Managing certificates in Exchange - Part 1

In Part 1 of this series, we will give you an overview of the different components of Exchange that use certificates.

Ilse Van Criekinge

Network administration - Certificates can be used to encrypt communication data streams between two end points (both servers and clients). Besides, certificates are also used by these endpoints to authenticate themselves against other components. Exchange 2007 uses X.509 certificates for authentication and encryption. These certificates follow a standard format when published by the ITU-T (Telecommunication Standardization Sector).

There are several components in Exchange 2007 that rely on certificates for encryption and authentication purposes or both. In Part 1 of this series, we will give you an overview of the different components of Exchange that use certificates. We will then take a closer look at the features of each self-signed certificate created by default.

Certificate Usage by Exchange Server 2007 components

As mentioned above, some components of Exchange Server 2007 use X.509 certificates for encryption and authentication or both. You will see that when installing the Exchange 2007 Hub Transport server role, the Client Access server role, Unified Messaging server role and the Edge Transport server role, Exchange will create a default self-signed certificate to ensure that the only components of It can use that certificate to perform the required function.

Figure 1 below shows you how the self-signed certificate was created by Exchange during the installation of the Exchange 2007 Client Access, Hub, and Unified Messaging roles. This certificate will be used by services: IIS, SMTP, POP, IMAP and UM.

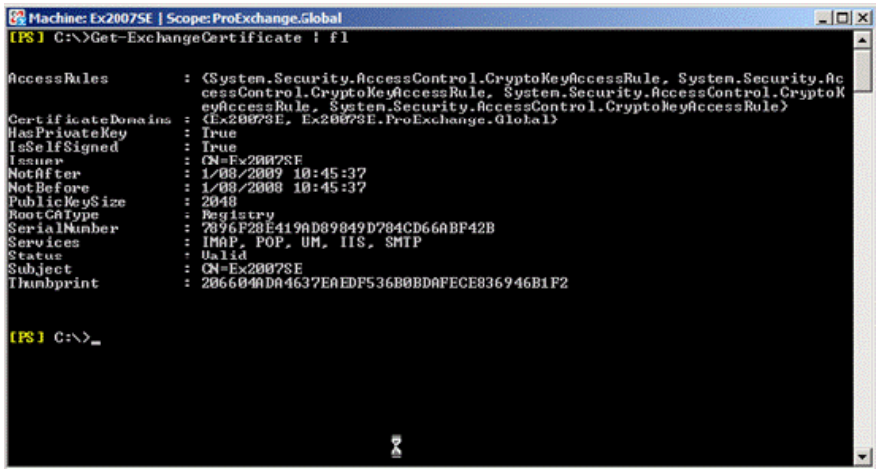

Figure 1: The self-signed certificate is created by default when installing the Exchange 2007 HUB, CAS, and UM server roles

Hub and Edge Transport certificates and roles

Transport layer security between Active Directory sites

The Exchange 2007 Hub Transport server role uses a certificate to encrypt all traffic between Active Directory sites. You cannot configure Exchange to allow unencrypted SMTP traffic between Hub Transport servers located in different sites.

To see which certificate is used between Hub Transport servers located in different Active Directory sites, use the SMTP login protocol to Send connector inside the organization on each Hub Transport server, see Figure 2 below. below, using the Exchange Management Shell Set-TransportServer command.

Figure 2: Setting up the IntraOrgConnectorProtocolLogging to verbose

By setting the *IntraOrgConnectorProtocolLoggingLevel* to verbose, the login protocol will be added to the Send connector protocol log. After sending a mail from Mailbox in Site B to a Mailbox located on the Exchange 2007 Mailbox server in Site A, observe the Send protocol log you will see that the Exchange Hub Transport server in Site B (Ex2007SE) uses the certificate. Only provided by the Exchange Hub Transport server in the destination Active Directory site (Ex2007EE) to start Transport Layer Security, see Figure 3 for details.

