Getting access for non-SINTEF users

External users will have to create a certificate request.

> **Instructions are for non-SINTEF users**
> The following instructions are to be followed by non-SINTEF users. The certificate request is to be generated by the non-SINTEF users. By no circumstances should a SINTEF employee generate the certificate request on behalf of the non-SINTEF user.

If you are a SINTEF employee and want to request access for a person not employed by SINTEF, please confer this page: Requesting access for non-SINTEF users

Background

Accessing code.sintef.no services requires the use of public-private cryptography. In brief, we will instruct you to use a private key by which you can generate a request for a digital certificate. Your private key is yours only, and we at SINTEF will never see this key nor know its contents. You should safeguard your private key so nobody else gets possession of it. Your private key is never transmitted over the network when contacting the code.sintef.no services. Note that if you are using Microsoft Windows, the private key you generate will be kept safe by the operating system and not written to file.

Using your private key, you can generate a certificate request. This results in a request file which you can use in a web service at SINTEF to enroll for a certificate. The combination of your private key and the certificate is used by your web browser in order to gain access in a very secure manner.

The certificate request and certificate file are not sensitive and can not be misused by anyone. Only your private key is sensitive, and should as the name implies be kept private.

The process of making a private key and generating a certificate request is partly automated by programs on your computer. Below are specific instructions depending on the operating system you are using.

The validity of this certificate will be 2 years from the date of enrollment, after which you can re-enroll if you still have an active account status with SINTEF.

> **Take care of your private key**
> - The private key is never transmitted over the network and is only known to you.
> - Should you lose or delete it, this will be a permanent loss. It can not be reconstructed.
> - You should safeguard your private key and not share it with others.
> - In case of accidental loss or theft of your private key, you should immediately inform your SINTEF contact.

Creating a user account at code.sintef.no

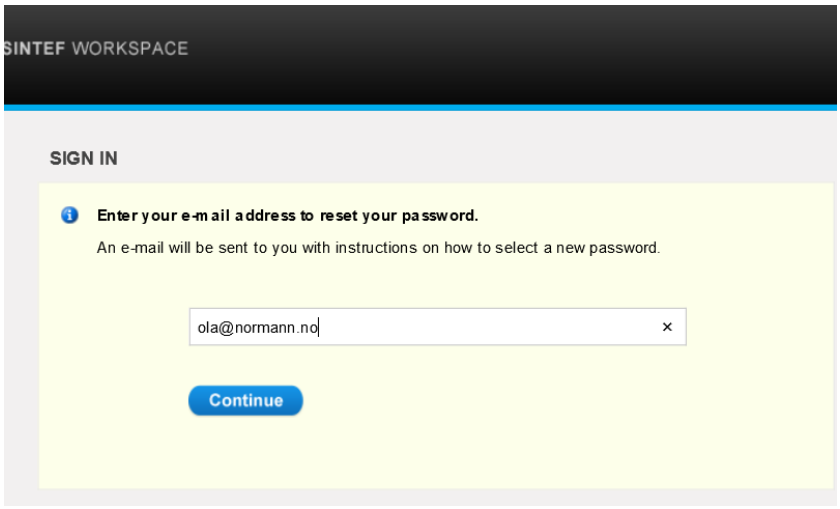
Your SINTEF contact will order the creation of a user account in the SINTEF infrastructure. You as a user must supply the following information to your SINTEF contact

1. Your full name
2. Your mobile phone number
3. Your email address

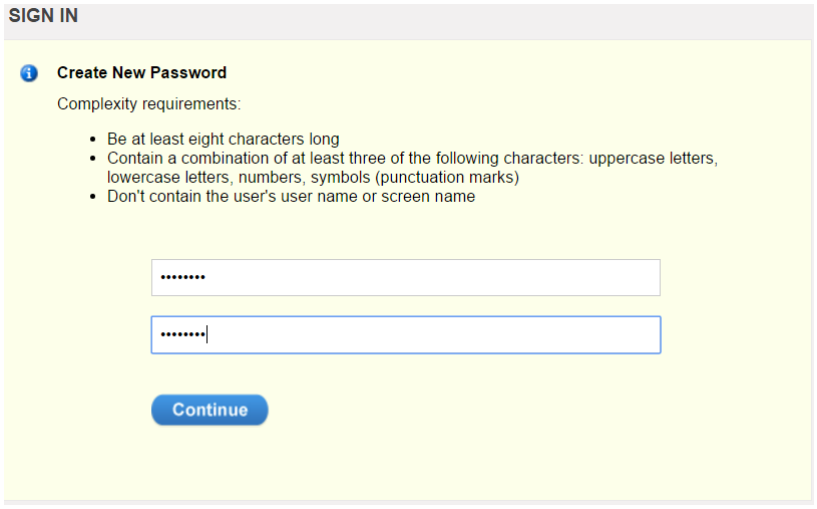
A user account will be created and you will be notified of the username from your SINTEF contact. The username will have the structure <username>@ext.sintef.no. When logging in to services, you will have to use the full form, including the @ext.sintef.no. So if you are granted the username 'oberg', use oberg@ext.sintef.no when loging in to the services.

Setting a password

If you already have a password for access to SINTEF services, you can skip this step. Otherwise, go to the site https://collaboration.sintef.no to reset your password by clicking the "I forgot my password" link at the bottom of the page.



Open your email to get a reset-link and follow the instructions at that link



After a successful reset, continue to the next point. **There is no use in logging in to the service on collaboration.sintef.no, as you will only use this site for password reset.**

