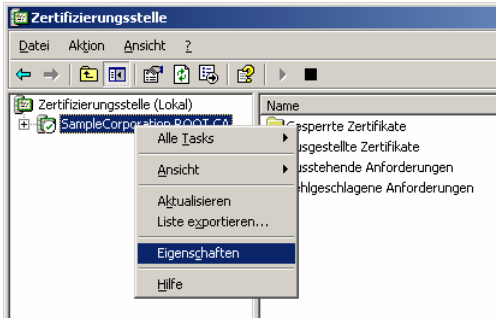
Im nächsten Schritt wird nun die ROOT CA installiert und ein Zertifikat für die CA erstellt. In einem weiteren Dialog kann angegeben werden, wo die Einstellungen der Zertifikatsdatenbank gespeichert werden sollen. Wir belassen diese auf die Standardwerte.

Zudem erhalten wir noch einen Warnhinweis, dass die Weboberfläche nicht verfügbar ist, da wir keinen Anwendungsserver (IIS) installiert haben. Dies ist im Falle der Offline CA nicht notwendig, deshalb können wir diesen Warnhinweis ignorieren.

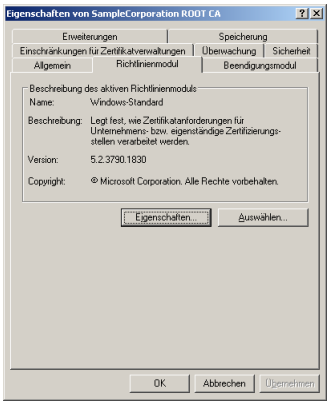
## *Schritt 3: Konfiguration der ROOT CA*

Nach der Installation muss die ROOT CA entsprechend konfiguriert werden. Dies geschieht in der Verwaltungskonsole der Zertifizierungsstelle. Die Konsole kann über Start → Verwaltung → Zertifizierungsstelle gestartet werden.

### Umgang der CA mit Zertifikatsanforderungen

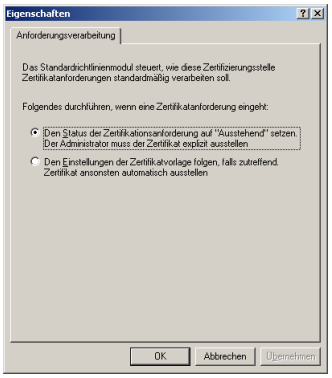



Zunächst wollen wir festlegen, wie die CA mit Zertifikatsanforderungen umgeht. Da es sich hierbei um eine Offline CA handelt, sollen Zertifikate nur nach expliziter Zustimmung des Administrators erstellt werden. Um dies einzustellen, müssen wir die Eigenschaften der CA ändern. Dazu klicken Sie auf die CA mit der rechten Maustaste und wählen im Kontextmenü den Eintrag „Eigenschaften".




Wie die CA mit Zertifikatsanforderungen umgeht wird in der Reiterseite „Richtlinienmodul" eingestellt. Durch klicken auf die Schaltfläche „Eigenschaften" bekommen Sie die Möglichkeit, die Anforderungsverarbeitung einzustellen.

In unserem Fall wählen wir hier die Option „Den Status der Zertifikatsanforderung auf „Ausstehend" setzen. Der Administrator muss das Zertifikat explizit ausstellen."

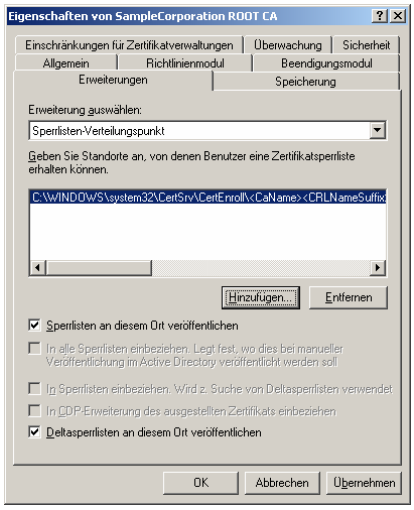



### Bekanntgabe der Certificate Distribution Points (CDP) und der Authority Information Access (AIA) Stellen

Im nächsten Schritt müssen nun die Verteilungspunkte der CA angegeben werden.

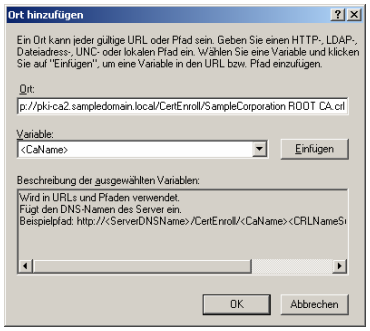
! Achtung: Da diese Information in den Zertifikaten gespeichert wird, muss dies geschehen noch bevor das erste Zertifikat durch die CA ausgestellt wurde. Werden die Verteilungspunkte zu einem späteren Zeitpunkt geändert und sind die ursprünglichen Verteilungspunkte nicht mehr erreichbar, so

müssen alle bis zu diesem Zeitpunkt ausgestellten Zertifikate zurückgezogen werden und erneuert werden!



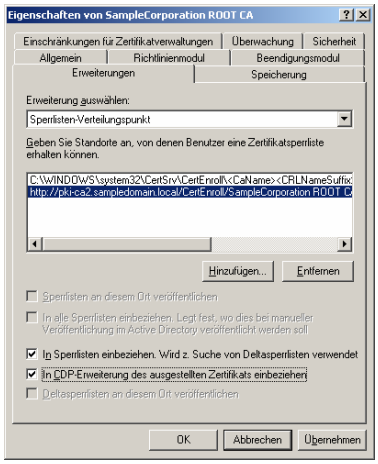

Die Verteilungspunkte werden ebenfalls in den Eigenschaften der CA, in der Reiterseite „Erweiterungen“ eingestellt. Dort sind bereits eine Reihe von Standardverteilungspunkte enthalten, die allerdings im Falle der Offline CA nicht genutzt werden können. Entfernen Sie alle Einträge bis auf den Eintrag mit dem Verweis im lokalen Dateisystem.

