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

Contents:

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.

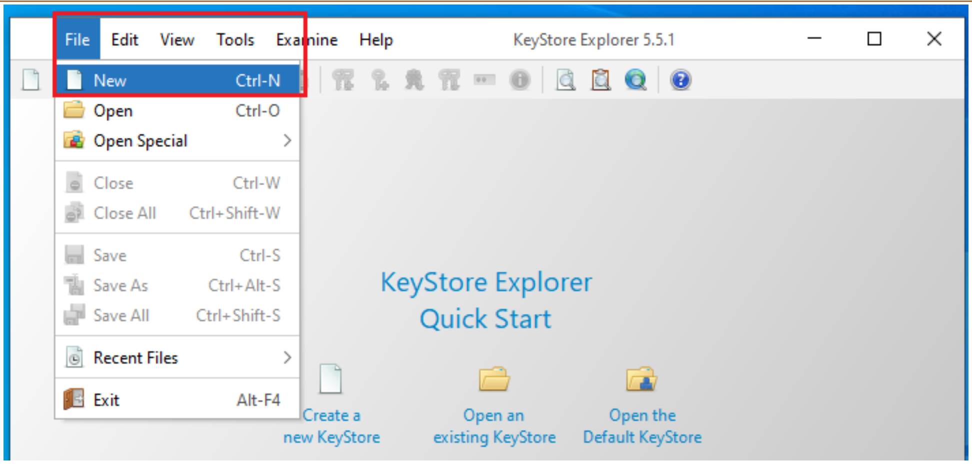
2.1 Entering identification data and choosing the type of keys

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

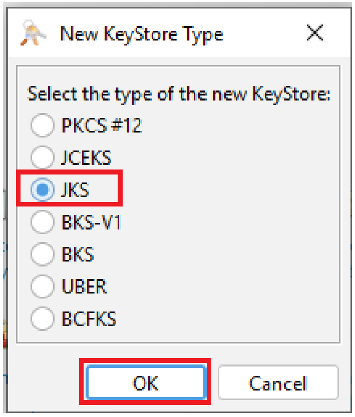
Examples of strings received from the Bank:

- 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**.

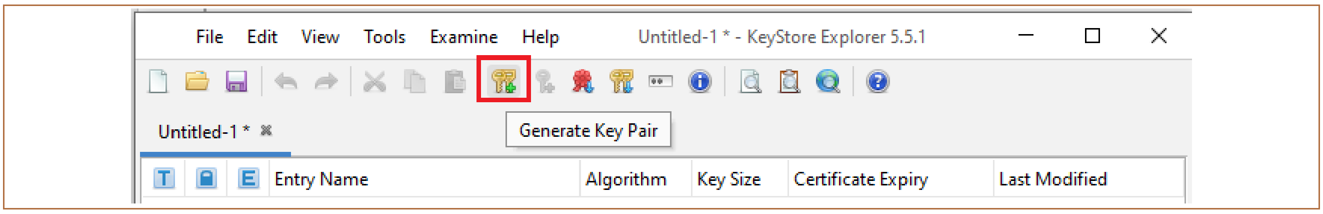


New KeyStore Type

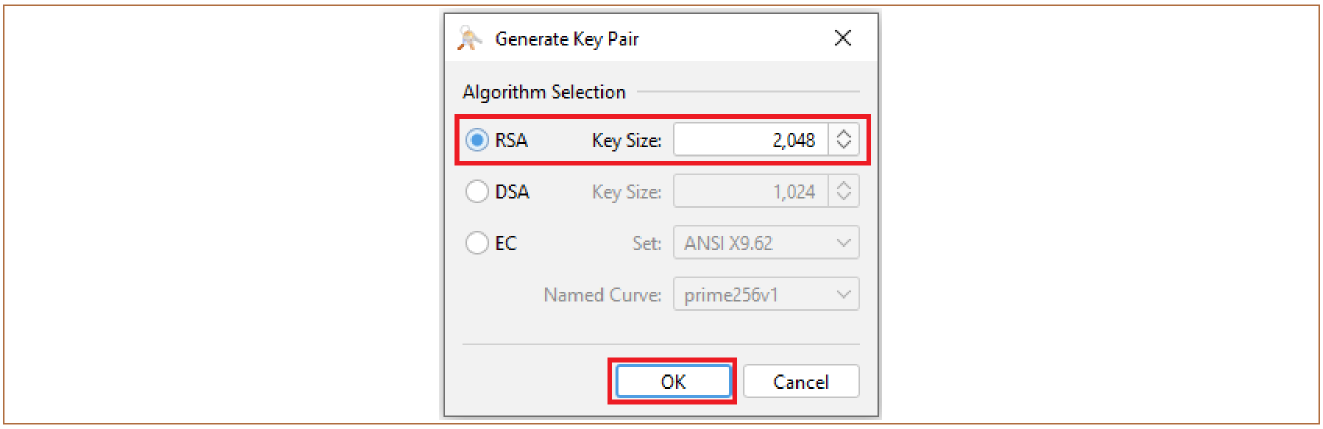
Select the type of the new KeyStore:

