
CS OTE

Documentation for external users



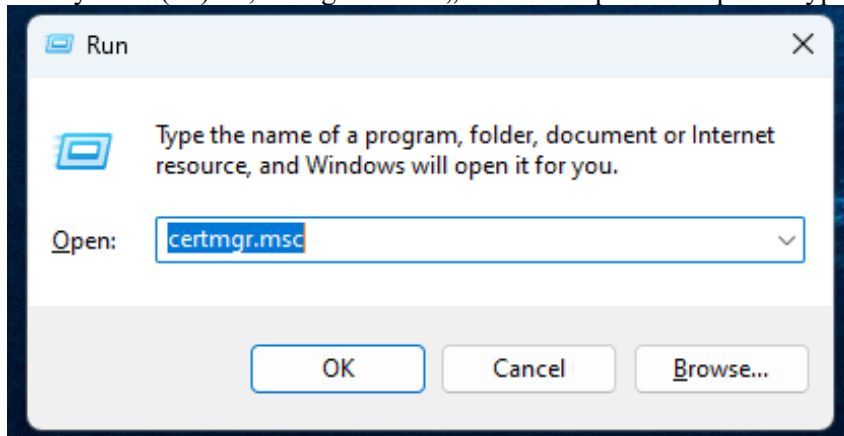
To set up local certificate storage

For the correct functionality of the local storage it is necessary to create a backup of the private part of the electronic signature, i.e. a file with the ***.p12** or ***.pfx** extension. The file can be exported from a computer where the certificate is already installed. To create a backup of the private part of the certificate, we recommend using the procedure below.

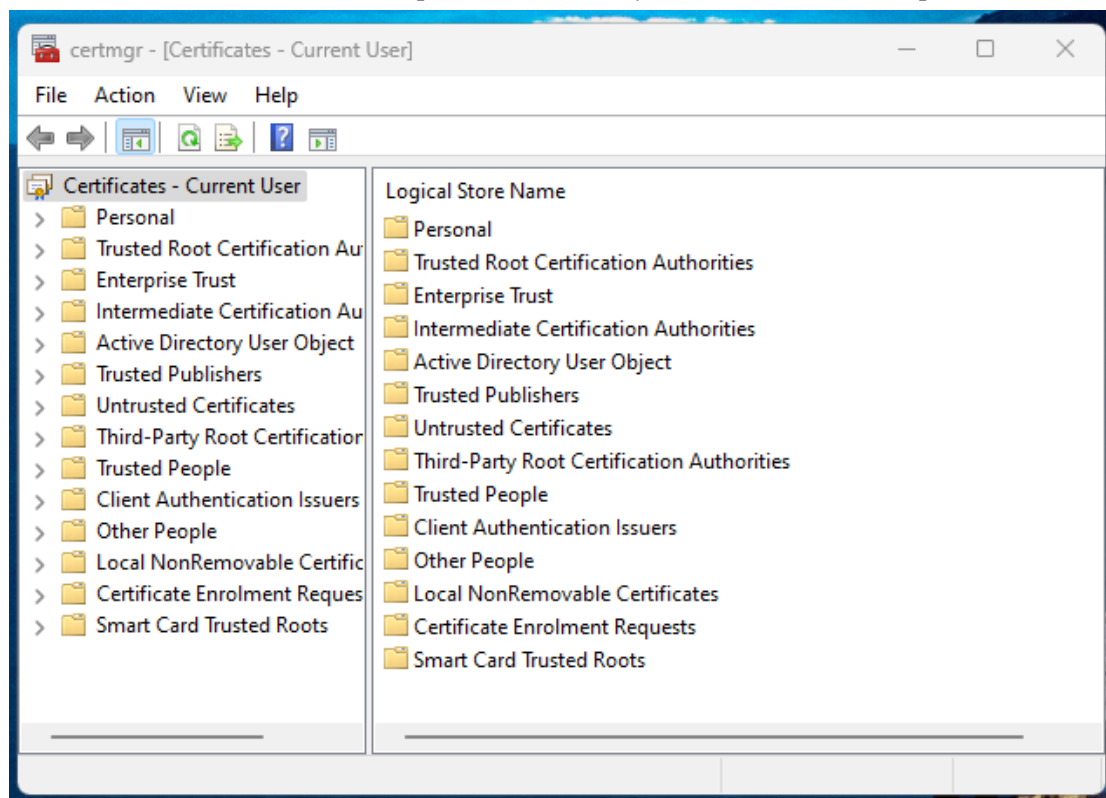
Please note that this manual is universal for all supported versions of the Windows operating system, and it is possible that some of the instructional images will differ from your device. The manual was created for the latest version of the Windows operating system, but the procedure is similar to older versions.

