Ministry of Finance

Właściciel

Instruction for obtaining a customs certificate and signing a document with an electronic signature

nazwa dokumentu

PUESC.P4.4

nazwa Projektu

2.16

Wersja

06.02.2026 r

Glossary of terms and abbreviations

Abbreviation/Term	Definition
Customs certificate	In the meaning of this instruction, this is an electronic certificate issued by the Ministry of Finance Certification Center, which enables assigning data used to verify an electronic signature to a person signing a document with an electronic signature registered on PUESC and enabling identification of this person.
SISC ID	A unique identification number assigned to the persons when registering the process in SISC.
e-Client instruction	An instruction of electronic registration for the purposes of managing the SISC services users.
PUESC	Tax and Customs Electronic Service Portal
Terms	Terms for digital certificates issued by the Ministry of Finance Certification Center.
SC	Tax and Customs Service
SISC	Tax and Customs Information System

1. Computer configuration

1.1 Installation of the CCK MF certificates

Proper operation of the certificate generation and signature process requires downloading and installing the certificates of the Ministry of Finance Certification Center (CCK MF). The CertSign application installs the necessary certificates in the Windows system at the first start (these are available for the pre-configured Internet Explorer, Edge, Chrome and Firefox browsers). The description of Firefox configuration is provided in chapter 1.3. If manual installation of the certificates is needed, these are available at https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny,in*Electronic signing of documents>Obtain or revoke a customs certificate* menu or in My Desktop ->*My data>Customs certificate* menu. The description of installation of the certificates is provided in addendum A.1

1.2 Configuration of Windows Firewall

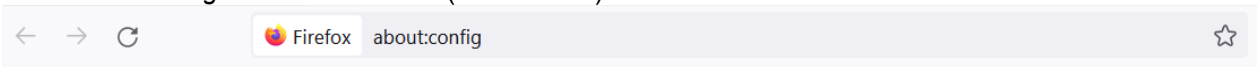
The CertSign application establishes the website connection in the computer. Manual enabling of communication between a browser and application, for example in Windows Firewall, may be necessary. A warning message may display, for example by Windows firewall. All options enabling network connection of the CertSign application should be ticked. Then click the “Enable access” button.
If any antivirus software with enabled firewall or traffic analysis is used, the following should be enabled in antivirus software:

- running the CertSign application
- unblocking communication between the browser and localhost address, ports 22443 and 22311.

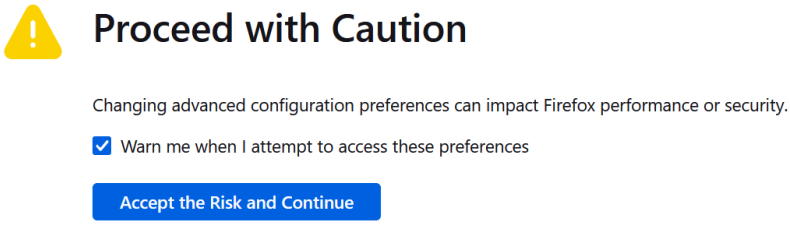
1.3 Configuration of Mozilla Firefox browser

The Firefox browser features its own *Certificate Manager,* storing the certificates required for proper cooperation between the browser and the CertSign application. In order for the browser to use the certificates registered in the Windows certificate store, the user needs to:

Enter *about:config* in the address bar (and confirm).



Confirm the warning message and select *Accept the Risk and Continue*

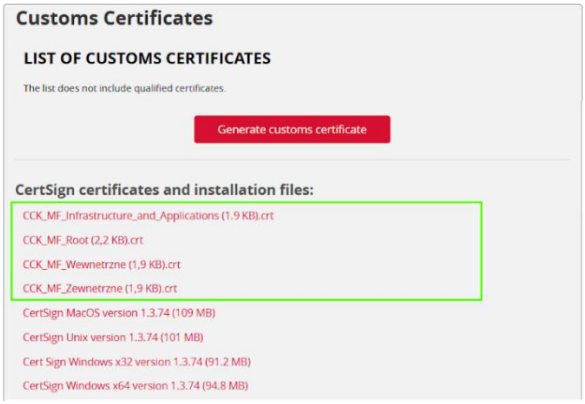


Search for the parameter *security.enterprise_roots.enabled* and set its value as *true*(logical value, change with arrows on the right side).

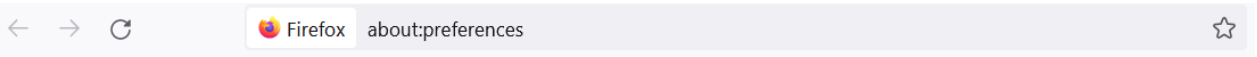
Close the browser.

After the restart, the browser should be ready to use the certificates registered in the Windows certificate store. If this setting fails to operate, the user can manually register the CCK MF certificates in the Firefox *Certificate Manager.*

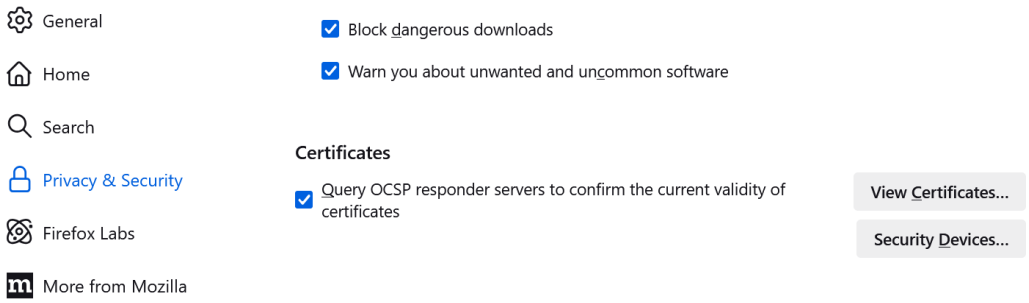
Download the following certificates from https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny: CCK MF Root, CCK MF Infrastructure and Applications, CCK MF Wewnetrzne (Internal), CCK MF Zewnetrzne (External) and save them on hard drive.



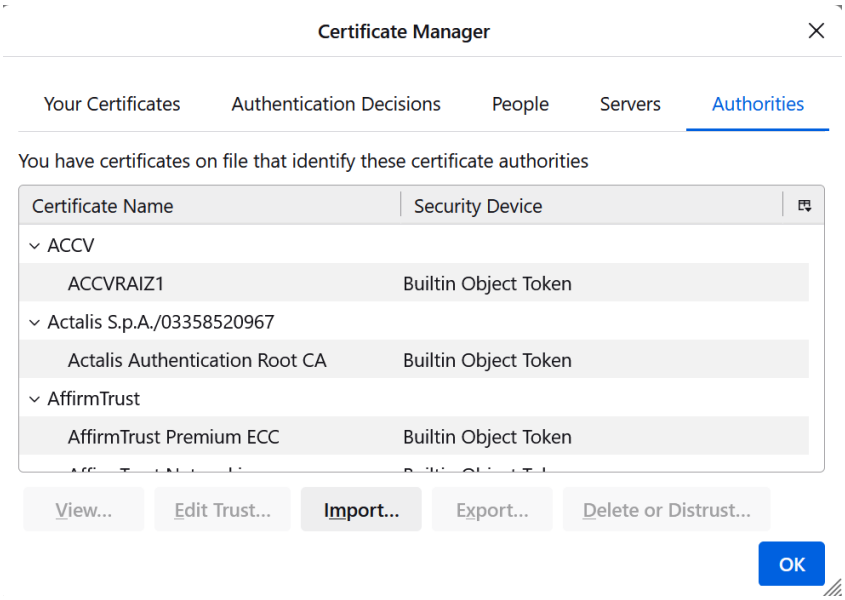
In the browser, go to Settings menu or enter *about:preferences* in the address bar and confirm.



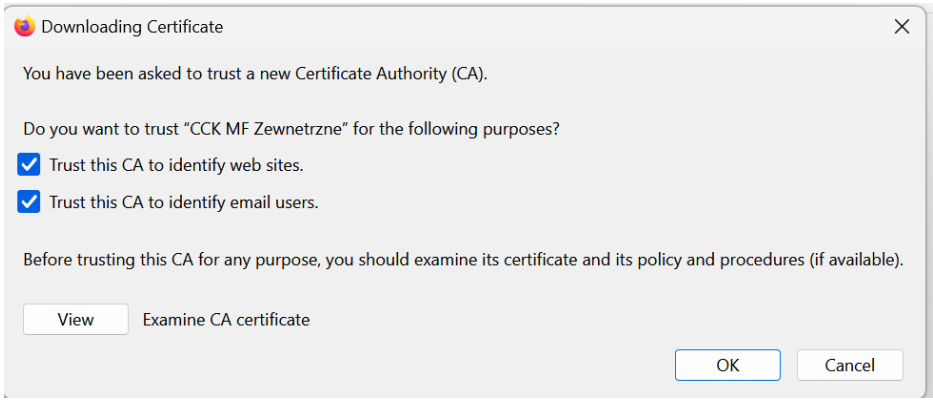
In Settings, go to *Privacy and security* and select *View Certificates.*



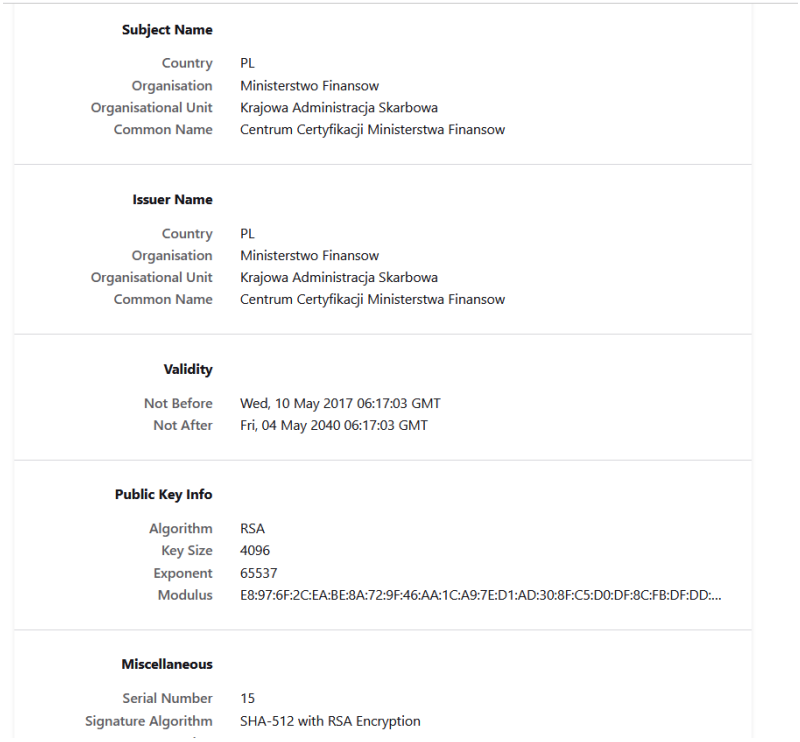
Specify the *Authorities* in the *Certificate Manager,* select *Import*, tick the certificates from the hard drive and confirm import.



At the confirmation stage, verify the certificate data and set the trust rules.



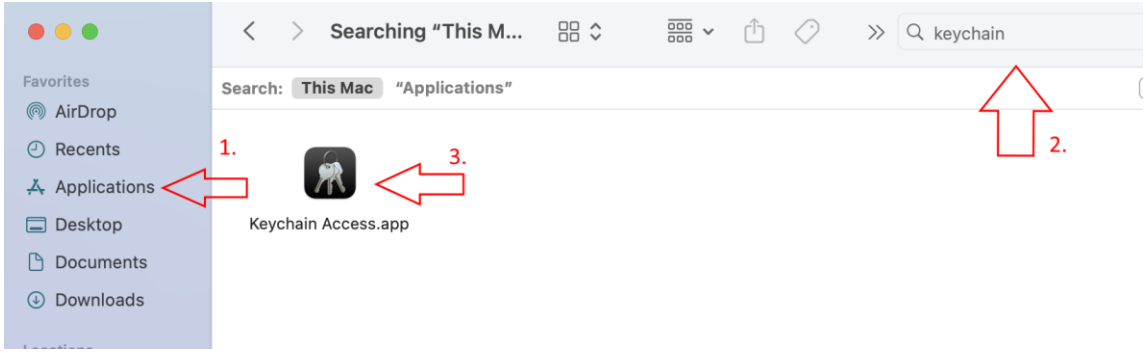
The *View* option enables verifying the certificate data.



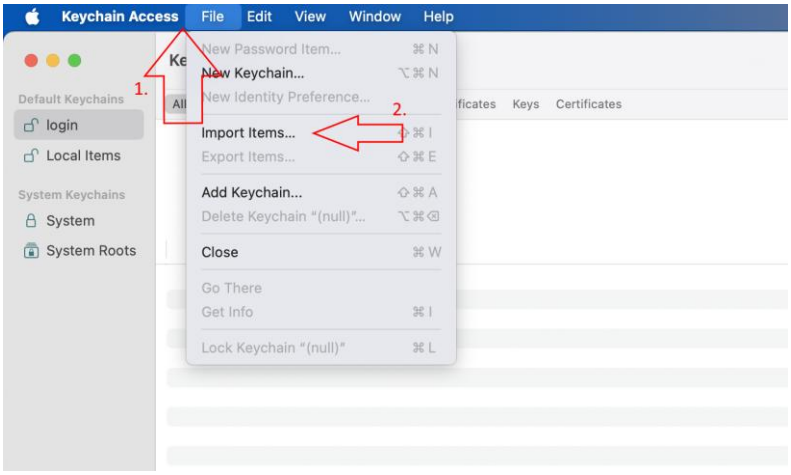
Repeat the import operations for all CCK MF certificates.

1.4 Configuration in macOS

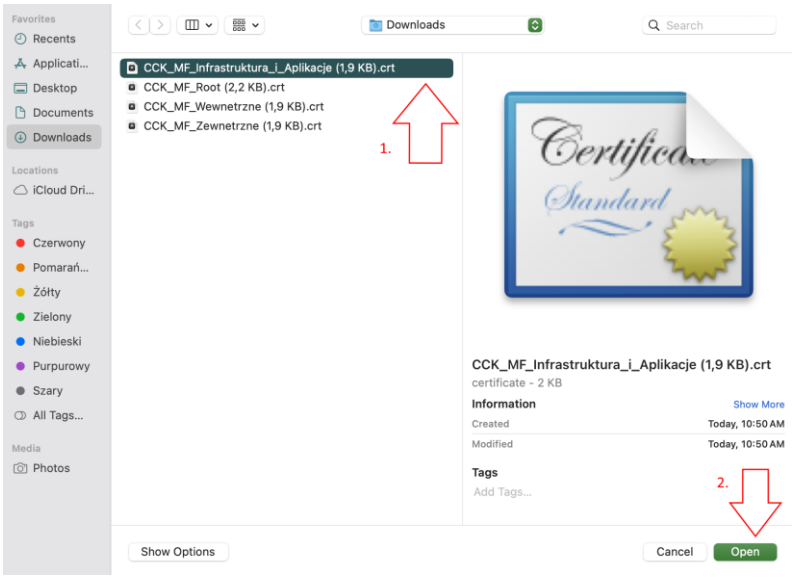
Import the certificates of the Ministry of Finance Certification Centre to the *Keychain Access.*



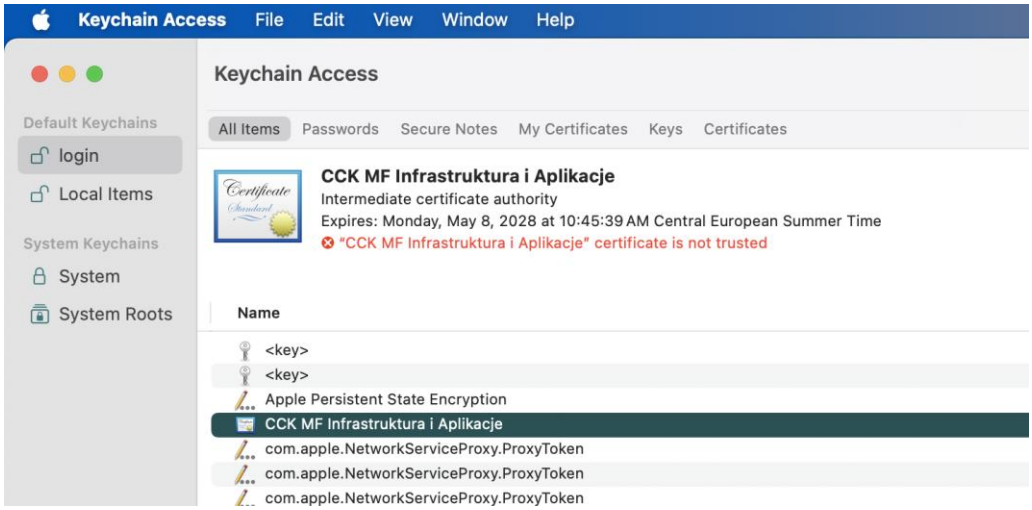
Select *File>Import items …* in the *Keychain access*



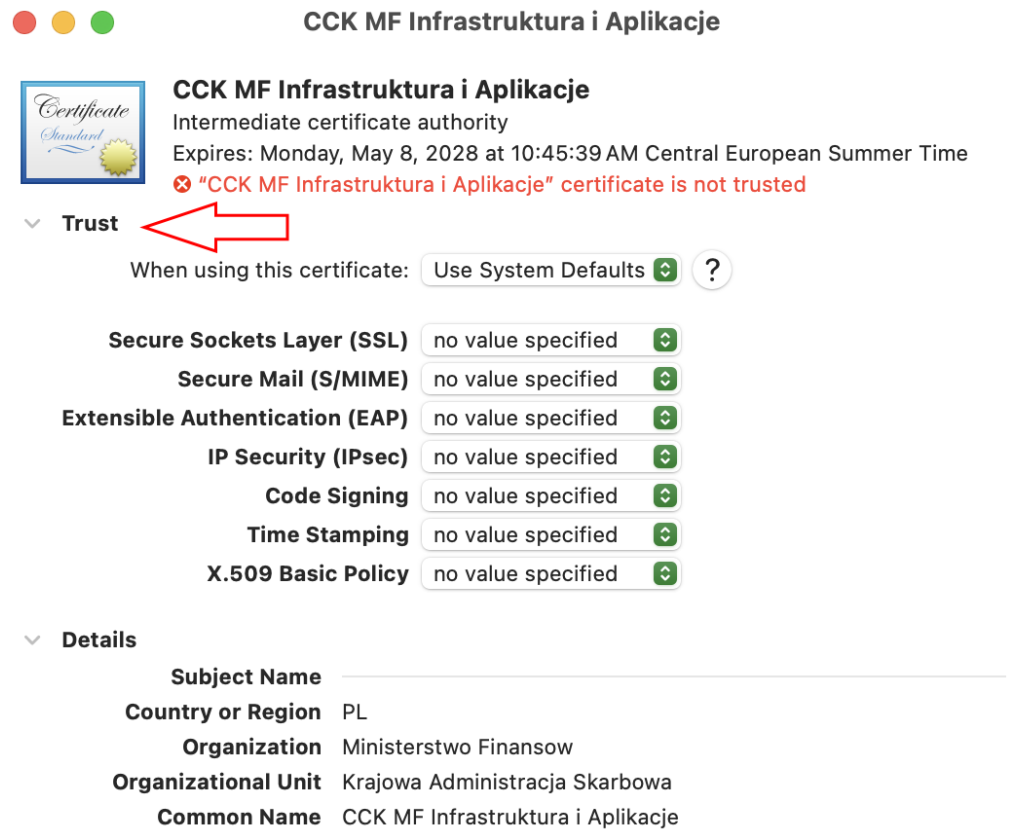
A window enabling identification of the location of the certification center's certificate files will display.



