NÁVOD NA GENEROVÁNÍ ŽÁDOSTÍ O CERTIFIKÁTY PRO KLIENTSKÉ API PPF BANKY A.S. VE WINDOWS

Obsah:

1 Instalace aplikace KeyStore Explorer

Pro generování žádostí o certifikáty ke Klientskému API si nejdříve nainstalujte aplikaci KeyStore Explorer (oficiální stránky: www.keystore-explorer.org).

2 Vygenerování žádosti o certifikát

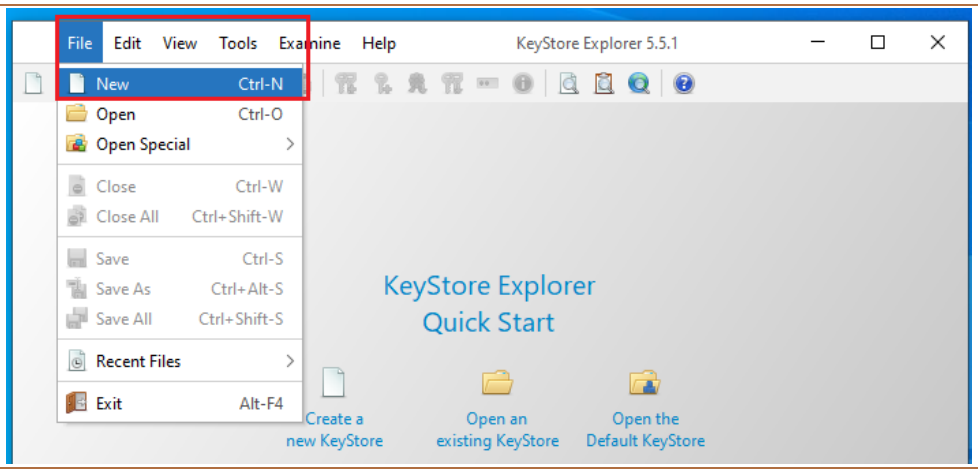
Postup je stejný jak pro generování žádosti o vystavení Klientského certifikátu, tak pro generování žádosti o vystavení Podpisového certifikátu. Rozdíl je pouze v zadávaných údajích.

Pro vygenerování žádostí o certifikáty budete potřebovat stringy, které vám zaslala PPF banka a.s. (dále jen „Banka“).

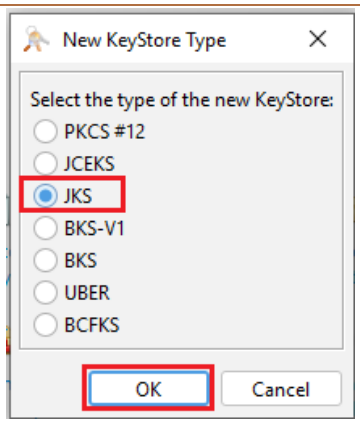
Příklad obdržených stringů:

- string pro Klientský certifikát: openssl req -new -newkey rsa:2048 -nodes -out Client_cert.csr -keyout Client_cert.key -subj "/O=První strojírenská a.s./CN=I00001234"
- string pro Podpisový certifikát: openssl req -new -newkey rsa:2048 -nodes -out User_cert.csr -keyout User_cert.key -subj "/O=Josef Novák/CN=P00012345"

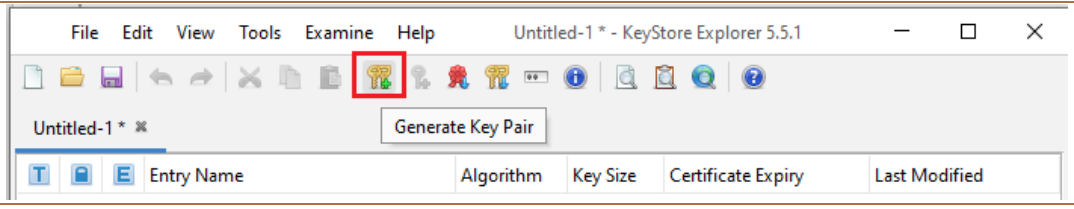
Pro vygenerování žádosti o certifikát klikněte na volby **File** a **New**.



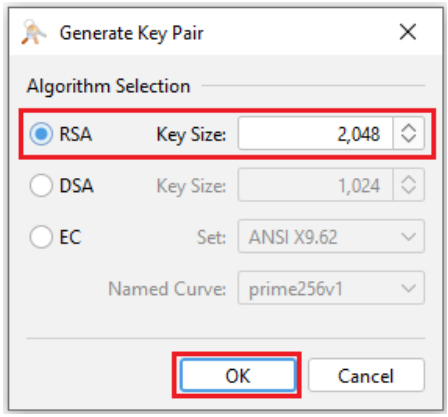
Zobrazí se okno pro výběr typu souboru – vyberte **JKS** a potvrďte tlačítkem **OK**.



