

GUIDE TO GENERATING CERTIFICATES FOR THE CLIENT API OF PPF BANKA A.S. IN WINDOWS

Contents:

1	INSTALLATION OF KEYSTORE EXPLORER	2
2	GENERATING A CERTIFICATE REQUEST	2
3	IMPORTING CERTIFICATE REQUESTS SIGNED BY THE BANK	8
4	EXPORTING THE FULL CERTIFICATE.....	10
5	USER SUPPORT	11

1 Installation of KeyStore Explorer

To generate certificate requests for the Client API, first install KeyStore Explorer.

(official website: www.keystore-explorer.org)

2 Generating a certificate request

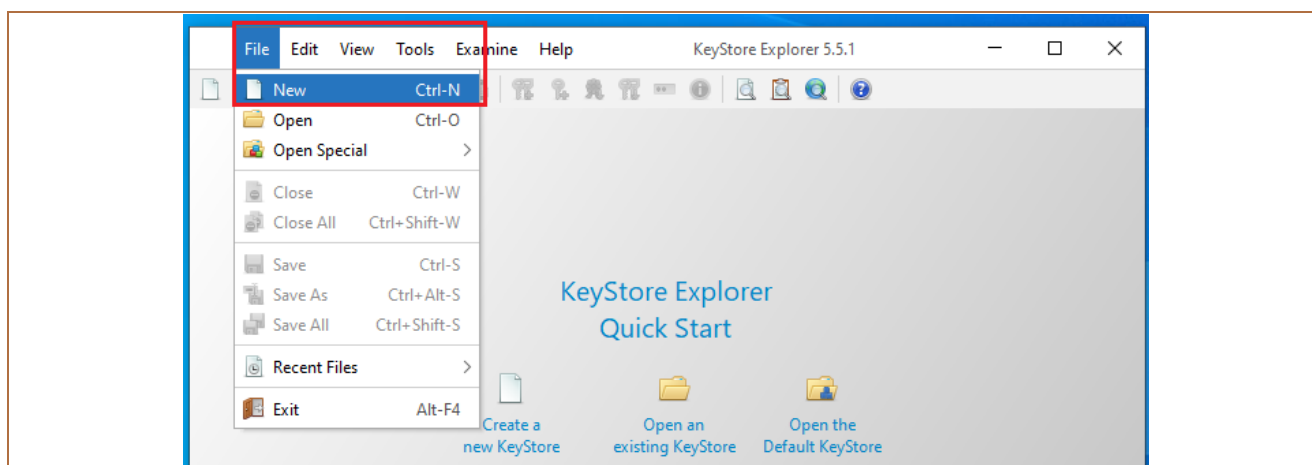
The same procedure is used to generate a Client Certificate request and to generate a Signing Certificate request. The only difference is in the data you enter.

To generate a certificate request you will need the strings sent to you by PPF banka a.s. (the "Bank").

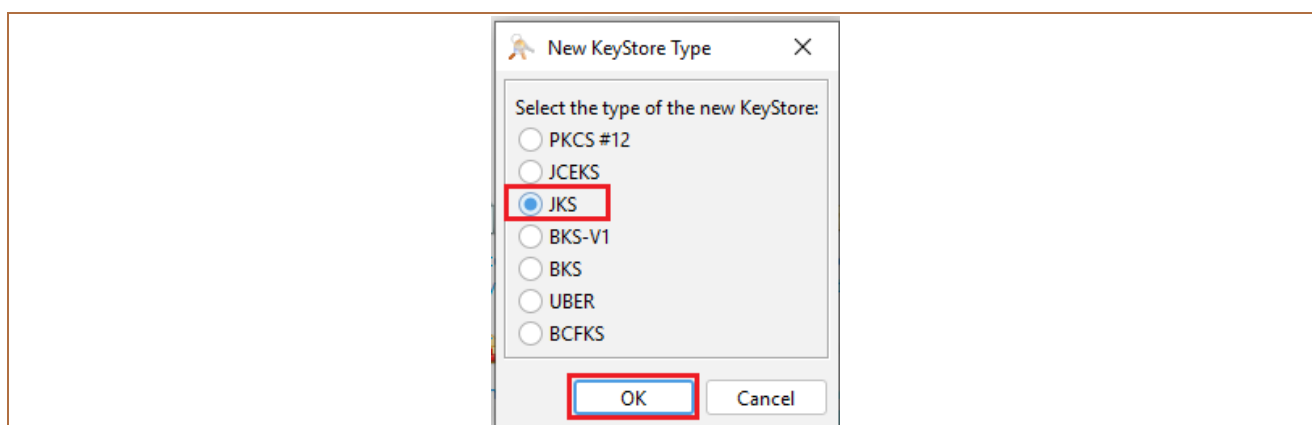
Examples of strings received from the Bank:

- Client Certificate string: `openssl req -new -newkey rsa:2048 -nodes -out Client_cert.csr -keyout Client_cert.key -subj "/O=První strojírenská a.s./CN=I00001234"`
- Signing Certificate string: `openssl req -new -newkey rsa:2048 -nodes -out User_cert.csr -keyout User_cert.key -subj "/O=Josef Novák/CN=P00012345"`

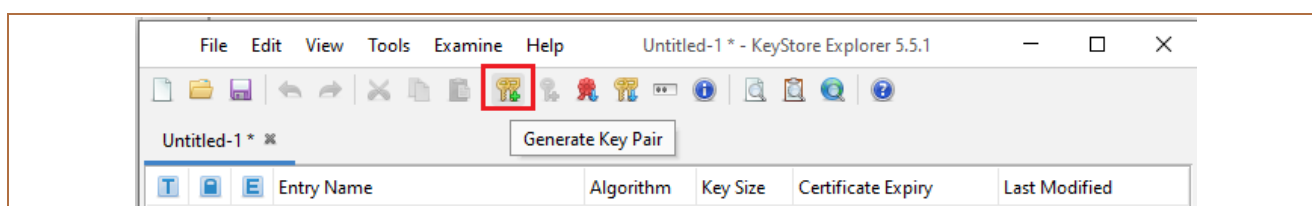
To generate a certificate request, choose **File** and **New**.