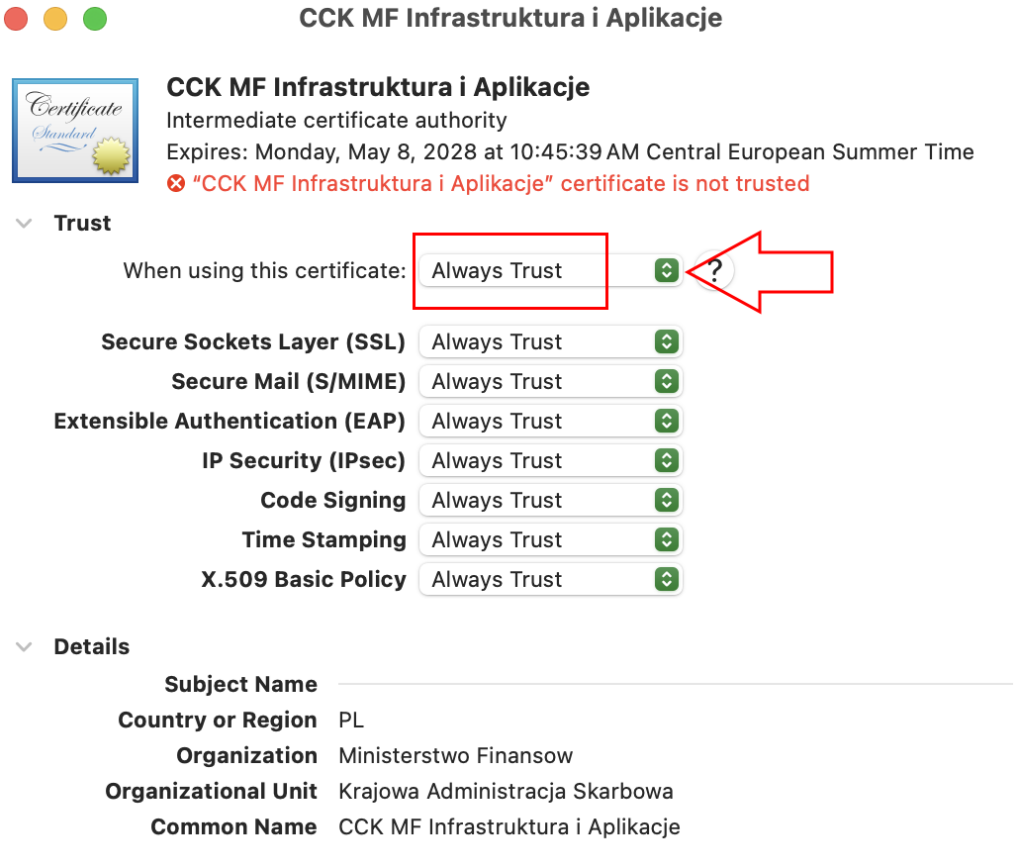
Tick the certificate file (1) and click *Open* (2). The certificate will be imported and obtain the "untrusted" status.



Click the certificate and unfold the *Trust* options.



In the *Trust* options, set *Always trust* in the *When using this certificate* field and save the settings.



Repeat these operations for all CCK MF certificates.

2. Installation of the CertSign application

2.1 Downloading and running the installer

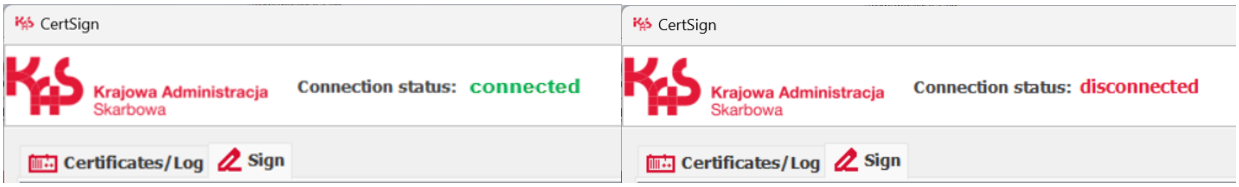
The installation files of the CertSign application are available on the PUESC portal in the *Electronic signing of documents* at section Download the CertSign program and sign documents with a customs signature https://puesc.gov.pl/uslugi/elektroniczne-podpisywanie-dokumentow
There are several program versions made available. Choose the version compatible with the current operating system of the computer. After downloading, run the application installer.

In the Microsoft Windows systems, the application installs in the user profile, without the need to level up the rights to the local administrator type.

The applications are intended for use neither in the server versions of the operating systems, nor for terminal operation.

2.2 Connection status

The application displays two possible website connection statuses:



Directly after starting, the application displays the *Connection status:* disconnected, which is correct.

The *Connection status:* **connected** message informs that the PUESC website correctly established the connection with the CertSign application. The **connected** status is required when generating a certificate and signing a document on PUESC. When signing a file from a computer hard drive, no connection with the PUESC website is required. In such case, the **disconnected** status is not a sign of improper operation.

After manual starting, the application will display the **disconnected** status, until the operation of signing a document or generating a customs certificate is run on the PUESC website.

If there is no connection at the time of generating a certificate or signing a document on PUESC (*Connection status:* **disconnected**), a computer and browser should be configured as set out in chapter 1. The **disconnected** mode enables signing the files stored on the computer hard drive (offline), provided that the user holds the certificate.

In the Linux and Linux and Mac OS X-family systems, it is recommended to use the pre-configured Firefox.

If there are any connection problems, proceed as described in addendum A.6

2.2 Automatic installation of the CCK MF certificates

At the first start in the Microsoft Windows systems, the application checks whether the certificates of the Ministry of Finance Certification Center are installed. If not, the application automatically suggests their installation.

After proper installation, the certificates are available for the following browsers: Internet Explorer, EDGE, Chrome (browsers using the Windows CSP) as well as Firefox configured as set out in chapter 1.3.

3. About the CertSign application

The CertSign application executes two functions:

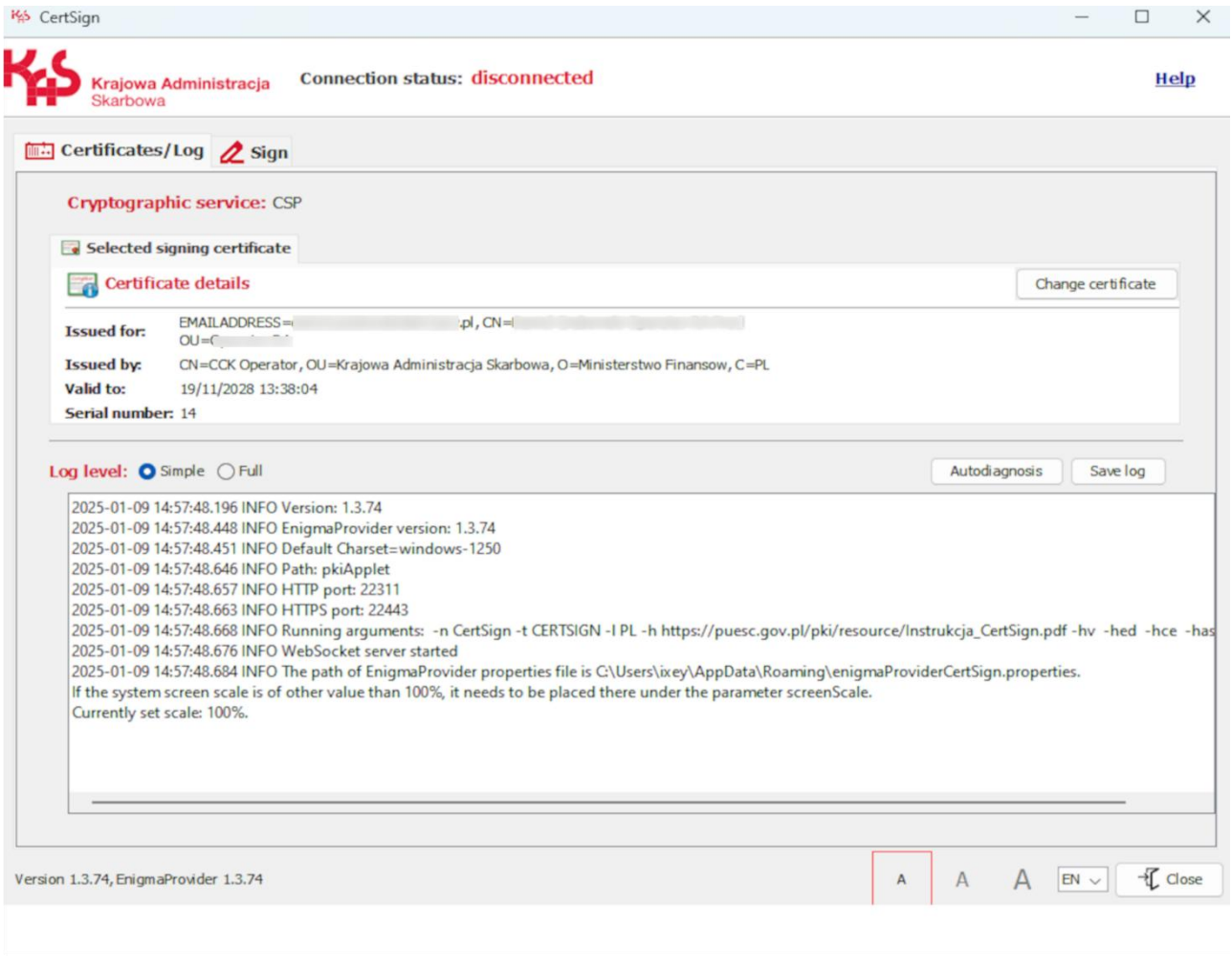
1. generating the certificates and operating the cryptographic keys,
2. signing a document with an electronic signature in the *online* and *offline* mode.

The application cooperates with the following browsers: Chrome, Firefox, Internet Explorer 11 and Edge.

3.1 Functions and settlings of the CertSign application

Connection status – informs whether the application established the connection with the PUESC website. The connection status has the following values: **connected** or **disconnected.** When operating in the offline mode, no connection is the proper status.

In the connected mode *(online)*, the application performs operations in the background of the website. After a potential selection of the option, the CertSign window should be minimised to the taskbar.

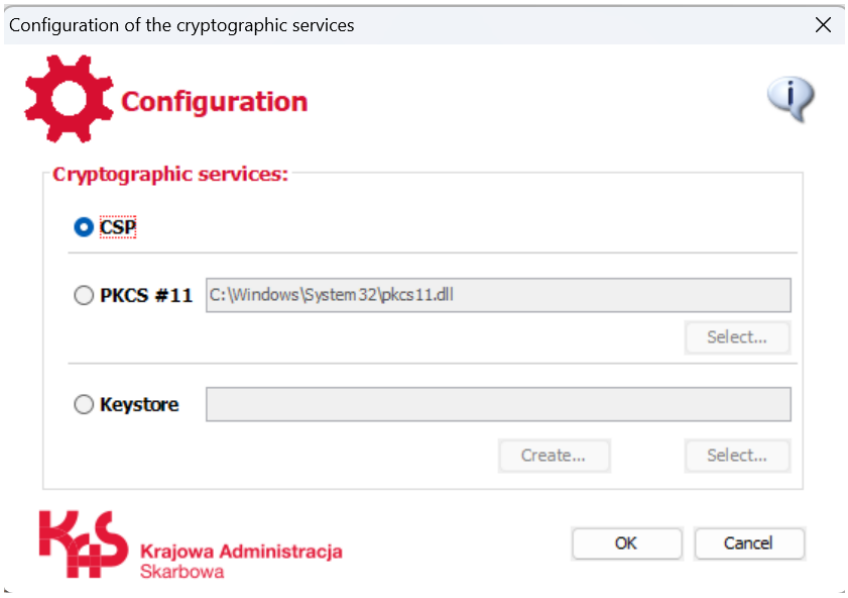


Clicking the "*Help*" button provides access to the operating instruction of the application.

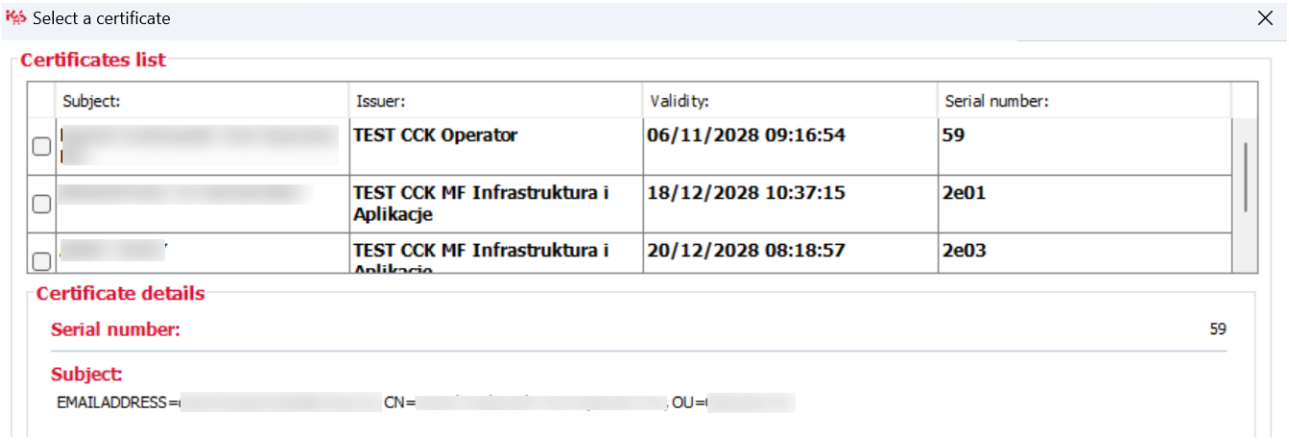
The ***"Certificates/Log"*** tab displays the current selection of the certificate used for electronic signature (the window is empty at the first start). The application log is displayed below. Setting the "*Full"* logging-in level should be used to collect information for help-desk in the event of any application problems.

The ***"Change certificate"*** option launches access to the configuration of cryptographic services, which enable selection of the key/certificate medium compliant with CSP, PKCS#11 or Java™ Keystore. Identifying the location of the driver file (*.dll library) of the PKCS#11 standard or encrypted key storage file on hard drive (Keystore) is also possible. The description of individual options is provided in addendum A.5.

The certificate used for signing a document with an electronic signature is selected using the *Change certificate* button. In the first place, the cryptographic service configuration window is displayed, where the certificate store is selected.



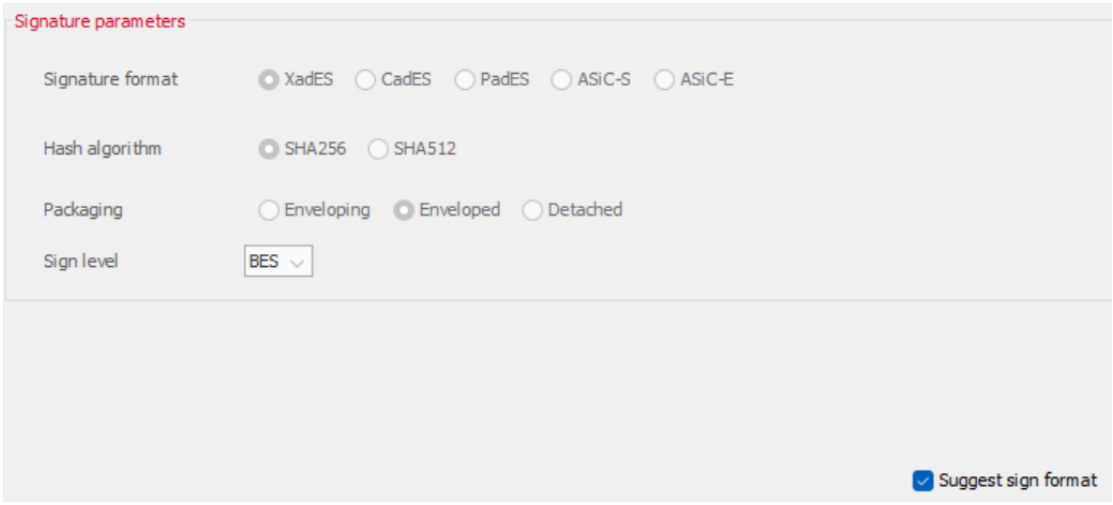
After selecting the requested service and confirming it by *OK* button, the certificate selection window from the selected certificate store will be displayed.



The certificate is selected from the list by ticking a certificate (to be highlighted in a colour) and clicking the *OK* button.

The **"*Sign*"** tab provides access to the functions used for local signing the file downloaded from a computer hard drive with an electronic signature. The signature requires neither PUESC running nor establishing a connection. The details are provided in chapter 5.

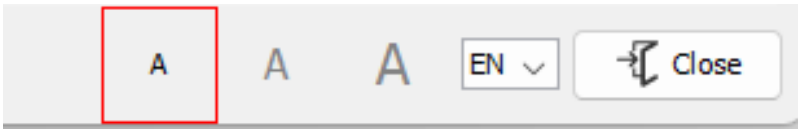
Selecting the ***"Suggest sign format"*** results in automatic selection of the format and type of signature on the basis of the type of file selected for signing. This option is enabled by default. Its opting out results in unblocking the manual settings of the signature parameters.



The applications enables **screen font scaling** to three sizes:

- standard
- larger
- the largest

In order to change a font size, select one of the scaling buttons (A A A), which is not currently selected. Each subsequent size is larger by 1.5 times from the previous one. This means that increasing the *standard* size to the *larger* size increases the current font size by 150%, while to the *largest* size – by 225%. Analogically, decreasing to the *larger* size decreases the level from 225% of the *standard* size to 150%, while returning to the *standard* size decreases the current size to the default value (100%).Scaling may be disabled on the displays with lower resolutions – the application verifies this parameter to protect against excessive zooming of elements.



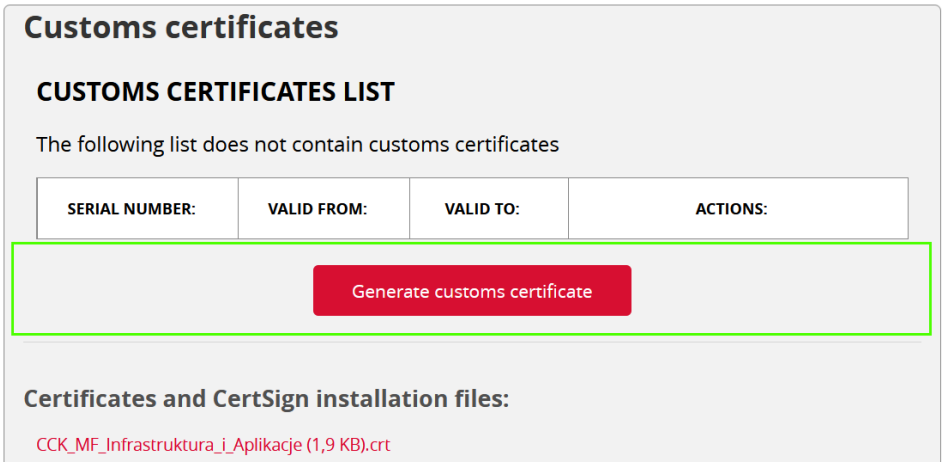
Change of a language version to English is made by clicking the PL field.
The “Close” button ends operation of the application.

The application has the ***“Autodiagnosis”*** function, which enables checking the application readiness to sign a document. The application checks availability of the network ports and performs a signing test using the certificate selected in the *“Certificates/Log”* tab. The application will request a password protecting the private key. If the user holds no certificate, the test will fail. The auto-diagnosis saves information on the course of test in the application log and displays the report window – Auto-diagnosis result.

4. Generating a certificate

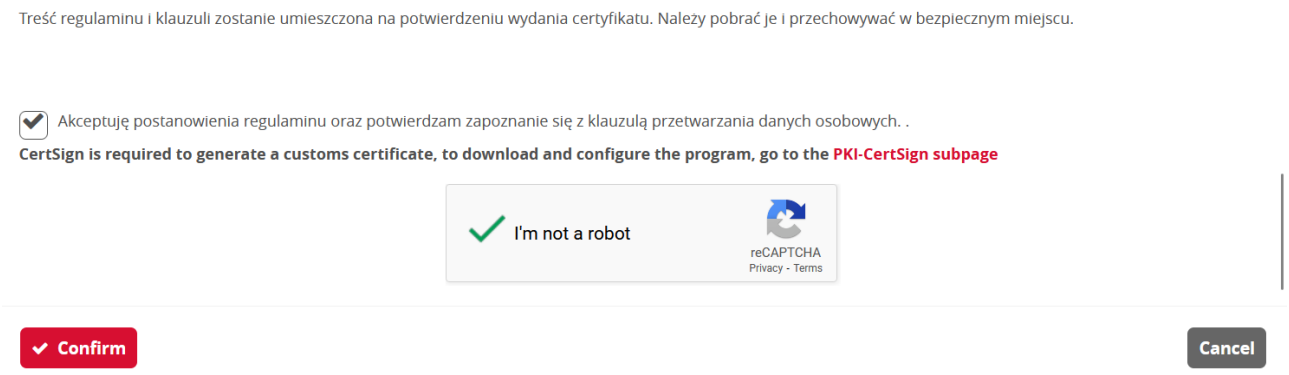
A customs certificate may be obtained only by a person holding an active IdSISC and registered in so called full procedure. A non-registered PUESC user should, in the first place, register by filling the *Application for registration of a natural person in SISC*.

PUESC provides the functionality of generating a customs certificate. The system has a dedicated view for managing and generating the customs certificate, accessible from My Desktop -> My data ->List of custom certificates. In order to generate a new certificate, select the “Generate a customs certificate” option.

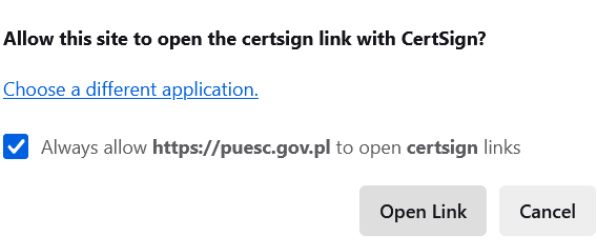


NOTE: In order to generate cryptographic keys, you should download and install the CertSign application before selecting the *Generate a customs certificate.* If the application is not installed properly, generating the keys will be impossible.

After selecting the *Generate a customs certificate,* the system will display a message with the terms of service. Before going to the next step, tick the statements below the terms, and perform captcha verification. At the end, confirm the action by clicking the ***“Confirm”*** button.

