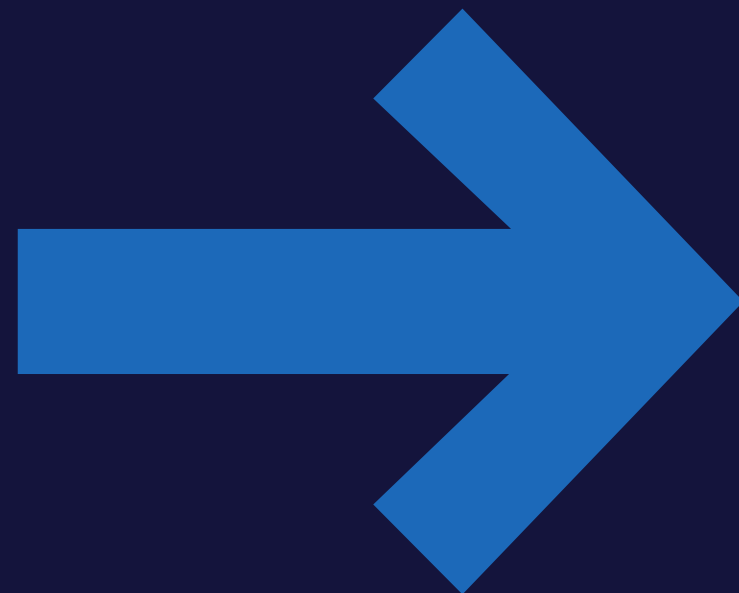


Certificates: Installation and Registration - Miniguide



Is this guide for you?

- This guide is primarily intended for the end-user accessing DMS through a System-to-System solution.
 - If you have a software vendor providing a system for you, they may help or perform some of the steps in this guide for you – we recommend you coordinate with your software vendor on the specifics.
- The focus will be on how to install and register OCES certificates, not how the System-to-System itself should be set up.
- Any developer, whether in-house or software vendor, would benefit from reading the [Connectivity Guide](#) in its entirety.

Table of contents

- Certificate Installation.
- Client Registration.



Certificate Installation



A step-by-step walkthrough to installing an OCES3 certificate, and how to verify the installation was successful