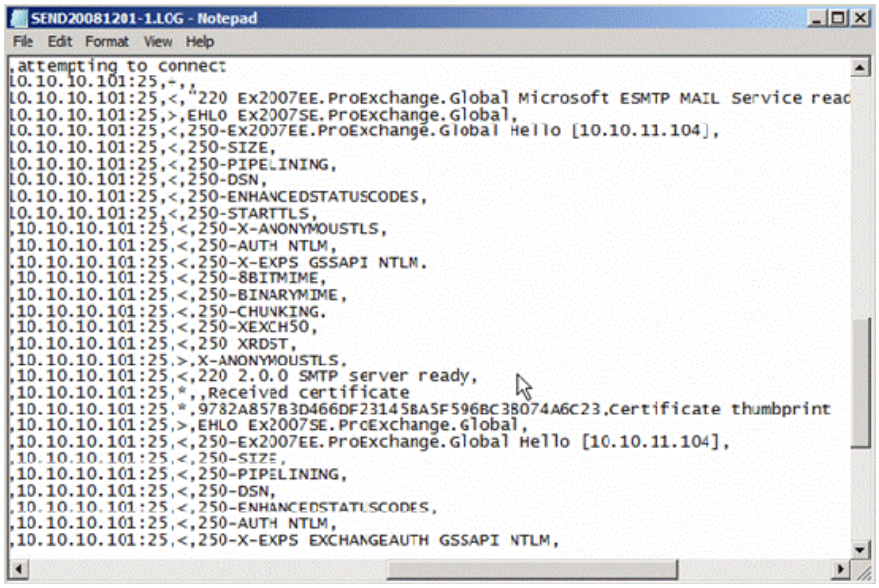

Figure 3: Sending the protocol record between Active Directory sites

You can immediately see the certificate on the Hub Transport server that is in the state available to TLS, indicating that it is a self-signed certificate that has been used (Figure 4).

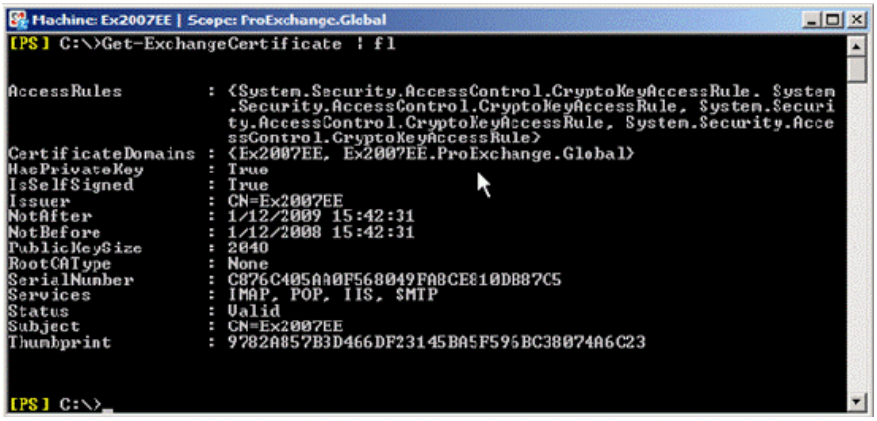

Figure 4: Self Signed certificate

EdgeSync

Once EdgeSync is configured between the internal Hub Transport servers and the Edge Transport, both servers will use a certificate to encrypt their communication problem. In addition, both will be used to provide direction for trust. This trust is an authentication method where the certificate can be used for authentication when the issued certificate is present in Active Directory (with the Hub Transport server role) or ADAM / LDS (for the Edge Transport server role). When setting up EdgeSync, the required certificates will be published in the correct location.

Transmission layer security

Whenever a server opens a connection to the Exchange 2007 Hub / Edge Transport server role, Exchange will allow a TLS by providing its certificate.

Domain security

Certificates can also be used by the Hub / Edge Transport to configure Domain Security with partner organizations, both encryption and authentication.

