



Securing an Exchange 2007 Client Access Server using a Trusted CA issued SAN Certificate

Previous versions of Exchange Server used certificates for several different purposes such as for securing EAS, DWA, RPC over HTTP, POP3, IMAP4 and SMTP. But all Exchange services/protocols were insecure by default that is you had to secure them by installing a SSL certificate manually after setup. This has changed with Exchange Server 2007. When you install an Exchange 2007 server a self-signed SSL certificate is created and applied during the setup process. For the purpose of Client Access servers, this SSL certificate is used to secure communication between Internet clients (Exchange ActiveSync, Outlook Web Access, Outlook Anywhere, POP3 and IMAP4) and internal clients (Outlook 2007) to the Client Access server. Although the self-signed SSL certificate isn't trusted by any clients by default, the Exchange Product group was of the opinion that it's a good idea to install a SSL certificate during setup in order to make Exchange Server 2007 a more secure product by default.

Exchange Server 2007 introduces a new Exchange web service called the Autodiscover service. The autodiscover service is used to configure Outlook 2007 clients. More specifically, the Autodiscover service is used by Outlook 2007 client features such as the

- Availability service (free/busy)
- Auto Account Setup (automatic profile creation)
- Out of Office (OOO)
- Offline Address Book (OAB) and
- Unified Messaging (UM).

This means that in order for these features to work correctly, the Autodiscover service must be properly configured. Since the Autodiscover service is a web-based service, it's located on the Client Access server (CAS). By default all web-based Exchange 2007 services are secured using the self-signed SSL certificate that is created during setup.

With Exchange Server 2007 a new type of certificate is introduced called **Subject Alternative Name (SAN) certificate**. The interesting thing about a SAN certificate is that it allows us to include multiple FQDNs (aka common names) in one single certificate (**Figure 1**). This is very useful in regards to Exchange Server 2007, since multiple FQDNs are used by the Outlook 2007 client when accessing an Exchange 2007 server.