Exporting the private part of a certificate in OS Windows

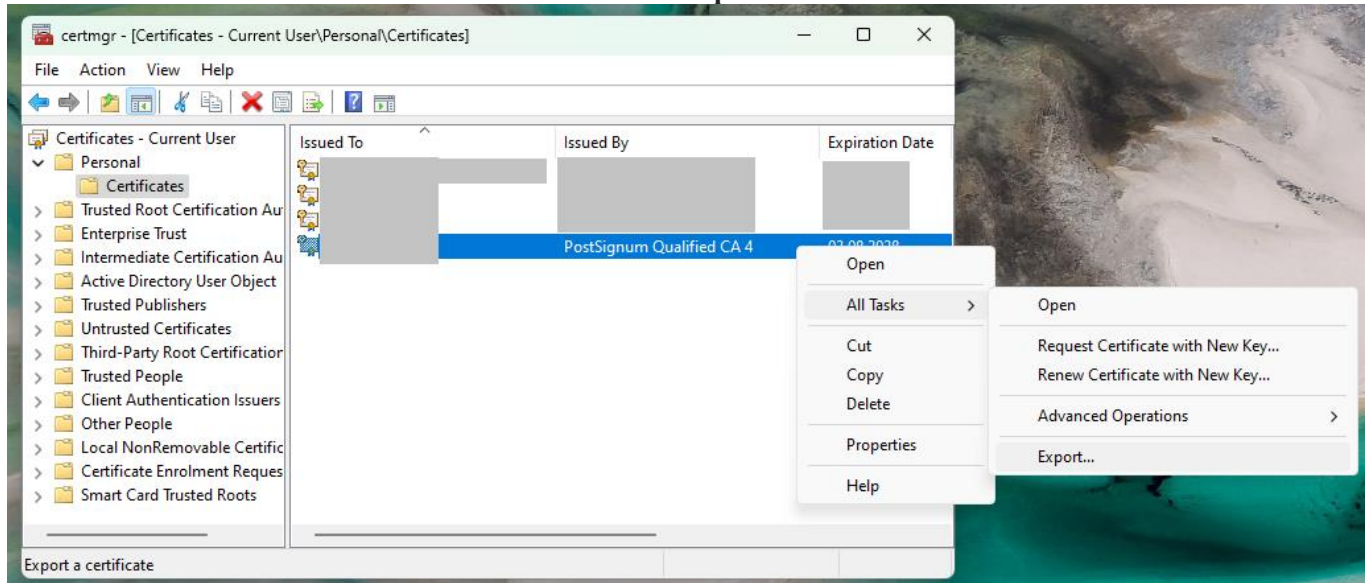
Press the keys **win** () + **R**, dialog window „Run“ will open. Here please type: „**certmgr.msc**“.



Then click on **OK**, or press the **Enter** key. Window below will open.