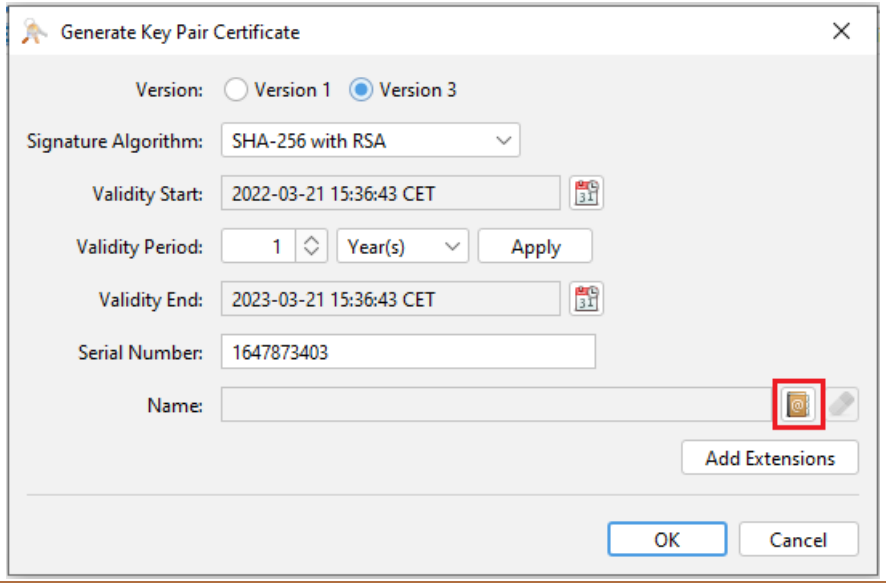
Následně v řádku nástrojů klikněte na ikonku s klíči a zeleným plus (Generate Key Pair).



V zobrazeném okně vyberte typ klíčů **RSA** a potvrďte tlačítkem **OK**.



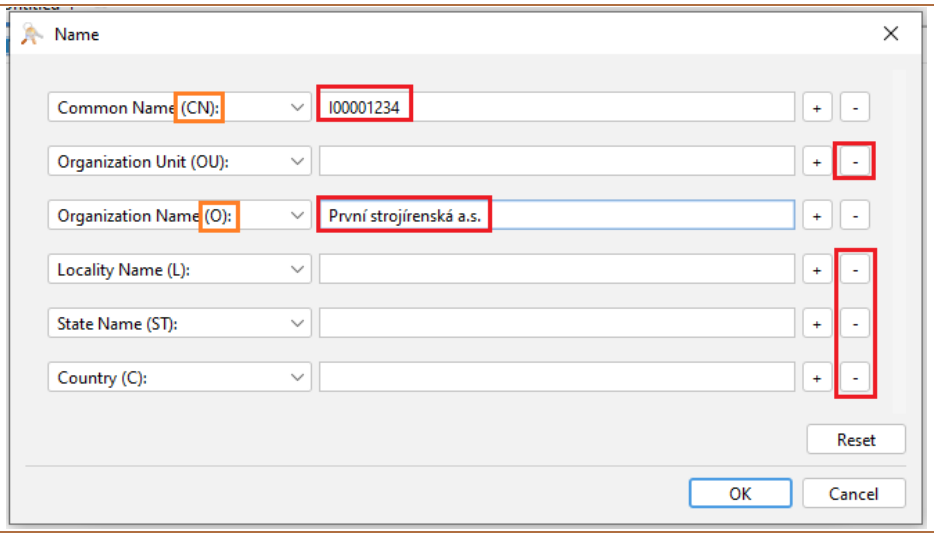
V následujícím okně klikněte na ikonku knížky.



Vyplňte identifikační údaje ze stringu obdrženého od Banky následovně:

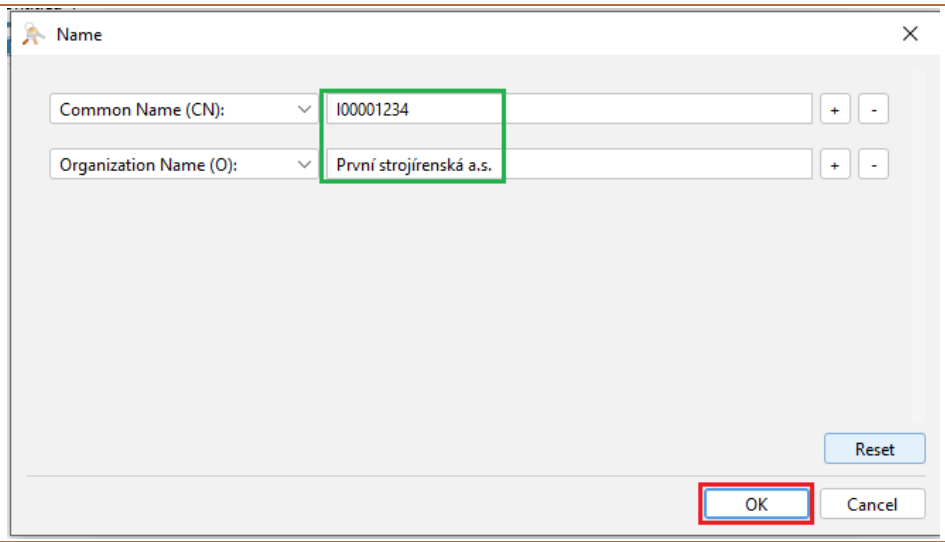
Pole	Vyplňované údaje
Common name (CN):	Uveďte údaj ze stringu za elementem CN: • pro Klientský certifikát údaj začíná písmenem **I** – např. I00001234 • pro Podpisový certifikát údaj začíná písmenem **P** – např. P00012345
Organization name (O):	Uveďte údaj ze stringu za elementem O: • pro Klientský certifikát se jedná o název klienta – např. První strojírenská a.s. • pro Podpisový certifikát se jedná o jméno a příjmení Uživatele API – např. Josef Novák

Ostatní pole odstraňte.



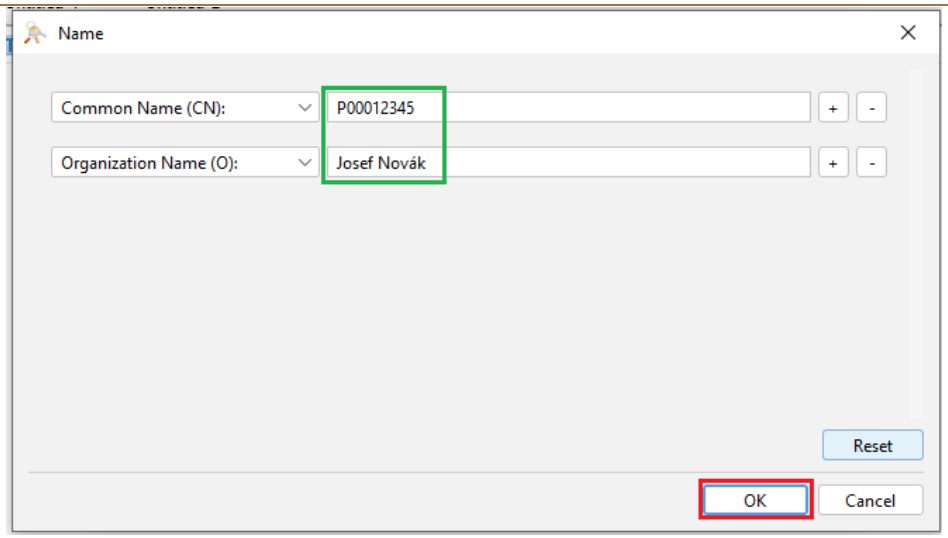
Příklad zadání pro žádost o Klientský certifikát:

