

UNIZETO



GENERAL
CERTIFICATION AUTHORITY



User's guide

Exchange 2007

SSL/TLS configuration on
Exchange 2007 Server

version 1.0

Table of Contents

1. GENERATING A REQUEST TO ISSUE A CERTIFICATE.....	3
2. SENDING REQUEST TO CERTUM.....	4
3. INSTALLING THE INTERMEDIATE CERTIFICATES	6
4. INSTALLING THE CERTIFICATE	7
5. BACKUP A CERTIFICATE AND PRIVATE KEY	8

1. Generating a request to issue a certificate

By default, Exchange 2007 mail server uses a certificate issued itself. However, it is possible to reconfigure the certificate obtained from a trusted certification authority. To configure your own certificate, you will have to generate a new request. You should open the management line of the Exchange Server (Exchange Management Shell).

Type the following command:

```
New-ExchangeCertificate -generaterequest -subjectname  
"o=Unizeto Technologies S.A.,ou=Bajeczna,cn=win2008.certum.local" -PrivateKeyExportable $true -  
path c:\win2008.certum.local.csr
```

The importance of each parameter is as follows:

- `generaterequest` – means the request and a new key pair generation,
- `subjectname` – here should be included names of parameters that occur in the certificate.

Note: Use only ASCII characters (without national diacritics).

All fields are not required. Depending on the class, purchased certificate may have different sets of attributes. In this case:

- `o` - the name of the organization, which will be placed on the certificate, in this case Unizeto Technologies SA
- `ou` - organizational unit. This could be for example "Sales"
- `cn` - common name. Key field. Includes the domain name under which you can see the mail server on the Internet.
- Other fields. Description of what field you put in a request can be found at MSDN: <http://technet.microsoft.com/en-us/library/aa998840.aspx>
- `PrivateKeyExportable ($ true)` - use generated keys as exportable. This means you can backup the private key and certificate, without additional tools.
- `path` - path to the file where you will save the request to issue a certificate.

2. Sending request to CERTUM

Once you have generated your request, please send them to CERTUM in order to obtain a certificate. Please visit www.certum.eu and select "SSL Certificates":



CERTUM offer will be presented. Please refer to our offer and select the type of certificate which will fit best your needs.



Click the "Buy Now" button on the desired type of certificate and log on to our portal. If you do not have an account on our site, please create one and sign up.
In the next step you should complete fields related to the certificate contract.

Start > Manage certificate > Buy Enterprise SSL

Buy Enterprise SSL

Your certificate request

Enter your certificate request (CSR) compliant with PKCS#10 in the following field:

Attention! Cryptographic keys in CSR must have at least 2048 bit length (for RSA or DSA algorithms) and 571 bit length (for EC algorithms: NIST K-571 and NIST B-571). CSR with shorter key length will not be processed.

E-mail address

Enter your e-mail address to receive further instructions.

E-mail:

Invoice details

I would like to receive an invoice of my purchase.

Cash Payment

I will pay 149.00EUR by Credit Card [PayPal](#)

The payment was made with activation card

Statement

certificate.

We provide our certification services in accordance with the rules set in the Certification Procedure Code (KPC) that becomes an integral part of this Declaration by reference. The Certification Procedure Code is available from the repository of CERTUM - Powszechnie Centrum Certyfikacji at the following address: <http://www.certum.pl/repozytorium/> or by e-mail, on request sent to: info@certum.pl.

In Poland, signing an instrument with this certificate has no legal consequences equivalent to those resulting from signing the instrument in person.

I agree

The most important is "Request a certificate". Paste here the request generated in the preceding paragraph. Please open the file with the request in a text editor (Notepad, Notepad + +) and copy the entire string from "----- BEGIN NEW CERTIFICATE REQUEST -----" and "----- END NEW CERTIFICATE REQUEST ---- -".

Note: It is important to copy the entire string, including the above-mentioned strings.

Attention!
Exchange 2007 generates a request with a break before the tag
----- END NEW CERTIFICATE REQUEST -----.
You have to remove the break.

Then complete details for the invoice - you will need to issue an invoice. Do not forget to include your e-mail. There will be sent information relating to the handling of certificates. This can be for example a message with activation link or reminders for expiring certificate.

In the next step please select a payment method, read the statement carefully and then accept them. At the end, press "Next" button.

The next step is to verify the domain. This can be done in two ways. The first way is to verify the domain name and address from the e-mail. Domain Verification involves placing a special tag on the sides which are verified. Review your e-mail and then click the special link in the message. The second way is to send the verification documents. Person who carries forward the process will receives them, and then CERTUM can verify domain membership of the organization.