Client Role Access Server and certificates

Client Access

Certificates are used by the Client Access server role to allow encrypted media traffic between the Client Access server and its clients. By default SSL is required for:

- Outlook Web Access
- Outlook Anywhere

- Exchange ActiveSync
- POP3
- IMAP4
- Exchange Web Services like Autodiscover, EWS and Unified Messaging

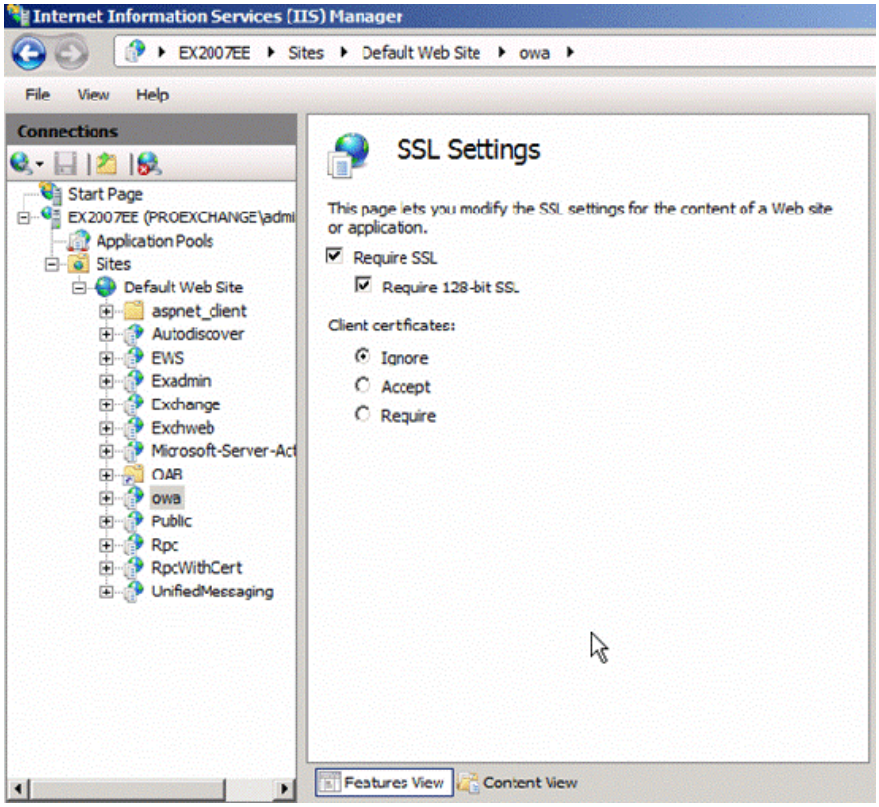

Figure 5: SSL request

With virtual directories, the use of certificates is not required by default, which makes the Offline Address Book available for download by Microsoft Office Outlook 2007 and newer clients.

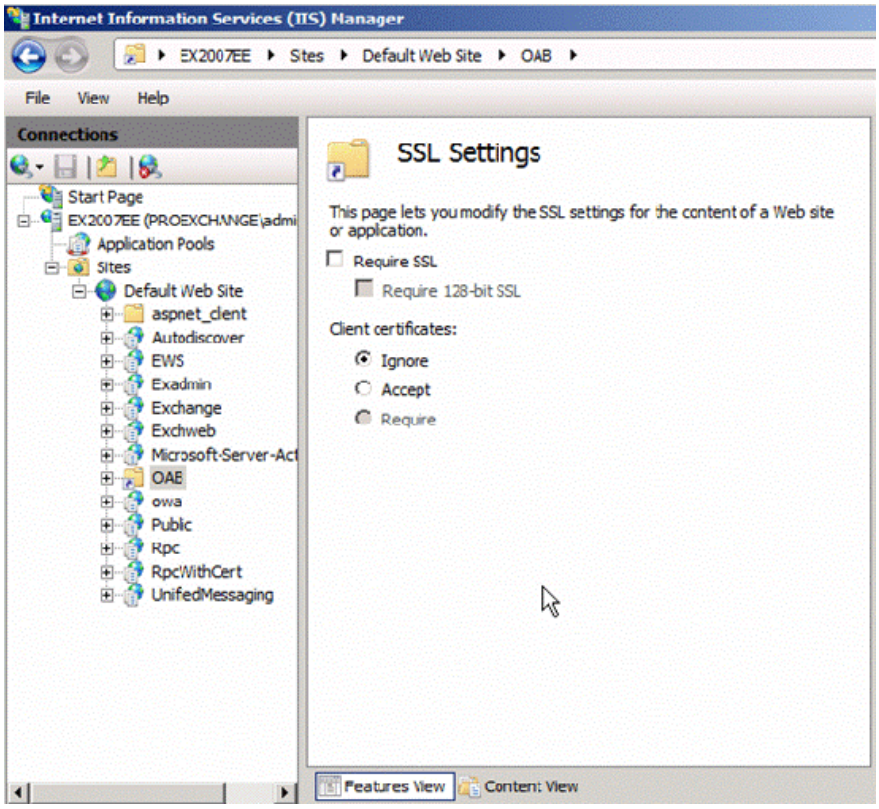

Figure 6: OAB Virtual Directory does not require SSL

Certification based on certificate

You can configure certificate-based authentication, by configuring it to allow clients to authenticate themselves to the Client Access server using their personal certificates.

