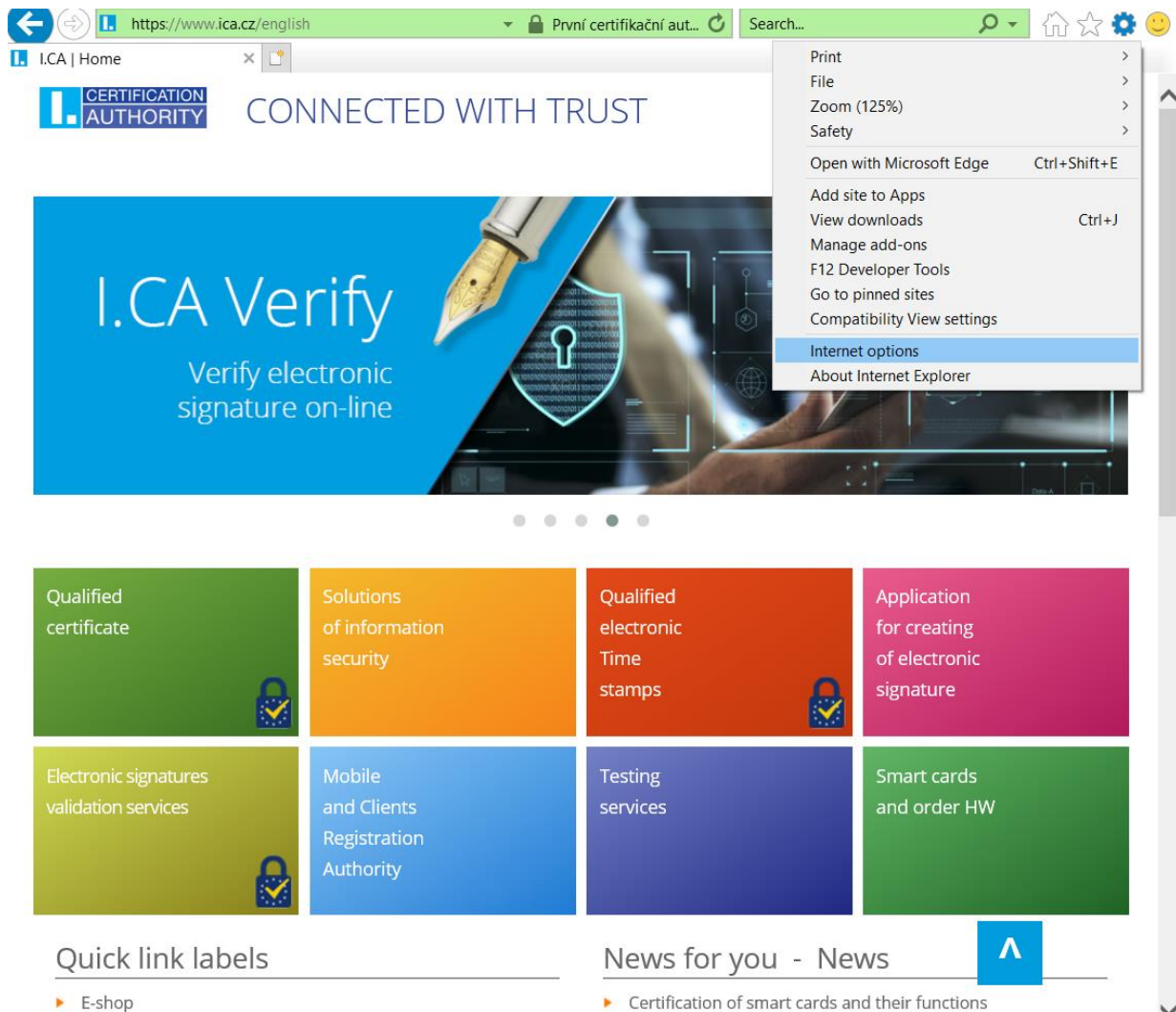


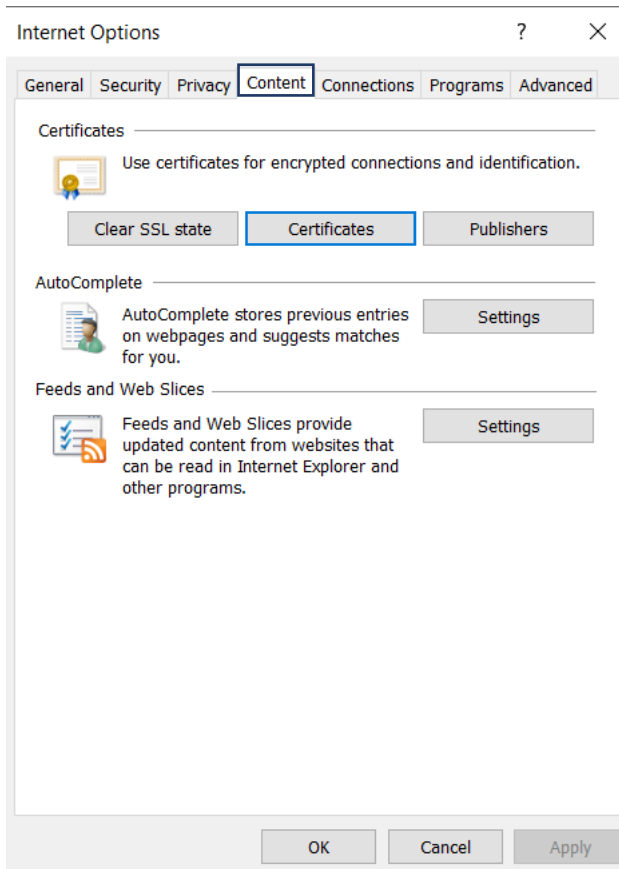
Certificate transfer between Windows systems

Start the Internet Explorer browser and click on the tools in upper right corner (see below). Then choose the “Internet options” .