Fügen Sie dann den zu verwendenden Online Verteilungspunkt hinzu, indem Sie auf die Schaltfläche „Hinzufügen“ klicken und die URL zum Verteilungspunkt angeben.



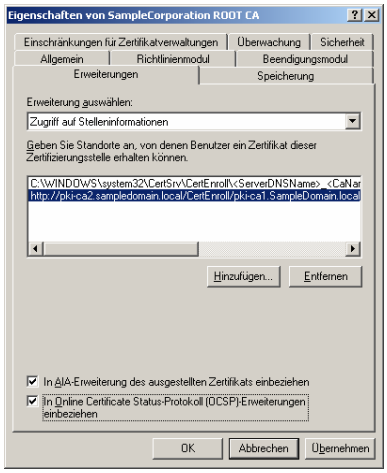

In unserem Beispiel schalten wir die Online CA frei und werden auch dort die CRLs und AIA publizieren. Deshalb geben wir im Dialog die URL zu unserer Online CA ein, die wir im nächsten Schritt installieren werden.

Die URL für den Sperrlisten-Verteilungspunkt der Online CA wird:
http://pki-ca2.sampledomain.local/CertEnroll/SampleCorporation ROOT CA.crl
lauten.




Nach hinzufügen des neuen Verteilungspunkts konfigurieren wir noch Option, dass dieser Verteilungspunkt im Zertifikat berücksichtigt wird. Dazu aktivieren wir die Optionen „In Sperrlisten einbeziehen. Wird z. Suche von Deltasperrlisten verwendet“ und „In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen“.

Die hier durchgeführten Schritte müssen nun für die AIA wiederholt werden. Wählen Sie dazu im Dialog in der ComboBox „Erweiterungen auswählen:“ die Option „Zugriff auf Stelleninformation“ aus.




Entfernen Sie wiederum alle Standard-verteilungspunkte bis auf den Verweis ins lokale Dateisystem. Fügen Sie analog zu den Sperrlisten einen neuen Verteilungspunkt hinzu. In unserem Beispiel werden wir wiederum die Online CA als Verteilungspunkt nutzen. Die URL dazu lautet (zusammengeschrieben): http://pki-ca2.sampledomain.local/CertEnroll/ pki-ca1.SampleDomain.local_ SampleCorporation ROOT CA.crt

Wiederum müssen die beiden Optionen „In AIA-Erweiterung des ausgestellten Zertifikats einbeziehen“ und „In Online Certificate Status-Protokoll (OCSP)-Erweiterungen einbeziehen“ ausgewählt werden, damit die Information im Zertifikat hinterlegt wird.

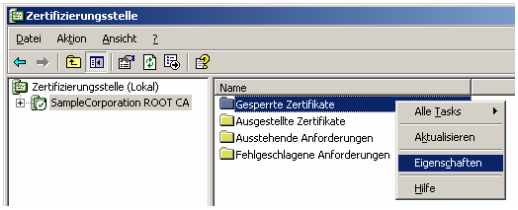
Nach dem Einstellen der Eigenschaften muss die CA neu gestartet werden, damit die Einstellungen übernommen werden. Klicken Sie hierzu auf „Übernehmen“ und anschließend auf „OK“.

ⓘ Beim Prüfen versucht der Client, die im Zertifikat angegebenen Verteilungspunkte der Reihe nach zu erreichen, bis ein entsprechender Verteilungspunkt gefunden ist. Je nach Art des Verteilungspunkts (Dateisystem, Web, etc.) ist ein Timeout verbunden, den der Client abwartet, bis er versucht den nächsten Verteilungspunkt zu kontaktieren. Falsche Einträge oder eine falsche Reihenfolge können somit zu erheblichen Verzögerungen bei der Zertifikatsverwendung führen!

## Einstellen des CRL-Distributionsintervalls

CRLs haben eine bestimmte Gültigkeitsdauer. Es ist wichtig, dass immer eine gültige CRL gefunden wird, auch wenn diese leer ist. Kann keine gültige CRL gefunden werden, können die Zertifikatsdienste nicht gestartet werden.

Da die Verteilung der CRL der Offline CA nur über Datenträger erfolgen kann und insofern mit Aufwand verbunden ist, empfiehlt es sich, ein entsprechend hohes CRL Distributionsintervall einzustellen. Wie lange eine solche CRL gültig ist, hängt von den internen Prozessen im Unternehmen ab.

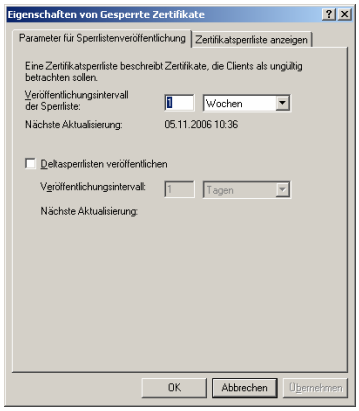


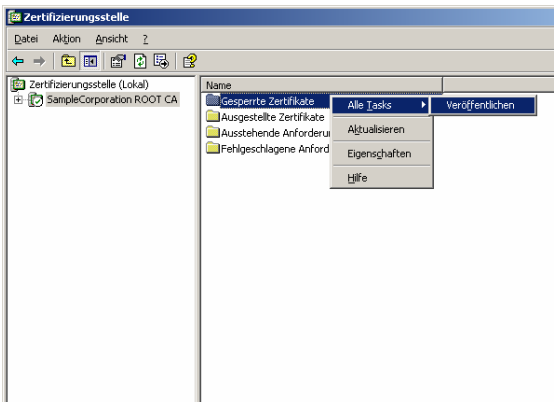

Das Distributionsintervall wird in der Zertifizierungsstellenkonsole angegeben. Wählen Sie dazu zunächst die entsprechende Zertifizierungsstelle und klicken dann auf den Eintrag „Gesperrte Zertifikate“ mit der rechten Maustaste und wählen Sie den Eintrag „Eigenschaften“ aus.

