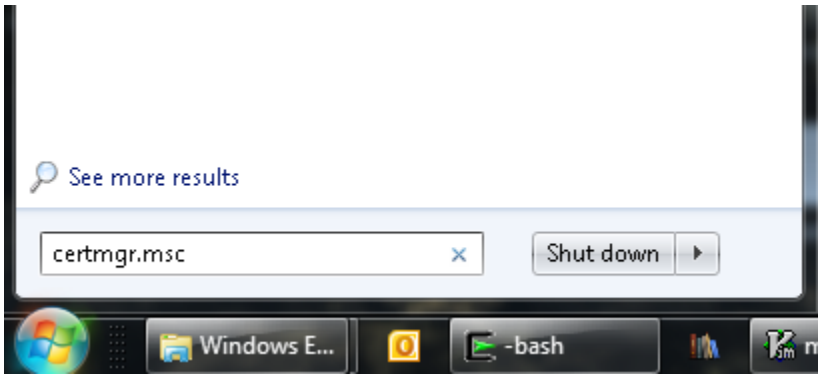
How to obtain your SINTEF x509 user certificate

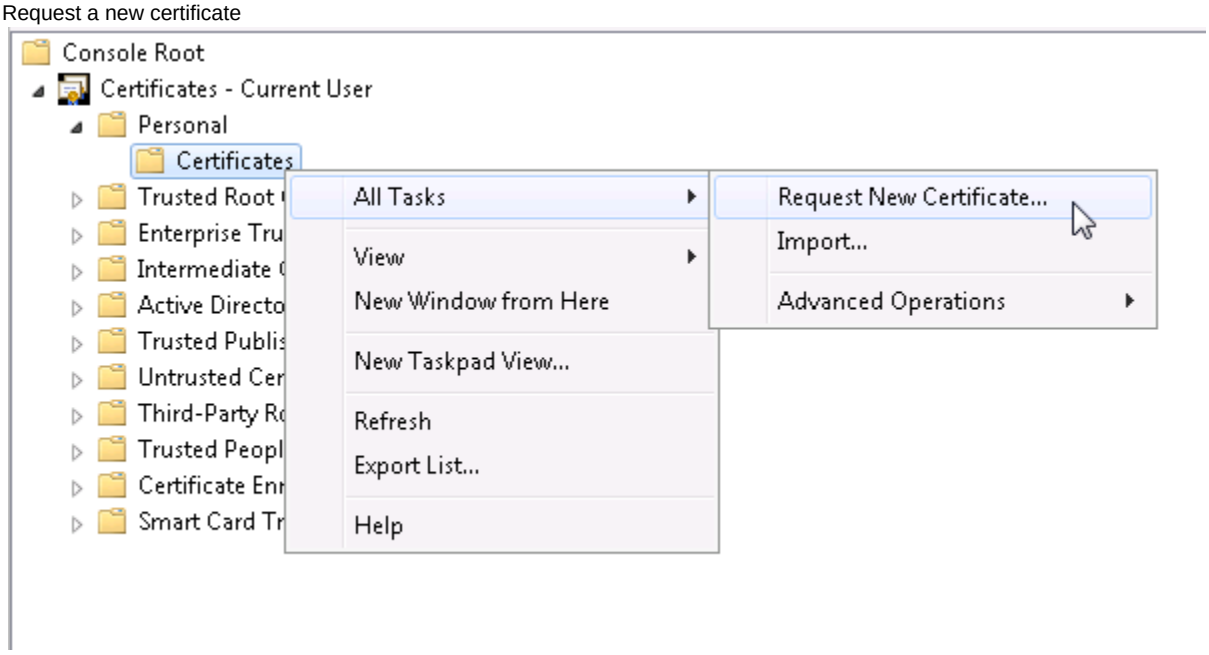
A step by step procedure to obtain a x509 certificate for a SINTEF user from the SINTEF Certificate Authority.

