CS OTE

Documentation for external users

To set up local certificate storage

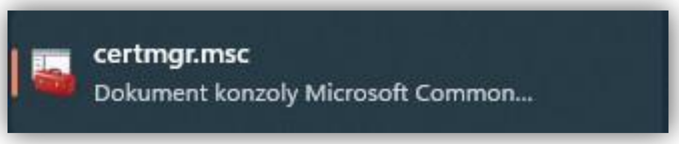
For the correct functionality of the local storage it is necessary to create a backup of the private part of the electronic signature, i.e. a file with the ***.p12** or ***.pfx** extension. The file can be exported from a computer where the certificate is already installed. To create a backup of the private part of the certificate, we recommend using the procedure below.

Please note that this manual is universal for all supported versions of the Windows operating system, and it is possible that some of the instructional images will differ from your device.
The manual was created for the latest version of the Windows operating system, but the procedure is similar to older versions.

Exporting the private part of a certificate in Windows

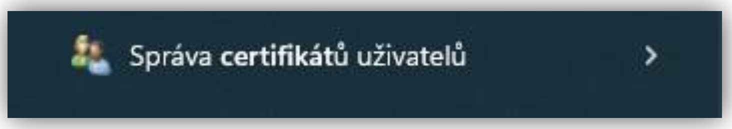
Open the Start menu or press ⊞ and search for „**certmgr.msc**" or "**Certificate**".
(just open the menu and start typing, you don't need to search for any search window)

- For **certmgr.msc,** select this option:

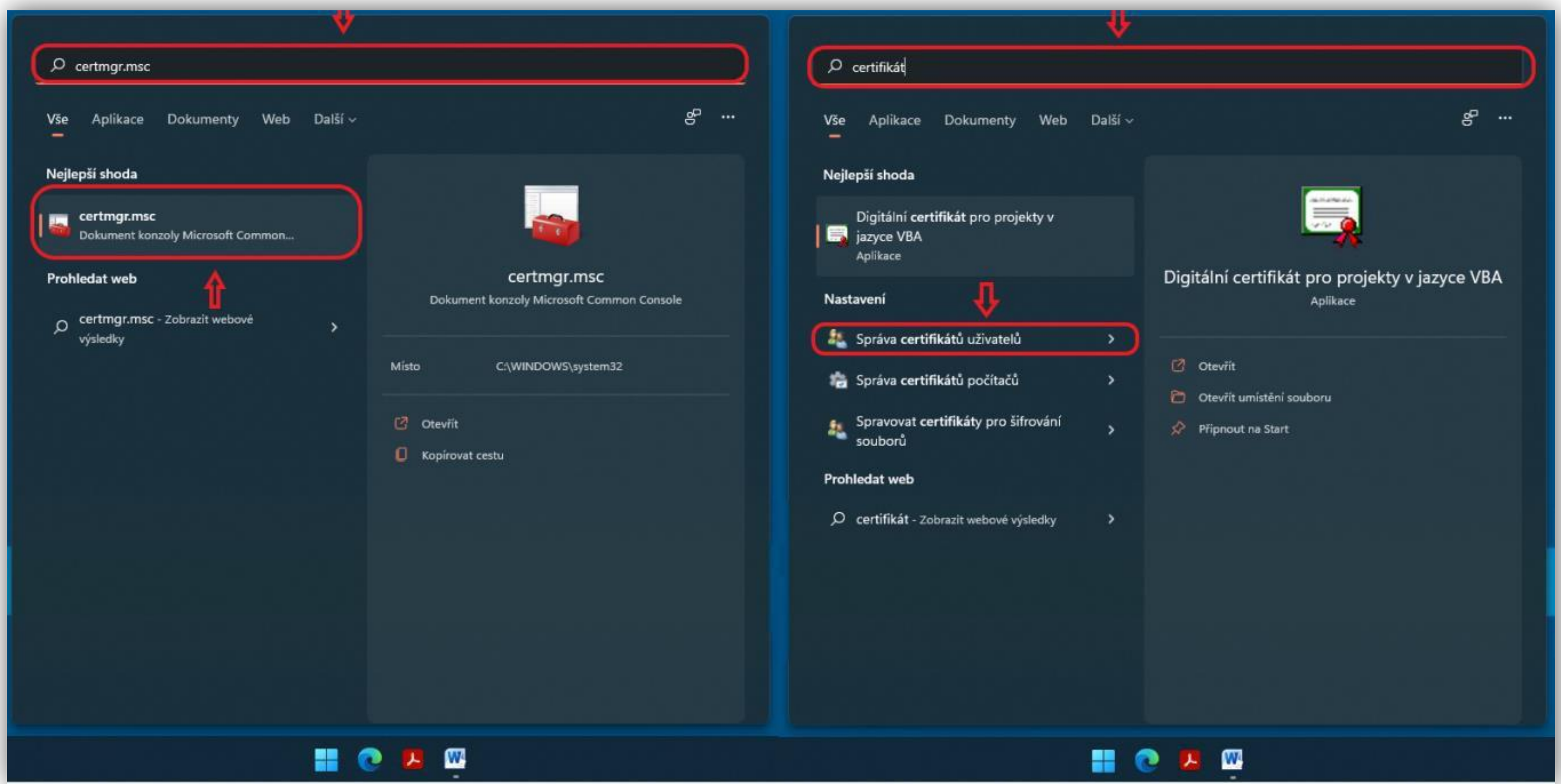


certmgr.msc
Dokument konzoly Microsoft Common...