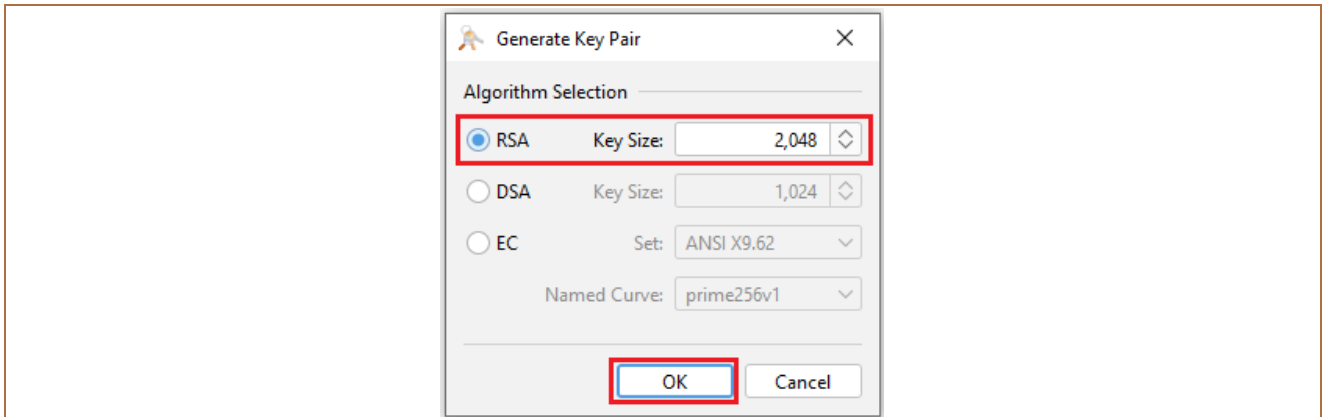
A window will appear where you can choose the file type – select **JKS** then confirm with **OK**.



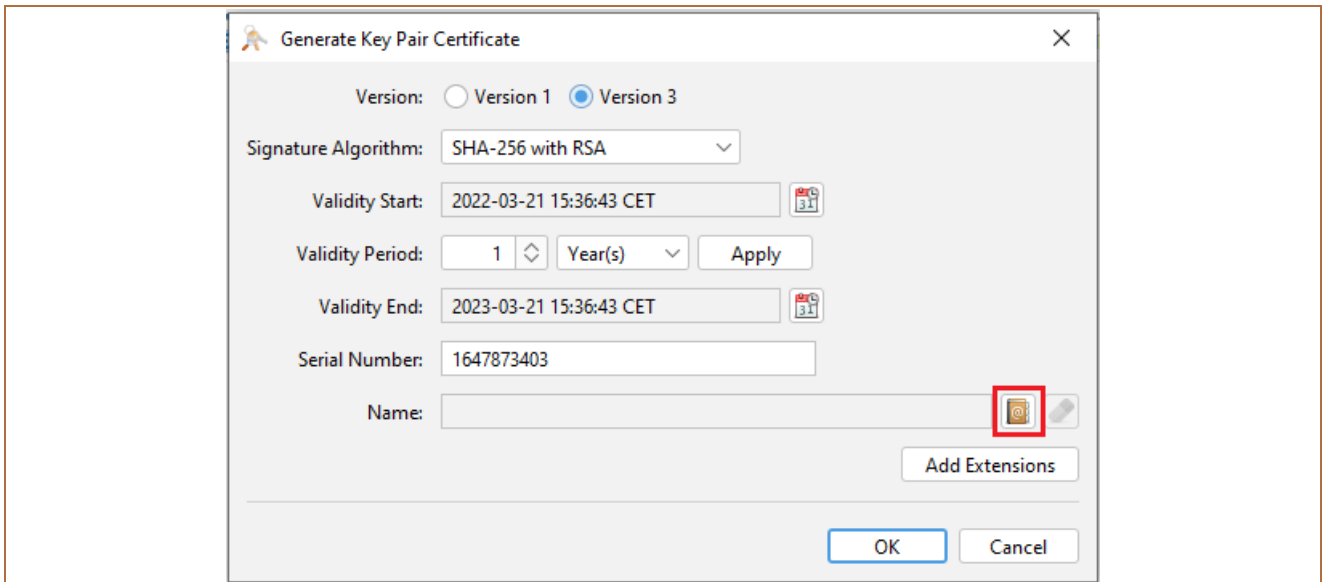
Next, click on the icon in the toolbar showing keys with a green plus sign (Generate Key Pair).



In the window that appears, select the **RSA** key type then confirm with **OK**.



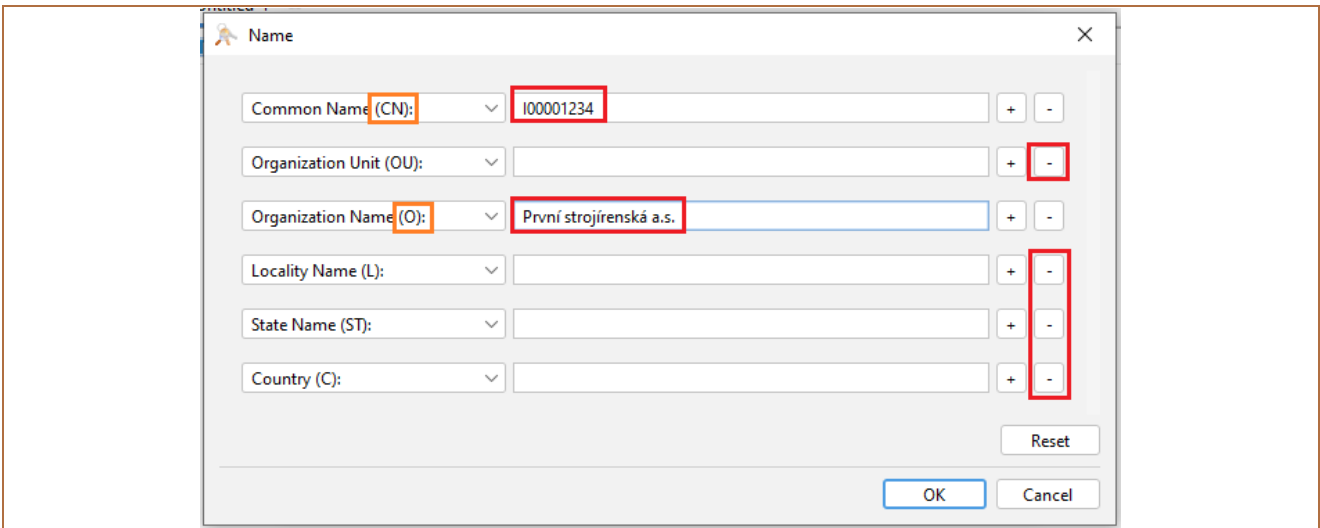
In the next window, click on the book icon.