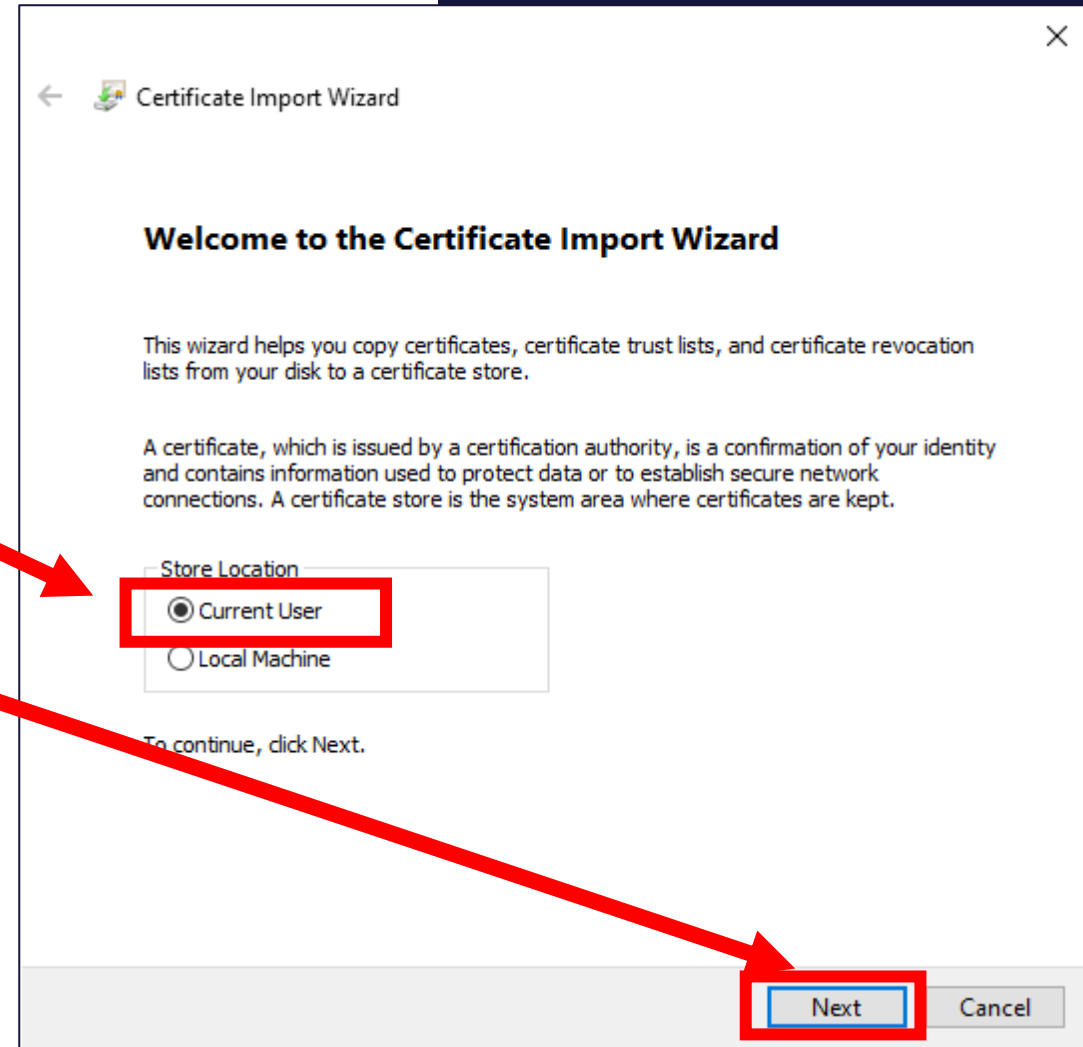
Certificate Installation step 1

- Obtain the certificate and download it (See chapter 2 of the [Connectivity Guide](#) for more info.)
 - The certificate must be a valid OCES3 certificate and is issued by mitid-erhverv.dk
 - The file should have either a .pfx or a .p12 appended to their names meaning they are of that format.
 - If the file format is not of these types, contact [support](#).
 - The file should be in your 'downloads' folder.
 - We advise you move the file to a location in another folder where it can easily be located when needed.
- Open the file by double clicking with the left mouse button.
 - This will open a program called 'Certificate Import Wizard'.



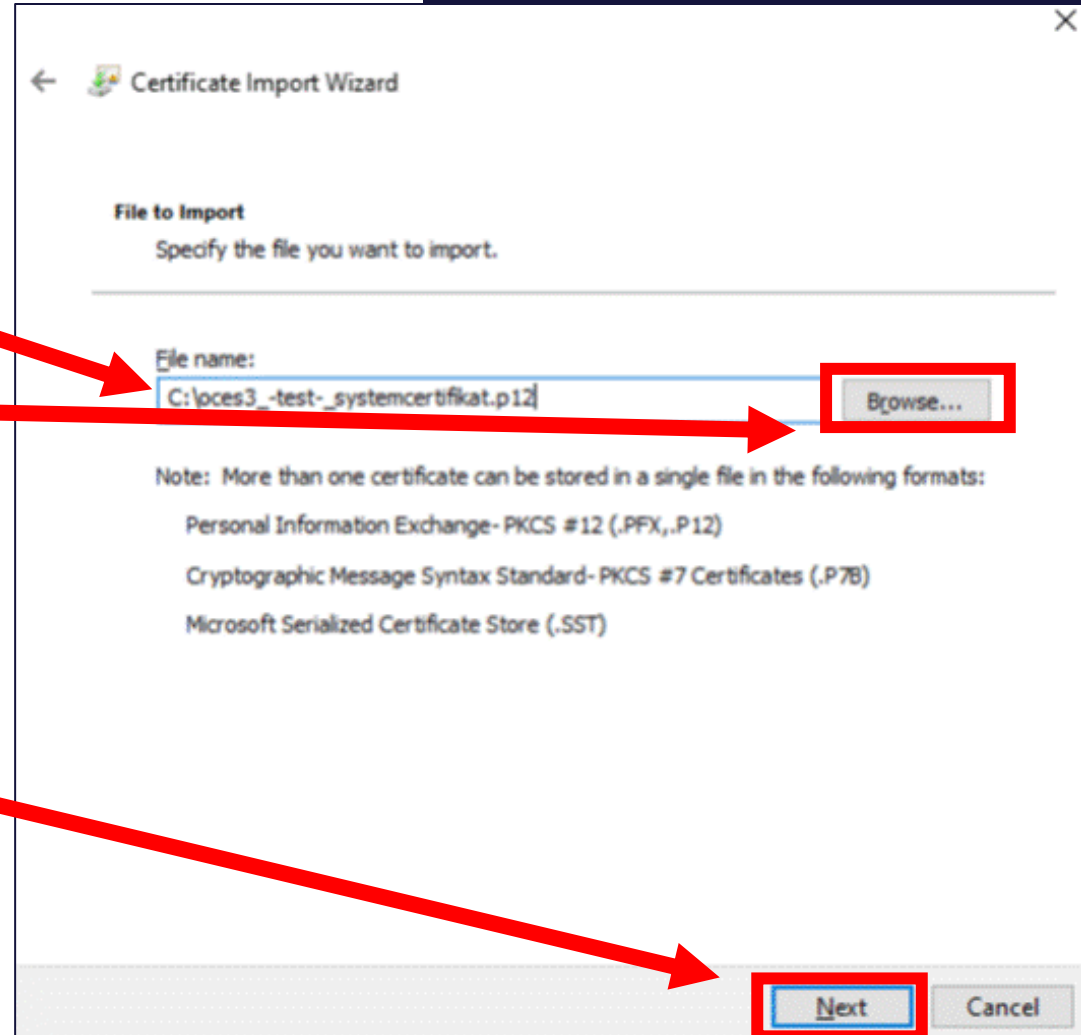
Certificate Installation step 2

- In the Certificate Import Wizard.
- Make sure 'Current User' is selected.
- Click 'Next' to proceed.