- For a **certificate**, select this option:



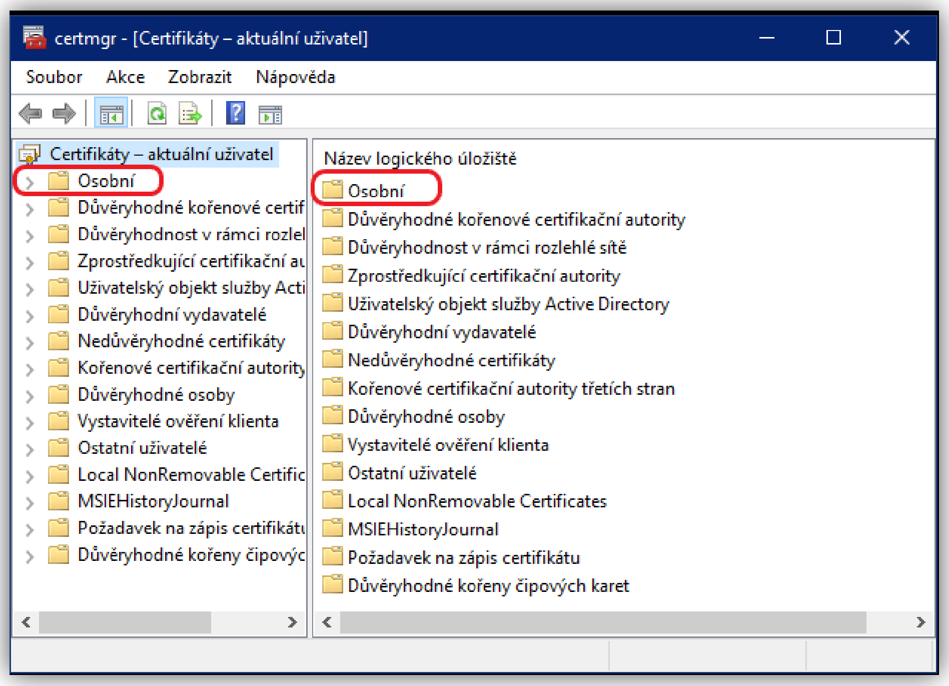
Správa certifikátů uživatelů



certmgr.msc
Vše
Aplikace
Dokumenty
Web
Další
Nejlepší shoda
certmgr.msc
Dokument konzoly Microsoft Common...
Prohledat web
certmgr.msc - Zobrazit webové výsledky
certmgr.msc
Dokument konzoly Microsoft Common Console
Místo
C:\WINDOWS\system32
Otevřít
Kopírovat cestu
certifikát
Vše
Aplikace
Dokumenty
Web
Další
Nejlepší shoda
Digitální certifikát pro projekty v jazyce VBA
Aplikace
Nastavení
Správa certifikátů uživatelů
Správa certifikátů počítačů
Spravovat certifikáty pro šifrování souborů
Prohledat web
certifikát - Zobrazit webové výsledky
Digitální certifikát pro projekty v jazyce VBA
Aplikace
Otevřít
Otevřít umístění souboru
Připnout na Start

In both cases, you will be taken to the same page, which we will work with later.

- Click the **personal** tab → **personal**

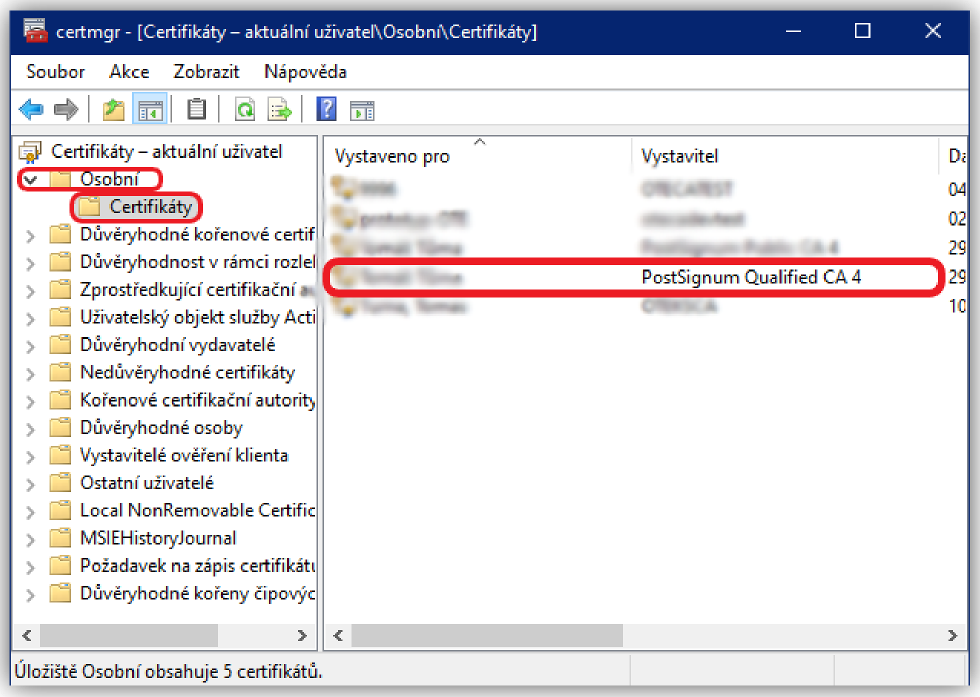


certmgr - [Certifikáty – aktuální uživatel]

Certifikáty – aktuální uživatel
- Osobní
- Důvěryhodné kořenové certif
- Důvěryhodnost v rámci rozlel
- Zprostředkující certifikační au
- Uživatelský objekt služby Acti
- Důvěryhodní vydavatelé
- Nedůvěryhodné certifikáty
- Kořenové certifikační autority
- Důvěryhodné osoby
- Vystavitelé ověření klienta
- Ostatní uživatelé
- Local NonRemovable Certific
- MSIEHistoryJournal
- Požadavek na zápis certifikátu
- Důvěryhodné kořeny čipovýc