Unified Messaging Server Role and certificates

Certificates used by the Unified Messaging Server role to encrypt communications when sending a Voice Mail message are recorded to the Exchange Hub Transport Server role. Certificates are also used to code SIP or RTP traffic for UM IP Gateway, and must be used when you decide to deploy Office Communications Server in your environment, because Office Communications Server only communicates with roles Other servers through encryption.

When you deploy the Exchange 2007 Server role, except for the Mailbox Server role, Exchange will create a self-signed certificate and allow Exchange to use this certificate when required for IIS, SMTP, POP3, IMAP4, and UM services.

Characteristics of Self-Signed certificates

Let's take a look at these default Self-Signed certificates features.

Self-Signed certificates are only valid for about a year, see Figure 7, and need to remew after a year.

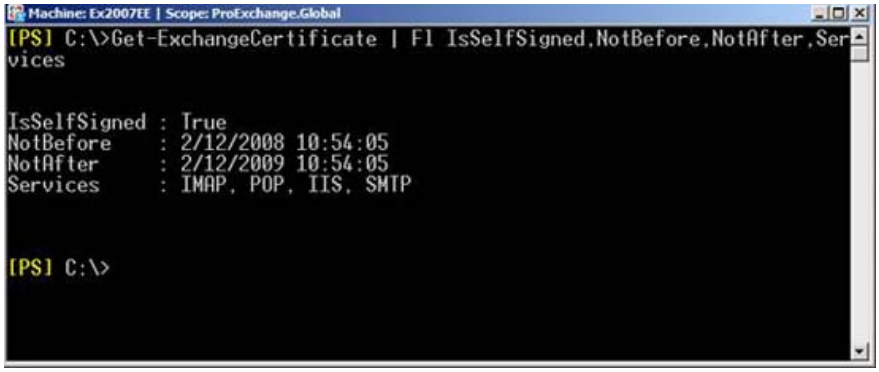

Figure 7: Self-Signed certificate is only valid for one year

To renew a Self-Signed certificate, you can use the New-ExchangeCertificate command. If this certificate exists by running Get-ExchangeCertificate, you can quote the object for the New-ExchangeCertificate command, then create a new Self-Signed certificate with the same settings and activate it. It gives the same service by default. In Figure 8, you can see the existing Self-Signed certificate is renewed.