Enter the following identification data from the string you received from the Bank:

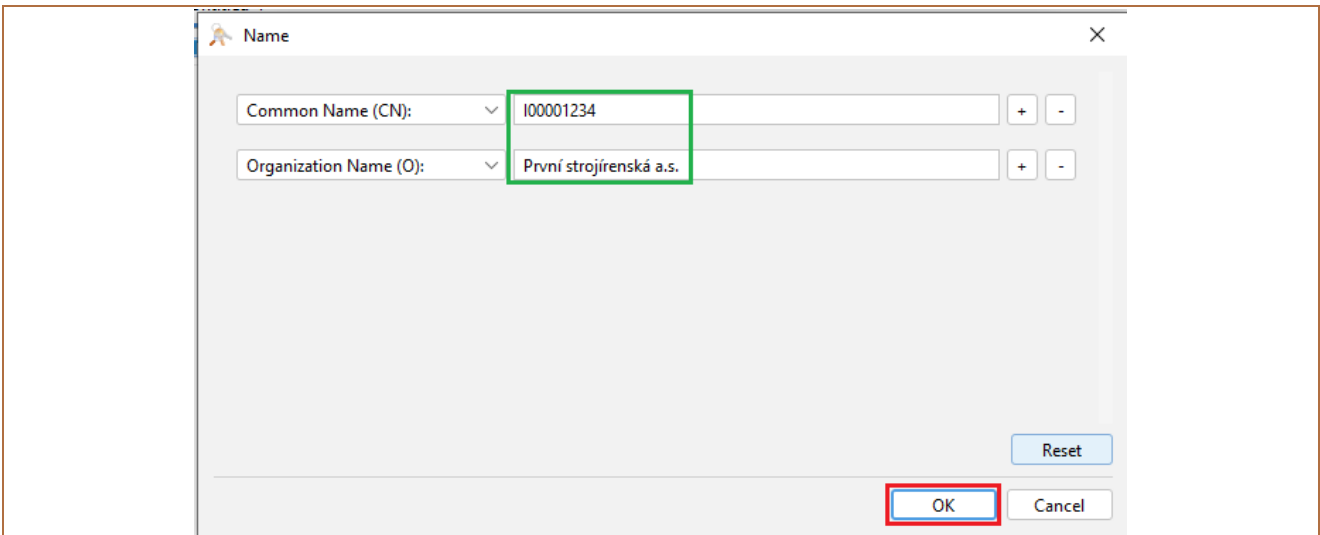
Field	Data to be entered
Common Name (CN):	Enter the data from the string that follows the element "CN": <ul style="list-style-type: none"> for a Client Certificate, this data starts with the letter I – e.g. I00001234 for a Signing Certificate, this data starts with the letter P – e.g. P00012345
Organization Name (O):	Enter the data from the string that follows the element "O": <ul style="list-style-type: none"> for a Client Certificate, this is the client name – e.g. První strojírenská a.s. for a Signing Certificate, this is the name and surname of the API User – e.g. Josef Novák

Remove the other fields.



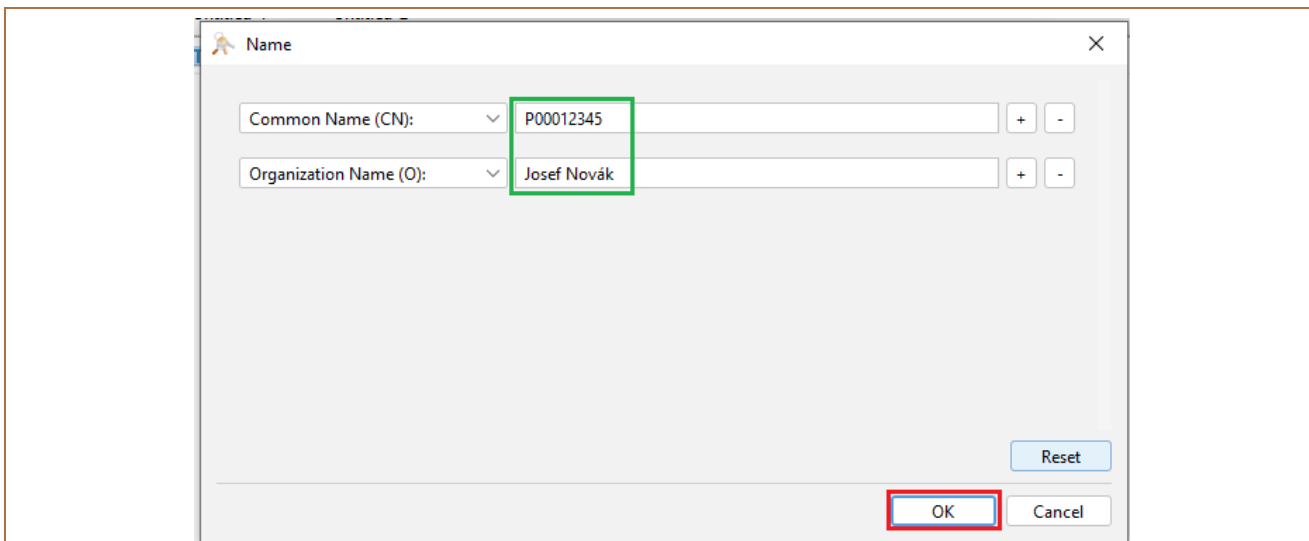
Example of the data entered for a Client Certificate request:

String received: openssl req -new -newkey rsa:2048 -nodes -out Client_cert.csr -keyout Client_cert.key -subj **"/O=První strojírenská a.s./CN=I00001234"**

