

Přístup do systému CS OTE přes prohlížeče Firefox s certifikátem PostSignum a I.CA

Stáhněte si nejnovější verzi Firefox a nainstalujte

<http://www.mozilla.org/cs/firefox/new/>

Stáhněte si podpisovou komponentu a nainstalujte ji

<http://www.ote-cr.cz/registrace-a-smlouvy/pristup-do-cs-ote/files-konfigurace-pc/PKIComponent-OTE-setup.exe>

Instalace veřejných částí certifikačních autorit

Mám softwarový komerční certifikát od PostSignum

Do prohlížeče Firefox vložte adresu www.postsignum.cz/certifikaty_autorit.html

(na odkaz stačí kliknout levým tlačítkem myši)

Na stránce najdete tabulku *Ruční instalace certifikátů certifikačních autorit*. Na plochu si uložte 3 veřejné části certifikační autority *PostSignum Root QCA 2* ve formátu DER.

Klikněte pravým tlačítkem myši na první certifikát DER a zvolte uložit odkaz jako...

Ruční instalace certifikátů certifikačních autorit

Stáhněte si soubory s certifikáty autorit (pro OS Windows DER) a v instalaci postupujte dle návodu k příslušné aplikaci.

Soubory s certifikáty autorit PostSignum Root QCA 2:		
 DER	 PEM	kořenová certifikační autorita PostSignum Root QCA 2
 DER	 PEM	kvalifikovaná certifikační autorita PostSignum Qualified CA 2
 DER	 PEM	kvalifikovaná certifikační autorita PostSignum Qualified CA 3
 DER	 PEM	komerční certifikační autorita PostSignum Public CA 2

Otevřít odkaz v novém panelu

Otevřít odkaz v novém okně

Otevřít odkaz v novém anonymním okně

Přidat odkaz do záložek

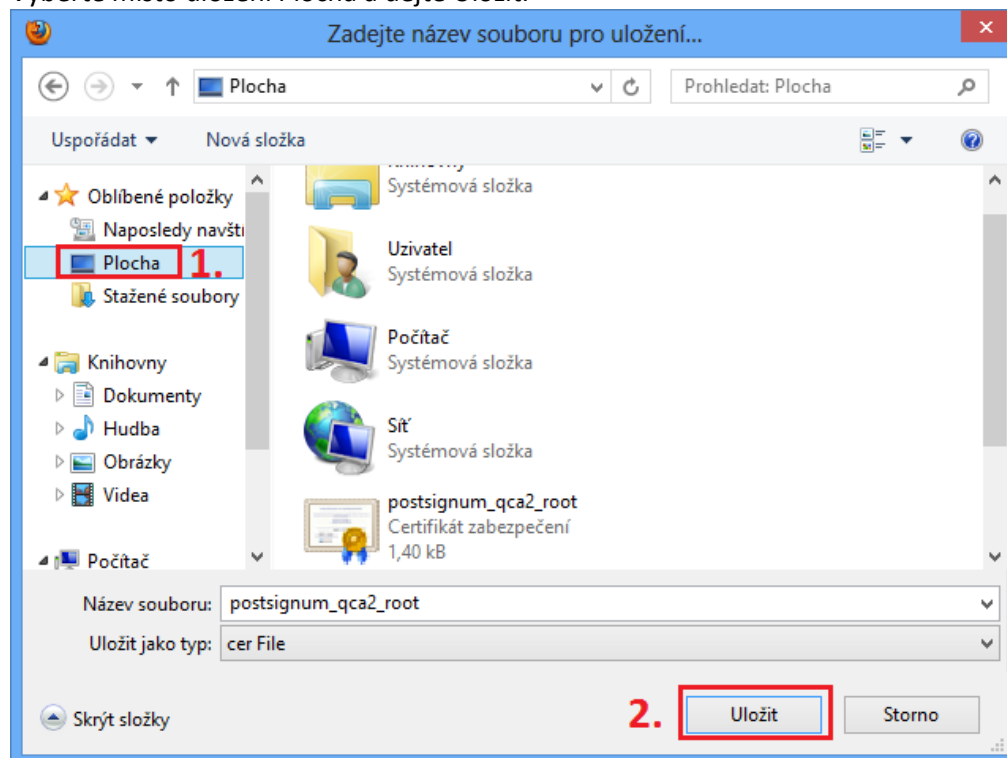
Uložit odkaz jako...

Kopírovat adresu odkazu

Hledat „DER“ na webu „Google“

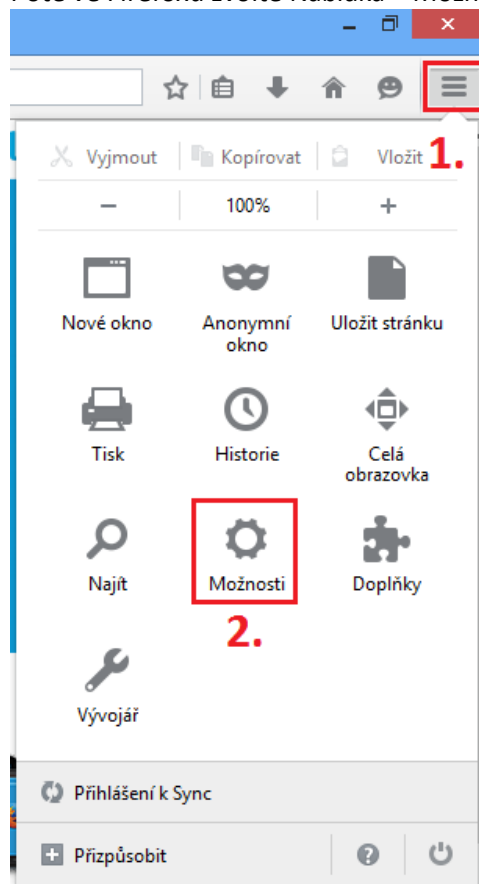
Prozkoumat prvek

Vyberte místo uložení Plocha a dejte Uložit.