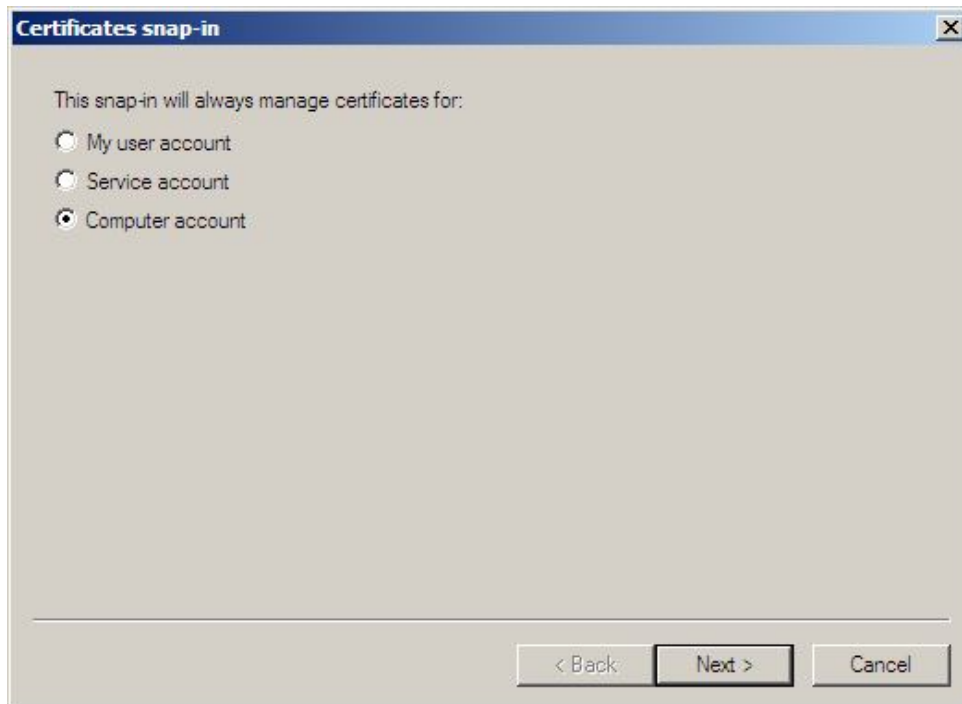
3. Installing the intermediate certificates

Intermediate certificates are very important element. It must be installed on a Web Server to let the web browser verify certificate issuer.

Please visit www.certum.eu top menu and select "Manage certificate" and then "certificates and keys." Please save your certificates Certum CA Level I, Level II, Level III and Level IV. Choose your server certificates for SSL / TLS.

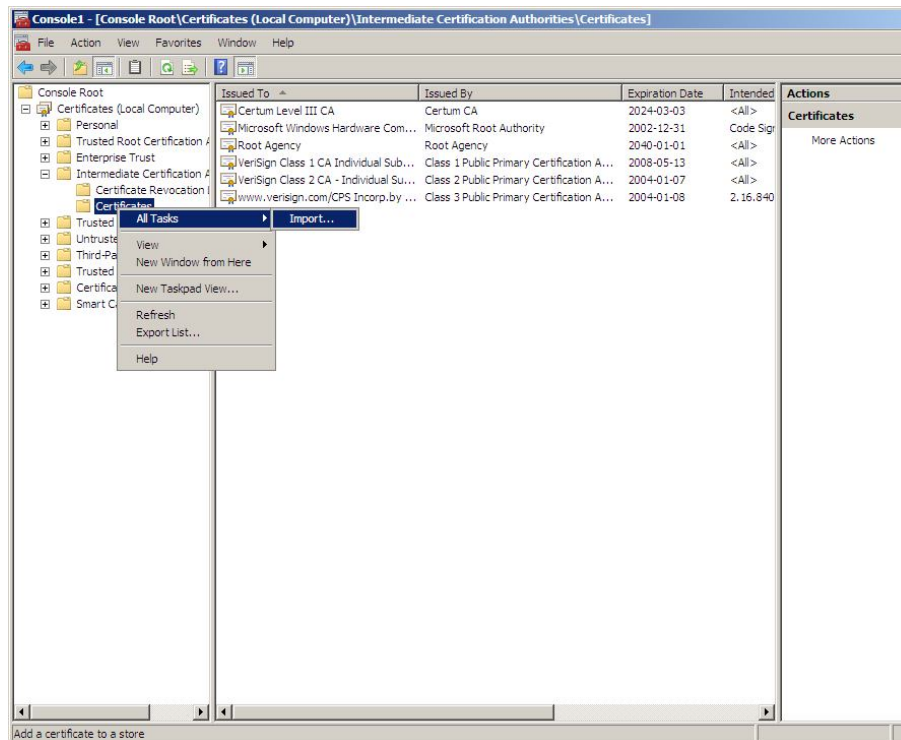
Please press the key combination [Winkey + R] type `mmc.exe`. This starts the editor MMC snap. On the File menu, select "Add / Remove Snap-in". In the new window you have to click on the Add button and then point to Snap "Certificates" and press "Add" button.

