Instructions for Setting Up a Workplace to Use Enhanced Unqualified Electronic Signature (EUES)

Table of Contents

1. Technical Specifications

The following technical specifications are required for the correct operation of the EUES

- Windows 10, 11 operating system
- Token drivers
- CryptoPro CSP software, version 5.0 and higher
- CryptoPro EDS Browser plug-in
- Installed root certificate of ROSELTORG Certification Authority
- Access to the certificate revocation list of ROSELTORG Certification Authority located at http://ntrust.roseltorg.ru.

2. Installing token drivers

The Bank issues Rutoken tokens, produced in Russia, as a secure carrier. It is mandatory to install the appropriate software (drivers) to work with it.

- Go to the software download page [Drivers for Windows / Download Center / Support (rutoken.ru)](https://www.rutoken.ru/support/download/windows/) (https://www.rutoken.ru/support/download/windows/)

- Select "**Rutoken Drivers for Windows, EXE**"
- Read the LICENSE AGREEMENT and check the box next to "**I have read and agree to the Terms and Conditions of the License Agreement in full**"
- Click the "**TERMS AND CONDITIONS ACCEPTED**" button
- The **rtDrivers.exe** file will start downloading
- Run the downloaded file
- On the installation dialog box that appears, click the "**Install**" button
- When the installation is complete, click the "**Close**" button
- Drivers installed

3. CryptoPRO software installation

The CryptoPro CSP installation kit can be found on the vendor's website cryptopro.ru. The kit is freely downloadable following simple registration on the site.

- Download the CryptoPro | CryptoPro CSP (cryptopro.ru) installation kit. (https://www.cryptopro.ru/products/csp?csp=download) It is recommended to download the latest version and edition of the software.
- Follow the CIPF Usage Guidelines, Section 1 to install the CryptoPro CSP software.

❗ The kit does not include a license. The demo version runs for 30 days from the date of first installation.

If an EUES **with an embedded CryptoPro license** has been obtained, the CryptoPro CSP software **will be fully functional** until the expiry of the EUES.

If the EUES was obtained **without an embedded CryptoPro license**, it is necessary to independently purchase a license for CryptoPro CSP and enter its serial number (CIPF Usage Guidelines, Section 2.3).

4. Installing CryptoPro EDS Browser plug-in

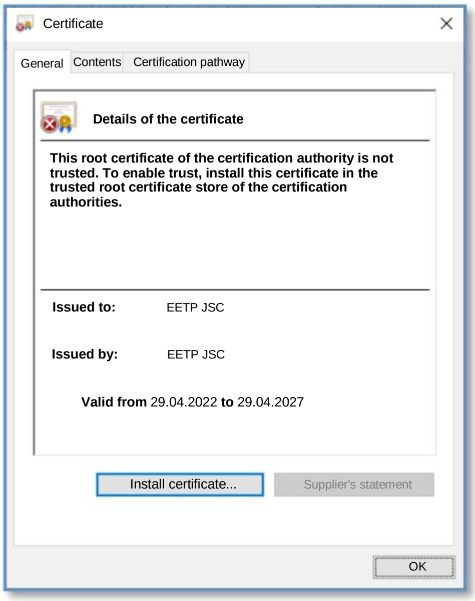
Browsers require the "**CryptoPro EDS Browser plug-in**" specialized extension to work with EUES. Please note that having CryptoPro CSP software installed is necessary.

Original Installation Instructions Installing CryptoPro EDS Browser plug-in in Windows (cryptopro.ru) (https://docs.cryptopro.ru/cades/plugin/plugin-installation-windows) Follow the provided installation instructions.

5. Installing the root certificate of the certification authority

For the correct operation of the EUES, having the ROSELTORG Certification Authority's root certificate installed is necessary.

- Download the EETP JSC Root Certificate (Unqualified CA) Root Certificate by clicking here. (https://www.roseltorg.ru/_flysystem/webdav/2022/11/18/inline-files/Koren_Nekval.cer)
- Open the downloaded certificate
- Click the "**Install Certificate**..." button



Details of the certificate

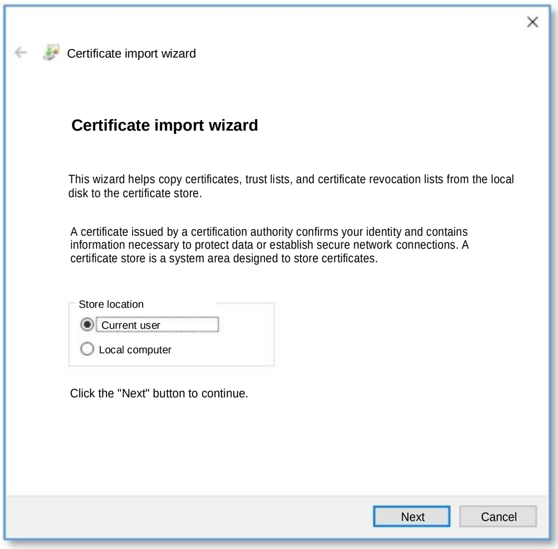
This root certificate of the certification authority is not trusted. To enable trust, install this certificate in the trusted root certificate store of the certification authorities.