○ PKCS #12
○ JCEKS
● JKS
○ BKS-V1
○ BKS
○ UBER
○ BCFKS

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



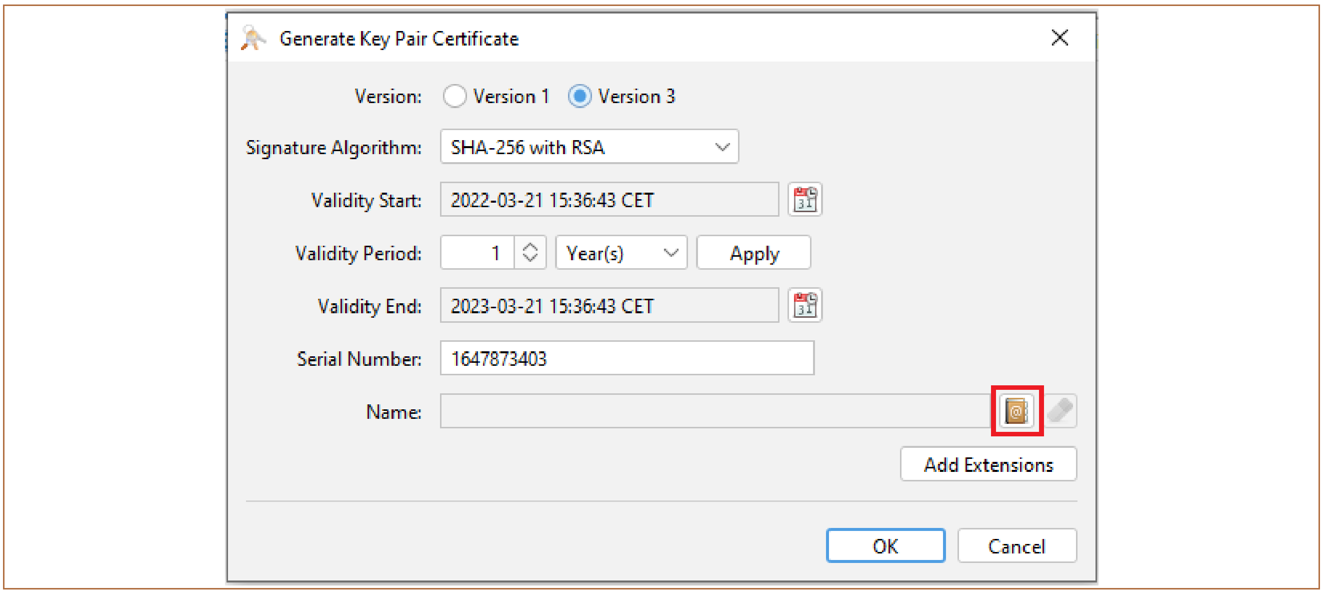
In the window that appears, select the **RSA** key type then confirm with **OK**.


Generate Key Pair

Algorithm Selection

- ● RSA Key Size: 2,048
- ○ DSA Key Size: 1,024
- ○ EC Set: ANSI X9.62
- Named Curve: prime256v1

In the next window, click on the book icon.


Generate Key Pair Certificate

Version: ○ Version 1 ● Version 3

Signature Algorithm: SHA-256 with RSA

Validity Start: 2022-03-21 15:36:43 CET

Validity Period: 1 Year(s) Apply

Validity End: 2023-03-21 15:36:43 CET

Serial Number: 1647873403

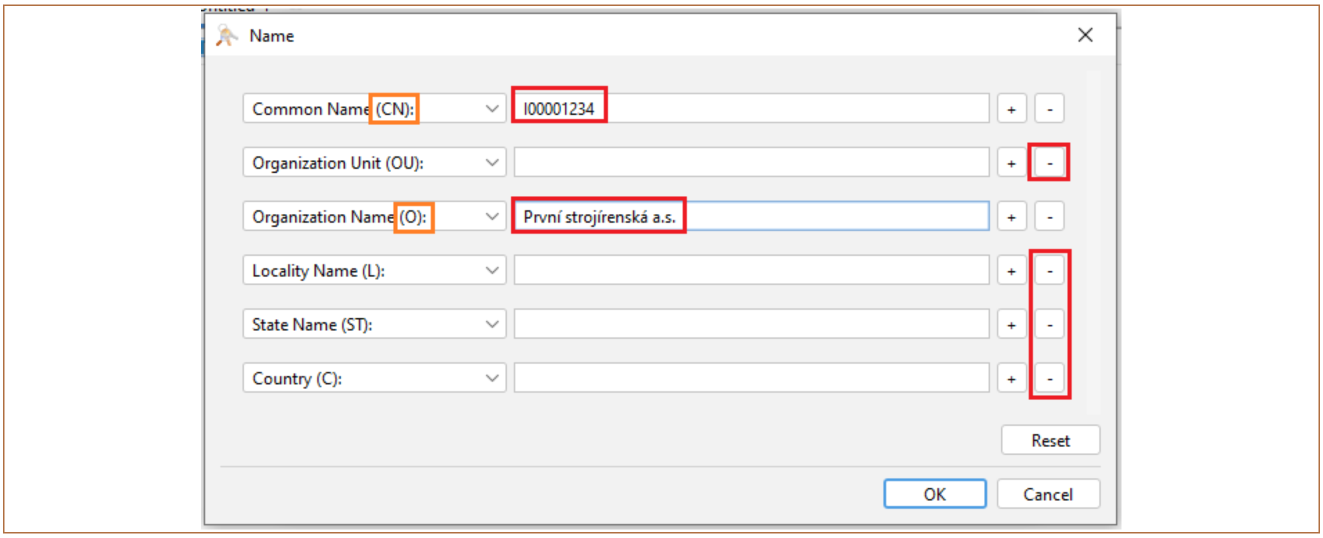
Name:

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**”: • for a Client Certificate: ○ received string: openssl req -new -newkey rsa:2048 -nodes -out Client_cert.csr -keyout Client_cert.key -subj "/O=První strojírenská a.s./CN=**I00001234**" ○ this data starts with the letter **I** – e.g. **I00001234** • for a Signing Certificate: ○ received string: openssl req -new -newkey rsa:2048 -nodes -out User_cert.csr -keyout User_cert.key -subj "/O=Josef Novák/CN=**P00012345**" ○ this data starts with the letter **P** – e.g. **P00012345**

Field	Data to be entered
Organization Name (O):	Enter the data from the string that follows the element “**O**”: • 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 with the minus button at the end of the field.



Common Name (CN): I00001234

Organization Unit (OU):

Organization Name (O): První strojírenská a.s.