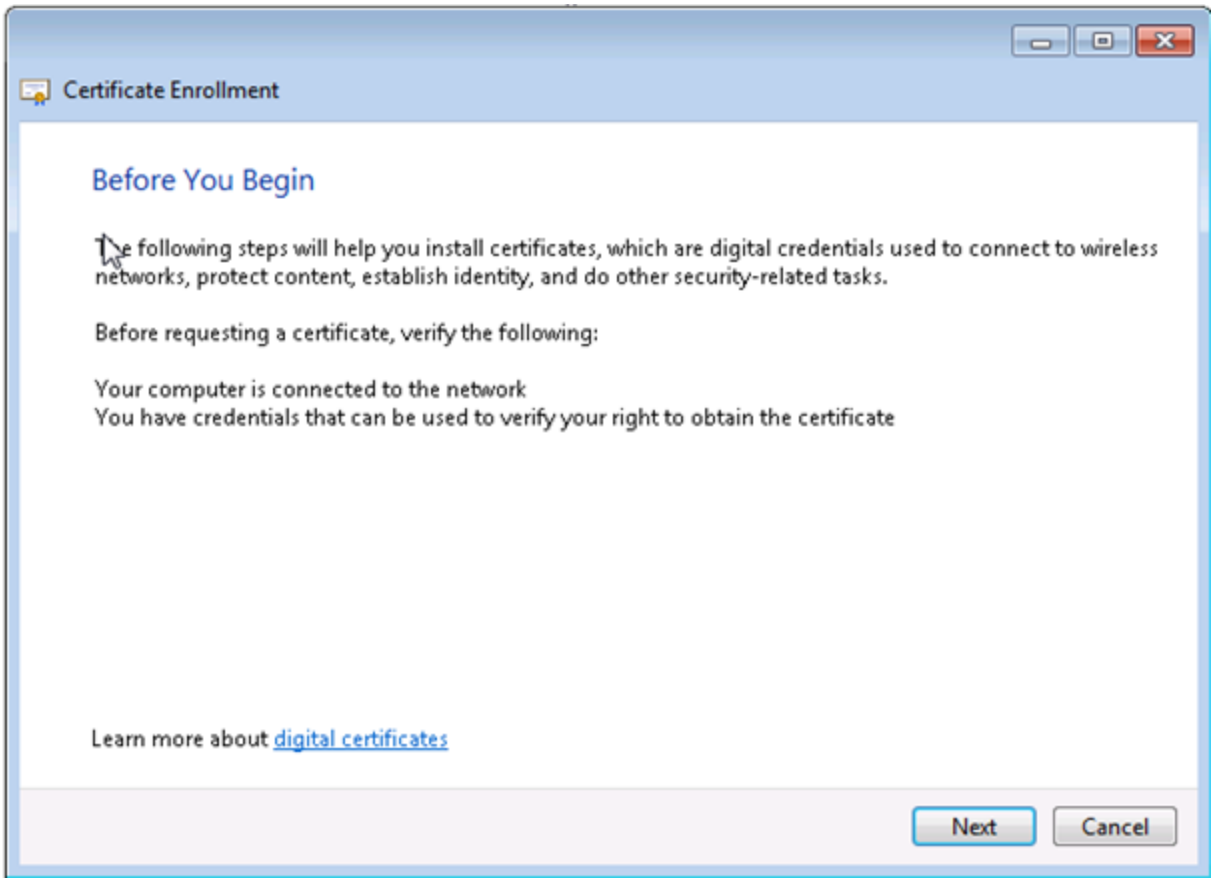
For users with access to a SINTEF Windows client machine

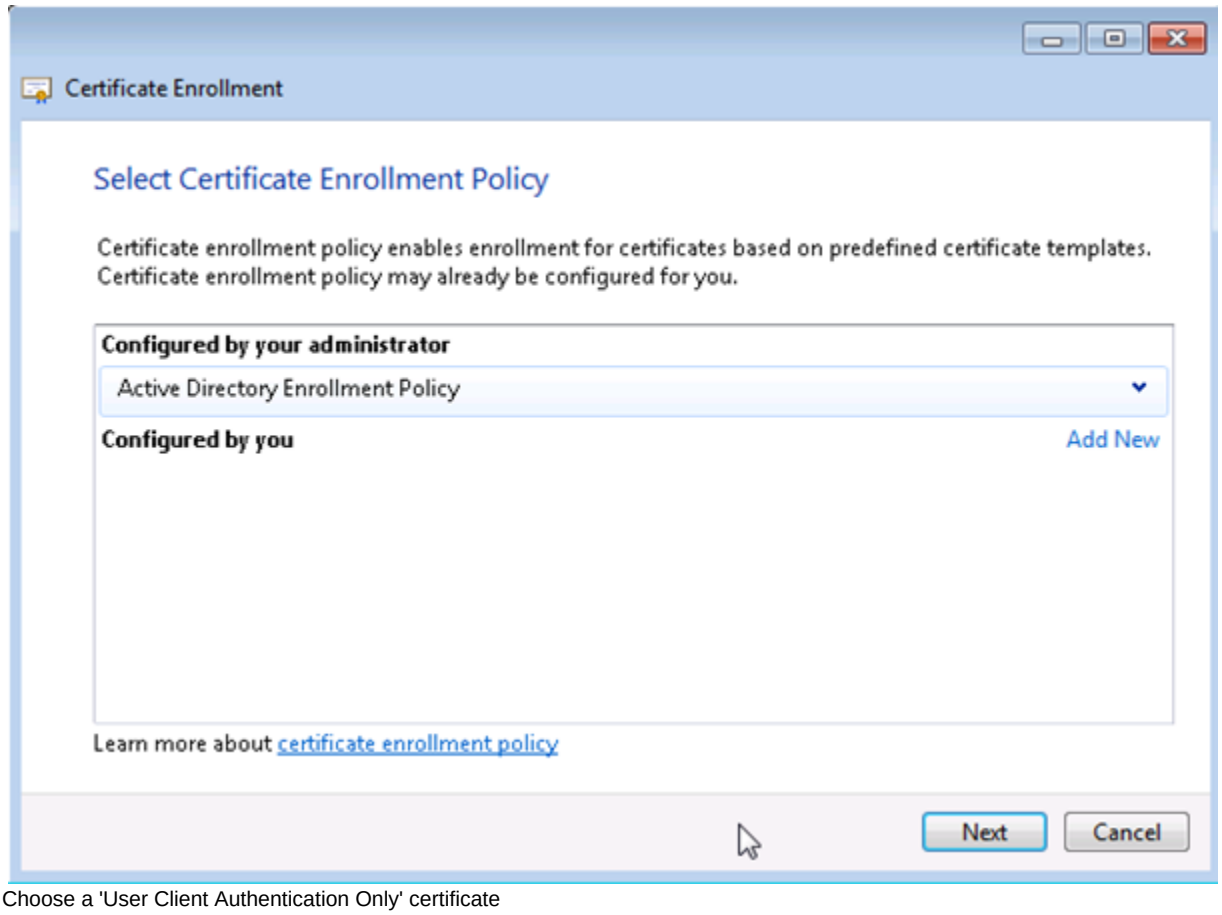
1. Start certmgr.msc:



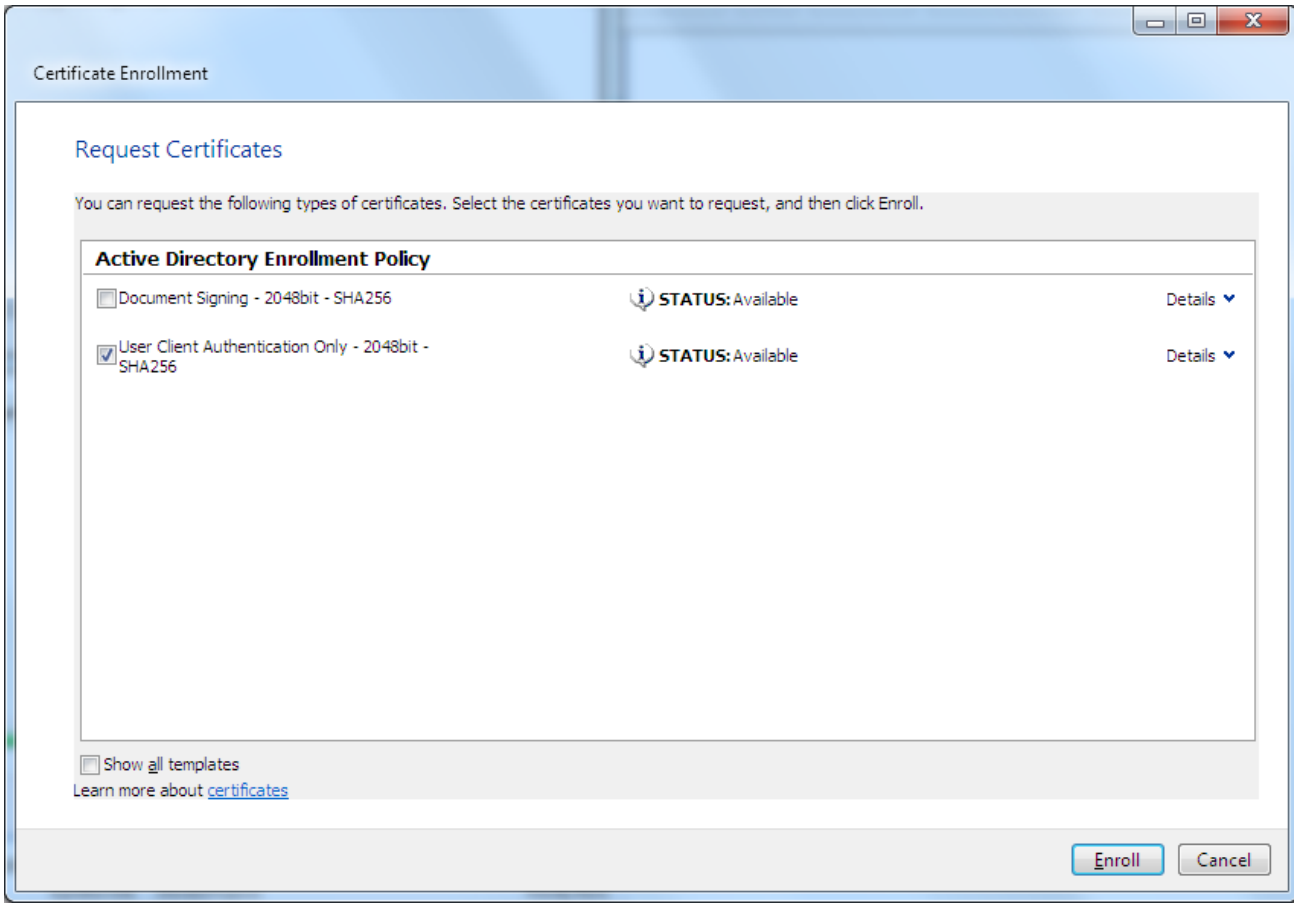
2. Request a new certificate

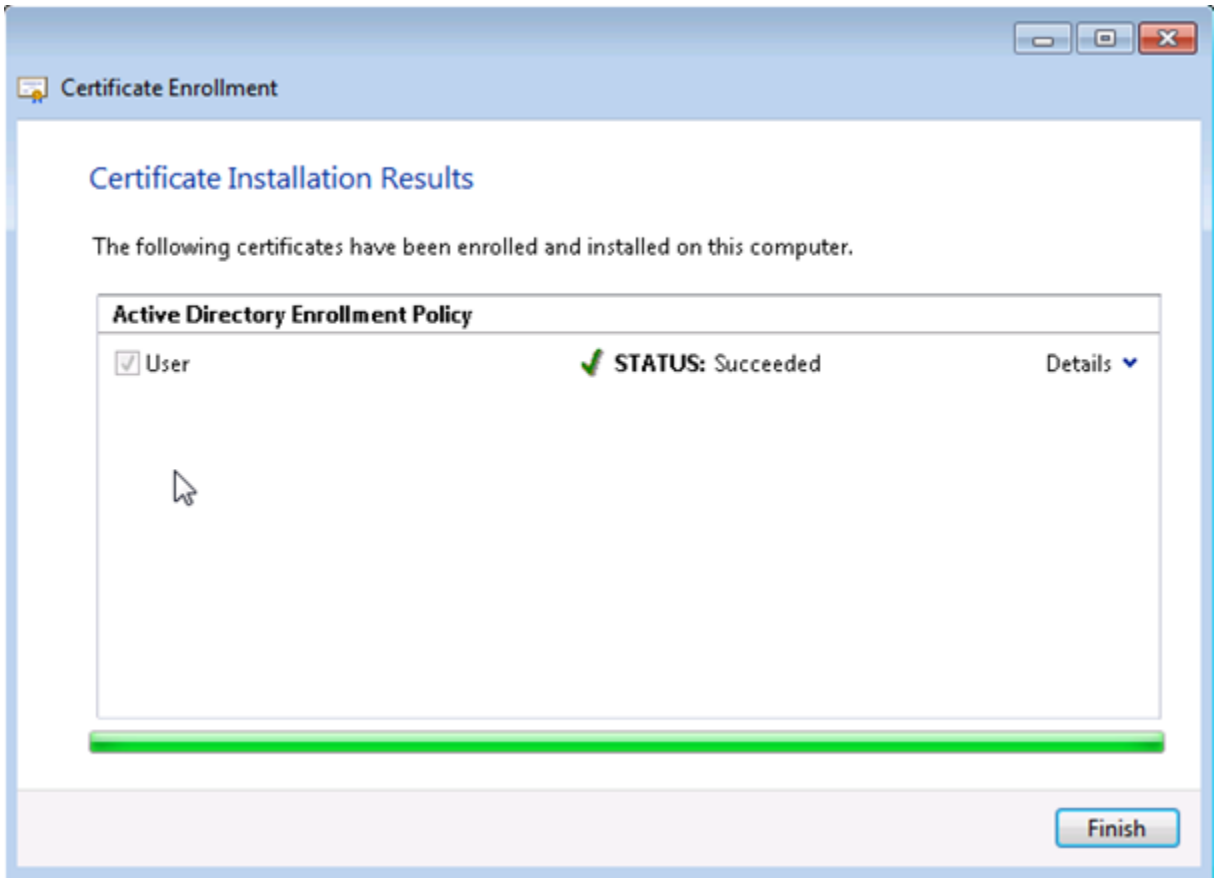




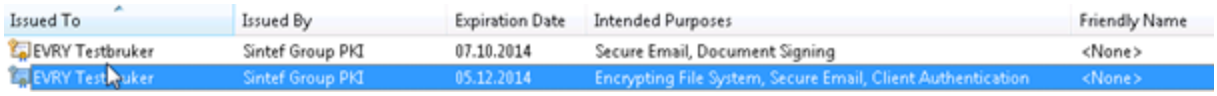


3. Choose a 'User Client Authentication Only' certificate



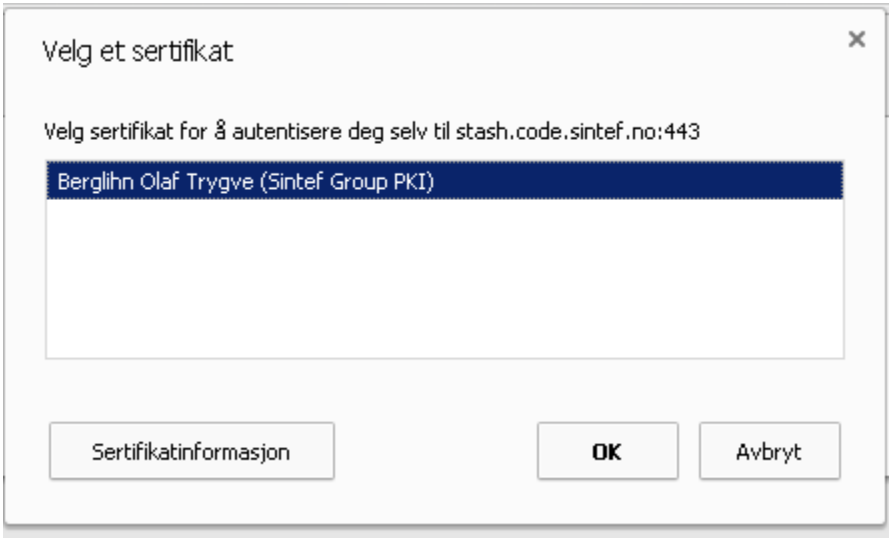


4. You will now see a new certificate in User Store:



For users of Windows with Internet Explorer, Google Chrome or Safari

You are now ready to go. The browsers will use your certificate when accessing the code.sintef.no services. You might be prompted to select a certificate from a list when you open the code.sintef. no pages in a new browser session.



For users of browsers that do not use the Windows certificate store - Firefox, Mac OS-X users, etc.

You will have to export the certificate from the Windows certificate store:

1. Right-click on the certificate (e.g. *EVRY Testbruker* in the image above), click *All Tasks* and then select the *Export...* item. This opens the *Certificate Export Wizard*.
2. Click *Next*, select *Yes, export the private key* and then click *Next* again.
   Verify that the *Personal Information Exchange - PKCS #12 (.PFX)* item is selected. Also tick the check box for *Include all certificates in the certification path if possible*. (It does not appear to be necessary to tick any of the other boxes.) Click *Next* again.
3. Enter a password of your choosing and click *Next*. (You need this when importing the certificate in Firefox again.)
4. Select a file name/location and click *Next*.
5. Click *Finish* to export the certificate.