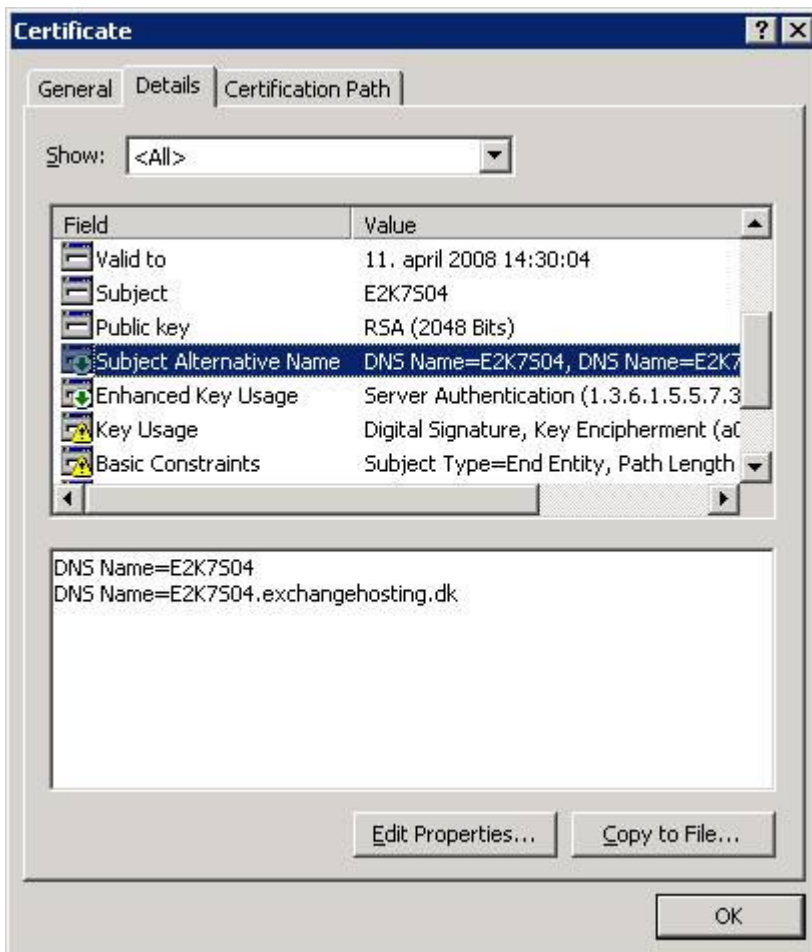


Figure 1: Property page for the Default Self-signed SAN Certificate

Since the self-signed certificate installed during setup isn't trusted by clients, Exchange ActiveSync and Outlook Anywhere will not work unless the certificate is installed on the respective clients. In addition, Outlook 2007 clients will have issues with features (mentioned earlier) that depend on the Autodiscover service. Submit and finally install a SAN certificate from a 3rd party certificate authority (CA) in order to get your Client Access server properly configured, so that all client types can connect and so all Outlook 2007 client features that depend on the Autodiscover service work as expected.



Creating the Public DNS Records

If you made a transition from Exchange 2000 or 2003 to Exchange Server 2007, most of you are likely to have a public DNS record called something like mail.domain.com or mobile.domain.com. With previous versions of Exchange Server this FQDN was typically used to access Exchange ActiveSync, Outlook Web Access and Outlook using RPC over HTTP (now known as Outlook Anywhere). This FQDN is also required in Exchange Server 2007, so if you haven't created it on a public DNS server, now is the time to do it. In addition, you must create another FQDN called autodiscover.domain.com, in order for Outlook Anywhere clients on the Internet to be able to use the features dependent on the Autodiscover service.

Requesting and Submitting the SAN Certificate

To order a SAN certificate from a 3rd party certificate authority (CA), the first step is to use the New-ExchangeCertificate cmdlet to issue a request for the certification of the Exchange 2007 Client Access server. For the purpose of this article included the following three FQDNs or SANs in the certificate request:

- **E2k7s04.exchangehosting.dk** (internal FQDN mainly used by internal clients such as OWA and Outlook 2007)
- **Autodiscover.exchangehosting.dk** (internal and external FQDN required in order for Autodiscover dependent features to work for internal and external Outlook 2007 clients)
- **Mobile.exchangehosting.dk** (FQDN used for external clients such as Exchange ActiveSync, Outlook Web Access 2007 and Outlook Anywhere)

Note:

We will be generating a SAN certificate request for a split-DNS setup, that is a setup where the same domain name (Exchangehosting.dk) is used internally (Active Directory DNS servers) as well as externally (public DNS servers). If you have an internal domain name, that's different from the external (such as a .local domain), you must add additional FQDNs or SANs to the certificate request. Let's assume an internal domain name as Exchangehosting.local. If this was the case we would need to add **e2k7s04.exchangehosting.dk**, **e2k7s04.exchangehosting.local**, **Autodiscover.exchangehosting.dk** and **autodiscover.exchangehosting.local** to the SANs list in the certificate.

The reason for this is because internally connected Outlook 2007 clients use these FQDNs or SANs for the autodiscover service and for connecting to the Exchange mailbox.

To generate a request for a new SAN certificate, we must use the New-ExchangeCertificate cmdlet (the IIS Manager isn't capable of creating requests for SAN certificates). To do so launch the Exchange Management Shell, then type the following command (replace the names with your own):

```
New-ExchangeCertificate -DomainName e2k7s04.exchangehosting.dk, autodiscover.exchangehosting.dk, mobile.exchangehosting.dk -FriendlyName "Exchange Hosting IN SAN Certificate" -GenerateRequest:$True -Keysize 1024 -path c:\Exchangehosting.txt -privatekeyExportable:$true -subjectName "c=in, o=My Company, CN=Exchangehosting.dk"
```



After hitting Enter the thumbprint for the certificate will be listed as shown in **Figure 2** below.

```
Machine: E2K7S04 | Scope: exchangehosting.dk
[PS] C:\>New-ExchangeCertificate -GenerateRequest -SubjectName "C=dk, O=Exchange
Hosting DK, CN=mobile.exchangehosting.dk" -DomainName mobile.exchangehosting.dk
, autodiscover.exchangehosting.dk, e2k7s04.exchangehosting.dk -FriendlyName "Exc
hange Hosting DK - CAS SAN Certificate" -KeySize 1024 -Path c:\cas_san_ssl_req.t
xt -PrivateKeyExportable:$true

Thumbprint                Services    Subject
-----
7DC74619E02F2E50B8A5A332218A73AFE39069B9    .....    CN=mobile.exchangehosti...

[PS] C:\>_
```