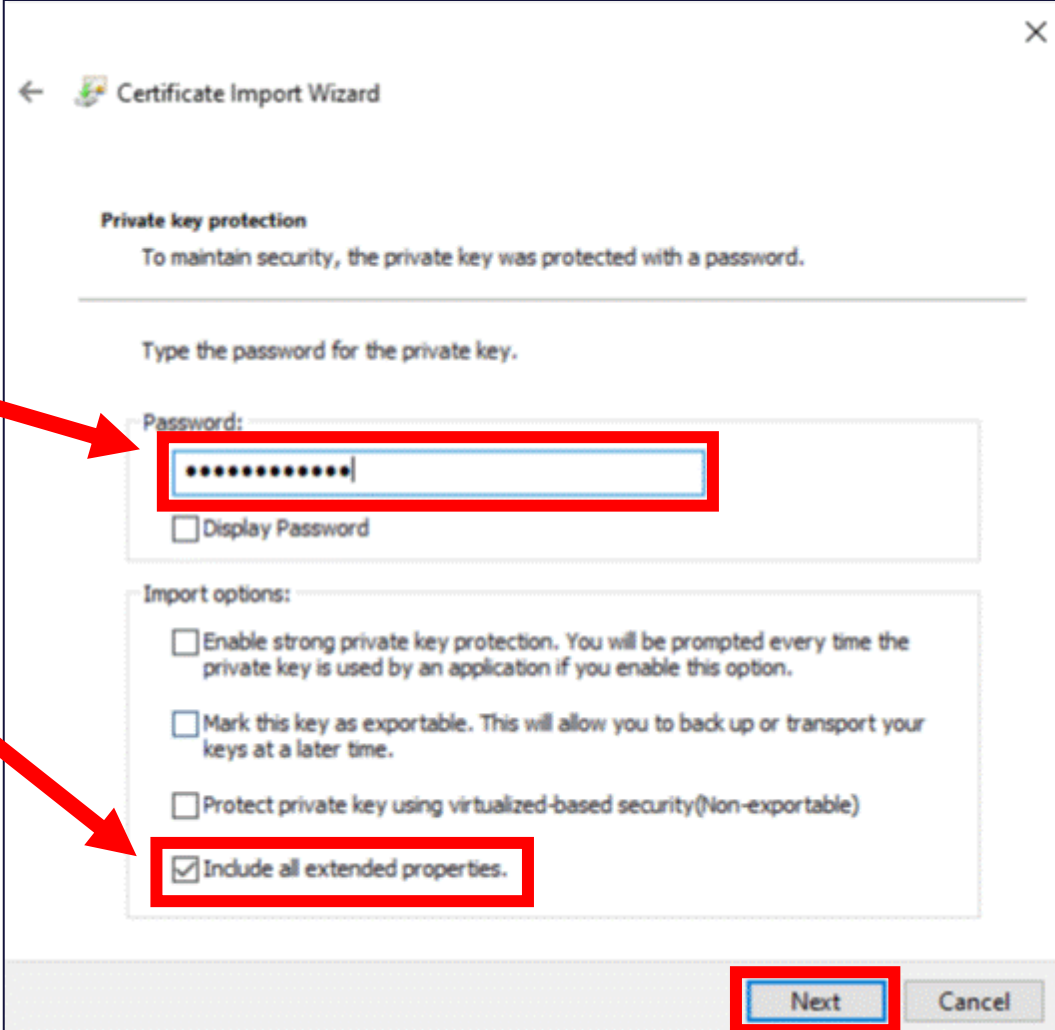
Certificate Installation step 3

- Check that the certificate file name is selected
- If the name is incorrect, click 'Browse'.
 - Locate the certificate and double click it.
- Click 'Next'.



Certificate Installation step 4

- Fill out the certificate password.
- You received this password when you were issued the certificate
- Check the box 'Include all extended properties'.
- Click 'Next'.



The image shows a Windows 'Certificate Import Wizard' dialog box. It has a title bar with a back arrow, a forward arrow, and the text 'Certificate Import Wizard'. The main content area is titled 'Private key protection' and contains the text 'To maintain security, the private key was protected with a password.' Below this, it says 'Type the password for the private key.' There is a 'Password:' label followed by a text box containing ten dots. A red rectangle highlights this text box, and a red arrow points from the first bullet point of the list to it. Below the text box is a checkbox labeled 'Display Password'. Underneath is a section titled 'Import options:' with three checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.', 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.', and 'Protect private key using virtualized-based security(Non-exportable)'. The fourth checkbox, 'Include all extended properties.', is checked and highlighted with a red rectangle. A red arrow points from the third bullet point of the list to this checkbox. At the bottom right, there are 'Next' and 'Cancel' buttons. The 'Next' button is highlighted with a red rectangle.