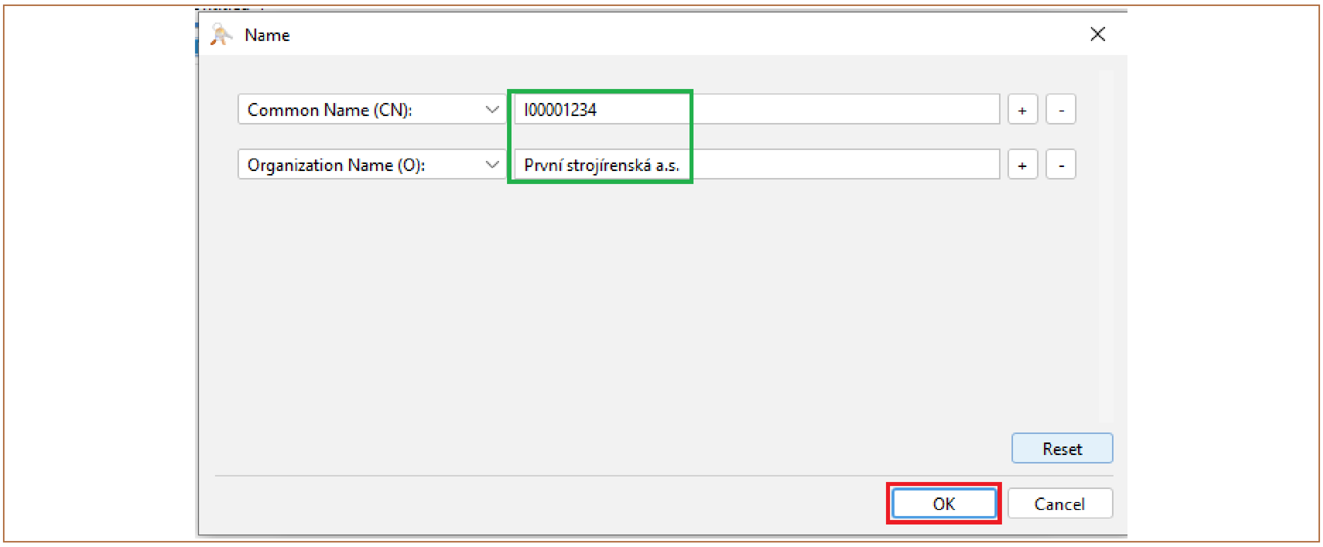
Locality Name (L):

State Name (ST):

Country (C):

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**"

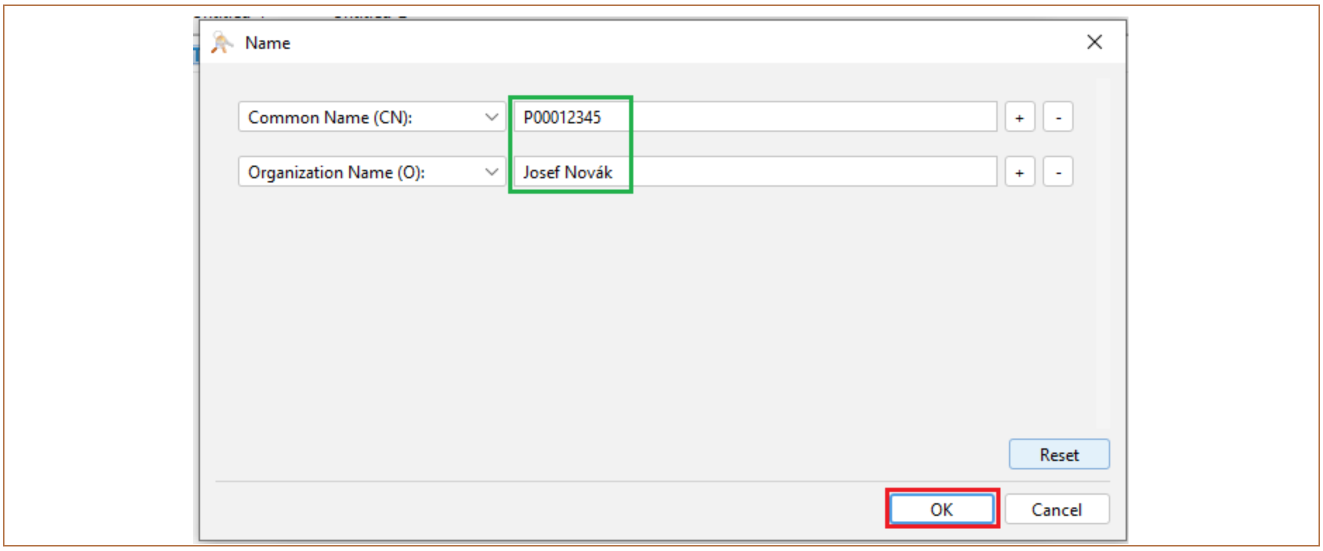


Common Name (CN): I00001234

Organization Name (O): První strojírenská a.s.

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**"

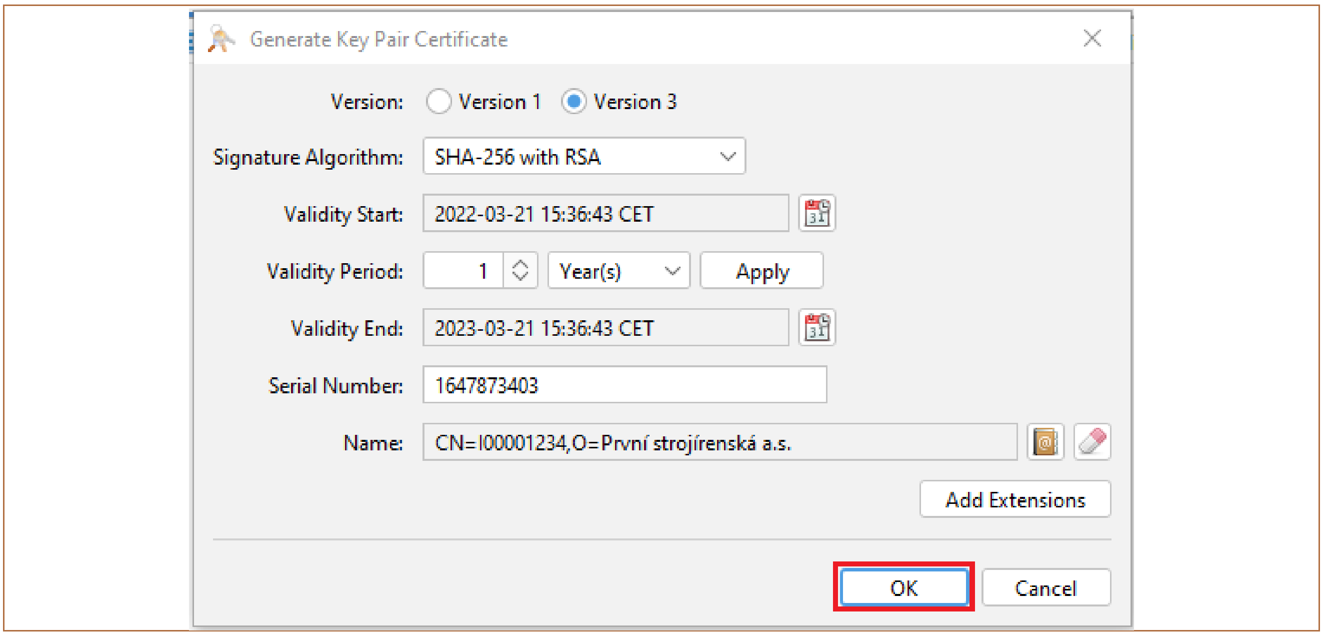


Name

Common Name (CN): P00012345

Organization Name (O): Josef Novák

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



Generate Key Pair Certificate

Version: ○ Version 1 ● Version 3

Signature Algorithm: SHA-256 with RSA

Validity Start: 2022-03-21 15:36:43 CET

Validity Period: 1 Year(s)