Issued to: EETP JSC

Issued by: EETP JSC

Valid from 29.04.2022 **to** 29.04.2027

- Select "**Current User**" and click the "**Next**" button



Certificate import wizard

This wizard helps copy certificates, trust lists, and certificate revocation lists from the local disk to the certificate store.

A certificate issued by a certification authority confirms your identity and contains information necessary to protect data or establish secure network connections. A certificate store is a system area designed to store certificates.

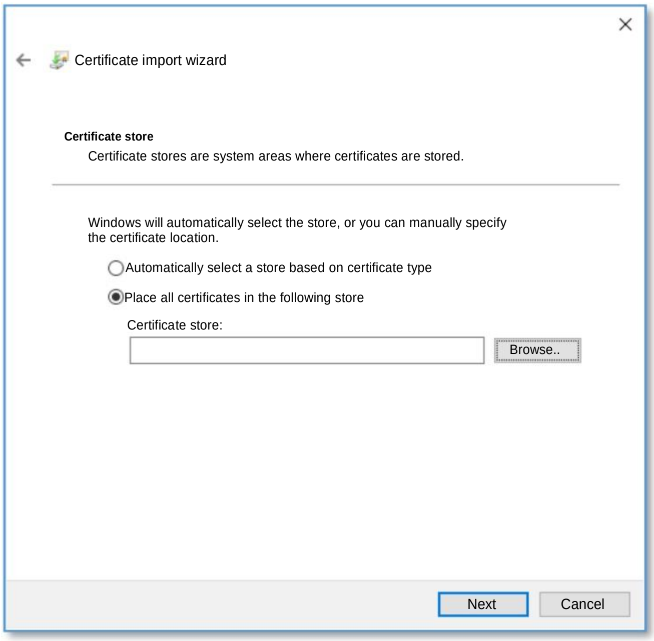
Store location

● Current user

○ Local computer

Click the "Next" button to continue.

- Select "**Place all certificates in the following store**" and click the "**Browse**" button:



Certificate import wizard

Certificate store

Certificate stores are system areas where certificates are stored.

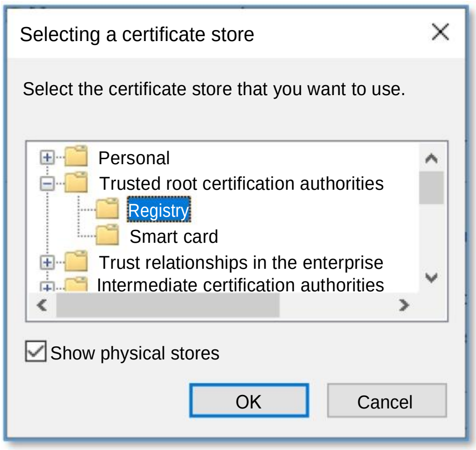
Windows will automatically select the store, or you can manually specify the certificate location.

○ Automatically select a store based on certificate type

● Place all certificates in the following store

Certificate store:

- Click the "**Show physical stores**" checkbox, expand the "**Trusted root certification authorities**" branch, select "**Registry**" and click "OK":



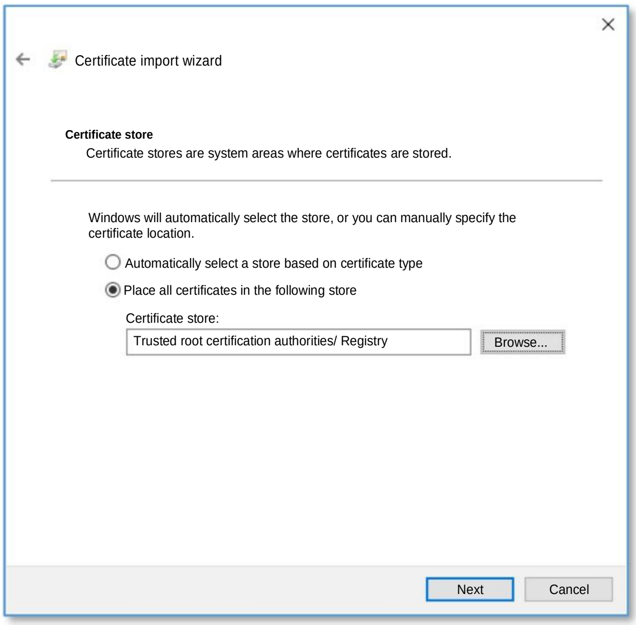
Selecting a certificate store

Select the certificate store that you want to use.