Making a certificate request

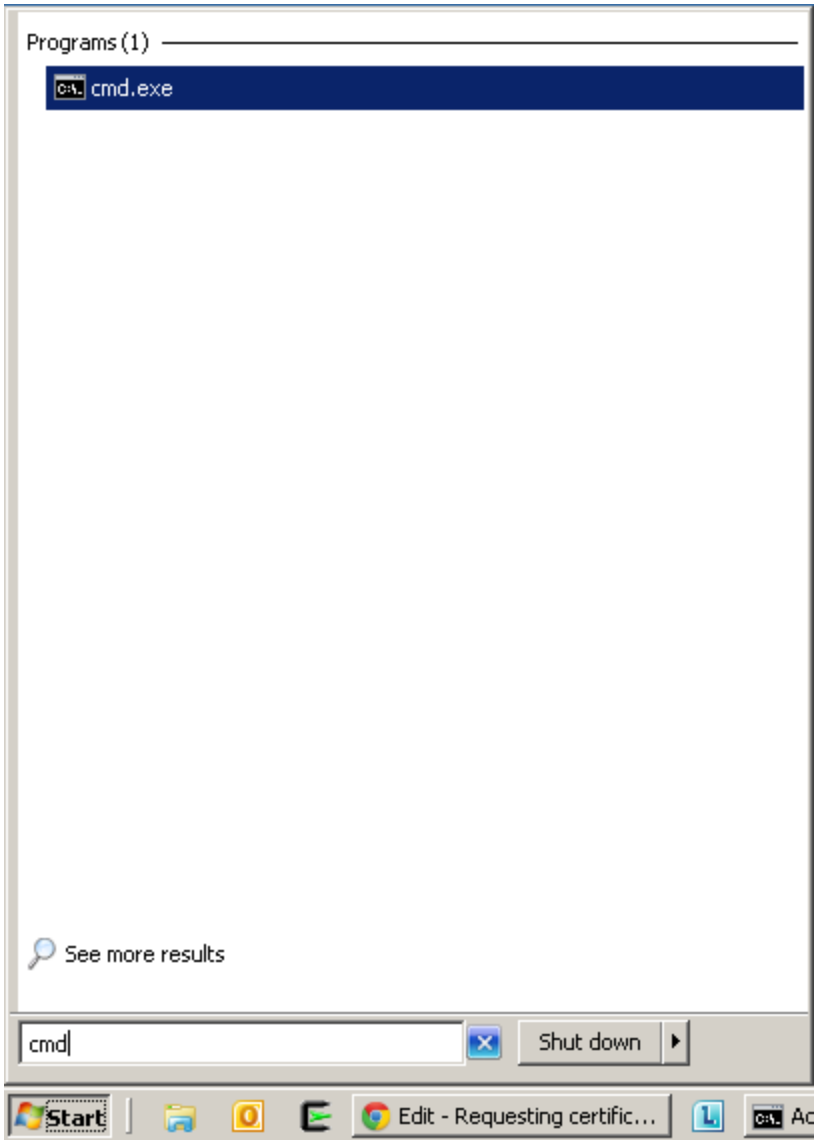
Windows

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

request.txt

```
;----------------- 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:

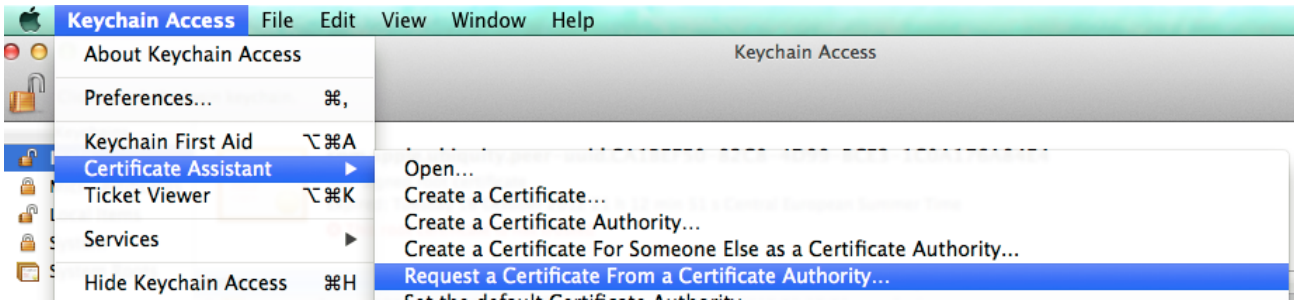
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.


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

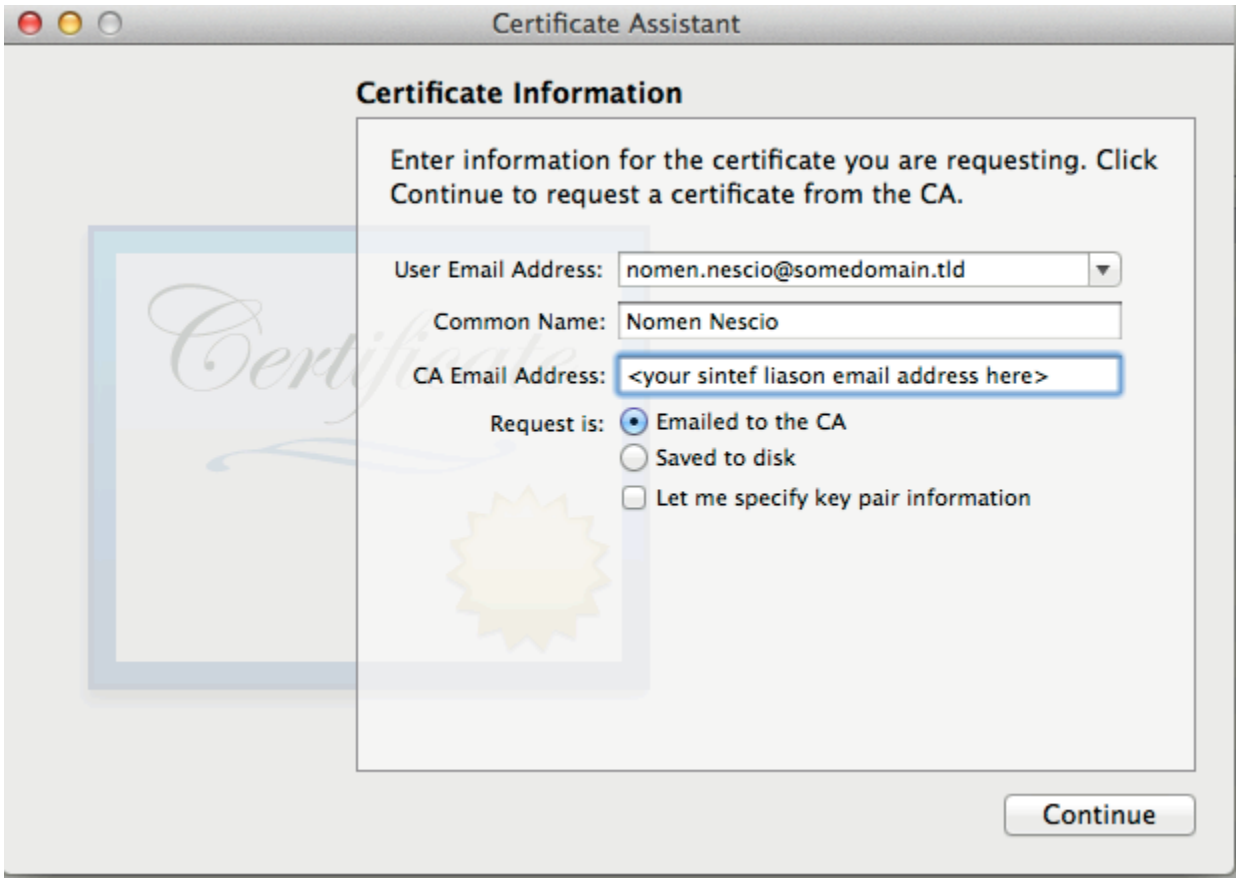
4. Type the following command to generate the certificate request file "certreq.txt"

```
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.

```
$ 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

conf.txt

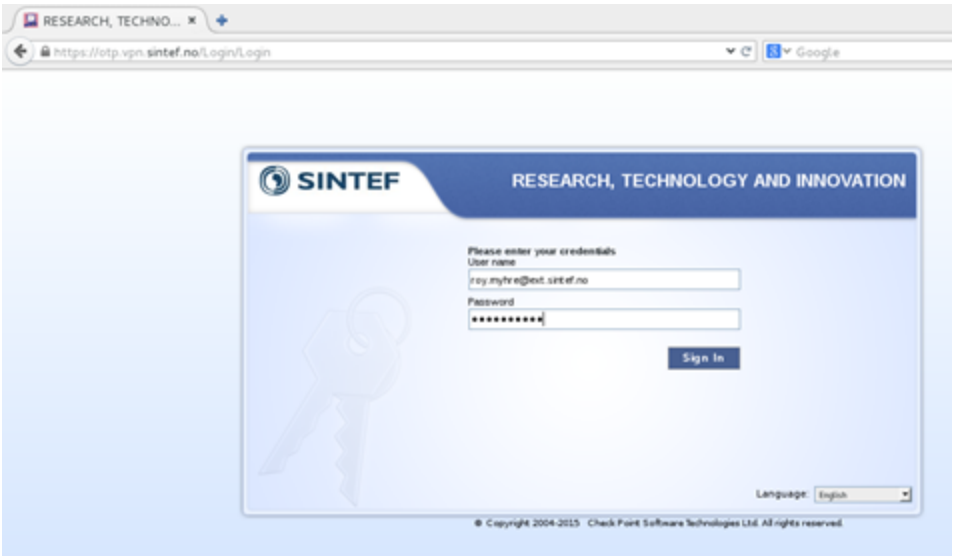
```
# Example file conf.txt for openssl req command