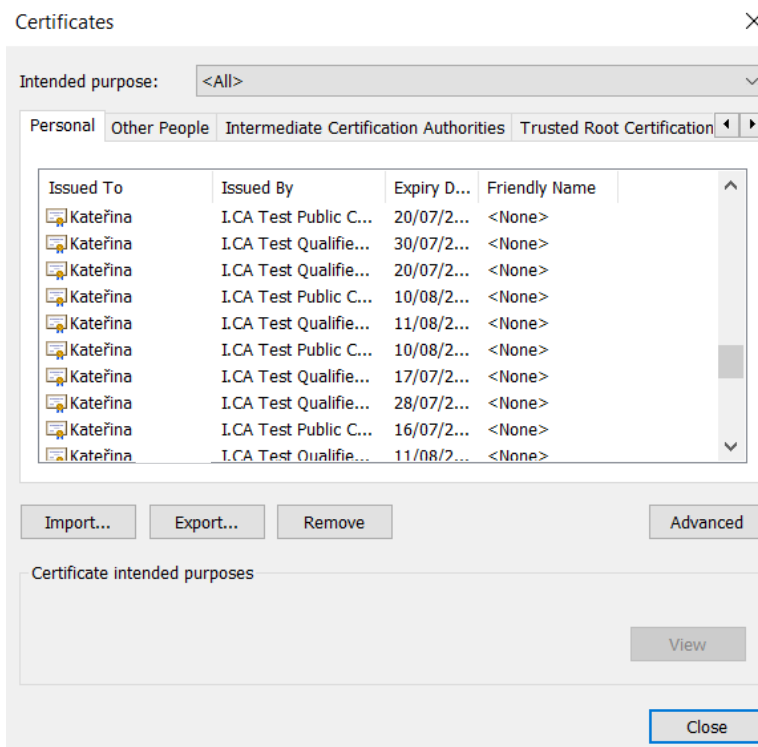


The screenshot shows the Internet Explorer browser interface. The address bar displays <https://www.ica.cz/english>. The page content includes the I.CA logo and the text "CONNECTED WITH TRUST". A large banner for "I.CA Verify" is visible, with the subtext "Verify electronic signature on-line". A context menu is open in the upper right corner, listing various options such as "Print", "File", "Zoom (125%)", and "Internet options". The "Internet options" option is highlighted. Below the banner, there is a grid of eight colored tiles representing different services: "Qualified certificate", "Solutions of information security", "Qualified