Validity End: 2023-03-21 15:36:43 CET

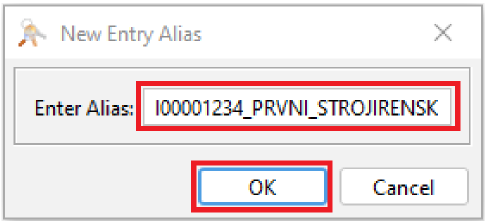
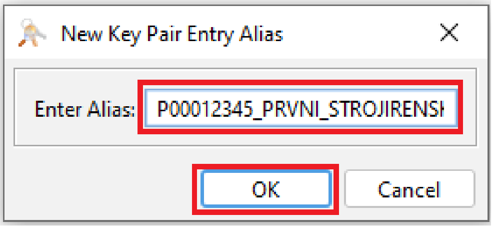
Serial Number: 1647873403

Name: CN=I00001234,O=První strojírenská a.s.

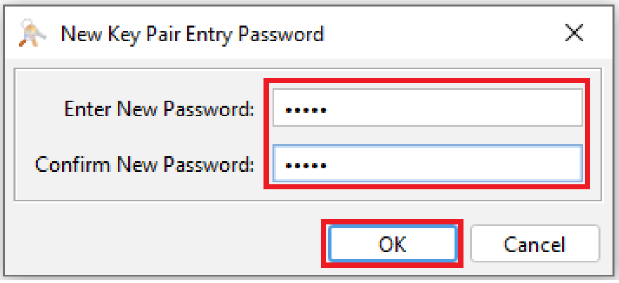
A window will appear for you to enter a name (alias) for the file. The data from the field **Common Name (CN)** will be automatically pre-populated here. Complete the name using the following format:

- 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**:

Client Certificate	Signing Certificate
 New Entry Alias Enter Alias: I00001234_PRVNI_STROJIRENSK OK Cancel	 New Key Pair Entry Alias Enter Alias: P00012345_PRVNI_STROJIRENSI OK Cancel

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

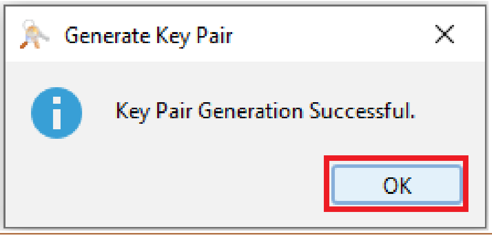


Enter New Password: •••••

Confirm New Password: •••••

A message will be displayed confirming that the keys have been successfully generated

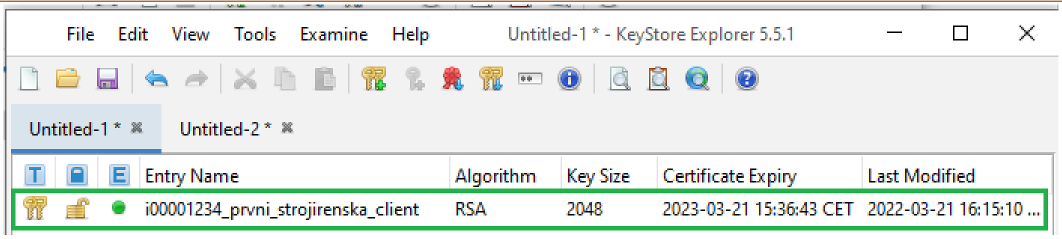
– confirm again with **OK.**



Key Pair Generation Successful.

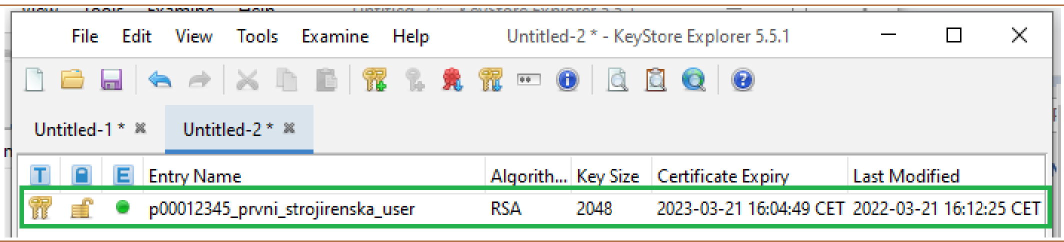
The generated file will appear in the application window:

Client Certificate request file:



T		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
		●	i00001234_prvni_strojirenska_client	RSA	2048	2023-03-21 15:36:43 CET	2022-03-21 16:15:10 ...

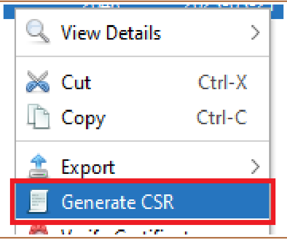
Signing Certificate request file:



T		E	Entry Name	Algorith...	Key Size	Certificate Expiry	Last Modified
		●	p00012345_prvni_strojirenska_user	RSA	2048	2023-03-21 16:04:49 CET	2022-03-21 16:12:25 CET

2.2 Generating and saving .csr files with the certificate request

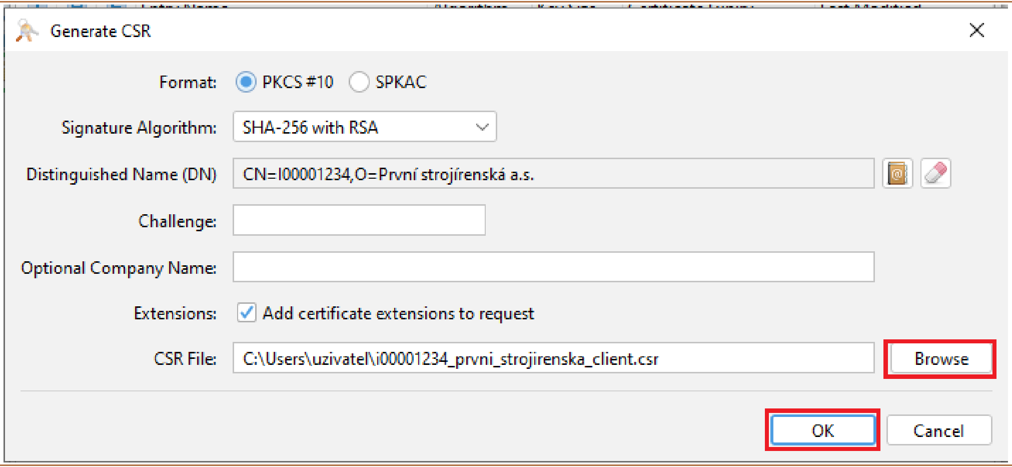
Then click the right mouse button on row with the file and from the context menu select **Generate CSR**.