Figure 2: Generating a New SAN Certificate Request in the Exchange Management Shell

The CSR file can be found under the specified path, which in this example is the root of the C: drive. Opening the certificate request file in Notepad will reveal the certificate request code just as is the case with traditional single-name certificates.

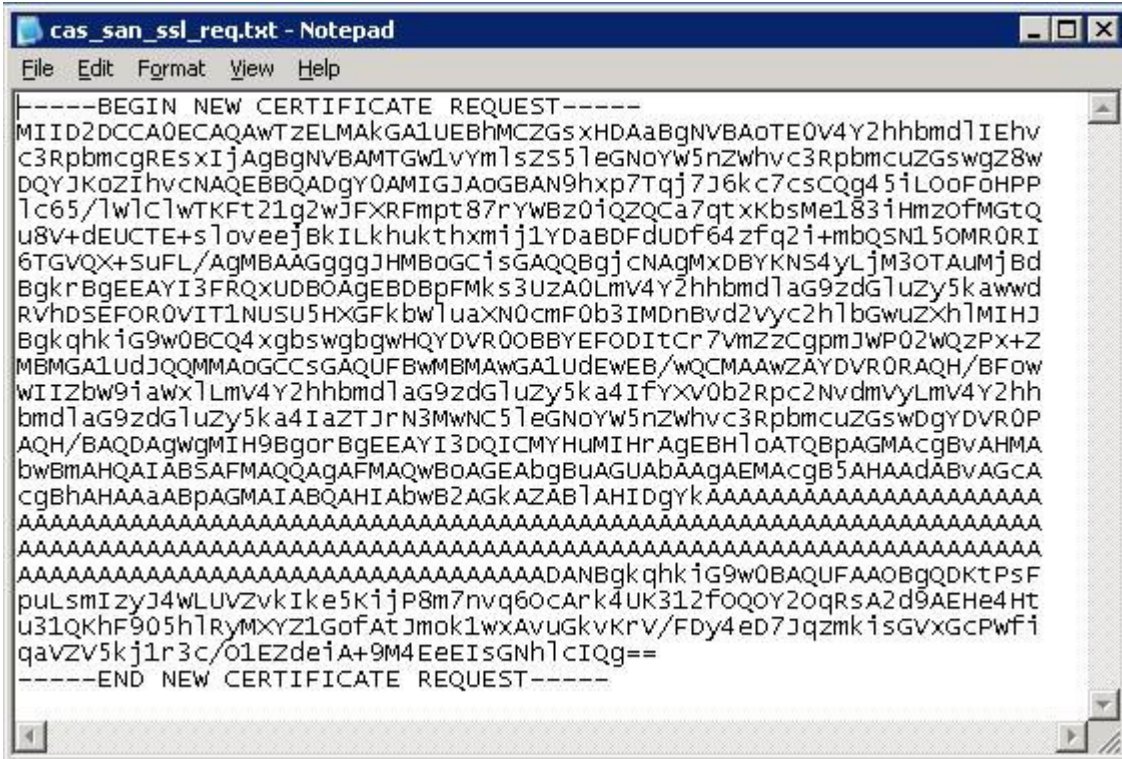


Figure 3: New SAN Certificate Request

Importing and Enabling the SSL SAN Certificate

After having submitted the certificate request to a 3rd party certificate authority, you'll receive an email message containing the issued certificate shortly thereafter. This certificate now needs to be imported and enabled on the Exchange 2007 server on which the Client Access server role has been installed. To do so type the following command in the Exchange Management Shell:

```
Import-ExchangeCertificate -Path c:\mobile.exchangehosting.dk.p7b | Enable-ExchangeCertificate -Services IIS
```

