

OCSP part 6 – Test OCSP service

Author : Tobias Hofmann

Date : July 21, 2016

To test if OCSP is working, you need to have a certificate with OCSP information included. This is only available for certificates emitted AFTER the service was installed, configured and activated on the CA. Therefore, you'll need to first create a new certificate for your tests. Depending on your CA configuration, you can use OpenSSL to create a request or will have to use the Windows integrated tools. I will show here how to use a CSR created by OpenSSL and a Windows Enterprise CA.

Create CSR with OpenSSL

```
openssl req -new -newkey rsa:2046 -nodes -keyout dummy.key -out dummy.csr
```

```
\OpenSSL-win32\bin>openssl.exe req -new -ne
wkey rsa:2048 -nodes -keyout dummy.key -out dummy.csr

Generating a 2048 bit RSA private key
.....
.....
.....
+++
.....+++
writing new private key to 'dummy.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:Rio de Janeiro
Locality Name (eg, city) []:Rio de Janeiro
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SAP
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:dummy
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

This creates a key file and the CSR in Base64.

Submit CSR to CA

Certificate snap-in

MSFT Enterprise CA needs the CSR created for a specific template, something that OpenSSL is not offering. If you submit such a request to the CA via MMC, you get an error message.

It's full of stars!

Where documentation meets reality

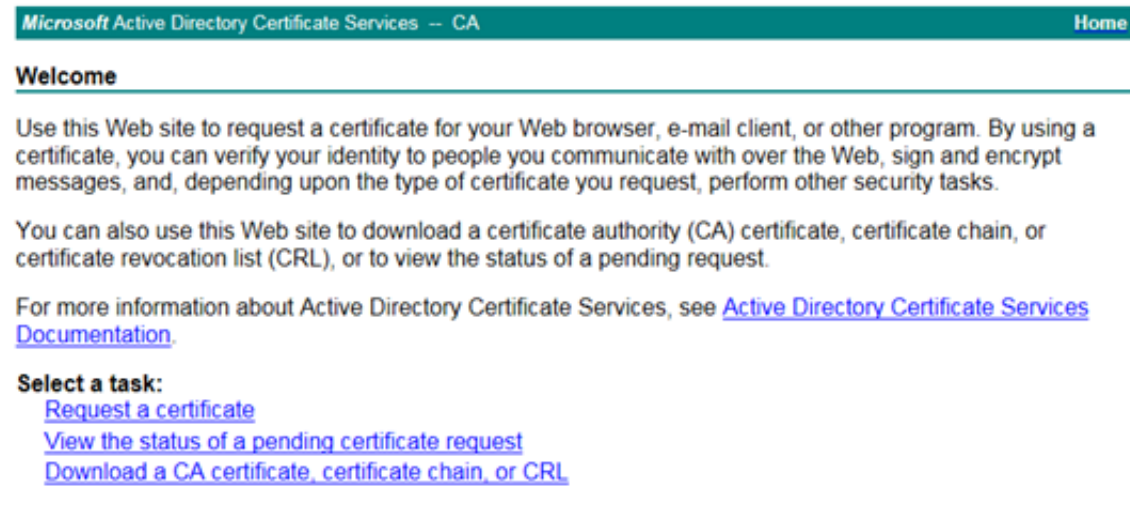


More information

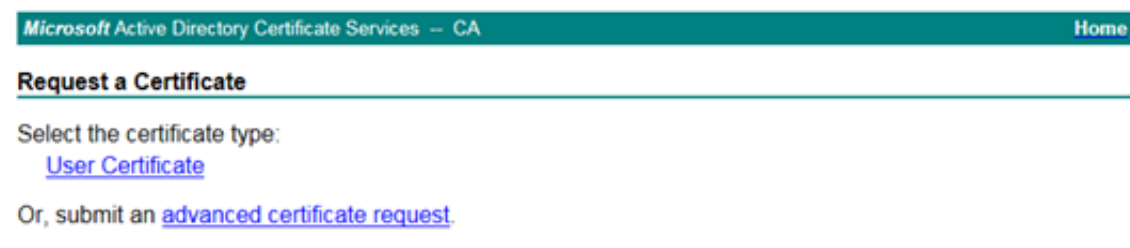
- <https://support.microsoft.com/en-us/kb/910249>
- <https://technet.microsoft.com/en-us/library/cc782583.aspx>

CA Web Interface

Open the web enrollment server in your browser. Click on Request a certificate.



Go to the advanced options.



Paste the Base64 encoded CSR in the input field. Select as certificate User.

It's full of stars!

Where documentation meets reality

Microsoft Active Directory Certificate Services -- CA Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIICojCCAYoCAQAwxTElMAkGA1UEBhMCQ1IxIzAV
aXJyMRcwFQYDVQOHDA5SsW8gZGUgSmFuZW1ybzEM
VQQDDAVkdW1teTCCASIwDQYJKoZIhvcNAQEBBQAD
glly7uvKXet7aeMpQPoIk20FJbYKQOCTtRdpKyo6r
LvqPcJUTzBi4BZfefB7B77PiaDwv3kTn/1tXQ5uM
```

Certificate Template:

User

Additional Attributes:

Attributes:


Submit the request and download the generated certificate.