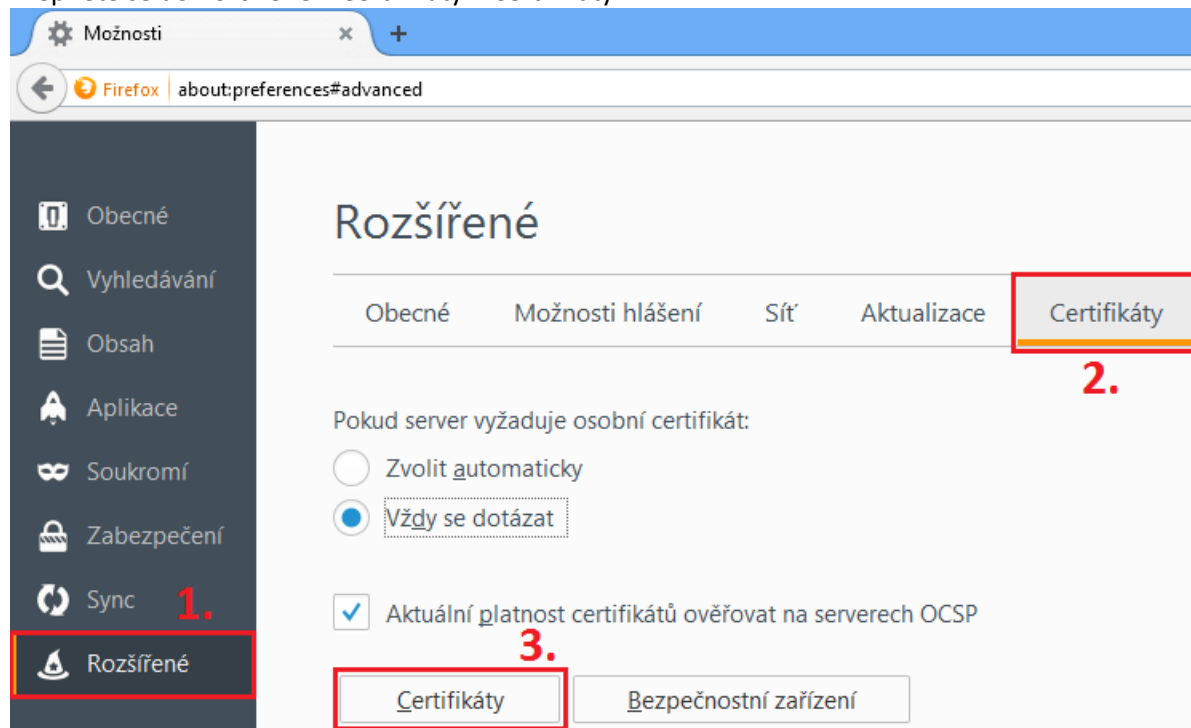


Stejným způsobem uložte zbylé tři certifikáty ve formátu DER.

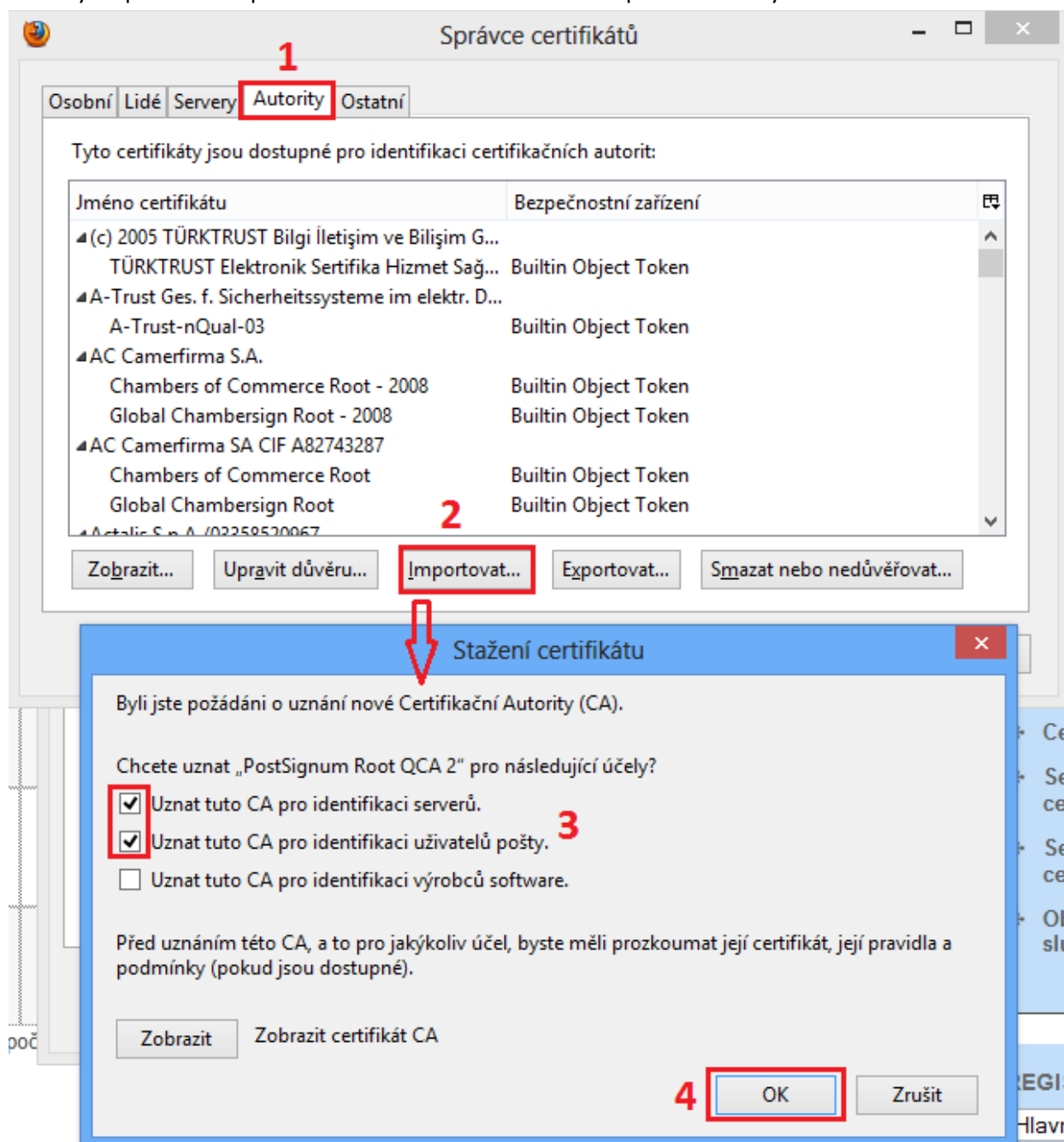
Poté ve Firefoxu zvolte Nabídka – Možnosti.