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

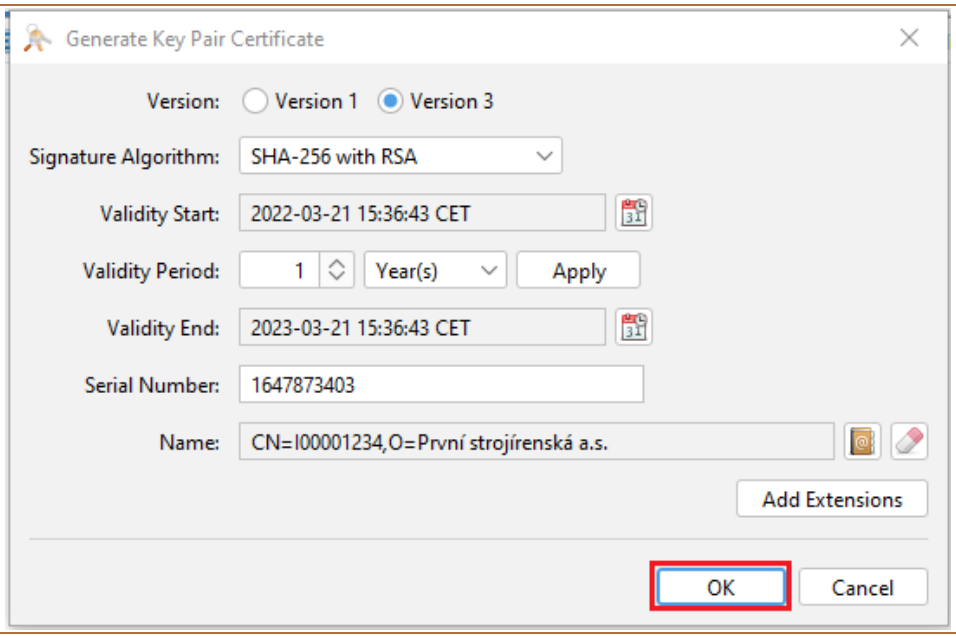


Příklad zadání pro žádost o Podpisový certifikát:

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



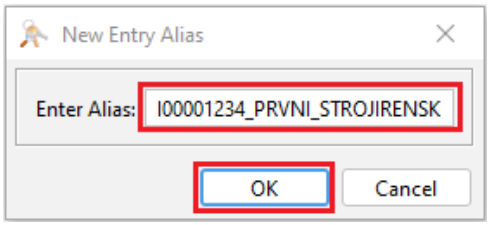
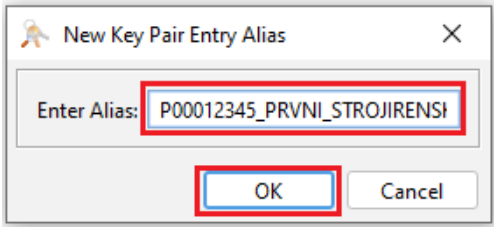
Zadání potvrďte tlačítkem **OK** a na další obrazovce opět klikněte na tlačítko **OK**.



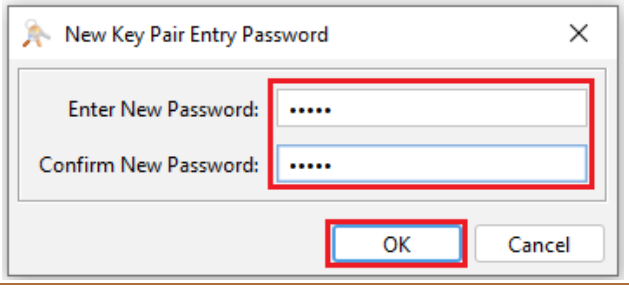
Zobrazí se okno pro zadání názvu souboru, ve kterém je předvyplněný údaj z pole **Common name (CN)**. Název doplňte následovně:

- soubor se žádostí o Klientský certifikát:
  - INNNNNNNN_NAZEV_KLIENTA_CLIENT, kde:
    - INNNNNNNN = údaj z pole **Common name (CN)** následovaný podtržítkem,
    - NAZEV_KLIENTA = název klienta bez diakritiky, místo mezer je nutné uvést podtržítka,
    - _CLIENT = označení, že se jedná o žádost o Klientský certifikát,
    - příklad: I00001234_PRVNI_STROJIRENSKA_CLIENT;
- soubor se žádostí o Podpisový certifikát:
  - PNNNNNNNN_NAZEV_KLIENTA_USER, kde:
    - PNNNNNNNN = údaj z pole **Common name (CN)** následovaný podtržítkem,
    - NAZEV_KLIENTA = název klienta bez diakritiky, místo mezer je nutné uvést podtržítka,
    - _USER = označení, že se jedná o žádost o Podpisový certifikát;
    - příklad: P00012345_PRVNI_STROJIRENSKA_USER.

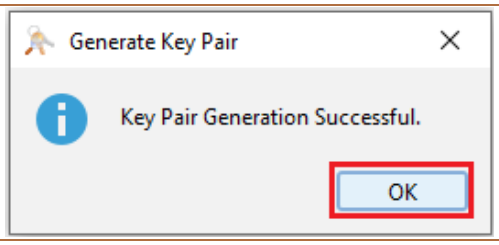
Příklad vyplnění názvu souboru – zadání potvrďte tlačítkem **OK**:

Klientský certifikát	Podpisový certifikát
	

Aplikace vás následně vyzve k zadání hesla k souboru – zadávané heslo si zapamatujte nebo uložte, zadání potvrďte tlačítkem **OK**.