← Certificate Import Wizard

Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:
[Password field with dots]

☐ Display Password

Import options:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

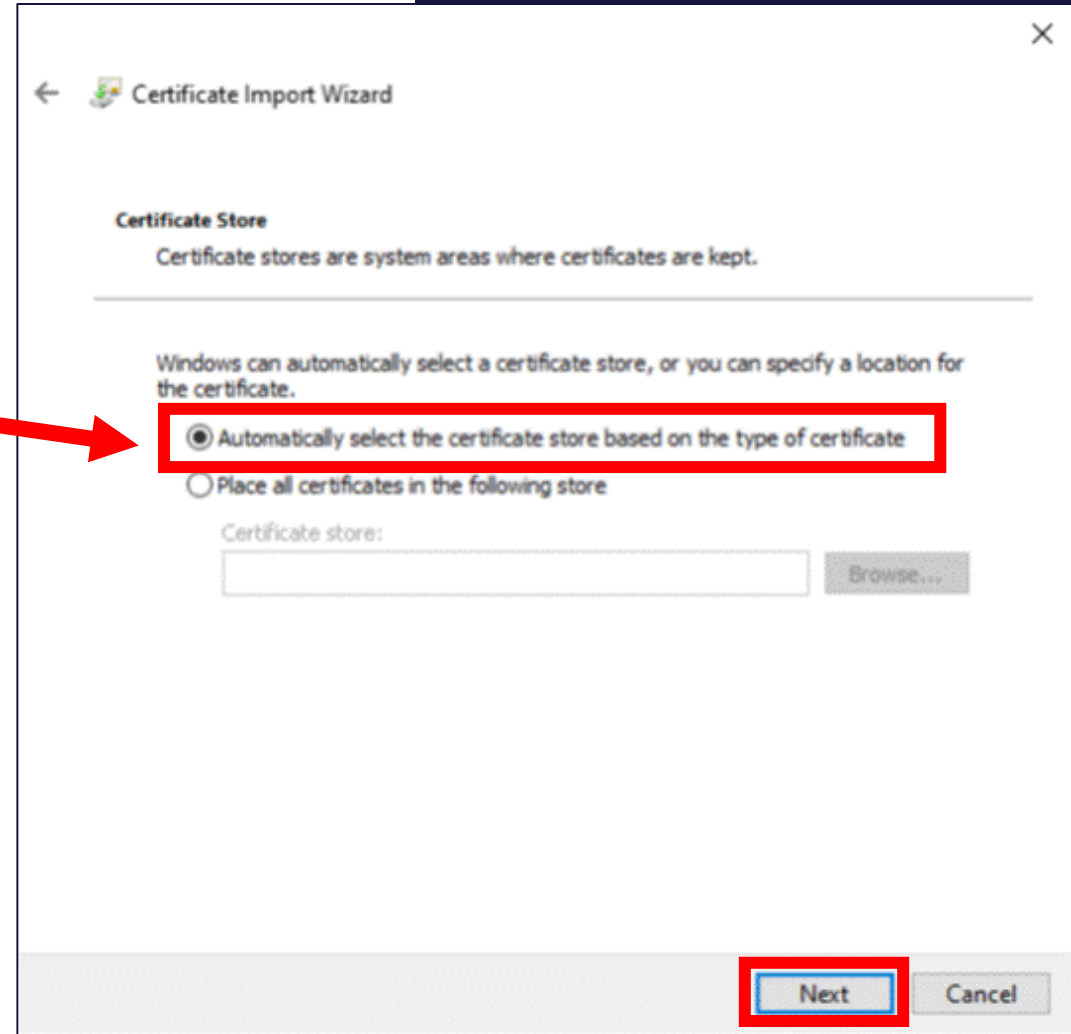
☐ Protect private key using virtualized-based security(Non-exportable)

☒ Include all extended properties.