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 and saving of the request with **OK**.

Generating a Client Certificate request:



Generate CSR

Format: ● PKCS #10 ○ SPKAC

Signature Algorithm: SHA-256 with RSA

Distinguished Name (DN): CN=I00001234,O=První strojírenská a.s.

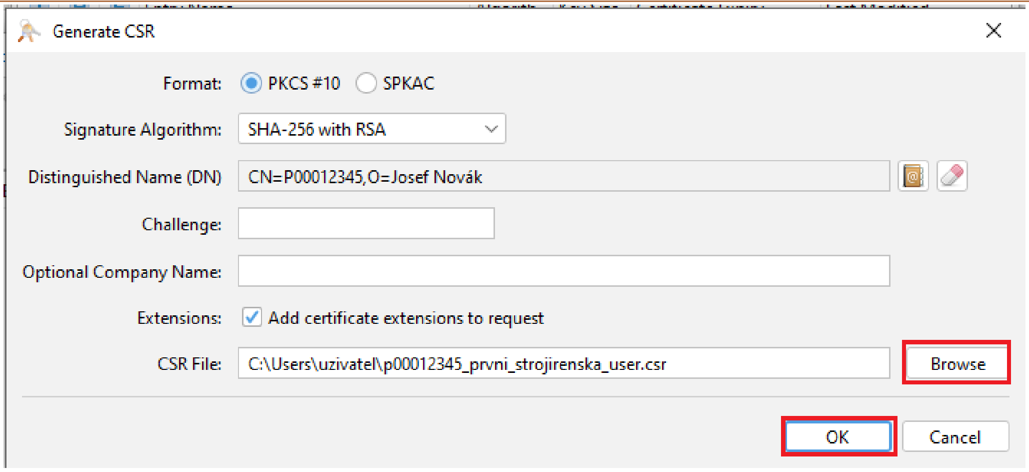
Challenge:

Optional Company Name:

Extensions: ☑ Add certificate extensions to request

CSR File: C:\Users\uzivatel\i00001234_prvni_strojirenska_client.csr

Generating a Signing Certificate request:



Generate CSR

Format: ● PKCS #10 ○ SPKAC

Signature Algorithm: SHA-256 with RSA

Distinguished Name (DN): CN=P00012345,O=Josef Novák

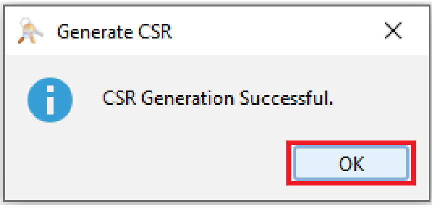
Challenge:

Optional Company Name:

Extensions: ☑ Add certificate extensions to request

CSR File: C:\Users\uzivatel\p00012345_prvni_strojirenska_user.csr

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



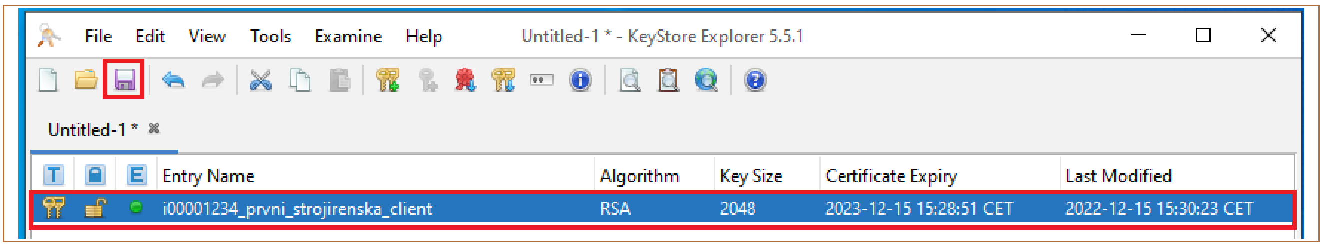
Generate CSR

CSR Generation Successful.

2.3 Saving files with the extension .jks

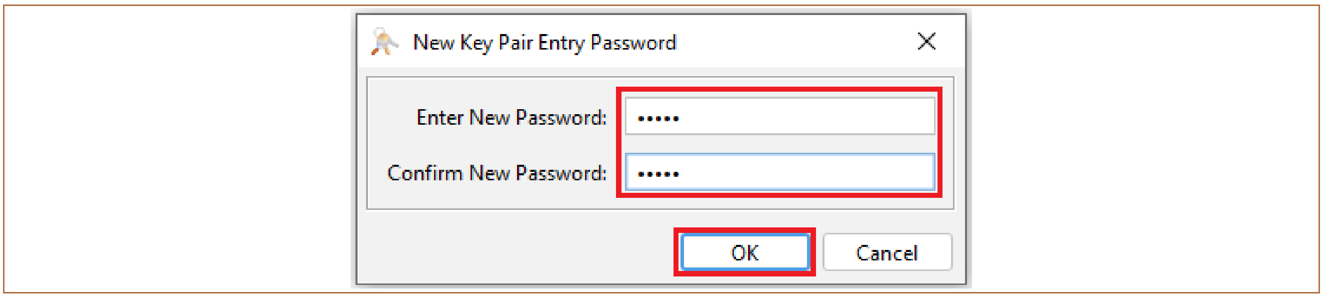
Save the generated files.

Click on the line with the file and then on the **Save** icon.



T		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
		●	i00001234_prvni_strojirenska_client	RSA	2048	2023-12-15 15:28:51 CET	2022-12-15 15:30:23 CET

The application prompts you to enter the password for the file – enter the password set in point 2.1 when generating the files, confirm the entry with the **OK** button.



