DÖRES.

Döres AG
Stolberger Straße 78
50933 Köln

Telefon: 0221-95 44 85-0
Telefax: 0221-95 44 85-80
Internet: www.doeres.com

PKI-Lösungen in Windows-Netzwerken

DÖRES.

Agenda:

I. Grundsätzliches zur Thema Windows PKI:

- Vorstellung einer „privaten“ Beispiel-PKI
- Diskussion „öffentliche“ vs. „private“ PKI
- Einführung in PKI unter Windows 2000

II. Notwendige Vorüberlegungen:

- Praktische Verwendungsmöglichkeiten von Zertifikaten
- Implementierung von Stand-Alone oder Enterprise *Certification Authorities* (CA)
- Mögliche Strukturen (Root CA, Online/Offline), CA Platzierung und Certificate Hierarchy

DÖRES.

Agenda:

III. Praktischer Umgang mit…

- *Certificate Revocation List Distribution Point* (CDP) und *Authority Information Access* (AIA) bei Offline Root CAs
- *Active Directory* Berechtigungen und *Access Control Lists* (ACL)
- *Microsoft Management Console* (MMC) und *Web Interface* für Certificate Services
- Zusatzprodukten anderer Hersteller

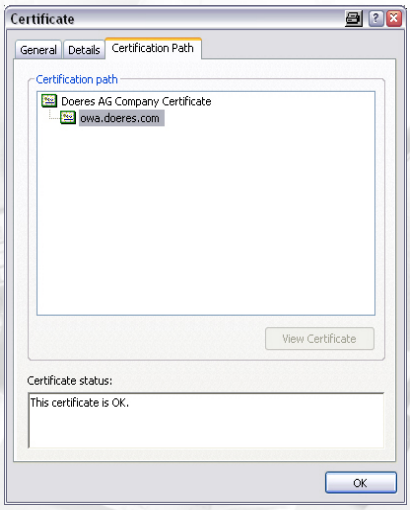
IV. Neuigkeiten und Änderungen in Windows 2003 Domänen mit XP Clients

DÖRES.

Eine Public Key Infrastruktur basiert…

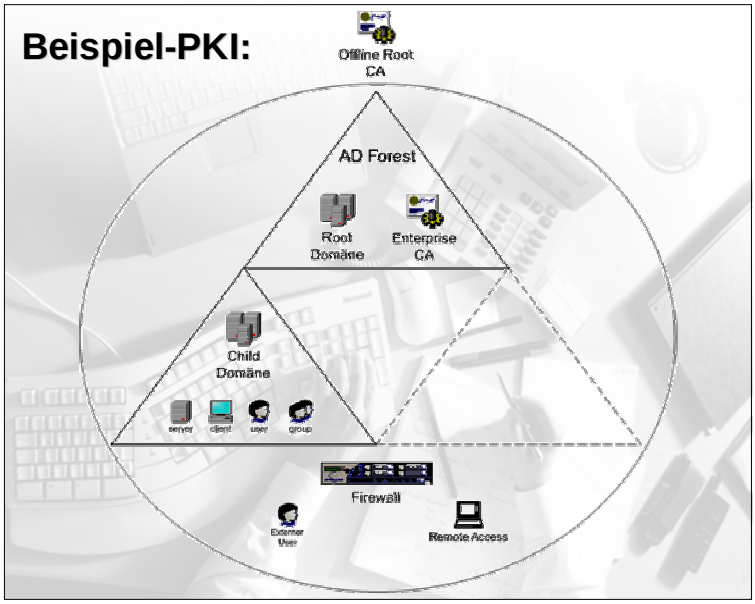
… auf X.509 Zertifikaten

… auf Trust-Hierarchien



DÖRES.

Beispiel-PKI:



3A04 Windows PKI
10.04.03 – Alexius/Lorenz

DÖRES.