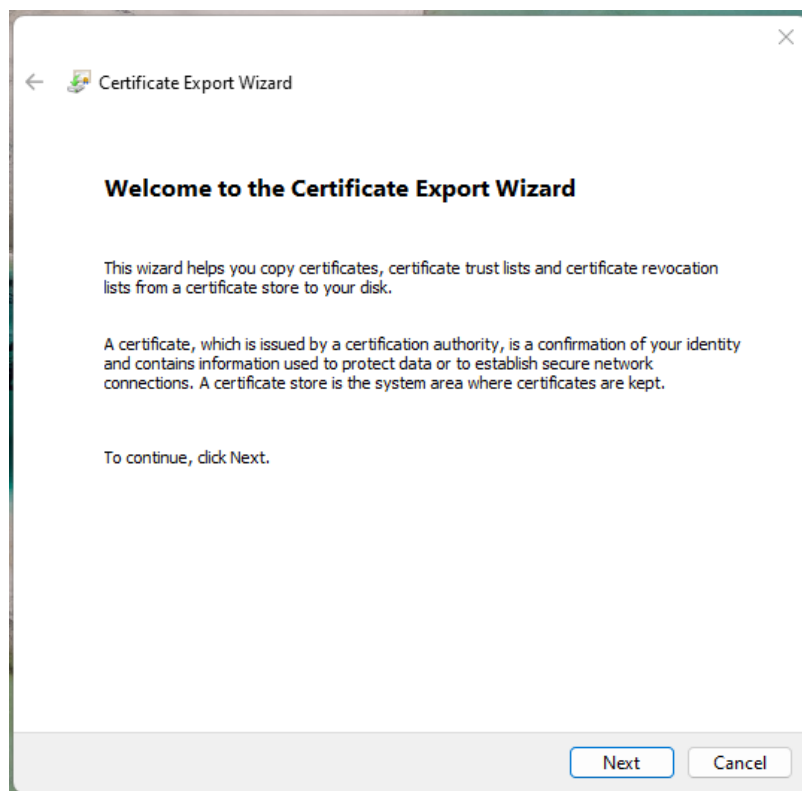


Open the **tab Personal** → **Certificates**
Choose your certificate and right click on it
→ **All tasks** → **Export**