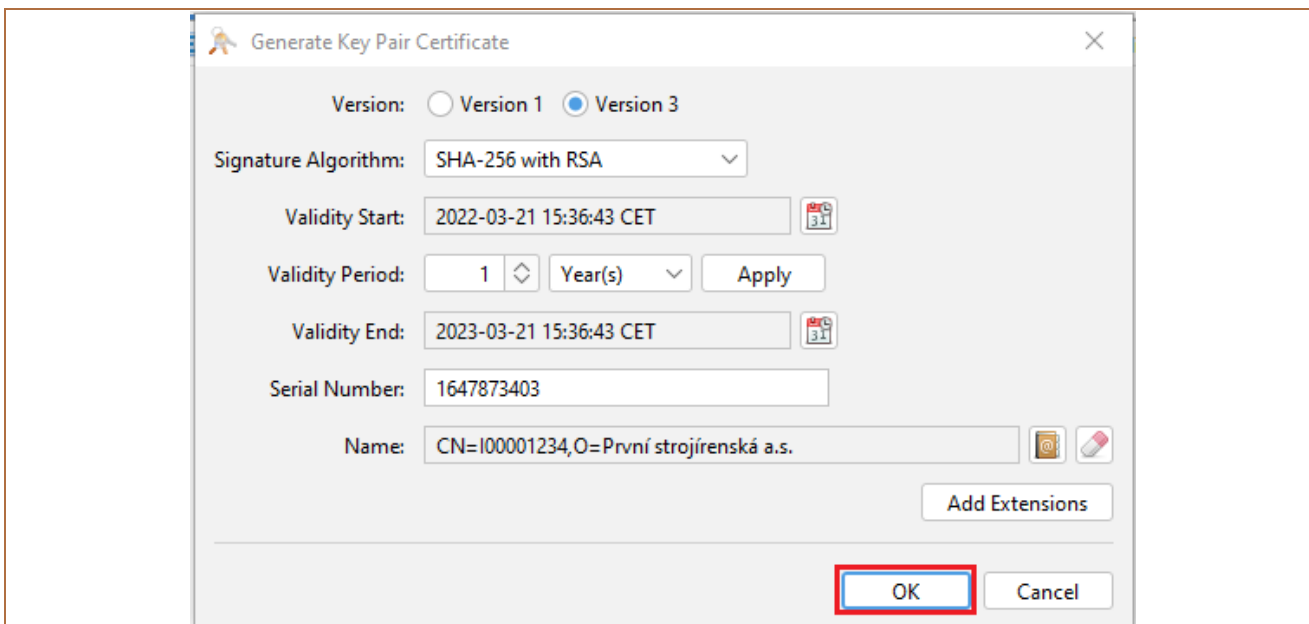


Example of the data entered for a Signing Certificate request:

String received: openssl req -new -newkey rsa:2048 -nodes -out User_cert.csr -keyout User_cert.key -subj **"/O=Josef Novák/CN=P00012345"**



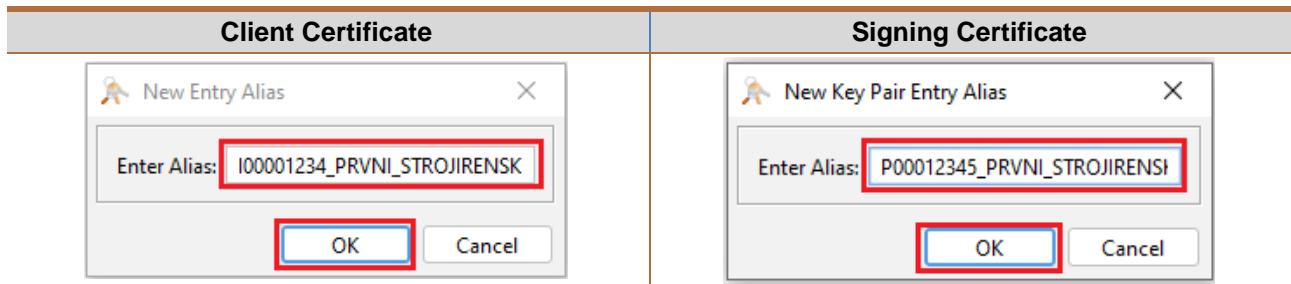
Confirm the data you entered with **OK**, and in the next window click **OK** again.



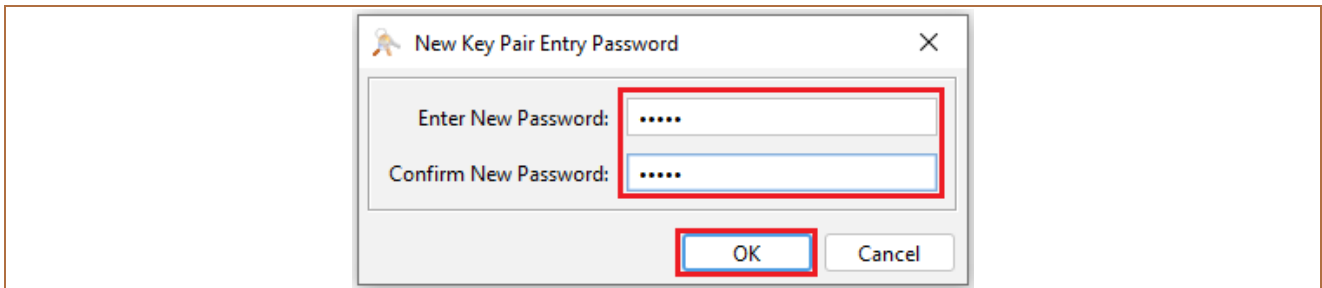
A window will appear for you to enter a name (alias) for the file. The data from the field **Common Name (CN)** will be automatically pre-populated here. Complete the name using the following format:

- Client Certificate request file:
 - INNNNNNNN_CLIENT_NAME_CLIENT, where:
 - INNNNNNNN = the data from the field **Common Name (CN)**, followed by an underscore,
 - CLIENT_NAME = the client name written without diacritics, where any spaces must be replaced with underscores,
 - _CLIENT = an identifier that shows this is a Client Certificate request,
 - for example: I00001234_PRVNI_STROJIRENSKA_CLIENT
- Signing Certificate request file:
 - PNNNNNNNN_CLIENT_NAME_USER, where:
 - PNNNNNNNN = the data from the field **Common Name (CN)**, followed by an underscore,
 - CLIENT_NAME = the client name written without diacritics, where any spaces must be replaced with underscores,
 - _USER = an identifier that shows this is a Signing Certificate request;
 - for example: P00012345_PRVNI_STROJIRENSKA_USER.

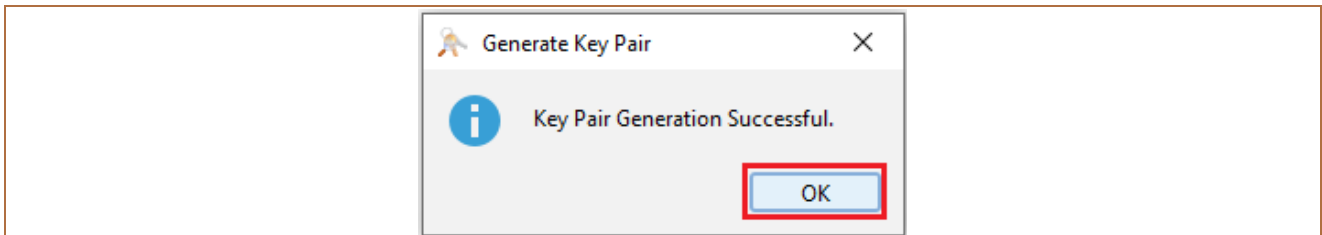
Example of completion of the file name (alias) – confirm the data entered with **OK**:



The application will prompt you to enter a password for the file – memorise or save this password, then confirm with **OK**.