electronic Time stamps", "Application for creating of electronic signature", "Electronic signatures validation services", "Mobile and Clients Registration Authority", "Testing services", and "Smart cards and order HW". At the bottom, there are two sections: "Quick link labels" with a link to "E-shop" and "News for you - News" with a link to "Certification of smart cards and their functions".

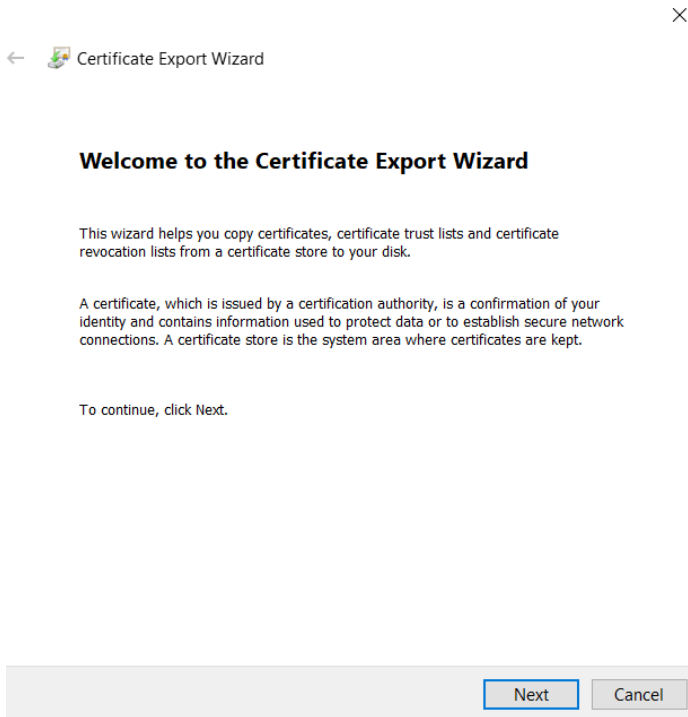
Then choose the tab **Content** and click on **Certificates** button



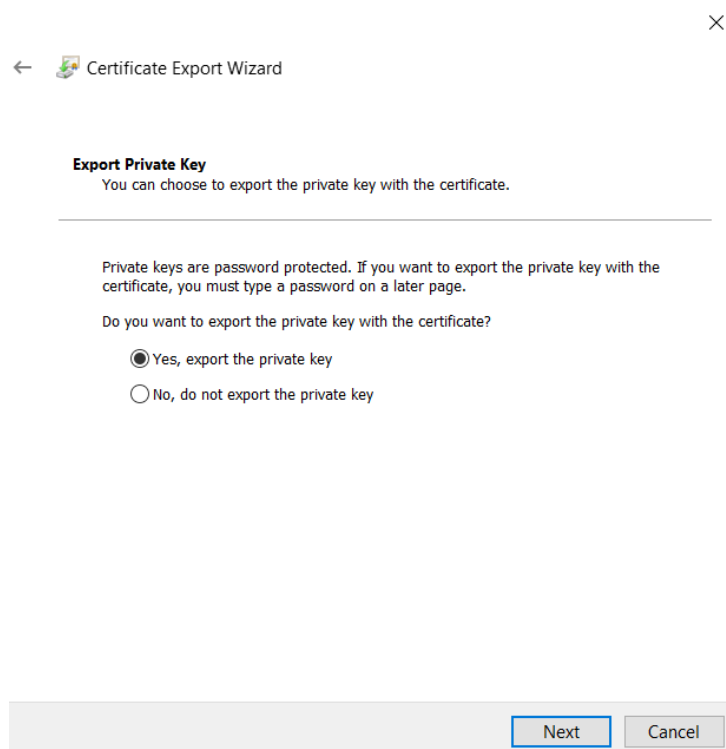
Mark the certificate which you want to back up and click on the **Export** button



In the export provider click **Next**.



