HP User Society
DECUS München e.V.

IT-Training Grote
Schulung & Consulting

Microsoft Windows Server System

Windows 2003 PKI: Einführung und Neuerungen

Referent: Marc Grote -
http://www.it-training-grote.de

Agenda

- **Bestandteile einer PKI**
- **Fachchinesisch I - IV**
- **CA-Hierarchien**
- **Windows 2003 PKI**
- **Einsatzgebiete**
- **GUI**
- **Featurities**
- **Zertifikatvorlagen**
- **Delta CRL**
- **Key Archiving and Recovery**
- **Administration**
- **CA-Konsole**
- **Certutil**
- **KRT.EXE**
- **Constraints**
- **Cross Certification**
- **Standard-Dateisuffixe**
- **Links**

Buchempfehlung

•*(nein, ich werde nicht für Werbung bezahlt)*

Was ist eine PKI?

Als Public-Key-Infrastruktur (PKI, engl.: public key infrastructure) bezeichnet man in der Kryptologie und Kryptografie ein System, welches es ermöglicht, digitale Zertifikate auszustellen, zu verteilen und zu prüfen. Die innerhalb einer PKI ausgestellten Zertifikate sind meist auf Personen oder Maschinen festgelegt und werden zur Absicherung computergestützter Kommunikation verwendet.

Quelle: http://de.wikipedia.org/wiki/PKI

Bestandteile einer PKI

Wesentliche Bestandteile einer (minimalen) PKI sind:

Digitale Zertifikate:
Digital signierte elektronische Daten, die sich zum Nachweis der Echtheit von Objekten verwenden lassen.

Certification Authority:
Organisation, welche die Bereitstellung von Zertifikaten übernimmt.

Registration Authority:
Organisation, bei der Personen und Maschinen Zertifikate beantragen können.

Certificate Revocation Lists:
(Sperrliste) Listen mit zurückgezogenen, abgelaufenen und für ungültig erklärten Zertifikaten.

Verzeichnisdienst:
Ein durchsuchbares Verzeichnis welches ausgestellte Zertifikate enthält, meist ein LDAP-Server, seltener ein X.500-Server.

Validierungsdienst:
Ein Dienst, der die Überprüfung von Zertifikaten in Echtzeit ermöglicht.

Fachchinesisch I

Application Constraints
A constraint that limits what purposes a certificate can be used for in a qualified subordination configuration. A presented certificate must contain the required application constraint to be accepted by the partner organization.

Authority Information Access (AIA)
A certificate extension that contains URL locations where the issuing CAs certificate can be retrieved. The AIA extension can contain HTTP, FTP, LDAP or FILE URLs.

Authority Key Identifier (AKI)
A certificate extension used by the certificate chaining engine to determine what certificate was used to sign a presented certificate. The AKI can contain the issuer name and serial number, public key information, or no information at all. By matching the information in a certificates AKI extension to a CA certificates Subject Key Identifier (SKI) extension, a certificate chain can be built.

Fachchinesisch II

CaPolicy.inf
A configuration file stored in the %SystemRoot% folder that defines Configuration settings for CAs when they are installed and when the CAs certificate is renewed.

CRL Distribution Point (CDP)
A certificate extension that indicates where the certificate revocation list for a CA can be retrieved. This extension can contain multiple HTTP, FTP, File, or LDAP URLs for the retrieval of the CRL.

Certificate Trust List (CTL)
A method of restricting certificates chaining to a designated CA for limited time periods or usages. It is used more prevalently in a Windows 2000 network. In a Windows Server 2003 environment, qualified subordination is the preferred method for restricting certificate usage between organizations.

Fachchinesisch III

Certificate Revocation List (CRL)

A digitally signed list issued by a CA that contains a list of certificates issued by the CA that have been revoked. The listing includes the serial number of the certificate, the date that the certificate was revoked, and the revocation Reason Applications can perform CRL checking to determine a presented Certificates revocation status

.

Cross-Certification

The process of issuing subordinate CA certificates for existing CAs that link two root CAs. Cross-Certification Authority Certificate A certificate issued by one CA for another CA's signing key pair (that is, for another CA's public verification key).

Issuance Policy

Constraint A constraint that defines what issuance practices must be followed for certificates to be trusted by your organization. Issuance policy object identifiers (OIDs) in your organization are mapped to the matching object identifiers in a partner organization, so that object identifiers in presented certificates are recognized by your PKI.