Im erscheinenden Dialog kann nun das Veröffentlichungsintervall der Sperrliste angegeben werden. Zudem wird davon abhängig das Datum der nächsten Aktualisierung angezeigt. In unserem Beispiel setzen wir das Intervall auf 1 Woche.

Im letzten Schritt muss nun die Zertifikatsliste veröffentlicht werden. Dies geschieht bei einer Offline CA manuell. Dazu muss mit der rechten Maustaste auf den Eintrag „Gesperrte Zertifikate“ geklickt werden und dann im Menü „Alle Tasks“ der Eintrag „Veröffentlichen“ ausgewählt werden. In einem erscheinenden Dialog wird nun gefragt, ob eine neue Sperrliste oder eine Deltasperrliste veröffentlicht werden soll. Handelt es sich um die erste Sperrliste die veröffentlicht wird, so steht nur die Option zur Veröffentlichung einer neuen Sperrliste zur Verfügung.

Veröffentlichen Sie die neue Sperrliste. Die Sperrliste und die AIA-Information wird nun in das Systemverzeichnis ‚\systemroot\system32\CertSrv\CertEnroll\’ abgelegt.




## Abschluss der Konfiguration

Kopieren Sie nun die für die Online CA benötigten Daten auf einen Wechseldatenträger:

- CRL und AIA-Information: Diese finden Sie im Verzeichnis <systemroot>\system32\CertSrv\CertEntroll. Die Dateien weisen die Endung „.crl’ und „.crt’ auf.

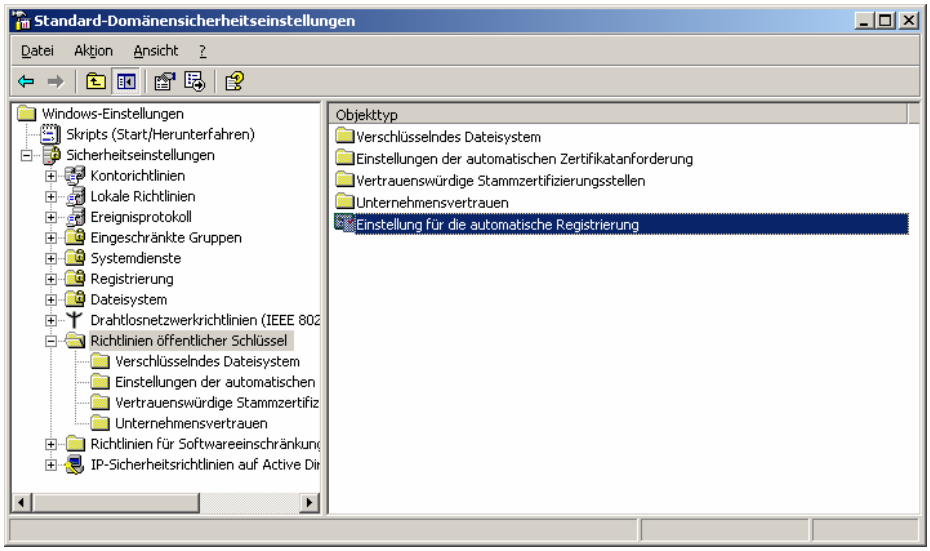
# Installation der Online Sub CA

Nun soll die Online Sub CA installiert werden. Die Sub CA ist der ROOT CA unterstellt und in das Active Directory integriert. Dies erlaubt die Möglichkeit, dass Zertifikate automatisch von Domänenbenutzern und Domänencomputern automatisch beantragt und ausgerollt werden können.

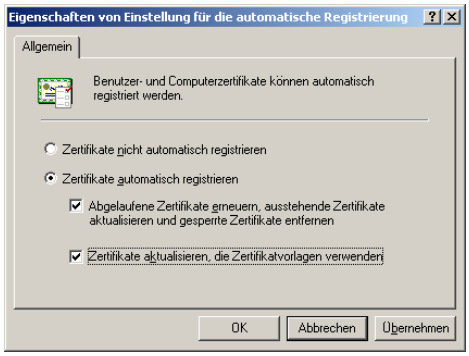
## *Schritt 1: Konfigurieren der Domänenrichtlinien*

Der Umgang mit Zertifikaten und den Zertifizierungsstellen innerhalb von Windows Domänen kann mittels der Richtlinien öffentlicher Schlüssel definiert werden. Im ersten Schritt sollten deshalb die Richtlinien entsprechend konfiguriert werden.

Öffnen Sie dazu am Domänenkontroller den Gruppenrichtlinien Editor. Diesen finden Sie unter Start → Verwaltung → Sicherheitsrichtlinie für Domänen. Die Richtlinien bezüglich PKI finden Sie unter den Windows-Einstellungen → Sicherheitseinstellungen → Richtlinien öffentlicher Schlüssel.




Da noch keine CA installiert wurde, sind die Objekttypen größtenteils leer. Allerdings sollten die „Einstellung für die automatische Registrierung“ konfiguriert werden. Klicken Sie bitte doppelt auf diesen Eintrag.

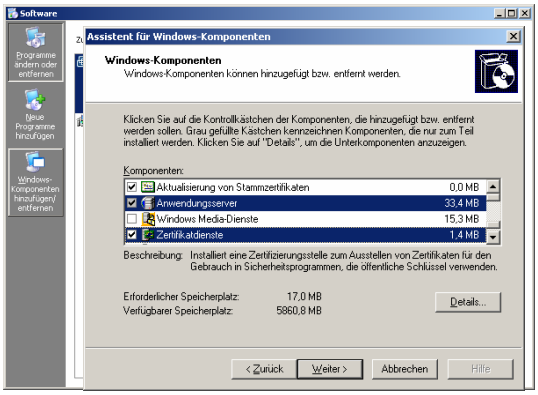



Im erscheinenden Dialog kann die automatische Registrierung für Benutzer- und Computerzertifikate in Domänen eingestellt werden. Standardmäßig ist die automatische Registrierung in einer Domäne aktiviert. Das würde bedeuten, dass bei der Installation der CA sich die Systeme automatisch registrieren und Zertifikate beantragen würden.