Next Cancel

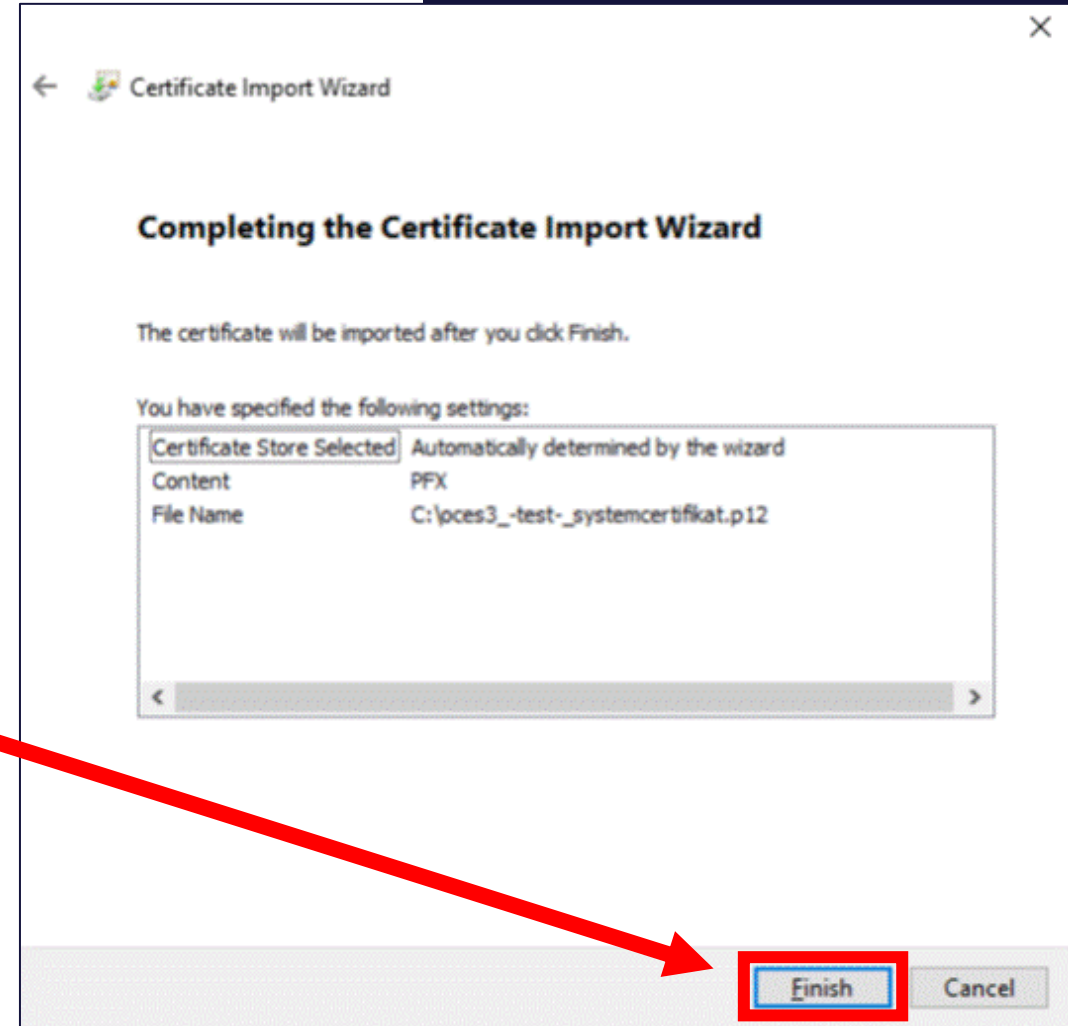
Certificate Installation step 5

- Choose the option:
 - ‘Automatically select the certificate store based on the type of certificate’.
- Click ‘Next’.