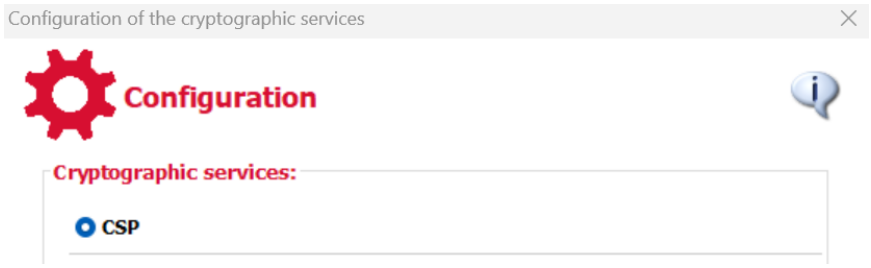


Note: after selecting *Confirm,* a message asking if to open the CertSign application may appear. If the application was not started, confirm, allowing the browser to open the program.

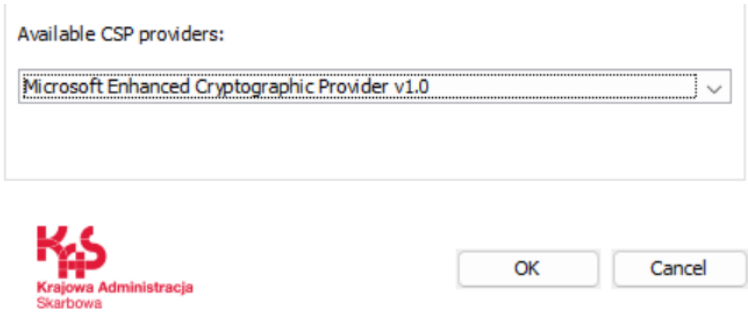


4.1. Generating a certificate to the Windows system store (CSP)

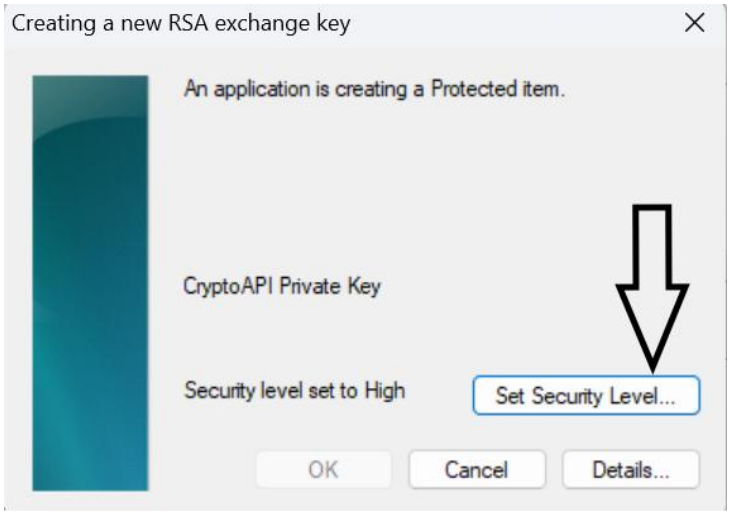
After running the application in the generating a certificate mode, the cryptographic service configuration window will display. Select the "*CSP"* option and confirm the selection by clicking the "*OK*" button.



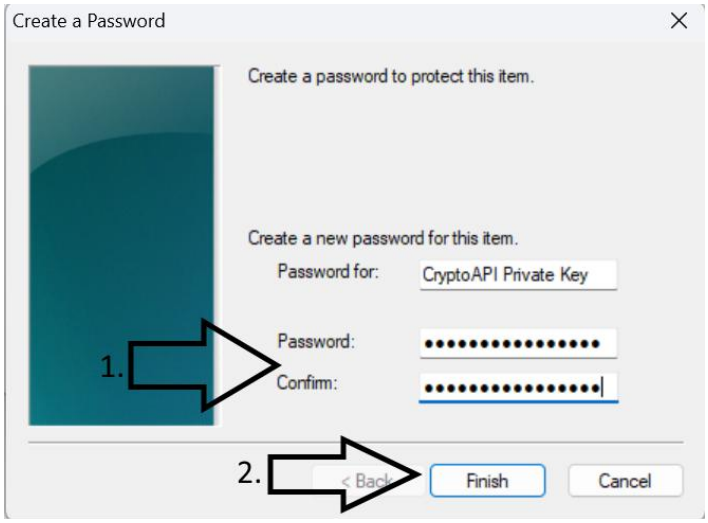
If the application for generating the certificates has never been run, the CSP option is selected by default In the next stage, select the provider of the CSP service used to generate a certificate.



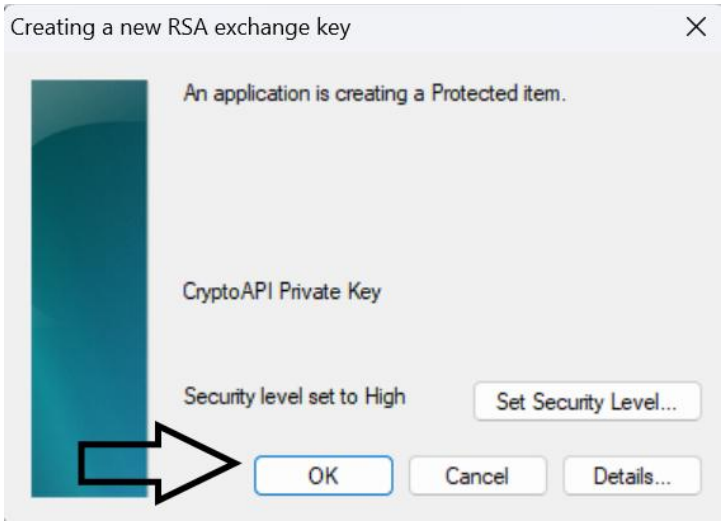
When generating the keys to the **Windows system store,** select ***Microsoft Enhanced Cryptographic Provider***… from the drop-down list and confirm by clicking *"OK"*.
The generated key security window will display. Select the *Set Security Level …* option.



Set up the password composed of at least 12 characters (uppercase and lowercase letters, digits and special characters) and then confirm by clicking the *Finish* button.



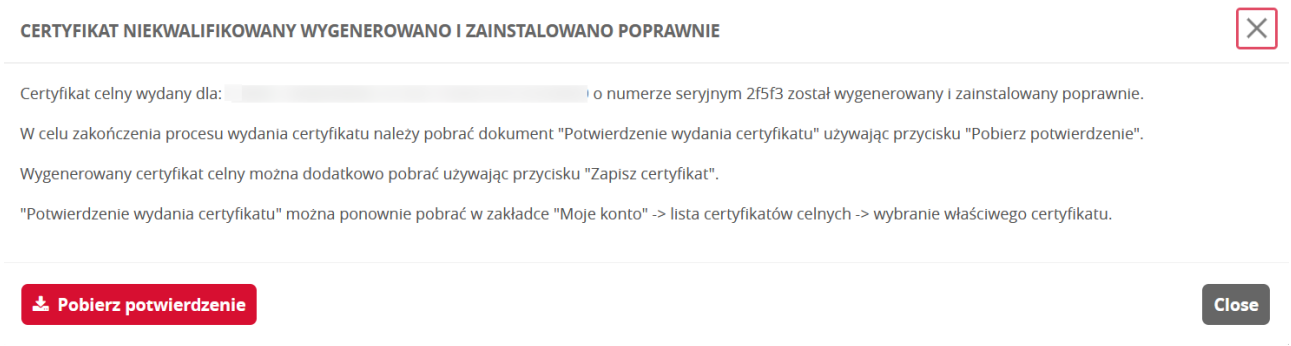
The password is confidential and necessary to use the certificate. Secure it in a manner preventing access of any third persons. **The password cannot be recovered from PUESC –** it is generated and stored locally. In the next window, confirm the selection of setting a high level of security by clicking the *OK* button.



The next step is generating the cryptographic keys and certificate. This process is non-visual and may take several minutes. Upon completion, the certificate is automatically installed in the user's computer. The certificate generated in such manner is exportable, which means that it can be transferred onto another computer.

As the certificate is generated, its data will be displayed in the *Certificate details…* window of the CertSign application.

In the next step, a document confirming the certificate issue should be downloaded from the PUESC website. The document is downloaded by selecting the ***Download confirmation*** *(Pobierz potwierdzenie)* option.



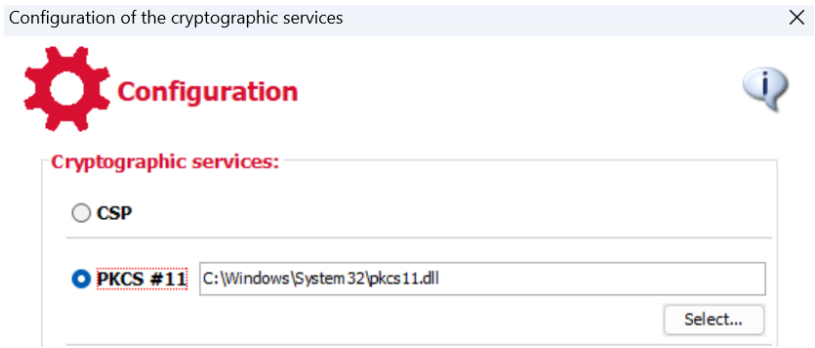
We recommend printing and storing the document confirming the certificate issue in a secured place, since it contains the code enabling the suspension or revocation of the certificate via help-desk.

The document confirming the certificate issue and a public part of the certificate (without a private key) can be re-downloaded as described in chapter 7.

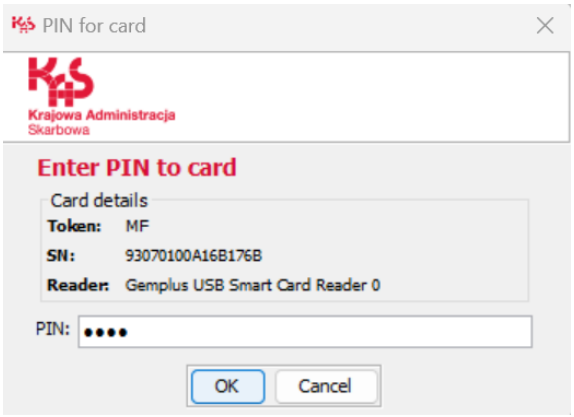
4.2. Generating a certificate using PKCS#11

This option is used for the certificates saved on cryptographic cards, regardless of the user's operating system. This is the safest method of storing the cryptographic keys and of the certificate. When using this method, the user must hold the cryptographic card driver compliant with the PKSC#11 standard, provided by its manufacturer. The keys are generated directly on the cryptographic card, which enables their safe use by the user on many computer devices.

We do not recommend generating the non-qualified certificates on cryptographic cards containing the qualified certificates due to the risk of their accidental deletion.



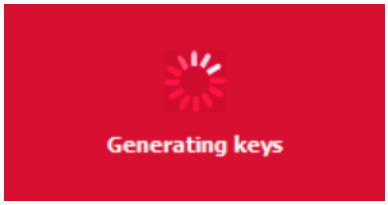
When generating a certificate, an access path to the PKCS#11 driver should be selected. After selecting the PKCS#11 driver file, click OK.



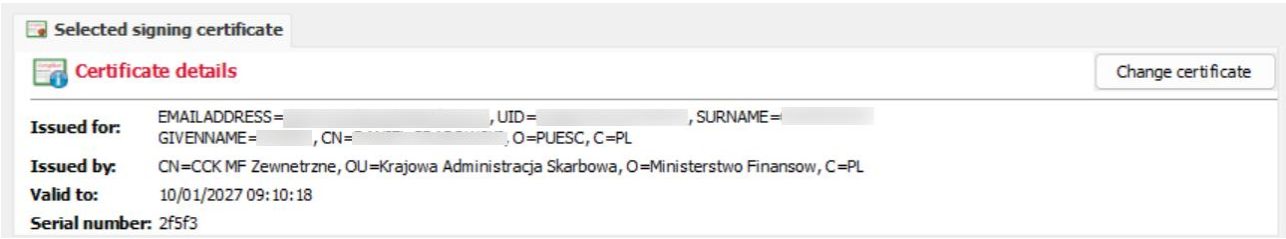
Then, enter the PIN code to the cryptographic card and confirm again by clicking *OK.*

PIN is confidential. It should be secured in a manner preventing access of any third persons.

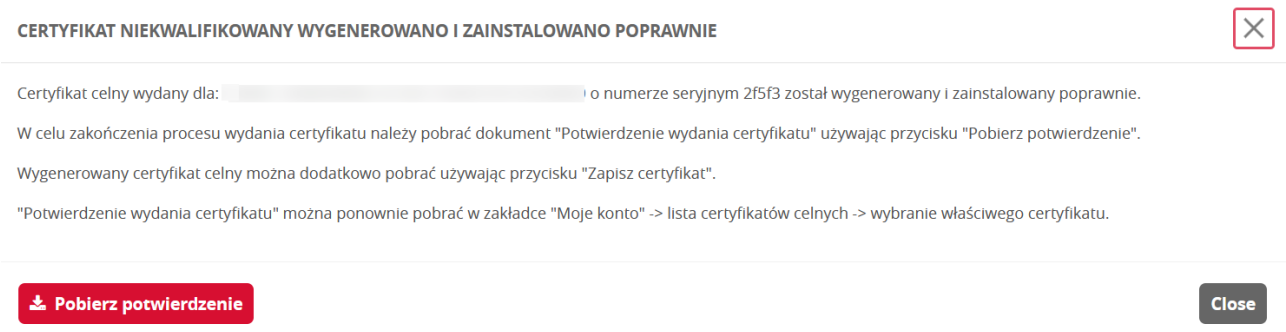
The certificate will be generated and saved on the card. When saving the certificate on the card, re-entering of the PIN code to the card will be necessary. This process is non-visual and may take several minutes. When generating the keys, the message is displayed:



As the certificate is generated, its data will be displayed in the *Certificate details…* window of the CertSign application.



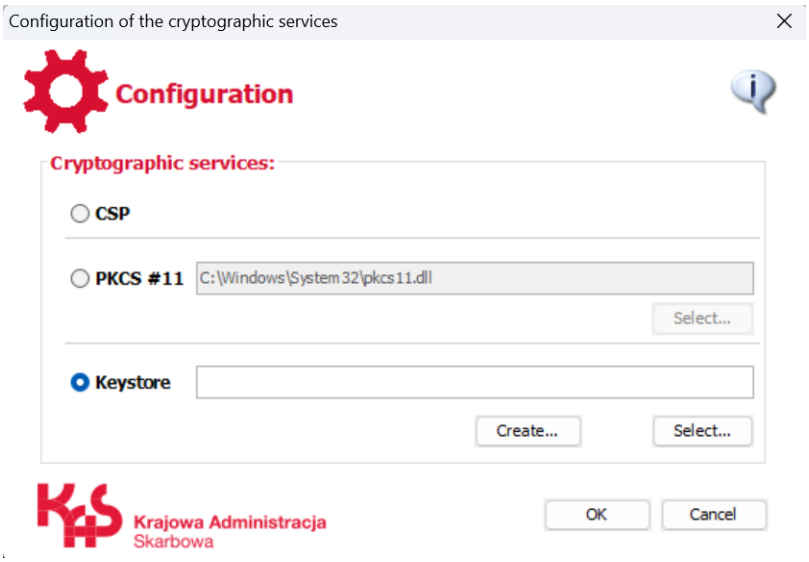
In the next step, a document confirming the certificate issue should be downloaded. The document is downloaded by selecting the *Download confirmation (Pobierz potwierdzenie)* option.



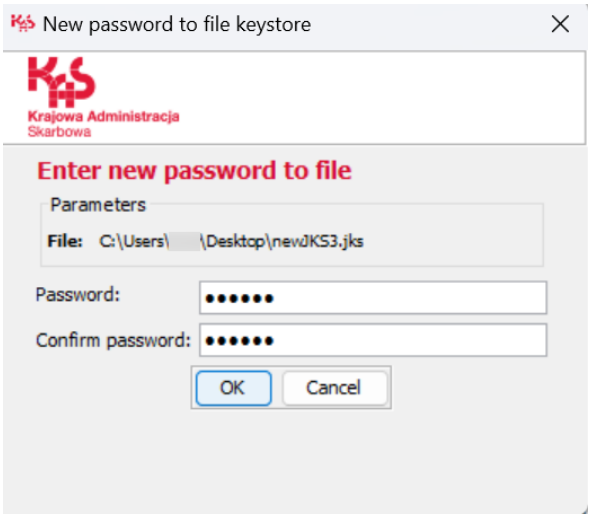
We recommend printing and storing the document confirming the certificate issue in a secured place, since it contains the code enabling the suspension or revocation of the certificate via help-desk.
The document confirming the certificate issue and a public part of the certificate (without a private key) can be re-downloaded as described in chapter 7.

4.3. Generating a certificate using Keystore

Selecting this option enables storage of keys and certificates in the encrypted file on a computer and their simple transfer between the computer devices. **One should remember however that the certificates generated in this way may be invisible for the other Windows system applications. At the same time, this is the least safe method of key storing.** This option can be used among others in the Mac OS X and Linux family operating systems.
After selecting the "*Keystore*" option, the buttons: "*Create…"* and *"Select…" will be enabled.*



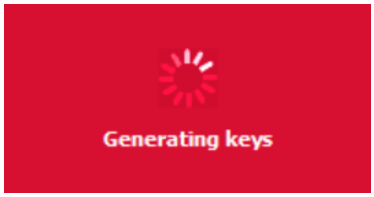
If the *Keystore* file has not been created earlier, select the *"Create…"* option (below the file path window). If the *Keystore* is already created, select it by clicking *"Select…"*.The selection should be confirmed by clicking the *OK* button. The created keys and certificates will be added to this file.
Then enter the password protecting access to the keys and certificates saved in the *Keystore* file.



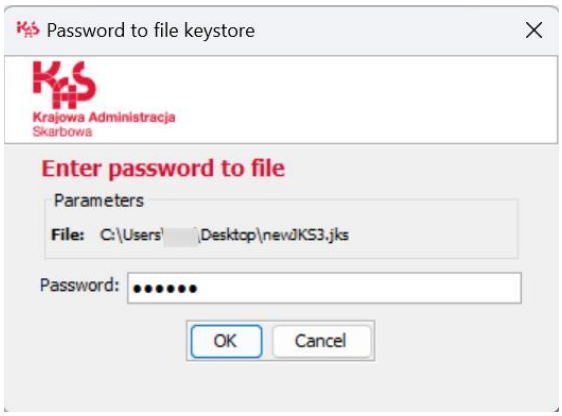
Repeat the entered password to validate it and confirm by clicking the *OK* button. If the entered passwords differ, an error message will be returned.

After correct entering of the password, the window informing that the keys are generated will display.

We recommend entering a complicated password i.e. composing of lowercase and uppercase letters, digits and special characters. Secure the password in a manner preventing access of any third persons.

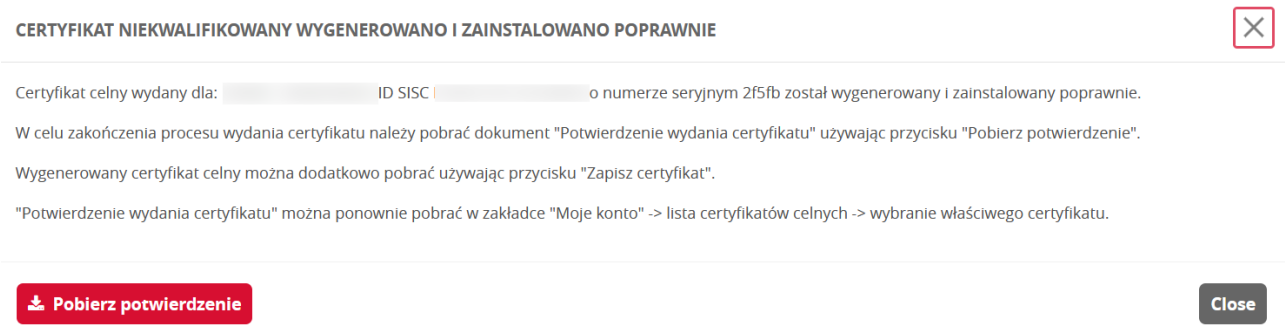


Then the certificate is generated and sent on the user's computer. This process is non-visual and may take several minutes. In order to save the generated certificate, provide the password entered at the stage of private key generation (1) and confirm it with *OK* (2).



As the certificate is generated, its data will be displayed in the "*Certificate details…"* window of the CertSign application.

In the next step, a document confirming the certificate issue should be downloaded. The document is downloaded by selecting the *Download confirmation (Pobierz potwierdzenie)* option.