Tipp: Es empfiehlt sich, die automatische Registrierung erst zu aktivieren, wenn die CA vollständig und korrekt installiert wurde. Somit kann vermieden werden, dass etwaige falsche Konfigurationen in zu früh beantragten Zertifikaten ausgerollt werden und später zurückgezogen werden müssen. Erst nach korrekter Konfiguration der CA sollte diese Richtlinie aktiviert werden.

In unserem Beispiel kennen wir die endgültige Konfiguration der Sub CA, deshalb können wir die automatische Registrierung sofort aktivieren. Zudem aktivieren wir die Optionen „Abgelaufene Zertifikate erneuern, ausstehende Zertifikate aktualisieren und gesperrte Zertifikate entfernen“ und „Zertifikate aktualisieren, die Zertifikatvorlagen verwenden“. Diese Optionen erlauben ein automatisiertes Zertifikatshandling durch Domänencomputer.

## Schritt 2: Installation der Sub CA

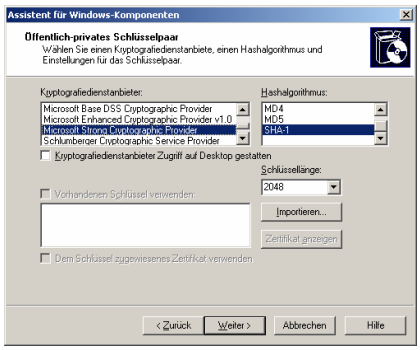



Ähnlich zur ROOT CA, installieren wir nun im nächsten Schritt die Windows Server Zertifikatsdienste. Diese können über die Softwarekonsole in der Systemsteuerung (Start → Systemsteuerung → Software) im Menüpunkt „Windows Komponenten hinzufügen / entfernen“ installiert werden.

Zusätzlich zu den Zertifikatsdiensten wollen wir nun auch die Webschnittstelle der CA installieren. Dazu muss zunächst die Komponente „Anwendungsserver“ ausgewählt werden. Im gleichen Dialog wählen wir dann zusätzlich die Zertifikatsdienste zur Installation aus. Es wird nun ein Warnhinweis eingeblendet, der darauf aufmerksam macht, dass nach der Installation der Zertifikatsdienste der Rechnername und dessen Domänenzugehörigkeit nicht mehr geändert werden kann. Diesen Hinweis bestätigen wir und setzen die Installation durch Klicken auf die Schaltfläche „Weiter >“ fort.

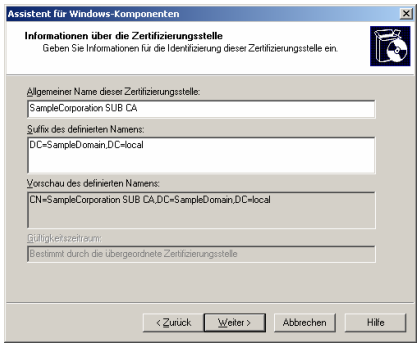

Es wird nun der Assistent zur Konfiguration der Zertifizierungsstelle gestartet.

Im Falle der Online CA ist eine Integration in das Active Directory erwünscht. Da es sich bei der Online CA allerdings eine der Offline ROOT CA untergeordnete CA handelt, müssen wir die Option „Untergeordnete Zertifizierungsstelle des Unternehmens“ wählen. Wiederum lassen wir uns ein Schlüsselpaar automatisch durch Anwählen der Option „Schlüsselpaar und ein Zertifizierungsstellenzertifikat mit diesen Einstellungen erstellen“ generieren.



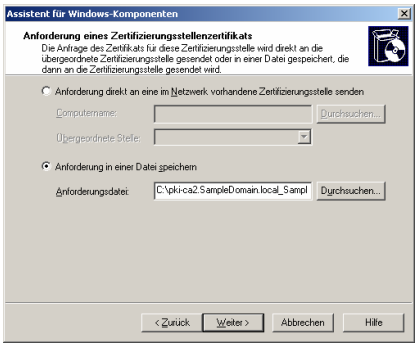

Im nächsten Dialog können wir die Parameter des Schlüsselpaars einstellen. Hier ist es mitunter möglich, bestehende Zertifikate (z.B. von einer Smartcard oder einer öffentlichen Zertifizierungsstelle) zu importieren.

In unserem Fall möchten wir uns selbst ein Zertifikat ausstellen und fahren mit den Standardeinstellungen fort.




Im nächsten Schritt werden wir aufgefordert, Informationen über die Zertifizierungsstelle bekannt zu geben. Die hier eingegebenen Informationen scheinen dann in den Zertifikaten auf, deshalb sollten hier sprechende Namen vergeben werden!

Anders als vorher kann nun keine Gültigkeitsdauer des CA-Zertifikats mehr eingegeben werden. Das liegt daran, dass im Falle einer untergeordneten CA das CA-Zertifikat von der übergeordneten CA ausgestellt wird und bereits mit einem Gültigkeitsdatum versehen wird. Damit dies geschieht, muss eine Anforderung für ein solches Zertifizierungsstellenzertifikats eingereicht werden. Dazu wird im nächsten Schritt ein entsprechender Dialog zur Verfügung gestellt. Da es sich bei unserer ROOT CA um einen Offline CA handelt, können wir nicht direkt eine Anforderung über das Netzwerk senden sondern müssen die Anforderung in eine Datei speichern und diese manuell zur ROOT CA übertragen.




Im nächsten Schritt wird nun die SUB CA installiert. Da noch kein Zertifikat für die SUB CA erstellt werden kann, da dies über die ROOT CA erfolgt, bekommen wir bei der Installation einen entsprechenden Hinweis, dass zuerst ein solches Zertifikat eingereicht und danach installiert werden muss. Zudem müssen wir die Installation der ASP-Erweiterungen bestätigen, die für den Betrieb der CA-Webschnittstelle notwendig sind.