Personal
Trusted root certification authorities
Registry
Smart card
Trust relationships in the enterprise
Intermediate certification authorities

☑ Show physical stores

- Click "**Next**" to proceed to the next step:



Certificate import wizard

Certificate store

Certificate stores are system areas where certificates are stored.

Windows will automatically select the store, or you can manually specify the certificate location.

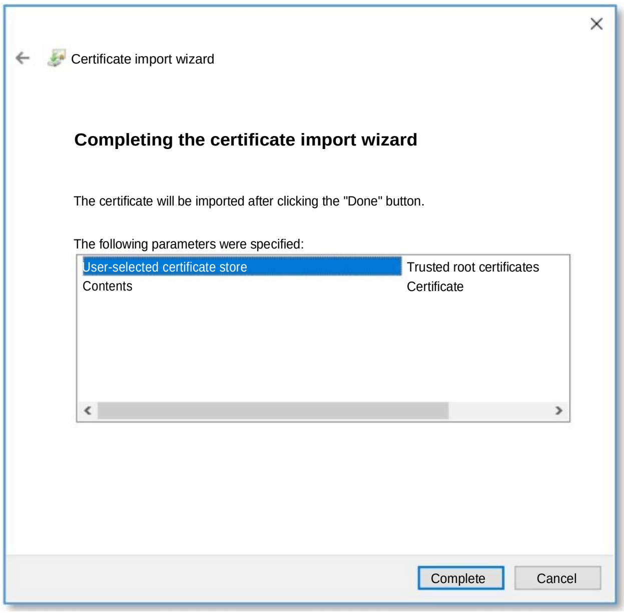
○ Automatically select a store based on certificate type

● Place all certificates in the following store

Certificate store:

Trusted root certification authorities/ Registry

- Complete the certificate import by clicking on the "**Finish**" button:



Certificate import wizard

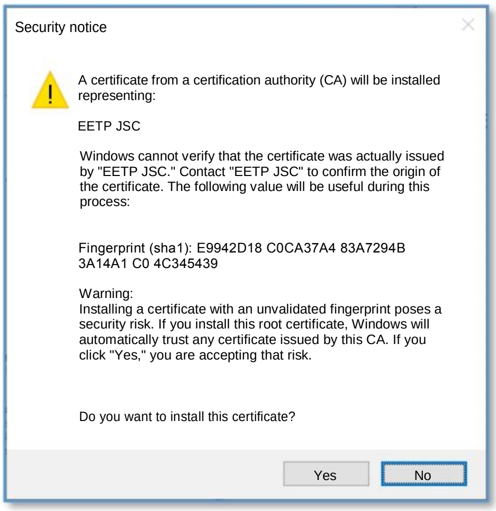
Completing the certificate import wizard

The certificate will be imported after clicking the "Done" button.

The following parameters were specified:

User-selected certificate store	Trusted root certificates
Contents	Certificate

- Confirm that the certificate will be installed by clicking on the "**Yes**" button:



Security notice

A certificate from a certification authority (CA) will be installed representing:

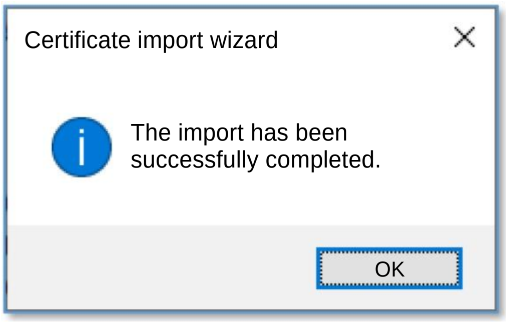
EETP JSC

Windows cannot verify that the certificate was actually issued by "EETP JSC." Contact "EETP JSC" to confirm the origin of the certificate. The following value will be useful during this process:

Fingerprint (sha1): E9942D18 C0CA37A4 83A7294B 3A14A1 C0 4C345439

Warning:
Installing a certificate with an unvalidated fingerprint poses a security risk. If you install this root certificate, Windows will automatically trust any certificate issued by this CA. If you click "Yes," you are accepting that risk.

Do you want to install this certificate?