Choose the option **YES, export the private key**



Keep the current set up of format **PKCS#12**.

×

←  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
 - Enable certificate privacy
- Microsoft Serialised Certificate Store (.SST)

Next

Cancel

Enter your password to protect your back up displayed in Windows 8, 8.1.

×

←  Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

Group or usernames (recommended)

Add

Remove

Password:

Confirm password:

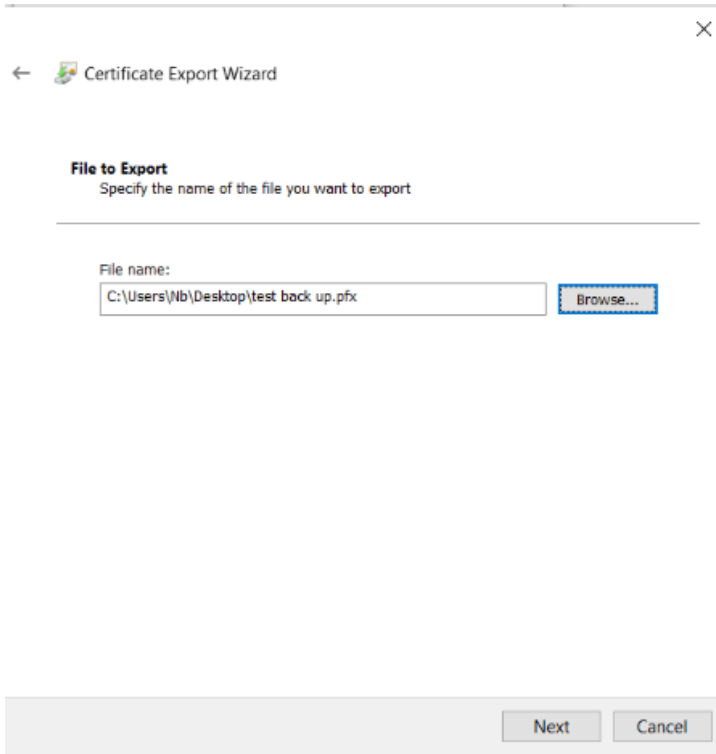