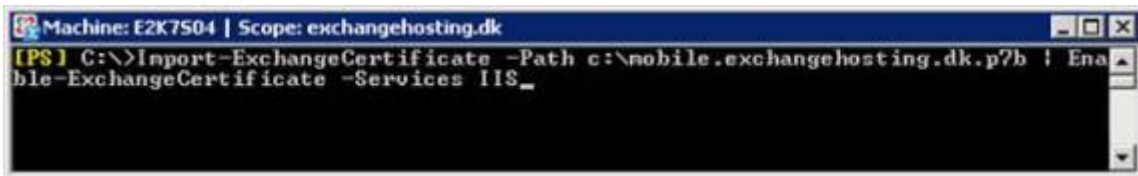


Figure 4: Importing and Enabling the SAN Certificate for IIS

After hitting Enter the certificate will be imported into the personal certificate store and enabled for Exchange ActiveSync, OWA and Outlook Anywhere.



Note:

If you also want to enable the certificate for POP3, IMAP4, SMTP or Unified Messaging, you would need to enter these services separated by commas. A command where we also enabled the certificate for POP3 and IMAP4 would look something like this: *Import-ExchangeCertificate -Path c:\mobile.exchangehosting.dk.p7b / Enable-ExchangeCertificate -Services IIS, POP, IMAP.*

To verify the certificate contains the correct information, you can run **Get-ExchangeCertificate | FL**, which will list issuer, status, subject alternative names and much more as shown in **Figure 5**.