Certificate import wizard

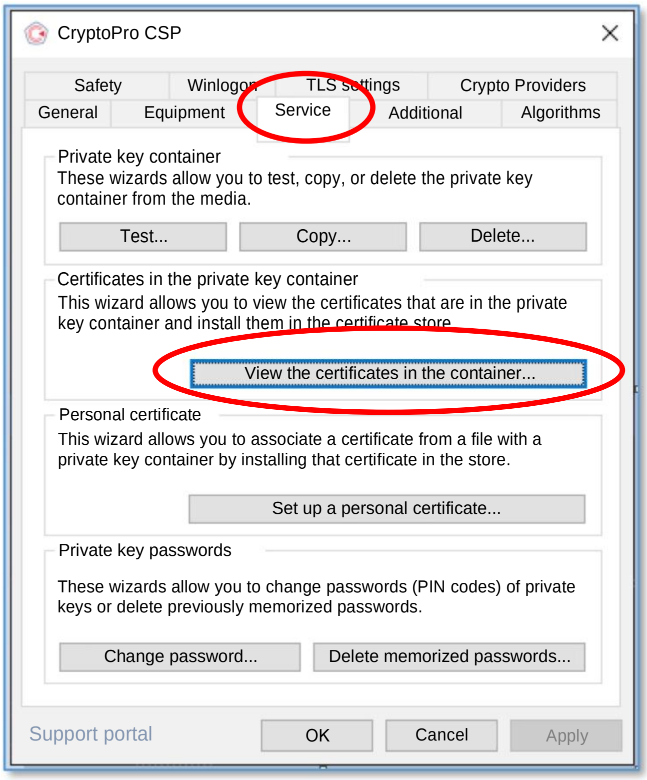
The import has been successfully completed.

- This will install the root certificate of the Certification Authority.

6. Installing a personal electronic signature verification key certificate

Use the CryptoPro CSP software to install a personal certificate.

- Insert the certificate token into the computer
- Start CryptoPro CSP
- Select the "**Tools**" tab and click on the "**View certificates in container**:..." button



CryptoPro CSP

Private key container

These wizards allow you to test, copy, or delete the private key container from the media.

Certificates in the private key container

This wizard allows you to view the certificates that are in the private key container and install them in the certificate store.

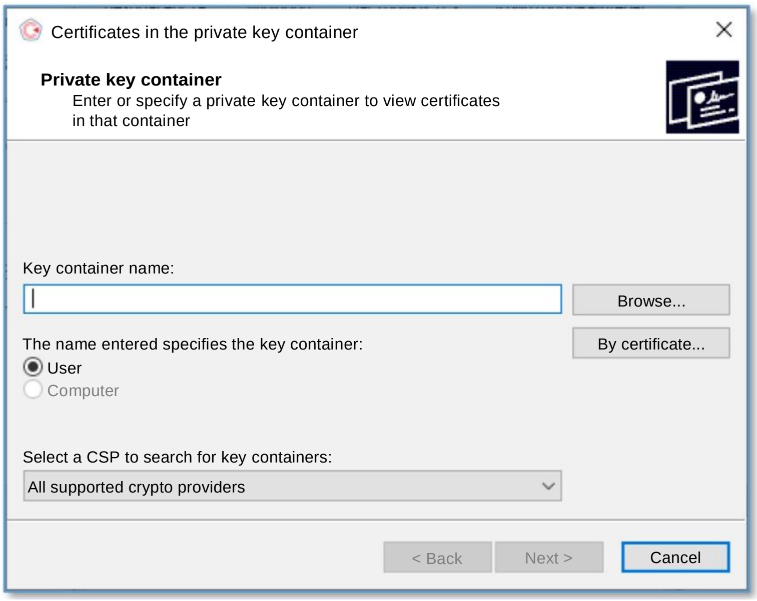
Personal certificate

This wizard allows you to associate a certificate from a file with a private key container by installing that certificate in the store.

Private key passwords

These wizards allow you to change passwords (PIN codes) of private keys or delete previously memorized passwords.

- In the window that appears, titled **"Certificates in the private key container"** , click the "**Browse...**" button:



Certificates in the private key container

Private key container

Enter or specify a private key container to view certificates in that container

Key container name:

The name entered specifies the key container:

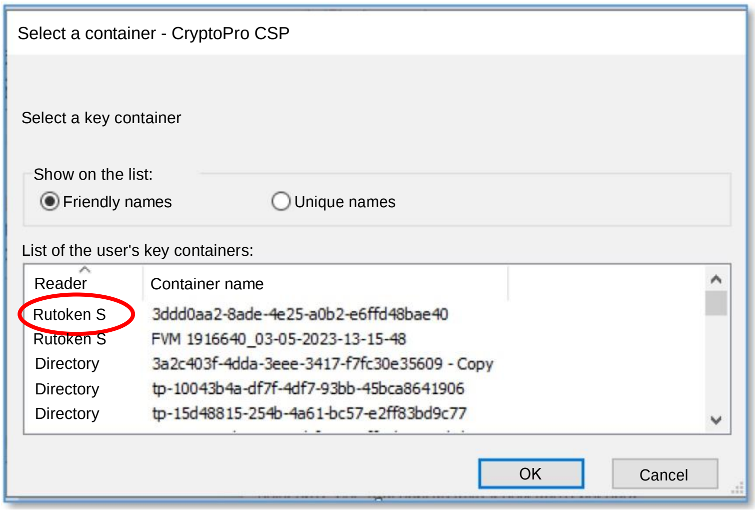
● User

○ Computer

Select a CSP to search for key containers:

All supported crypto providers

- In the container selection dialog, locate the reader named "**Rutoken S**", then click the "**OK**" button:



Select a container - CryptoPro CSP

Select a key container

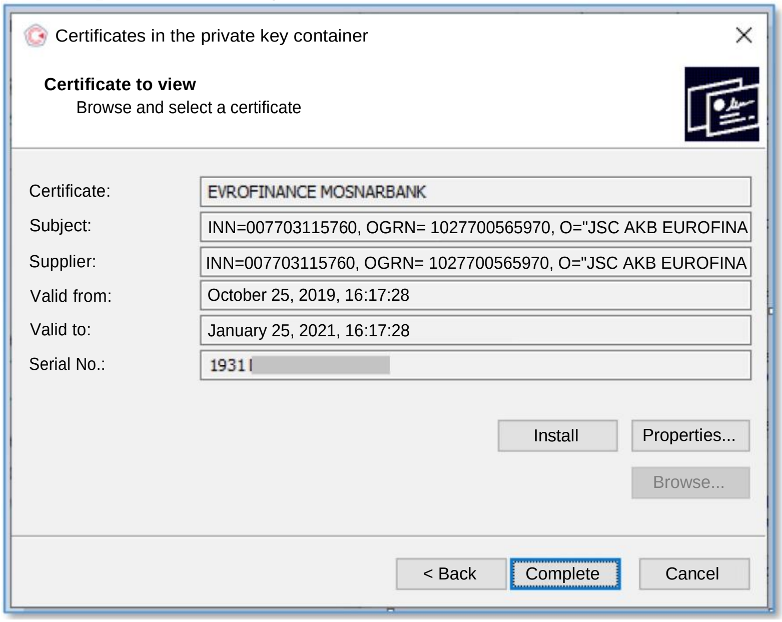
Show on the list:

● Friendly names ○ Unique names

List of the user's key containers:

Reader	Container name
Rutoken S	3ddd0aa2-8ade-4e25-a0b2-e6ffd48bae40
Rutoken S	FVM 1916640_03-05-2023-13-15-48
Directory	3a2c403f-4dda-3eee-3417-f7fc30e35609 - Copy
Directory	tp-10043b4a-df7f-4df7-93bb-45bca8641906
Directory	tp-15d48815-254b-4a61-bc57-e2ff83bd9c77

- A dialog box will appear on the screen with an option to view the properties of the certificate by clicking the "**Properties**" button and an option to install the certificate in the computer's memory:



Certificates in the private key container

Certificate to view

Browse and select a certificate

Certificate: EVROFINANCE MOSNARBANK

Subject: INN=007703115760, OGRN= 1027700565970, O="JSC AKB EUROFINA

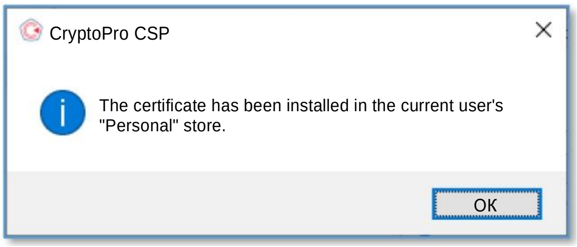
Supplier: INN=007703115760, OGRN= 1027700565970, O="JSC AKB EUROFINA

Valid from: October 25, 2019, 16:17:28

Valid to: January 25, 2021, 16:17:28

Serial No.: 1931[redacted]

- Click on the "**Install**" button to install the certificate in the computer memory.
- Upon completion of the installation, the software will display a window with the results. Click the OK button:



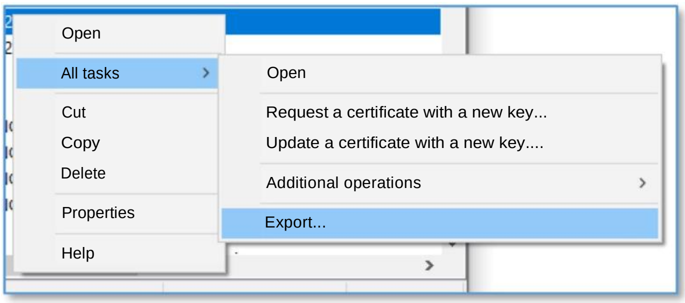
CryptoPro CSP

The certificate has been installed in the current user's "Personal" store.