## Schritt 3: Abschluss der Installation

Damit die SUB CA verwendet werden kann, muss noch ein entsprechendes Zertifikat von der ROOT CA ausgestellt werden. Damit dieses Zertifikat später auch akzeptiert wird, muss im Active Directory die ROOT CA bekannt gemacht werden. Zudem müssen die CRLs und AIA der ROOT CA in den Distribution Points zur Verfügung stehen.

Wir kopieren deshalb die im vorigen Kapitel kopieren Dateien auf dem Wechseldatenträger in das Distribution-Verzeichnis der neu erstellen SUB CA. Dieses befindet sich in <systemroot>\system32\CertSrv\CertEnroll.

In einem weiteren Schritt müssen wir nun das Zertifikat der ROOT CA im Active Directory veröffentlichen. Dazu öffnen wir eine Kommandozeile und geben folgenden Befehl ein:

```
for %i in (%systemroot%\system32\certsrv\certenroll\*.crt) do
certutil -f -dspublish "%i" RootCA
```

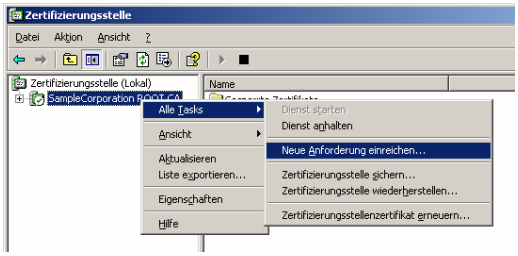
Bitte prüfen Sie, dass das Kommando erfolgreich durchgeführt wurde und ein neues Zertifikat dem Zertifikatsspeicher hinzugefügt worden ist!

## Schritt 4: Beantragen des SUB CA-Zertifikats

Kopieren Sie den im Schritt 2 erstellten Zertifikatsantrag (Dateiendung .req) auf den Wechselspeicher und gehen Sie damit zum ROOT CA.

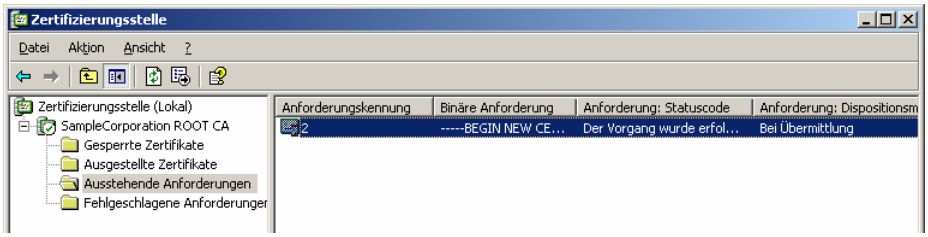
! Hinweis: Die folgenden Schritte werden auf dem Offline ROOT CA-Server durchgeführt!

Kopieren Sie den am Wechselspeicher befindlichen Zertifikatsantrag auf den ROOT CA Server. Starten Sie dort die Zertifizierungsstellenkonsole.

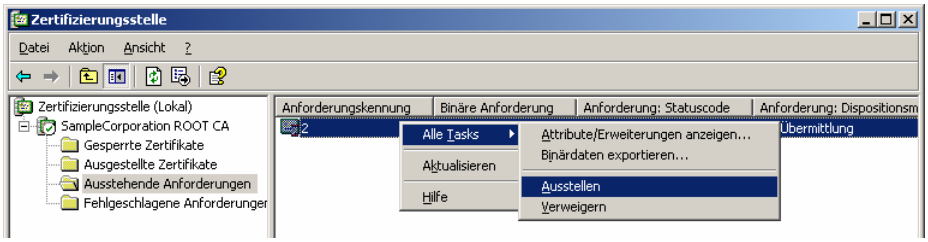



Über die Konsole kann nun durch Klicken der rechten Maustaste auf die CA und im Menü „Alle Tasks“ der Menüpunkt „Neue Anforderung einreichen“ der Zertifikatsantrag bearbeitet werden. Öffnen Sie im erscheinenden Dialog den zuvor kopierten Zertifikatsantrag.

Die CA bearbeitet nach den Richtlinien den Antrag nicht automatisch sondern wartet auf Bestätigung durch den Administrator. Deshalb befindet sich die Anforderung zunächst in der Kategorie „Ausstehende Anforderungen“.



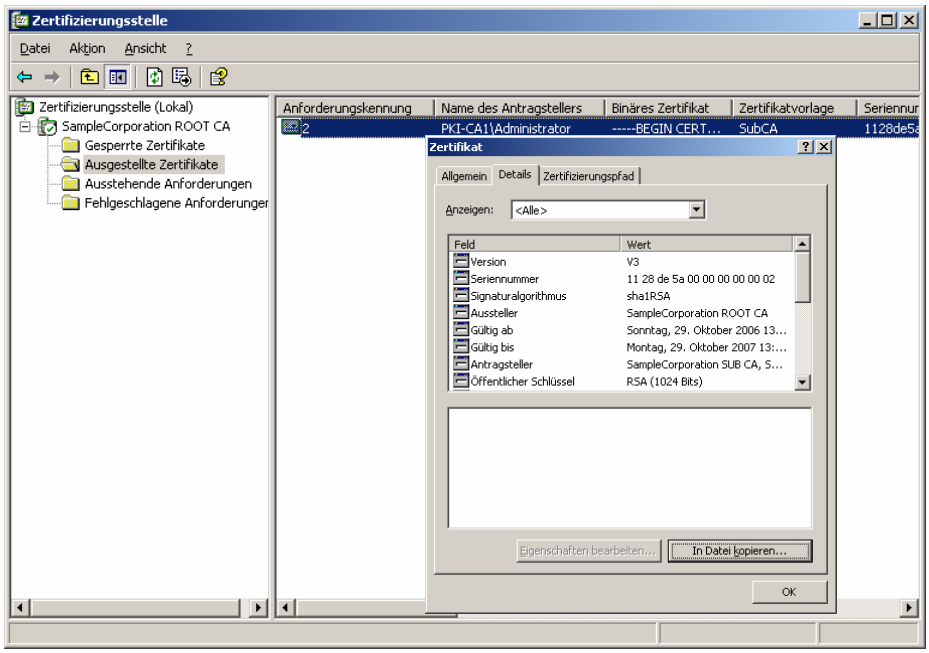

Klicken Sie mit der rechten Maustaste auf die Zertifikatsanforderung und wählen Sie dann im Kontextmenü unter „Alle Tasks“ den Menüpunkt „Ausstellen“.