Encryption: TripleDES-SHA1

Next

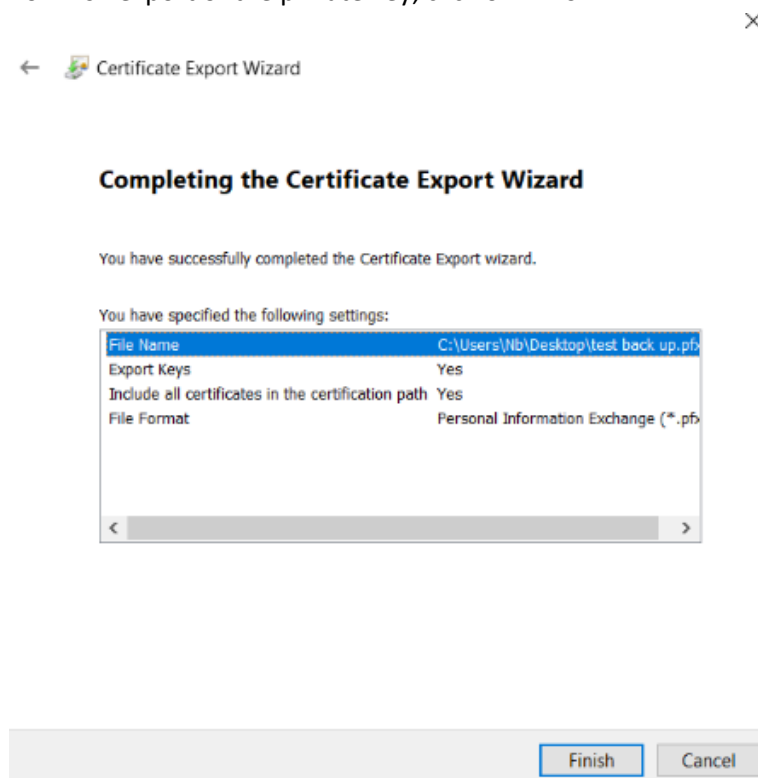
Cancel

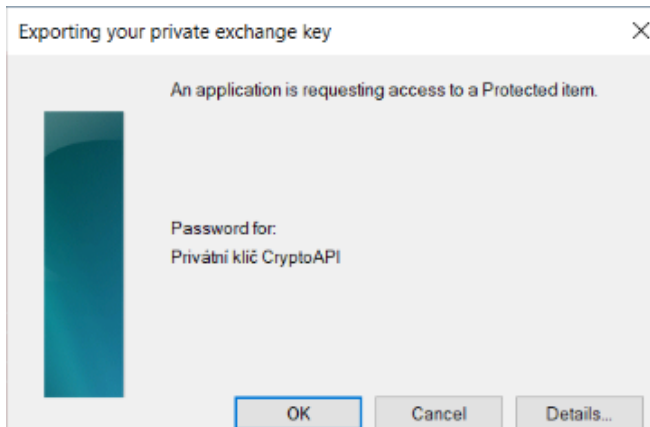
Choose the file, where the private key will be exported. Use the **Browse** button.

Continue with **Next** button



To finish export of the private key, click on **Finish**.





Certificate Export Wizard

The export was successful.

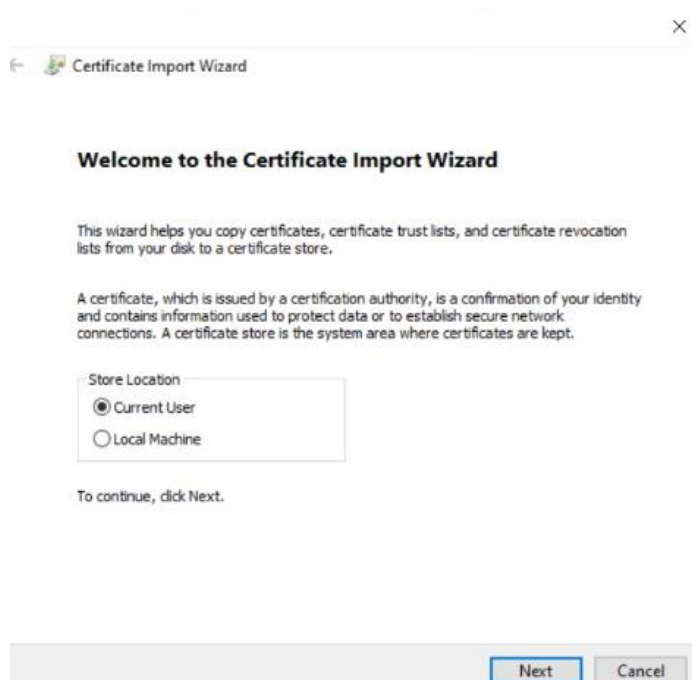
OK

Now the back up containing certificate and private key is saved in chosen file.