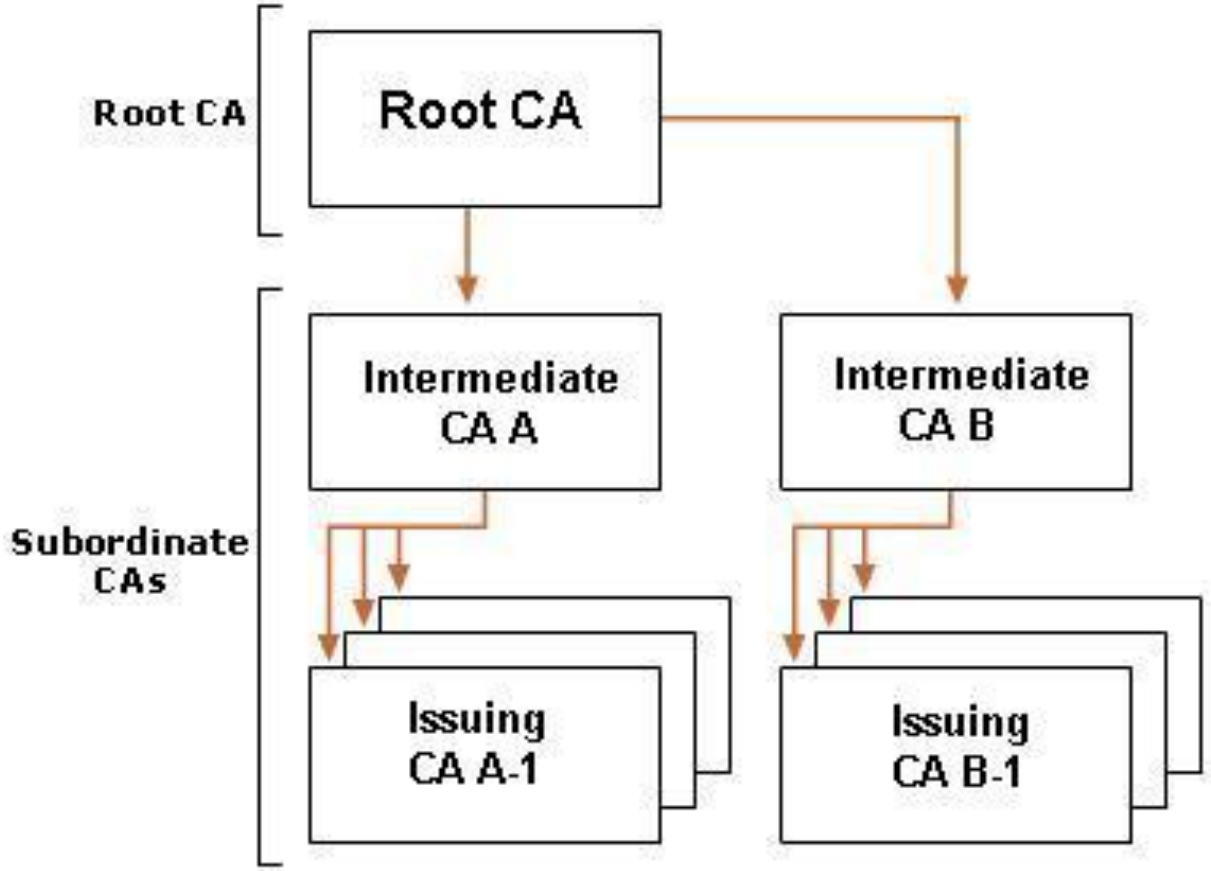
Fachchinesisch IV

Policy.inf
A configuration file that defines the constraints that are applied to a CA certificate when qualified subordination is defined.

Public Key Infrastructure (PKI)
A PKI provides an organization with the ability to securely exchange data over a public network using public-key cryptography. A PKI consists of CAs that issue digital certificates, directories that store the certificates (including Active Directory in Windows 2000 and Windows Server 2003), and X.509 certificates that are issued to security entities on the network. The PKI provides validation of certificate-based credentials and ensures that the credentials are not revoked, corrupted, or modified.

Qualified Subordination
The process of configuring cross-certification with basic constraints, name constraints, application constraints, and issuance policy constraints to govern what certificates are trusted from a partner organization.

CA-Hierarchien



Windows 2003 PKI

- Windows Server 2003 Standard
  - Alle Basisfunktionen einer Windows 2000 PKI
- Windows 2003 Enterprise und Datacenter
  - Alle Funktionen der Windows 2003 Standard PKI
  - Key Archiving and Recovery
  - V2 Certificate Templates
  - Role Separation (ISIS-MTT)

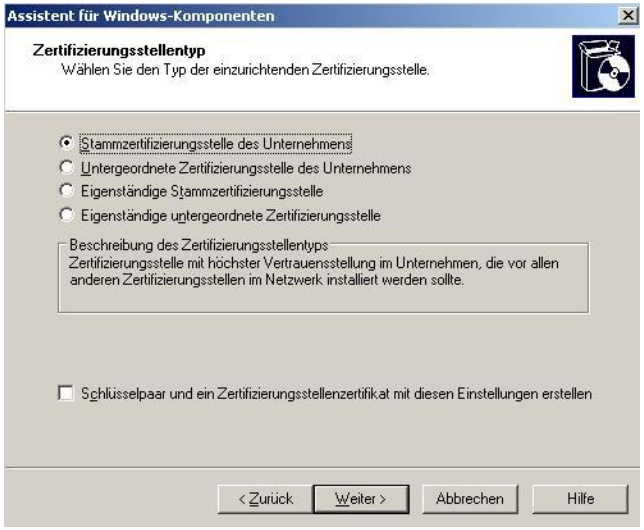
Einsatzgebiete

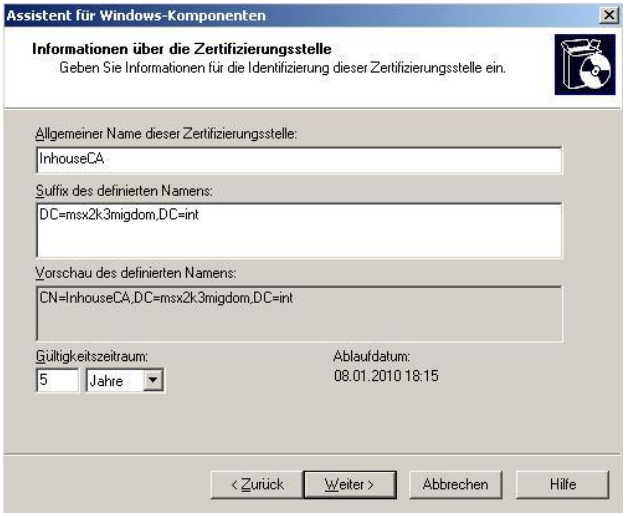
- **Smartcards**
- **X.509 Zertifikate**
- **Kerberos**
- **Token basierende Authentifizierungsmechanismen**
- **IPSec**
- **PPTP**
- **L2TP/IPSec**
- **SSL**
- **TLS**
- **EFS**
- **Code Signierung**

Windows 2003 CA-Arten

- Stammzertifizierungsstelle des Unternehmens
- Untergeordnete Zertifizierungsstelle des Unternehmens
- Eigenständige Stammzertifizierungsstelle
- Eigenständige untergeordnete Zertifizierungsstelle