Die öffentliche PKI:

Vorteile:

- Die CA ist international anerkannt
- Das Root Zertifikat ist in Betriebssystemen und Browsern enthalten

Nachteile:

- Die Zertifikate sind kostenpflichtig
- Die Signierung der firmeneigenen ausstellenden CA ist mit hohem Kosten verbunden.

DÖRES.

Die private PKI:

- Wird primär organisationsintern eingesetzt

Vorteile:

- Ist kostengünstig
- Bietet stärkere Kontrolle über den Verwendungszweck und die Verbreitung der Zertifikate

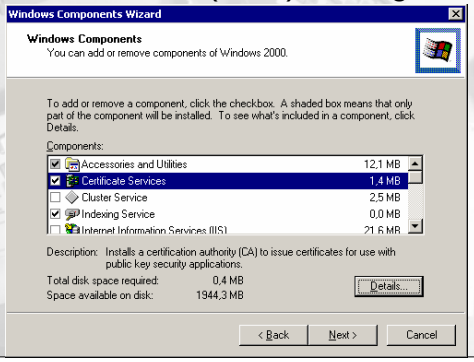
Nachteile:

- Das Root Zertifikat muss bekannt gemacht werden

DÖRES.

In Windows 2000 Server sind die Mittel zum PKI-Aufbau enthalten…

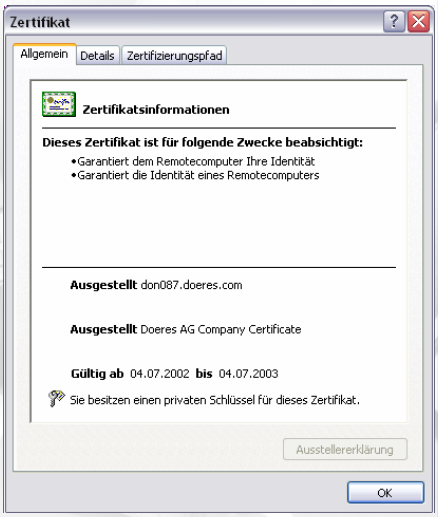
- Standard X.500 Zertifikate werden genutzt
- Eine Integration in Active Directory und in Exchange Server 2000 (KMS) ist möglich



DÖRES.

Einsatzmöglichkeiten von Basis-Zertfikaten:

- Web Server
- Code Signing
- Computer
- User
- S/MIME
- IPSec
- Subordinate CA



3A04 Windows PKI
10.04.03 – Alexius/Lorenz

DÖRES.

Einsatzmöglichkeiten von erweiterten Zertfikaten (AD):

- SmartCard
- EFS (Recovery)
- Domain Controller
- IPSec (online)

Grundsätzliches
Eine Beispiel-PKI
Öffentlich <> Privat
PKI in Windows

Vorüberlegungen
- Wofür Zertifikate?
CA-Modelle
Platzierung/Struktur

Die Praxis
CDP/AIA-Pfade
AD-Berechtigungen /ACLs
Management-GUIs
Drittthersteller?

Evolution
Windows Server 2003/XP Client

Q&A

DÖRES.

Die Online Stand-Alone CA:
(Stand-Alone Server)

- Wird primär im Extra- und Internet eingesetzt
- Benötigt kein Active Directory

- Das Root Zertifikat muss in der Organisation bekannt gemacht werden
- Es ist kein SmartCard Logon realisierbar
- Certificate Templates sind nicht verfügbar
- Die automatische Zertifikatsausstellung ist nicht möglich

3A04 Windows PKI
10.04.03 – Alexius/Lorenz

DÖRES.

Die Online Stand-Alone CA:
(Member Server)

- Das Root Zertifikat wird in der AD Domäne automatisch verteilt
- Die *Certificate Revocation List* (CRL) wird im Active Directory publiziert
(als Member der AD Root Domäne)

Grundsätzliches
Eine Beispiel-PKI
Öffentlich <> Privat
PKI in Windows

Vorüberlegungen
Wofür Zertifikate?
• CA-Modelle
Platzierung/Struktur

Die Praxis
CDP/AIA-Pfade
AD-Berechtigungen /ACLs
Management-GUIs
Dritthersteller?