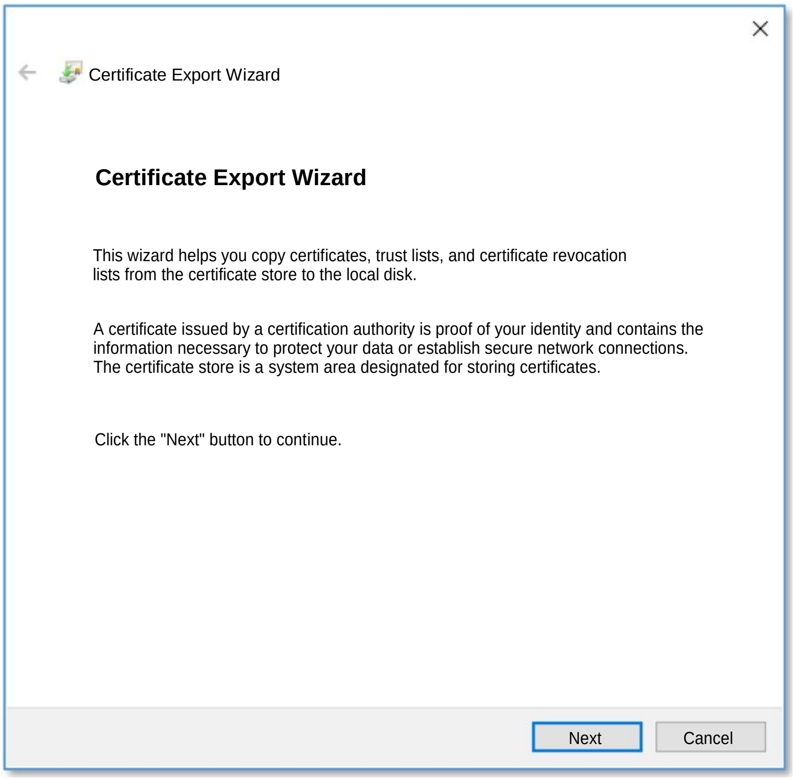
- In the "**Certificates in the private key container**" window, click "**Finish**" to complete the operation.
- In the "**CryptoPro CSP**" window, click the "OK" button to exit the program.

7. Downloading a certificate for subsequent installation in the DFA IS

- Right-click on the "**Windows**" icon
- Select the "**Run**" menu
- In the window that appears, type "**certmgr.msc**" and click "**OK**"
- In the window that appears, select the "**Certificates - Current User**" section, expand the "**Personal**" subsection and select the "**Certificates**" section
- In the right part of the window, find the installed certificate of the EUES issued by the bank and single click on the right mouse button to open the menu.
- From the menu that appears, select "**All Tasks**" > "**Export...**" to start the procedure to export the certificate to a file:


Open
All tasks
Cut
Copy
Delete
Properties
Help
Open
Request a certificate with a new key...
Update a certificate with a new key....
Additional operations
Export...

- In the "**Certificate Export Wizard**" window that opens, click the "**Next**" button



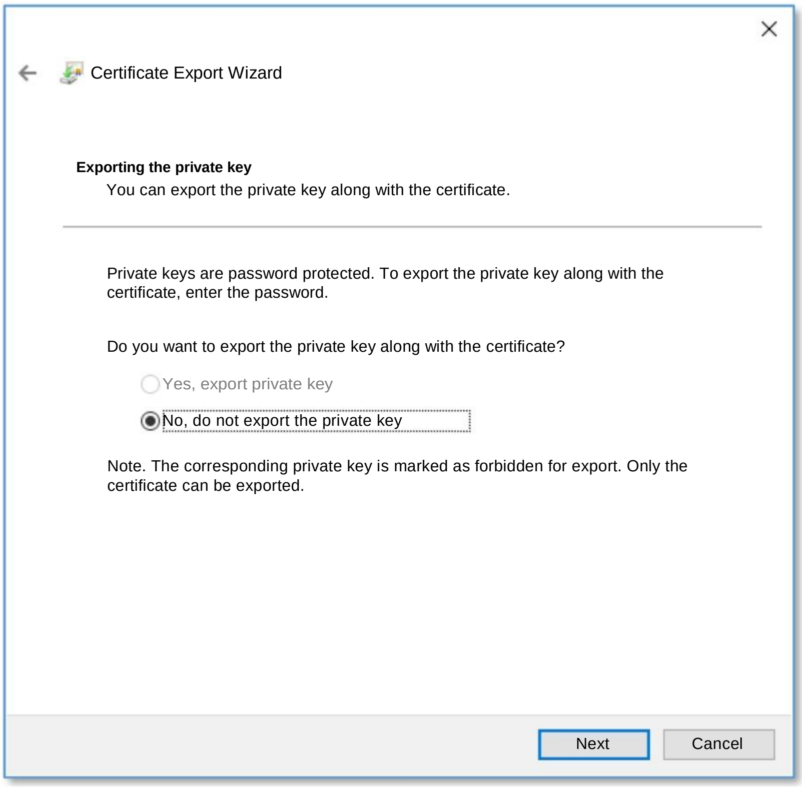
Certificate Export Wizard

This wizard helps you copy certificates, trust lists, and certificate revocation lists from the certificate store to the local disk.

A certificate issued by a certification authority is proof of your identity and contains the information necessary to protect your data or establish secure network connections. The certificate store is a system area designated for storing certificates.