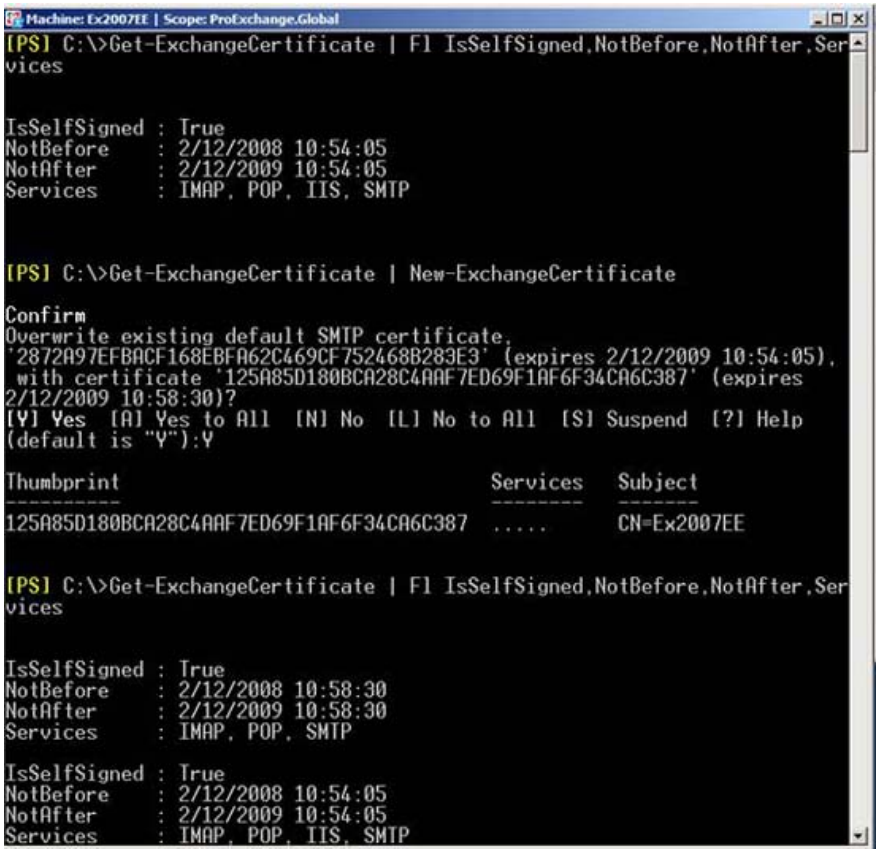

Figure 8: Refresh an existing Self-Signed certificate

The Exchange 2007 Client Access server only allows one certificate to be enabled for use with IIS, but you may still have multiple certificates enabled for POP, IMAP, UM and SMTP. When multiple certificates are available,

Exchange will select a certificate based on different standards. We will cover this selection process in part two of the series.

The Self-Signed certificate created when deploying Exchange 2007 will have a common name set for the Host name of the Exchange server and there are two Subject Alternative Names setting for its Host name and its Fully Qualified Domain Name.

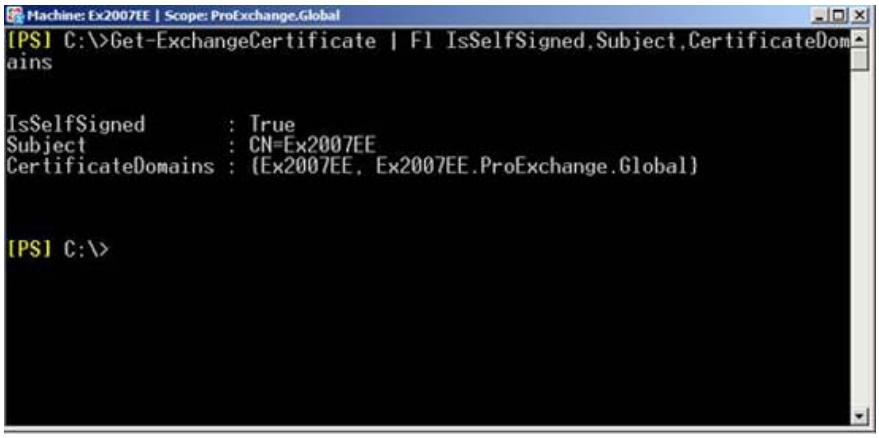

Figure 9: Certificate of Self-Signed and Subject and its CertificateDomains

However, it is possible to create a Self-Signed certificate with the Subject and Subject Alternative Names to ensure that it can be used in the Exchange organization.

Using the New-ExchangeCertificate command, you can create an example of a certificate with Common Name is webmail.proexchange.global, then specify Subject Alternative Names as Exchange for Host and Fully Qualified Domain Name, see Figure 10.

Don't forget to add the PrivateKeyExportable boolean parameter and set True, if you want, you can export this certificate to allow your users to trust it (details will be introduced in Part 2).