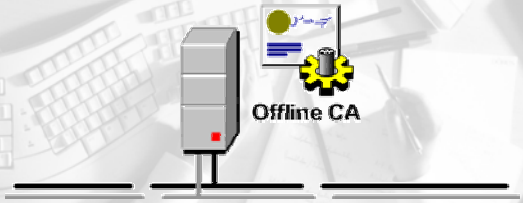
Evolution
Windows Server 2003/XP Client

Q&A

DÖRES.

Die Offline Stand-Alone CA:

- Ist eine Stand-Alone CA, die nie am Netz angeschlossen ist
- Wird für Root CAs empfohlen



3A04 Windows PKI
10.04.03 – Alexius/Lorenz

DÖRES.

Die Enterprise CA:

- Benötigt ein Active Directory
- Ermöglicht volle Active Directory Integration
- Das Root Zertifikat wird automatisch publiziert
- Requests werden an Hand von Policies (automatisiert) abgearbeitet
- Es werden Default-Zertifikatsvorlagen verwendet
- Ein Windows 2000 SmartCard Logon kann realisiert werden

Grundsätzliches
Eine Beispiel-PKI
Öffentlich <> Privat
PKI in Windows

Vorüberlegungen
Wofür Zertifikate?
CA-Modelle
Platzierung/Struktur

Die Praxis
CDP/AIA-Pfade
AD-Berechtigungen /ACLs
Management-GUIs
Dritthersteller?

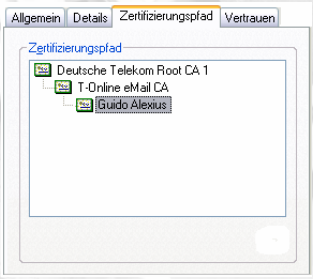
Evolution
Windows Server 2003/XP Client

Q&A

DÖRES.

Die Certificate Hierarchy:

- **Root CA**
  - Untergeordnete (subordinate) CA (Organisatorisch/ Geografisch)
    - Subordinate CA (Organisatorisch/Geografisch)
      - Ausstellende (Issuing) CA
      - Zertifikat



3A04 Windows PKI
10.04.03 – Alexius/Lorenz

DÖRES.

Platzierung der Root CA:

Mögliche Alternativen:

- Enterprise Root CA
- Stand-Alone Root CA
- Offline Root CA (Stand-Alone oder Extern)

Grundsätzliches
Eine Beispiel-PKI
Öffentlich <> Privat
PKI in Windows

Vorüberlegungen
Wofür Zertifikate?
CA-Modelle
Platzierung/Struktur

Die Praxis
CDP/AIA-Pfade
AD-Berechtigungen /ACLs
Management-GUIs
Drittthersteller?

Evolution
Windows Server 2003/XP Client

Q&A

DÖRES.

Überlegungen zur Struktur:

Sicherheitsaspekte:

- Offline Root CA und Online Subordinate
- Online Root und Online Subordinate
- Einfache Online CA (Root und Issuing)

Organisatorische Gegebenheiten:

- Subordinate CAs für Organisationseinheiten
- Unterschiedliche Zertifikatsrichtlinien (Policies)

Geografische Gegebenheiten:

- Subordinate CAs für verschiedene Standorte

3A04 Windows PKI
10.04.03 – Alexius/Lorenz

DÖRES.