This brings up a window similar to the following:



Please select "Computer account" and click "Next". On the next screen, please indicate the local computer and click "Finish".

In the left panel of the newly opened window, please expand the "Certificates intermediate offices." Please right-click on the folder "Certificates" and from the context menu, select "All Tasks" then "Import ...".



The setup wizard will guide you through the installation of intermediate certificates. You have to indicate CA Certum Level I CA and as a warehouse for installation select "Intermediate Certification Authorities" (this should be the default choice). Previous steps must be repeated for certification authorities CA Cetum Level II, Level III and Level IV.

4. Installing The Certificate

After the proper verification you will receive an e-mail with the installation ID.

To activate your certificate, please go to the page specified in the message and paste the ID installation certificate. After pressing the "Activate" you will see a new page, where you can download the certificate. Please save your certificate on your hard disk by selecting "Save Binary". The next step is to install the certificate in Exchange Server 2007. Turn on the management console server and issue the command:

```
Import-ExchangeCertificate -path path_to_file.cer -friendlyname "win2008.certum.local"
```

Individual parameters have the following meanings:

- path - the directory where you stored the certificate
- friendlyname - name under which you will see the certificate in the certificate store

Then find the fingerprint of the installed certificate. In the management console and issue the command:

```
Get-ExchangeCertificate -DomainName "win2008.certum.local"
```

You will see the installed certificates and their fingerprints. Output should be similar to that shown in the picture:

```
[PS] C:\Windows\System32>Get-ExchangeCertificate -DomainName "win2008.certum.local"
```

Thumbprint	Services	Subject
7E829F05B52C98A498EE07A309A0073836FDD618	IP.WS	CN=win2008.certum.local, O=Unizeto Technolo...
91B2243030641B8992FB3149129ED29ECAA7CCD0	IP..S	CN=WIN2008
6CB3E7545797173B8F037E69DFE63B4E717F3FF1	IP..S	CN=WIN2008

```
[PS] C:\Windows\System32>_
```

You have to copy the thumbprint of the certificate issued by CERTUM.

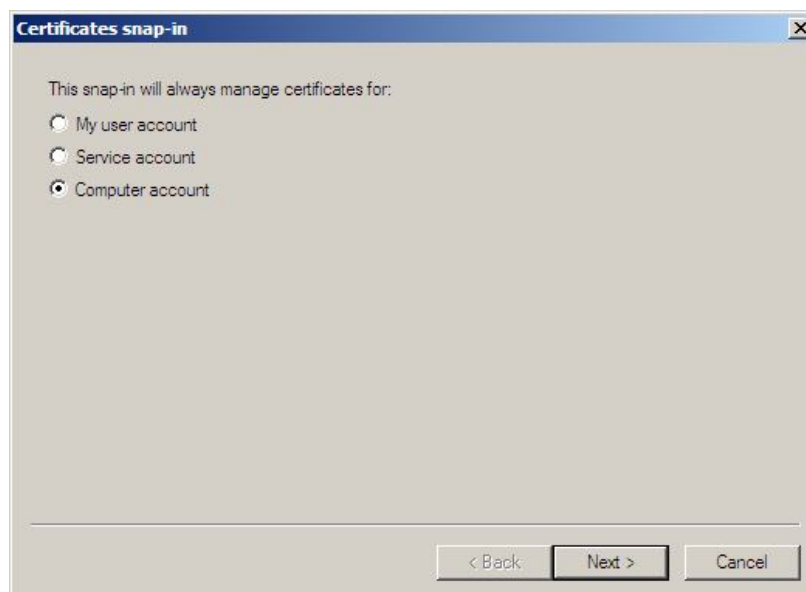
The next stage of implementation is to assign a certificate to each services of the Exchange server. You have to type the command:

```
Enable-ExchangeCertificate -thumbprint <thumbprint> -services "IIS,POP,IMAP"
```

After this, you should restart the server. Configuring the certificate has been completed.

5. Backup a certificate and private key

In the "Run" window please enter mmc.exe. This starts the editor MMC snap. Choose the "File" menu, select "Add / Remove Snap-in". In the new window select "Certificates" and click "Add". In the next window, please select your computer:



Now select "Local Computer" and please expand the "Personal" and "Certificates". Please right-click on the icon of the certificate and the context menu select "All Tasks" > "Export". This starts the Certificate Export wizard. While exporting you have to select the following options:

- "Yes, export the private key (Step 1)
- "Enable strong private key protection" (Step 2)
- "If it is possible to attach all certificates in the certification path" (Step 3)

After selecting this option, you have to provide a password to protect your private key (Step 4).

The last step is to identify the location where you saved the file in PKCS12 format. It will contain a backup copy of a private key and certificate.