# 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

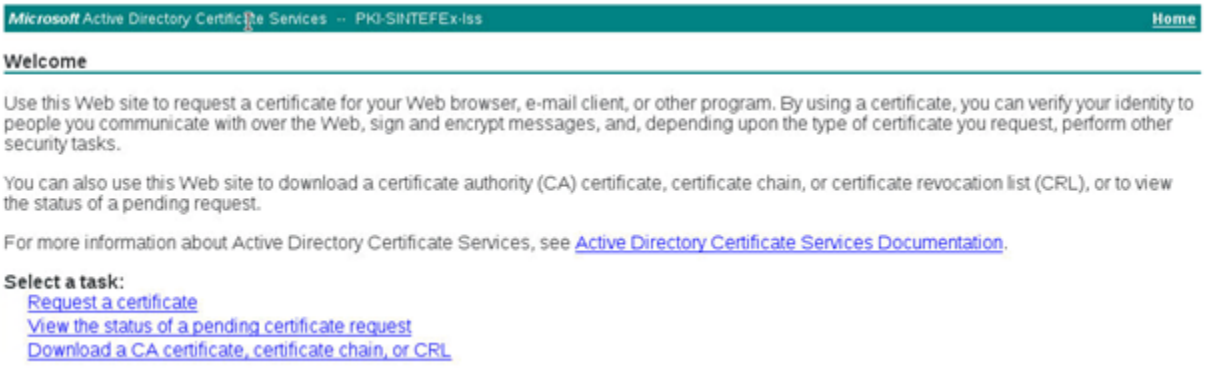
1. Go to the site https://otp.vpn.sintef.no
2. Log in with the username you have been given by SINTEF and add the extension @ext.sintef.no - e.g. username@ext.sintef.no.



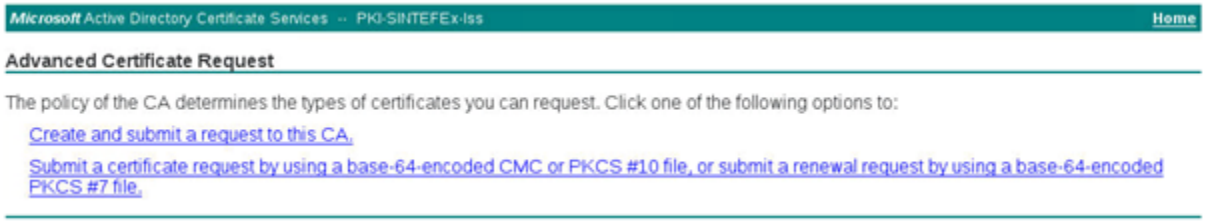
3. The system will send you an SMS to the mobile number you have been registered with at SINTEF when you press Sign In. Enter the code you received by SMS.

4. The User access portal opens.

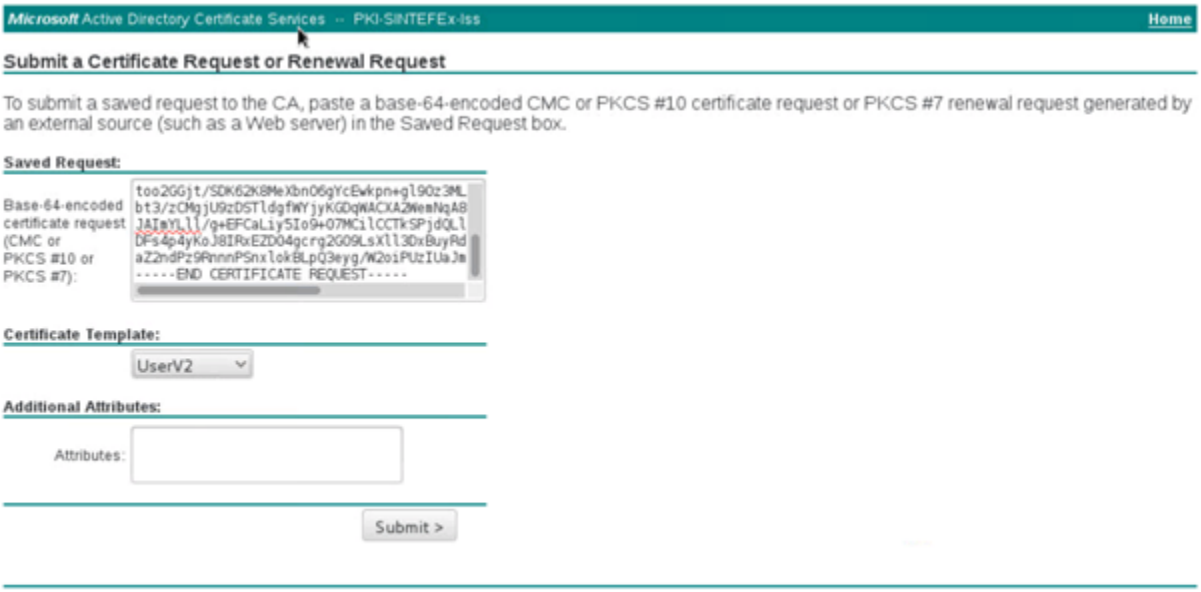
5. Click on the published "**Microsoft Active Directory Services – PKI-SINTEFEX-Iss**" URL as outlined above.
6. The certificate enrollment portal opens



7. Click "Request a certificate"



8. Click “**Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file…**”
9. Paste the text from the file certreq.txt in the Saved Request-field, and make sure Certificate Template reads **UserV2**.