Überlegungen zur Struktur:

Active Directory Gesichtspunkte:

- Offline Root CA und Online Enterprise
- Online CA in der Root Domäne
- Online CA in der Root Domäne und Issuing CA in der (den) Child Domäne(n)
- Online CA in der Child Domäne

Kostenbetrachtungen:

- Hardware
- Administration

Grundsätzliches
Eine Beispiel-PKI
Öffentlich <> Privat
PKI in Windows
Vorüberlegungen
Wofür Zertifikate?
CA-Modelle
• Platzierung/Struktur
Die Praxis
CDP/AIA-Pfade
AD-Berechtigungen /ACLs
Management-GUIs
Dritthersteller?
Evolution
Windows Server 2003/XP Client
Q&A

DÖRES.

Design-Beispiel:

Anforderungen:

- Hohe Sicherheit
- AD Integration
- User und Gruppenzertifikate
- Code Signing Zertifikate
- Automatische DC und Server Zertifikate
- Automatische IPSec Zertifikate
- Offline IPSec Zertifikate für Firewall und VPN

3A04 Windows PKI
10.04.03 – Alexius/Lorenz

DÖRES.

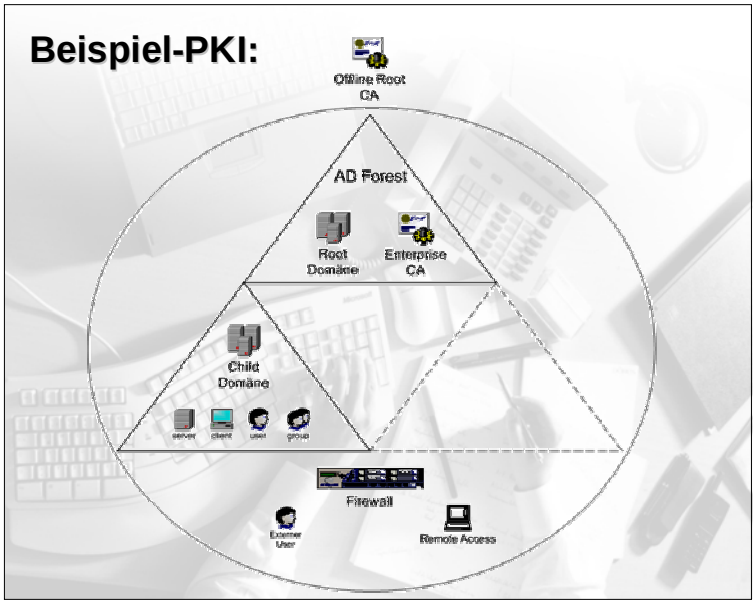
Design-Beispiel:

Verwendungszwecke:

- SmartCard Logon
- Makro Signierung
- EFS (EFS Recovery Agent)
- SSL für Intranet Server und Firewall Management
- VPN
- IPSec Gruppenrichtlinien

DÖRES.

Beispiel-PKI:



DÖRES.

Notwendige Implementierungschritte:

- Vorbereitung zur Online-Publizierung der *Certificate Revocation List* (CRL) der späteren *Offline* Root CA
  - Einrichtung eines erreichbaren *CRL Distribution Point* (CDP)
  - Publizierung der Pfade zum CDP und *Authority Information Access* (AIA) im AD
- Installation der Root CA
- Modifizierung der (Offline) Root CA Policy
- Berechtigungen im Active Directory

DÖRES.

Online-Publizierung der Offline Root CRL:

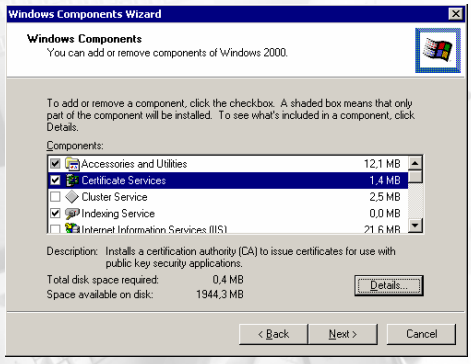
- Festlegung der Online Speicherplätze
- Erstellung der capolicy.inf

```
[Version]
Signature="$Windows NT$"

[CRLDistributionPoint]
URL="ldap:///CN=Root_CA_Name,CN=FQDN_CDP_Server,CN=CDP,CN=Public%20Key%20Services,CN=Services,
      CN=Configuration,DC=Root_Domäne,DC=de?certificateRevocationList?base?objectclass=cRLDistributionPoint"
URL="http://FQDN_webserver/CertEnroll/Root_CA_Name.crl"
URL="file://\\Fileserver\CertEnroll\Root_CA_Name.crl"

[AuthorityInformationAccess]
URL="ldap:///CN=Root_CA_Name,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=Root
      _Domäne,DC=de?cACertificate?base?objectclass=certificationAuthority"
URL="http://FQDN_webserver/CertEnroll/Root_CA_Name.crt"
URL="file://\\Fileserver\CertEnroll\Root_CA_Name.crt"
```