Das Zertifikat wird nun ausgestellt und ist in der Liste der ausgestellten Zertifikate einsehbar.

Im nächsten Schritt muss nun das gerade erstellte Zertifikat exportiert werden, auf den Wechseldatenträger kopiert werden und zur Online SUB CA gebracht werden.

Klicken Sie dazu in der Kategorie „Ausgestellte Zertifikate“ auf das neue Zertifikat doppelt.




Im erscheinenden Zertifikatsdialog kann nun das Zertifikat durch Anwählen der Schaltfläche „In Datei kopieren…“ (Reiterseite Details) exportiert werden. Wählen Sie dazu das Format „*DER-codiert-binär X.509 (.CER)*“ und kopieren danach das exportierte Zertifikat auf den Wechseldatenträger.

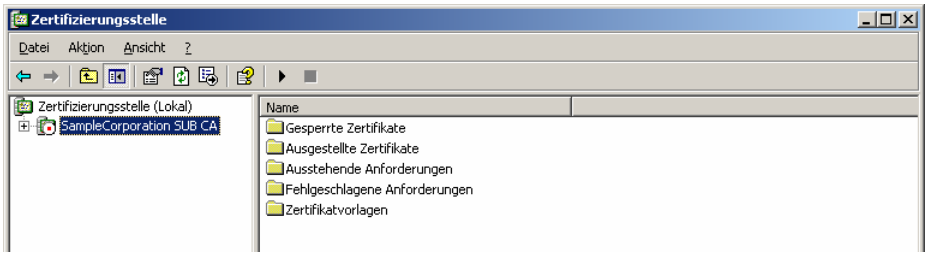
ⓘ Hinweis: Es sind nun alle Schritte, für welche die Offline CA notwendig war, durchgeführt worden. Theoretisch könnten Sie nun die Offline CA abschalten, obwohl dies keinen Unterschied machen würde, da die Offline CA ja sowieso vom Netz genommen wurde. Allerdings wäre es sinnvoll, zum jetzigen Zeitpunkt eine Sicherungskopie der ROOT CA zu erstellen!

## Schritt 5: Installieren des SUB CA Zertifikats

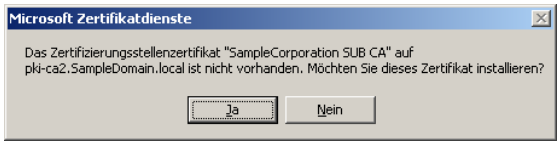
! Hinweis: Die folgenden Schritte werden auf dem Online SUB CA-Server durchgeführt!

Kopieren Sie zunächst das von der ROOT CA ausgestellte Zertifikat für die SUB CA auf den Server. Starten Sie dann die Zertifizierungsstellenkonsole. Die Zertifizierungsdienste sind derzeit auf Grund der unvollständigen Konfiguration gestoppt.

Starten Sie nun die Zertifikatsdienste.




Beim Start der Zertifikatsdienste werden Sie aufgefordert, das fehlende SUB CA-Zertifikat zu installieren. Klicken Sie hier auf „Ja“ und öffnen Sie dann die zuvor kopierte Zertifikatsdatei.




Gegebenenfalls müssen Sie auch das ROOT CA-Zertifikat installieren. Dieses befindet sich in <systemroot>\system32\CertSrv\CertEnroll und hat die Dateiendung .crt.

Nach Angabe der Zertifikate startet nun die SUB CA.

ⓘ Sollte die CA zu diesem Punkt nicht starten, so liegt höchstwahrscheinlich eine Fehlkonfiguration in den Distribution Points (CRL und AIA) der ROOT CA vor. In diesem Fall müssten Sie die Konfiguration der ROOT CA überprüfen und ggf. ändern. Das hätte allerdings auch zur Folge, dass für die SUB CA ein neues Zertifikat ausgestellt werden muss.

Nach dem Start der SUB CA beginnt die Replikation der Zertifikatsdienste ins Active Directory. So ist z.B. unter der Kategorie „Zertifikatsvorlagen“ vorerst eine Fehlermeldung zu sehen, die darauf hindeutet, dass die Replikation noch nicht abgeschlossen ist. Sie können die Replikation manuell anstoßen, indem Sie entweder den Server neu starten oder folgenden Befehl an der Konsole eingeben:

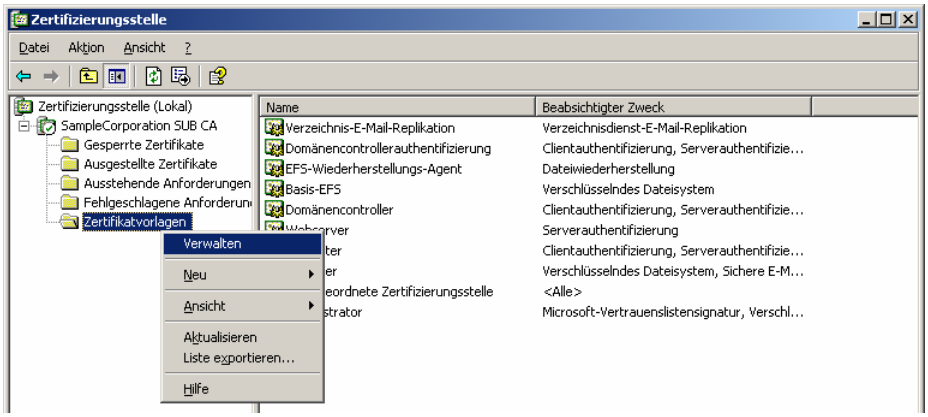
```
gpupdate /force /target:computer
```