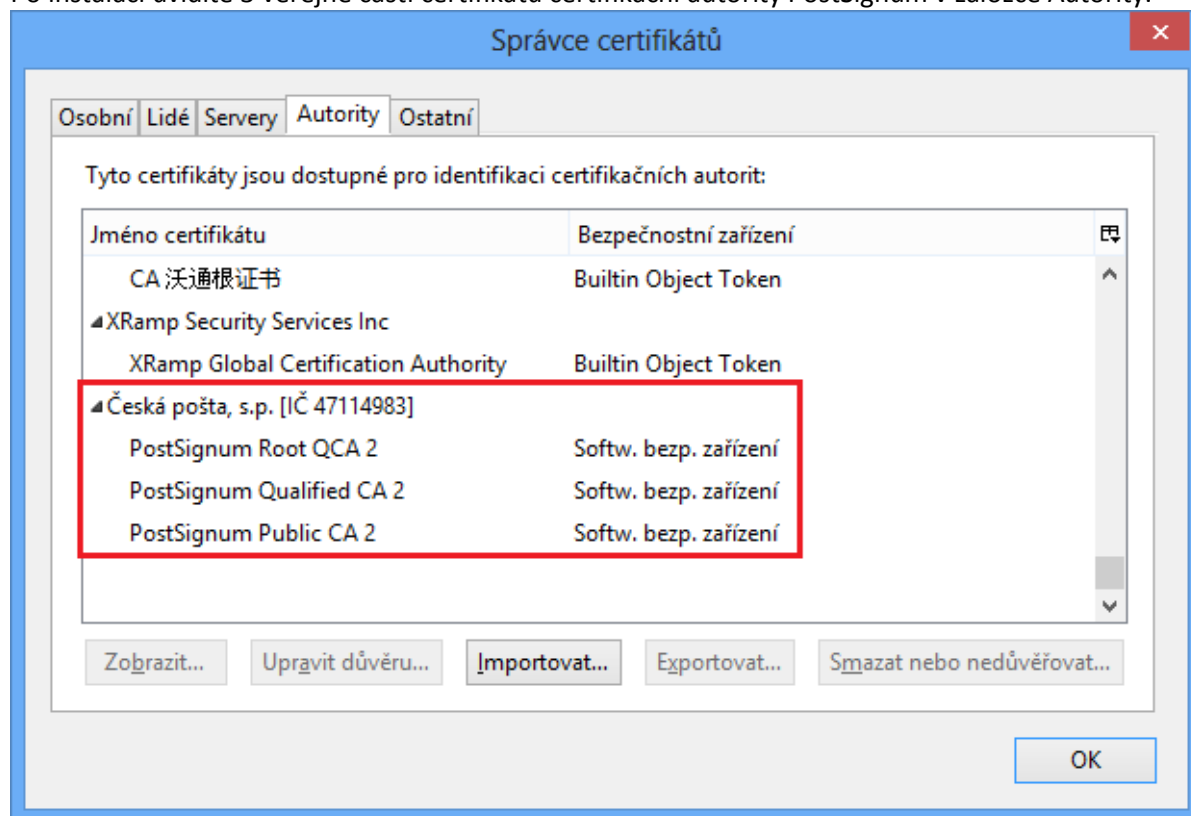
Přepněte se do Rozšířené – Certifikáty – Certifikáty.



V záložce Autority nainportujte všechny 3 veřejné části certifikační autority PostSignum, které máte uloženy na ploše. Při importu nastavte u každého certifikátu první dvě volby.



Po instalaci uvidíte 3 veřejné části certifikátu certifikační autority PostSignum v záložce Authority.



Mám softwarový komerční certifikát od I.CA

Do prohlížeče Firefox vložte adresu www.ica.cz/SHA2-Komerčni
(na odkaz stačí kliknout levým tlačítkem myši)

Na plochu si uložte veřejné části certifikační autority I.CA ve formátu DER. Klikněte pravým tlačítkem myši na první certifikát DER a zvolte uložit odkaz jako...