Click the "Next" button to continue.

- Select "**No, do not export private key**" and click the "**Next**" button



Certificate Export Wizard

Exporting the private key

You can export the private key along with the certificate.

Private keys are password protected. To export the private key along with the certificate, enter the password.

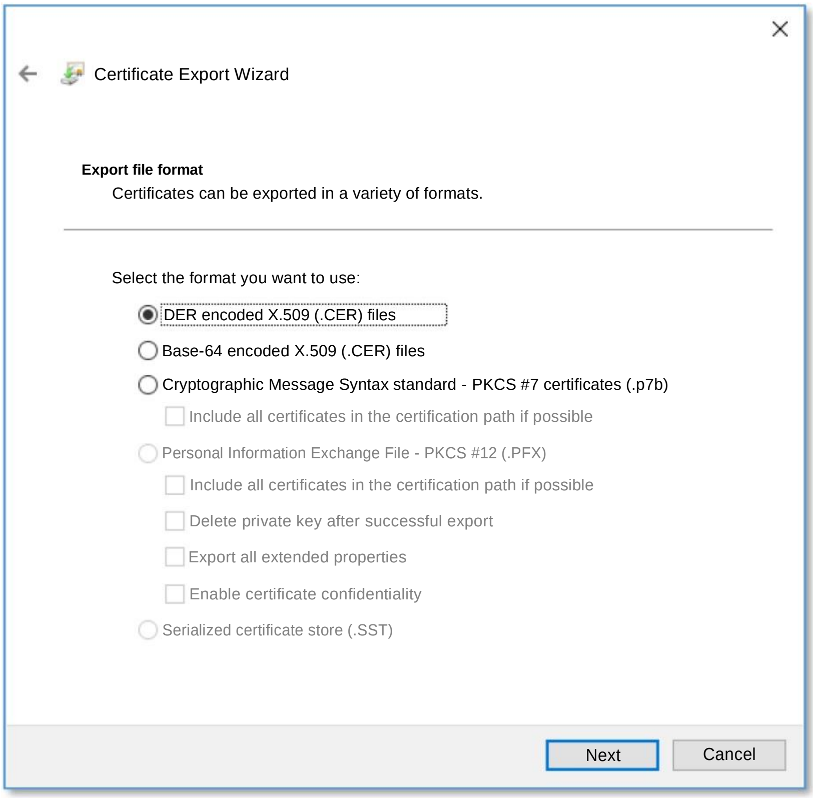
Do you want to export the private key along with the certificate?

○ Yes, export private key

● No, do not export the private key

Note. The corresponding private key is marked as forbidden for export. Only the certificate can be exported.

- Make sure that "**DER encoded X.509(.CER) files**" is selected and click the "**Next**" button



Certificate Export Wizard

Export file format

Certificates can be exported in a variety of formats.

Select the format you want to use:

● DER encoded X.509 (.CER) files

○ Base-64 encoded X.509 (.CER) files

○ Cryptographic Message Syntax standard - PKCS #7 certificates (.p7b)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange File - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

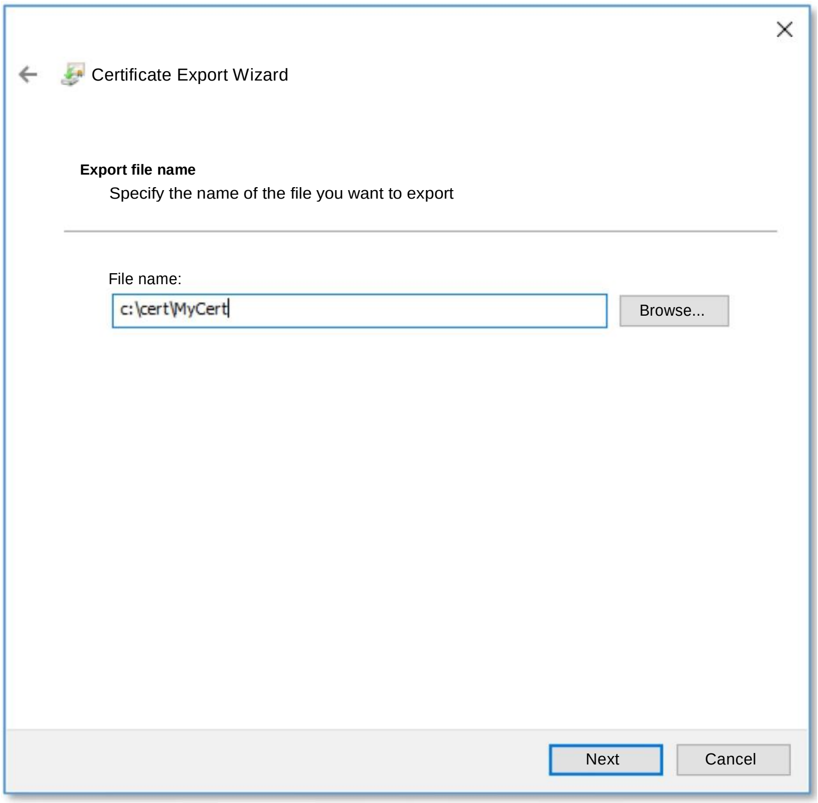
□ Delete private key after successful export