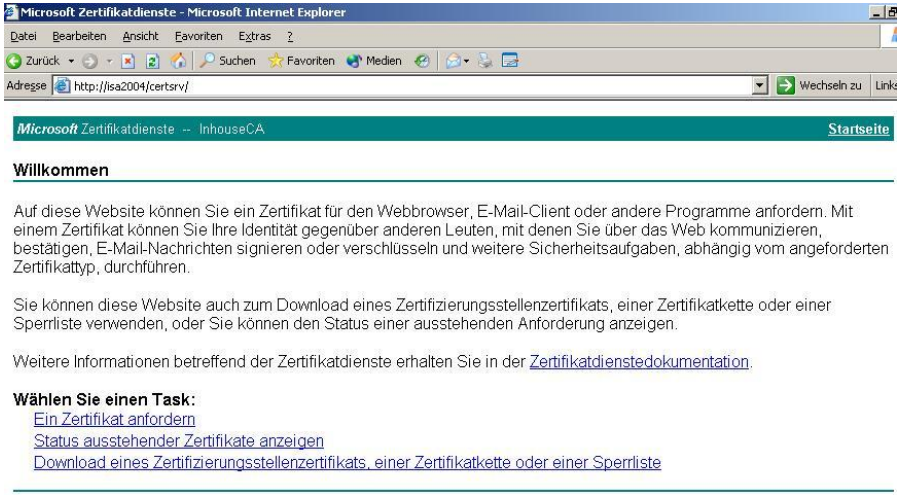
GUI


Assistent für Windows-Komponenten
Zertifizierungsstellentyp
Wählen Sie den Typ der einzurichtenden Zertifizierungsstelle.
Stammzertifizierungsstelle des Unternehmens
Untergeordnete Zertifizierungsstelle des Unternehmens
Eigenständige Stammzertifizierungsstelle
Eigenständige untergeordnete Zertifizierungsstelle
Beschreibung des Zertifizierungsstellentyps
Zertifizierungsstelle mit höchster Vertrauensstellung im Unternehmen, die vor allen anderen Zertifizierungsstellen im Netzwerk installiert werden sollte.
Schlüsselpaar und ein Zertifizierungsstellenzertifikat mit diesen Einstellungen erstellen
< Zurück
Weiter >
Abbrechen
Hilfe


Assistent für Windows-Komponenten
Informationen über die Zertifizierungsstelle
Geben Sie Informationen für die Identifizierung dieser Zertifizierungsstelle ein.
Allgemeiner Name dieser Zertifizierungsstelle:
InhouseCA
Suffix des definierten Namens:
DC=msx2k3migdom,DC=int
Vorschau des definierten Namens:
CN=InhouseCA,DC=msx2k3migdom,DC=int
Gültigkeitszeitraum:
5
Jahre
Ablaufdatum:
08.01.2010 18:15
< Zurück
Weiter >
Abbrechen
Hilfe


Zertifizierungsstelle
Datei Aktion Ansicht ?
Zertifizierungsstelle (Lokal)
InhouseCA
Gesperrte Zertifikate
Ausgestellte Zertifikate
Ausstehende Anforderungen
Fehlgeschlagene Anforderung
Zertifikatvorlagen
Name
Beabsichtigter Zweck
EFS-Wiederherstellungs-Agent
Dateiwiederherstellung
Basis-EFS
Verschlüsselndes Dateisystem
Domänencontroller
Clientauthentifizierung, Serverauthentifizierung
Webserver
Serverauthentifizierung
Computer
Clientauthentifizierung, Serverauthentifizierung
Benutzer
Verschlüsselndes Dateisystem, Sichere E-Mail, Clientauthentifizierung
Untergeordnete Zertifizierungsstelle
<Alle>
Administrator
Microsoft-Vertrauenslistensignatur, Verschlüsselndes Dateisystem, Sichere E-Mail, Clientauthe