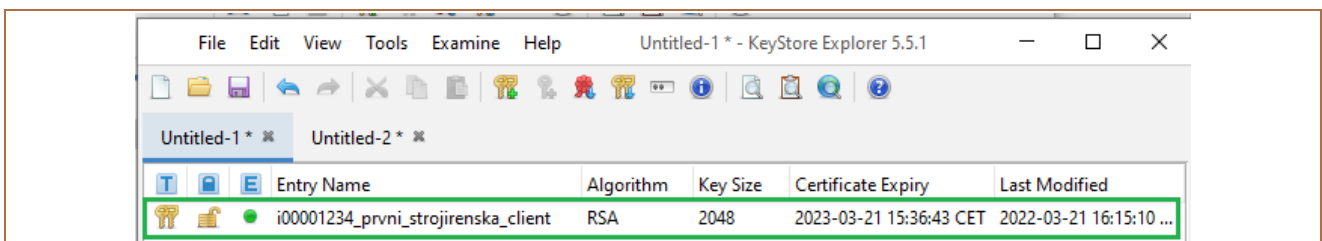


A message will be displayed confirming that the keys have been successfully generated – confirm again with **OK**.

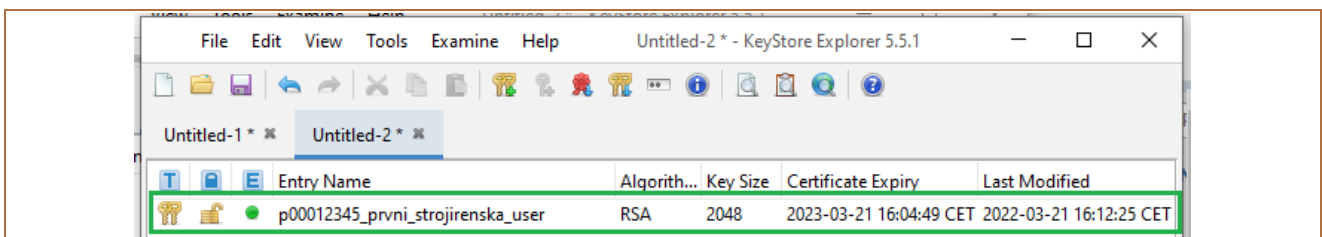


The generated file will appear in the application window:

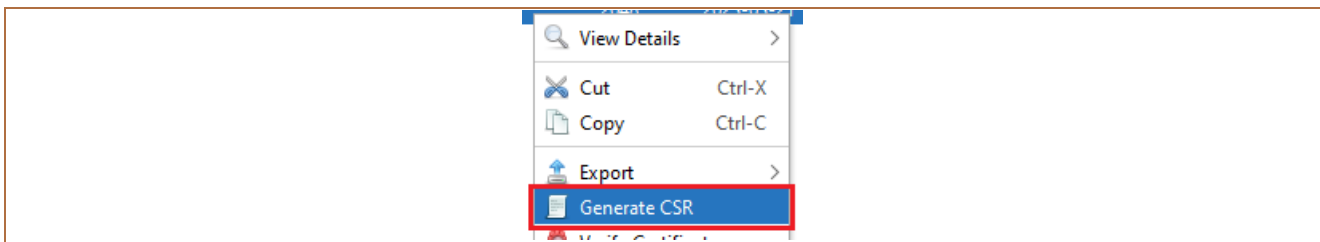
Client Certificate request file:



Signing Certificate request file:



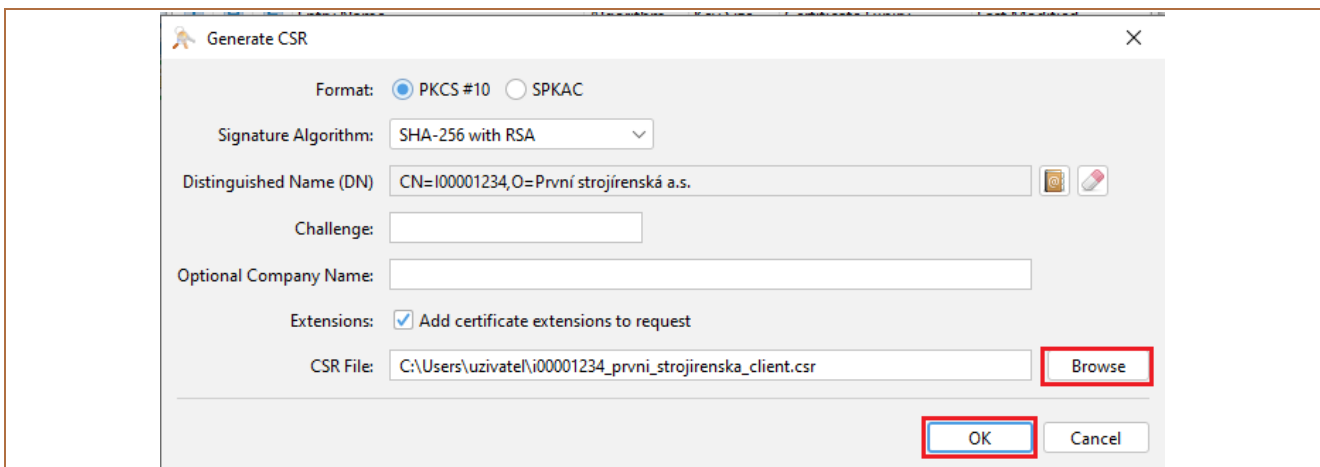
Right-click on this row and from the context menu select **Generate CSR**.



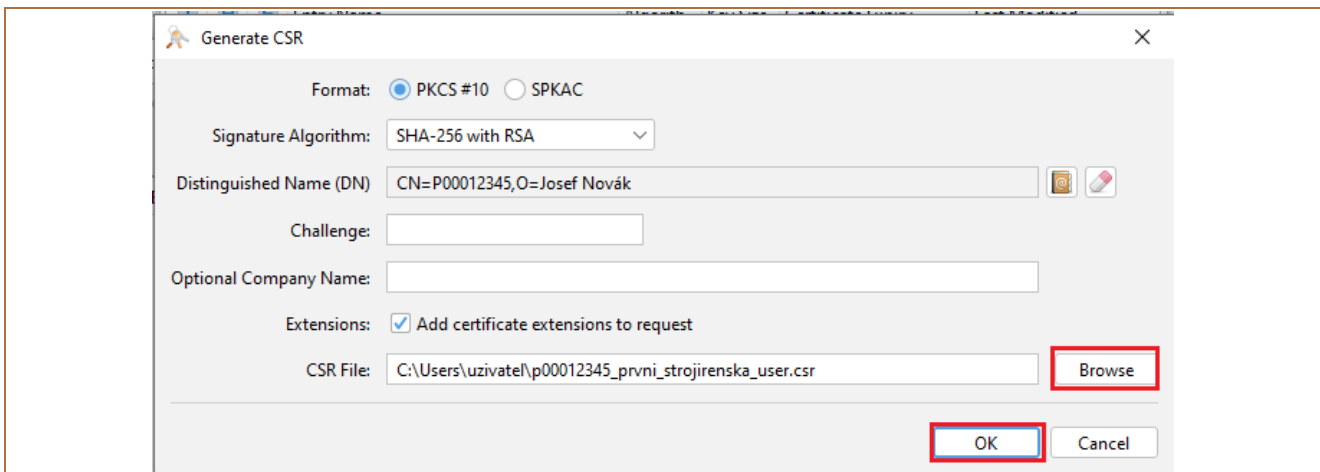
The details for generating the request will be displayed. Make sure the data is correct, and if necessary change the directory where the request will be saved by using the **Browse** button – **but do not change the file name**.