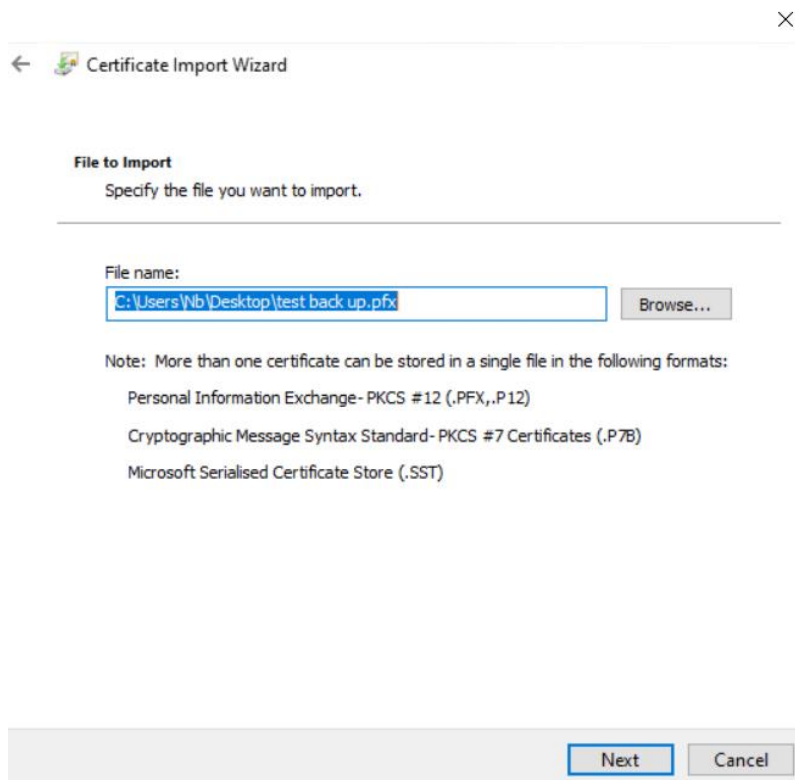
Transfer the file with back up into the new PC and open the file. After this step the **Certificate Import Wizard** will be open.



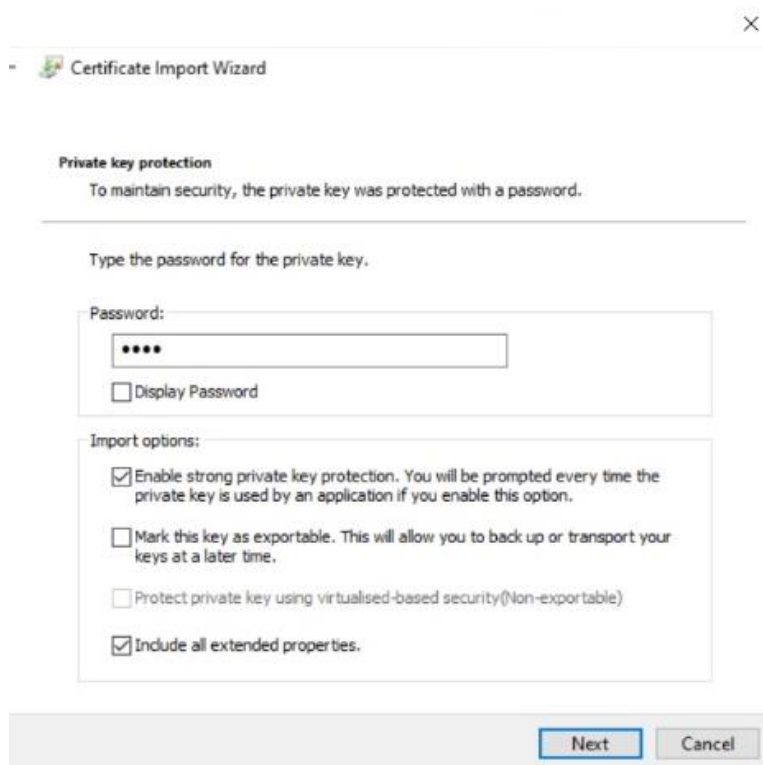
Choose the field with **Current User** and continue with **Next** button.