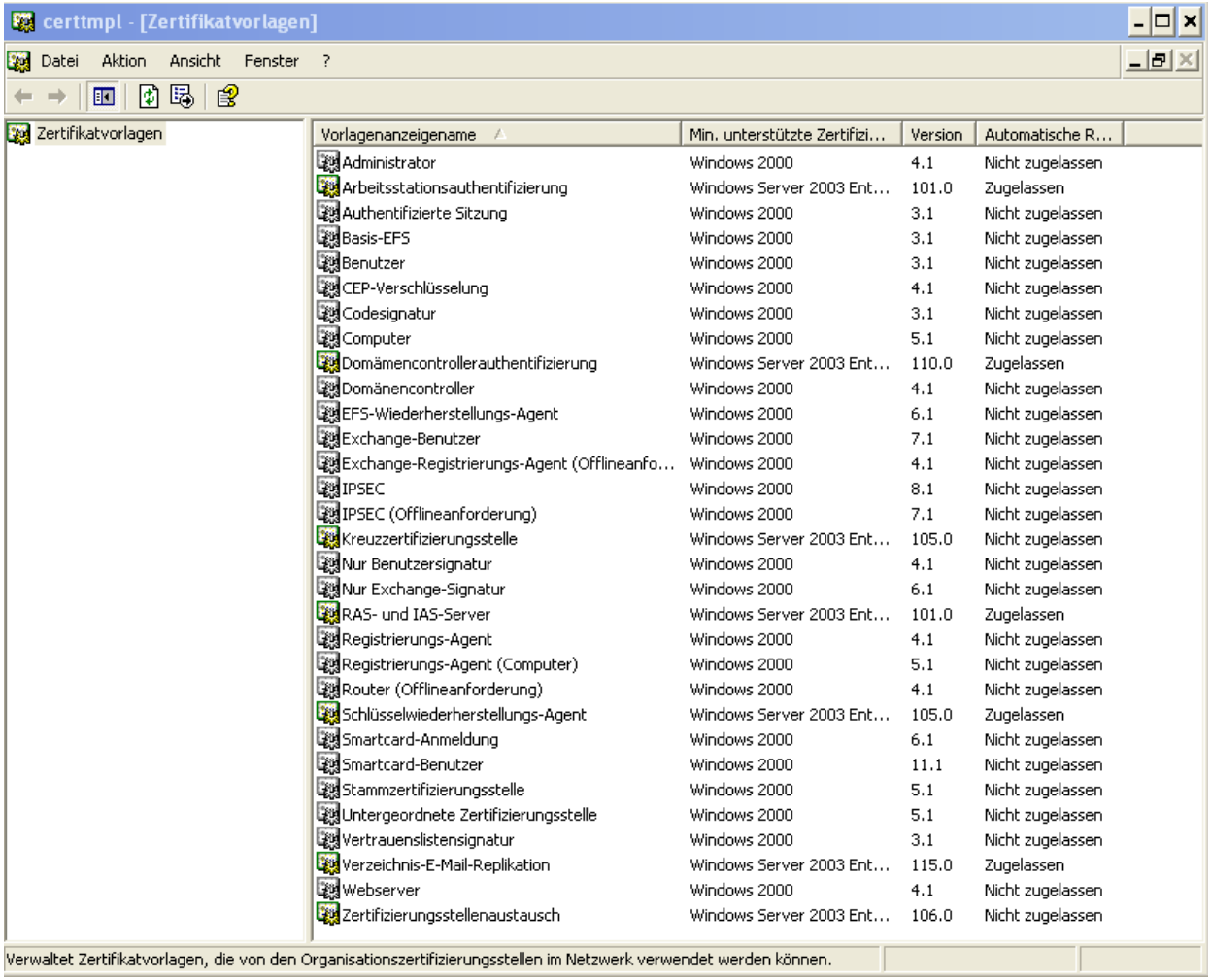

Assistent für Windows-Komponenten
Einstellungen der Zertifikatdatenbank
Geben Sie Pfade für die Zertifikatdatenbank, das Datenbankprotokoll und Konfigurationsinformationen ein.
Zertifikatdatenbank:
C:\WINDOWS\system32\CertLog
Durchsuchen...
Zertifikatdatenbankprotokoll:
C:\WINDOWS\system32\CertLog
Durchsuchen...
Konfigurationsinformationen in einem freigegebenen Ordner speichern
Freigegebener Ordner:
Durchsuchen...
Vorhandene Zertifikatdatenbank nicht löschen
< Zurück
Weiter >
Abbrechen
Hilfe


Microsoft Zertifikatdienste - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Favoriten
Medien
Adresse
http://lisa2004/certsrv/
Wechseln zu
Microsoft Zertifikatdienste -- InhouseCA
Startseite
Willkommen
Auf diese Website können Sie ein Zertifikat für den Webbrowser, E-Mail-Client oder andere Programme anfordern. Mit einem Zertifikat können Sie Ihre Identität gegenüber anderen Leuten, mit denen Sie über das Web kommunizieren, bestätigen, E-Mail-Nachrichten signieren oder verschlüsseln und weitere Sicherheitsaufgaben, abhängig vom angeforderten Zertifikattyp, durchführen.
Sie können diese Website auch zum Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Sperrliste verwenden, oder Sie können den Status einer ausstehenden Anforderung anzeigen.
Weitere Informationen betreffend der Zertifikatdienste erhalten Sie in der Zertifikatdienstedokumentation.
Wählen Sie einen Task:
Ein Zertifikat anfordern
Status ausstehender Zertifikate anzeigen
Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Sperrliste

Featurities

- **Full PKI cross-certification**
- **Name constraints, policy constraints, and policy mapping**
- **Delta certificate revocation lists (CRLs)**
- **Bridge certificate authority (CA) configurations**
- **Delegated policy administration**
- **Unified user management through Microsoft Active Directory**
- **Increased Kerberos performance**
- **Automatic user enrollment for PKI certificates**
- **Streamlined access control list (ACL) evaluation**
- **Simplified authorization framework and ACL editor**
- **New credential manager for secure multiple identities**
- **Smart card support for administrators**
- **Extensible authentication protocol (EAP) for standard 802.11 wireless networking**
- **Integrated PKI key archival and recovery tools**
- **Encrypting offline files (client-side cache)**