Confirm generation of the request with **OK**.

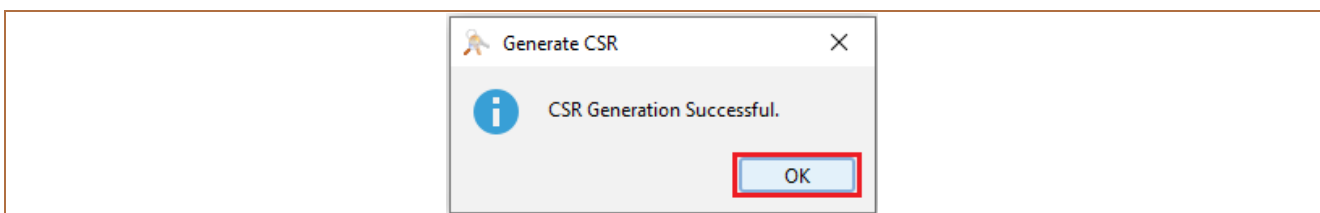
Generating a Client Certificate request:



Generating a Signing Certificate request:



A message is displayed, confirming the successful generation of a .csr file with the certificate request. Close the message with **OK**.



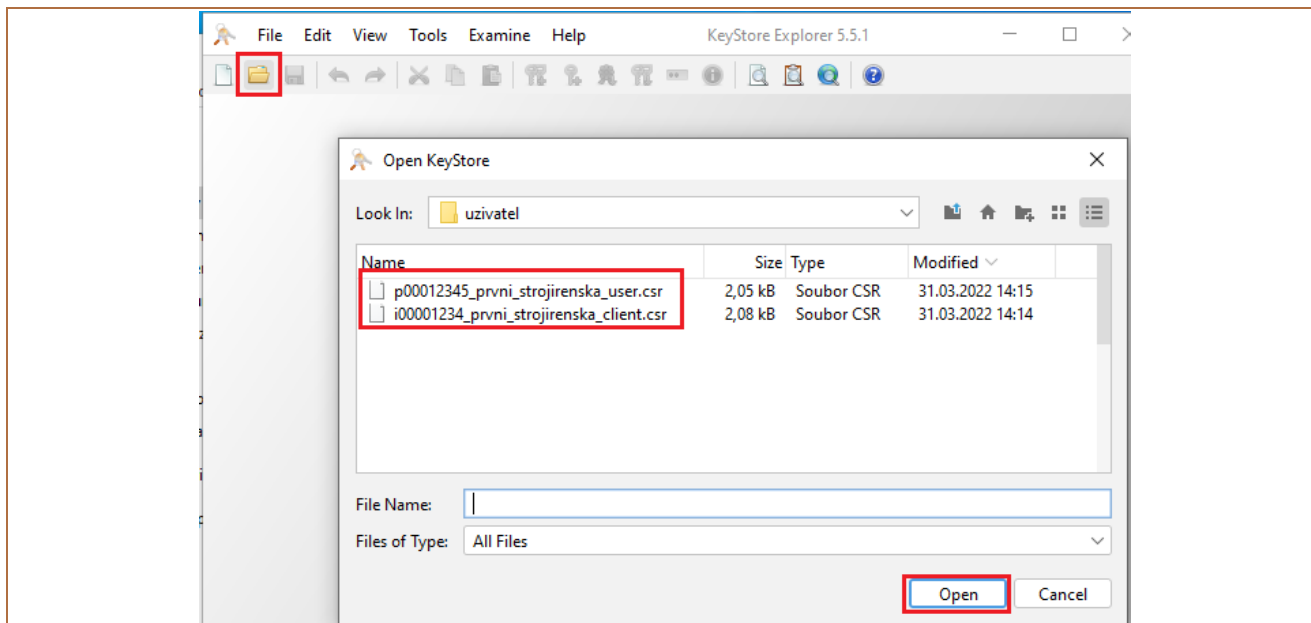
Then send the certificate request file(s) to the Bank in the required manner.

Close the application and save the generated requests – to save them, the application will require the password you entered when generating the files (see above).

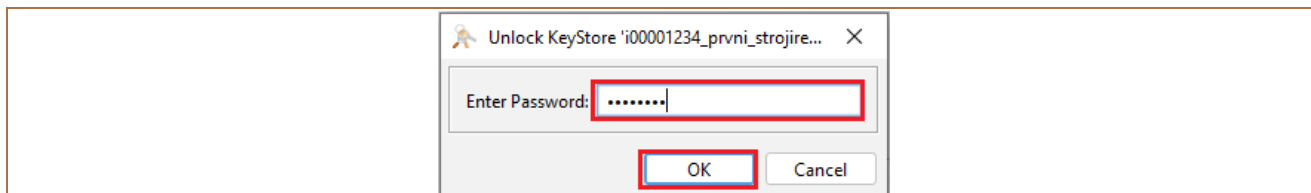
3 Importing certificate requests signed by the Bank

After processing your certificate requests, the Bank will send back new files with the .cer extension. Save these files in the directory you already created (see section 2), and then import them into KeyStore.

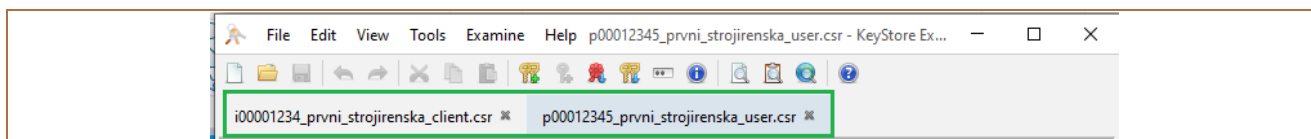
Click the **Open** icon and browse to the directory where you saved the .csr files.