Kořenový certifikát certifikační autority pro vydávané komerční certifikáty SHA2

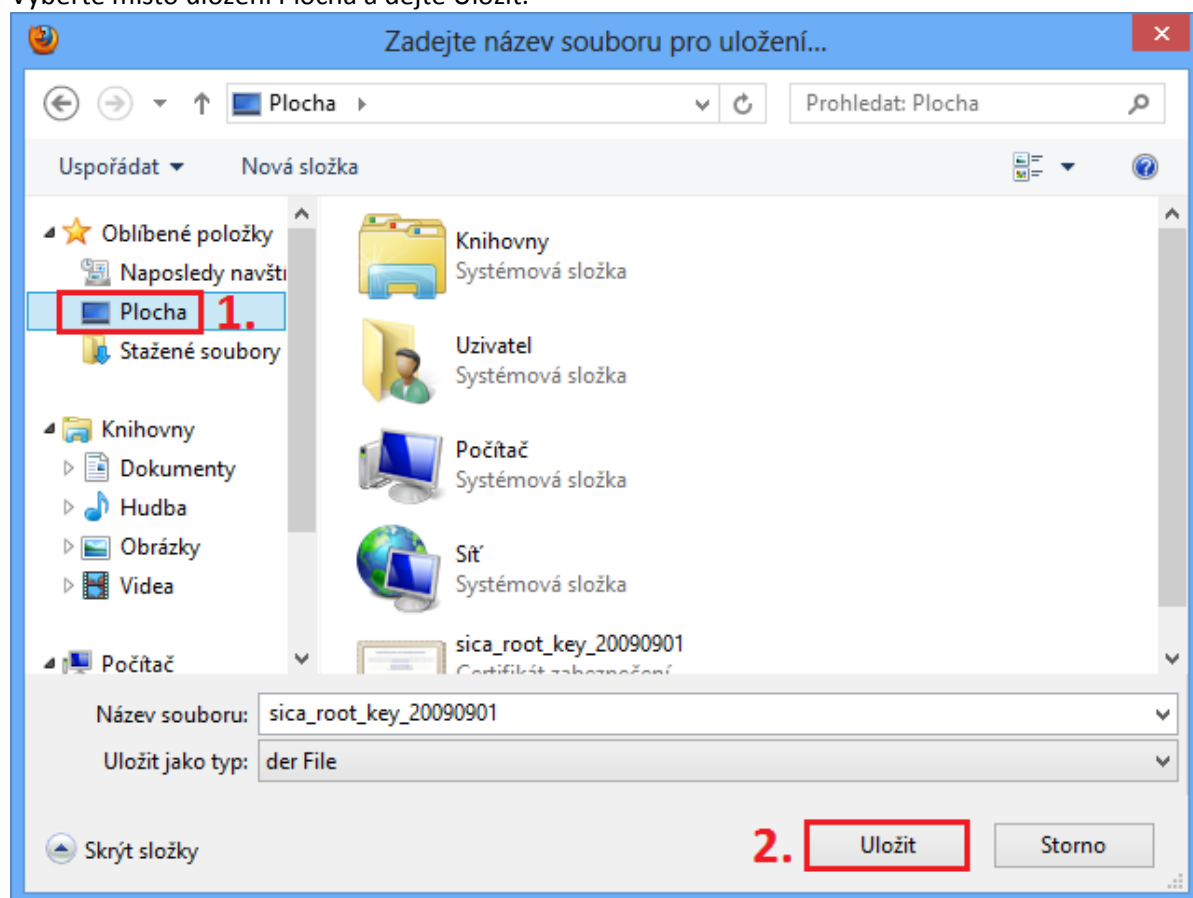
Kryptografický algoritmus: SHA-256

Délka kryptografického klíče pro algoritmus RSA: 2048 bitů

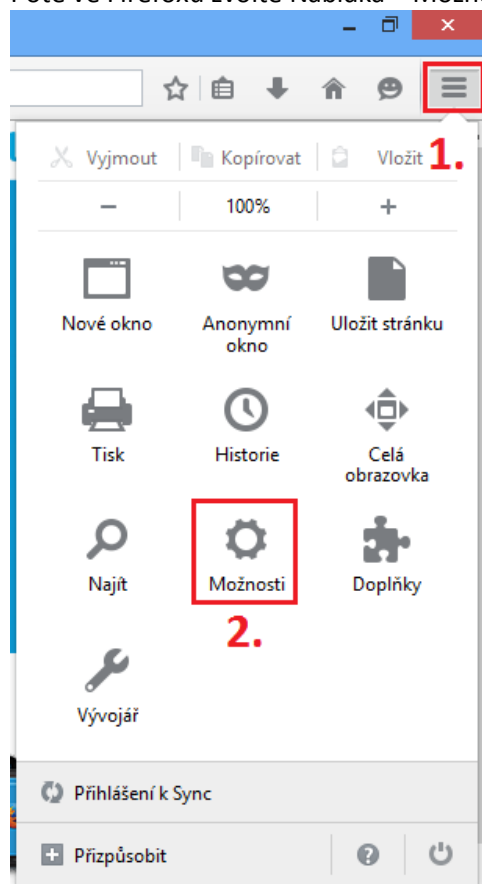
Doba platnosti: od 1.9.2009 do 1.9.2019

Odkaz	ZIP	Algoritmus otisku: otisk*
↓ DER 1070 byte		Otevřít odkaz v novém panelu Otevřít odkaz v novém okně Přidat odkaz do záložek Uložit odkaz jako... Kopírovat adresu odkazu Prozkoumat prvek
↓ PEM 1509 byte		0e97b5229b49df8690d7b74193e9ce3886141 ebd635e1be20cf7327dd a127168ba1b 77b95dee77c79666ff9ada1e3b5acea27a7bce 636382ac640225df1ff91 5cca623103d

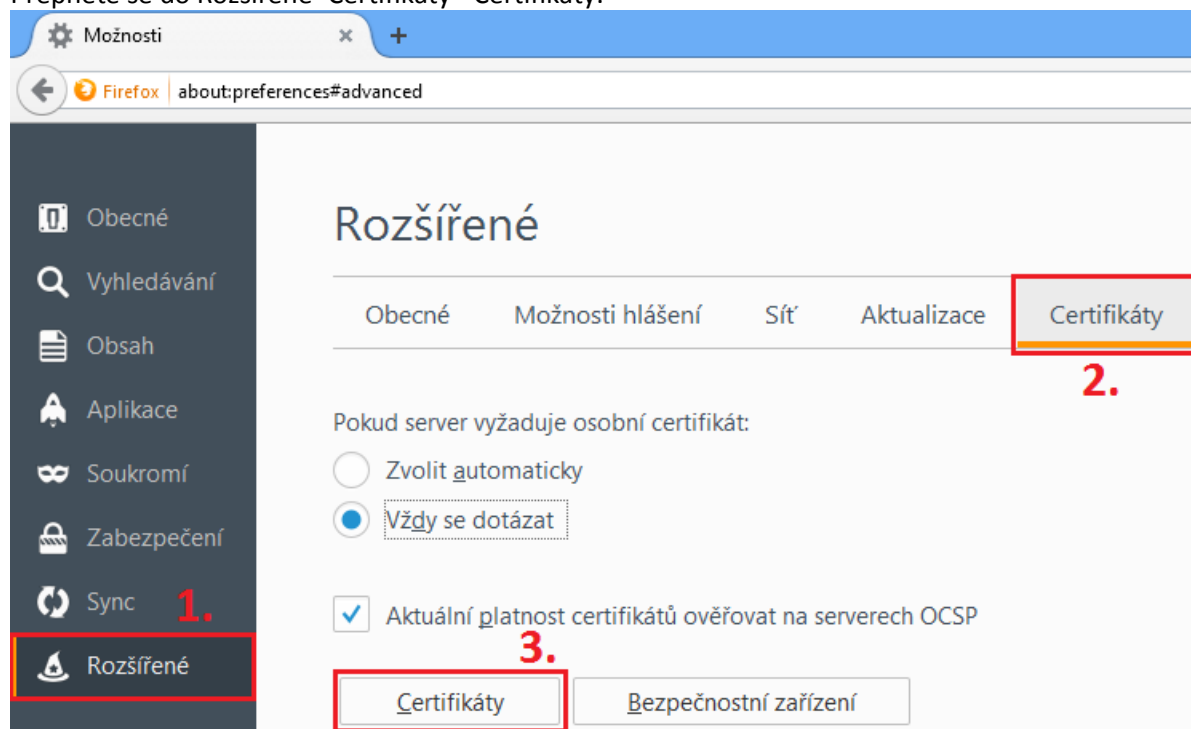
Vyberte místo uložení Plocha a dejte Uložit.