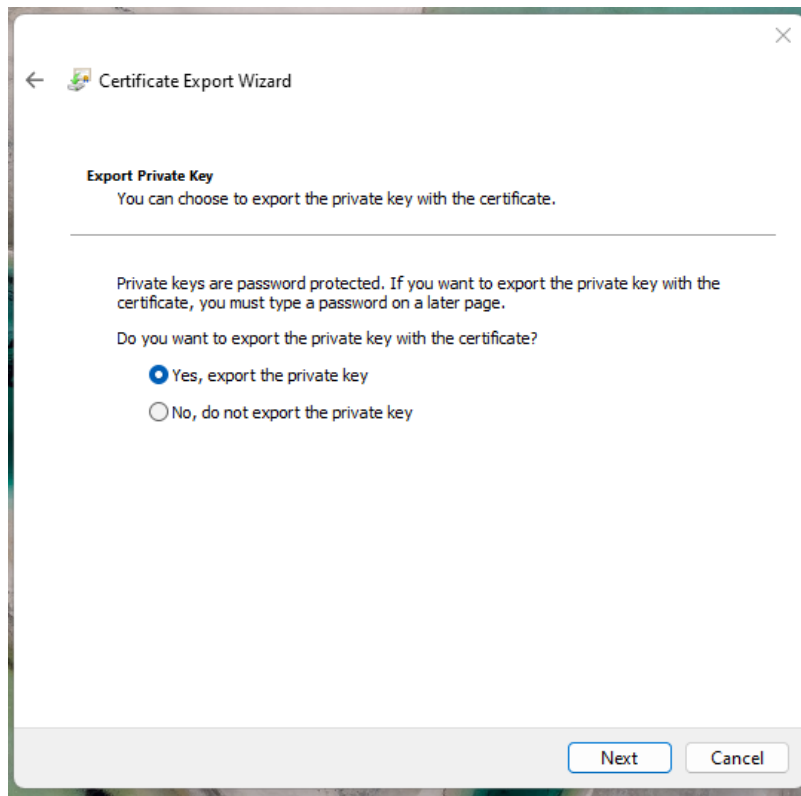


New window opens called:
Certificate Export Wizard

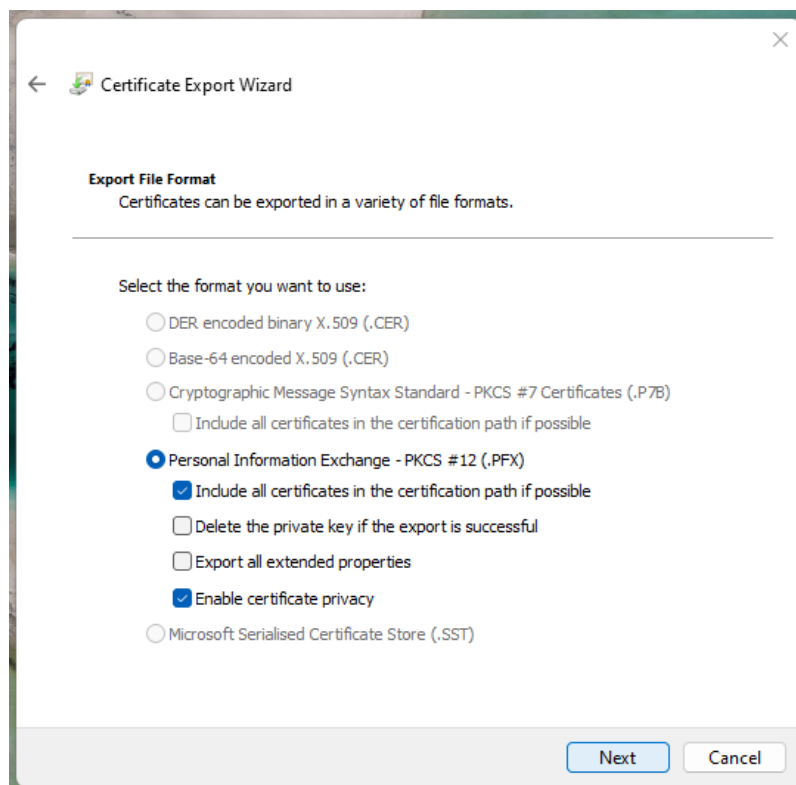
Continue by pressing **Next** button.



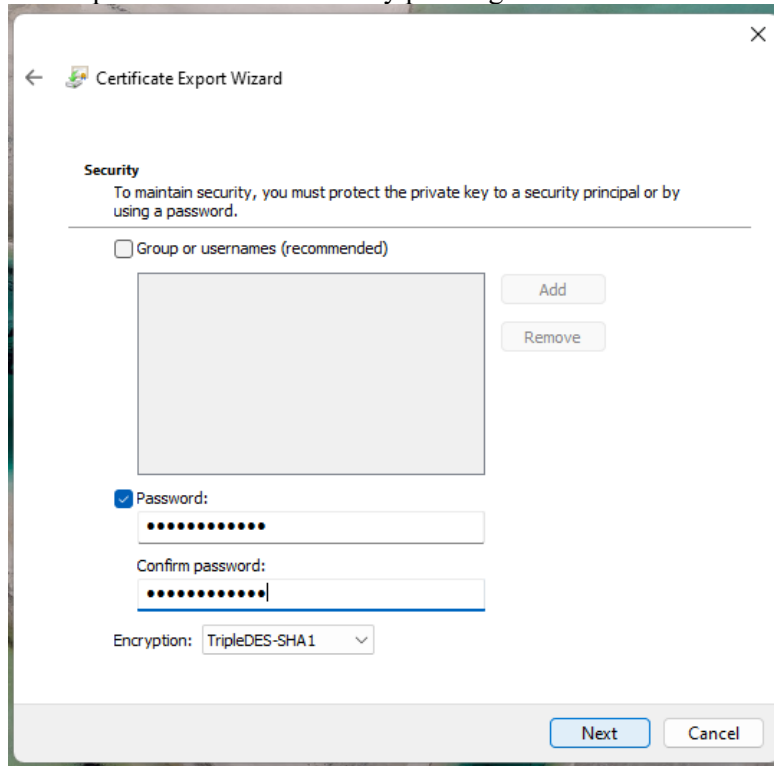
In the next step choose the option „**Yes, export the private key**” And click on the **Next** button



Keep the default options „**Personal Information Exchange - .pfx**” and continue by pressing the **Next** button.