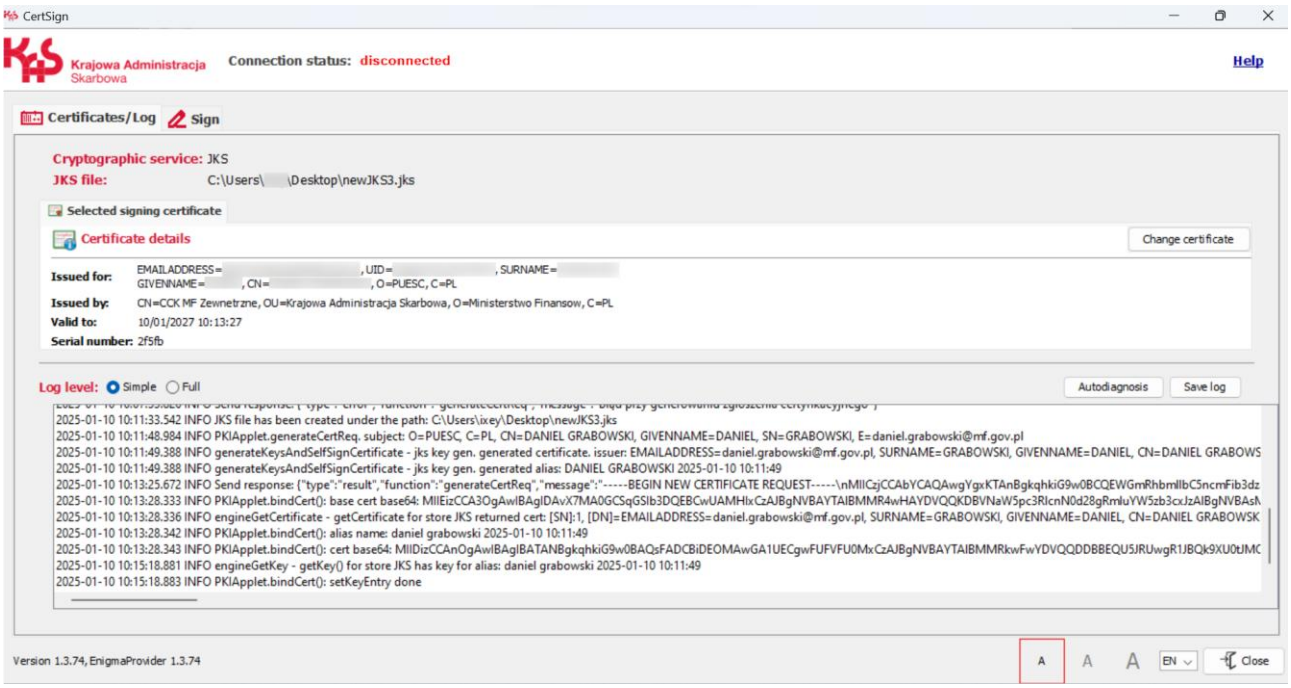


We recommend printing and storing the document confirming the certificate issue in a secured place, since it contains the code enabling the suspension or revocation of the certificate via help-desk.

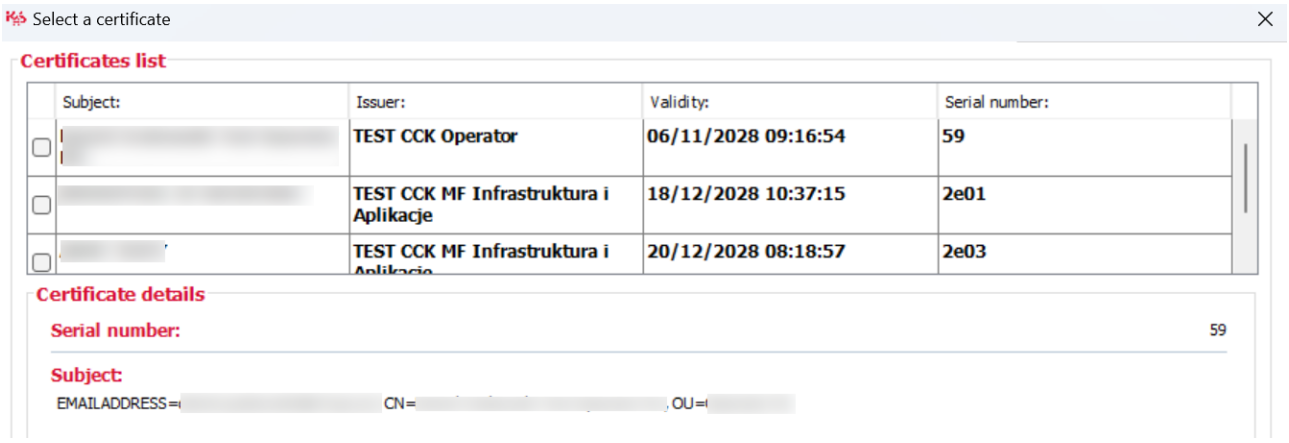
The document confirming the certificate issue and a public part of the certificate (without a private key) can be re-downloaded as described in chapter7.

5. Signing a document with an electronic signature

Signing a document with an electronic signature can be made on-line (on the PUESC website) and offline – locally by selecting the files on the computer hard drive. In both cases, the CertSign application must run, however when signing in the offline (local) mode, establishing the connection with the PUESC website is not necessary.
The *Change certificate* button in the *Certificates/Log* tab is used to select the signing certificate.



If the *Certificates/Log* tab displays no certificates, the *Change certificate* option should be selected. Then select proper certificate on the list (it will be highlighted) and confirm by clicking the *OK* button.



After selecting the certificate, its details will be displayed in the *Signature certificate details* window.
The selection window displays no expired certificates.

The certificates saved on a cryptographic card and properly installed in the operating system will display on the list only upon **placing the card in the reader.**

The qualified certificates used in the Windows system should be first registered in the system certificate store.

5.1 Signing a document with an electronic signature on PUESC

Signing a document with an electronic signature is enabled upon correct filling-in and generating the documents on the portal. Signing the documents (applications, letters) is available in the *My Desktop>To send and drafts>Documents to send* view.

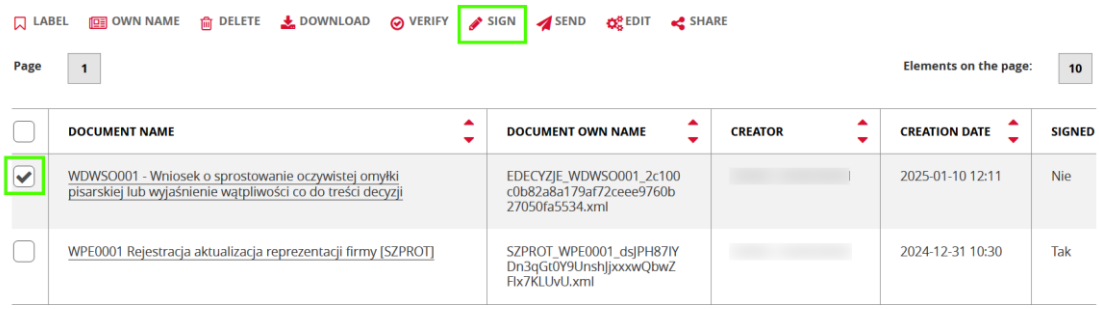
The CertSign application enables placing a signature using a qualified certificate, certificate embedded in the electronic layer of an ID card (personal signature) or a customs certificate (unqualified) – depending on the types of signatures permitted for a specific document.

When using a qualified certificate in the Windows system – install the embedded software onto the user's computer device and register the qualified certificate held by the user in the system certificate store (according to the qualified certificate documentation). Software provided by the Polish qualified centers usually installs the qualified certificate in the Windows system certificate store on an automatic basis. Analogically, **when using a personal signature (data in the electronic layer of an ID card),** first install and configure the reader and software. The description is provided in Addendum B.

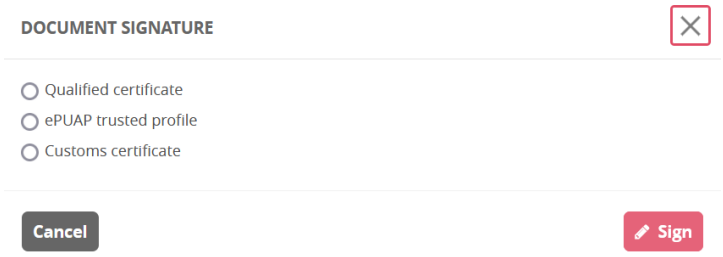
The operation of placing a signature is enabled only for the documents, which have not been signed yet. An unsigned document has the assigned *"No"* value in the *"Signed"* column, while a signed document with a *"Yes"* value.

In order to sign a document with an electronic signature on a document to send:

a) in the *To send and drafts > To send* tab, in the first column of the table, select the document to be signed using the check-box; then select the *Sign* action.

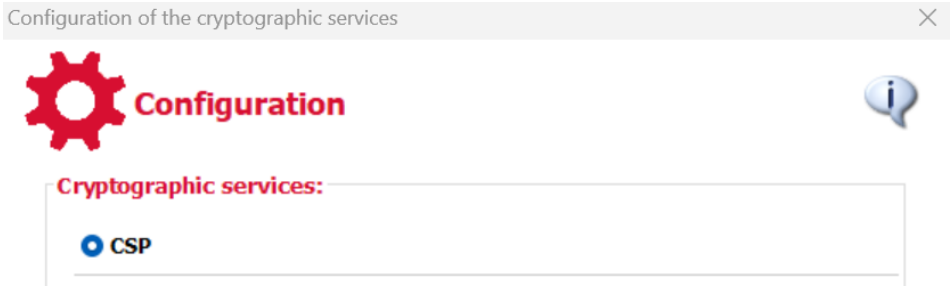


The system will display a window with the document signing method selection option. Select the proper signing method and confirm by clicking the *Sign* button.

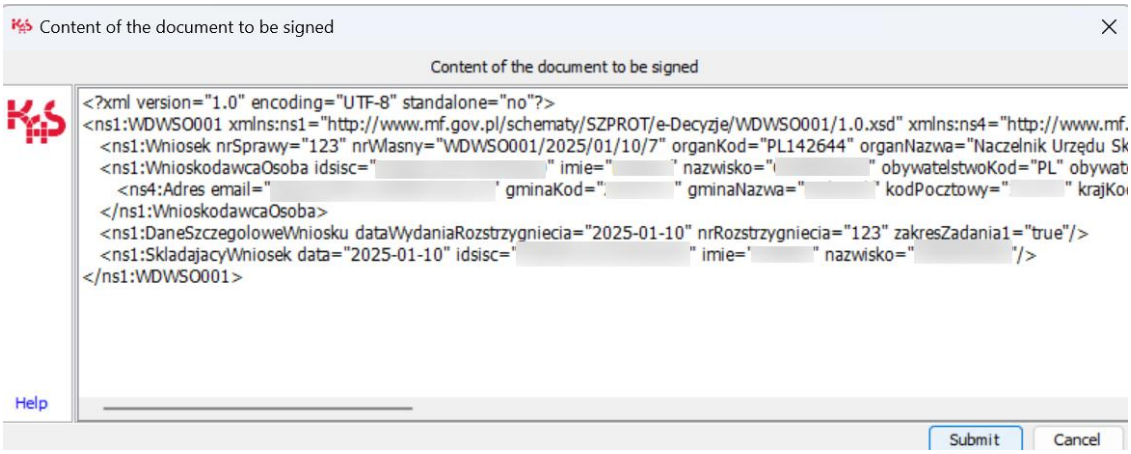


The options: ***qualified signature, customs certificate, personal signature*** will run signing in the CertSign application. ***Signature with an ePUAP trusted profile*** will redirect to the trusted profile provider service. Selecting the *Qualified signature* or *Customs certificate* or *Personal signature* will run the CertSign application and establish the connection between the PUESC website and the application. Since the connection is established for a few seconds, the connection status may change after a longer while.

5.2 Placing a signature with a certificate in the Windows store (CSP)

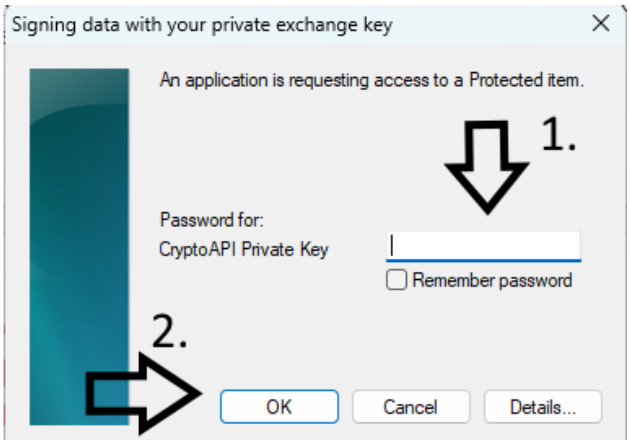


After confirming the certificate access method, the signing application will display data for signature in the form, in which they are sent to SISC.



Confirm the correctness of entered data by clicking the *Submit* button. The application will sign using the pre-selected certificate.
A dialogue window will be displayed, in which you need to enter password (PIN) protecting access to the private key. Depending on the certificate storage method and type of certificate, the following windows may display:

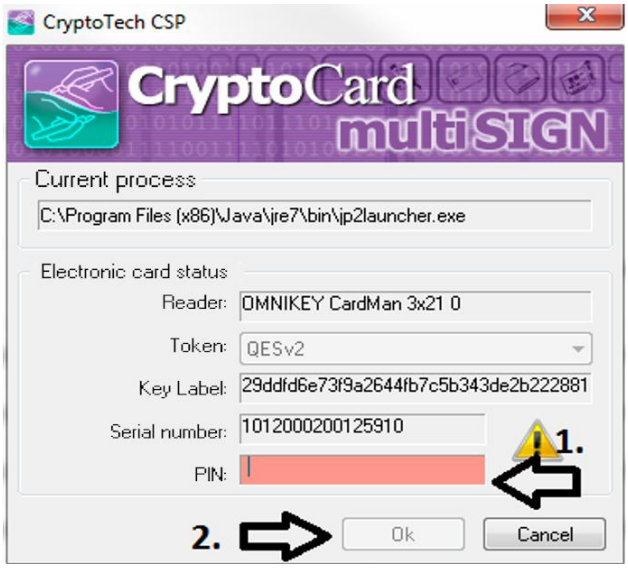
a) For a customs certificate saved in the Windows system and not recorded on a cryptographic card:



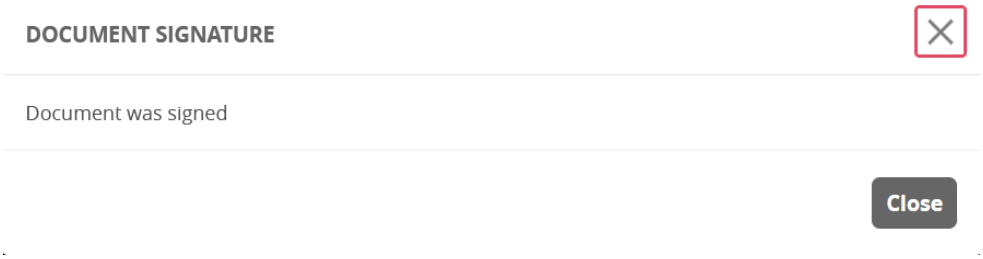
Enter access password to the certificate (1) and confirm by clicking the "*OK*" button (2).

b) For a qualified certificate saved on the cryptographic card, the dialogue window of software operating the qualified cryptographic card will be displayed. Layout of this window may differ depending on the type of card and installed operating software.

Exemplary view for a qualified certificate issued by the Polish certification center

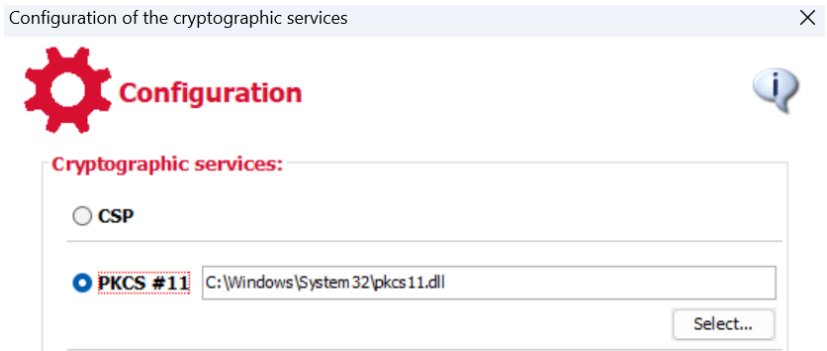


Ender card PIN (1) and confirm by clicking the "*OK*" button (2).
After sending the signed document, the PUESC portal will display the following message:

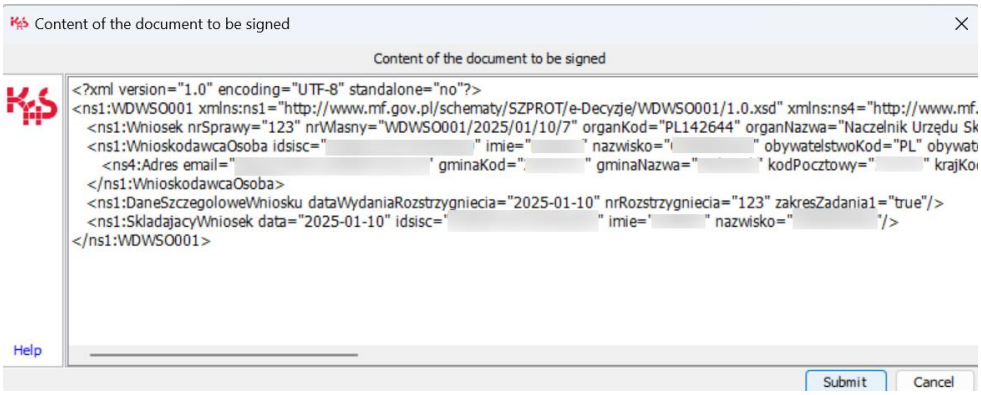


The signed document is presented in the table of documents to send with *"Yes"* status in the "*Signed"* column.

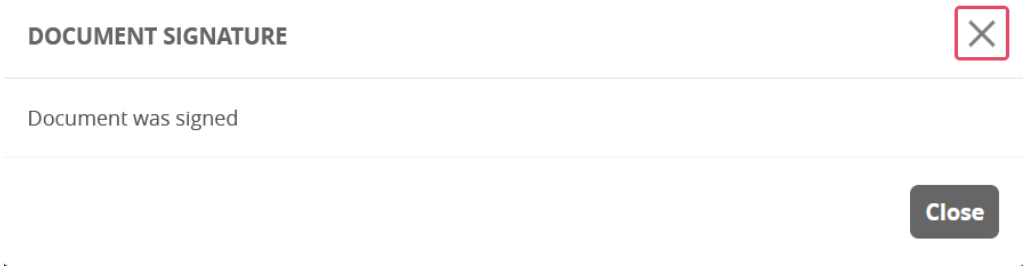
5.3 Placing a signature from a cryptographic card compliant with PKCS#11



The signing application will display data for signature in the form, in which they are sent to SISC.



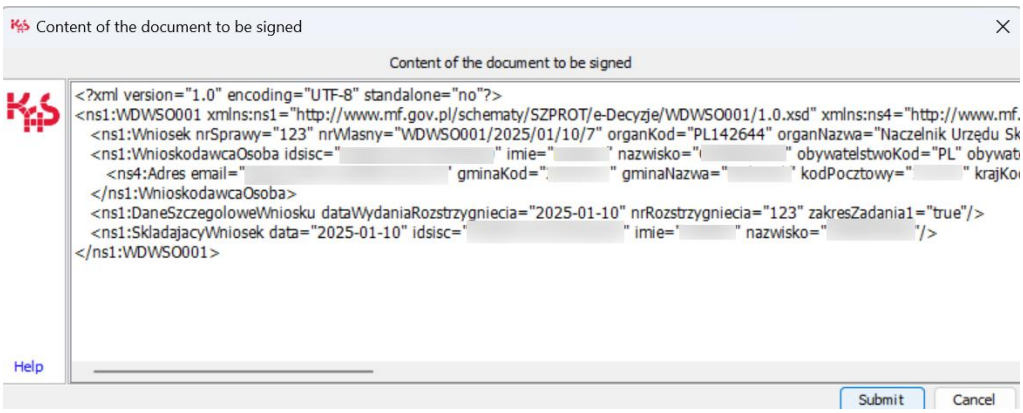
Confirm the correctness of entered data by clicking the *Confirm* button.
A dialogue window will be displayed, in which you need to enter password (PIN) protecting access to the private key. Layout of this window may differ depending on the type of card and installed operating software.
After proper sending the signed document, the PUESC portal will display the following message:



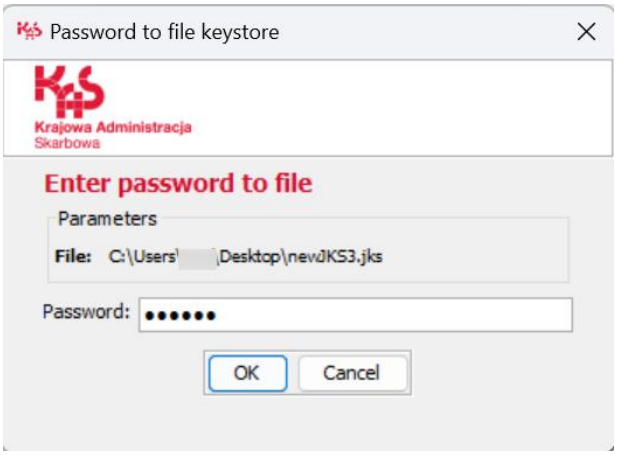
The signed document is presented in the table of documents to send with *"Yes"* status in the "*Signed"* column.