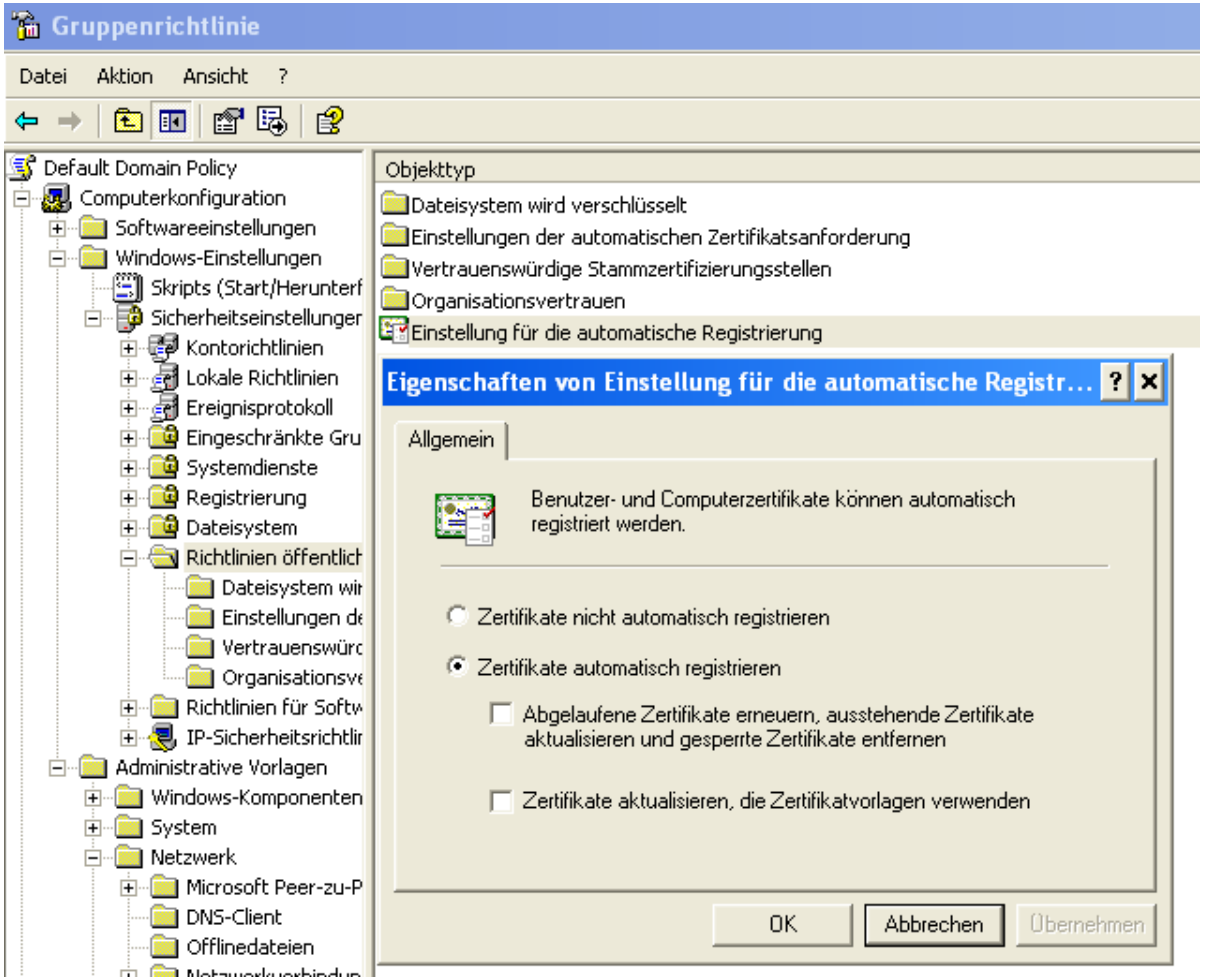
Zertifikatvorlagen



Autoenrollment I

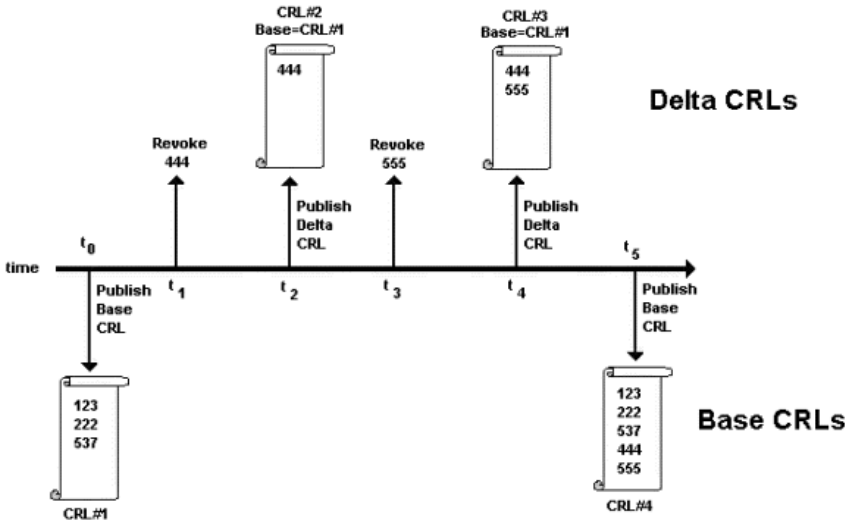
- Zertifikate werden automatisch mit Hilfe von Gruppenrichtlinien auf die Clients „ausgerollt“
- Anpassung der Zertifikatsvorlagen + Berechtigungen + GPO Einstellung
- Windows 2000 CA
  - Nur für Computer
- Windows 2003 CA
  - Computer und Benutzer (Windows XP)