# Verwenden der Zertifizierungsstelle

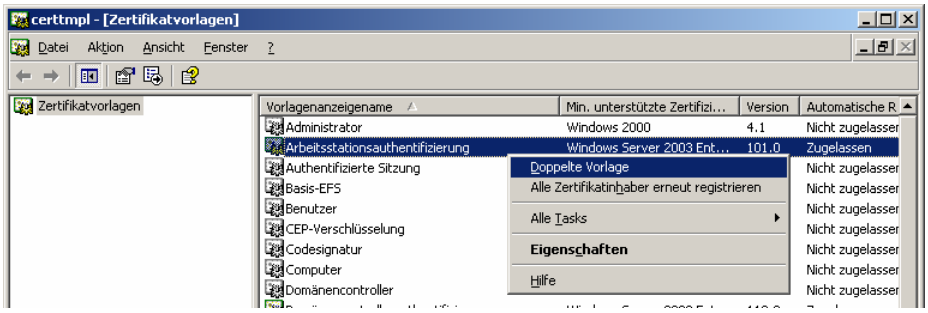
In diesem Kapitel soll nun noch die Verwendung der Zertifizierungsstelle gezeigt werden. Dazu erstellen wir eine neue Zertifikatsvorlage für Domänencomputer zu Clientauthentifizierungszwecken.

## *Erstellen einer neuen Zertifikatsvorlage*

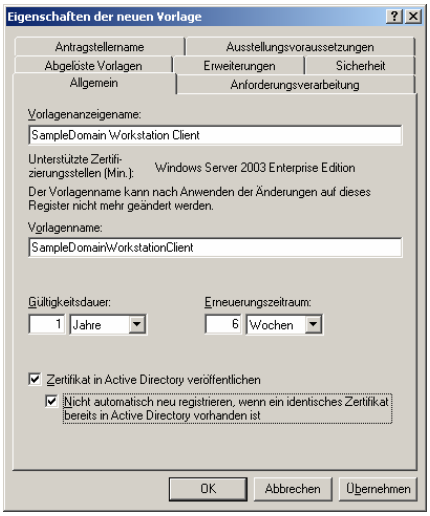
Zunächst muss eine neue Zertifikatsvorlage erstellt werden. Klicken Sie dazu in der Zertifizierungsstellenkonsole mit der rechten Maustaste auf den Bereich „Zertifikatvorlagen“ und wählen dann im Kontextmenü den Eintrag „Verwalten“.




Es öffnet sich nun eine neue Konsole, in der alle installierten Zertifikatsvorlagen verwaltet werden können. In unserem Beispiel wollen wir die bereits existierende Vorlage „Arbeitsstationsauthentifizierung“ als Basis heranziehen. Dazu klicken wir mit der rechten Maustaste auf diese Vorlage und wählen den Menüpunkt „Doppelte Vorlage“.

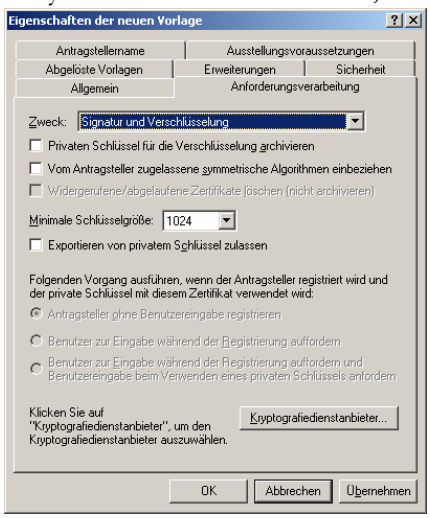



Im erscheinenden Dialog können nun in den einzelnen Reiterseiten die Zertifikatseigenschaften der Vorlage geändert werden.



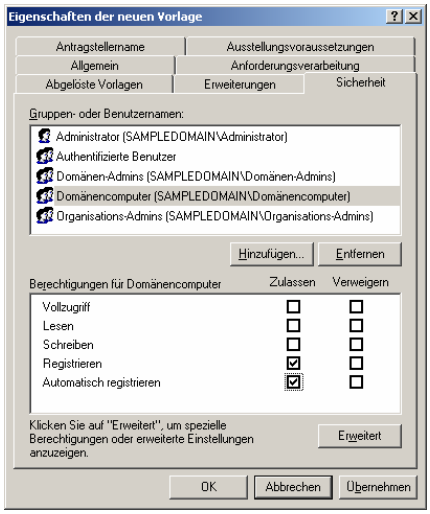

Zunächst wird auf der Reiterseite „Allgemein“ die allgemeinen Angaben zur Zertifikatsvorlage (dessen Anzeigename) sowie dessen Gültigkeitsdauer und Erneuerungszeitraum angegeben. Der Erneuerungszeitraum gibt an, in welcher Zeitspanne vor Ablauf der Gültigkeit die automatische Erneuerung des Zertifikats angestoßen werden soll.

Soll die Vorlage im Active Directory veröffentlicht werden, dann ist zudem die Option „Zertifikat in Active Directory veröffentlichen“ anzuwählen. Das Anwählen der Schaltfläche „Nicht automatisch neu registrieren, wenn ein identisches Zertifikat bereits in Active Directory vorhanden ist“ stellt sicher, dass eine Vorlage nur dann registriert wird, wenn nicht bereits eine gleiche Vorlage existiert.




In der Reiterseite „Anforderungsverarbeitung“ können Angaben zum Zweck des Zertifikats (Signatur- und / oder Verschlüsselung) definiert werden, sowie allgemeine kryptographische Einstellungen vorgenommen werden.