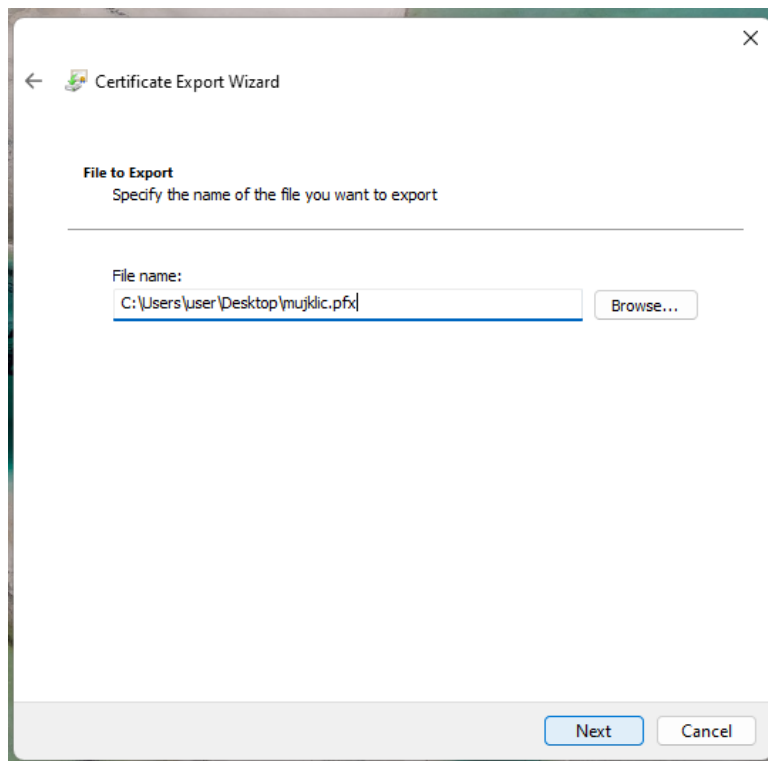


Next choose a **password** for the file (choose password that will protect the private key) Confirm the password and continue by pressing the **Next** button.



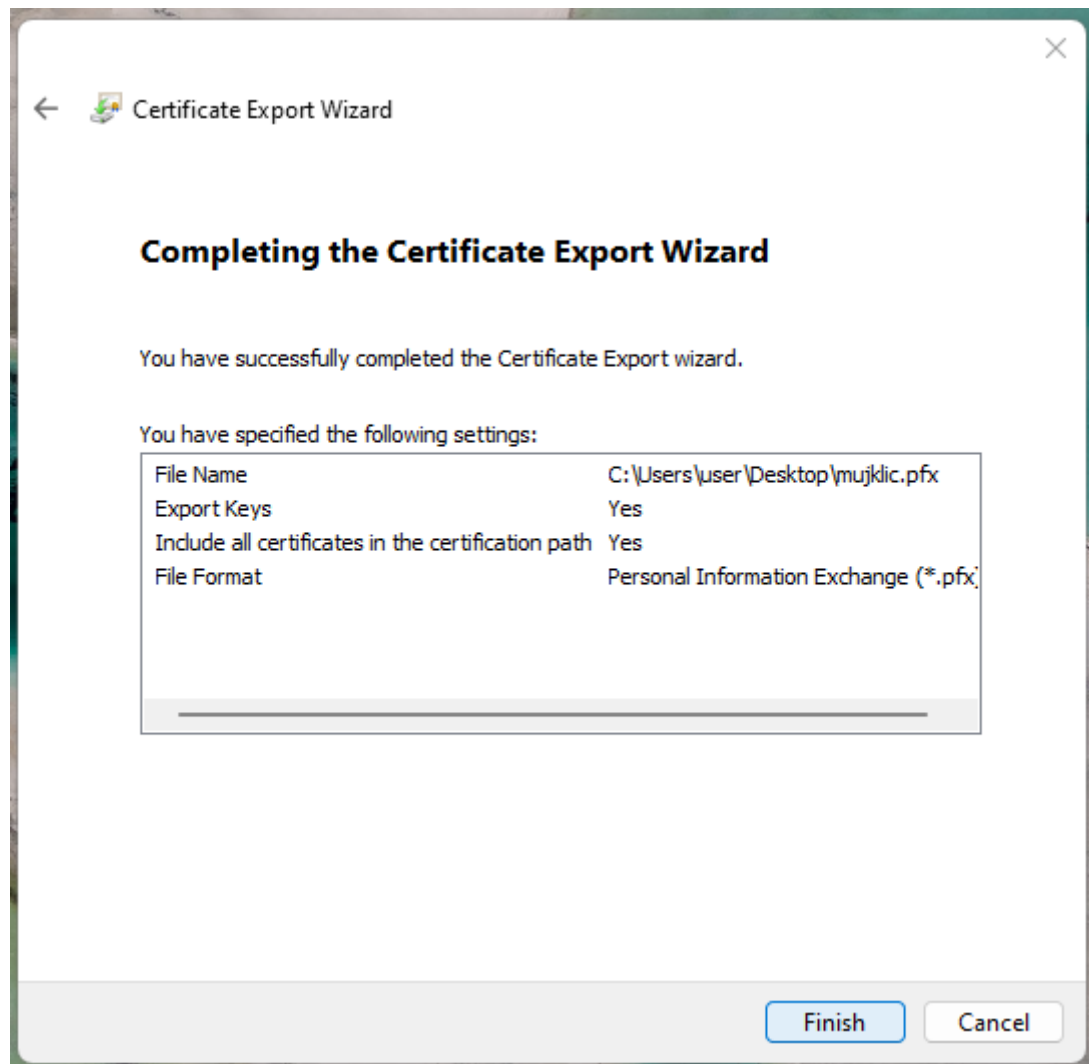
The screenshot shows the 'Security' step of the Certificate Export Wizard. It includes a checkbox for 'Group or usernames (recommended)', a list box, and 'Add'/'Remove' buttons. The 'Password' checkbox is selected, with fields for 'Password' and 'Confirm password'. The 'Encryption' dropdown is set to 'TripleDES-SHA1'. 'Next' and 'Cancel' buttons are at the bottom right.