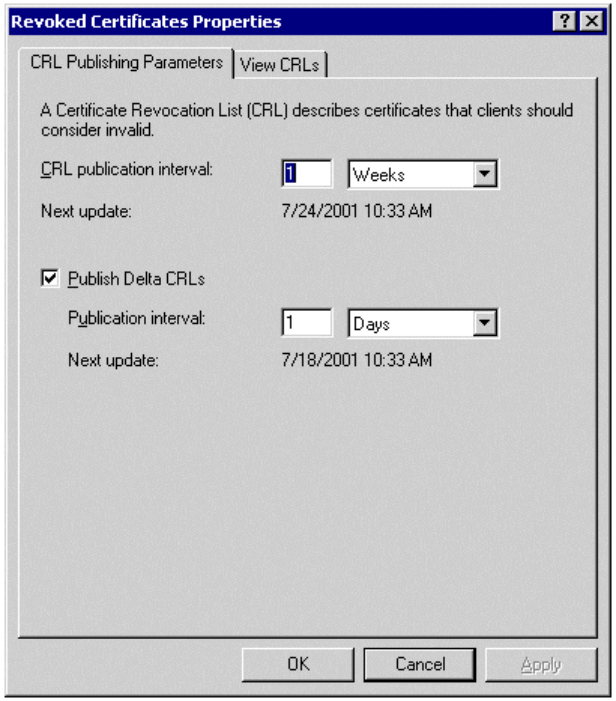
Autoenrollment II



Delta CRL

- Übertragung nur der letzten Änderungen einer CRL – Certificate Revocation List

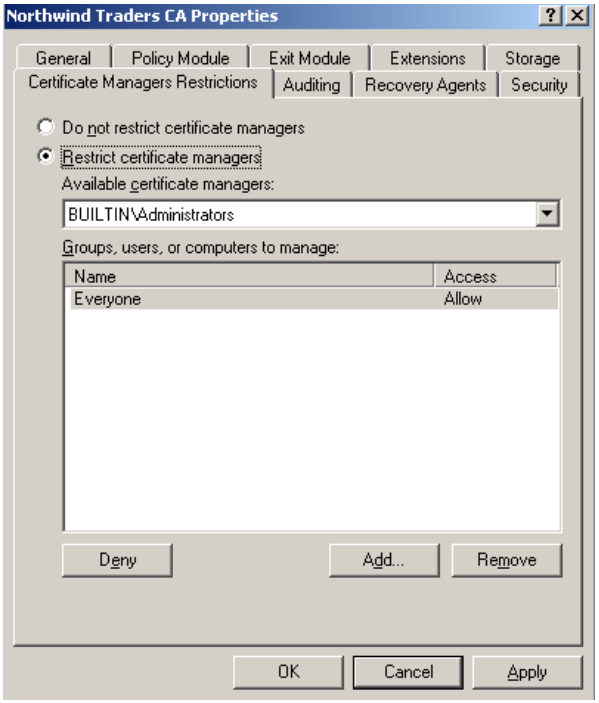


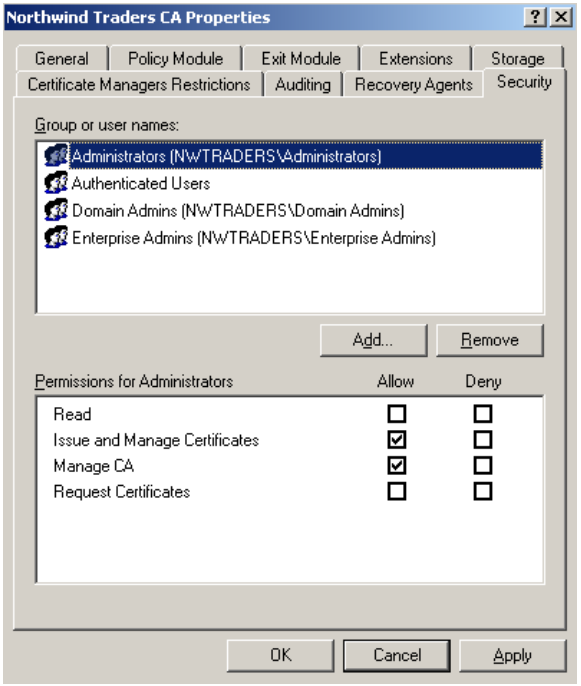


Key Archiving and Recovery

- CA muss für Key Archiving aktiviert werden
- KRA – Key Recovery Agent Certificate muss ausgerollt werden
- 4-Augen Prinzip möglich
- Zertifikatsvorlagen müssen für Key Archiving eingerichtet sein
- Recovery mit KRT.EXE oder CERTUTIL.EXE

Role Separation





ISIS-MTT:

http://support.microsoft.com/default.aspx?scid=kb;en-us;890772

```
C:\Documents and Settings\Administrator>certutil -setreg ca\setroleseparartionenabled 1
SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Northwind Traders CA\setroleseparartionen

New Value:
  setroleseparartionenabled REG_DWORD = 1
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.

C:\Documents and Settings\Administrator>
```