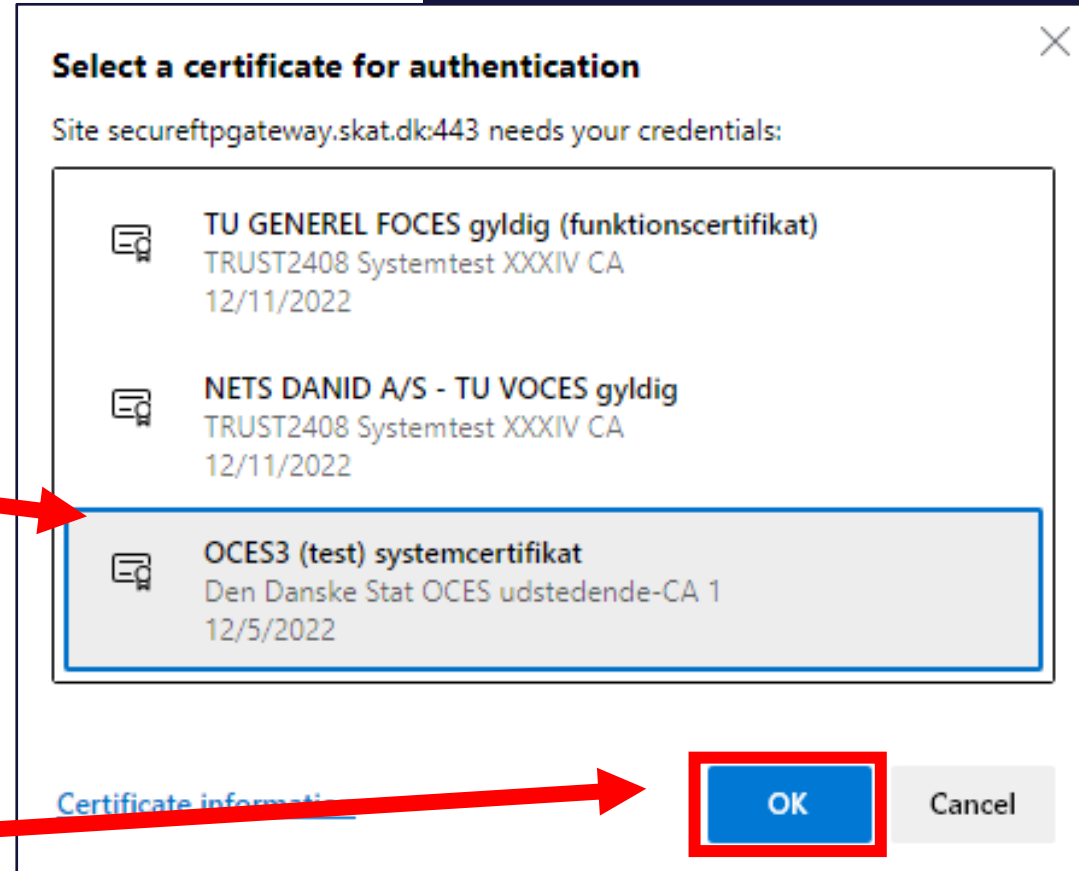
Certificate Installation step 6

- You have reached the final part of the installation.
- Click 'Finish'.
- A warning will show up.
 - This is to be expected. Simply click 'Ok' to proceed.



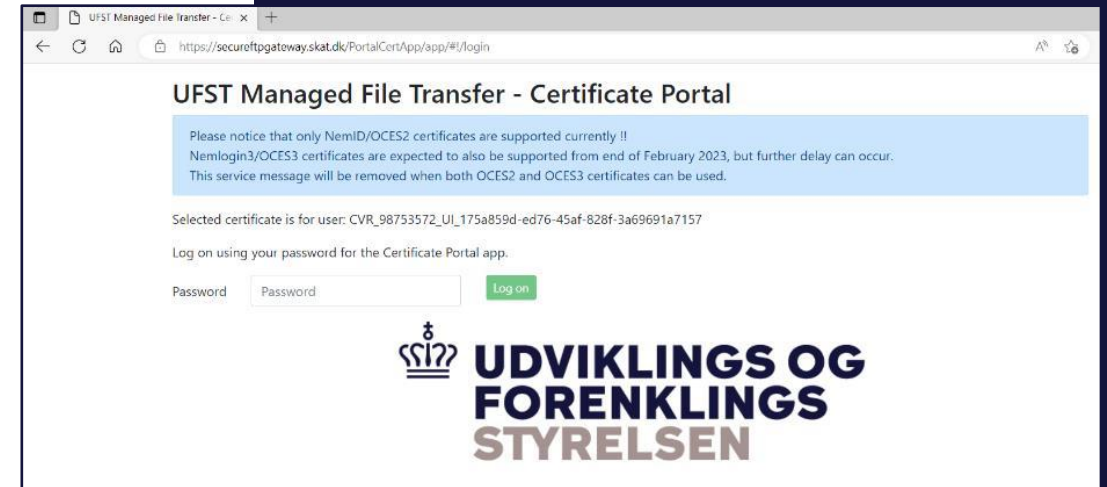
Certificate Installation step 7

- To verify that the installation was a success, go to an internet browser.
- Type in the URL secureftpgateway.skat.dk.
- Select your certificate.
- The certificate will be of type **OCES3**.
- Refer to section 8.1.1 and 8.1.2 of the [Connectivity Guide](#) for identification and display of the certificate
- Click 'OK'.