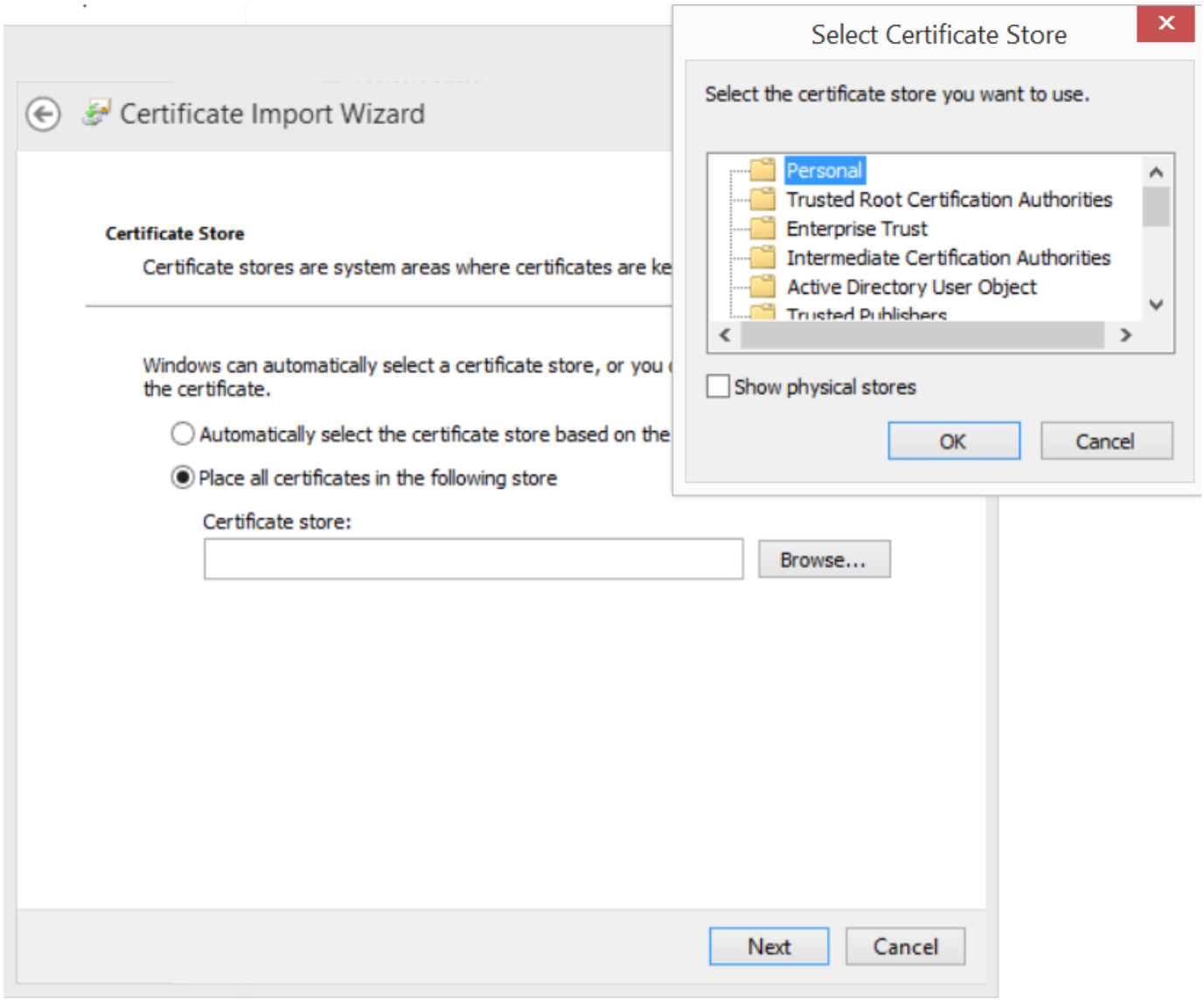
10. Then click **Submit**.
11. New certificate has now been enrolled.

12. Press "Download certificate chain", which will give you a file "certnew.p7b" for download.
13. Save your request to file by supplying a filename and press <Finish>.

Installing the certificate

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

First time log-on

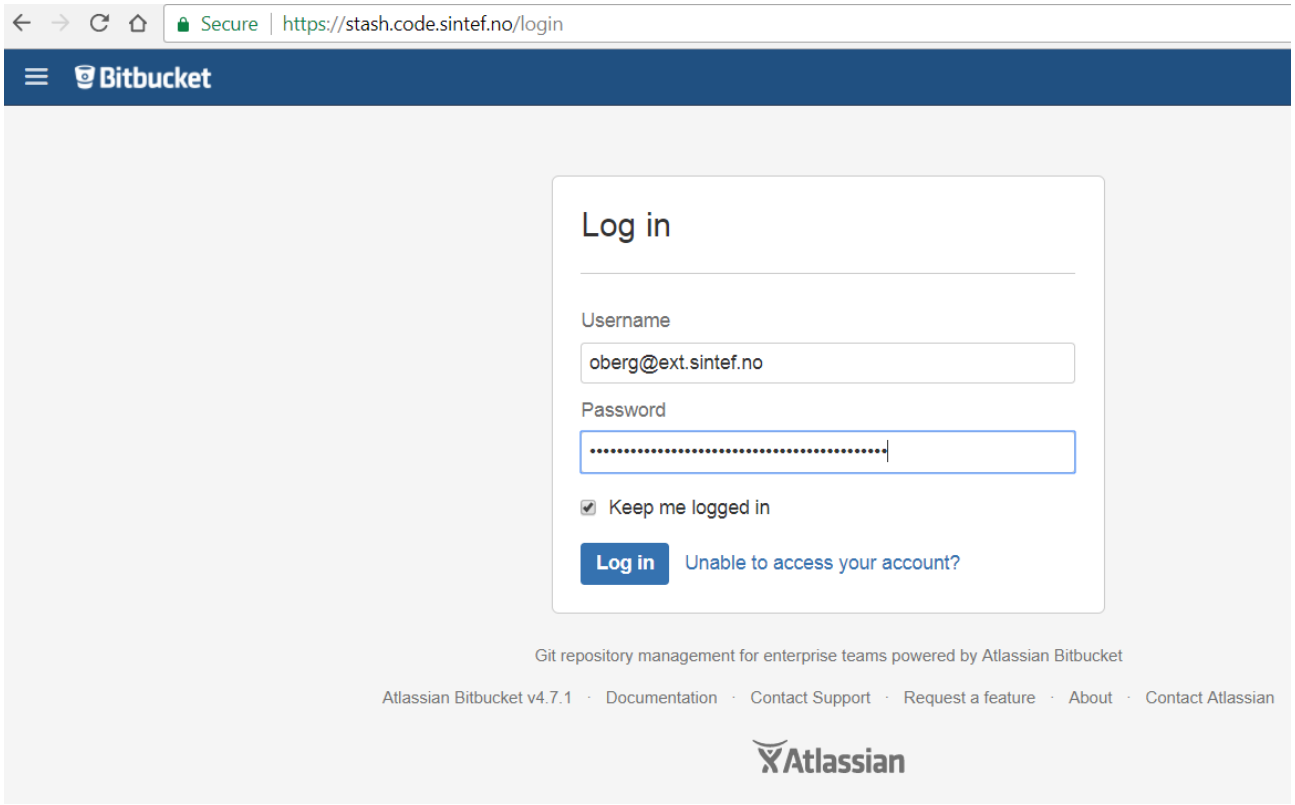
You have now set a password, requested a cerificate and installed the certificate. The next step is to log in to the services at code.sintef.no

Point your web-browser to http://www.code.sintef.no and select the service you want to log in to.