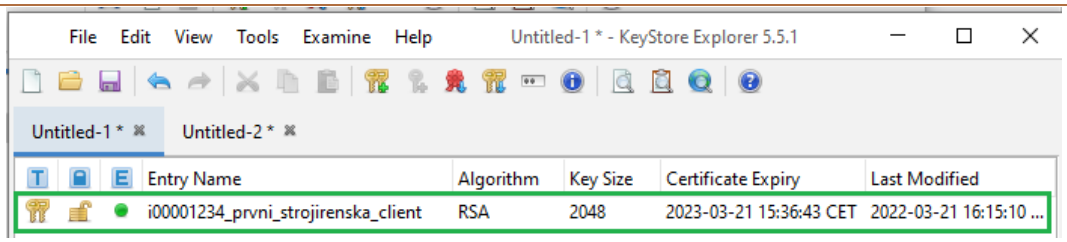


Zobrazí se zpráva o úspěšném vygenerování klíčů – opět potvrďte tlačítkem **OK**.

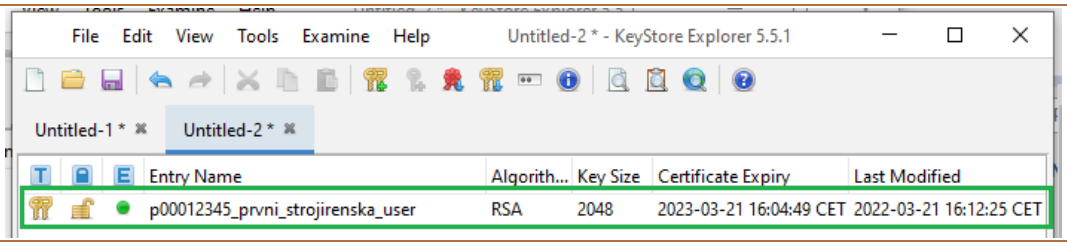


Vygenerovaný soubor se zobrazí v aplikaci:

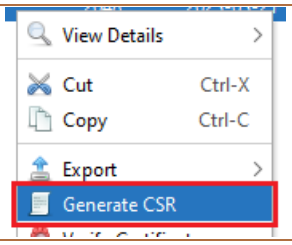
Soubor se žádostí o Klientský certifikát:



Soubor se žádostí o Podpisový certifikát:



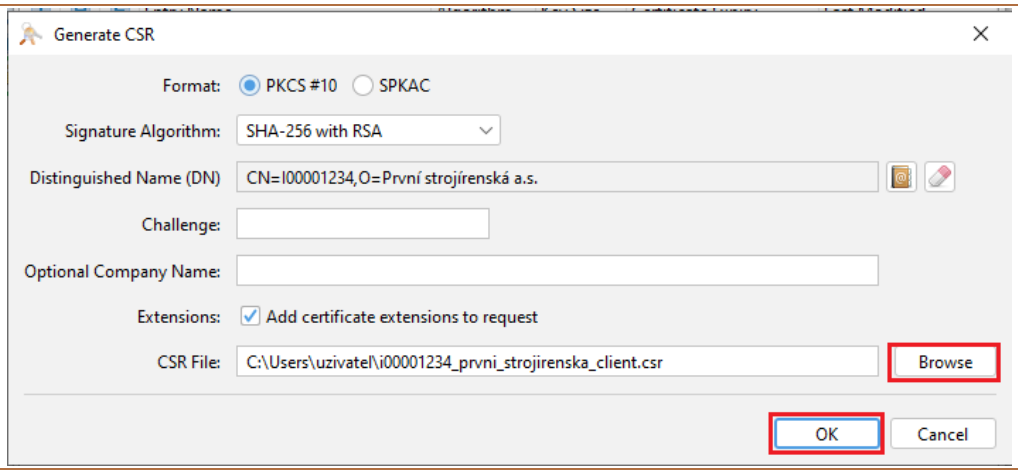
Klikněte pravým tlačítkem myši na tento řádek a dále zvolte **Generate CSR**.