5.4 Placing a signature with a certificate (key) saved in the *Keystore* file

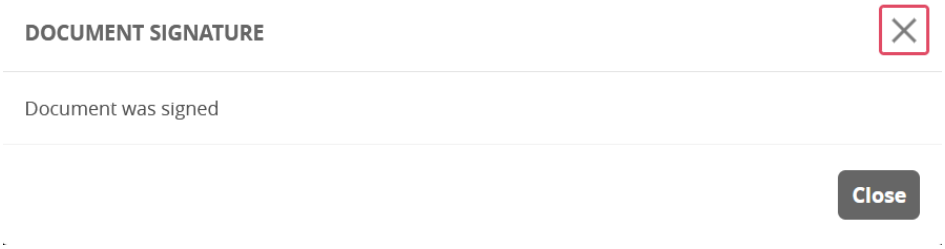
The application uses the selected *Keystore* file storing the keys and certificates. The signed document is presented in the form, in which it is sent to SISC.



Confirm the correctness of entered data by clicking the "*Confirm"* button.
A dialogue window will be displayed, in which you need to enter password (PIN) protecting access to the private key.



After proper sending the signed document, the PUESC portal will display the following message:



The signed document is presented in the table of documents to send with *"Yes"* status in the "*Signed"* column.

5.5 Signing a document with an electronic signature locally on a computer – in the offline mode

Placing a signature locally consist in the selection in the CertSign application of the location of file to be signed on the computer hard drive. This file can be pre-downloaded from PUESC. **In this case, no connection of the PUESC website with the application is necessary.**

To enable file signing, the signing certificate should be selected in the *Certificates/Log* tab.

The electronic signature functions are available in the *Signature* tab. Specify the location of the file or files to be signed and the destination folder on the computer hard drive; alternatively, select the format and type of signature and then confirm the operation by clicking the *Sign files* button.
Select in the *Signature level* menu whether the selected file is to be signed only with an electronic signature ("BES" level) or with added electronic time stamp ("T" level). When adding a time stamp, the address of time stamp server (to which the user has access) should be selected in *Settings.*
For the forms sent on PUESC, the XAdES signature format, Enveloped type should be selected in the signature parameters.
The ***Suggest signature formats*** option ensures automatic adjustment of the parameters on the basis of the type of file selected for signing. Unchecking this option enables manual setting of parameters.

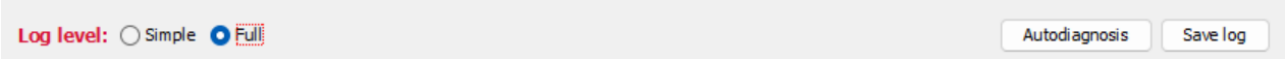
6. Problem reporting, log viewing

6.1 Data necessary to analyse the problems with operation of the application

- Operating system - type and version, system language version (for example: Windows 10 – Polish version)
- Type and version of browser
- Log from the CertSign application console
- View of screen with an error – full screen (PrtScr keyboard button)
- Detailed description of the problem, circumstances of occurrence.
- Result of auto-diagnosis of the application.

6.2 Enabling logging in the CertSign application

The CertSign application provides the option of enabling “full” logging of events from the application operation. In order to enable full logging, change the Logging level to “Full” in the application window.

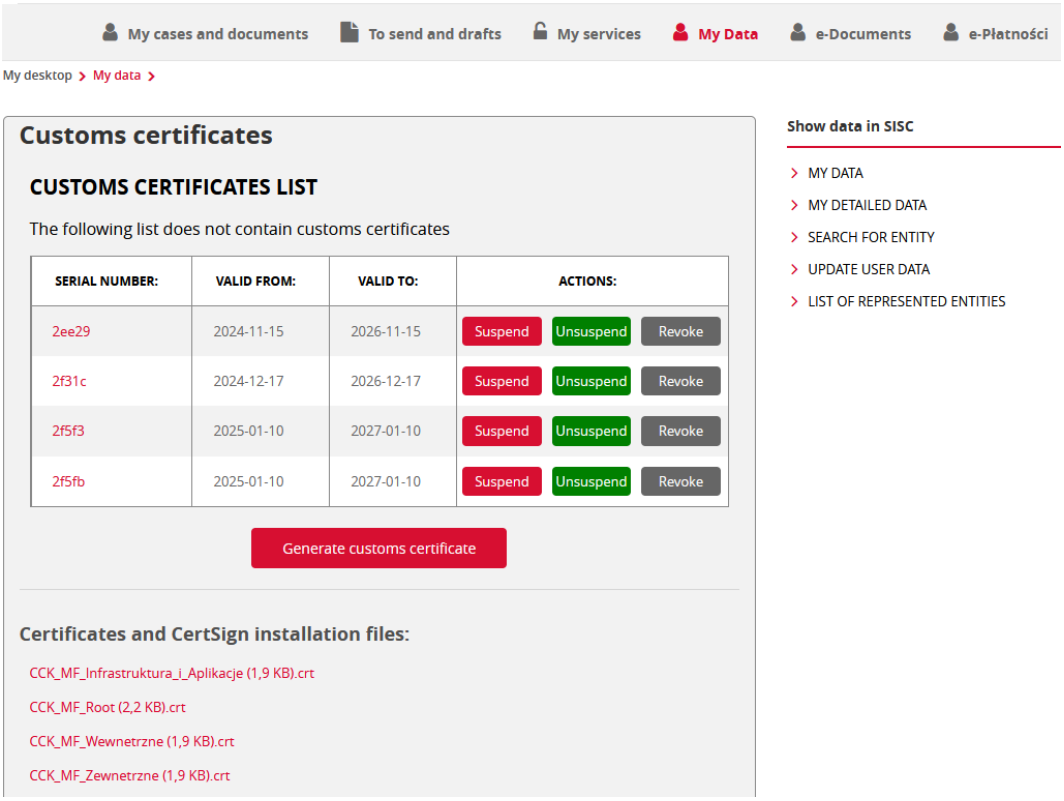


The window below will display the logs from the application operation, which can be saved by clicking the “Save log” button.
In the case of errors, the saved logs should be attached to the report in HELPDESK.

7. Downloading a certificate or confirmation document from the account on PUESC

A dedicated view of customs certificate on PUESC is available from the side menu in the My desktop>My data>List of custom certificates view. It consists in the two main areas:

1. List of customs certificates of the user – in this part of view, the user can view the list of its customs certificate. By clicking the serial number highlighted in red, the user can preview and download the certificate.
2. Additional files – this section contains the certificates to download and certificate-related documentation.



In order to download a certificate or document confirming the certificate issue, click the serial number of the certificate. A window will be displayed:

In order to download a confirmation document, click the *Download confirmation* button (1). In order to download a certificate (public part), click the *Save certificate* button (2).

NOTE! Only a public part of a certificate will be downloaded. A private part is not stored in SISC and its recovery is impossible.

8. Updating the CertSign application

The CertSign application has the embedded update checking system. If updates are available, a message with downloading suggestion will be displayed. Updates can be downloaded or resigned (cancelled). If an update is downloaded, the installer will suggest its installation. Installation can be performed immediately or later. Installation of the new version deletes no user certificate settings.

9. Appendix A

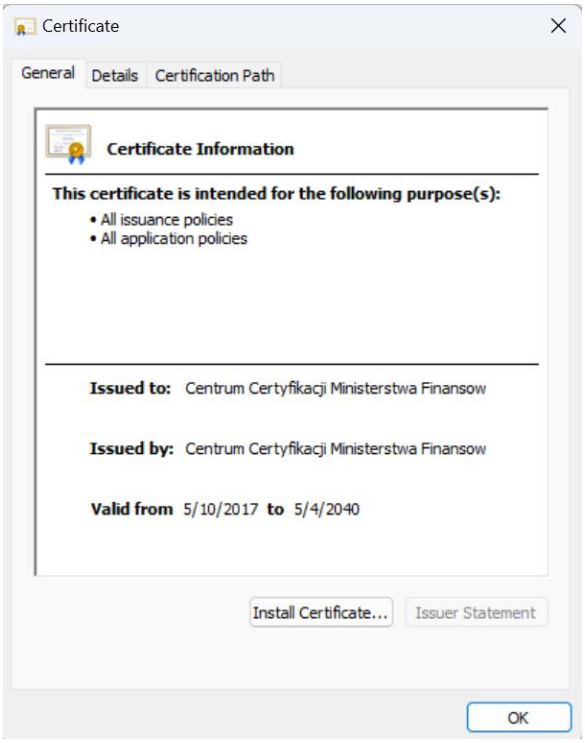
A.1 Manual installation of the certificates in the Windows system

In order to perform proper verification of the customs certificates it is necessary to install the certificates of the certification centers in the system, links to which are available at https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny

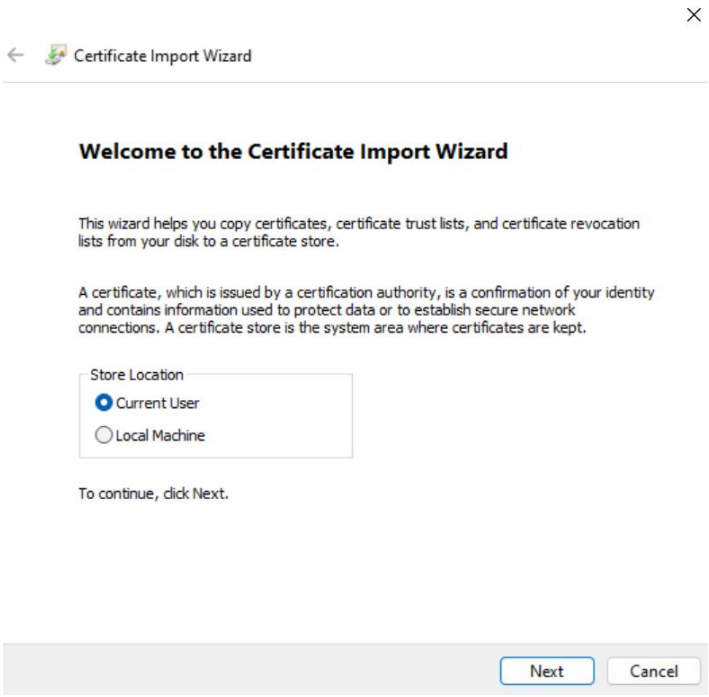
In order to install the Ministry of Finance Certification Center certificates, find and download the following certificates on a computer device:

- CCK MF Root,
- CCK MF Zewnetrzne (Internal),
- CCK MF Wewnetrzne (External),
- CCK MF Infrastruktura i Aplikacje (Infrastructure and Applications)

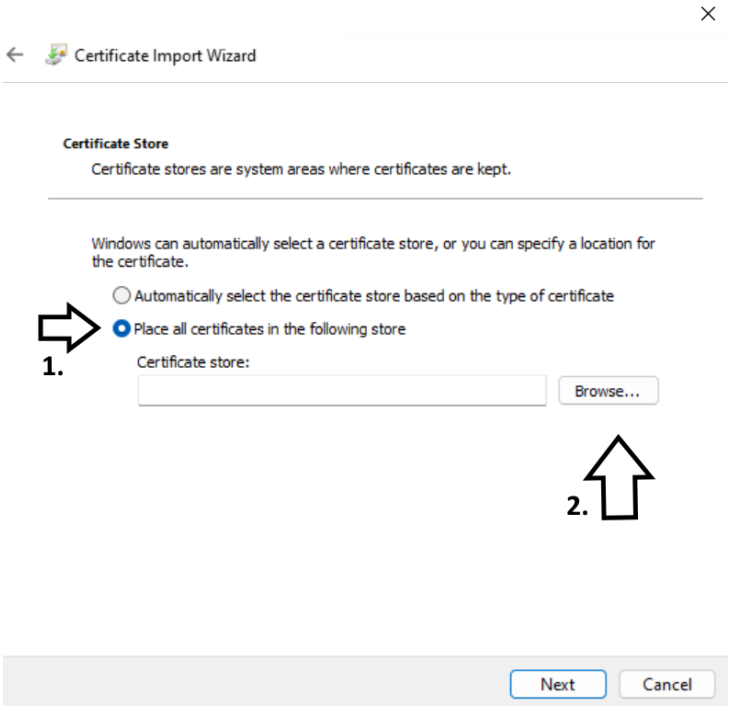
After downloading the certificate file, double-click the file – a window presenting the certificate will display. Then click the “Install certificate” button.



The “Certificate import wizard” will run.

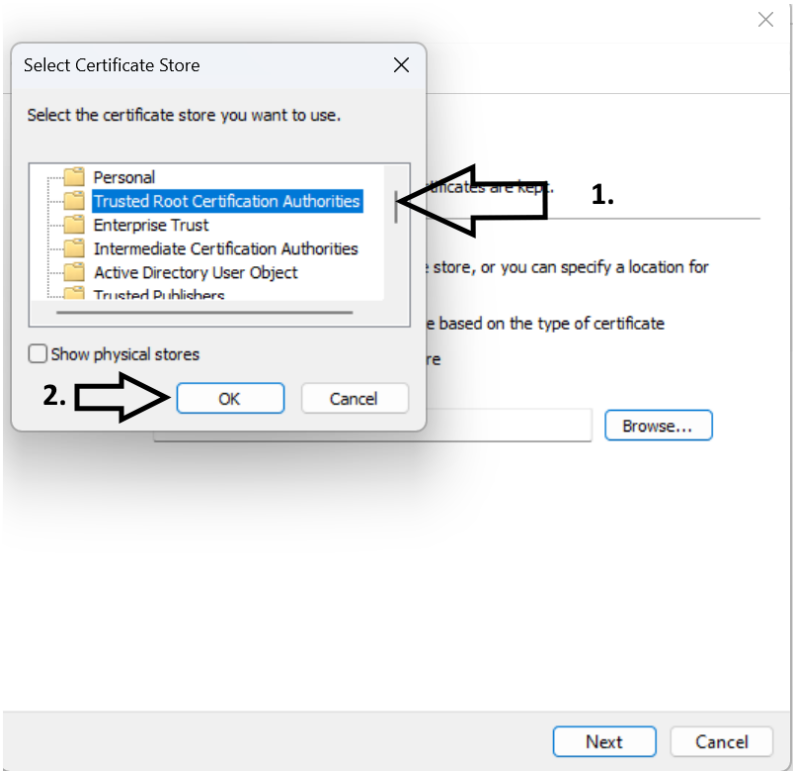


Click the *"Next"* button in the window.
In the next window, select the *"Place all certificates in the following store"(1)*option and then select *"Browse" (2).*

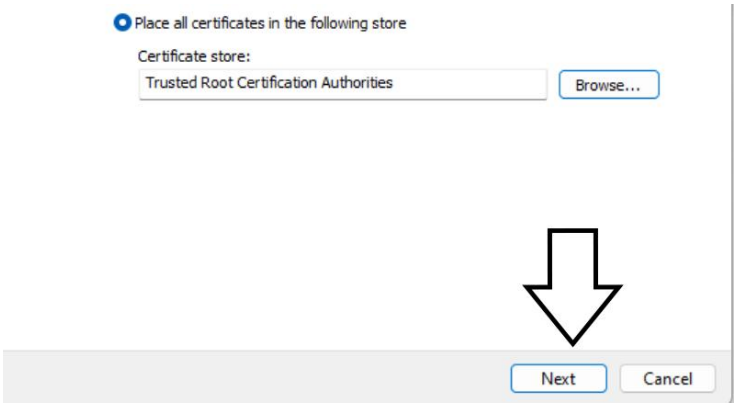


The CCK MF Root certificate should be placed in the "Trusted Root Certification Authorities" store. The CCK MF Zewnetrzne (External), CCK MF Wewnetrzne (Internal), CCK MF Infrastruktura i Aplikacje (Infrastructure and Applications) certificates should be placed in the "Intermediate Certification Authorities" store.
The screen views for the installation of the CCK MF Root certificate are presented further in the document.

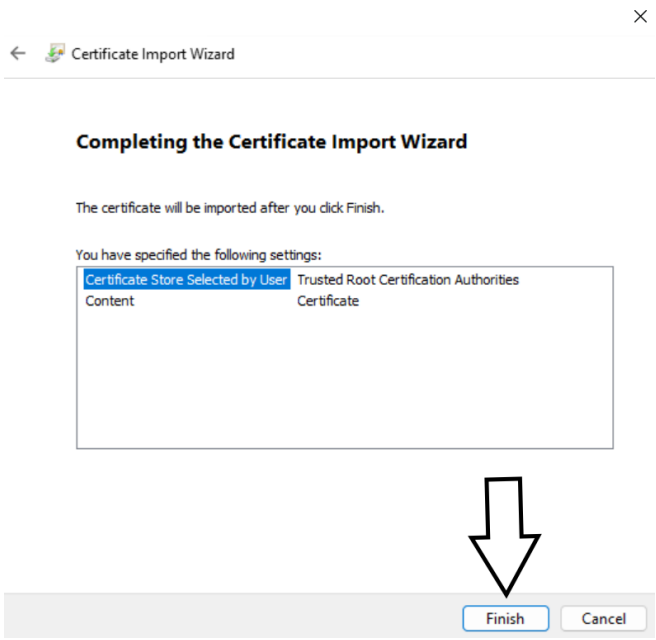
1. A certificate store selection window will display.



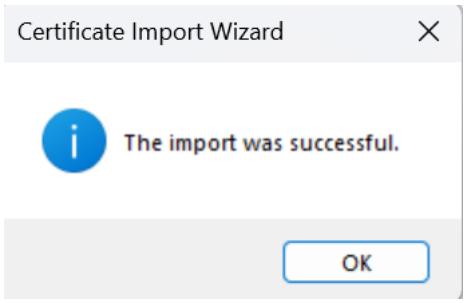
Select the *Trusted Root Certification Authorities* (1) and confirm the selection by clicking the *OK* button (2).Continue by confirming with the *Next* button.



In the *Finishing the certificate import wizard* window, select *Finish.*



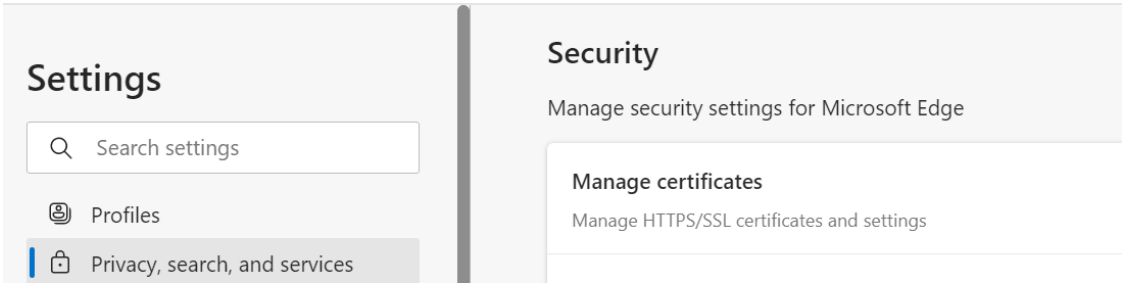
After successful finishing of a certificate import, the following message will display:



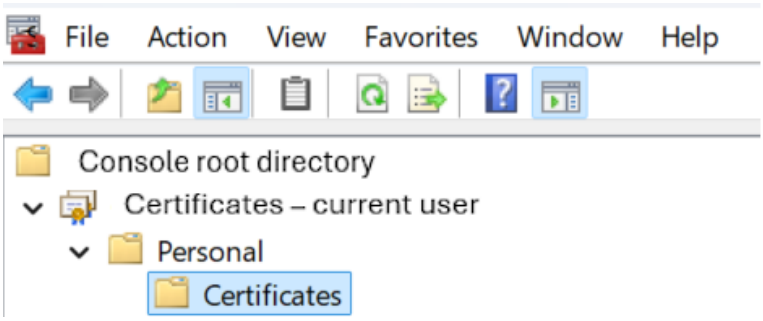
Repeat the procedure for the remaining CCK MF certificates.