Název logického úložiště
- Osobní
- Důvěryhodné kořenové certifikační autority
- Důvěryhodnost v rámci rozlehlé sítě
- Zprostředkující certifikační autority
- Uživatelský objekt služby Active Directory
- Důvěryhodní vydavatelé
- Nedůvěryhodné certifikáty
- Kořenové certifikační autority třetích stran
- Důvěryhodné osoby
- Vystavitelé ověření klienta
- Ostatní uživatelé
- Local NonRemovable Certificates
- MSIEHistoryJournal
- Požadavek na zápis certifikátu
- Důvěryhodné kořeny čipových karet

- Select your certificate and right-click it → **all tasks** → **export**

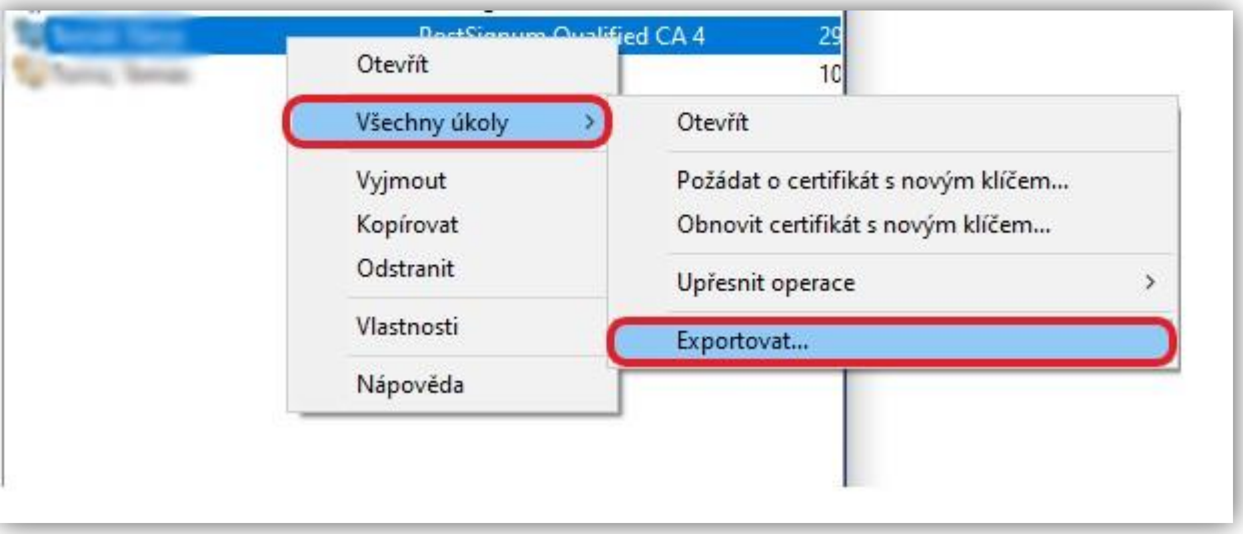


certmgr - [Certifikáty – aktuální uživatel\Osobní\Certifikáty]

Certifikáty – aktuální uživatel
- Osobní
  - Certifikáty
- Důvěryhodné kořenové certif
- Důvěryhodnost v rámci rozlel
- Zprostředkující certifikační a
- Uživatelský objekt služby Acti
- Důvěryhodní vydavatelé
- Nedůvěryhodné certifikáty
- Kořenové certifikační autority
- Důvěryhodné osoby
- Vystavitelé ověření klienta
- Ostatní uživatelé
- Local NonRemovable Certific
- MSIEHistoryJournal
- Požadavek na zápis certifikátu
- Důvěryhodné kořeny čipovýc

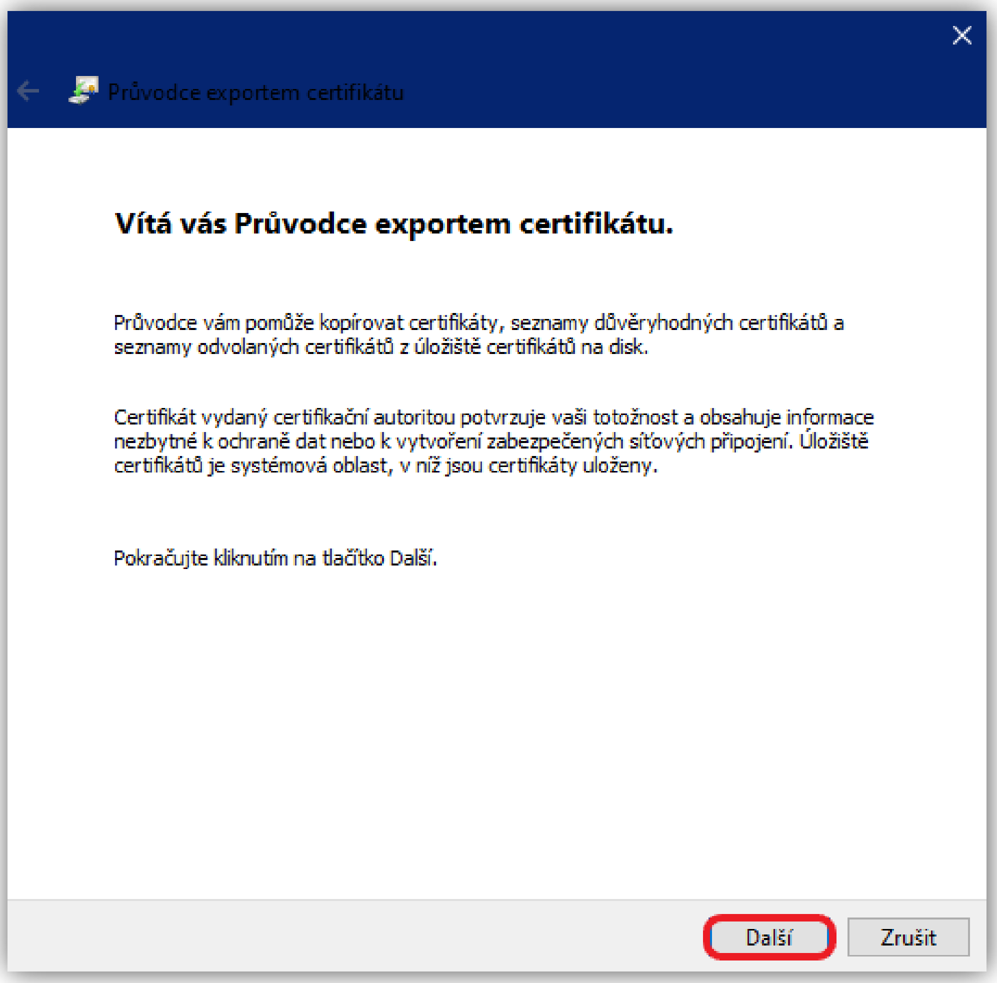
Vystaveno pro	Vystavitel	Da
[redacted]	[redacted]	04
[redacted]	[redacted]	02
[redacted]	[redacted]	29
[redacted]	PostSignum Qualified CA 4	29
[redacted]	[redacted]	10