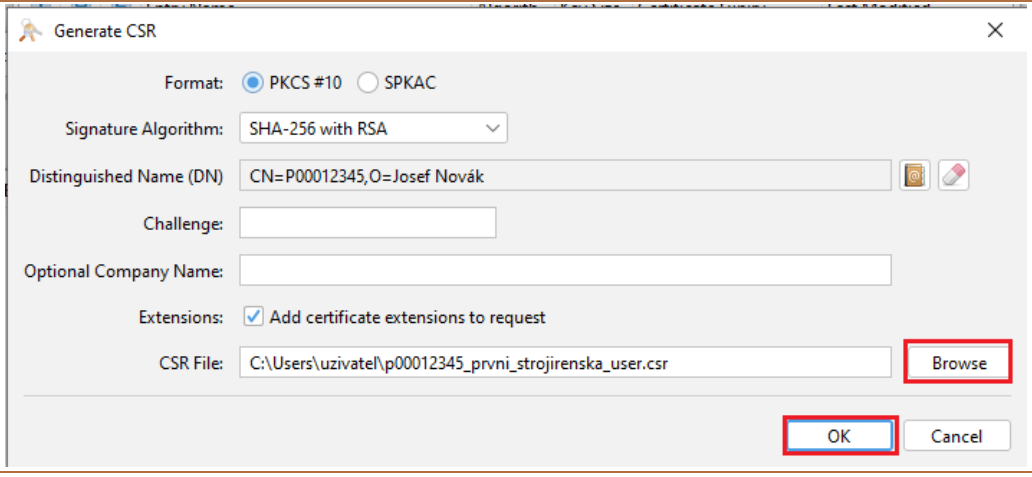
Zobrazí se detaily pro vygenerování žádosti. Údaje zkontrolujte, v případě potřeby změňte adresář, kam má být žádost uložena prostřednictvím tlačítka **Browse** – **<u>název souboru ale neměňte</u>**.

Generování žádosti potvrďte tlačítkem **OK**.

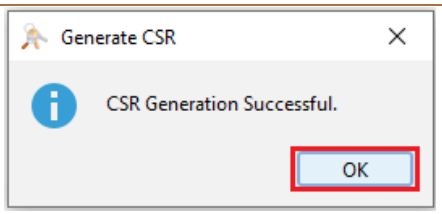
<u>Generování žádosti o Klientský certifikát:</u>



<u>Generování žádosti o Podpisový certifikát:</u>



Zobrazí se informace o úspěšném vygenerování souboru .csr se žádostí o certifikát – okno uzavřete tlačítkem **OK**.



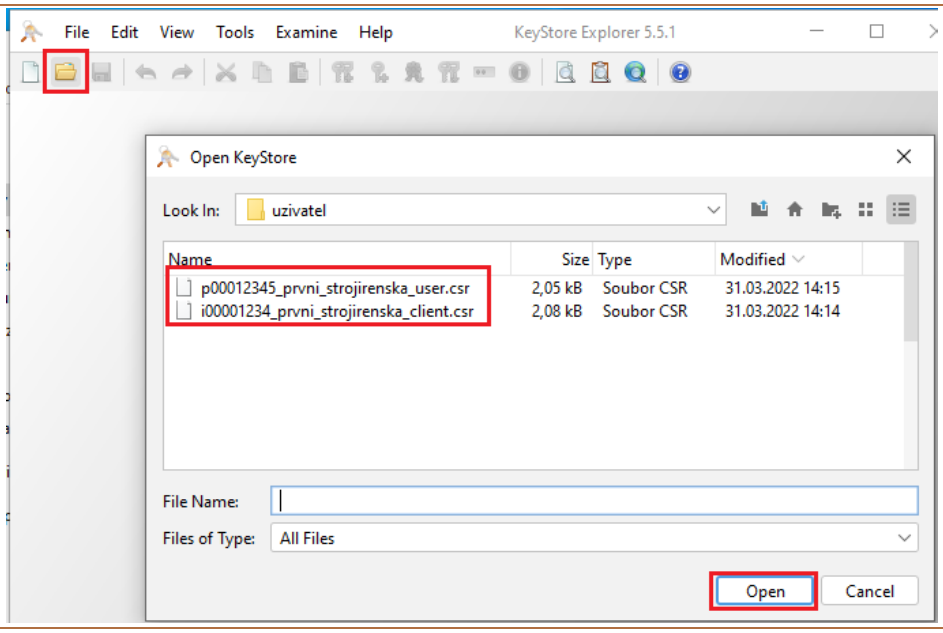
Soubor, resp. soubory se žádostí o vygenerování certifikátů následně odešlete požadovaným způsobem Bance.

Aplikaci zavřete a vygenerované žádosti uložte – aplikace bude pro jejich uložení vyžadovat heslo, které jste zadávali při generování souborů (viz výše).

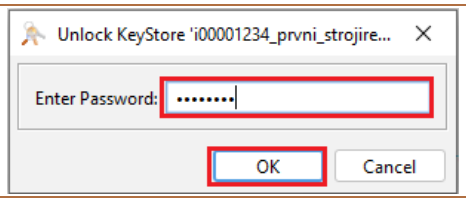
3 Import Bankou podepsaných žádostí o certifikát

Po zpracování žádostí o certifikáty Banka zašle zpět nové soubory s příponou .cer. Tyto soubory uložte do vytvořeného adresáře (viz bod 2) a importujte je do aplikace KeyStore.