A.2 Validation of the personal certificate in the Windows system

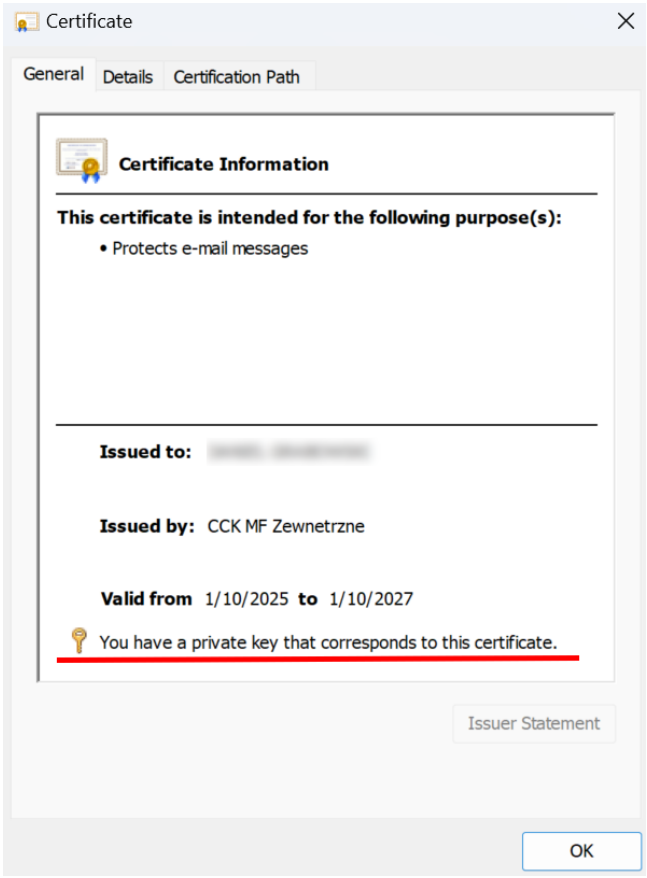
In order to validate the personal certificate installed in the Windows system, run the Internet Explorer browser and then select *Tools>Internet options* > *Content>Certificates*
The certificate store view can be also displayed from Edge browser by selecting *Settings>Privacy, search and services>Security>Manage certificates*



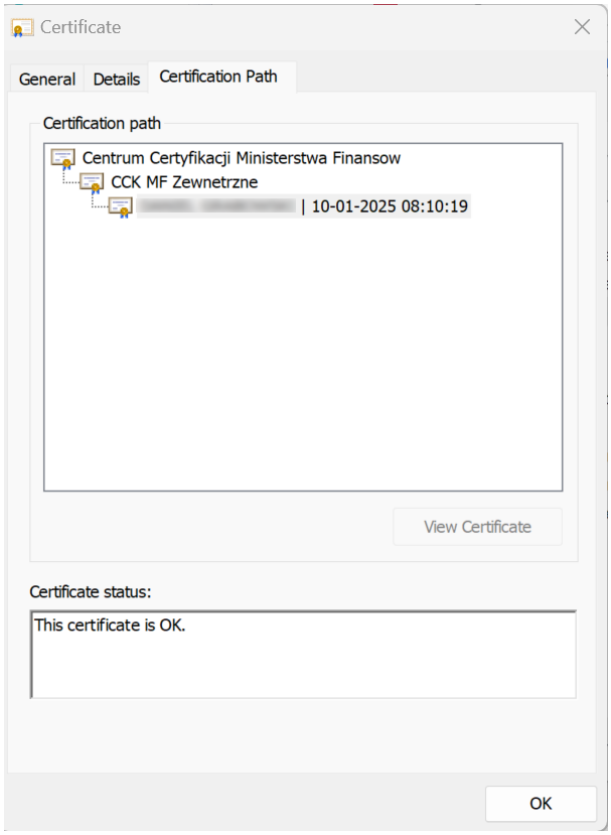
The third option (for advanced users) is running the *mmc* system console, add the *Certificates – current user* snap-in and displaying the certificate in the *Personal* branch.



In order to view the selected certificate you need to double-click it. The content view will display. In the case of a personal certificate, the message **"You have a private key that corresponds to this certificate"** should display in the first tab. You cannot sign a document with an electronic signature without a private key.



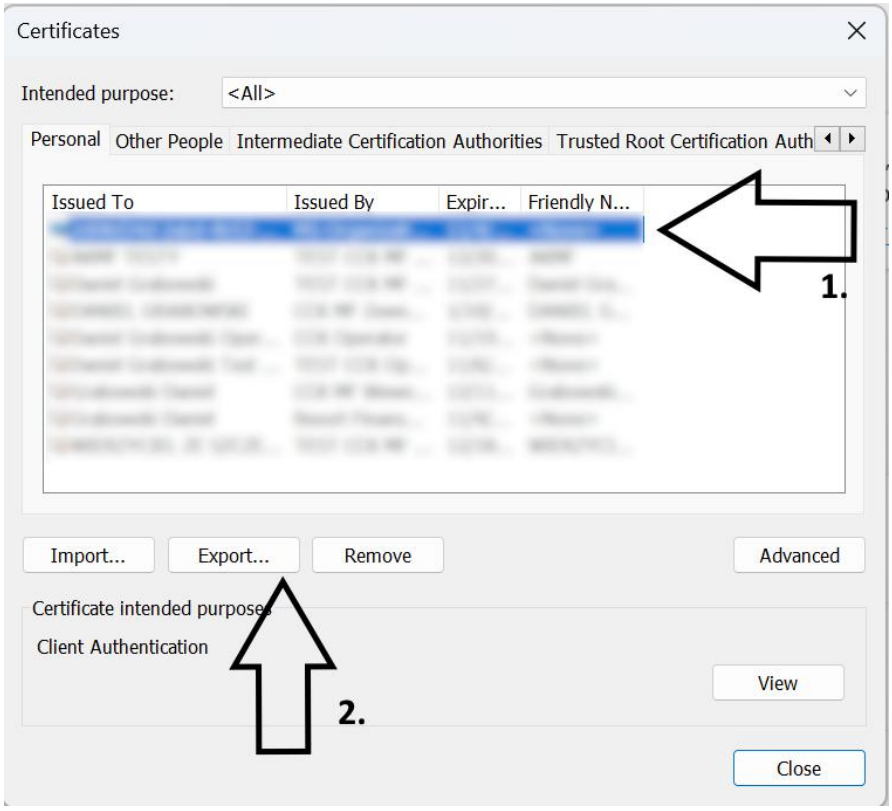
Then go to the *Certification path* tab. If the certificates are installed correctly, the certificates of the certification center and a personal certificate will be presented in the displayed window.



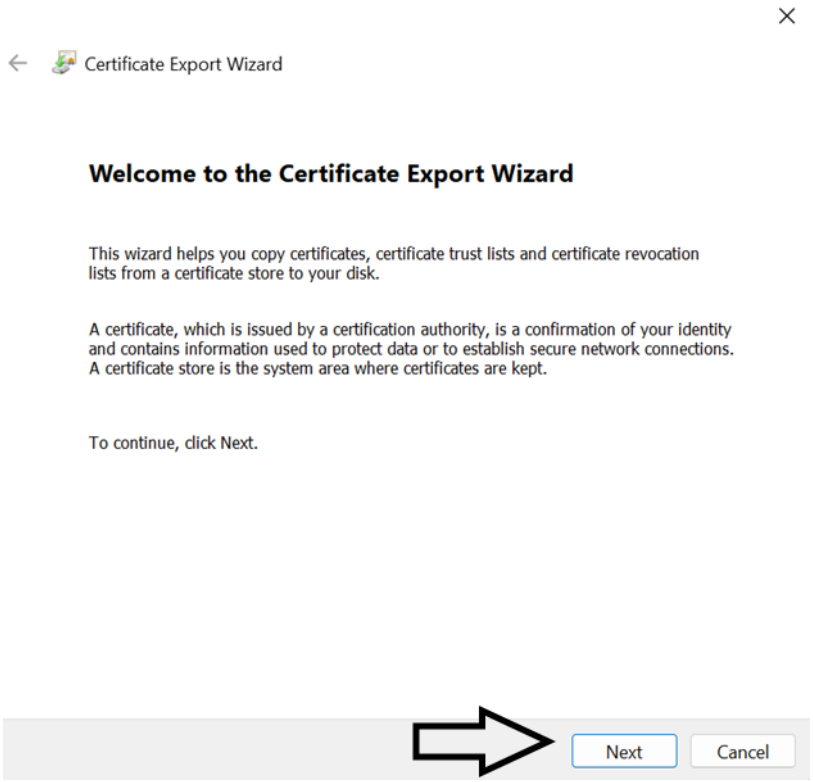
If an additional mark (“x” in a red circle) displays on the certificate icon above the personal certificate, this means that this certificate is not installed or is invalid and the certification path cannot be established successfully. In such case, download and install the missing certificate.

A.3 Export of a certificate from the Windows system certificate store

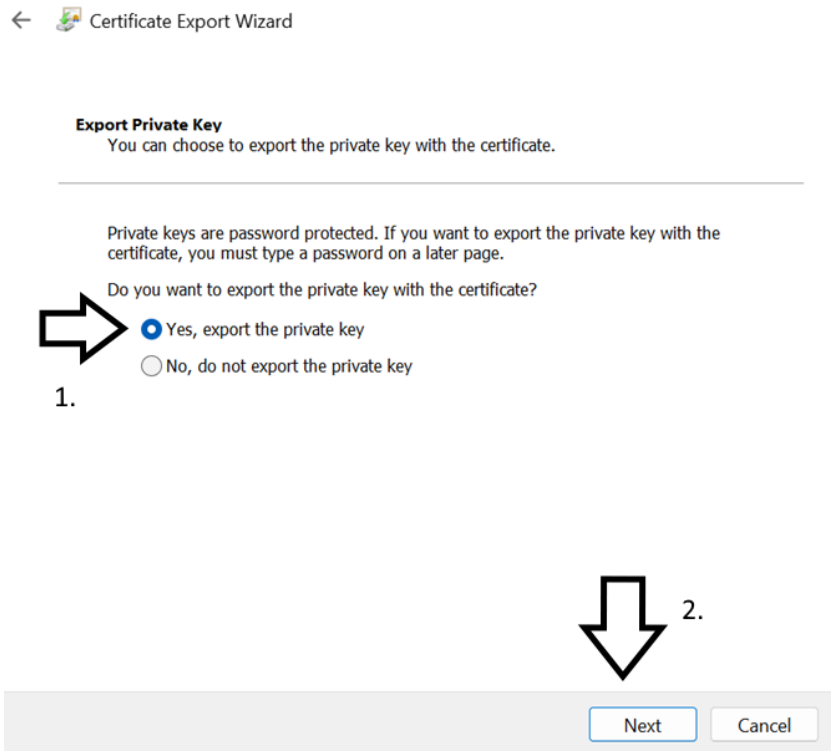
In order to export a certificate installed in the Windows system store (CSP), a certificate store should be displayed via Internet Explorer (*Tools>Internet options>Content > Certificates)* or Edge (*Settings>Privacy, search and services > Security > Manage certificates)* – analogically as described in the introduction to A.2. In the *Certificates* window, select the certificate for export (1) in the *Personal* tab and then click the *Export* button (2)



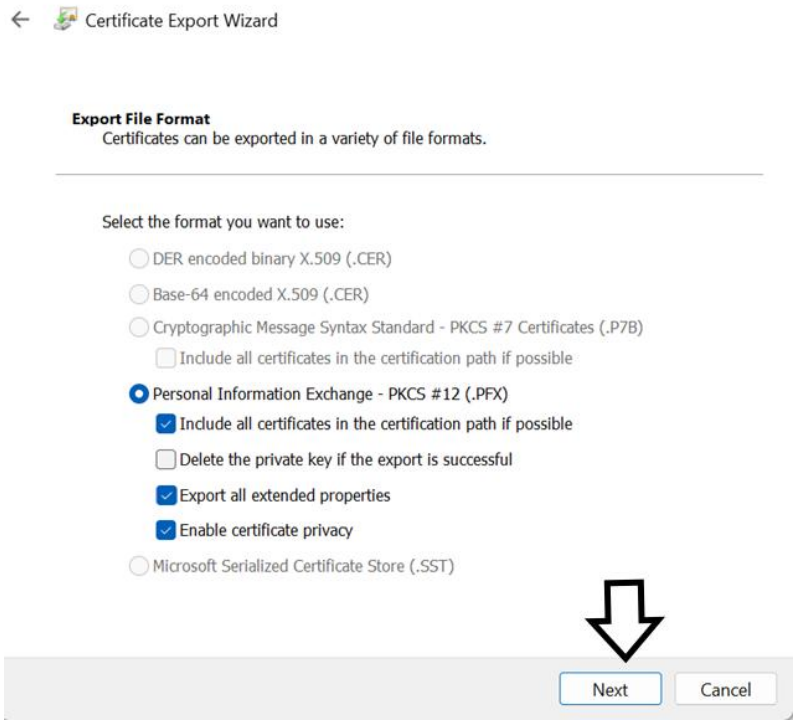
The Certificate export wizard window will display.



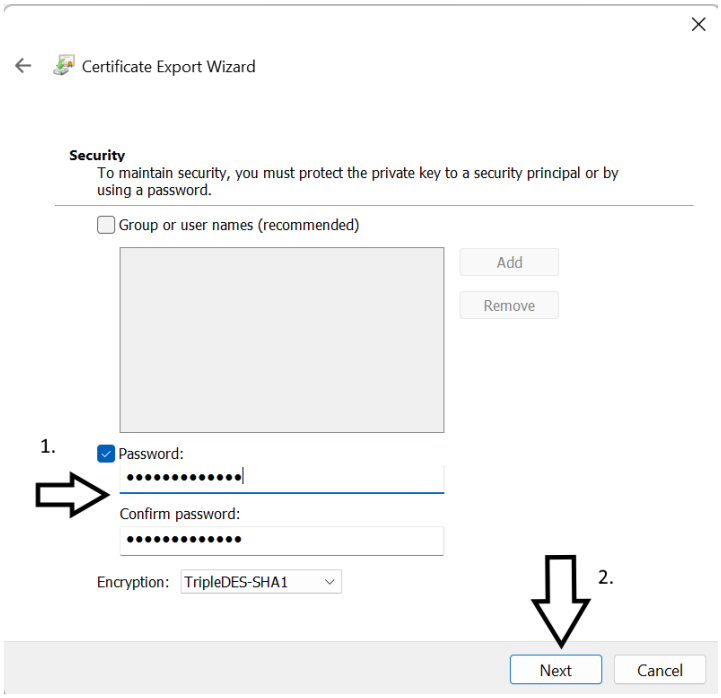
Then click the *Next* button
Select the *Yes, export private key (1)* option in the Private key export window.



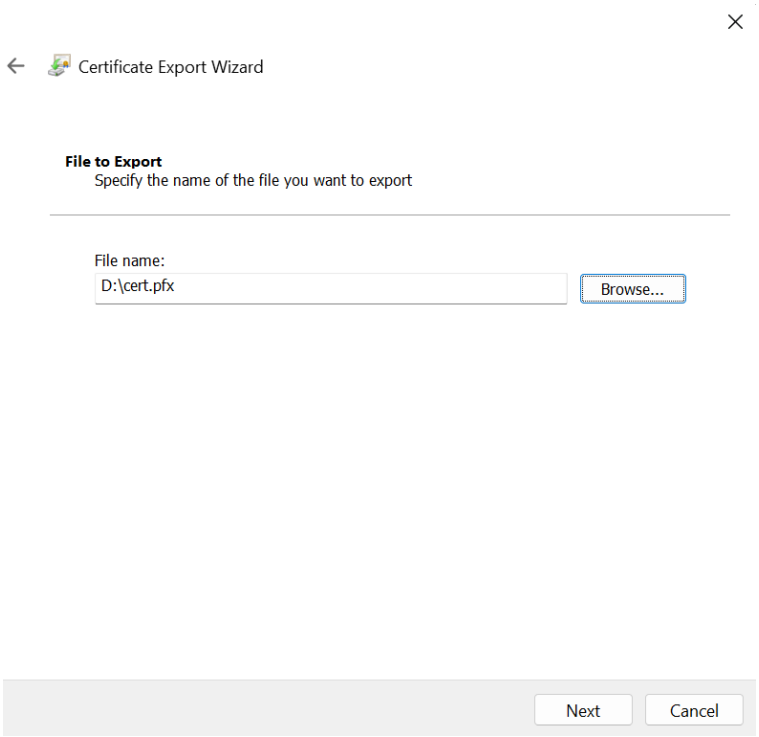
Then click the *Next* button (2)
If a certificate is still to be used on a computer, from which it is exported, select the option as in the view below. In the opposite case, select also the *Delete private key…* option.



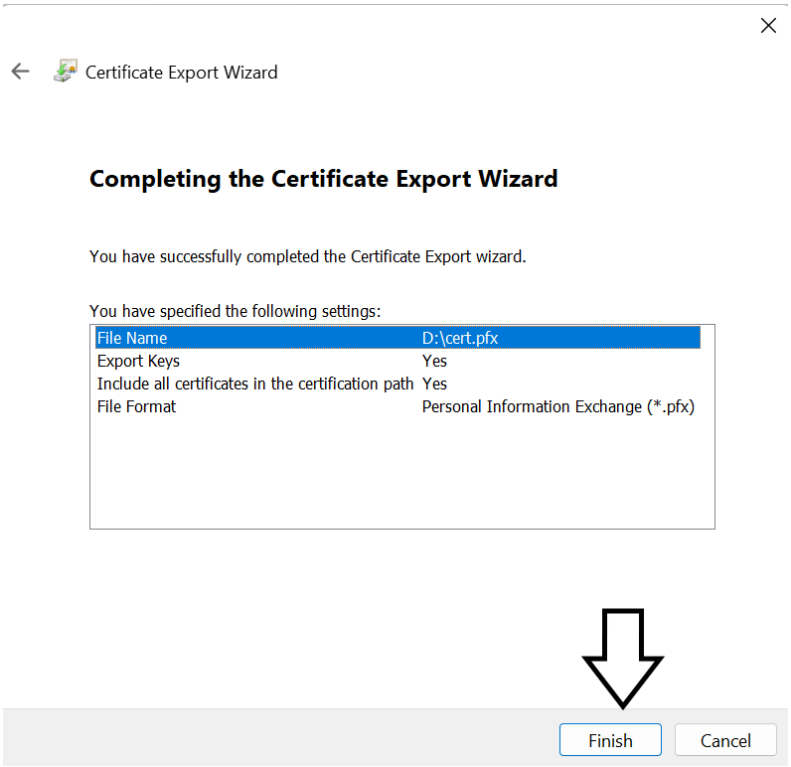
Then click the *Next* button. In the next step, set the password protecting the exported certificate (1) and click the *Next* button.



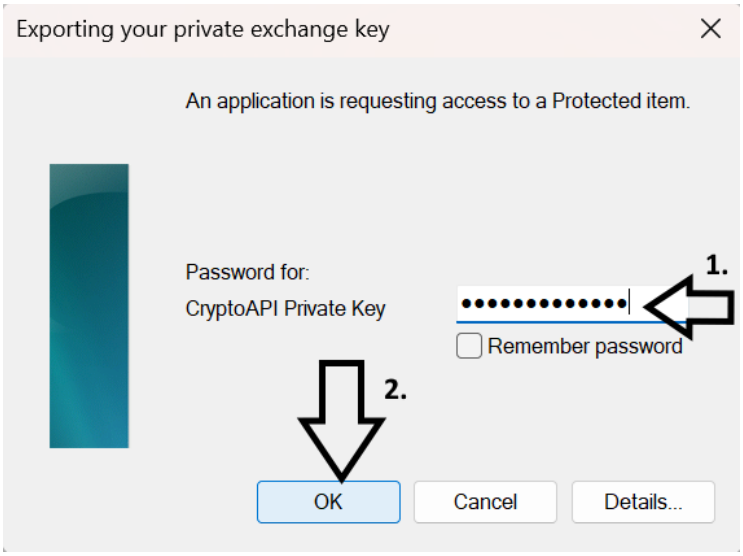
In the next step, enter the file name, to which the certificate will be exported and click *Next.*



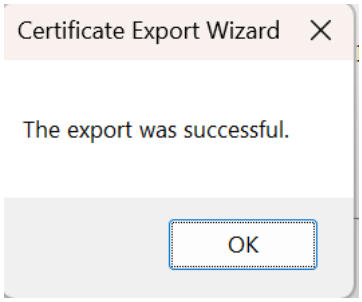
In order to finish the process, click the *Finish* button.



The system will start exporting the certificate and display the window with a query on the password protecting the private key. This is the password, which was entered at the time of generating the certificate – **it is not the password entered in the** *"password protecting the exported certificate"* **step**.