Firefox:

Start Firefox and do the following to import the certificate:

1. Click the *Firefox* menu in the top left corner, select *Options* and then *Options* again. (On Linux, select *Edit*, then *Preferences*.)
2. Go to the *Advanced* section, open the *Certificates* tab and click *View Certificates*.
3. Under *Your Certificates*, select *Import...* and select the file you exported earlier.
4. Enter the password you chose during export.

The certificate is now installed and can be used by Firefox (but you have to confirm that you want use it the next time you try to log on to any of the code.sintef.no services).

For users without access to a SINTEF Windows client machine

This procedure constists of 3 steps:

1. Making a certificate request.
2. Enrolling for a certificate.
3. Installing the certificate on your client compter.

Find the relevant instructions for your operating system for each step in the text below.

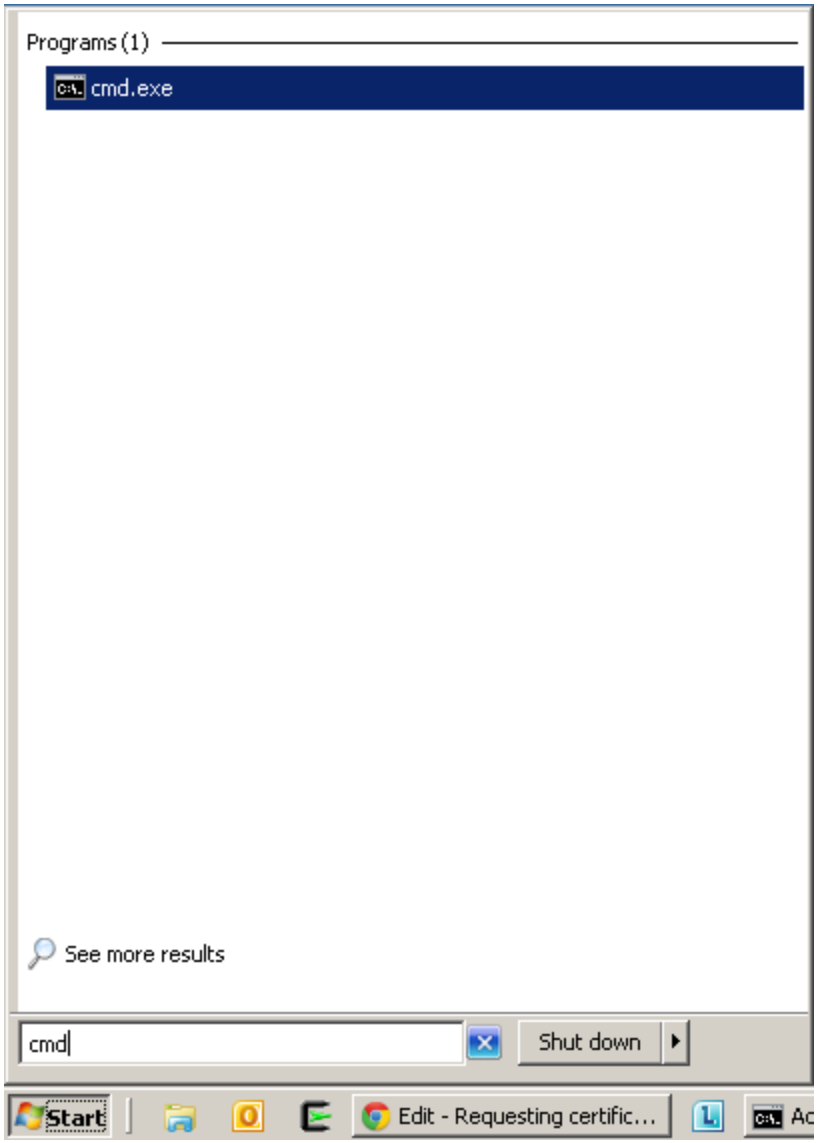
Making a certificate request

Windows

1. Edit the file request.txt and modify values as indicated. Save the file as request.txt in the "My Documents" folder.

```
;----------------- request.txt -----------------
[Version]
Signature="$Windows NT$"

[NewRequest]
; C: two letter country code
; O: organization name
; CN: Common name, typically "Givenname Familyname"
; Change bellow to your country code, organization, common name and email address.
Subject = "C=no, O=Your organization, CN=Your Name, E=your.email@company.tld"

; Leave these values
KeySpec = 1
KeyLength = 2048
Exportable = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.2
```

2. Open a command shell



3. Use the commands "cd %userprofile%\Documents" to move to the folder where you put the request.txt file:

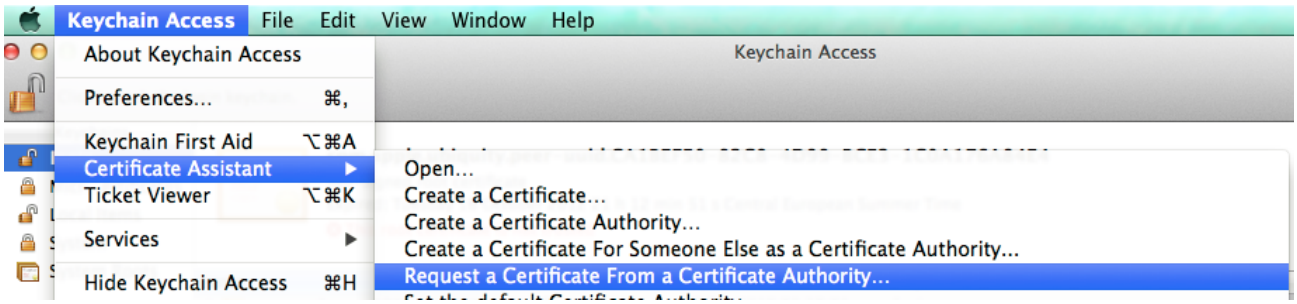
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.