Microsoft Active Directory Certificate Services -- CA Home

Certificate Issued

The certificate you requested was issued to you.

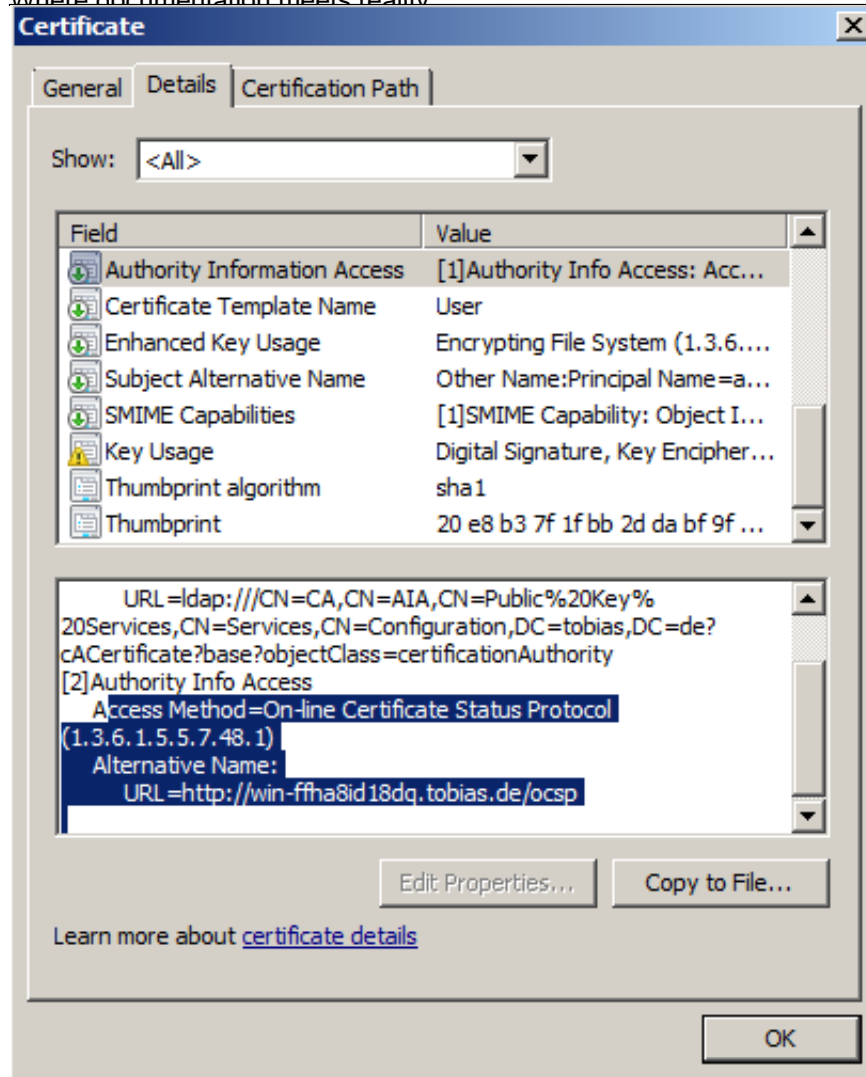
DER encoded or Base 64 encoded

 [Download certificate](#)
[Download certificate chain](#)

Take a closer look at the certificate. In the AIA section, OCSP must be shown.

It's full of stars!

Where documentation meets reality



Test OCSP service

In the above step, a new user certificate was created, containing OCSP information. To test if OCSP is working, Microsoft is offering the certutil tool.