The code.sintef.no services

- Knowledge sharing: Confluence
- Project management: Jira
- Code management: Stash
- Continous integration and build server: Bamboo

At the log-on prompt of the service, enter your username, e.g. oberg@ext.sintef.no



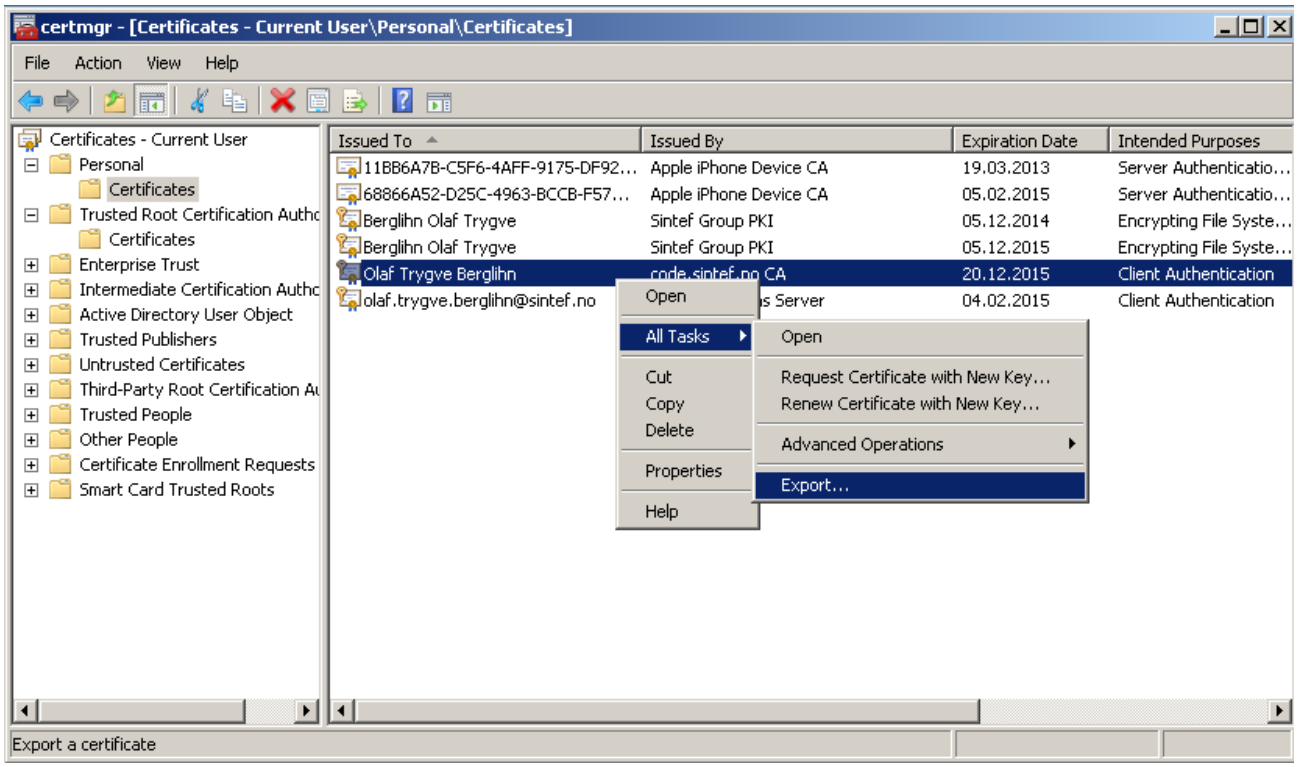
If you encounter a log-on failure the first time, please be patient. The system sometimes requires 5 minutes from the first log on attempt to update all sub-systems with your user account info. Just try again after a short wait. Once you have successfully logged in the first time, your SINTEF contact can grant you credentials to access the relevant projects and pages. So now is a good time to inform your SINTEF contatct that you are ready to use the services.

Making a backup of the certificate and private key in Windows systems.

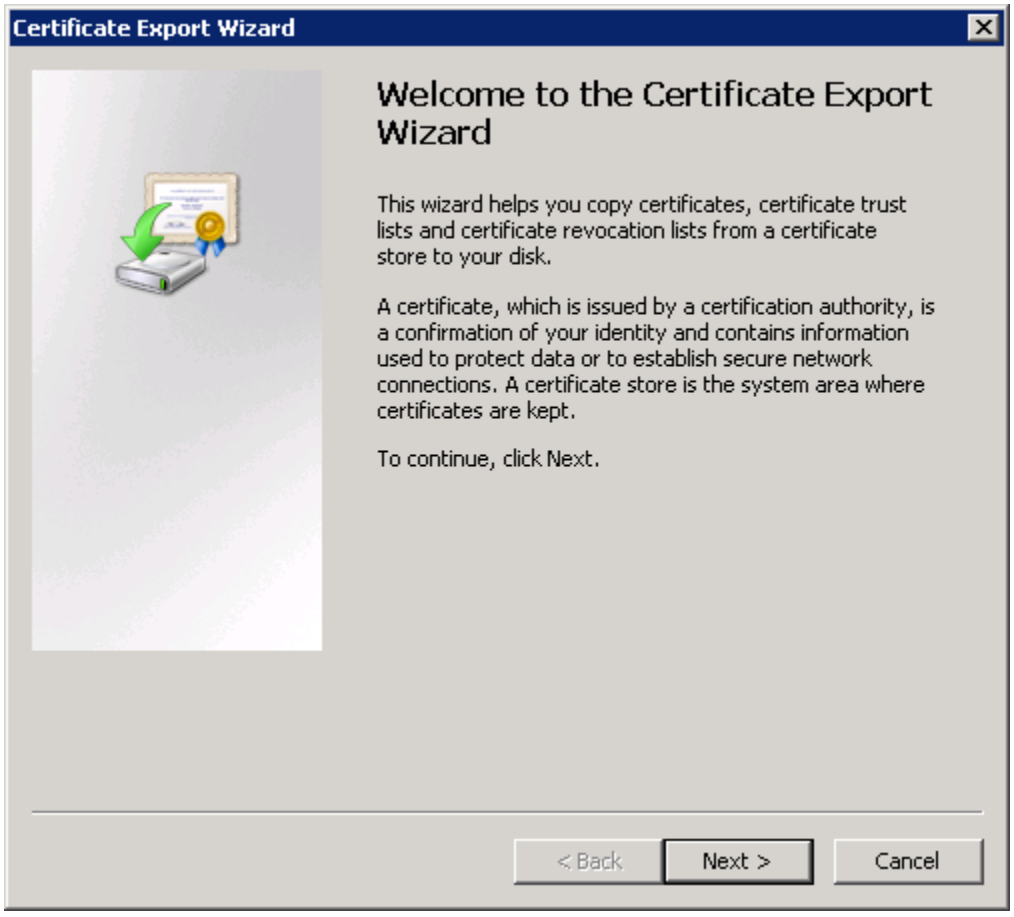
In case you should need to re-install your computer, it can be a good idea to save the certificate and private key to a file. Beware that you must keep this file in a safe place, as unauthorized personnel can exploit your credentials for illicit purposes.