C:\Users\oberg>cd %userprofile%\Documents
C:\Users\oberg\Documents>
```

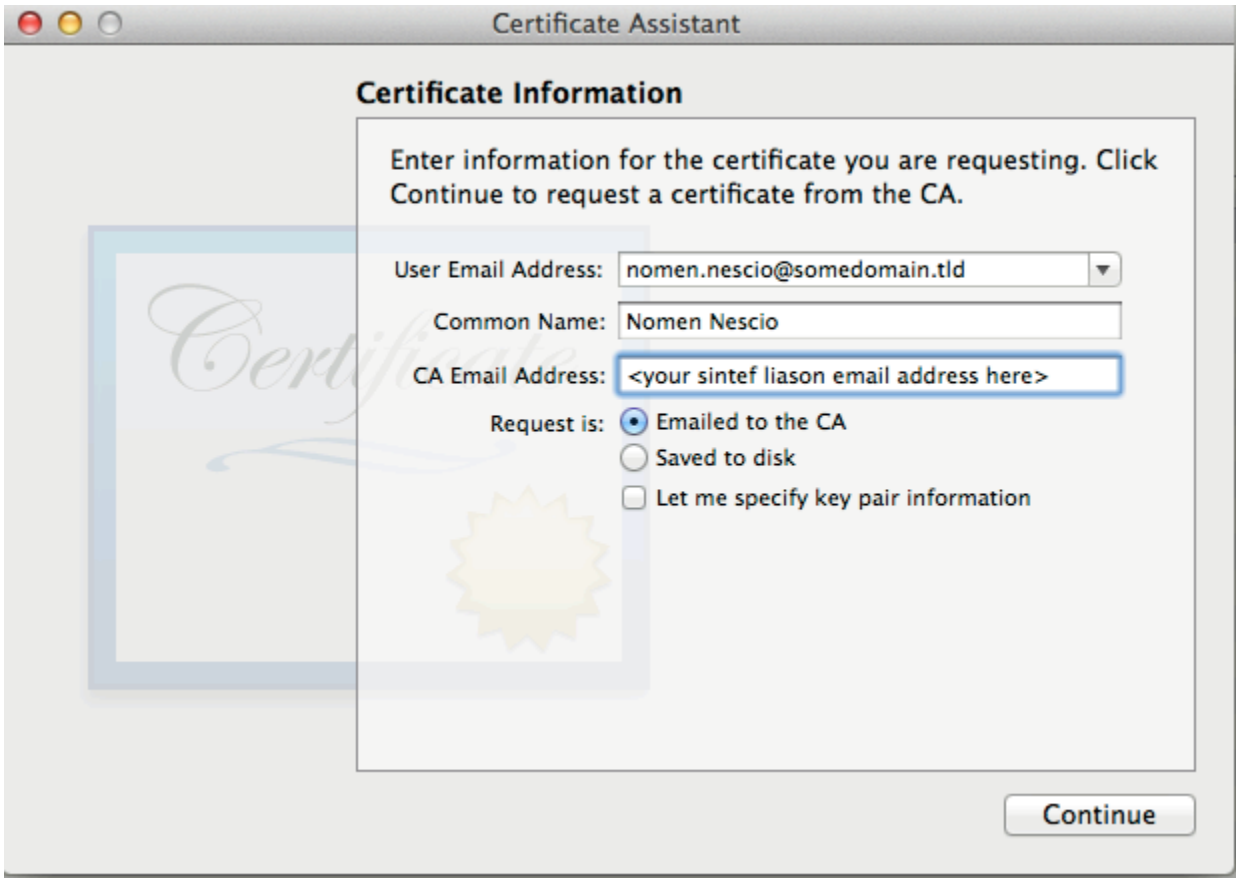
4. Type the following command to generate the certificate request file "certreq.txt"

```
C:\Users\oberg\Documents>certreq  -new request.txt certreq.txt
C:\Users\oberg\Documents>
```

Apple OS-X

1. Open the key chain application found in Programs->Utilities->Keychain access (Programmer->Verktøy->Nøkkelringtilgang)
2. Select the keyring "login" (pålogging).
3. Create a certificate request (Nøkkelringtilgang->Sertifikatassistent->Be om et sertifikat fra en sertifikatautoritet...)





Select "Saved to disk" and press "Continue".

Linux, BSD and other systems

Generate an RSA private key (Triple DES 2048 bits). Make sure you keep the private key file safe (code_sintef_no.key). Never share this file it with anyone. If you have already created a RSA private key, you can reuse this.