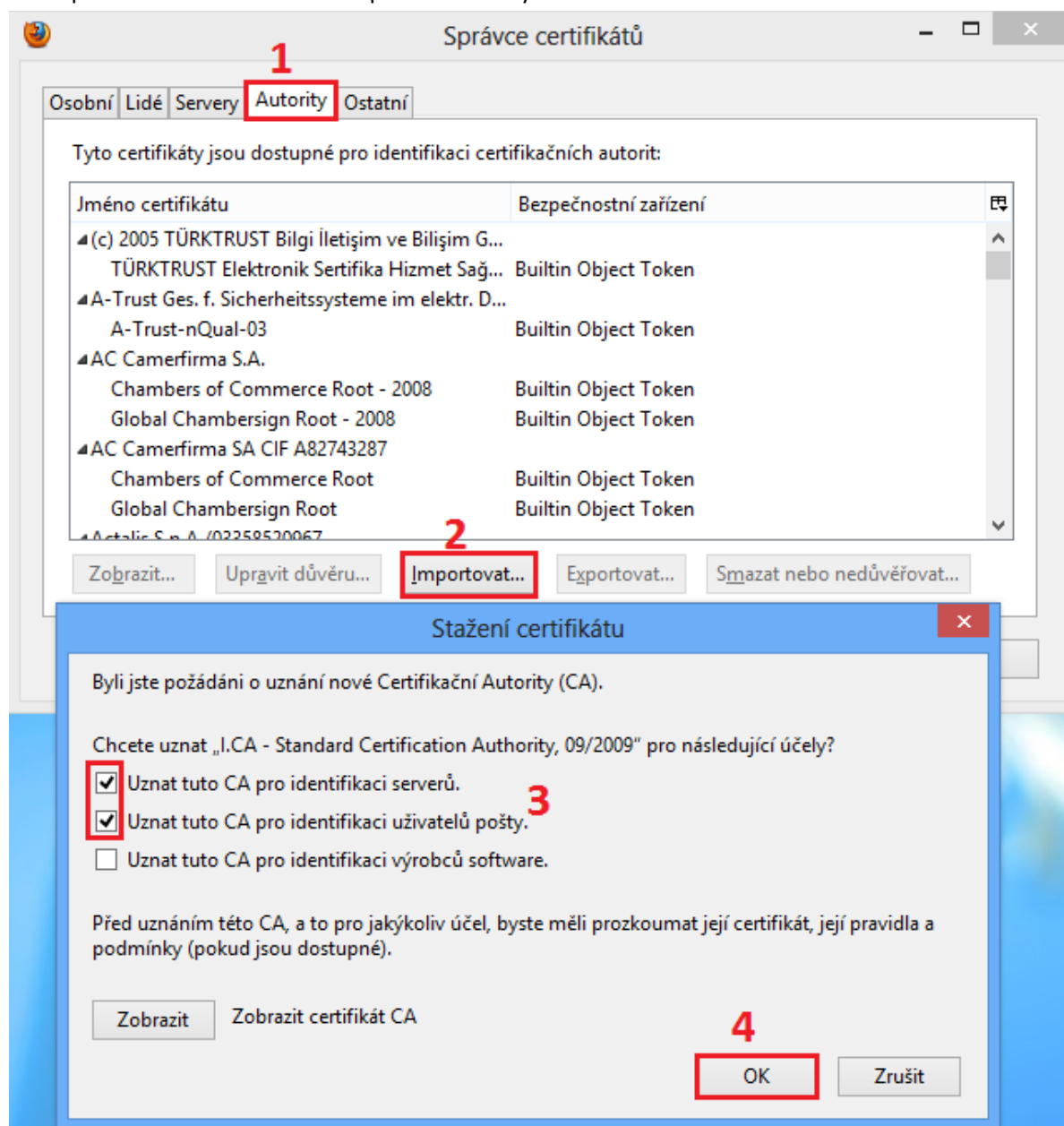
Poté ve Firefoxu zvolte Nabídka – Možnosti.



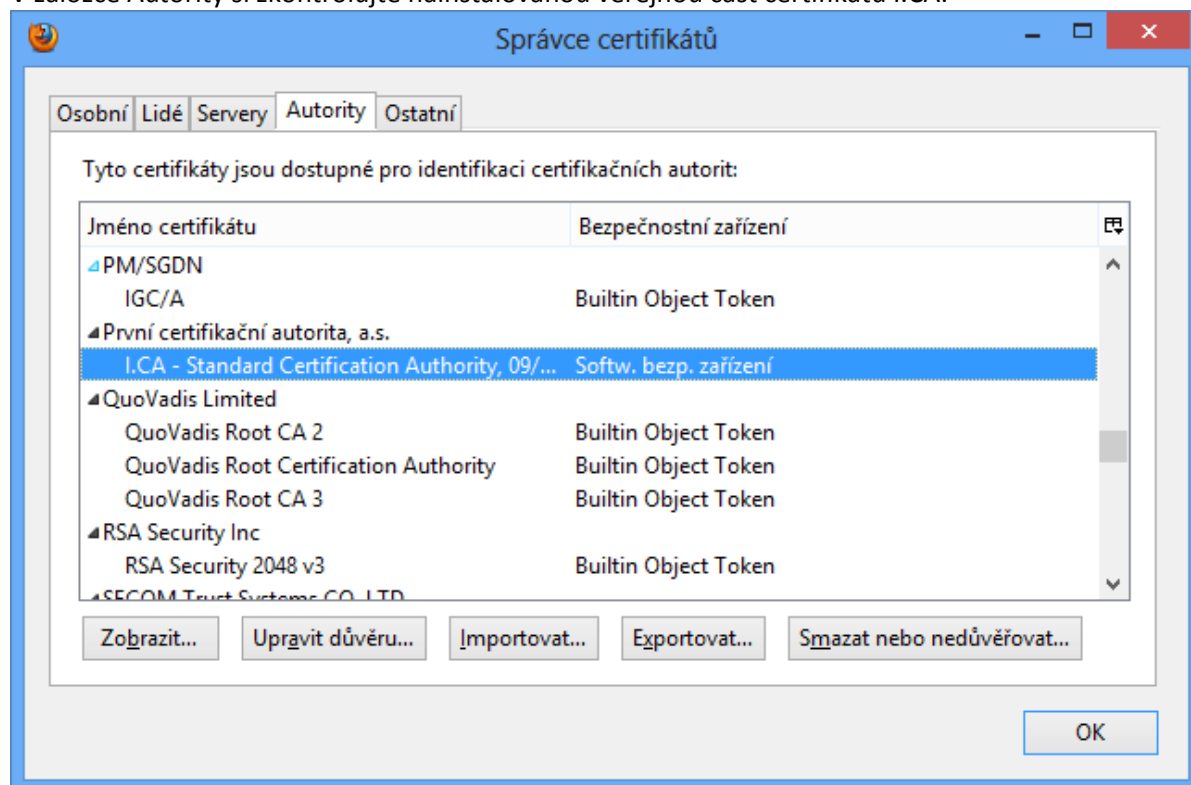
Přepněte se do Rozšířené -Certifikáty - Certifikáty.