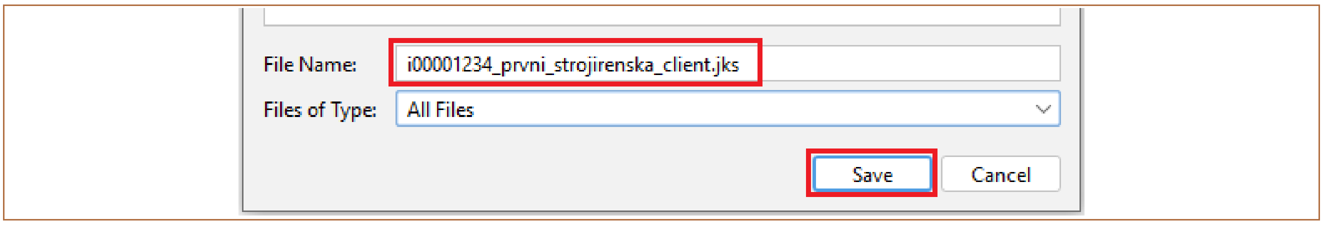
New Key Pair Entry Password

Enter New Password: •••••

Confirm New Password: •••••

The directory where you saved the .csr files during generation will open. Save the file with the same name but with the extension .jks. Confirm the save with the **Save** button.

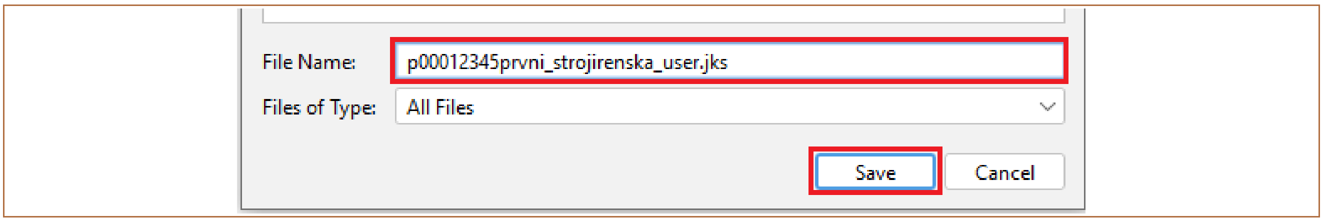
Client certificate request file:



File Name: i00001234_prvni_strojirenska_client.jks

Files of Type: All Files

Signing certificate request file:



File Name: p00012345prvni_strojirenska_user.jks

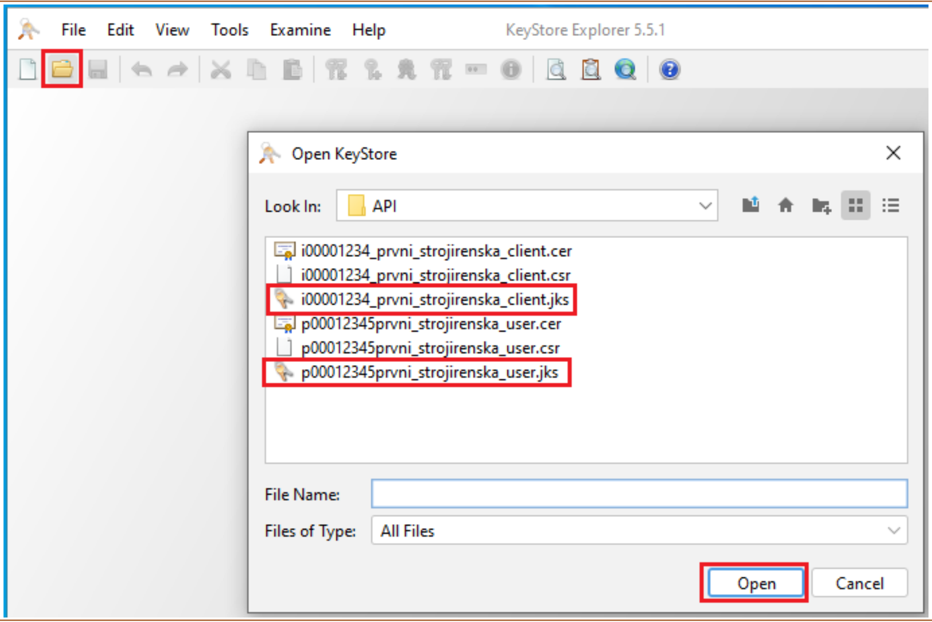
Files of Type: All Files

Then send file or files with extension .csr with a request to generate certificate to the Bank via message in Internet banking.

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 .jks files.



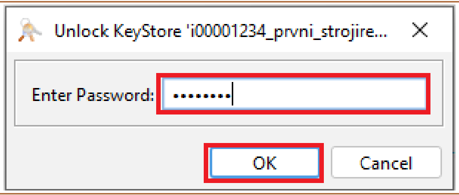
Look In: API

i00001234_prvni_strojirenska_client.cer
i00001234_prvni_strojirenska_client.csr
i00001234_prvni_strojirenska_client.jks
p00012345prvni_strojirenska_user.cer
p00012345prvni_strojirenska_user.csr
p00012345prvni_strojirenska_user.jks

File Name:

Files of Type: All Files

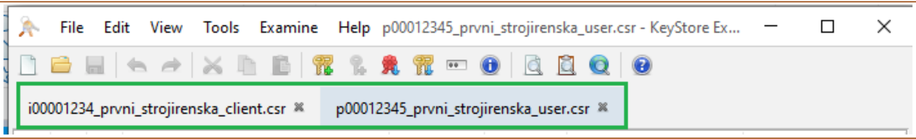
Open each of the two files. The system will request the password you entered when you generated the certificate request (see section 2.1). Enter the password in the **Enter Password** field and confirm with **OK**.



Unlock KeyStore 'i00001234_prvni_strojire...

Enter Password: ••••••••

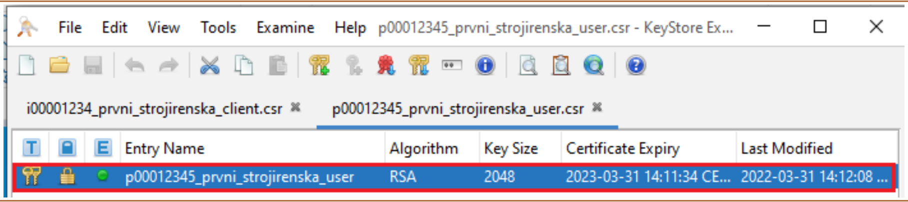
The files will open in separate windows.



p00012345_prvni_strojirenska_user.csr - KeyStore Ex...

i00001234_prvni_strojirenska_client.csr ✖ p00012345_prvni_strojirenska_user.csr ✖

Click on the row with the file.

