

HowTo: Eigene Zertifikate für Exchange 2007

Um Exchange richtig und Sicher zu betreiben benötigt man mit dem Exchange 2007 einen neuen Zertifikats-Typ mit mehreren Servernamen im Zertifikat. Es reicht nicht mehr nur noch ein Zertifikat für owa.firma.ch zu registrieren, damit man mit SSL auf das OWA zugreifen kann. Importiert man dieses so, kommt spätestens beim öffnen des Outlook 2007 eine Fehlermeldung, dass der Name auf dem Zertifikat nicht mit dem Namen des Servers übereinstimmt. Daher müssen im Zertifikat mehrere Namen hinterlegt werden können. Dies geht mit sogenannten x509 oder TLS Zertifikaten.

Ich beschreibe hier einen Weg, wie man ein solches Zertifikat mit einer eigenen Zertifizierungsstelle einrichtet.

Bis jetzt gibt es 3 offizielle CA's die auch Exchange 2007 Zertifikate anbieten.

Eine aktuelle Liste findet man hier:

<http://support.microsoft.com/?kbid=929395>

Annahmen

In folgendem Beispiel nehmen wir folgende Gegebenheiten an:

Exchange-Server Netbios Name:	SVVALIANT4
Exchange-Server DNS Name:	SVVALIANT4.scolab.lan
Externer DNS Name:	mail.scolab.ch
Autodiscover:	autodiscover.mail.scolab.lan
Zertifizierungsstelle	SVVALIANT4

Erklärungen

In der Untenstehenden Tabelle sind die Typen der benötigten Angaben für das erstellen eines Requests. Es ist zu empfehlen auf Umlaute und Sonderzeichen bei diesen Typen nicht zu verwenden.

Name	Abkürzung	Typ	Im Beispiel
Land/Region	C	ASCII	CH
Bundesland/Kanton	S	Unicode	Optional
Ort	L	Unicode	Zurich
Organisation	O	Unicode	Scolab.ch
Organisations Einheit	OU	Unicode	IT Dept.
Gemeinsamer Name	CN	Unicode	mail.scolab.ch

Request erstellen

Den Request muss man in der Exchange Managementshell ausführen und zwar mit folgendem Befehl:

Damit wird eine request.req auf das Laufwerk C: geschrieben

-SubjectName Hier werden alle Zertifikats Informationen über den Eigentümer mitgegeben

-DomainName kann man alle anderen Namen angeben also z.B. den NetBios Namen des Servers für den internen Gebrauch und für das Outlook.

-Force wird ein Request erzwungen, das heisst, wenn man vorher schon mal geprübelt hat, werden die vorgängigen Requests überschrieben.

-PrivateKeyExportable kann der Key Exportiert und importiert werden. Dies wird benötigt, damit das Zertifikat nachher installiert werden kann.

-IncludeAutodiscover mit diesem Schalter wird vor jedem DomänenName das Präfix Autodiscover vorgehängt.

```
[PS] New-ExchangeCertificate -GenerateRequest -Path c:\request.req  
-SubjectName "c=CH, L=Zurich, O=Scolab.ch, OU=IT Dept.,  
CN=mail.scolab.ch" -DomainName mail.scolab.ch, svvaliant4,  
svvaliant4.scolab.lan, autodiscover.scolab.ch -Force -  
IncludeAutodiscover -PrivateKeyExportable:1
```

Zertifikat an die Zertifikatsstelle übergeben

Damit wir das Zertifikat installieren können müssen wir den Request an die Zertifizierungsstelle übergeben damit ein Zertifikat erstellt werden kann. Dies muss über das Webinterface der Zertifizierungsstelle geschehen.

- Dafür gehen wir auf <https://svvaliant4/certsrv>
Hier klicken wir auf "Ein Zertifikat anfordern"
- Danach "Erweiterte Zertifikatanforderung ein" anklicken
- Reichen Sie eine Zertifikatanforderung ein, die eine Base64-codierte CMD- oder PKCS10-Datei verwendet, oder eine Erneuerungsanforderung, die eine Base64-codierte PKCS7-Datei verwendet, ein.
- Jetzt muss der Inhalt der Datei request.req in das Feld „Gespeicherte Anforderung“ rein kopiert werden oder das File hochgeladen werden.
- Bei der Zertifikatsvorlage „Webserver“ auswählen
- Jetzt kann man das Cer File herunterladen und auf der Festplatte abspeichern.
Der Einfachheit habe ich es auf C:\cert.cer abgespeichert

Importieren des Zertifikates

Nun muss das Zertifikat noch auf dem Exchange installiert werden und zwar mittels Managementshell

```
[PS] Import-ExchangeCertificate -Path c:\cert.cer -FriendlyName  
"Scolab Zertifikat" | Enable-ExchangeCertificate -Services "IIS"
```

- Path gibt den absoluten Pfad für die Zertifikatsdatei an
- FriendlyName ist ein einfach zu merkender Name für das Zertifikat mit welchem es im Zertifikatsmanager angezeigt wird
- Enable-ExchangeCertificate wird das Zertifikat auf dem Exchange und IIS aktiviert. Im IIS wird danach eine SSL Verbindung erzwungen
- Services Damit wird angegeben welche Dienste mit diesem Zertifikat konfiguriert werden.

Es sind folgende Optionen möglich IMAP, POP, UM, IIS, SMTP oder None.

Es können gleichzeitig mehrere Dienste gesichert werden z.B. mit:

```
Import-ExchangeCertificate -Path c:\cert.cer -FriendlyName "Scolab Zertifikat" | Enable-  
ExchangeCertificate -Services "IIS, SMTP, POP, UM"
```

Weiterführende Links:

[Creating a Certificate or Certificate Request for TLS](#)

[How to Request an SSL Certificate](#)

[Managing SSL for a Client Access Server](#)

8.2007 – Daniel Oberli, scolab.ch