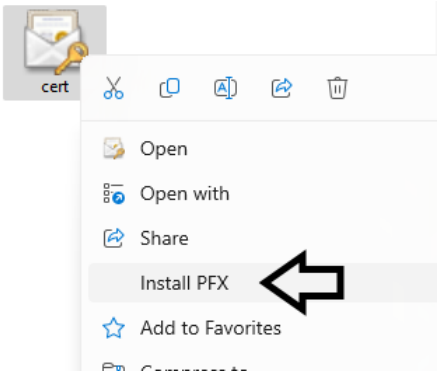


Enter the correct password (1) and click the *OK* button (2).
If you entered the correct password, the certificate will be exported and saved to the selected file and the system will display a confirmation message:

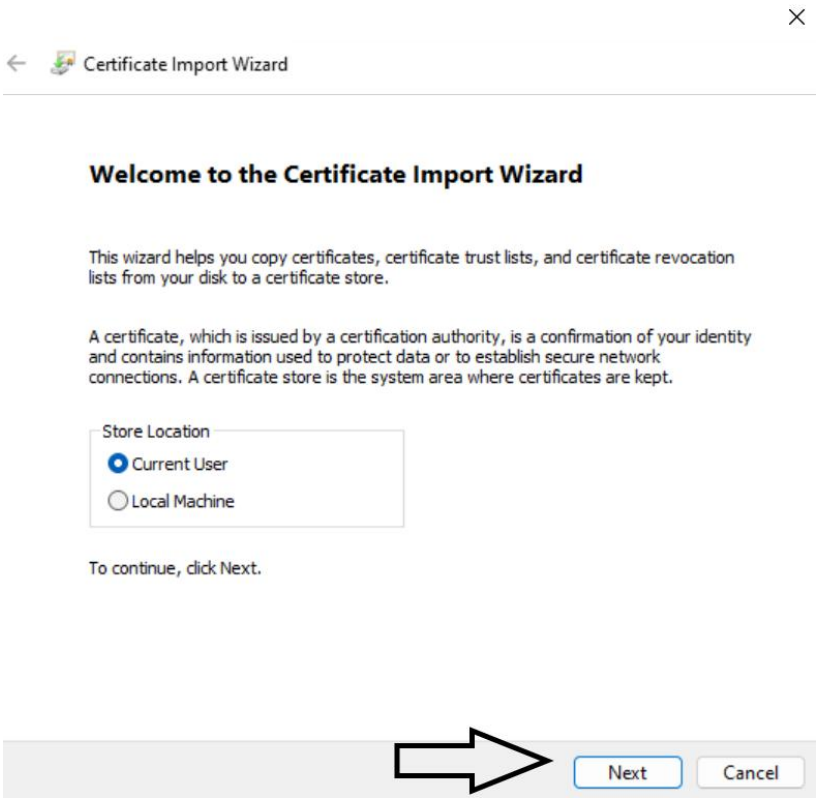


A.4Import of a certificate to the Windows system certificate store (CSP)

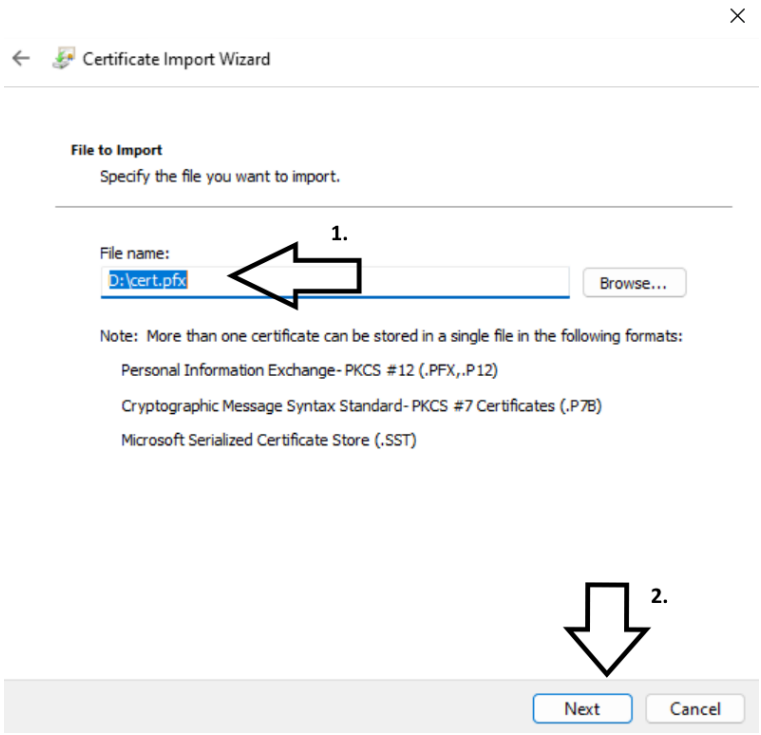
In order to import a previously exported certificate, select the *.pfx (or *.p12) file with the exported certificate and right click.



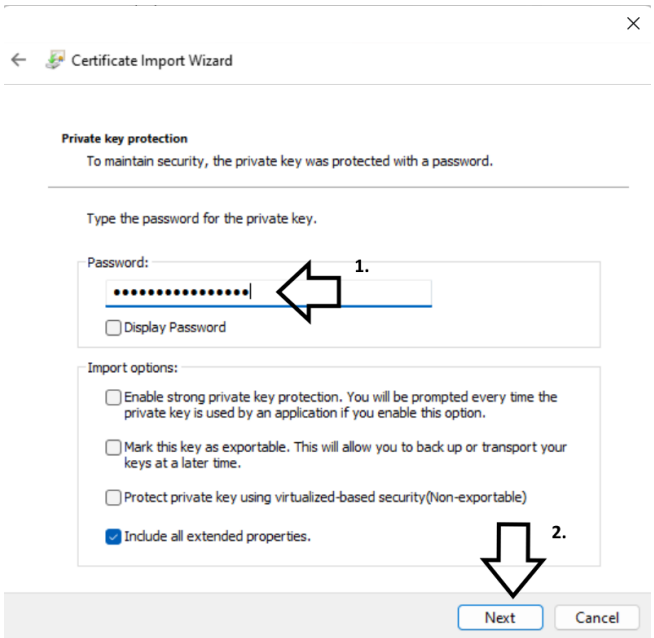
The menu will display, from which *"Install PFX"* should be selected.



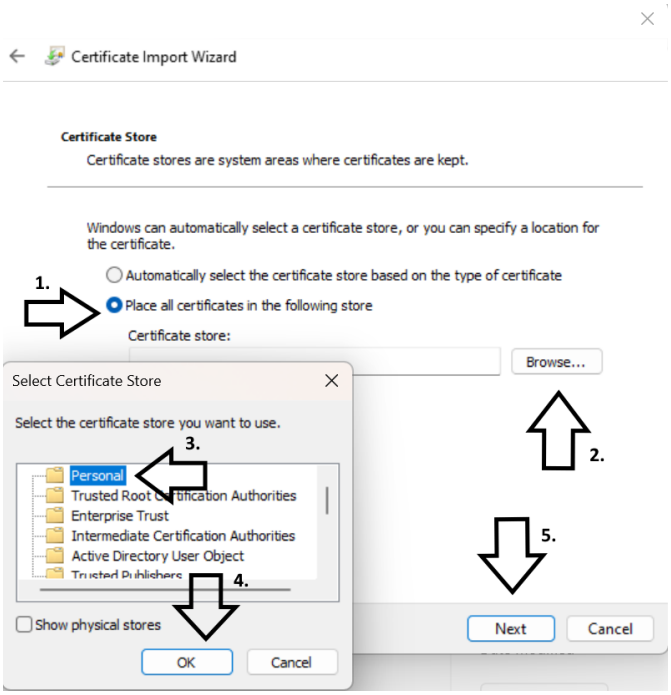
Then click the *Next* button. The Certificate import wizard window will display



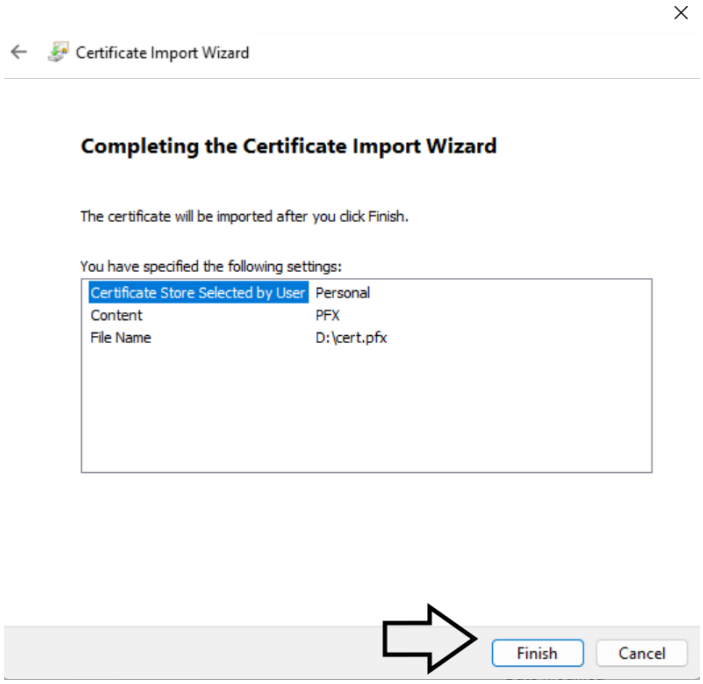
The exported certificate file path will be entered automatically in the *file name* field. If the field is empty, select the exported certificate file (1) and then click the *Next* button (2)
A window will be displayed with a query on the password protecting the exported certificate (1) – the password was entered when exporting the certificate in the *Password* window of the certificate export wizard. If you want to enable further certificate export in future, tick the *Mark this key as exported*…. option (however the subsequent exports pose an additional risk of loss of control over the private key, so this option should not be misused).



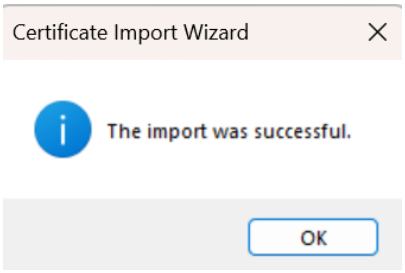
Then click the *Next* button. The certificate store selection window in the Windows system will display.



Select the *"Place all certificates in the following store"(1)* option and then select *"Browse" (2).*
The certificate store selection window will open. In the window, select *Personal* (3). Then click the *OK* button (4) and *Next* (5)



In order to finish the process, click the *Finish* button.
After successful completion of the certificate import process, a window with confirmation of process completion will display.



Click the *OK* button. After completing the import certification process, it should be validated as set out in Addendum A.2. If additional installation of the certificate center certificates is necessary, follow the instructions provided in Addendum A.1.

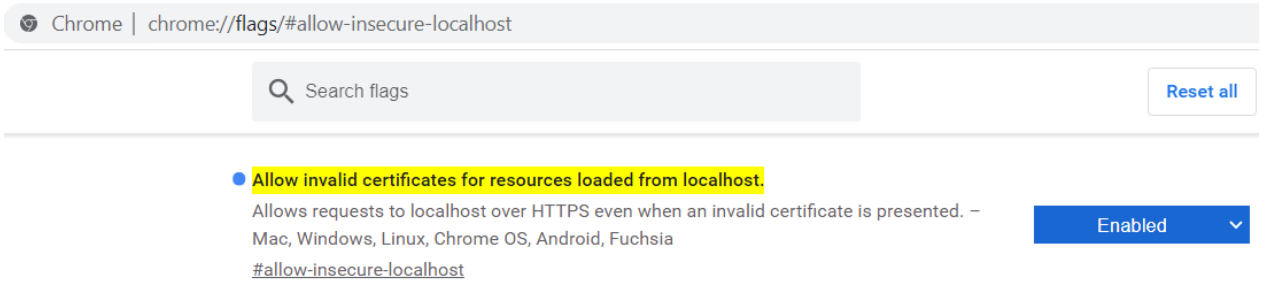
A.5 Description of the Configuration of cryptographic services option

1. **CSP** – a default certificate storage method in the Windows system. The certificates stored in the Windows system enable their export and installation on another computer device. If the Windows system has pre-installed cryptographic card drivers compliant with the CSP standard, it will be possible to generate the keys and saving the certificate directly on the user's cryptographic card. If the application for generating the certificates has never been run, the CSP option is selected by default.
2. **PKCS#11** – a standard for cryptographic cards, an alternative method for certificate storage, not depended on the installed operating system. It may be applied for example in the Linux system. The generated certificate will be saved on the cryptographic card compliant with PKCS#11. This is the safest method of storing the cryptographic keys and certificate, enabling the use of certificate on many computer devices. In the configuration process, you need to select the location of the PKCS#11 driver (this information should be pre-delivered by the producer or distributor of the installed cryptographic card).
3. **Keystore**– an alternative method for certificate storage supported by Java™ (JKS – Java KeyStore) mechanisms. This method does not depend on the installed operating system. It should be noted that the certificates generated with this method can be invisible for the Windows system applications.

A.6 Solving problems with the connection between the PUESC website and the CertSign application

The PUESC website establishes a connection with CertSign **when generating a certificate or signing a document**. In the remaining time, CertSign displays the **disconnected** status, which is correct. The most common causes of no connection at the time of generating a certificate or signing a document on PUESC (in the online mode) is absence of the CCK MF certificates or blocking the localhost connections by the Windows firewall, antivirus software or other security mechanisms. There may be also specific situations associated with the individual computer or software configuration.

Chrome may generate a problem with connecting the browser to the CertSign application. The solution is to change the browser configuration. Go to the advanced options of Chrome by entering: *chrome://flags/#allow-insecure-localhost* in the address bar and set the value to *Enabled.*



Then restart the browser.

A.7 Validation of signature on the PUESC portal

In order to validate a signature on PUESC:

1. Select a document from *My desktop* > *To send and drafts,* by clicking its name.
2. Select the *Verify sign* option.

After selecting this action, the system will validate the signature and display a message with the validation result.

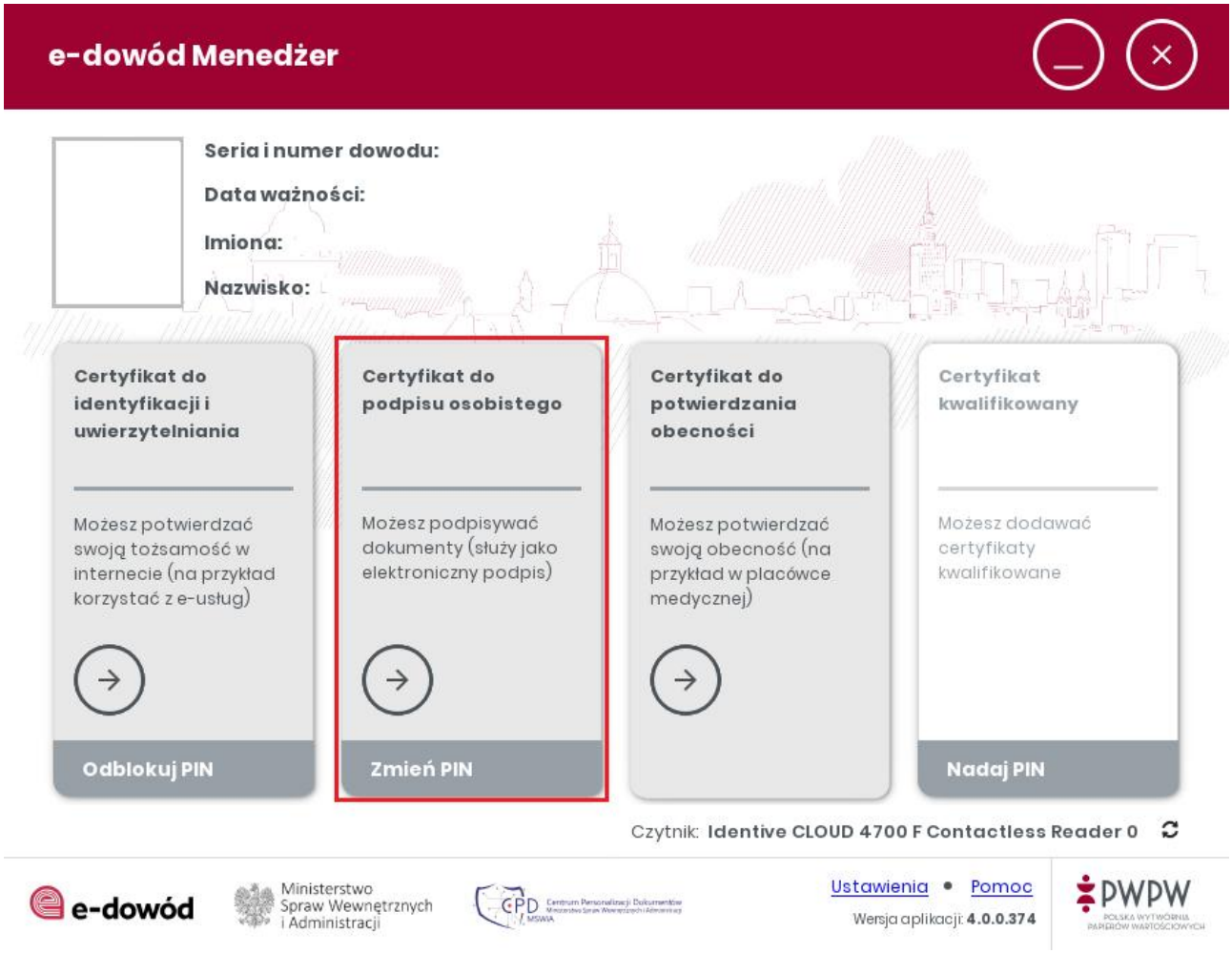
PUESC provides also a dedicated service ***Verify The Electronic Signature*** section available also via a tile on home page.

Addendum B

B.1 Signing with data from the electronic layer of ID card

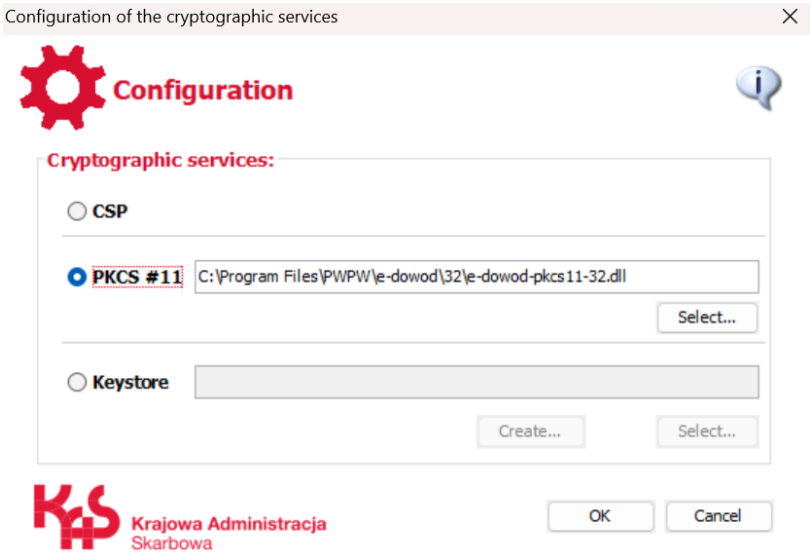
From the 1.3.60 version onwards, the application supports the signatures with the use of data of electronic layer of the ID card. In order to sign with a personal signature, the ***E-dowód menedżer (e-ID card manager)*** and ***E-dowód podpis elektroniczny (e-ID card electronic signature)*** software should be installed.
More information on the e-ID card available at https://www.gov.pl/web/e-dowod

Before placing a signature, the PIN code of personal signature certificate should be enabled in the *E-dowód Menedżer* application:

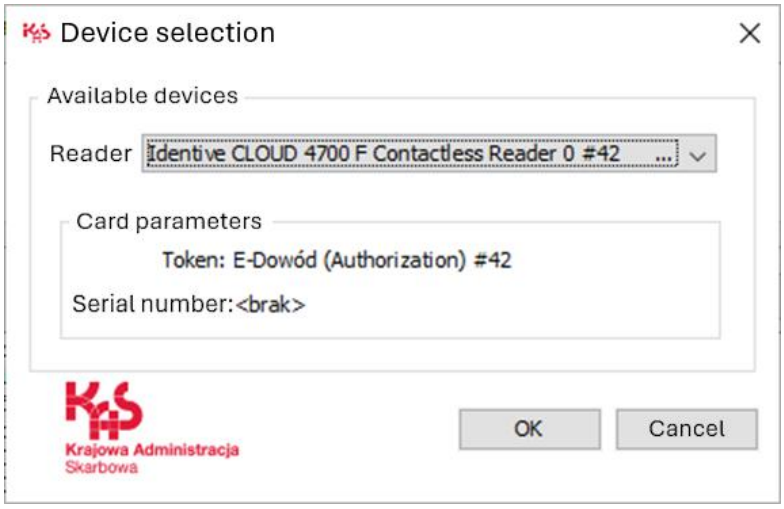


If PIN of this certificate is enabled, signing with an electronic signature is possible.

Signing with the use of CertSign is the same as for the other PKCS#11 media. Select the appropriate library and token for signature in the cryptographic service configuration, as described in chapter 5.3. PKCS#11 libraries are located in the installation folder of the *E-dowód Menedżer* application. Select the version compatible with the installed platform i.e. in the case of 32-bit architecture and 32-bit distribution of CertSign, select the 32-bit library of*e-dowod-pkcs11-32.dll,*as presented below:



In the next step, select the token for signature. The default token for signature is **Authorization**, containing the personal signature certificate.



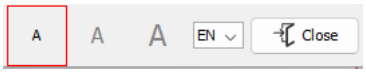
The following operations are performed as described in chapter 5.3.

B.2 Graphic interface elements scaling functions

From the version 1.3.60onwards, the application enables scaling the screen fonts to three sizes:

- standard
- larger
- the largest

In order to change a font size, select one of the scaling buttons, which is not currently selected. Each subsequent size is larger by 1.5 times from the previous one. This means that increasing the *standard* size to the *larger* size increases the current font size by 150%, while to the *largest* size – by 225%. Analogically, decreasing to the *larger* size decreases the level from 225% of the *standard* size to 150%, while returning to the *standard* size decreases the current size to the default value (100%).
The scaling sequence does not matter – it can be made in any sequence.