3A04 Windows PKI
10.04.03 – Alexius/Lorenz

DÖRES.

Installation der Root CA



Root Zertifikat und CRL in den Online Speicherort kopieren.

Grundsätzliches
Eine Beispiel-PKI
Öffentlich <> Privat
PKI in Windows

Vorüberlegungen
Wofür Zertifikate?
CA-Modelle
Platzierung/Struktur

Die Praxis
- **CDP/AIA-Pfade**

AD-Berechtigungen /ACLs
Management-GUIs
Drittthersteller?

Evolution
Windows Server 2003/XP Client

Q&A

DÖRES.

Publizierung der CDP und AIA Pfade im AD mit *dsstore.exe:*

- Publizierung der CRL

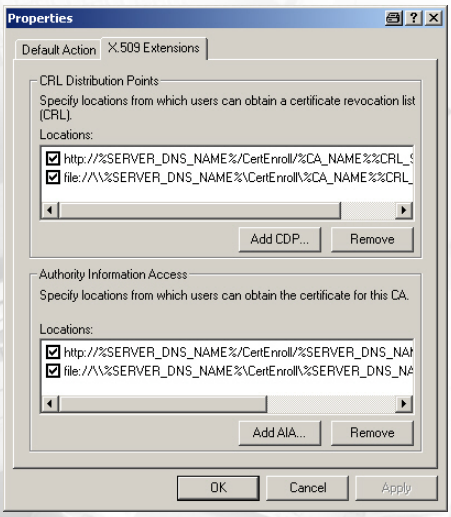
  dsstore DC=*Root_Domäne*,DC=de –addcrl *RootCA_Name*.crl Root_CA_Name FQDN_Online_Server

- Publizierung des Root Zertifikats

  dsstore DC=*Root_Domäne*,DC=de –addroot Root_CA_Name.crt Root_CA_Name

DÖRES.

Modifizierung der Offline Root CA Policy:



DÖRES.

Modifizierung der Offline Root CA Policy:

Einträge für die CDP Pfade:

http://FQDN_Webserver/CertEnroll/%CA_NAME%%CERT_SUFFIX%.crl

file://\\Fileserver/CertEnroll/%CA_NAME%%CERT_SUFFIX%.crl

ldap:///CN=Root_CA_Name,CN=FQDN_Servername,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=*Root_Domäne*,DC=de?certificateRevocationList?base?objectclass=cRLDistributionPoint

3A04 Windows PKI
10.04.03 – Alexius/Lorenz

DÖRES.

Modifizierung der Offline Root CA Policy:

Einträge für die AIA Pfade:

http://FQDN_Webserver/CertEnroll/CertEnroll/%CA_NAME%%CERT_SUFFIX%.crt

file://\\Fileserver/%CA_NAME%%CERT_SUFFIX%.crt

ldap:///CN=Root_CA_Name,CN=FQDN_Servername,CN=CDP,CN=Public Key Services, CN=Services,CN=Configuration,DC=dfg,DC=de?cACertificate?base?, objectclass=certifica tionAuthority

DÖRES.