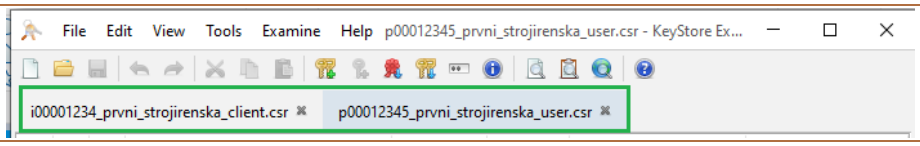
Klikněte na ikonku **Open** a vyhledejte adresář s uloženými soubory .csr.



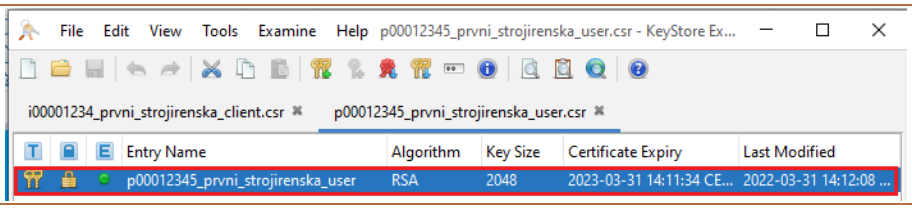
Otevřete postupně oba soubory. Systém si vyžádá heslo, které jste zadávali při vytvoření žádostí o certifikát (viz bod 2.) Heslo zadejte do pole **Enter Password** a potvrďte tlačítkem **OK**.



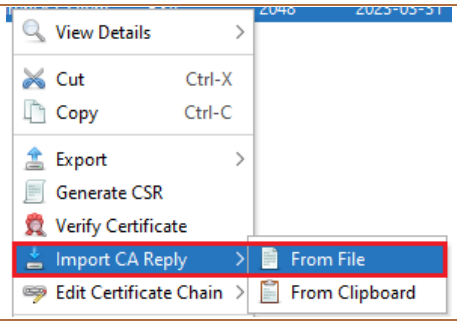
Soubory se žádostmi o certifikát se otevřou v samostatných oknech.



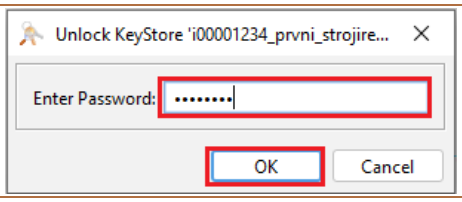
Klikněte do detailu jednoho souboru na řádek se žádostí o certifikát.



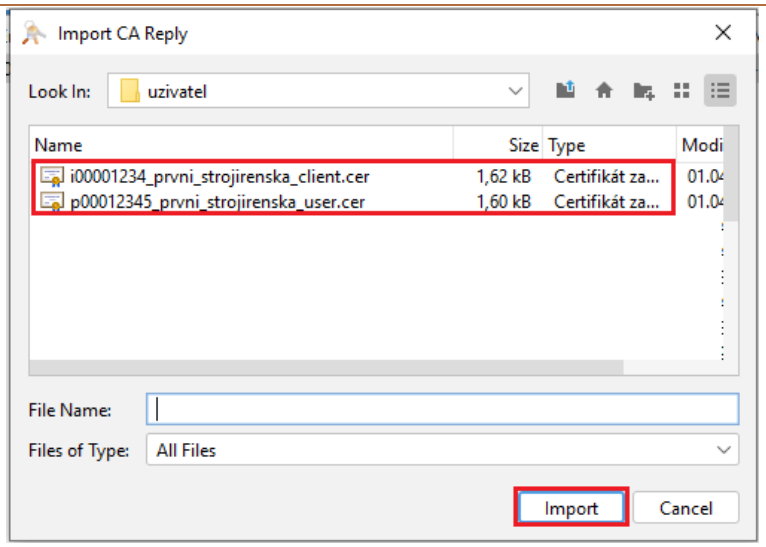
Klikněte pravým tlačítkem myši na tento řádek a dále zvolte **Import CA Replay** a **From File**.



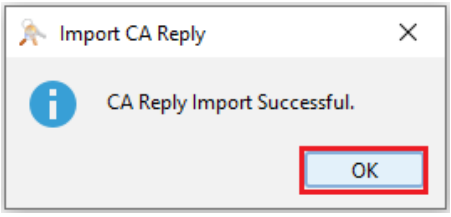
Systém si vyžádá heslo, které jste zadávali při vytvoření žádostí o certifikát (viz bod 2.) Heslo zadejte do pole **Enter Password** a potvrďte tlačítkem **OK**.



Vyberte soubor s odpovídající Bankou podepsanou žádostí a klikněte na tlačítko **Import**.