Next choose where will your exported certificate be saved – Click on the **Browse** button, name the file, and continue by pressing the **Next** button.



The screenshot shows the 'File to Export' step of the Certificate Export Wizard. It has a text field for 'File name' containing 'C:\Users\user\Desktop\mujklic.pfx' and a 'Browse...' button. 'Next' and 'Cancel' buttons are at the bottom right.

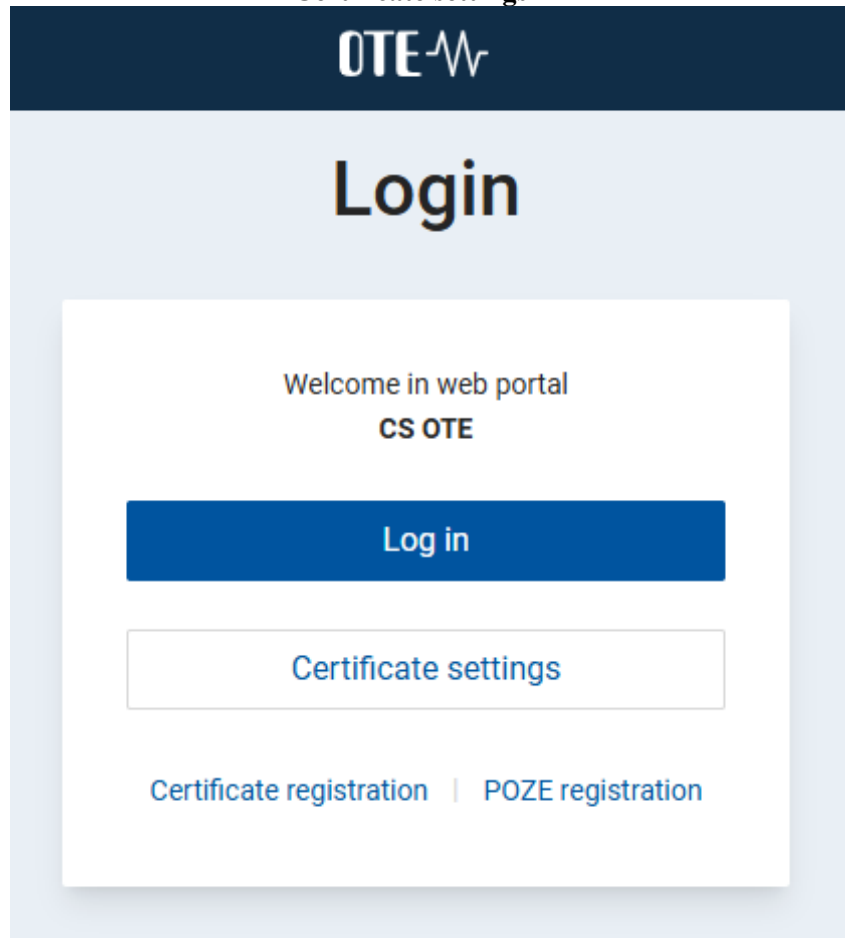
Now press the **Finish** button. After a successful export, there will be your file in previously chosen destination.