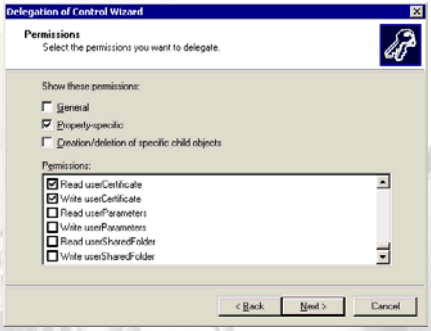
Notwendige Konfiguration im AD:

- Zertifikatsanfragen für Benutzer erlauben
- Berechtigungen auf die Certificate Templates festlegen
- Zugriff der CA auf Benutzerattribute in der Child Domain regeln
  - via Delegation
  - via ACLs

3A04 Windows PKI
10.04.03 – Alexius/Lorenz

DÖRES.

Delegation für die *CertPublishers* Gruppe der Root Domäne:



ACLs einrichten mit dsacls.exe (Server Tools):

dsacls“ cn=adminsdholder,cn=system,dc=*Child_Domäne*,dc=de" /G “*Root_Domäne*\Cert Publishers:WP;userCertificate"

dsacls "cn=adminsdholder,cn=system,dc=*Child_Domäne*,dc=de" /G “*Root_Domäne*\Cert Publishers:RP;userCertificate"

Grundsätzliches
Eine Beispiel-PKI
Öffentlich <> Privat
PKI in Windows

Vorüberlegungen
Wofür Zertifikate?
CA-Modelle
Platzierung/Struktur

Die Praxis
CDP/AIA-Pfade
• **AD-Berechtigungen /ACLs**
Management-GUIs
Dritthersteller?

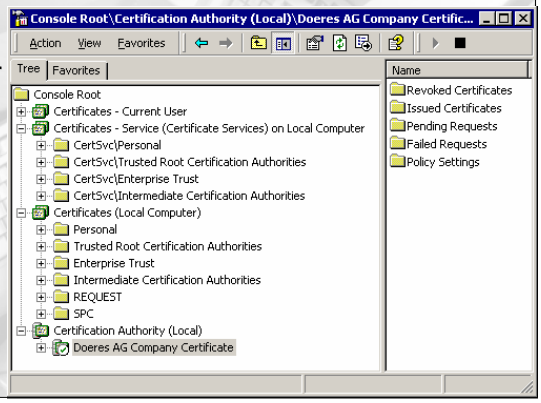
Evolution
Windows Server 2003/XP Client

Q&A

DÖRES.

Certificate Services MMC Snap-Ins:

- Certification Authority Snap-In
- Certificates Snap-In
  - User
  - Computer
  - Service

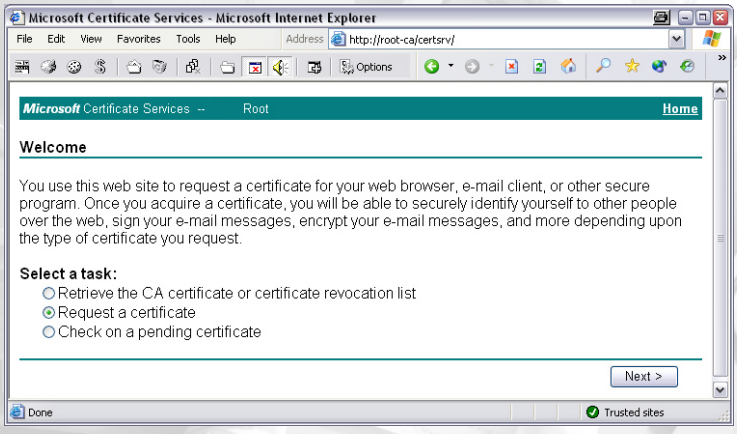


3A04 Windows PKI
10.04.03 – Alexius/Lorenz

DÖRES.