□ Export all extended properties

□ Enable certificate confidentiality

○ Serialized certificate store (.SST)

- Select the path and file name for the certificate to be exported (in the example, this file will be called "**MyCert"**) and click the "**Next**" button:



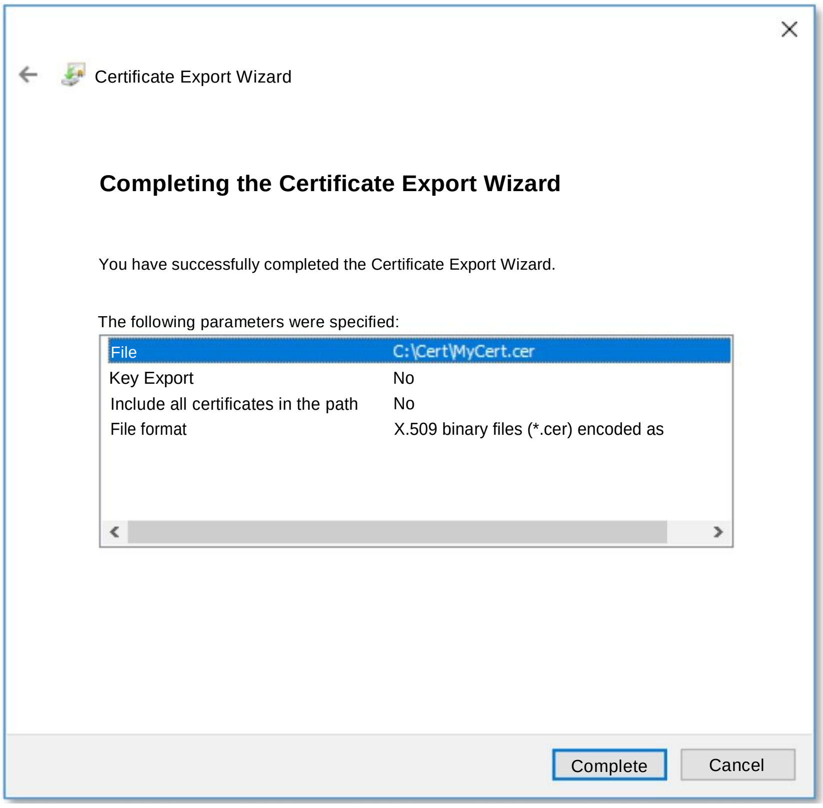
Certificate Export Wizard

Export file name

Specify the name of the file you want to export

File name: c:\cert\MyCert

- Upon completion, the "**Certificate Export Wizard Completion**" window will be displayed, where you need to click the "**Finish**" button



Certificate Export Wizard

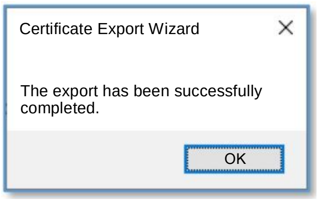
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export Wizard.

The following parameters were specified:

File	C:\Cert\MyCert.cer
Key Export	No
Include all certificates in the path	No
File format	X.509 binary files (*.cer) encoded as

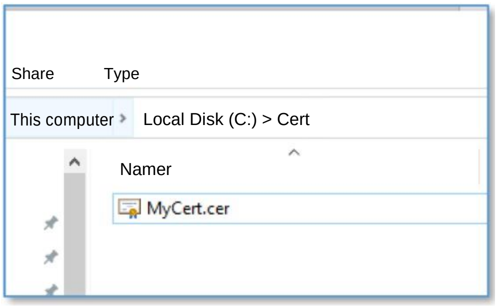
- Complete the process by clicking the "**OK**" button in the certificate export confirmation dialog:



Certificate Export Wizard

The export has been successfully completed.

- As a result, the exported certificate file will be in the directory you selected, which can be uploaded to the DFA IS (**My Account - Profile - Add Certificate**):



8. Checking the validity of the installed EUES certificate

- Right-click on the "**Windows**" icon
- Select the "**Run**" menu
- In the window that appears, type "**certmgr.msc**" and click "**OK**"
- In the window that appears, select the "**Certificates - Current User**" section, expand the "**Personal**" subsection and select the "**Certificates**" section
- In the right part of the window, find the installed EUES certificate issued by the bank and double-click the left mouse button to open it.
- The "**Certificate**" window will open
- Go to the "**Certification Path**" tab
- At the bottom of the window, in the "**Certificate Status**" field, you can obtain information about the certificate status.