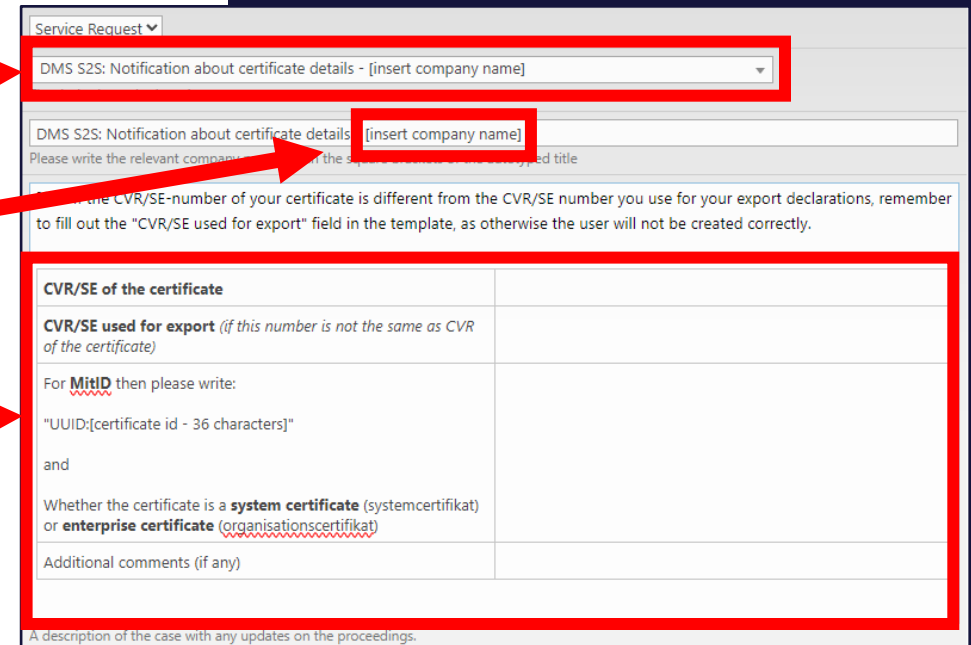
Certificate Installation step 8

- If the certificate is installed correctly, you should be presented with the web page shown on the right.
 - Notice that above the log in field, the user ID is displayed, which will become important later
- If the certificate is not installed correctly, the web page will display an error.
- Should this be the case, submit a case to the DMS onboarding team via [Toolkit](#) (the Toolkit User Guide can be found [here](#)).



Certificate Installation step 9

- Once a certificate has been successfully installed, submit a case to the DMS onboarding team via [Toolkit](#) for registration.
- In the 'Service' category, chose the 'DMS S2S: Notification about certificate details - [...]' option.
- Fill in the '[insert company name]' with your company name in the 'Title' field.
- Fill out the form in the 'Description'.
- The purpose of this case is to grant the system-to-system rights to the certificate for the test environment (TFE).
- Click 'Save' at the bottom of the page.



The screenshot shows a 'Service Request' form. A red box highlights the 'Service Request' dropdown menu, which is set to 'DMS S2S: Notification about certificate details - [insert company name]'. Another red box highlights the 'Title' field, which contains '[insert company name]'. A third red box highlights the 'Description' field, which contains the following text: 'CVR/SE of the certificate', 'CVR/SE used for export (if this number is not the same as CVR of the certificate)', 'For MitID then please write:', '"UUID:[certificate id - 36 characters]"', 'and', 'Whether the certificate is a **system certificate** (systemcertifikat) or **enterprise certificate** (organisationscertifikat)', and 'Additional comments (if any)'. Red arrows point from the list items to these specific fields.

CVR/SE of the certificate	
CVR/SE used for export (if this number is not the same as CVR of the certificate)	
For MitID then please write:	
"UUID:[certificate id - 36 characters]"	
and	
Whether the certificate is a system certificate (systemcertifikat) or enterprise certificate (organisationscertifikat)	
Additional comments (if any)	

A description of the case with any updates on the proceedings.

Certificate Registration



How to register a certificate for the TFE and
PROD environment

Attention!

- Before registering the certificate on the AS4 gateway it is **very** important to register roles and rights.
- Failing to do so may potentially result in a delay in your planned onboarding and can result in having to do the entire process over again.
- Do not register on AS4, unless you are completely sure that you have registered roles and rights.
- You will receive a confirmation email from the onboarding team when roles and rights have been successfully assigned.
- The guide on how to register roles and rights for TFE can be found in section 3 of the [DMS Connectivity Guide](#).

Certificate Registration step 1

- It is prerequisite that a certificate has been successfully installed on the computer in question already before any further actions take place.
- Determine which environment you would like to register for :
 - **Test Environment (TFE).**
 - Use the link: secureftpgatewaytest.skat.dk.
 - **Production Environment (PROD).**
 - Use the link: secureftpgateway.skat.dk.

Certificate Registration step 2

- Type in your self-service portal password.
- First time you log in your default certificate password is your user ID which will be displayed on the page.
- Click 'Log on'.

UFST Managed File Transfer - Certificate Portal

Please notice that only NemID/OCES2 certificates are supported currently !!
Nemlogin3/OCES3 certificates are expected to also be supported from end of February 2023, but further delay can occur.
This service message will be removed when both OCES2 and OCES3 certificates can be used.

User ID: CVR_98753572_UI_175a859d-ed76-45af-828f-3a69691a7157

Log on using your password for the Certificate Portal app.

Password:

**UDVIKLINGS OG
FORENKLINGS
STYRELSEN**

Certificate Registration step 3

TFE: Before the 10th of April, the following will appear when you register.

PROD: Before the 17th of April, the following will appear when you register.

After these dates, this will appear when you log in.

- The first time you log in you are required to change your certificate password.

- Enter your current certificate password (User ID).
- Enter the new certificate password.
- This will only change your password for logging on to the website not the password for connecting to the AS4 gateway.
- In the 'Confirm password' row, repeat your new password.
- Click 'Change password' to proceed.

The screenshot shows a 'Change password' dialog box. At the top, there is a red error message: 'You must change the default password!'. Below this, there are three input fields: 'Current password', 'New password', and 'Confirm password'. Each field is highlighted with a red rectangle. Red arrows point from the list items to these fields: from 'Enter your current certificate password (User ID)' to the 'Current password' field, from 'Enter the new certificate password.' to the 'New password' field, and from 'In the 'Confirm password' row, repeat your new password.' to the 'Confirm password' field. At the bottom of the dialog, there are two buttons: 'Change password' (highlighted with a red rectangle and a red arrow from the list item 'Click 'Change password' to proceed.') and 'Cancel'.