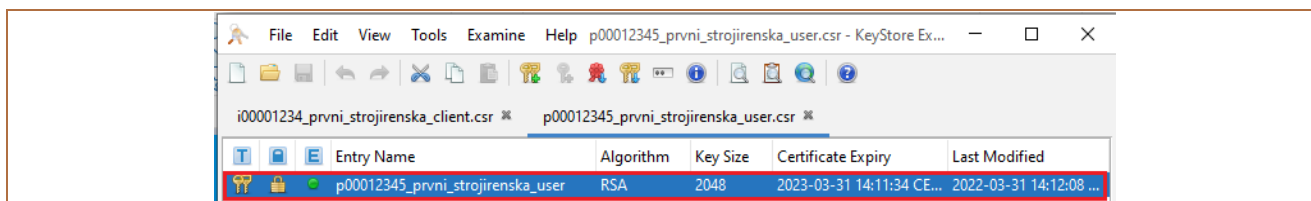
Open each of the two files. The system will request the password you entered when you generated the certificate request (see section 2). Enter the password in the **Enter Password** field and confirm with **OK**.



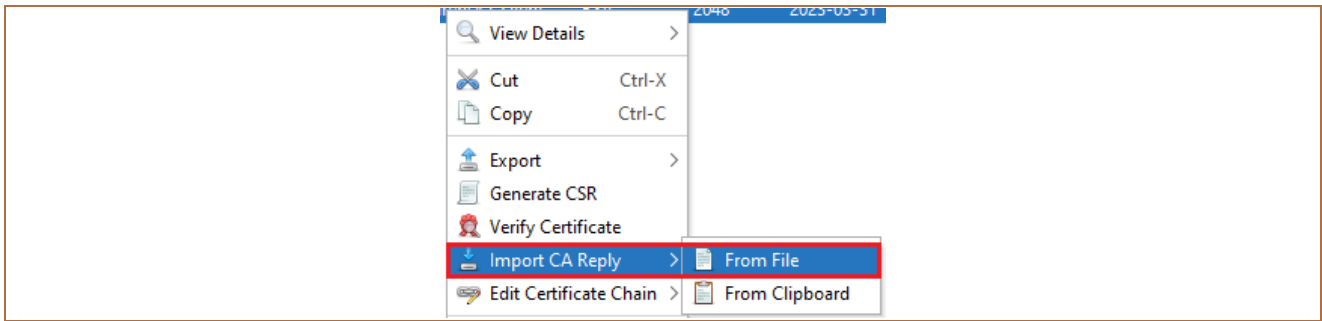
The certificate request files will open in separate windows.



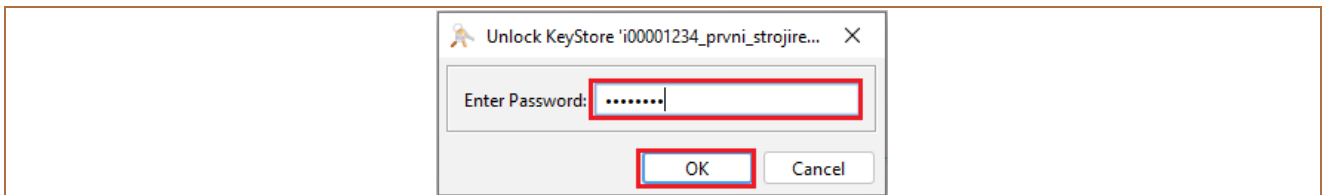
In the details view for one of the files, click on the row showing the certificate request.



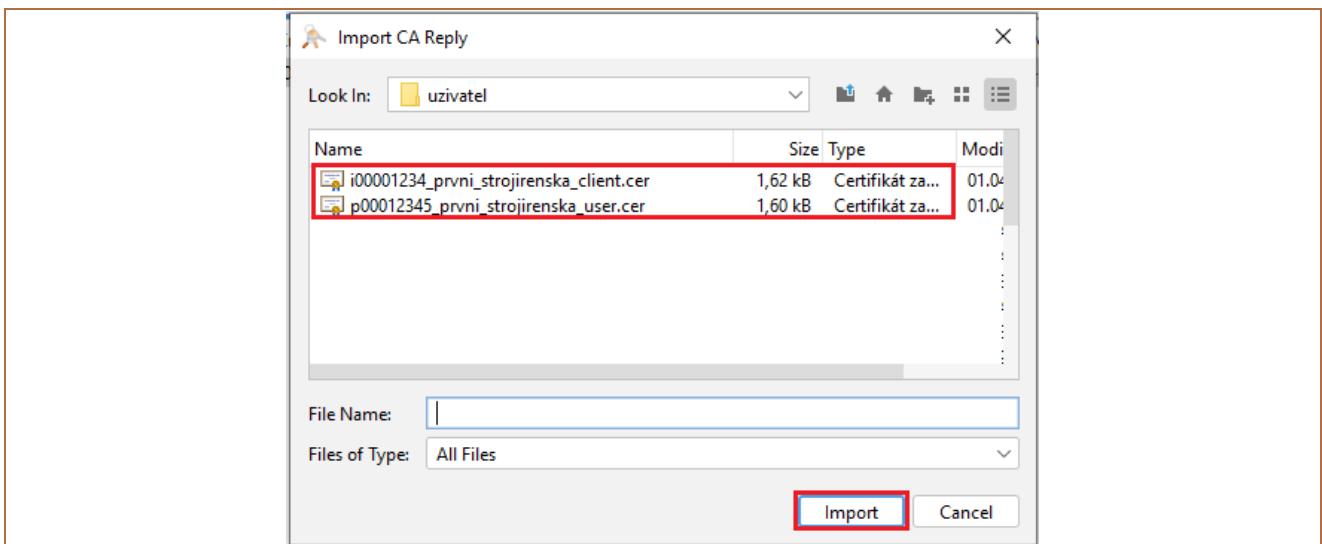
Right-click on this row and from the context menu choose **Import CA Replay** and **From File**.



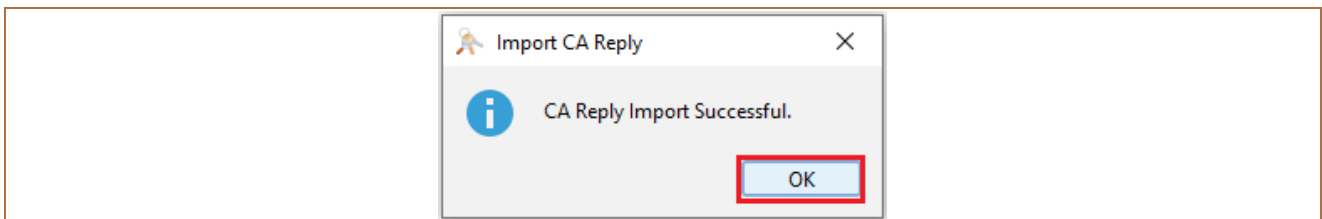
The system will request the password you entered when you generated the certificate request (see section 2). Enter the password in the **Enter Password** field and confirm with **OK**.



Select the file with the corresponding certificate request signed by the Bank, then click **Import**.



A message displays, confirming the successful import of a .cer file with a certificate request signed by the Bank. Close the message with **OK**.