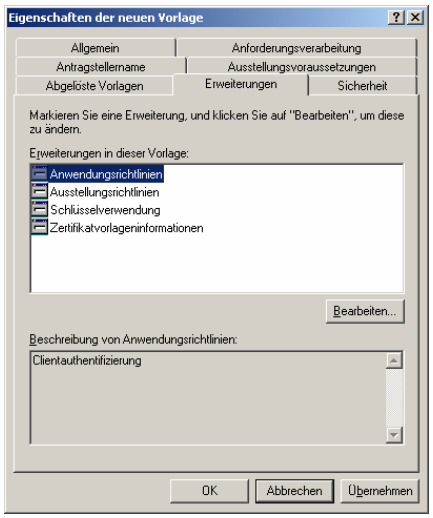
Die Sicherheitseinstellungen bezüglich der Zertifikate können auf der Reiterseite „Sicherheit“ eingestellt werden. Hier kann der Vorlage eine Access Control List hinterlegt werden, die einzelne Berechtigungen in der Zertifikatsverwendung durch Benutzer und Benutzergruppen regelt.




In unserem Beispiel wollen wir, dass Domänencomputer automatisch ein Zertifikat beantragen und installieren können.

Dazu ist es notwendig, der Benutzergruppe „Domänencomputer“ die Rechte „Registrieren“ und „Automatisch registrieren“ zu geben.

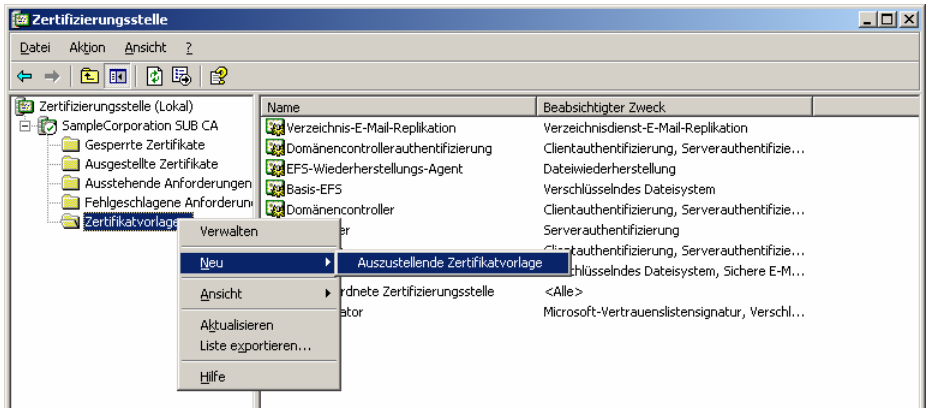
Mit Hilfe dieses Rechts können nun Computer in der Domäne automatisch ein entsprechendes Zertifikat von der CA anfordern und installieren.



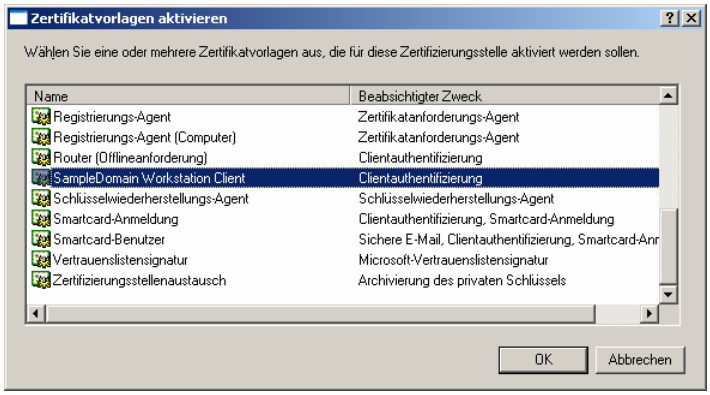

In der Reiterseite „Erweiterungen“ können die Verwendungszwecke des Zertifikats definiert werden. Die Verwendungszwecke sind hersteller-spezifische Nummern, die dann von den einzelnen Applikationen geprüft werden. Durch Klicken auf Anwendungsrichtlinien können einzelne Verwendungszwecke durch den Bearbeiten-Dialog verändert werden. Hier finden Sie eine Auflistung aller Verwendungszwecke der Microsoft Suite.

Die neue Zertifikatsvorlage wird durch das Klicken auf die Schaltfläche „Übernehmen“ und „OK“ gespeichert.

Um die Zertifikatsvorlage verwenden zu können, muss diese nun in der Zertifizierungsstellenkonsole aktiviert werden. Klicken Sie dazu mit der rechten Maustaste auf „Zertifikatsvorlagen“ und wählen Sie unter dem Menüpunkt „Neu“ den Eintrag „Auszustellende Zertifikatsvorlage“ aus.




Im nun erscheinenden Dialog können Sie die zuvor erstellte neue Zertifikatsvorlage auswählen und durch Klick auf OK aktivieren.



Die Verwendung der neuen Zertifikatsvorlage wird nun im Active Directory repliziert. Dies kann mitunter einige Zeit dauern. Es empfiehlt sich daher, die Replikation mit folgendem Befehl manuell anzustoßen.

```
gpupdate /force /target:computer
```

## *Prüfen der Ausstellung am Client*

Nachdem die Verwendung repliziert wurde, kann die automatische Verwendung am Client erfolgen. Dabei stellt der Client automatisch eine Zertifikatsanforderung und installiert das darauf erhaltene Zertifikat und die Zertifikate der CAs (ROOT und SUB).

Dieser Prozess ist wiederum Teil der Replikation durch das Active Directory. Auch hier empfiehlt es sich die Replikation manuell mit folgendem Befehl anzustoßen:

```
gpupdate /force /target:computer
```

Hinweis: Mitunter kann es sein, dass dieser Befehl öfters ausgeführt werden muss, da benötigte ROOT und SUB-CAs getrennt von der Verwendung der Zertifikatsvorlage repliziert werden müssen. In diesem Fall wiederholen Sie einfach den Befehl.

Nach erfolgreicher Replikation sollten Sie im Zertifikatsspeicher des Clientcomputer ein neues Zertifikat automatisch erhalten haben.