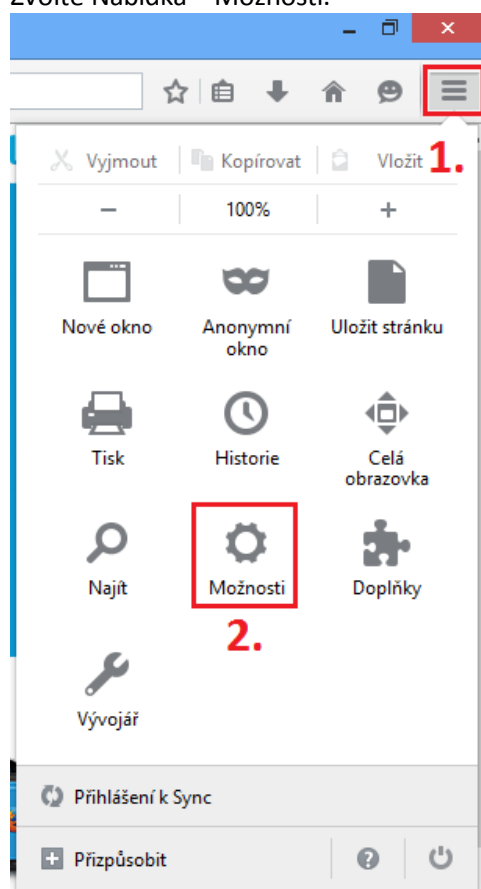
V záložce Autority nainportujte veřejnou část certifikační autority, kterou máte uloženou na ploše. Při importu nastavte u certifikátu první dvě volby.



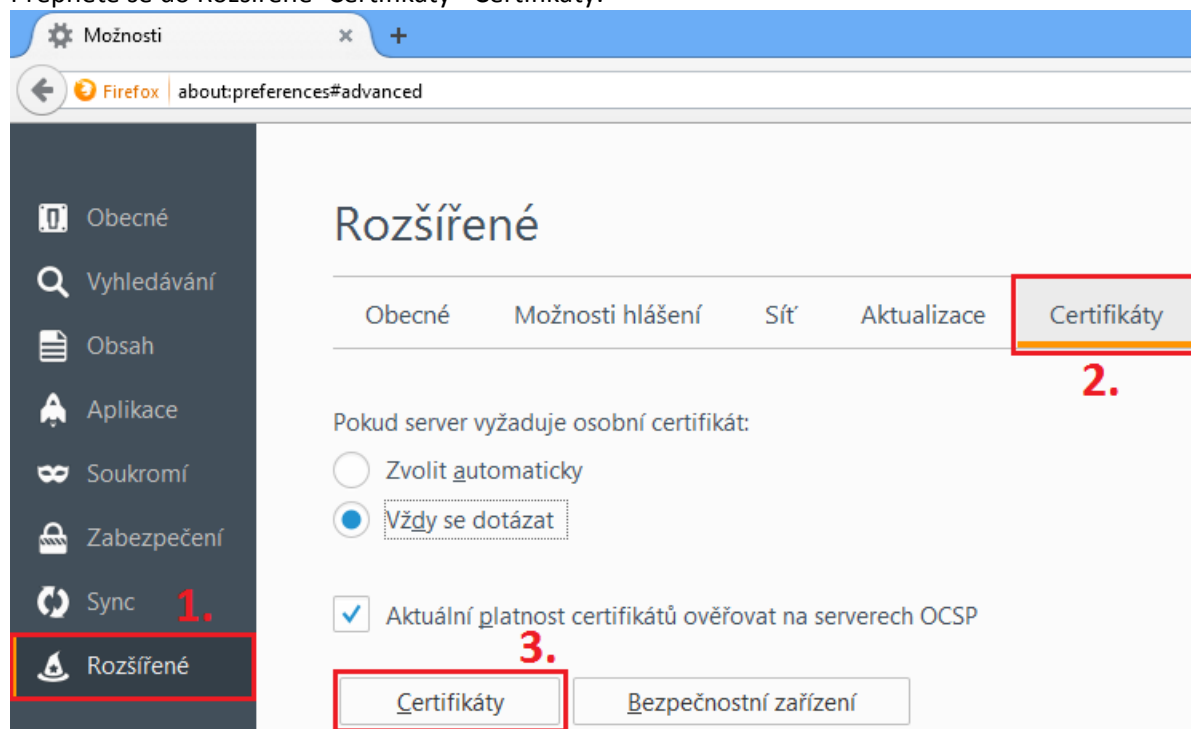
V záložce Autority si zkontrolujte nainstalovanou veřejnou část certifikátu I.CA.



Nyní budete importovat Váš privátní certifikát od PostSignum případně I.CA do Firefoxu. Zvolte Nabídka – Možnosti.