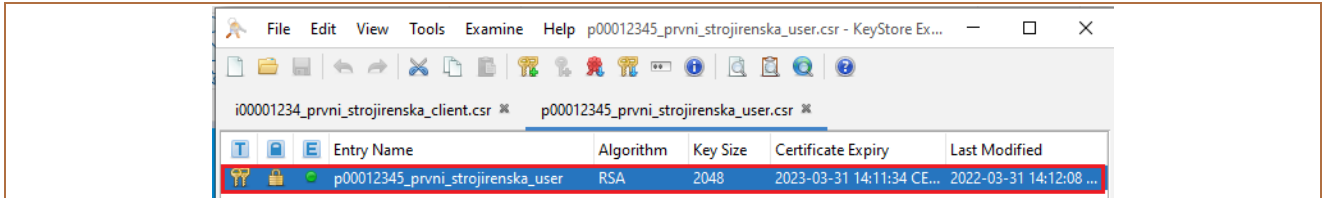


Repeat this procedure with the second file.

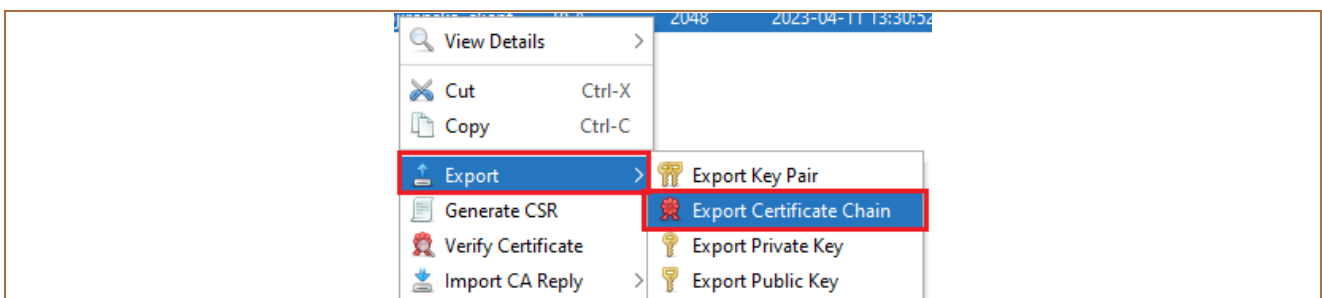
4 Exporting the full certificate

After successfully importing the certificate requests signed by the Bank, export the full certificates for use in the Client API.

In the details view for one of the open files (see section 3), click on the row showing the certificate request.



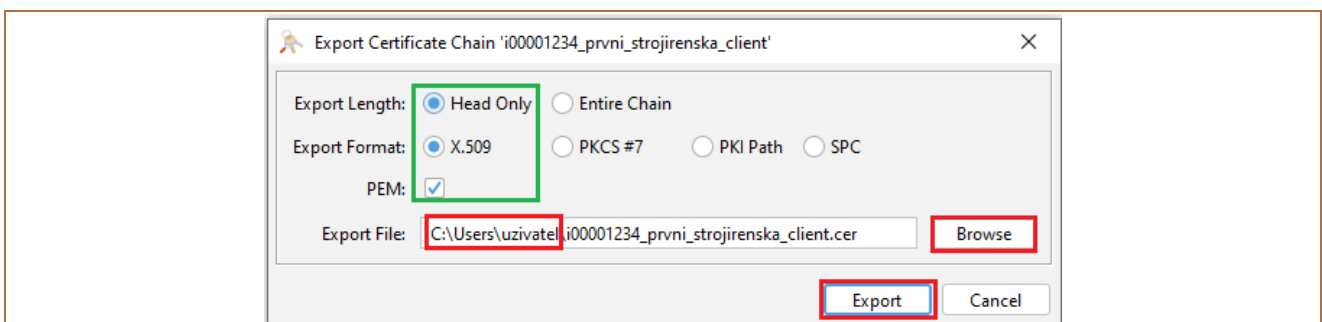
Right-click on this row and from the context menu choose **Export** and **Export Certificate Chain**.



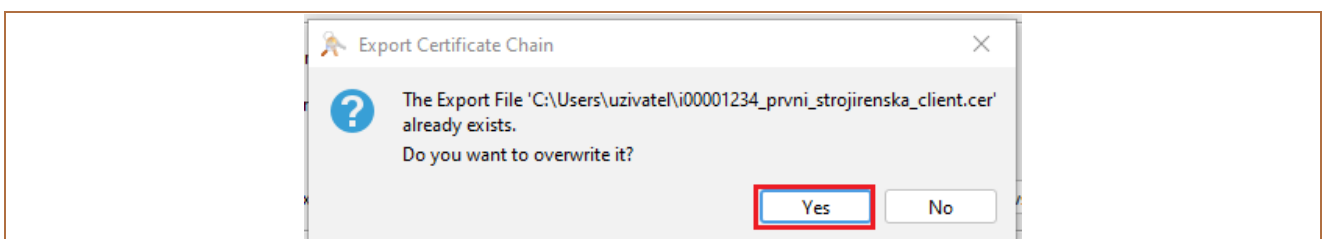
Select the following options for certificate generation:

Field	Data to be entered
Export Length:	Check Head Only
Export Format:	Check X.509
PEM:	Check this option
Export File:	Make sure the data is correct, and if necessary change the directory where the request will be saved by using the Browse button – but do not change the file name .

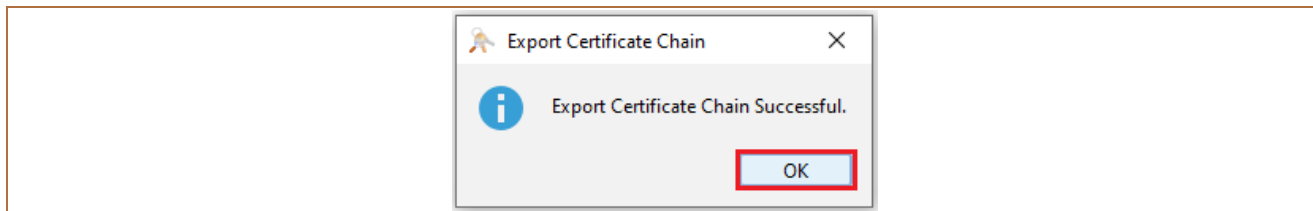
Confirm the export of the certificate with **Export**.



The system will display a warning that a file with this name already exists, and ask if you want to overwrite it – confirm using the **Yes** button.



A message confirming the successful export of the certificate will be displayed. Close the window with **OK**.



Repeat this procedure with the second file.

5 User support

User support for the Client API is provided by Customer Service. Contact details for Customer Service and its Business Hours can be found at [the Bank's website](#).