Úložiště Osobní obsahuje 5 certifikátů.



Certificate Export Wizard

- In the Export Certificate Wizard, click Next (N ext) to continue.



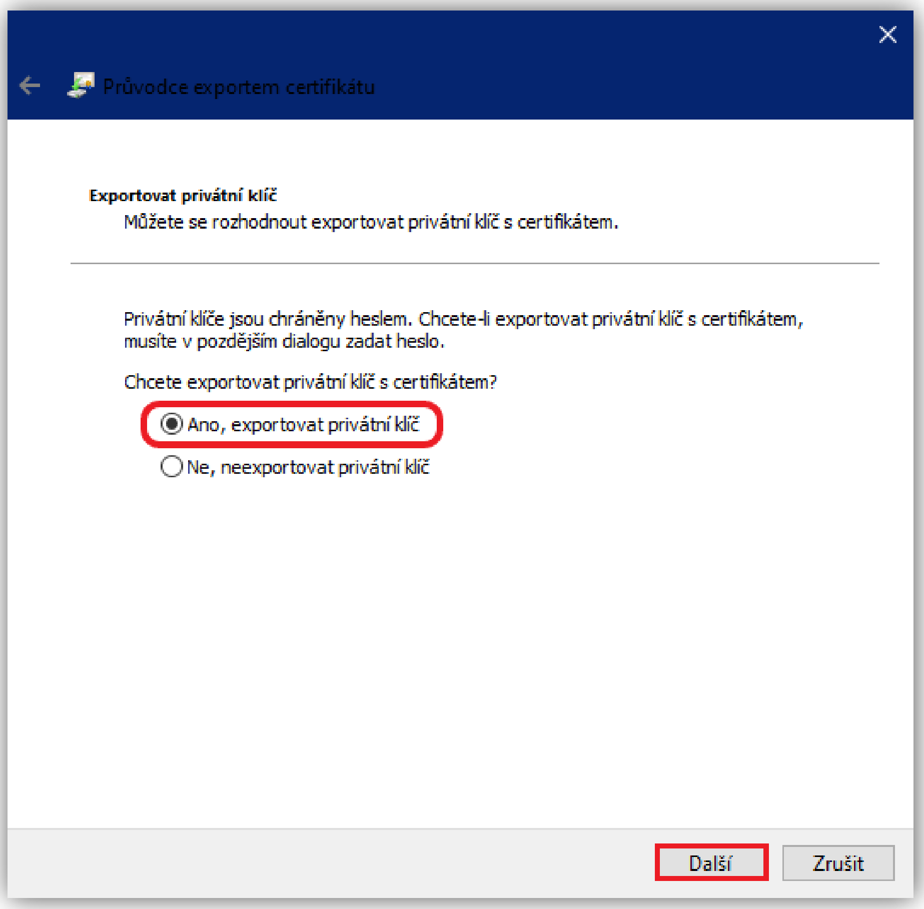
Vítá vás Průvodce exportem certifikátu.

Průvodce vám pomůže kopírovat certifikáty, seznamy důvěryhodných certifikátů a seznamy odvolaných certifikátů z úložiště certifikátů na disk.

Certifikát vydaný certifikační autoritou potvrzuje vaši totožnost a obsahuje informace nezbytné k ochraně dat nebo k vytvoření zabezpečených síťových připojení. Úložiště certifikátů je systémová oblast, v níž jsou certifikáty uloženy.

Pokračujte kliknutím na tlačítko Další.

- In the second step, select **Yes**, export the private key and click **Next**.



Exportovat privátní klíč

Můžete se rozhodnout exportovat privátní klíč s certifikátem.