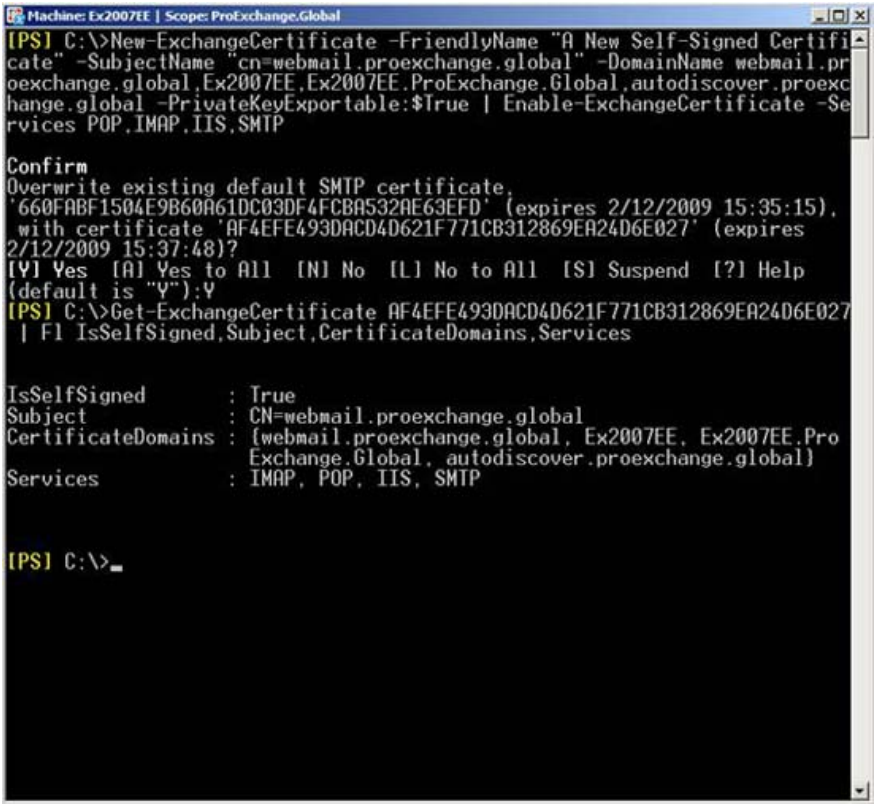

Figure 10: Create a Self-Signed certificate with the customized Subject Alternative Names

In part two of this series, we will return to the required names of the certificate. In part three, we will explain more about the commands used.

Be aware that the Self-Signed certificate is only trusted by its issuer, which can cause Exchange to fail if not configured properly. Let's take a look at what you need to consider if you decide to use a Self-Signed certificate:

- Outlook Anywhere and Exchange ActiveSync do not support the use of a self-signed certificate.
- The Autodiscover web service will not check if the certificate issuer is trusted when launching Microsoft Office Outlook 2007 from a domain client, but will complain about the certificate if you are using Microsoft Office Outlook 2007 from the machine. The guest is not in the domain, as shown in Figure 11.

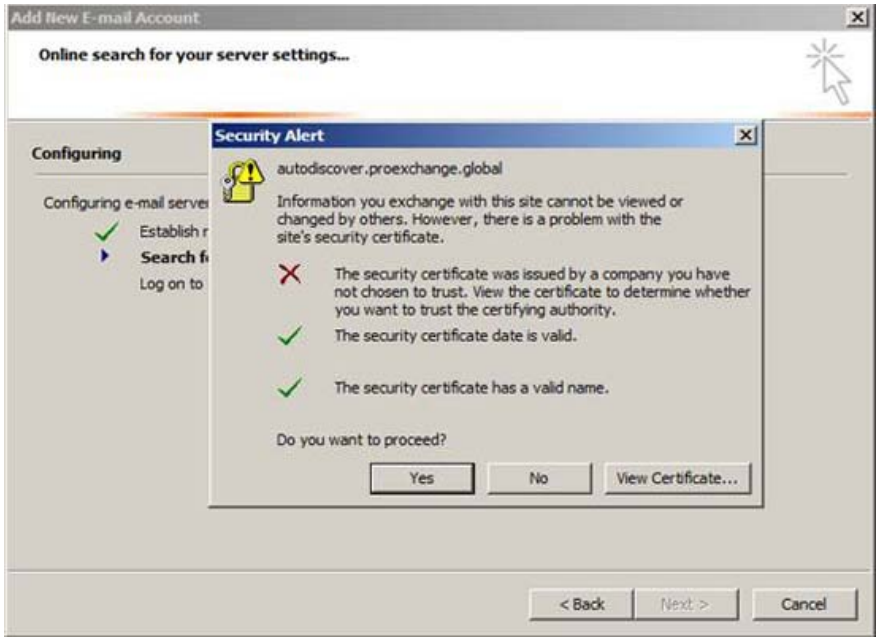

Figure 11: Self-Signed certificate is not trusted

- When Microsoft Office Outlook 2007 clients (in domain or non-domain) use Exchange Web Services provided by the Microsoft Exchange Client Access server, they will be prompted by Outlook that the certificate is issued by an unbelieving company. depend. Figure 2 shows a security warning when someone requests Free and Busy information.

