Date: 09/10/2012
Procedure: Exchange 2007 – Certificato Scaduto
Source: **LINK**
Permalink: **LINK**
Created by: HeelpBook Staff
Document Version: 1.0

EXCHANGE 2007 – CERTIFICATO SCADUTO

If your **Exchange 2007** is nearing its first birthday, there is a good chance you will soon come across some event log warnings concerning the expiry of an internal transport certificate.

If you ignore these, users will start chasing you!! **Outlook 2007** is now popping an expired certificate warning dialog.

With so many changes, it is easy to overlook some of the less shiny Exchange 2007 improvements, especially if you haven't been using earlier Exchange versions. **Exchange 2007** automatically installs a self-signed certificate.

Amongst other benefits, this certificate immediately secures **OWA** access enabling users to login to their mailbox using HTTPS.

One may replace this with the one issued by a **Certification Authority**. In any case earlier Exchange users will certainly appreciate that starting from the security of a self-signedcertificate is much better than starting from the no security of port **80** HTTP.

ONE YEAR LATER…

Those choosing to continue working with the self-signed certificate will have the opportunity to appreciate how time flies!! In fact Exchange will remind you of its first anniversary with events of the type:

Event Type: Warning
Event Source: MSExchangeTransport
Event Category: TransportService
Event ID: 12018
Date: 13/04/2008
Time: 09:01:00
User: N/A
Computer: EXSERVER
Description:
The STARTTLS certificate will expire soon: subject: exserver.domain.local, hours remaining: 157700393E5D76615E855A773CFA08AB5842DFB0. Run the New-ExchangeCertificate cmdlet to create a new certificate.

Event Type: Warning
Event Source: MSExchangeTransport
Event Category: TransportService
Event ID: 12017
Date: 13/04/2008
Time: 09:01:00
User: N/A
Computer: EXSERVER
Description:

An internal transport certificate will expire soon.
Thumbprint:157700393E5D76615E855A773CFA08AB5842DFB0, hours remaining: 295

The events are informative enough to point you to the right direction for resolving the issue i.e. calling the **New-ExchangeCertificate** cmdlet. **Exchange** is also kind enough to alert you days in advance. In the above event example we have 295 hours left, approximately 12 days.

You do check the event logs right? If not, or you simply ignore these events someone else will remind you! Most commonly **Outlook 2007** users will be amongst the first to start knocking at your door. If the certificate expires, opening Outlook will cause an annoying dialog saying:

exserver.domain.local
Information you exchange with this site cannot be viewed or changed by others.
However, there is problem with the site's security certificate…

GENERATING A NEW CERTIFICATE

Solving the problem is simple. To begin let see the currently installed certificate by running:

```
Get-ExchangeCertificate | List
```
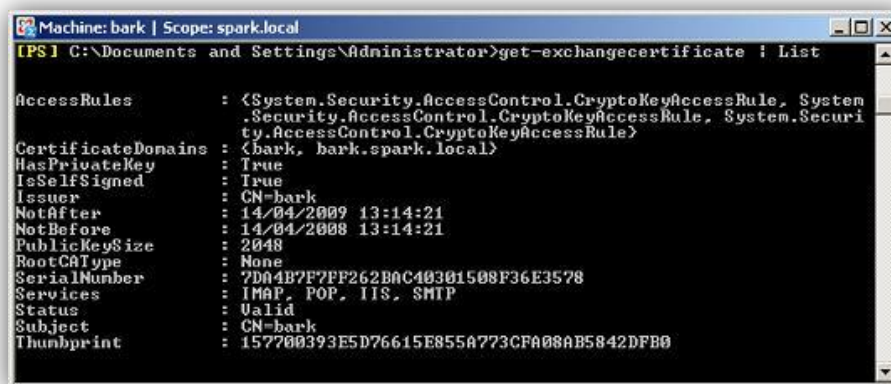

Note that here I am taking screen shots from a test machine whose certificate is not about to expire! Some properties worth noticing include:

NotAfter - shows the certificate expiry date
Services - shows that the certificate applies to **IMAP**, **POP**, **IIS** and **SMTP**
Thumbprint - will use this to identify and make changes to this certificate

Creating a new certificate is just a matter of running the cmdlet:

```
New-ExchangeCertificate
```

This will warn you about overwriting the **SMTP** certificate.

To be honest the first time I ran into this, I thought that was it. After all there were no more event log warnings. However this is not the case.

Re-running **Get-ExchangeCertificate** we see that the **IIS** service is still using the old certificate. This means **Outlook** users will still be knocking at our door.

We need to move the **IIS** service using **Enable-ExchangeCertificate**. To do this we need the thumbnail value of the newly created certificate. In my case I used this command:

```
Enable-ExchangeCertificate -Thumbprint F7A8F1B443A0E7266C72CDE0603302C07B856076 -Service IIS
```

With the new certificate in place we may now remove the old certificate using **Remove-ExchangeCertificate** with the thumbprint value of the old certificate:

```
Remove-ExchangeCertificate -Thumbprint 157700393E5D76615E855A773CFA08AB58
```