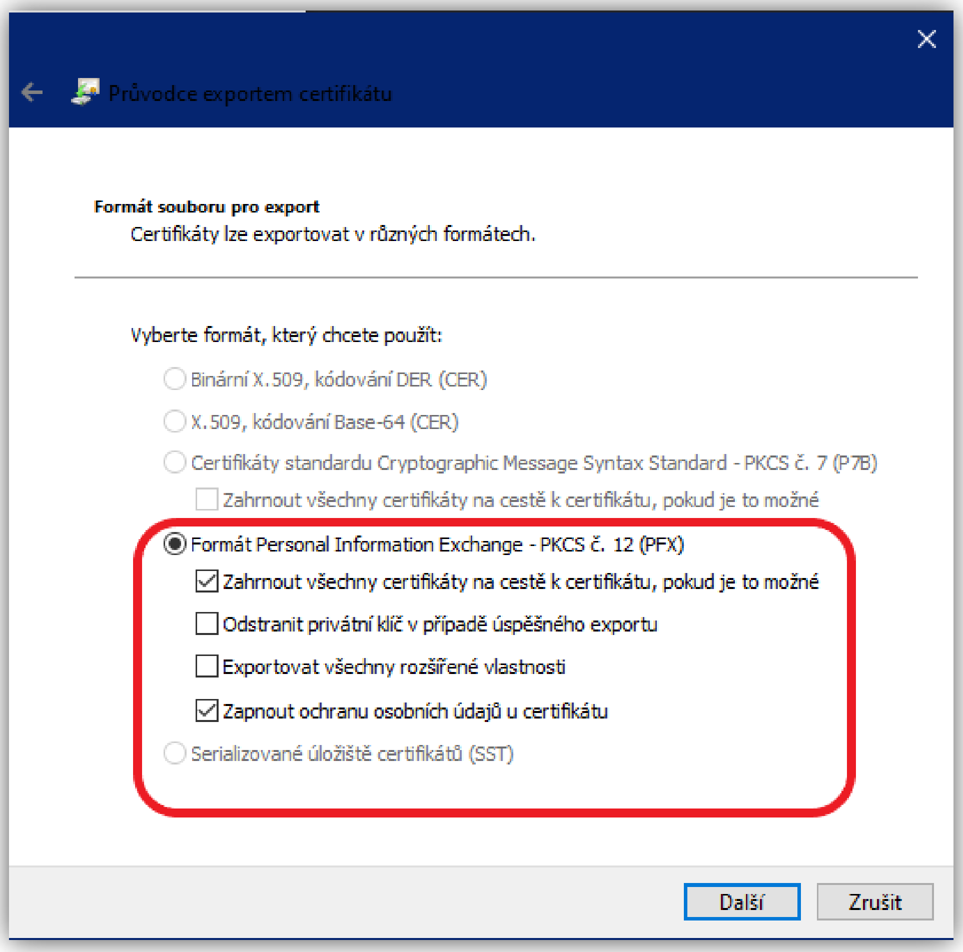
Privátní klíče jsou chráněny heslem. Chcete-li exportovat privátní klíč s certifikátem, musíte v pozdějším dialogu zadat heslo.

Chcete exportovat privátní klíč s certifikátem?

● Ano, exportovat privátní klíč

○ Ne, neexportovat privátní klíč

- Leave the default option „**Personal Information Exchange - .pfx**" and click **Next**.



Průvodce exportem certifikátu

Formát souboru pro export

Certifikáty lze exportovat v různých formátech.

Vyberte formát, který chcete použít:

○ Binární X.509, kódování DER (CER)

○ X.509, kódování Base-64 (CER)

○ Certifikáty standardu Cryptographic Message Syntax Standard - PKCS č. 7 (P7B)

□ Zahrnout všechny certifikáty na cestě k certifikátu, pokud je to možné

● Formát Personal Information Exchange - PKCS č. 12 (PFX)

☑ Zahrnout všechny certifikáty na cestě k certifikátu, pokud je to možné

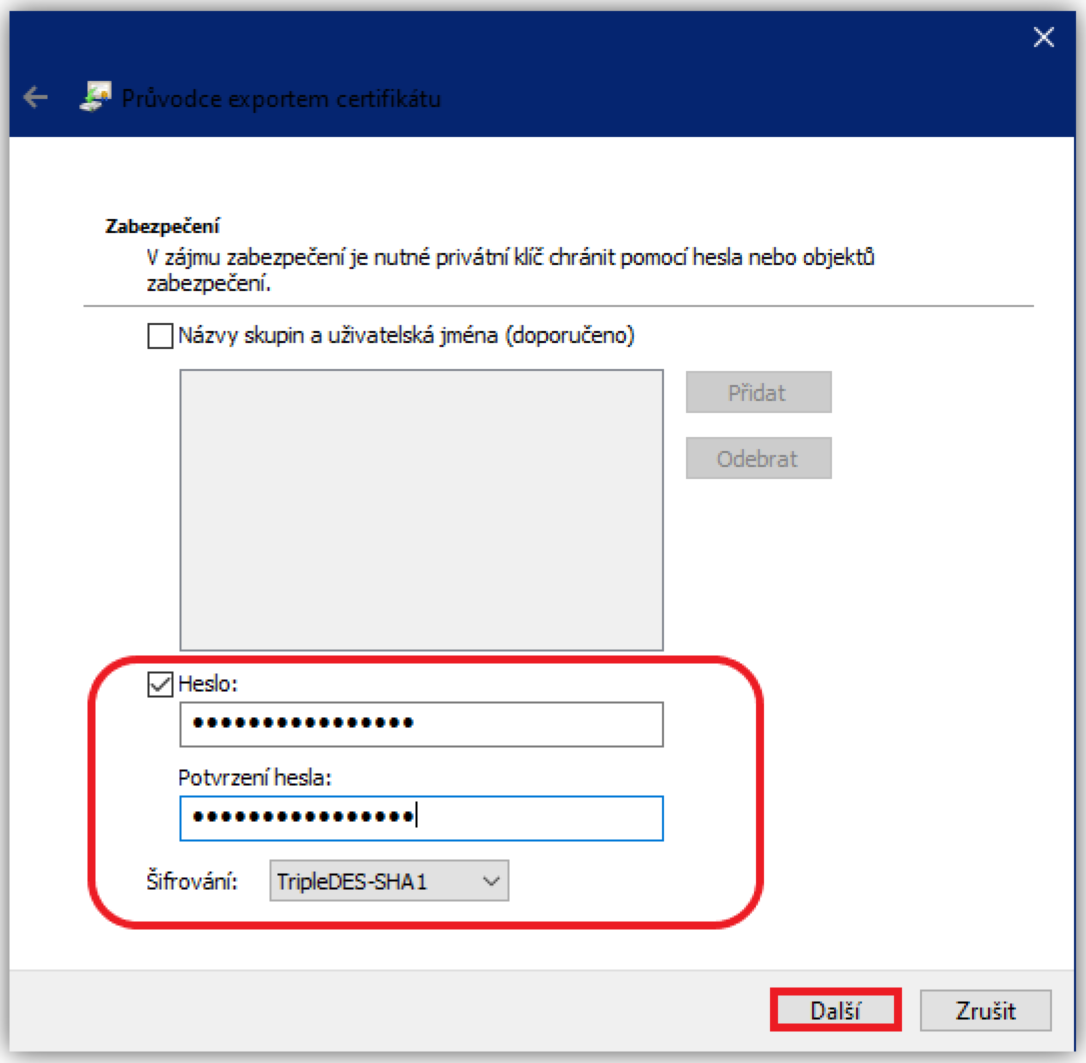
□ Odstranit privátní klíč v případě úspěšného exportu

□ Exportovat všechny rozšířené vlastnosti

☑ Zapnout ochranu osobních údajů u certifikátu

○ Serializované úložiště certifikátů (SST)

Next, encrypt the file (choose a password to protect the private key). Confirm the password and click **Next**.