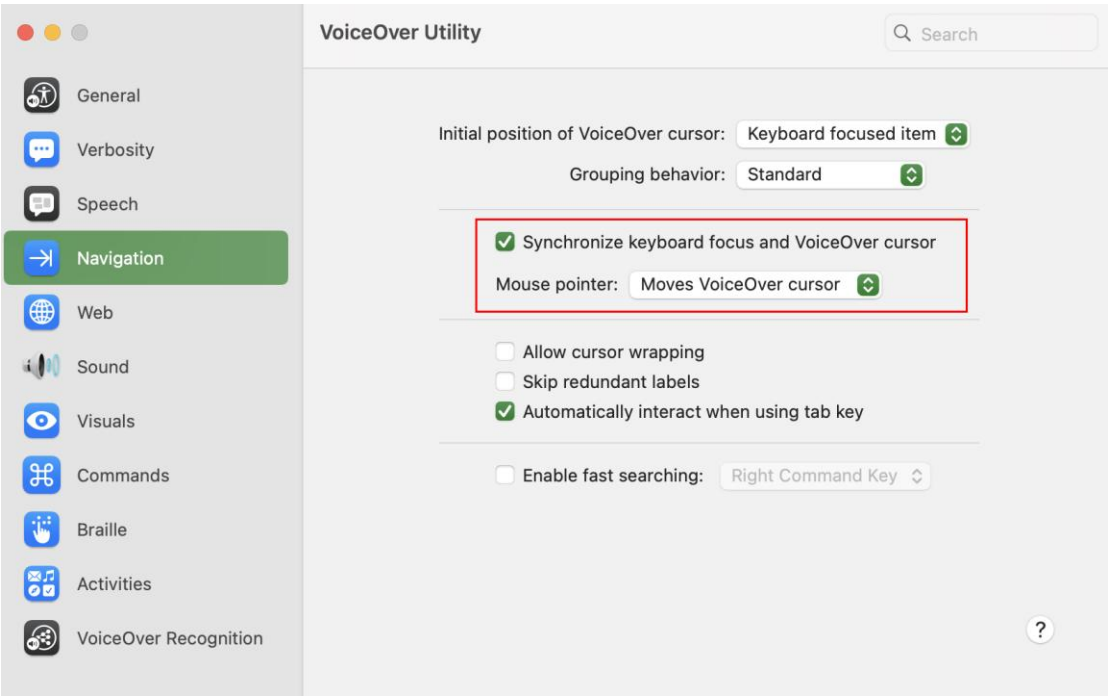


The font size increase buttons are marked with a red frame on the screen view above.

The application may partially o entirely disable the scaling functions on the displays with lower resolutions to avoid errors related to excessive scaling of the application interface elements.

B.3 Operating the application via a screen reader

From the version 1.3.60 onwards, the application is operable via the NVDA reader for Windows and VoiceOver for macOS.
The default configuration of VoiceOver application is adapted to be operated with a keyboard. In such case, it enables using the *Tab* button to navigate between the components and to read or select them. If a component is not available for the *Tab* button, navigation with the VoiceOver program cursor using the right and left arrow on the keyboard is still enabled.
If there is a need to read each text content by placing a mouse cursor on it, select the Synchronise keyboard focus and VoiceOver cursor option in the VoiceOver program settings.



In this way, the VoiceOver cursor will be set by placing the mouse cursor on an item.

B.4 Navigation and control with a keyboard

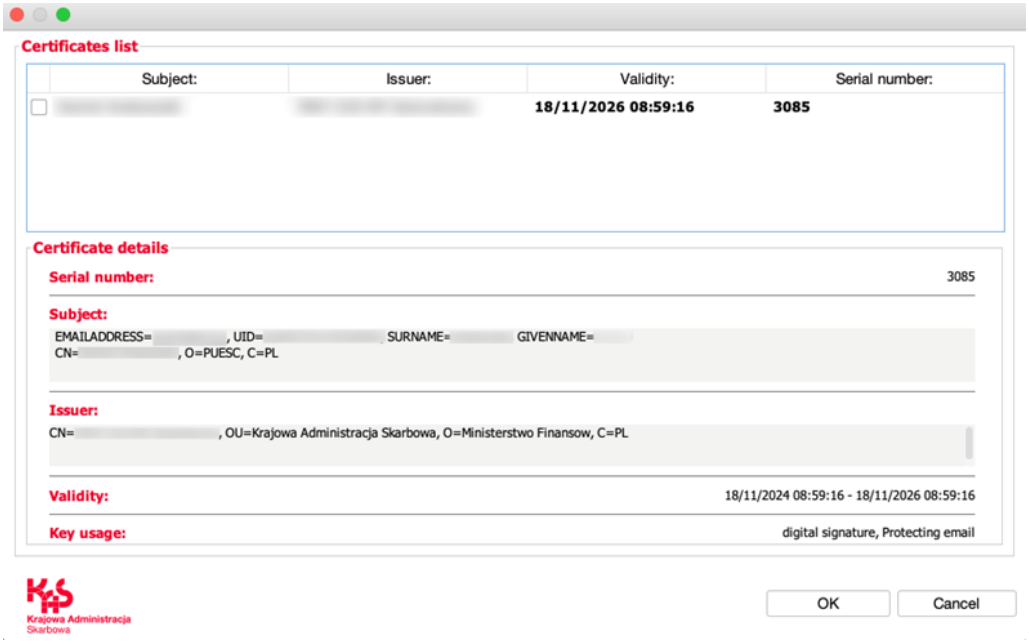
The CertSign application can be operated with a keyboard. Navigation between the elements is made with the *Tab* button. The undue function is enabled with Shift + Tab combination.
In order to select another tab using a keyboard, if the first element is selected, you can navigate forward and backward with Ctrl + Tab and Shift + Ctrl + Tab combinations, respectively.
More tips and default keyboard shortcuts are available at: https://www.ibm.com/docs/en/sdk-java-technology/8?topic=applications-default-swing-key-bindings

Operating the ComboBox-type object (dropdown list)
In order to display the list of elements for selection, after placing the cursor on a ComboBox-type object, press:

- for Windows: *Alt* + down arrow
- for Linux and MacOS: *Space*

In order to select another element, navigate up or down using the relevant arrow. To select a specific element immediately, select the key with the first letter of the name of this element at a dropdown list.

Control in the certificate selection window

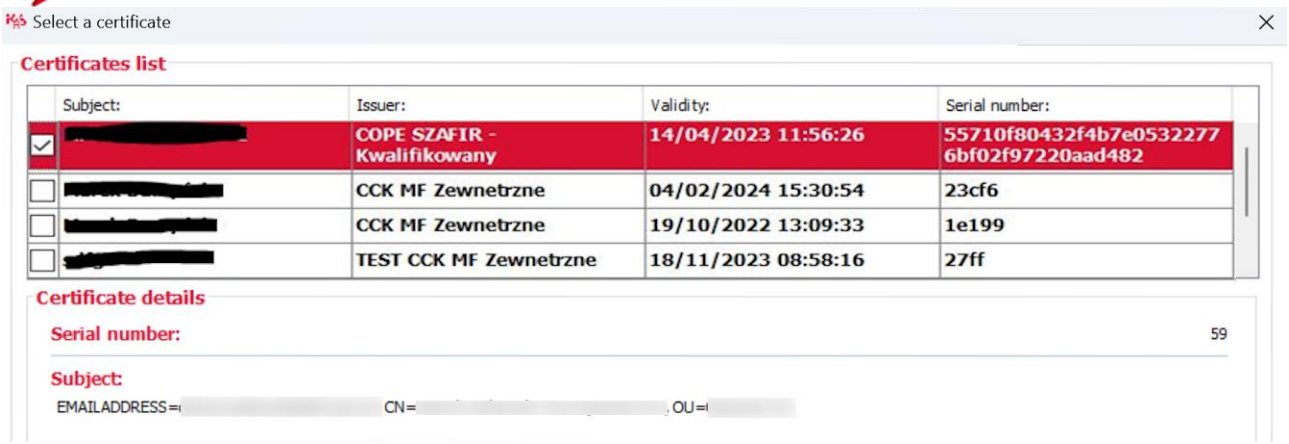


There are two options to navigate with a keyboard in this window, depending on the currently selected component:
- You can navigate with *Tab* button between the main elements (table component, text field and scrollbars, buttons).
- You can navigate with up and down arrows between the listed certificates in the table component.

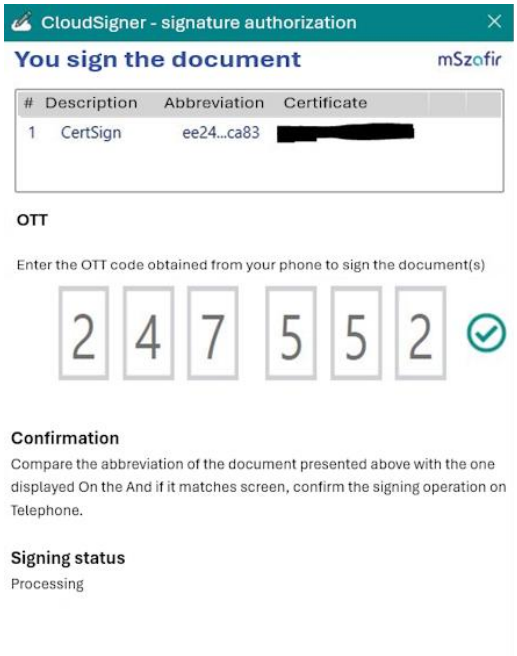
In order to select a certificate highlighted in red, press Enter or Space. Selection of the certificate is signalled by ticking the checkbox on the left side of the table row.

B.5 Cooperation with the mobile electronic signature service

The CertSign application can cooperate with the mobile electronic signature service, provided that the provider ensures software for cryptographic card support emulation, enabling registration of the certificate in the Windows certificate store (CSP) or access via PKCS#11 driver. Preparation of CertSign for cooperation consists in selecting the certificate provided under the mobile service in the CSP (Windows store) or PKCS#11configuration. The remaining steps are performed as for the standard signature, with consideration to authorisation in the mobile application. The exemplary cooperation with the mSzafir services is described below. Cooperation with another service, for example SimplySign can be established in a similar way described at https://pomoc.certum.pl/pl/simplysign-faq/
In order to prepare mSzafir, follow the instruction at:
https://www.mszafir.pl/gfx/mszafir/userfiles/_public/tutoriale/jak_wykorzystac_certyfikat_mszafir_w_dowolnej_aplikacji_podpisujacej.pdf
After enabling a virtual card, select the “Change certificate” option in CertSign and select the mobile service certificate, analogically as in the case of a standard certificate (in CSP or PKCS#11 configuration).



After selecting the certificate, you can go to signing a document, provided that the signature is authorised with a code generated in the mobile application.

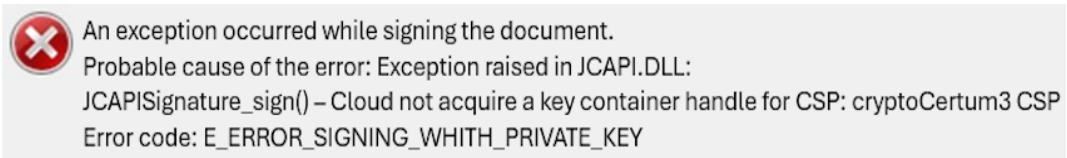


B.6 Specific cases of cards with qualified certificates

In the case of a qualified signature, CrtSign uses the CSP or PKCS#11 services to communicate with the cryptographic card. In some cases however, the specifics of the cryptographic card interfaces and CertSign forces the use of only one from the abovementioned services.

NOTE! A qualified certificate provider software needs to be installed, since it contains the cryptographic card drivers.

If there is an error when signing with the selected CSP option, for example:



select the *Change certificate* option in CertSign, select *PKCS#11*and path to the dll. file of the card driver provided with the certificate provider software. Remember to select the file corresponding to the operating system architecture (32- or 64-bit).
Information on location of these files is available on the websites or in the certificate provider documentation. For the Polish providers, these **may** include:

CERTUM:
C:\Windows\System32\cryptoCertum3PKCS64.dll
C:\Windows\System32\cryptoCertum3PKCS.dll
https://pomoc.certum.pl/pl/ekw-reczne-wskazanie-sterownika-karty-kryptograficznej/

SIGILLUM:
C:\Windows\System32\asepkcs.dll

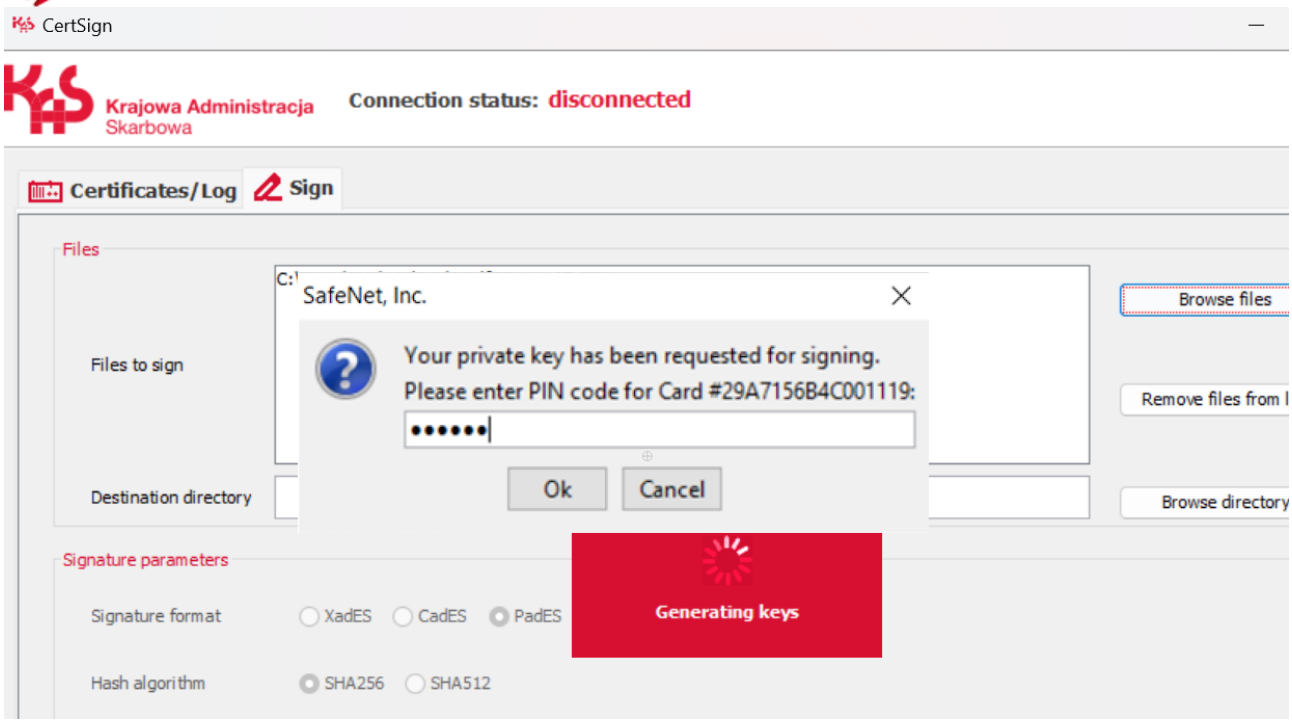
EUROCERT:
C:\Windows\System32\cmP11.dll
C:\Windows\System32\cmP1164.dll
C:\Windows\SysWOW64\cmP11.dll
https://eurocert.freshdesk.com/support/solutions/articles/48001213718-niezb%C4%99dna-biblioteka-localizacja-

KIR (Szafir):
C:\Program Files\Krajowa Izba Rozliczeniowa S.A.\Szafir 2.0\bin\CCGraphiteP11p.x64.dll
C:\Program Files\Krajowa Izba Rozliczeniowa S.A.\Szafir 2.0\bin\CCGraphiteP11p.x86.dll
https://www.elektronicznypodpis.pl/gfx/elektronicznypodpis/userfiles/_public/informacje/instrukcje/instrukcja_konfiguracji_kart_cryptocard_graphite_w_jpk.pdf
C:\Program Files\CryptoTech\CCP1164.dll
C:\Program Files\CryptoTech\CCPkiP11.dll
https://www.elektronicznypodpis.pl/gfx/elektronicznypodpis/userfiles/_public/informacje/instrukcje/jpk_2.pdf

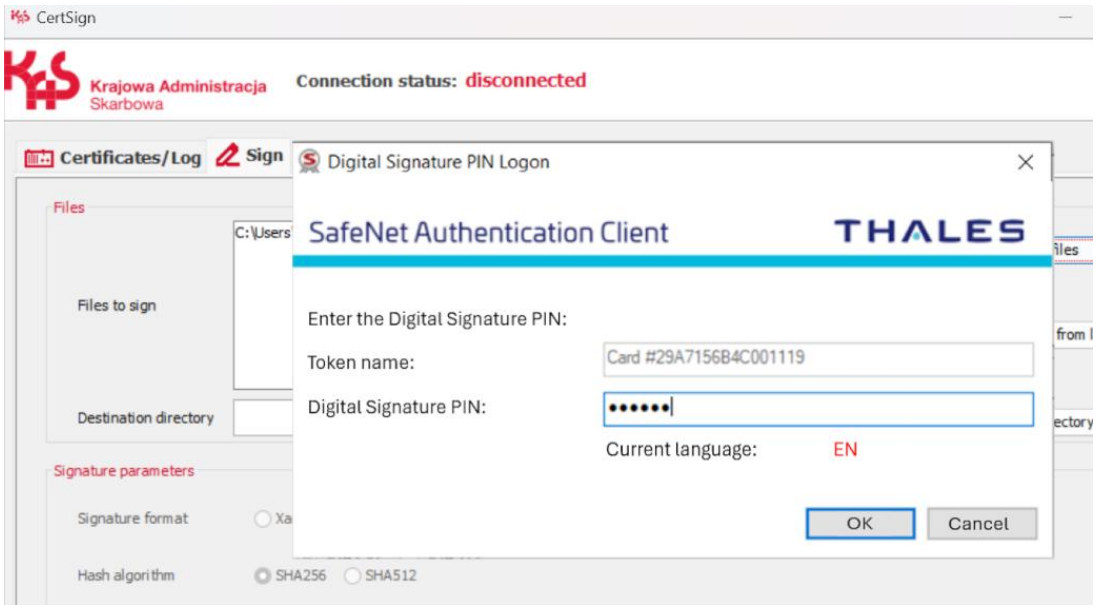
CENCERT:
C:\Program Files\ENCARD\enigmap11-x64.dll
C:\Program Files (x86)\ENCARD\enigmap11.dll

A specific case is the cryptographic cards with 2-level security: with a PIN code to the card and a separate PIN for signature purposes. The example is the IDPrime card provided by CenCert, which has a PIN to a card and *Digital Signature PIN* for signature purpose. The signing process in CertSign requires entering both PIN in the correct order, which is available **only in the CSP configuration.** When using PKCS#11, only the card Pin is provided, in effect of which the signing is impossible.
The exemplary signing with the use of IDPrime card by CenCert is presented below (it requires pre-installed *SafeNet Authentication Client* software).

With the selected CSP configuration and a qualified certificate (*Certificates/Log* tab), select the file to be signed and confirm signing. In the first step, the query on PIN to the cryptographic card will display.



After entering the correct card PIN, the *Digital Signature PIN* request will display.



Placing a signature will be confirmed with a message.

B.7 Impact of Windows update on the application – Could not acquire a key container handle for CSP problem

It has been observed that certificate-related operations may fail after installing the Windows 10 and 11 updates released on October 14, 2025 - KB5066835 (OS builds 26200.6899 and 26100.6899). The most common symptom is that the previously running application fails with the message "Could not acquire a key container handle for CSP." If this issue occurs, it can be resolved by manually setting the value of a Windows registry key.

WARNING: Changing the Windows registry poses a risk of system damage and should be performed with extreme caution, preferably by someone experienced in managing Windows workstations. We recommend backing up the registry before making any changes.

Detailed steps to modify registry key:

1. Open Registry Editor.
    - press Win + R, type regedit, and press Enter,
    - if prompted by User Account Control, click Yes.
2. Search for the subkey HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais
3. Create or edit (if exists) the key and set the appropriate value:
    - inside Calais folder, check if the key DisableCapiOverrideForRSA exists; if not – create it,
    - double-click on DisableCapiOverrideForRSA,
    - in the Data field enter: „0” (if it is 1, change it to 0).

Nazwa	Typ	Dane
(Domyślna)	REG_SZ	(wartość nie ustalona)
DisableCapiOverrideForRSA	REG_DWORD	0x00000000 (0)

Note: The DisableCapiOverrideForRSA registry setting is not added by the default OS install or the installation of Windows Updates.

4. Close and restart.

- Close Registry Editor.
- Restart the computer for changes to take effect and then select the certificate again in the CertSign application – „Change certyficate” option.

Link to article on Microsoft website:
https://learn.microsoft.com/en-us/windows/release-health/resolved-issues-windows-11-25h2#smartcard-authentication-issues-might-occur-with-the-october-2025-windows-update