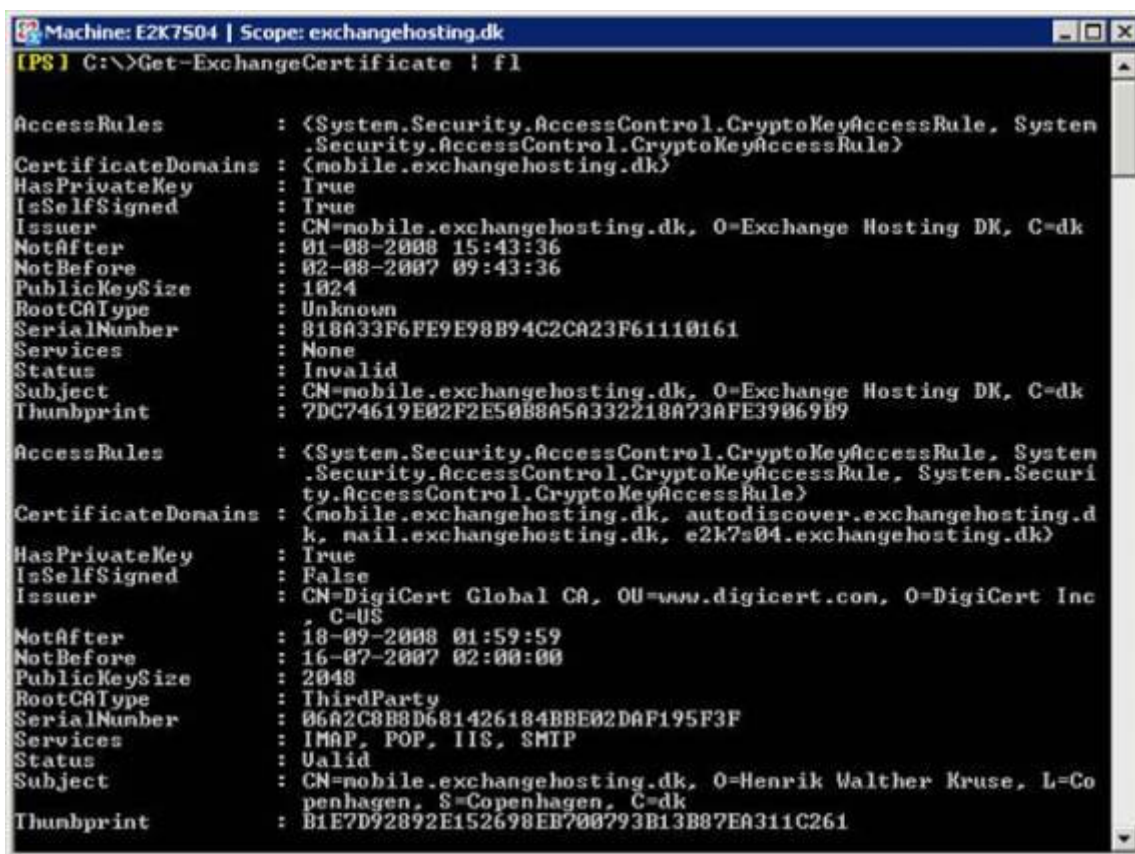


Figure 5: List SAN Certificate Properties in the Exchange Management Shell



Testing whether the SAN Certificate works as Expected

The SAN certificate has now been properly enabled on the Client Access server, and we should no longer get security warnings, when accessing OWA, as shown in **Figure 6**.