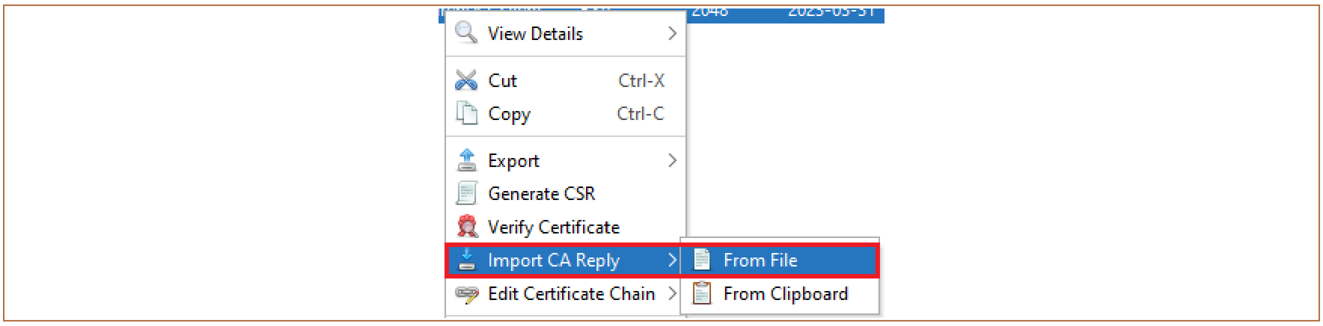


p00012345_prvni_strojirenska_user.csr - KeyStore Ex...

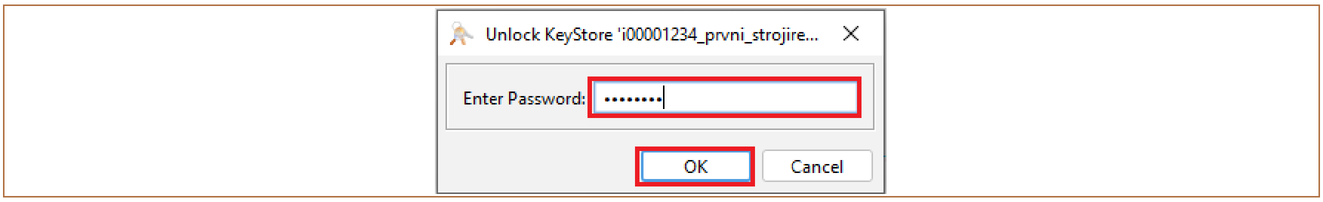
i00001234_prvni_strojirenska_client.csr ✖ p00012345_prvni_strojirenska_user.csr ✖

T		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
		●	p00012345_prvni_strojirenska_user	RSA	2048	2023-03-31 14:11:34 CE...	2022-03-31 14:12:08 ...

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

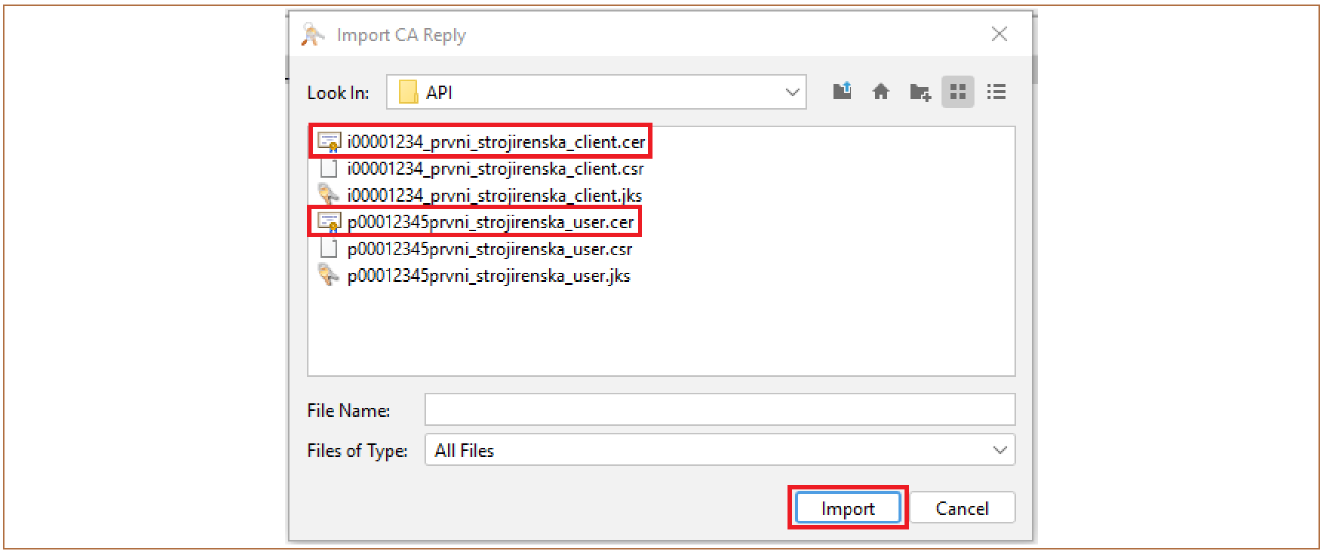


The system will request the password you entered when you generated the certificate request (see section 2.1). Enter the password in the **Enter Password** field and confirm with **OK**.


Unlock KeyStore 'i00001234_prvni_strojire...

Enter Password: ••••••••

Select the corresponding .cer file, then click on the **Import** button.