```
$ openssl genrsa -des3 -out code_sintef_no.key 2048
2048 Generating RSA private key, 2048 bit long modulus
..............................+++
..................................+++
e is 65537 (0x10001)
Enter pass phrase for code_sintef_no.key:
Verifying - Enter pass phrase for code_sintef_no.key:
$
```

Generate a certificate request by editing the file conf.txt containing the following

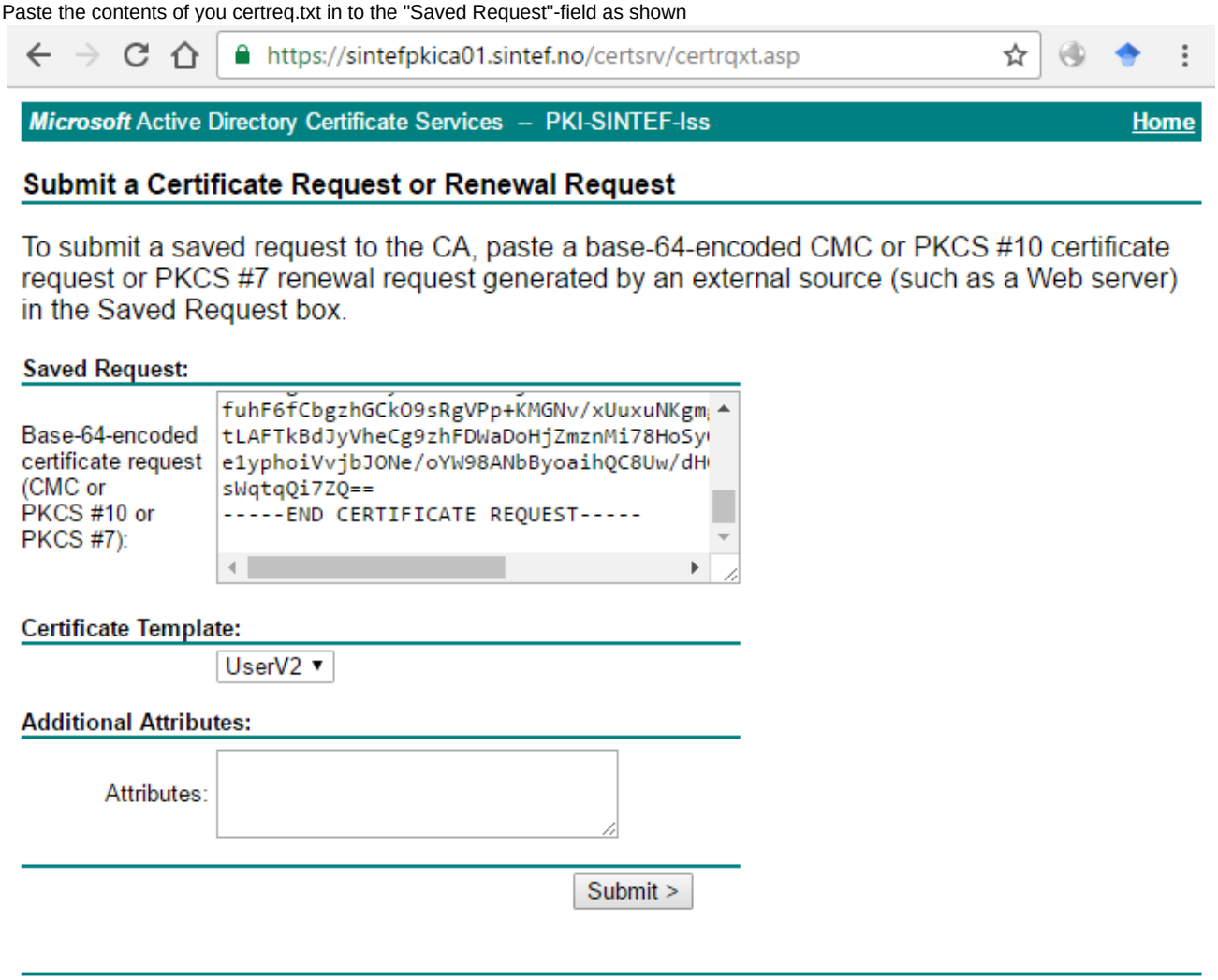
```
# Example file conf.txt for openssl req command

# No need to change anything in the req section.
#
[ req ]
default_bits        = 2048
default_md          = sha256
prompt              = no
string_mask         = utf8only
distinguished_name  = req_distinguished_name
req_extensions      = req_cert_extensions

# Below, you should set your country two letter code,
# company affiliation and your full name.
#
# Use two letter short name for country as found here:
# https://www.digicert.com/ssl-certificate-country-codes.htm
# Examples: Norway=NO, Sweden=SE, USA=US, Great Britain (UK)=GB
#
[ req_distinguished_name ]
countryName         = NO
organizationName    = Your organization name
commonName          = Your full name

# Below, you should set your email address as indicated
# with the dummy your.email@company.tld
#
[ req_cert_extensions ]
extendedKeyUsage    = clientAuth
subjectAltName      = email:your.email@company.tld
```

Create the certificate request