Zobrazí se informace o úspěšném importu souboru .cer se Bankou podepsanou žádostí o certifikát – okno uzavřete tlačítkem **OK**.

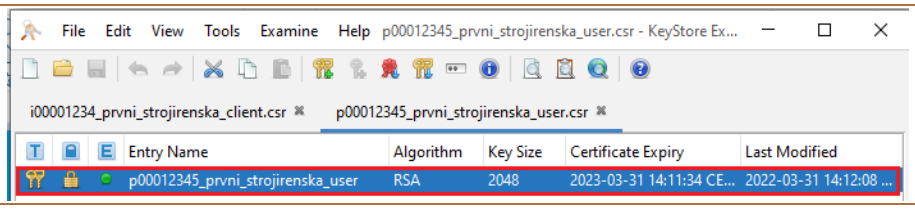


Tento postup opakujte i s druhým souborem.

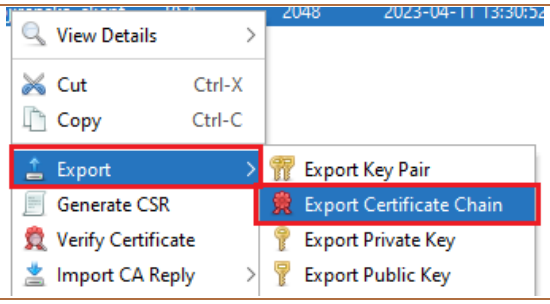
4 Export plnohodnotného certifikátu

Po úspěšném importu Bankou podepsaných žádostí o certifikát exportujte plnohodnotné certifikáty pro použití v Klientském API.

V otevřených souborech (viz bod 3) klikněte do detailu jednoho souboru na řádek se žádostí o certifikát.



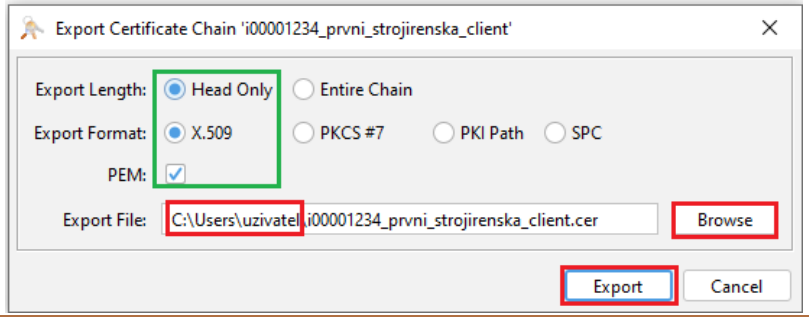
Klikněte pravým tlačítkem myši na tento řádek a dále zvolte **Export** a **Export Certificate Chain**.



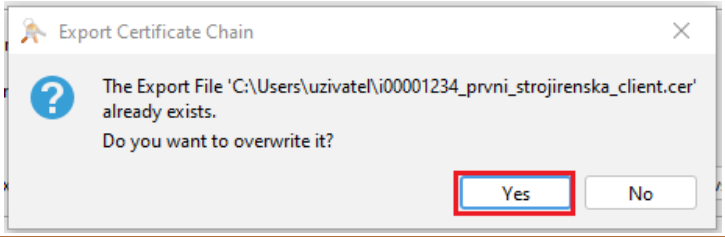
Vyberte následující volby pro generování certifikátu:

Pole	Vyplňované údaje
Export Length:	Zaškrtněte **Head Only**
Export Format:	Zaškrtněte **X.509**
PEM:	Zaškrtněte tuto možnost
Export File:	Údaje zkontrolujte, v případě potřeby změňte adresář, kam má být žádost uložena prostřednictvím tlačítka **Browse** – **<u>název souboru ale neměňte</u>**.

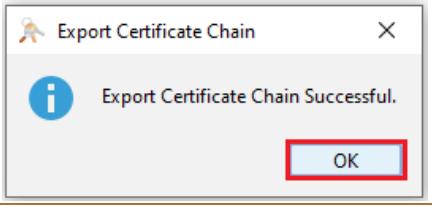
Export certifikátu potvrďte tlačítkem **Export**.



Systém zobrazí upozornění, že soubor s tímto názvem již existuje a s dotazem, zda jej chcete přepsat – potvrďte jej tlačítkem **Yes**.



Zobrazí se informace o úspěšném exportu certifikátu – okno uzavřete tlačítkem **OK**.



Tento postup opakujte i s druhým souborem.

5 Uživatelská podpora

Uživatelská podpora pro Klientské API je poskytována Zákaznickým servisem. Kontakty na Zákaznický servis a jeho Provozní dobu naleznete na Internetových stránkách banky.