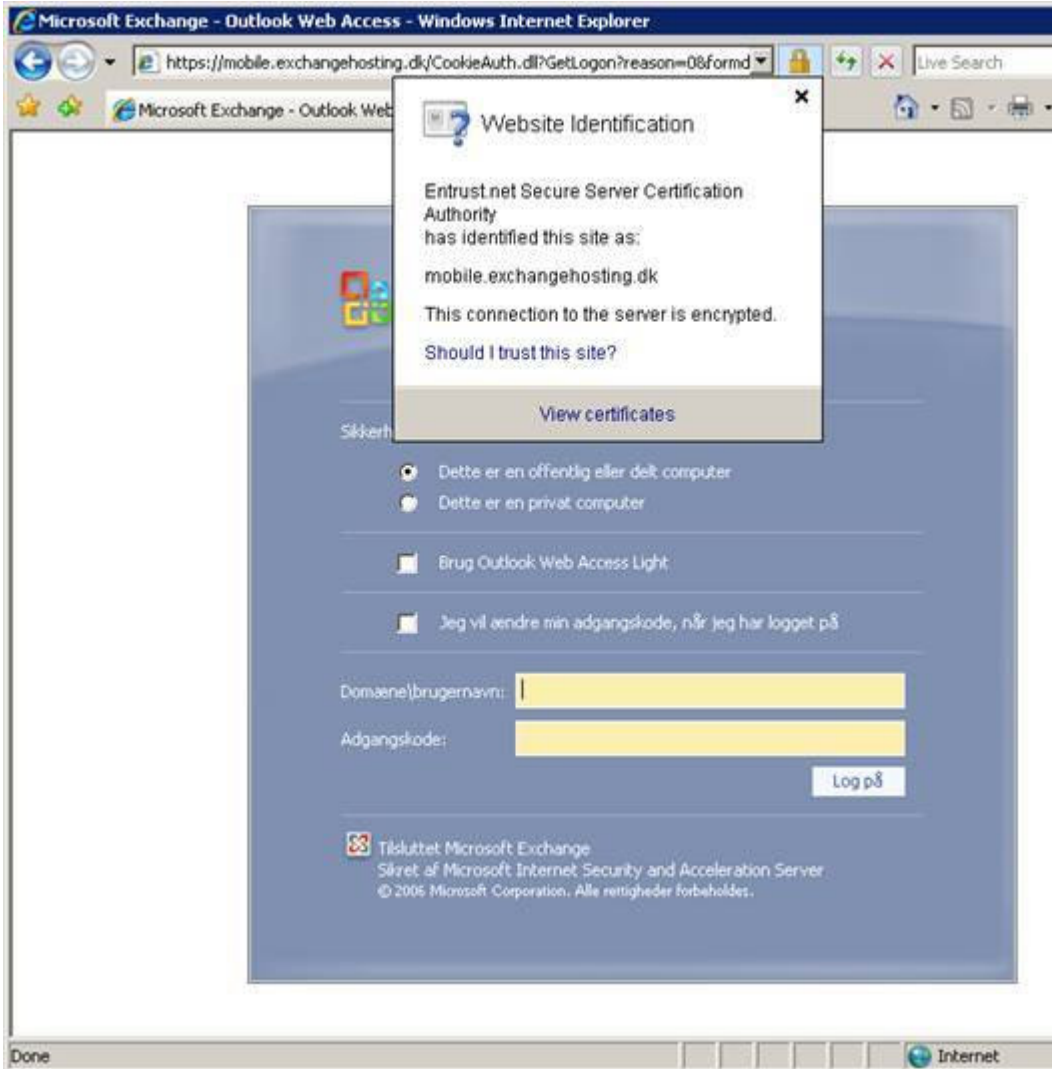


Figure 6: SSL Connection to OWA without security warnings

The same goes for Outlook 2007 no matter if we're accessing an Exchange 2007 user mailbox from the Internet or the internal network. In addition, the Autodiscover service and all features that depend on it should work too as shown in **Figure 7**.



Note:

You can perform the Outlook 2007 E-mail AutoConfiguration test by holding down CTRL while right-clicking the Outlook icon in the System tray, and then selecting **Test E-mail AutoConfiguration** on the context menu.

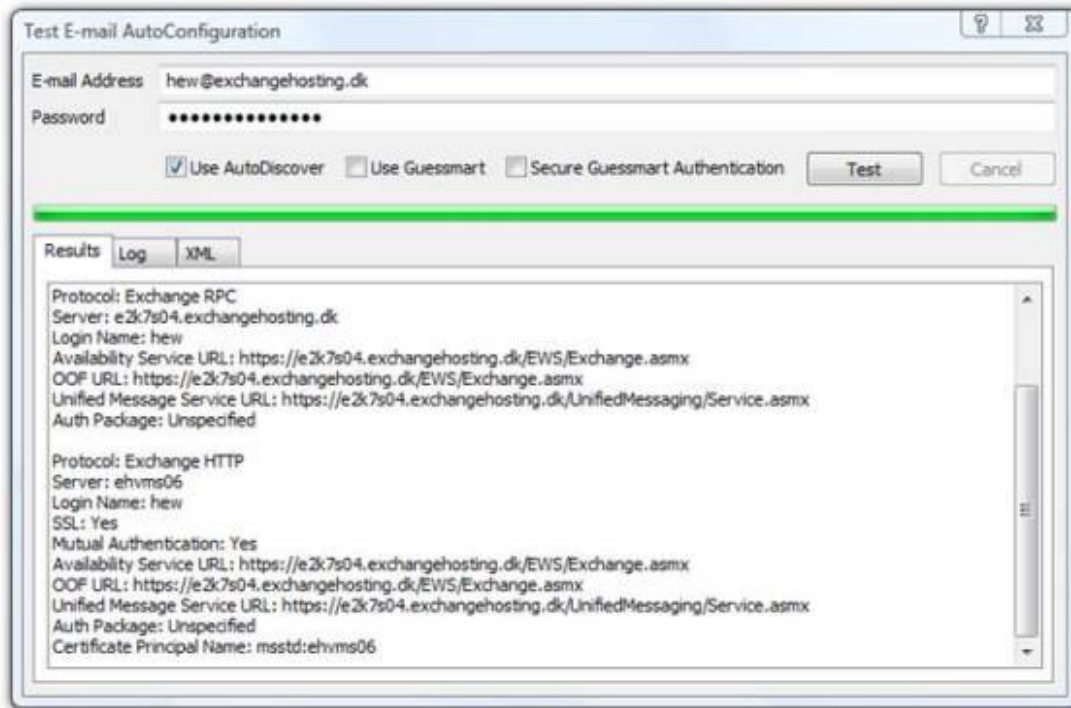


Figure 7 Successful E-mail AutoConfiguration Test

Finally, Exchange ActiveSync works as expected as long as we use the first SAN in the SANs list in our certificate, which is mobile.exchangehosting.dk (**Figure 8**)



Figure 9: Exchange ActiveSync Connection

Conclusion

A trusted CA's SAN certificate is not only a requirement in order to properly secure client access to our Exchange 2007 client access server, but it's important to note that Outlook client features such as the Availability service (free/busy), Auto Account Setup (automatic profile creation), Out of Office (OOO), Offline Address Book (OAB), and Unified Messaging (UM) will not work, if the certificate doesn't include the required SANs.