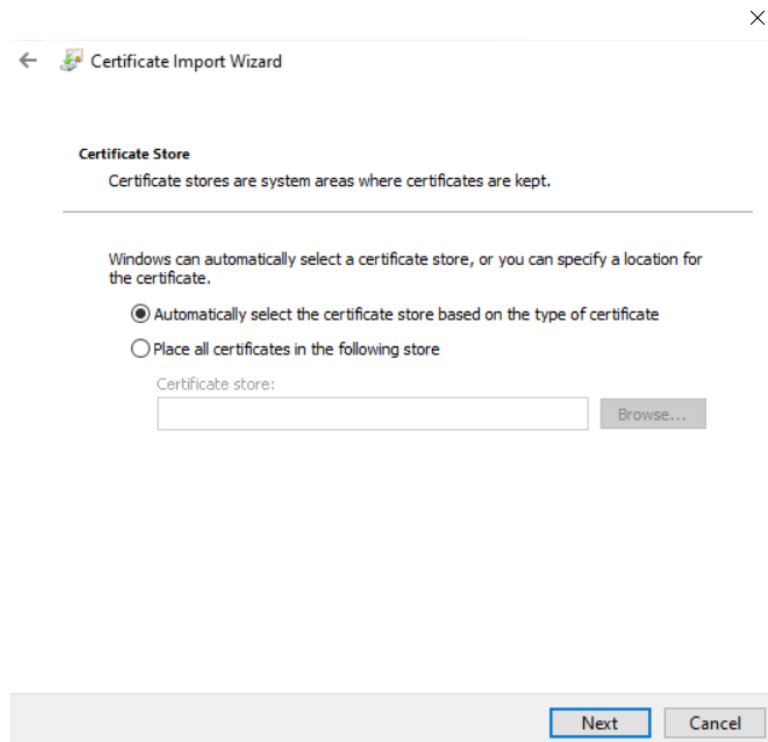
Choose the file to import by the button Browse. Click on **Next** button.



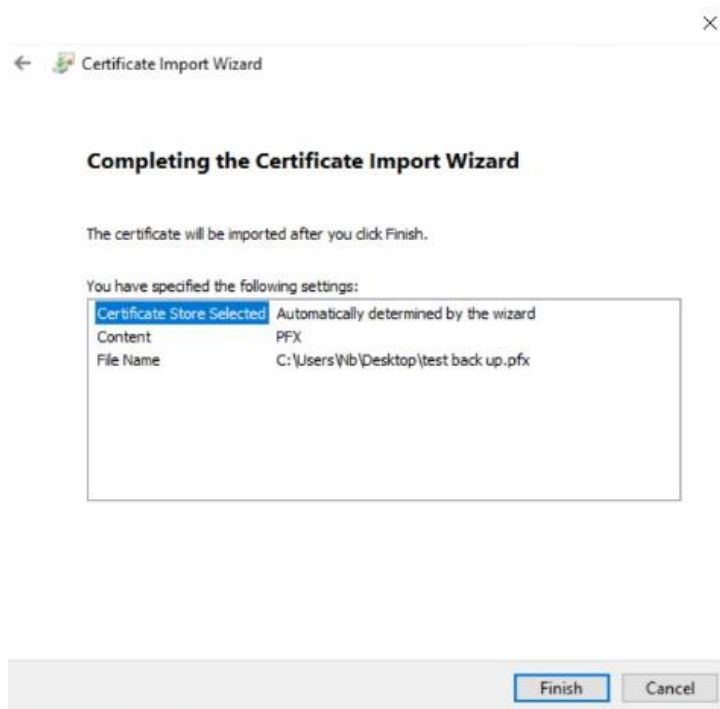
Insert the **password**, chosen while export of back up and then continue with **Next** button.

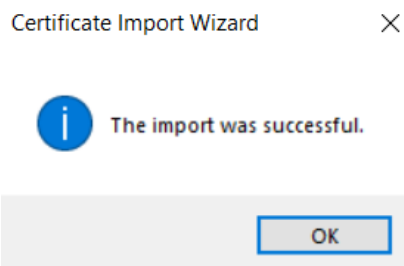


Choose the option “**Automatically select the certificate store based on the type of certificate**” and then click on **Next**.



Now you can finish the certificate import by click on **Finish** button.





Now your certificate is completely functional.