1. Start the certmgr.msc by pressing windows-key + r and input "certmgr.msc"

2. In the certmgr.msc, navigate to your certificate, right click, select "All tasks" and "Export"

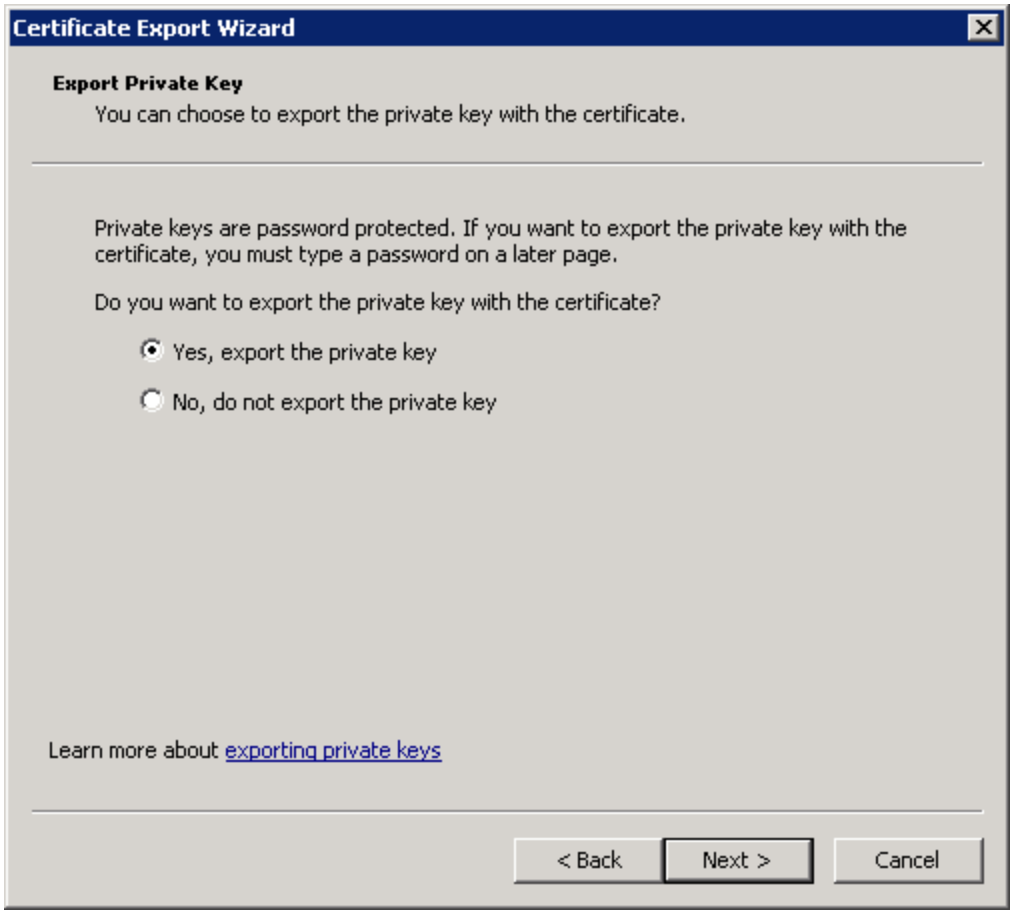


3.

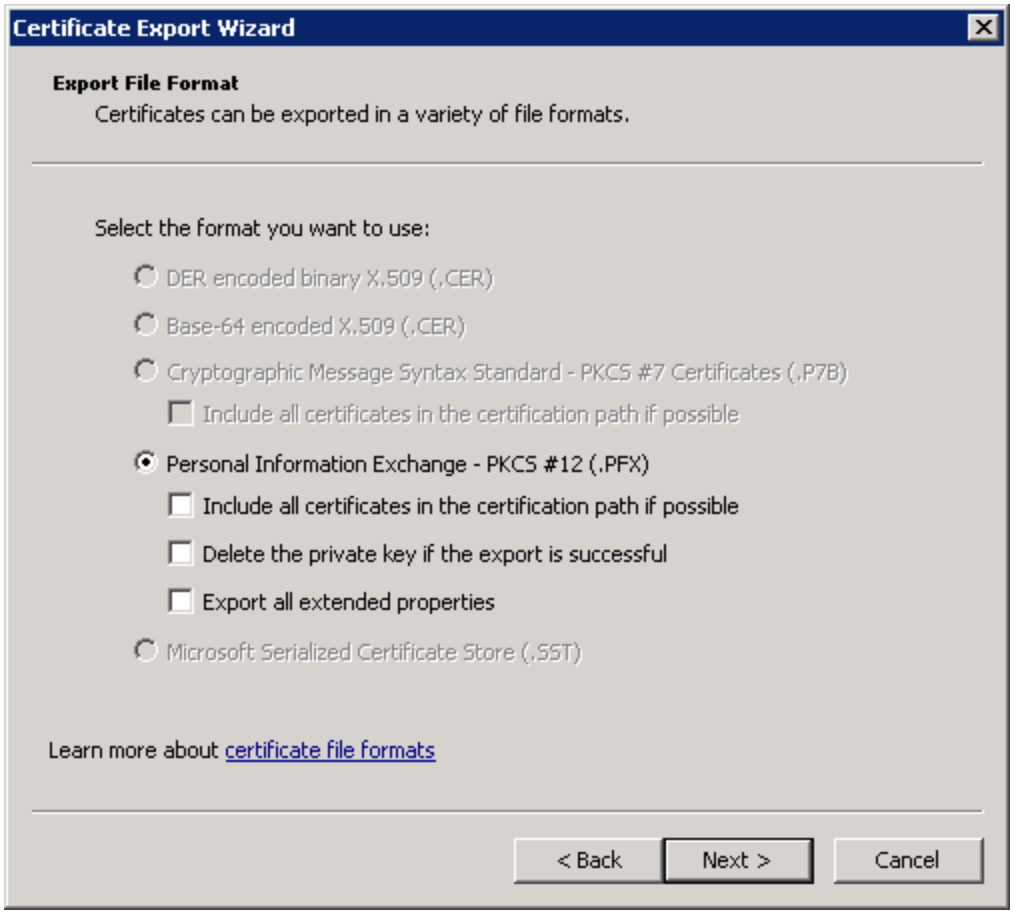


Press <Next>

4.