Import CA Reply

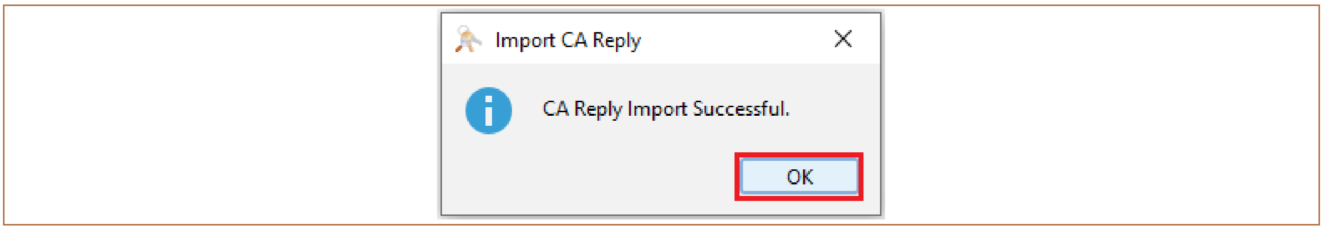
Look In: API

i00001234_prvni_strojirenska_client.cer
i00001234_prvni_strojirenska_client.csr
i00001234_prvni_strojirenska_client.jks
p00012345prvni_strojirenska_user.cer
p00012345prvni_strojirenska_user.csr
p00012345prvni_strojirenska_user.jks

File Name:

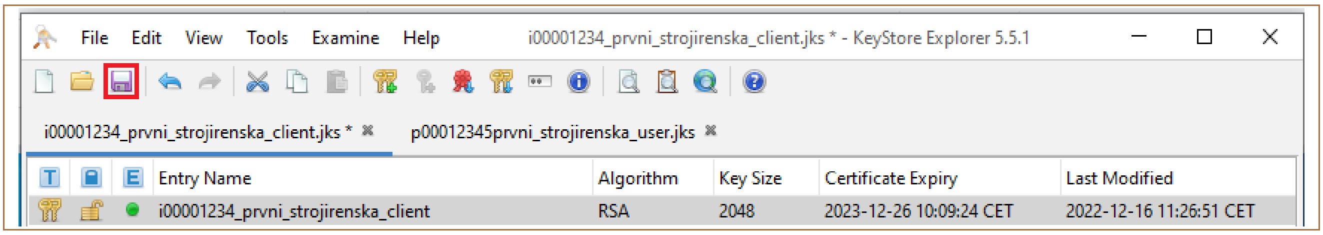
Files of Type: All Files

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


Import CA Reply

CA Reply Import Successful.

Then click on the line with the file and on the **Save** icon.


i00001234_prvni_strojirenska_client.jks * - KeyStore Explorer 5.5.1

File
Edit
View
Tools
Examine
Help
i00001234_prvni_strojirenska_client.jks *
p00012345prvni_strojirenska_user.jks

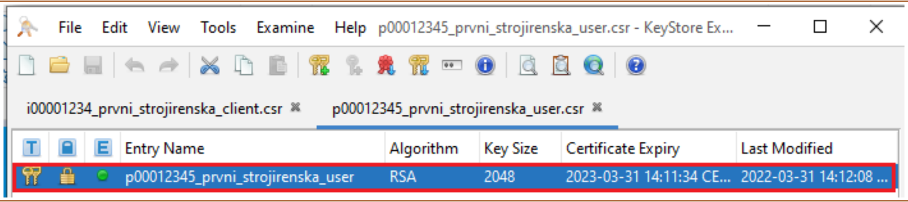
T		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
		●	i00001234_prvni_strojirenska_client	RSA	2048	2023-12-26 10:09:24 CET	2022-12-16 11:26:51 CET

Repeat this procedure with the second file.

4 Exporting keys for communication with the Client API

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

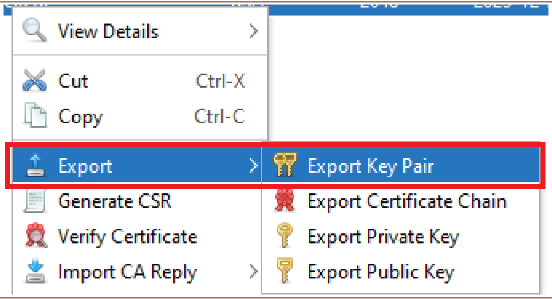
In the details view for one of the open files (see section 3), click on the row showing the certificate request.



File
Edit
View
Tools
Examine
Help
p00012345_prvni_strojirenska_user.csr - KeyStore Ex...
i00001234_prvni_strojirenska_client.csr
p00012345_prvni_strojirenska_user.csr

T	🔒	E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
			p00012345_prvni_strojirenska_user	RSA	2048	2023-03-31 14:11:34 CE...	2022-03-31 14:12:08 ...

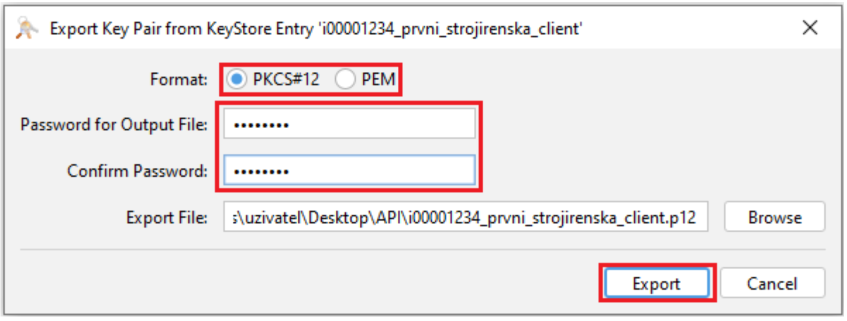
Right-click on this row and from the context menu choose **Export** and **Export Key Pair**.



Select the following options for keys generation:

Field	Data to be entered
Format:	Select PKCS#12 or PEM format according to your system settings.
Password for Output File:	Enter the password for the file used when generating the request (see point 2.1).
Confirm Password	Confirm the entered password.
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 – **<u>but do not change the file name</u>**.

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



Export Key Pair from KeyStore Entry 'i00001234_prvni_strojirenska_client'

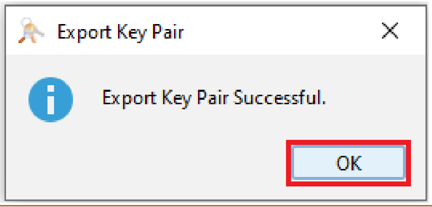
Format: ● PKCS#12 ○ PEM

Password for Output File: ••••••••

Confirm Password: ••••••••

Export File: :\uzivatel\Desktop\API\i00001234_prvni_strojirenska_client.p12

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



Export Key Pair

Export Key Pair Successful.

Repeat this procedure with the second file.

Then upload the files with the keys to your system, through which you will communicate with the Client API.

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.