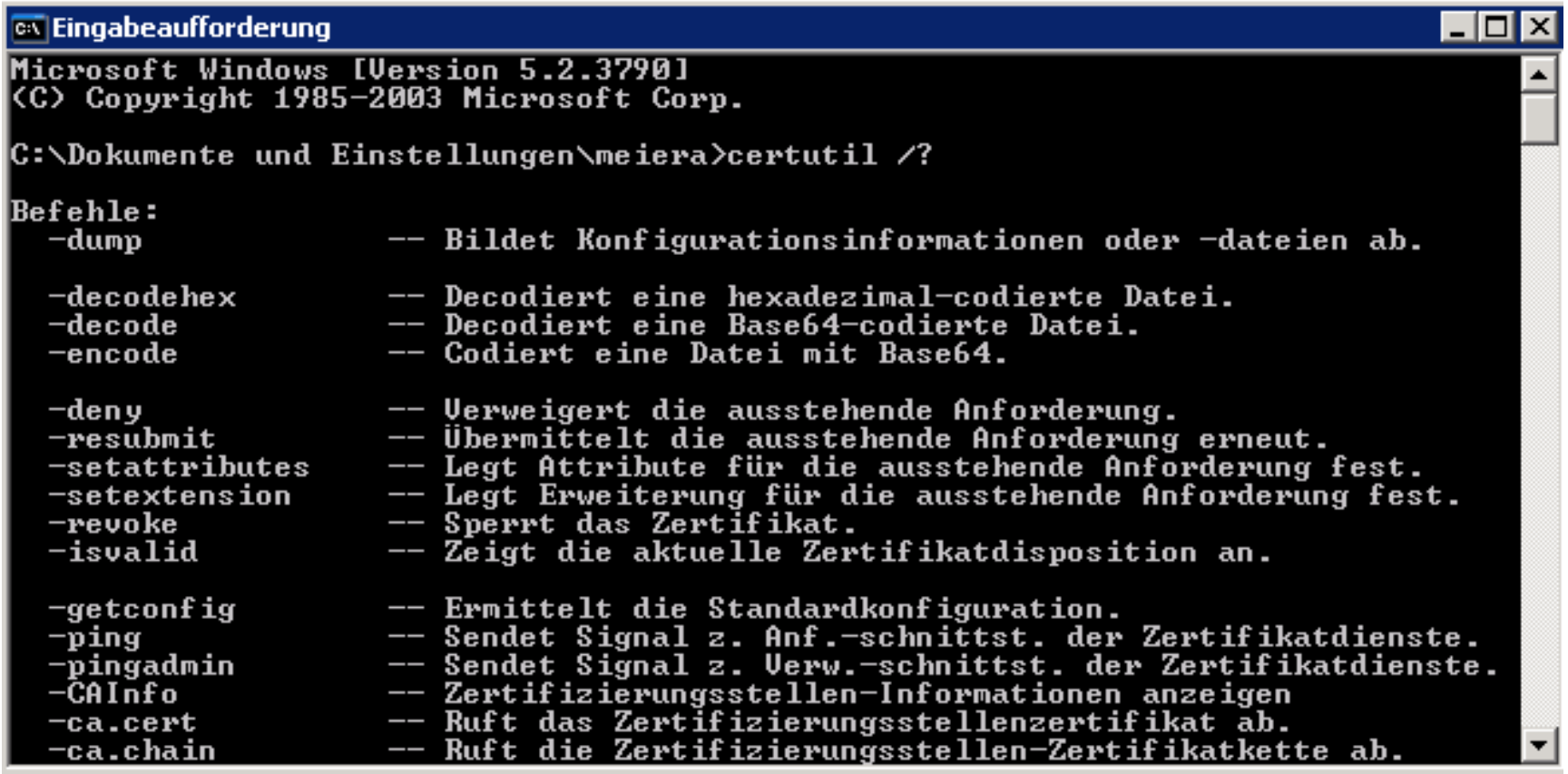
Administration

- CA-Konsole
- Certutil /? (viele viele Befehle mit schwarzem Hintergrund)
- Webkonsole (http://caserver/certsrv)
- PKIview.msc (CA Health, W2K3 Reskit)
- KRT.EXE (Key Recovery, W2K3 Reskit)
- Policy.inf + CAPolicy.inf

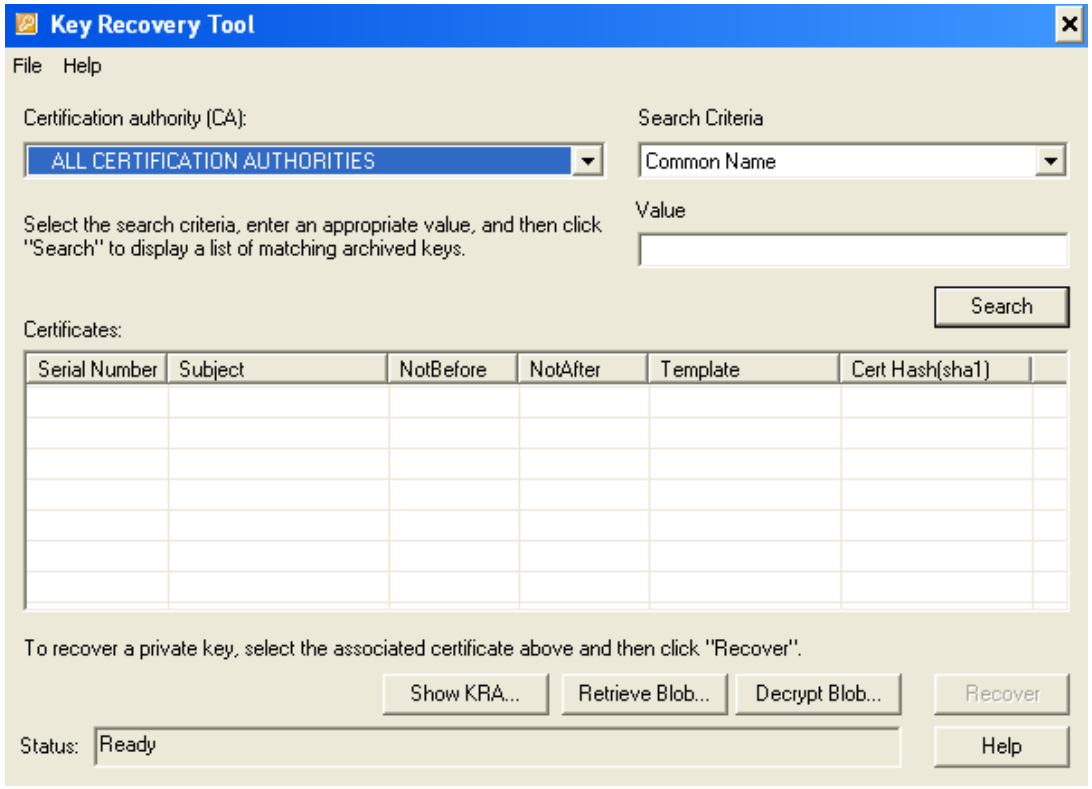
CA-Konsole


Zertifizierungsstelle
Datei
Aktion
Ansicht
?
Zertifizierungsstelle
Zertifizierungsstelle
Gesperrte Zertifikate
Ausgestellte Zertifikate
Ausstehende Anforderungen
Fehlgeschlagene Anforderung
Zertifikatsvorlagen
Name
Beabsichtigter Zweck
Exchange-Benutzer
Sichere E-Mail
EFS-Wiederherstellungs-Agent
Dateiwiederherstellung
Basis-EFS
Verschlüsselndes Dateisystem
Domänencontroller
Clientauthentifizierung, Serverauthentifizierung
Webserver
Serverauthentifizierung
Computer
Clientauthentifizierung, Serverauthentifizierung
Benutzer
Verschlüsselndes Dateisystem, Sichere E-Mail, Clientauthentifizierung
Untergeordnete Zertifizierungsstelle
<Alle>
Administrator
Microsoft Vertrauenslistensignatur, Verschlüsselndes Dateisystem, Sic