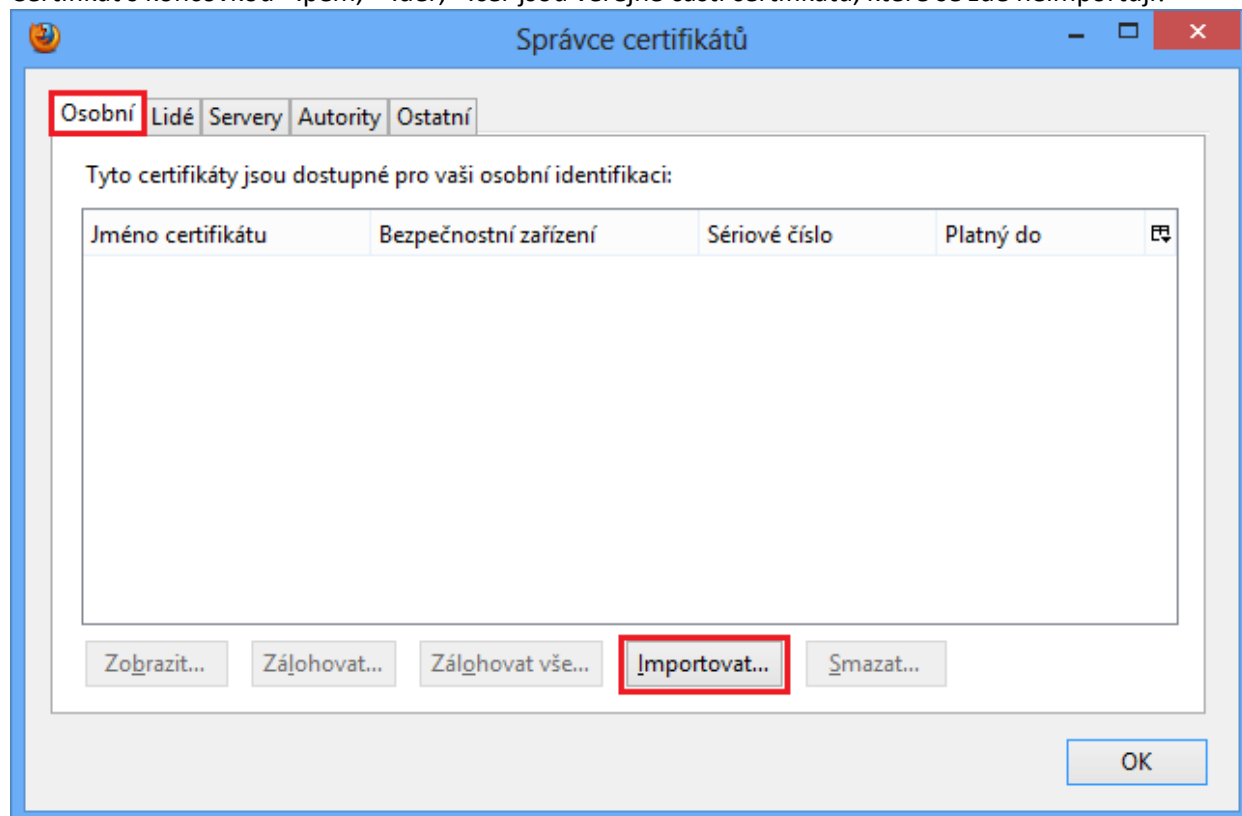


Přepněte se do Rozšířené - Certifikáty - Certifikáty.

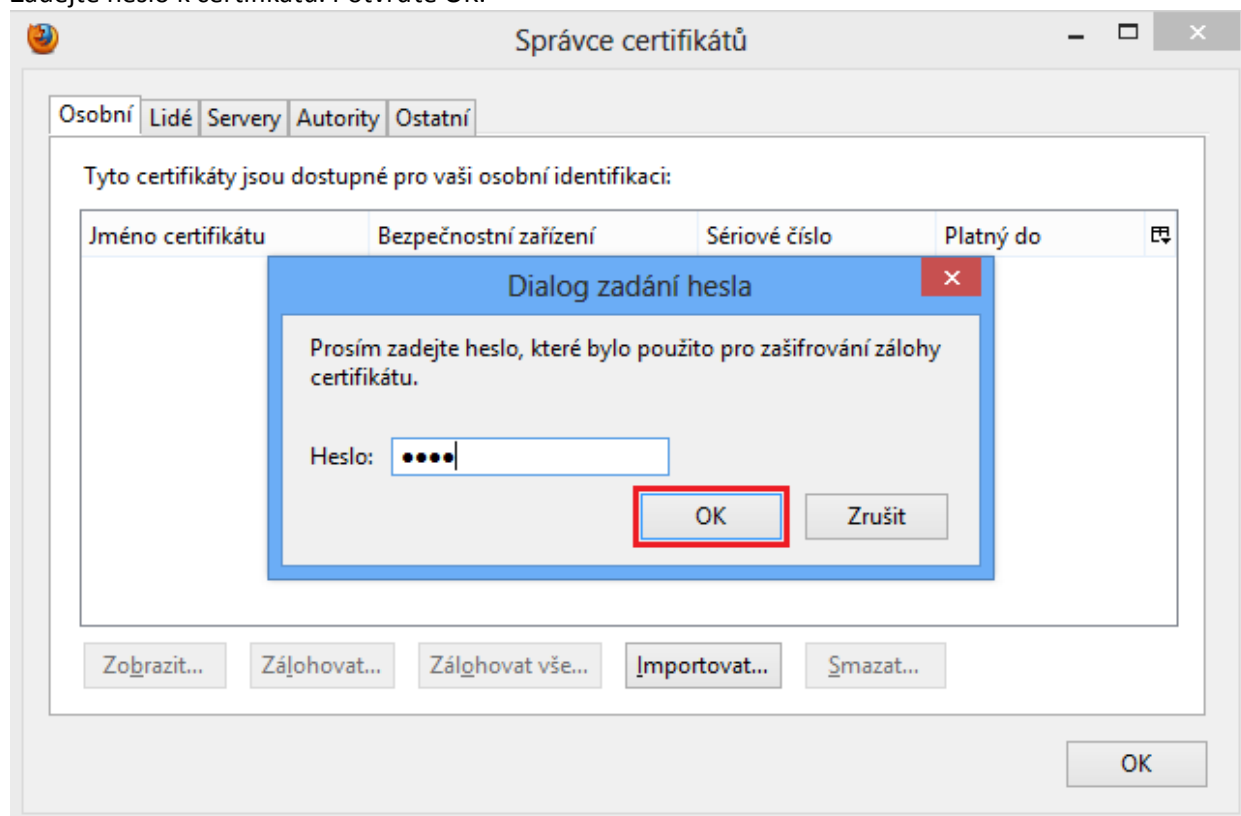


V záložce Osobní zvolte Importovat a vyberte místo, kde máte uložený privátní klíč. Privátní klíč poznáte podle koncovky *.pfx nebo *.p12

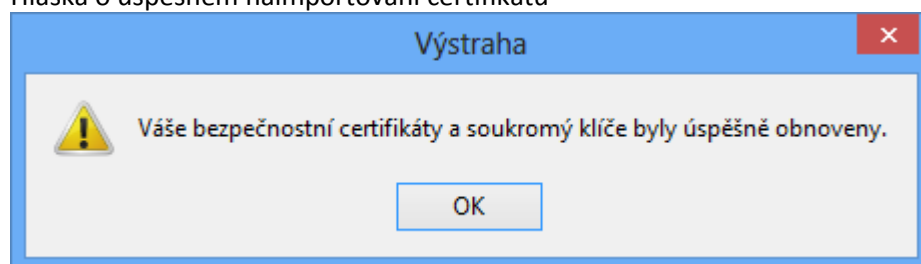
Certifikát s koncovkou *.pem, *.der, *.cer jsou veřejné části certifikátu, které se zde neimportují!