Certificate Services Web Interface:

http://CA_Server_Name/CertSrv



Grundsätzliches
Eine Beispiel-PKI
Öffentlich <> Privat
PKI in Windows

Vorüberlegungen
Wofür Zertifikate?
CA-Modelle
Platzierung/Struktur

Die Praxis
CDP/AIA-Pfade
AD-Berechtigungen /ACLs
- **Management-GUIs**

Dritthersteller?

Evolution
Windows Server 2003/XP Client

Q&A

DÖRES.

Certificate Services Web Interface:

- Der IIS muss zwingend *vor* der Installation der Certificate Services installiert werden um das Web Interface zu nutzen
- Gängige Verwendungsbeispiele sind:
  - User- und SSL Zertifikate
  - Offline Zertifikate
  - Certificate Enrollment (SmartCard)

3A04 Windows PKI
10.04.03 – Alexius/Lorenz

DÖRES.

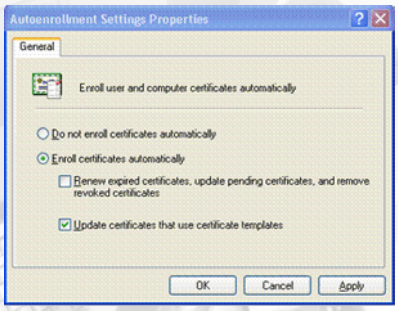
Ggf. sinnvolle Ergänzungen:

- SmartCard
  - Kobil SmartKey KOBIL
  - ActiveCard ActivCard
- Zertifikatsbasierte Einmalpasswörter (OTP)
  - Kobil SecOVID KOBIL
- Zertifikatsbasierte IPSec Implementationen
  - Netscreen VPN NETSCREEN
- Aktuelle PGP-Produktpalette PGP

DÖRES.

Windows XP Client:

- Konfigurierbares Auto-Enrollment für Zertifikate



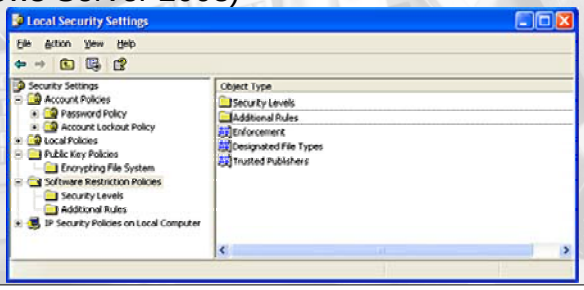
- Smart Card Unterstützung für Administrative Werkzeuge (z.B. Net.exe, Runas.exe)
- Smart Card Logon für Terminal Server (erfordert Windows Server 2003)

3A04 Windows PKI
10.04.03 – Alexius/Lorenz

DÖRES.

Windows XP Client:

- Eigener logischer Certificate Store für 3rd Party Root Zertifikate, via Gruppenrichtlinien abschaltbar
- Verwendung von Zertifikaten zur Beschränkung nutzbarer Software (sinnvoll durch Einsatz der Group Policy Management Console, Add-On zu Windows Server 2003)



Grundsätzliches
Eine Beispiel-PKI
Öffentlich <> Privat
PKI in Windows

Vorüberlegungen
Wofür Zertifikate?
CA-Modelle
Platzierung/Struktur

Die Praxis
CDP/AIA-Pfade
AD-Berechtigungen /ACLs
Management-GUIs
Dritthersteller?

Evolution
- **Windows Server 2003/XP Client**

Q&A

DÖRES.