Průvodce exportem certifikátu

Zabezpečení

V zájmu zabezpečení je nutné privátní klíč chránit pomocí hesla nebo objektů zabezpečení.

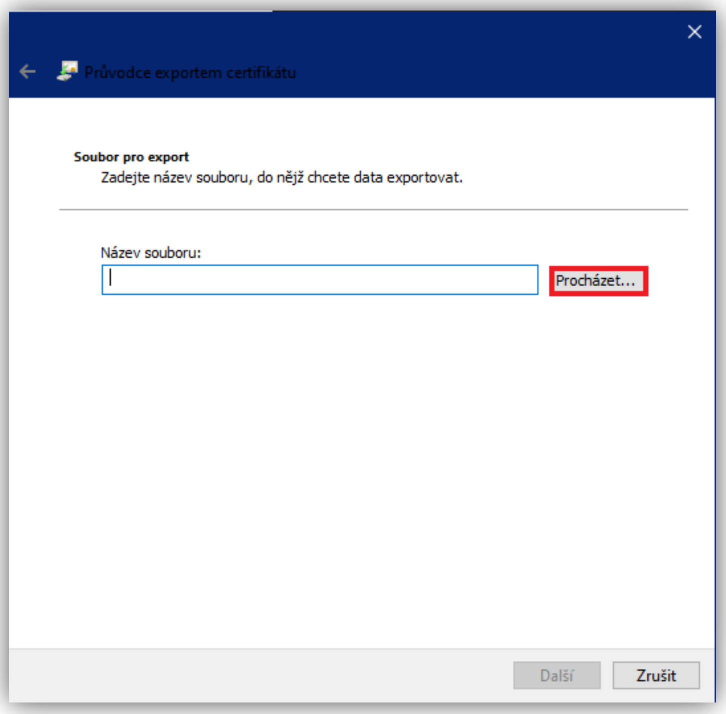
□ Názvy skupin a uživatelská jména (doporučeno)

☑ Heslo: ••••••••••••••••

Potvrzení hesla: ••••••••••••••••

Šifrování: TripleDES-SHA1

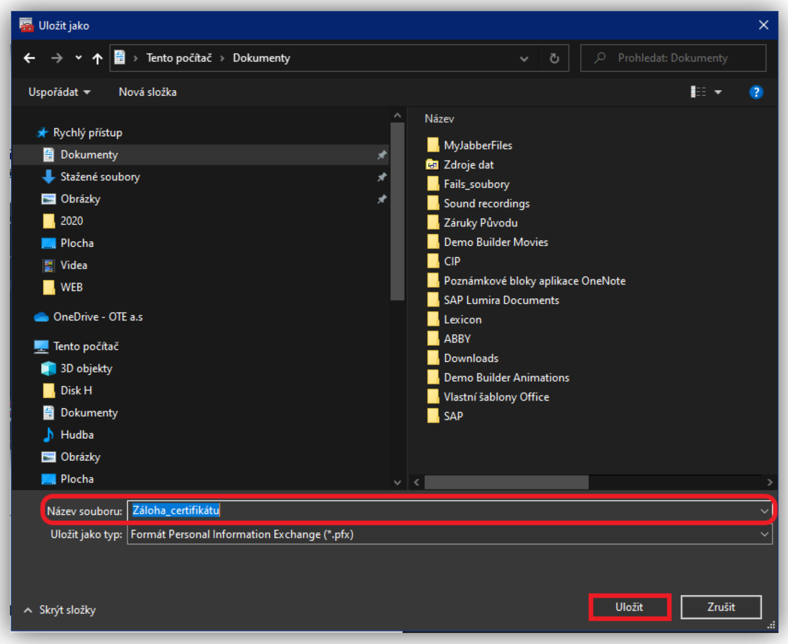
Next, select where you want to save the private portion of the certificate by clicking Browse, naming the file, clicking Save, and then clicking **Next**.



Soubor pro export

Zadejte název souboru, do nějž chcete data exportovat.

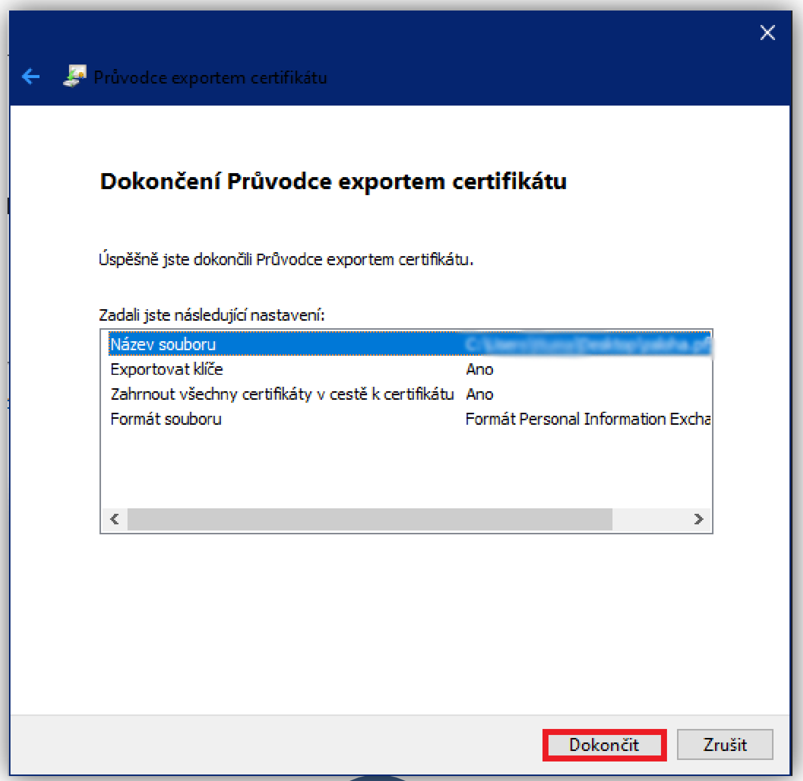
Název souboru:



Název souboru: Záloha_certifikátu

Uložit jako typ: Formát Personal Information Exchange (*.pfx)

Now press **Finish**. After the successful export, the private part of the certificate is now available at the location of your choice.



Dokončení Průvodce exportem certifikátu

Úspěšně jste dokončili Průvodce exportem certifikátu.

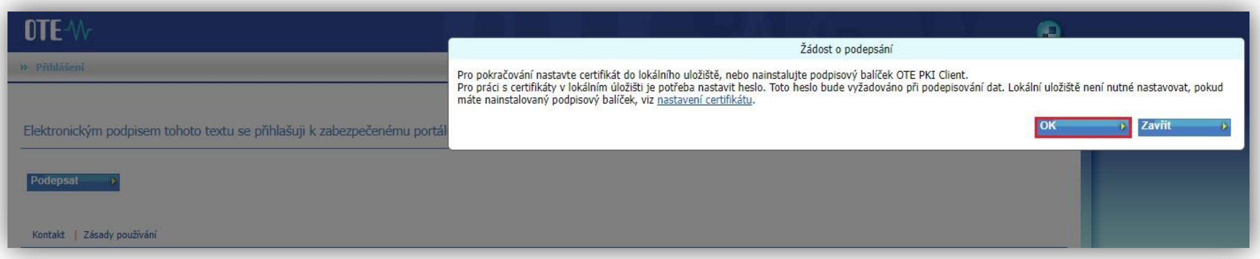
Zadali jste následující nastavení:

Název souboru	[redacted]
Exportovat klíče	Ano
Zahrnout všechny certifikáty v cestě k certifikátu	Ano
Formát souboru	Formát Personal Information Excha

To set up local certificate storage

- Local storage allows you to store certificates for data signing.
- The local storage is always password protected, if the existing password is reset, it will delete the currently recorded electronic signature from the local storage.
- You must import the private part of the certificate (the *.p12 or *.pfx file) that you created in the previous step into the local storage.
- The private key is only imported into the browser's web storage, no one else but you has access to it.
- You must import the certificate into the local store after each certificate renewal.

When you try to sign electronically in **Google Chrome**, **Microsoft Edge**, **Mozilla Firefox**, you will get a warning that it is necessary to insert the certificate into the local certificate store first. After clicking **OK**, you will be redirected to the local certificate store.

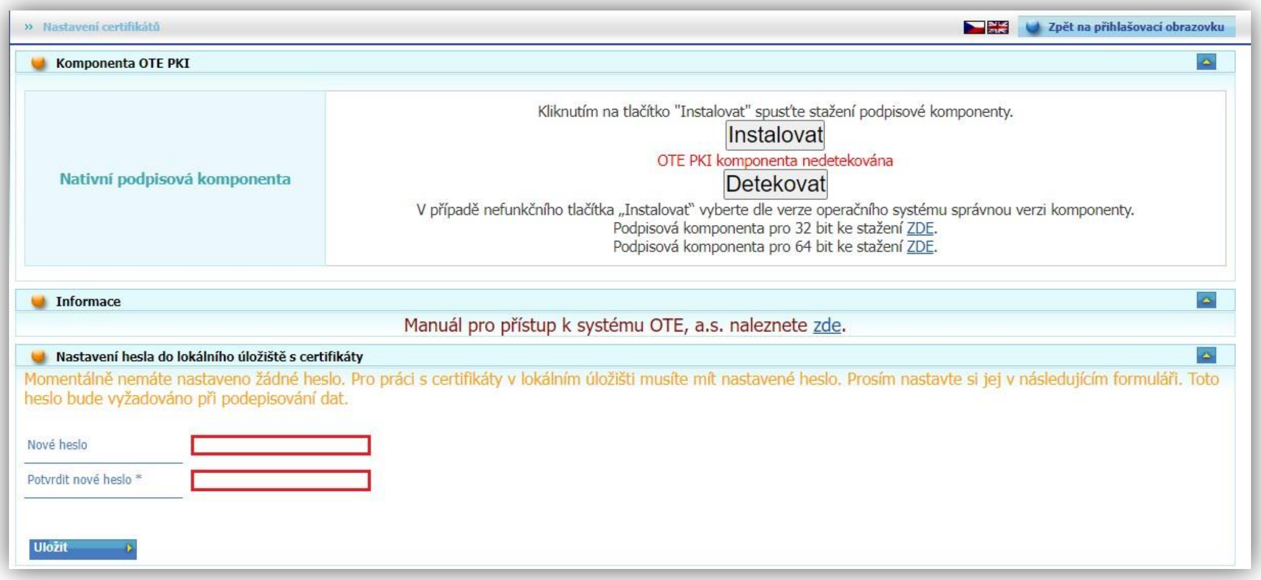


Elektronickým podpisem tohoto textu se přihlašuji k zabezpečenému portál

Žádost o podepsání

Pro pokračování nastavte certifikát do lokálního uložiště, nebo nainstalujte podpisový balíček OTE PKI Client.
Pro práci s certifikáty v lokálním úložišti je potřeba nastavit heslo. Toto heslo bude vyžadováno při podepisování dat. Lokální uložiště není nutné nastavovat, pokud máte nainstalovaný podpisový balíček, viz nastavení certifikátu.