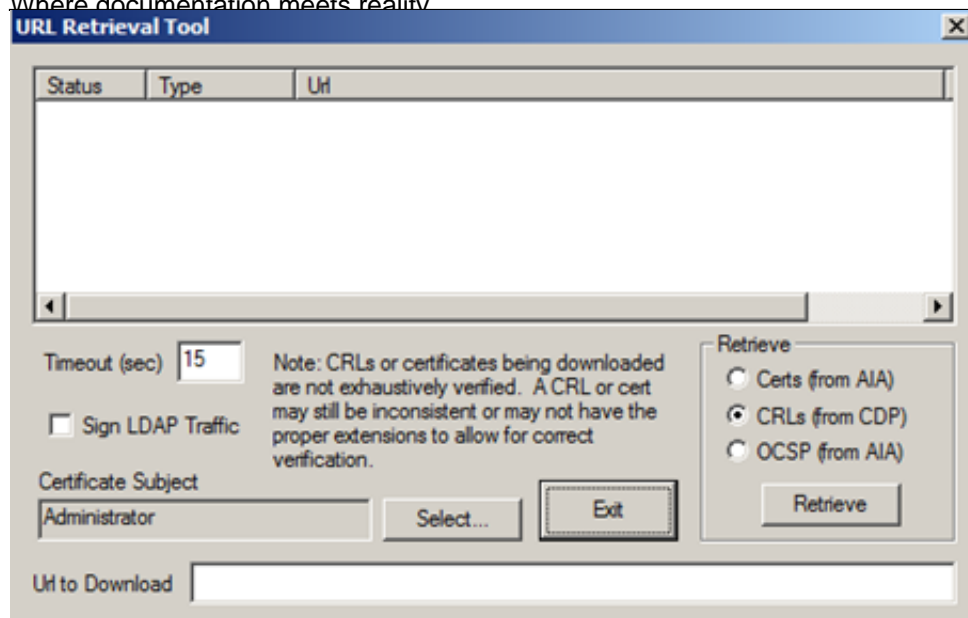
certutil -URL dummy.cer

```
C:\Users\Administrator\Desktop>certutil -URL dummy.cer
```

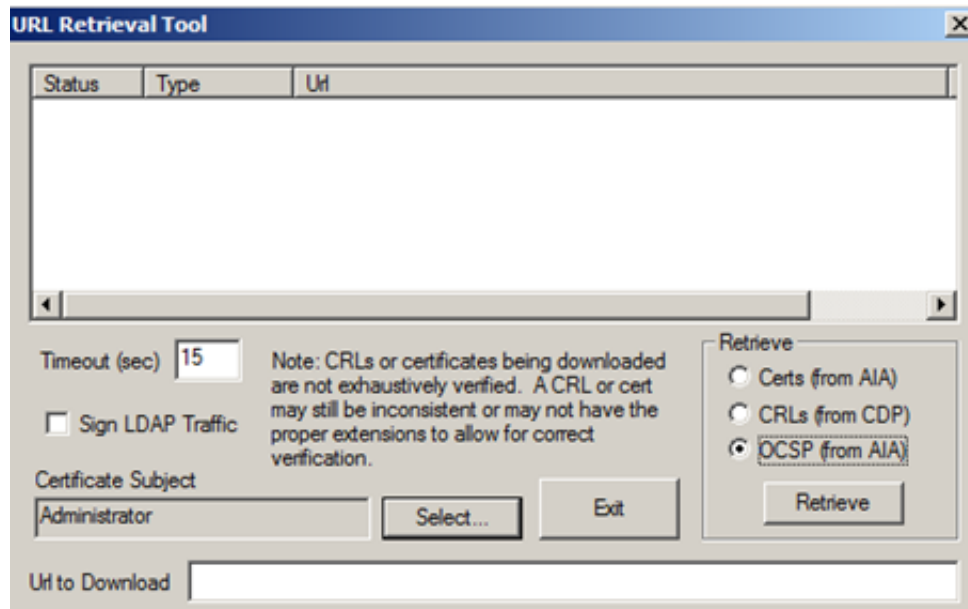
In the Retrieve box, you can select how to certificate information should be retrieved.

It's full of stars!

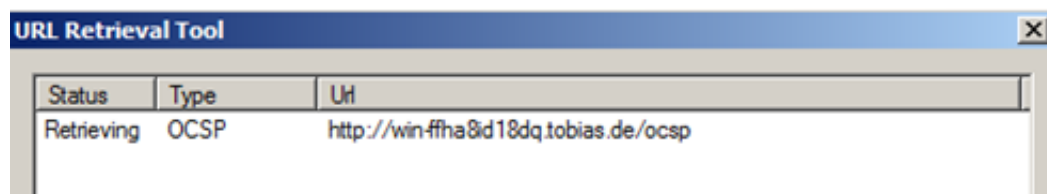
Where documentation meets reality



Select OCSP.



Check the status



Result: Failed

Status	Type	Url
Failed	OCSP	http://win-ffha8id18dq.tobias.de/ocsp

Result: Unsuccessful

Status	Type	Url
Unsuccessful	OCSP	[0.0] http://win-ffha8id18dq.tobias.de/ocsp

Result: Verified

Status	Type	Url
Verified	OCSP	[0.0] http://win-ffha8id18dq.tobias.de/ocsp