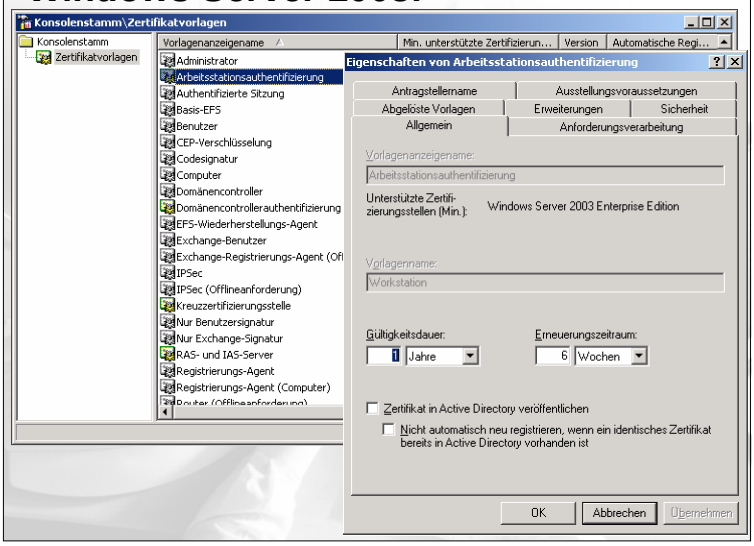
Windows Server 2003:

- Zertifikatvorlagen, Version 2
- Vorlagen sind neu erstellbar (in Windows 2000 sind nur Default-Vorlagen nutzbar)
- Vorhandene Vorlagen können editiert und kopiert werden
- Die Funktionalität der Vorlagen wurde erweitert, z.B. für
  - Anpassung der Enrollment Policies
  - Zertifikats Authorisierung
  - Domänenauthentisierung
  - Schlüsselarchivierung

3A04 Windows PKI
10.04.03 – Alexius/Lorenz

DÖRES.

Windows Server 2003:



Grundsätzliches
Eine Beispiel-PKI
Öffentlich <> Privat
PKI in Windows

Vorüberlegungen
Wofür Zertifikate?
CA-Modelle
Platzierung/Struktur

Die Praxis
CDP/AIA-Pfade
AD-Berechtigungen /ACLs
Management-GUIs
Dritthersteller?

Evolution
- **Windows Server 2003/XP Client**

Q&A

DÖRES.

Windows Server 2003:

- Geänderter Schlüsselarchivierungs- und Wiederherstellungsprozess:
  - Windows 2000 Server: Data Recovery Agent
  - Windows Server 2003: Festlegung, ob der private Schlüssel direkt beim Request archiviert werden soll (via Policy)→ optionale Schlüsselwiederherstellung
- Delta Certificate Revocation Lists
- Qualifizierte Subordination von CAs (RFC 2459)
- Separierung administrativer Rollen

3A04 Windows PKI
10.04.03 – Alexius/Lorenz

DÖRES.

Weitere Informationen:

PKI Übersicht:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/pubkey/default.asp

Windows Server 2003:

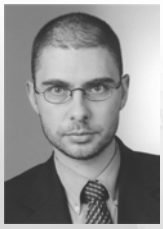
http://www.microsoft.com/windowsserver2003/evaluation/overview/default.mspx

PKI Enhacements in Windows XP und Windows Server 2003:

http://www.microsoft.com/windowsxp/pro/techinfo/planning/pkiwinxp/default.asp

Grundsätzliches
Eine Beispiel-PKI
Öffentlich <> Privat
PKI in Windows
Vorüberlegungen
Wofür Zertifikate?
CA-Modelle
Platzierung/Struktur
Die Praxis
CDP/AIA-Pfade
AD-Berechtigungen /ACLs
Management-GUIs
Drittthersteller?
Evolution
- Windows Server 2003/XP Client
Q&A

DÖRES.



Guido Alexius, Döres AG
Diplom-Physiker & Associate Consultant
Leiter Rechenzentrum
Manager Product Group IT Operations
MCP, Microsoft Inner Circle Systemplatform
alexius.guido@doeres.com

Jens Lorenz, Döres AG
Senior Consultant
Product Engineer Security
NCSA Certified, MCSE, MCP+I, CLS
Security-Manager, Designer und Reviewer
lorenz.jens@doeres.com

Microsoft GOLD CERTIFIED Partner

netiQ Work Smarter.

NETSCREEN