Certutil

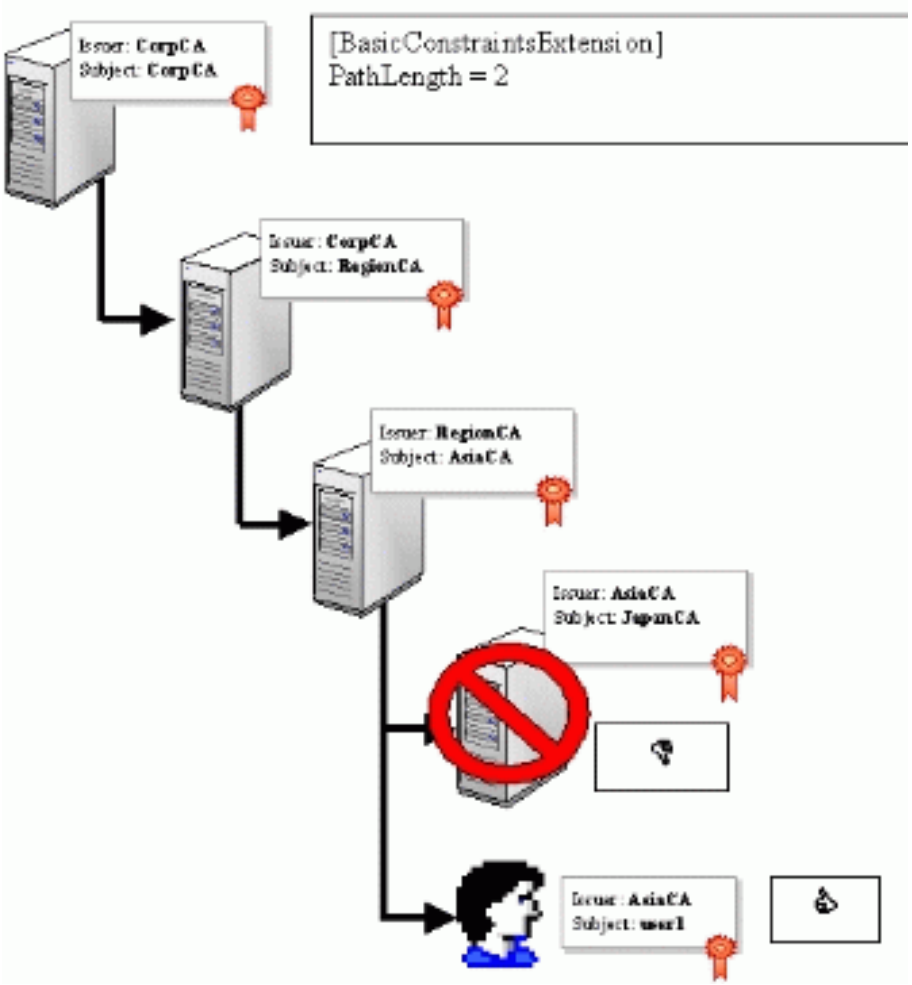

Eingabeaufforderung
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\Dokumente und Einstellungen\meiera>certutil /?
Befehle:
-dump -- Bildet Konfigurationsinformationen oder -dateien ab.
-decodehex -- Decodiert eine hexadezimal-codierte Datei.
-decode -- Decodiert eine Base64-codierte Datei.
-encode -- Codiert eine Datei mit Base64.
-deny -- Verweigert die ausstehende Anforderung.
-resubmit -- Übermittelt die ausstehende Anforderung erneut.
-setattributes -- Legt Attribute für die ausstehende Anforderung fest.
-setextension -- Legt Erweiterung für die ausstehende Anforderung fest.
-revoke -- Sperrt das Zertifikat.
-isvalid -- Zeigt die aktuelle Zertifikatdisposition an.
-getconfig -- Ermittelt die Standardkonfiguration.
-ping -- Sendet Signal z. Anf.-schnittst. der Zertifikatdienste.
-pingadmin -- Sendet Signal z. Verw.-schnittst. der Zertifikatdienste.
-CAInfo -- Zertifizierungsstellen-Informationen anzeigen
-ca.cert -- Ruft das Zertifizierungsstellenzertifikat ab.
-ca.chain -- Ruft die Zertifizierungsstellen-Zertifikatkette ab.

KRT.EXE



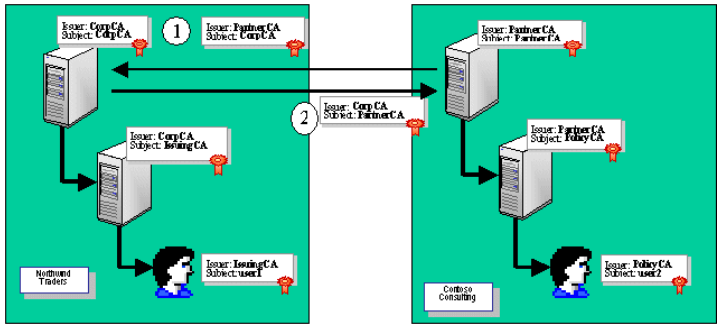
Achtung bei deutscher CA !! Und Dllcache ☺

Constraints



Cross Certification

- Vertrauensstellung zwischen CAs
  - Cross CA
  - Bridge CA



Standard-Dateisuffixe

Schlüssel	Beschreibung
PKCS #12	**Privater Informationsaustausch**
.PFX	**Privater Informationsaustausch**
.P12	**Privater Informationsaustausch**
PKCS #7	**Syntaxstandard kryptografischer Meldungen**
.P7B	**Syntaxstandard kryptografischer Meldungen**
.SST	**Microsoft serieller Zertifikatsspeicher**
.CER	**DER-kodiert-binär X.509** **Base-64-codiert-X.509**
.PFX	**Privater Informationsaustausch PKCS #12**
.CRL	**Certification Revocation List**
.P7C	**Digitale ID-Datei**
.P7M	**PKCS #7 MIME-Nachricht**
.P7R	**PKCS #7 Zertifikat**
.P7S	**PKCS #7 Signatur**

Lust auf Links?

- http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx
- http://www.it-training-grote.de/download/w2kmag-pki-092004.pdf
- http://www.microsoft.com/technet/prodtechnol/winxppro/plan/pkienh.mspx
- http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/advcert.mspx
- http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/advcert.mspx
- http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/ws3PKIBP.asp
- http://www.microsoft.com/technet/prodtechnol/windowsserver2003/maintain/operate/ws03pkog.asp?frame=true
- http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspx
- http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspx
- http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/mngpki.mspx
- http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/kyacws03.mspx
- http://www.msisafaq.de/Anleitungen/2004/Konfiguration/Zertifikate.htm

The End?

Vielen Dank für Ihre Aufmerksamkeit