In case you do not have a **password** set in the local storage, you need to set it here (min. 4 characters). This password will be required when you log into the application again. After entering the password and confirming it, click the **Save** button.



» Nastavení certifikátů

Zpět na přihlašovací obrazovku

Komponenta OTE PKI

Nativní podpisová komponenta

Kliknutím na tlačítko "Instalovat" spusťte stažení podpisové komponenty.

Instalovat

OTE PKI komponenta nedetekována

Detekovat

V případě nefunkčního tlačítka „Instalovat" vyberte dle verze operačního systému správnou verzi komponenty.
Podpisová komponenta pro 32 bit ke stažení ZDE.
Podpisová komponenta pro 64 bit ke stažení ZDE.

Informace

Manuál pro přístup k systému OTE, a.s. naleznete zde.

Nastavení hesla do lokálního úložiště s certifikáty

Momentálně nemáte nastaveno žádné heslo. Pro práci s certifikáty v lokálním úložišti musíte mít nastavené heslo. Prosím nastavte si jej v následujícím formuláři. Toto heslo bude vyžadováno při podepisování dat.

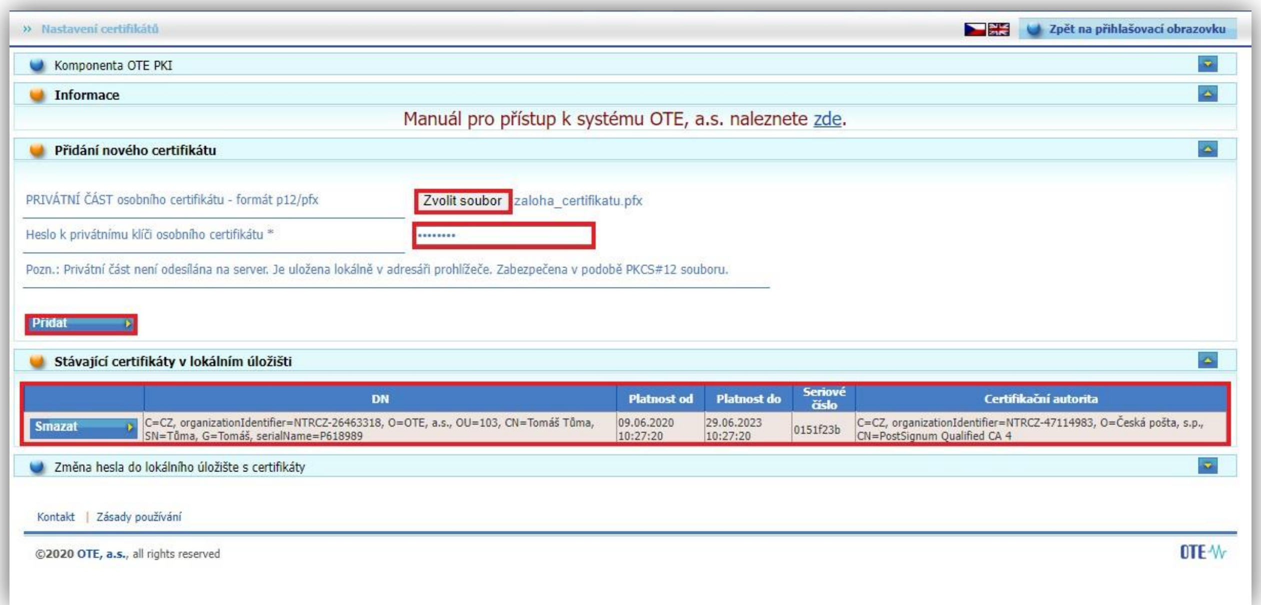
Nové heslo

Potvrdit nové heslo *

Uložit

Now you need to import the private part of the certificate, a file in *.**p12** or *.**pfx** format. Click on the **Browse** (Choose File) button and locate the backup of your certificate. After selecting the certificate in ***.p12** or ***.pfx** format, enter the password for the private key of the personal certificate (this is the password you set when you backed up **the private part of the certificate**). Finally, click the **Add** button.

When you click the button, the certificate appears in the *Existing Certificates* section of *the local store*. You can then proceed to register the certificate or log in



» Nastavení certifikátů

Zpět na přihlašovací obrazovku

Komponenta OTE PKI

Informace

Manuál pro přístup k systému OTE, a.s. naleznete zde.

Přidání nového certifikátu

PRIVÁTNÍ ČÁST osobního certifikátu - formát p12/pfx — Zvolit soubor zaloha_certifikatu.pfx

Heslo k privátnímu klíči osobního certifikátu * — ••••••••

Pozn.: Privátní část není odesílána na server. Je uložena lokálně v adresáři prohlížeče. Zabezpečena v podobě PKCS#12 souboru.

Přidat

Stávající certifikáty v lokálním úložišti

	DN	Platnost od	Platnost do	Seriové číslo	Certifikační autorita
Smazat	C=CZ, organizationIdentifier=NTRCZ-26463318, O=OTE, a.s., OU=103, CN=Tomáš Tůma, SN=Tůma, G=Tomáš, serialName=P618989	09.06.2020 10:27:20	29.06.2023 10:27:20	0151f23b	C=CZ, organizationIdentifier=NTRCZ-47114983, O=Česká pošta, s.p., CN=PostSignum Qualified CA 4

Změna hesla do lokálního úložište s certifikáty

Kontakt | Zásady používání

©2020 OTE, a.s., all rights reserved

Now you can successfully log in - OTE Portal (ote-cr.cz)