```
$ openssl req -new -config conf.txt -key code_sintef_no.key -out
certreq.txt
```

Enrolling for a certificate

1. **Go to the site https://sintefpkica01.sintef.no/certsrv/certrqxt.asp**
2. Log in with SINTEF username and password if required.
3. Paste the contents of you certreq.txt in to the "Saved Request"-field as shown

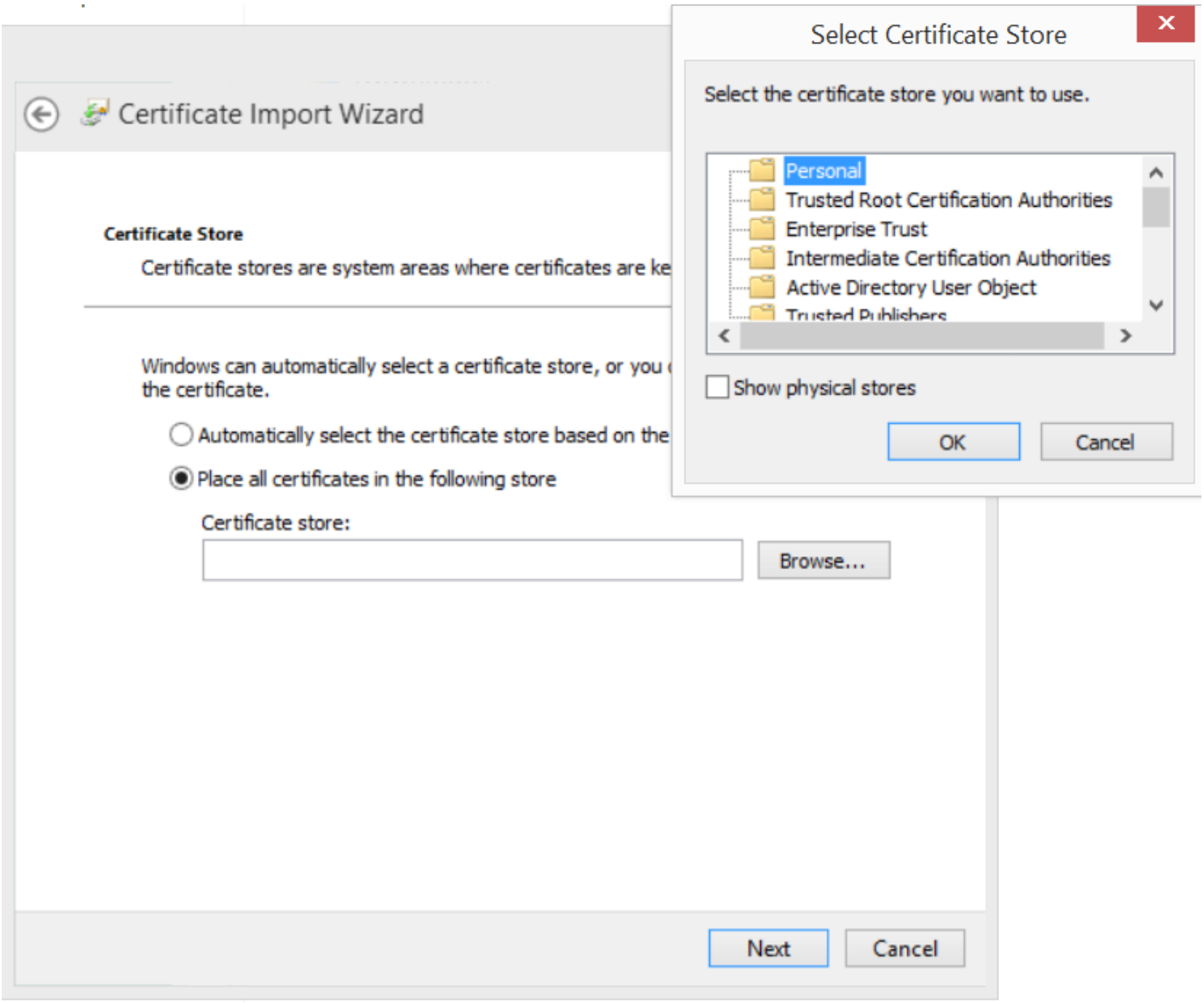


4. Then click **Submit**.
5. New certificate has now been enrolled. Press select the "Base64-option" and "Download certificate chain", which will give you a file "certnew.p7b" for download.
6. Save your request to file by supplying a filename and press <Finish>.

Installing the certificate on your client computer

Windows

Locate the file certnew.p7b that you downloaded, left-click with the mouse button, and choose "Install Certificate".



After installing the certificate successfully, point your web browser to https://www.code.sintef.no

Apple OS-X

1. Double click the certnew.p7b file to install the certificate.
2. You are now ready to use the code.sintef.no services by pointing the Safari browser to https://www.code.sintef.no . When accessing the services with Safari, you will get the following prompt (with your name instead of "Nomen Nescio"):

Press "Allow" or "Always Allow" and you will arrive at the login page.

Linux, BSD, and other systems

You can combine the private key and your certificate to a PKCS#12 file which are recognized by most web browsers. Install the certificate in your web browser as described in your web browser manual. Note that the .p12 file contains your private key, so you should keep this file safe and never share it with anyone.

```
$ openssl pkcs7 -inform pem -in certnew.p7b -print_certs -out
code_sintef_no.pem
$ openssl pkcs12 -export -in code_sintef_no.pem -inkey code_sintef_no.key
-out code_sintef_no.p12
$
```

After importing the .p12-file in your broser, point the browser to After installing the certificate successfully, point your web browser to https://www.code.sintef.no

Keep your certificate safe

Your certificate is an access token. If you export the certificate from the Windows certificate store, make sure you keep the exported certificate file safe.

- Your certificate is personal.
- Your certificate should not be shared with anyone.
- Do not distribute the certificate file by email.
- Do not even send the certificate file by email to your own email account, neither private email-accounts nor your SINTEF email-account.

A violation of the above will significantly compromise security and is on par with giving someone your SINTEF access card or keys to door locks.

Using the certificate for other purposes

Notice that the user also has Secure Email and Document Signing capabilities. This is a part of the SINTEF 'autoenrollment'-policy and enables e.g. signing of PDF-documents, etc.