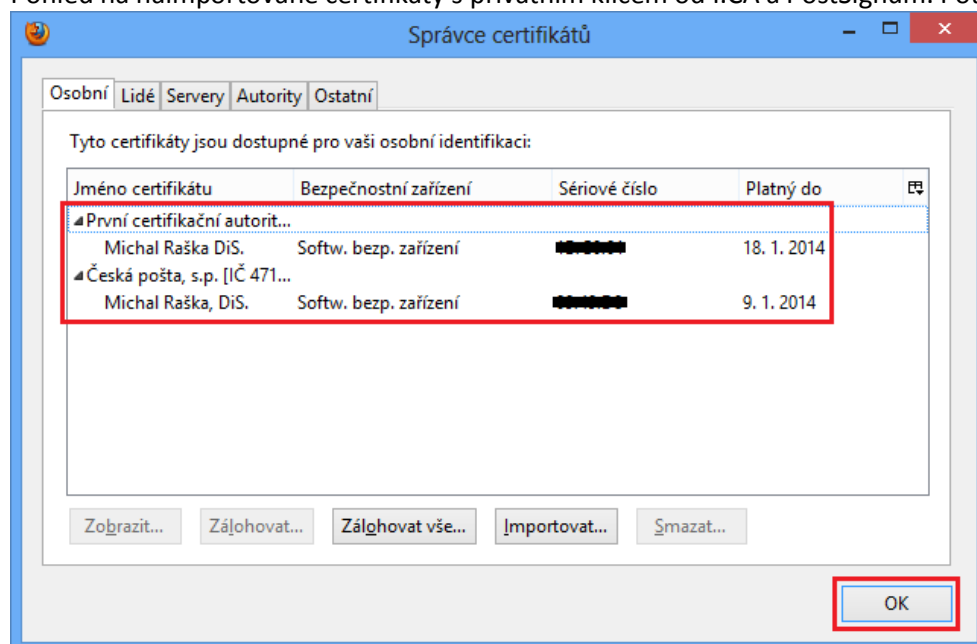
Zadejte heslo k certifikátu. Potvrďte OK.



Hláška o úspěšném naimportování certifikátu

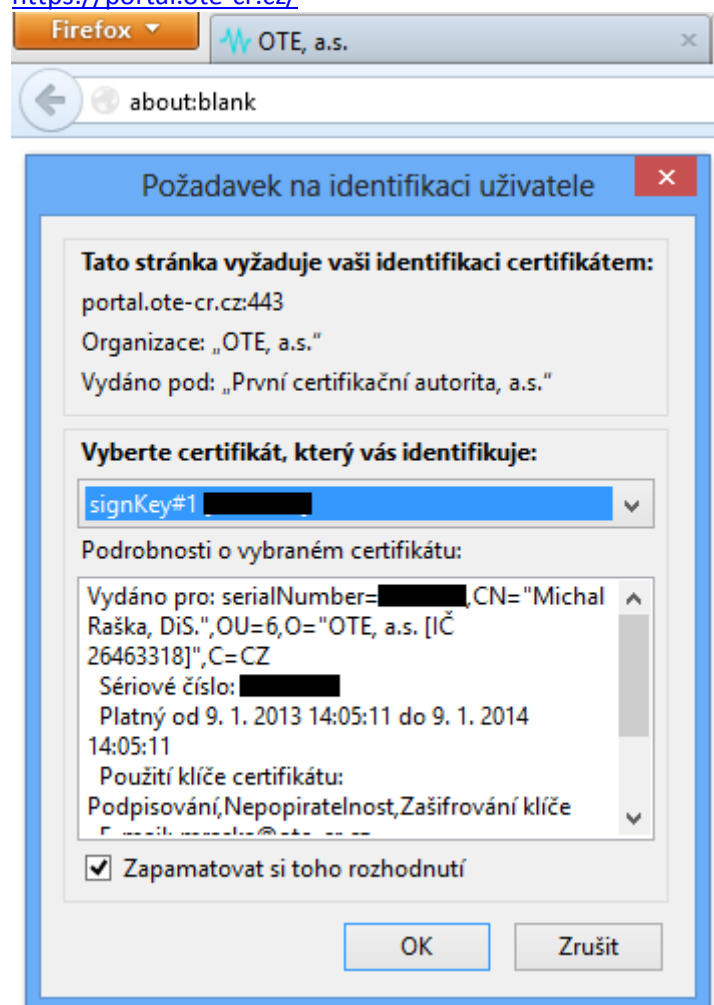


Pohled na naimportované certifikáty s privátním klíčem od I.CA a PostSignum. Potvrďte OK.



Přihlaste se na adresu obchodního systému CS OTE

<https://portal.ote-cr.cz/>



Při prvním přihlašování Vám vyskočí hláška o přidání stránek obchodního portálu OTE do důvěryhodných. Klikněte na řádek „Vím, o co se jedná“ a potom na „Přidat výjimku“.



Toto připojení není důvěryhodné

Požádali jste Firefox o zabezpečené připojení k serveru **portal.ote-cr.cz**, ale nelze ověřit, že tomu tak skutečně je.

Pokud je požadováno zabezpečené připojení, měl by server předložit důvěryhodnou identifikaci a tím prokázat, že se připojujete na správné místo. Nicméně, identita tohoto serveru nemohla být ověřena.

Co mám teď dělat?

Pokud se k tomuto serveru obvykle připojujete bez problému, může tato chyba znamenat, že se za tento server někdo snaží vydávat, a neměli byste pokračovat.

[Rychle odsud pryč!](#)

► **Technické detaily**

▼ **Vím, o co se jedná**

Pokud chápete rizika, můžete Firefox požádat o výjimku a začít identifikaci tohoto serveru důvěřovat. I když tomuto serveru důvěřujete, může tato chyba znamenat, že vám někdo odposlouchává připojení.

Nepřidávejte výjimku, pokud si nejste jisti, že tento server má dobrý důvod nepoužívat důvěryhodnou identifikaci.

[Přidat výjimku...](#)

V dalším okně klikněte na „Získat certifikát“ a potom na „Schválit bezpečnostní výjimku“

Přidání bezpečnostní výjimky

Chystáte se změnit způsob, jakým aplikace Firefox identifikuje tento server.

Legitimní banky, obchody a ostatní veřejné servery vás o toto žádat nebudou.

Server

Adresa:

[Získat certifikát](#)

Stav certifikátu

Tento server se prokazuje neplatnými informacemi. [Zobrazit...](#)

Neznámá identita

Certifikát je nedůvěryhodný, protože nebyl ověřen důvěryhodnou autoritou pomocí bezpečného podpisu.

☒ Uložit tuto výjimku trvale

[Schválit bezpečnostní výjimku](#) [Zrušit](#)

Nyní jste se přihlásili do obchodního systému CS OTE prostřednictvím prohlížeče Firefox



Důležité upozornění chování prohlížeče Firefox při odesílání a podepisování dat!

Při odesílání dat Vám vyskočí okno, kde si zkontrolujete, jakým certifikátem data podepisujete. Ve spodní části okna je pole pro zadání hesla. Jde o dodatečné/extra heslo, které je možné ve Firefoxu zadat navíc k Vašemu certifikátu. Nejde o heslo, jaké máte nastavené u certifikátu, které jste použili při importu certifikátu. Pokud jste si sami toto dodatečné heslo nenastavili (v tomto manuálu to není popsáno), tak toto pole nevyplňujte!!!