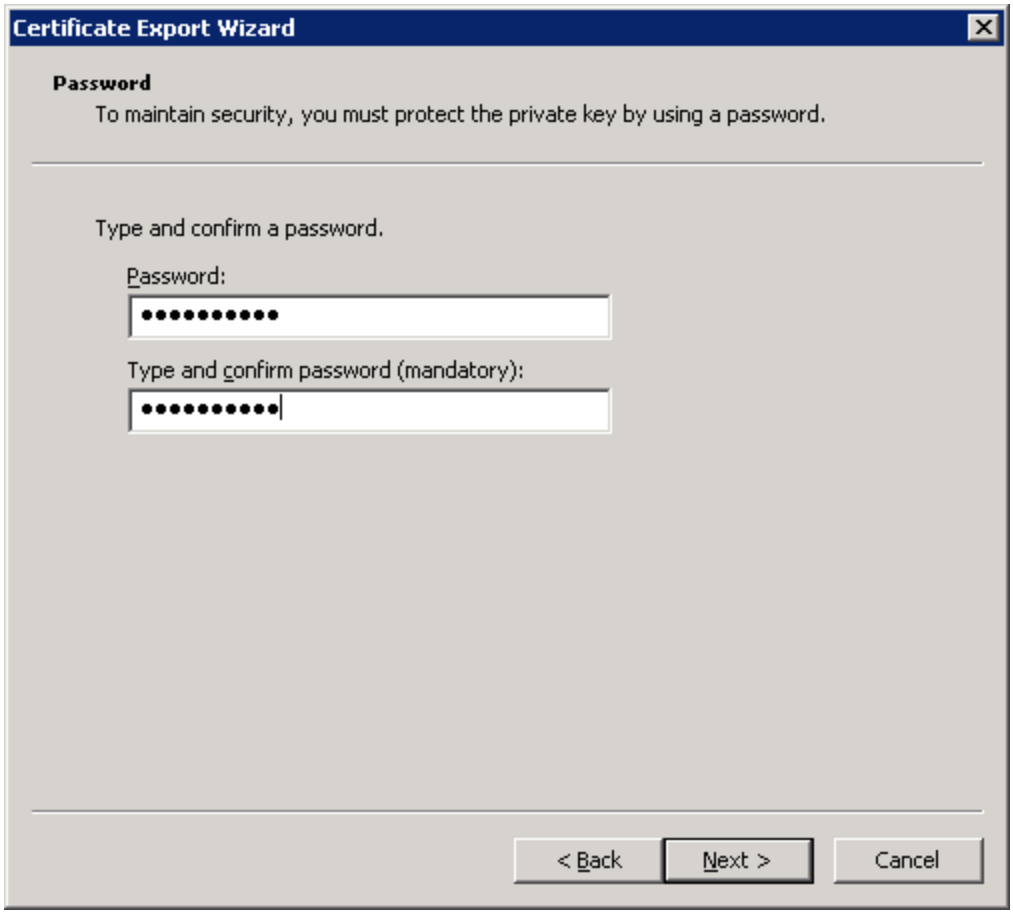


5. Select "Yes, export the private key".

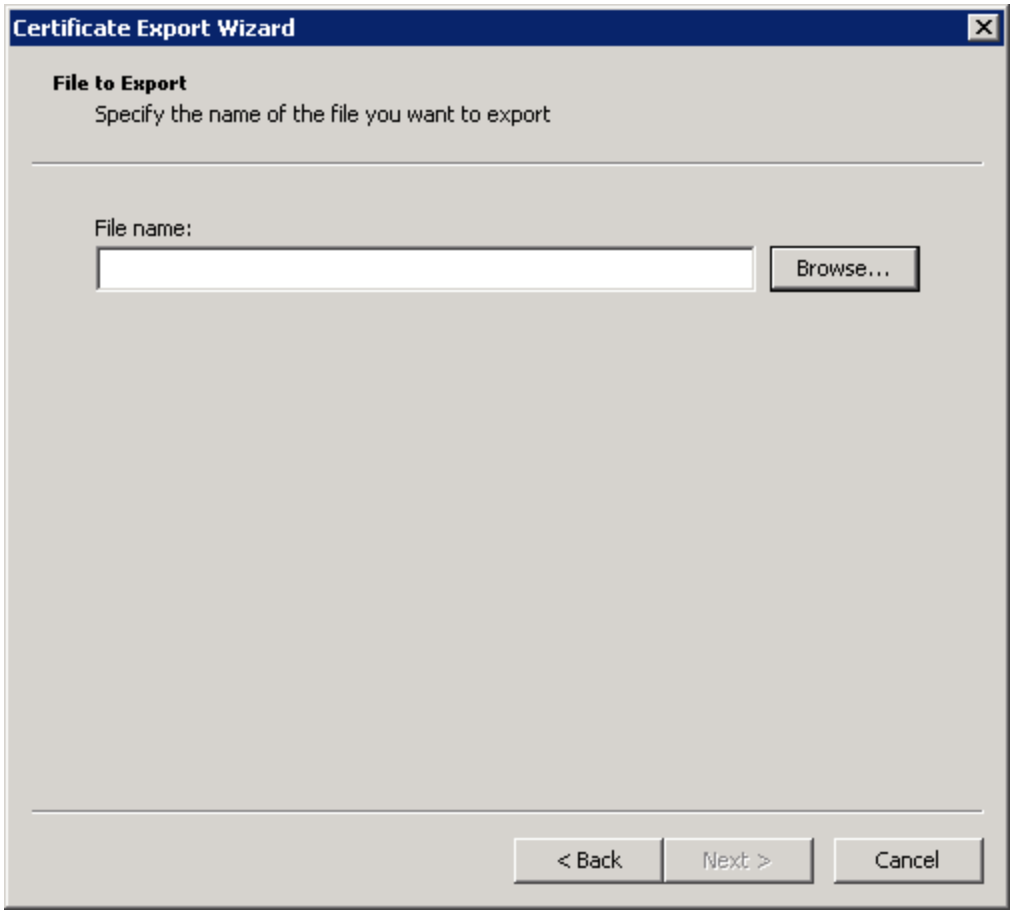

Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Delete the private key if the export is successful
Export all extended properties
Microsoft Serialized Certificate Store (.SST)
Learn more about certificate file formats
< Back
Next >
Cancel

Press <Next>.

6.