Certificate Registration step 4

This is how it looks before the 13th of March on TFE and the 17th of April on PROD

- If you lodge declarations using an SE-number:
 - Enter this number in the 'SE-number' field.
 - Otherwise leave the 'SE-number' field blank.
- Check the 'AS4' box.
- When you press the button, a warning will appear
- It is important to only proceed once you have received confirmation from the Onboarding Team that roles and right have been registered.

UFST Managed File Transfer - Certificate/User overview

Your certificate is not registered in UFST MFT. Press 'Register Certificate' in order to update the certificate in UFST MFT.

Common name	OCE3 (test) systemcertifikat
Expiry date	04-12-2025
Type	CVR
E-mail	
Legal identifier	CVR_98753572
Account	UI_175a859d-ed76-45af-828f-3a69691a7157
SE-number	
Interfaces	FTP <input checked="" type="checkbox"/> AS4

Register certificate

Refresh

secureftpgateway.skat.dk says

WARNING! Please ONLY select this function if your certificate has been approved to send Import, Export or Transit documents

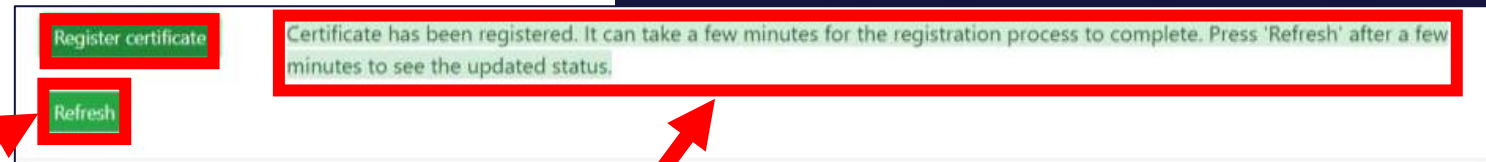
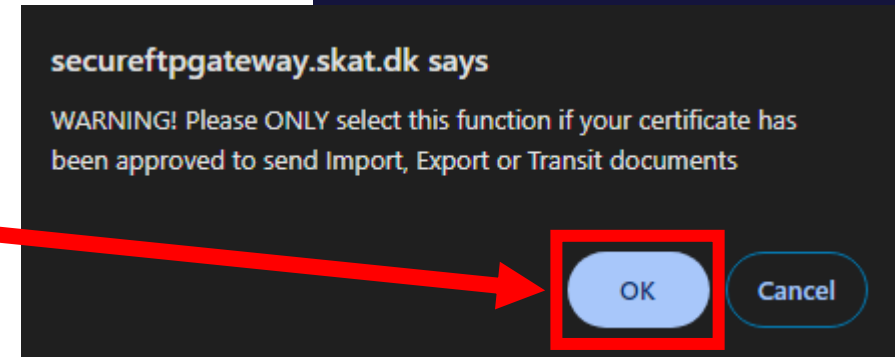
OK

Cancel

Certificate Registration step 5

This is how it looks before the 13th of March on TFE and the 17th of April on PROD

- Having checked the certificate is properly authorized proceed to click 'OK'
- Click 'Register Certificate'.
- The registration can take up to a few minutes
- Use the 'Refresh' to update the status.
- When the process has concluded a green message will appear next to the 'Register Certificate' button confirming registration



Certificate Registration step 3-4

This is how it looks after the 13th of March on TFE and the 17th of April on PROD

- If you lodge declarations using an SE-number:
 - Enter this number in the 'SE-number' field.
 - Otherwise leave the 'SE-number' field blank.
- Click 'Register Certificate'.
- The registration can take up to a few minutes
 - Use the 'Refresh' to update the status.
- When the process has concluded a green message will appear next to the 'Register Certificate' button confirming registration

UFST Managed File Transfer - Certificate/User overview

Your certificate is not registered in UFST MFT. Press 'Register Certificate' in order to update the certificate in UFST MFT.

Common name	dcs61-systemtest-1
Expiry date	12-06-2025
Type	CVR
E-mail	
Legal identifier	CVR_94683633
Account	UL_a761fa6c-9044-41b4-b7f1-75167d5dfe3a
SE-number	

Register certificate

Refresh

Register certificate

Refresh

Certificate has been registered. It can take a few minutes for the registration process to complete. Press 'Refresh' after a few minutes to see the updated status.

Certificate Registration step 5

- If the installation is successful, the web page will have a confirmation message displayed.
- Remember to note down your new password as it is used for setting up the AS4 session.
- Finish the registration by logging out.



Appendix

- More details about the installation process and verification can be found in chapter 8 of the [DMS Connectivity Guide](#).
- More details about Certificate registration can be found in chapter 4 of the [DMS Connectivity Guide](#).
- A video guide can also be found by watching the video '[Møde om adgang til DMS](#)' around the timestamp 1:10:00 .