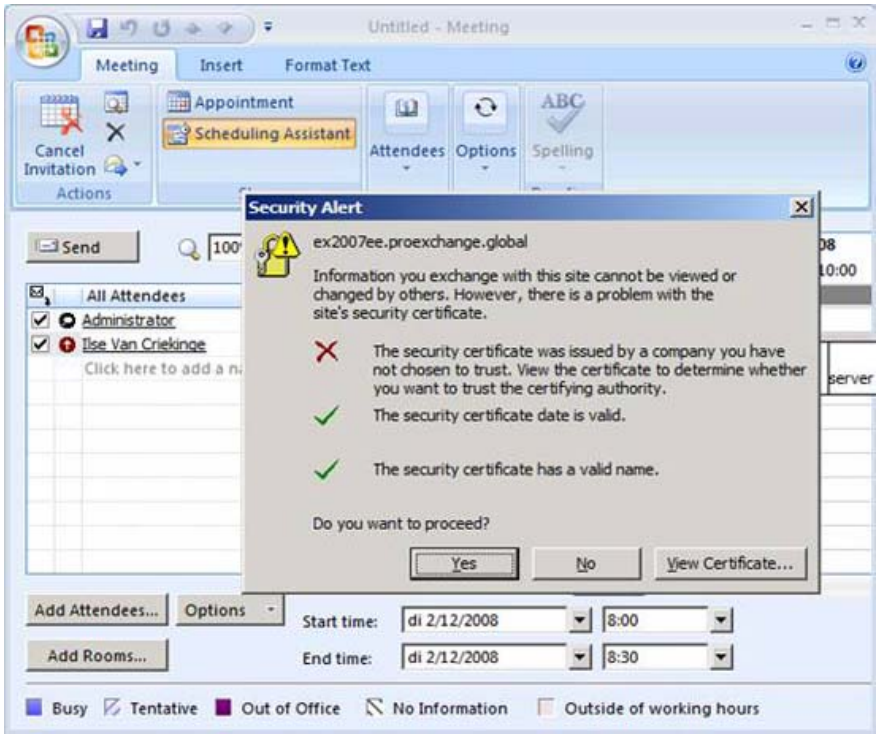

Figure 12: Self-Signed certificate is not trusted

- Microsoft supports the use of Self-Signed certificates, but for internal scenarios such as:

    1. To encrypt SMTP sessions between Hub Transport servers and other sites;
    2. To encrypt SMTP sessions between Hub Transport servers and Edge Transport servers;
    3. To encrypt the synchronization of configuration and recipient information by configuring EdgeSync between internal Hub Transport servers and Edge Transport servers.
    4. To encrypt SMTP sessions between Unified Messaging and Hub Transport servers;
    5. To encrypt SIP and RTP sessions between Unified Messaging servers and Office Communications (requires that you ensure that the Office Communication Mediation server trusts your Exchange server as the server issues that Self-Signed certificate only);
    6. To encrypt internal client access to Exchange (POP, IMAP, Outlook Web Access).

- If you do not want Exchange to create a self-signed certificate during installation, you can specify the */ NoSelfSignedCertificates parameter* next to Setup in the command prompt. Note: this parameter can only be used when installing the Client Access server role or the Unified Messaging server role. If your server does not have a valid certificate available to encrypt communication between clients and the Client Access server or the Unified Messaging server, then the communication will not be encrypted and therefore not secure.

Conclude

In this article, I have explained that Exchange 2007 components use certificates and the characteristics of the 'self-signed' certificate. In part two of this series, we will introduce you to the factors that help you trust and this certificate and the requirements of a certificate that you need to keep in mind when using them. The final part of the series will give you a closer look at the Exchange Management Shell commands used to create, manage, and remove Exchange certificates.