Exchange 2007 Zertifikate

Basics:

- Verwendungszweck von Zertifikaten
- Symmetrische und asymmetrische Verschluesselung, Hybrid Verschluesselung
- Schluessel-Archivierung- und Wiederherstellung
- Arbeiten mit der CA Konsole, MMC, CERTSRV Webseite

Wofuer werden Zertifikate in Exchange verwendet?:

- SMTP TLS
- OWA
- EAS
- OA
- Autodiscover

CA installieren

- Enterprise CA (wegen Custom Templates)
- Webseitenregistrierung
- Template erstellen und konfigurieren
- Berechtigungen konfigurieren

Laufzeit von self signed Zertifikaten in Exchange Server 2007
Standardmaessig 1 Jahr self signed
Wenn eine CA verwendet wird, basiert die Lebensdauer des Zertifikats auf dem Gueltigkeitszeitraum des Templates (Max. CA Lebensalter)

Nachteil Self signed Certificate

- Begrenzte Laufzeit (1 Jahr)
- Nicht trusted (loesbar ueber den Import des Zertifikats in den vertrauenswuerdigen Stammzertifizierungsstellenspeicher per Gruppenrichtlinien)
- Keine zentrale Kontrolle und Verwaltung der Zertifikate aufgrund der fehlenden Zertifizierungsstelle

Anzeigen von Zertifikaten

Anzeigen der Zertifikate mit get-exchangecertificate | fl
Anzeigen eines Zertifikats: get-exchangecertificate -thumbprint "Thumbprint" | fl

Verwendungszwecke

Gueltige Verwendungszwecke fuer ein Zertifikat in Exchange Server 2007:
IMAP, POP, IIS, SMTP

Zertifikat erneuern

Self signed Certificate erneuern: get-exchangecertificate -thumbprint "Thumbprint" | new-exchangecertificate

CA fuer SAN aktivieren (2003)
certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2
net stop certsvc
net start certsvc
Hinweis: Eine Windows Server 2008 CA ist automatisch bereit, SAN Zertifikate auszustellen

Zertifikatberechtigungen
Wenn eigene V2 oder V3 Certificate Templates verwendet werden, muessen die Template Berechtigungen ggfs. angepasst werden. Wie steht hier:
http://www.it-training-grote.de/download/certrequest2k8.pdf

Zertifkattypen
- Normal (Single)
- Wildcard (Bsp.: *.it-training-grote.de)
- SAN (Ein Zertifikat mit mehreren alternativen Namen (CN = Common Name))

Zertifikatanforderung erzeugen

Einfach:
https://www.digicert.com/easy-csr/exchange2007.htm
Oder per EMS:
new-exchangecertificate ....
New-ExchangeCertificate -GenerateRequest -Path c:\certificates\request.req -SubjectName "c=DE, o=IT-TRAINING-GROTE.DE, cn=Hyper. it-training-grote.de" -DomainName it-training-grote.de, autodiscover.it-training-grote.de, hyper, hyper.test.intern, autodiscover.test.intern -PrivateKeyExportable $true
Anzeigen des Request:
get-exchangecertificate -Thumbprint "Thumbprint" | fl

Zertifikat (.CER) erzeugen
den IIS (Website) ggfs. mit HTTPS binden, falls noch nicht erfolgt
https://servername/certsrv ....

Certificate einspielen
Import-ExchangeCertificate –Path c:\certnew.cer
Thumbprint notieren

Certificate aktivieren
Enable-ExchangeCertificate –Thumbprint <thumbprint> -Services “IIS, POP, IMAP, SMTP"

Source:
http://technet.microsoft.com/de-de/library/aa998327.aspx

SAN Request per MMC
Subject eintragen

Weitere Informationen

W2K8 PKI Neuerungen - Windows Server 2008 Launch Frankfurt
http://download.microsoft.com/download/3/3/9/33961897-bb53-42d7-895f-2e381a240c0d/T04_DO_1345_WindowsServer2008PKIUeberblickUndNeuerungen[300].pptx

CA Migration 2003 --> 2008
http://www.it-training-grote.de/download/ca-2k3-2k8-migration.pdf

CA verschieben
http://www.it-training-grote.de/download/ca-move.pdf

CA Zertifikatvorlagen anpassen
http://www.it-training-grote.de/download/certrequest2k8.pdf

W2K3 PKI Ueberblick
http://www.it-training-grote.de/download/w2kmag-pki-092004.pdf

W2K3 PKI Ueberblick PPT
http://www.it-training-grote.de/download/decus-w2k3-pki.pdf