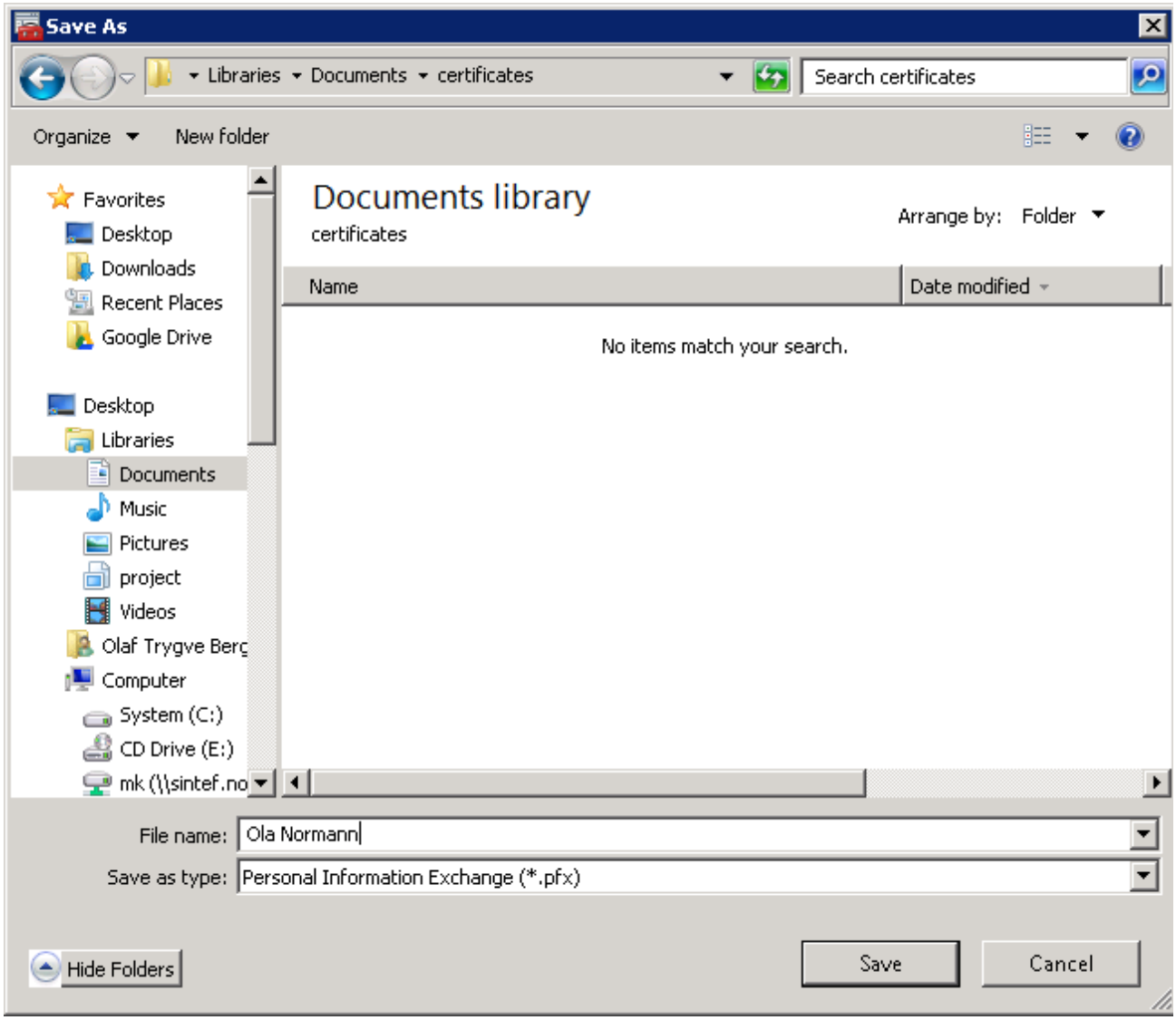


7. Choose a password to protect the certificate and private key, then press <Next>.

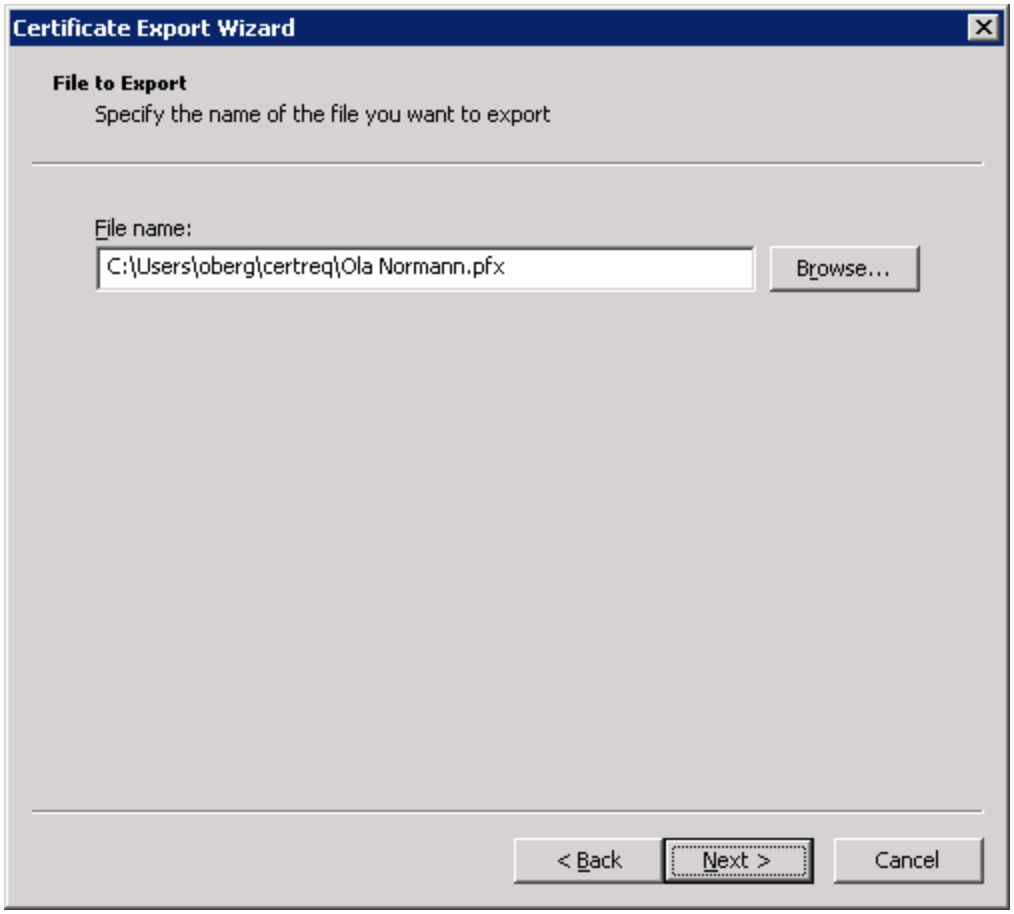


Choose where to save the file by pressing <Browse>

8.

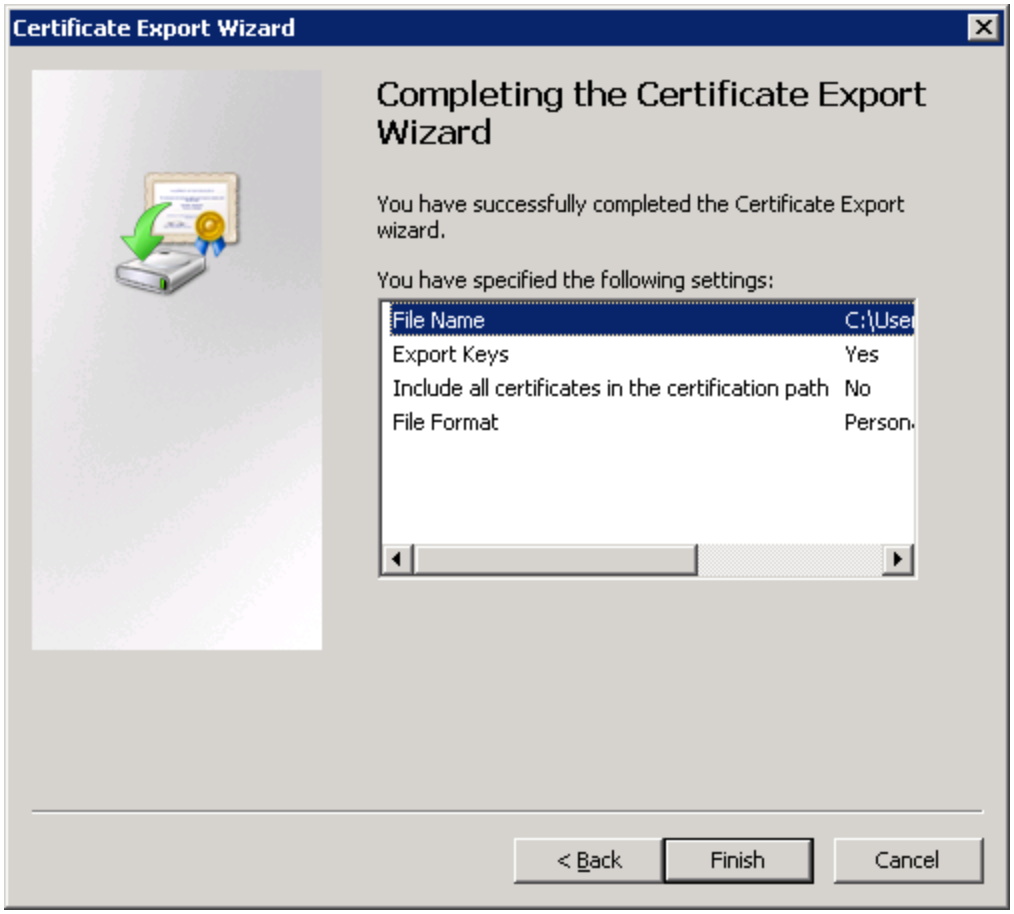

Save As
Libraries
Documents
certificates
Search certificates
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Google Drive
Desktop
Libraries
Documents
Music
Pictures
project
Videos
Olaf Trygve Berg
Computer
System (C:)
CD Drive (E:)
mk (\\sintef.no
Documents library
certificates
Arrange by: Folder
Name
Date modified
No items match your search.
File name: Ola Normann
Save as type: Personal Information Exchange (*.pfx)
Hide Folders
Save
Cancel

9. Press <Save>.



Press <Next>.

10.



Press <Finish>.

11. You are done and can copy the file to a safe place for later retrieval. This file contains **both your private key and your certificate**.

Make sure you never share this file with anyone.

Take care of your private key
The private key is known only to you (or rather your computer). This means that you should take care of your private key and it is a good idea to make a backup copy of your certificate.