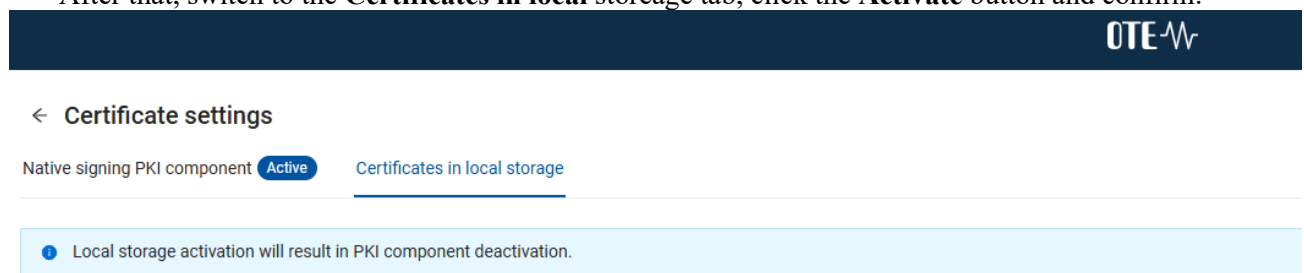
Local certificate storage setup

Local storage of a web browser allows storing certificates for digital signing. The private key of your certificate is always safely kept inside your browser behind a password. If the password is reset, the certificate is deleted from the local certificate storage. It is recommended to keep a backup of your exported certificate somewhere safe. It is needed to import your exported certificate containing the private key, as we've went through in the steps above. (file in the *.p12 or *.pfx file type). New import is needed after each certificate renewal.

To import certificate and setup the local certificate storage please open the **CS OTE Portal** and click on the **Certificate settings** button.



After that, switch to the **Certificates in local** storage tab, click the **Activate** button and confirm.



Local storage is not active

Do you want to activate it now?

Aktivovat

OTE

Would you like to set it up now?

Save

[+ Add certificate](#)

Add certificate

Drag the file here

or

Select a file

kvalifikovany-zaloha.pfx

* Password for personal certificate private key

.....

The private part is not sent to the server. It is stored locally in the browser directory. Secured as a PKCS#12 file.

Back

Import

After a successful import, you will see your certificate in the list. That means the process was successful, your certificate is now in the system and should work.

OTE
🔍 ⚙️ CZ

← Certificate settings
Manual for OTE system

Native signing PKI component
Certificates in local storage Active

Certificates in local storage
Change password to local storage Deactivate local storage

● Local storage is active.

Imported certificates in local storage
+ Add certificate

| Primary certificate | DN | Certification authority | Serial number | Valid from | Valid to | State |
|---------------------|----|---|---------------|------------|----------|-------|
| 🔍 | | C=CZ, NTRCZ-47114983, O=Česká pošta, s.p., CN=PostSignum Qualified CA 4 | | | | Valid |

A total of 1 entries
< 1 >
Go to page 1

Now you can login using your certificate in the local certificate storage - [Portal OTE \(ote-cr.cz\)](https://portal.ote-cr.cz)