

Uživatelský přístup do centrálního systému operátora trhu (CS OTE) - přechod z komerčních certifikátů na kvalifikované.

Od 1. 7. 2017 bude možné v systému OTE registrovat pouze kvalifikované certifikáty. Komerční certifikáty registrované v CS OTE nebude po 1. 10. 2017 možné použít pro přístup do systému CS OTE ani pro zadávání dat.

Pokud jste držiteli komerčního certifikátu a zadáváte data o výrobě do CS OTE, doporučujeme pořídit si kvalifikovaný certifikát co nejdříve.

Změna přístupu vychází z evropského nařízení č. 910/2014 (eIDAS) a zákona č. 297/2016, o službách vytvářejících důvěru v elektronické transakce.

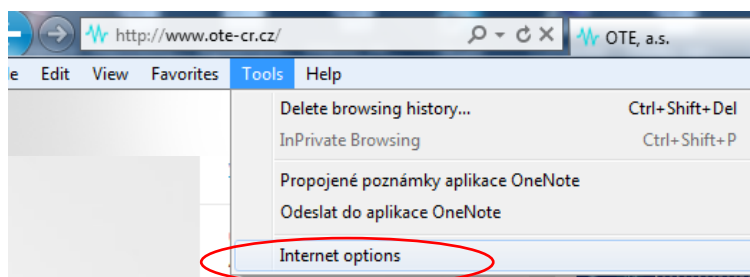
Podporované certifikační autority kvalifikovaných certifikátů:

Certifikační Autorita	Země	Doporučený Certifikát	Odkaz
PostSignum (Česká pošta)	Česká republika	Kvalifikovaný certifikát	http://www.postsignum.cz/
První certifikační autorita, a.s.	Česká republika	Kvalifikovaný certifikát	http://www.ica.cz/
eidentity a.s.	Česká republika	Kvalifikovaný certifikát	http://www.eidentity.cz/app

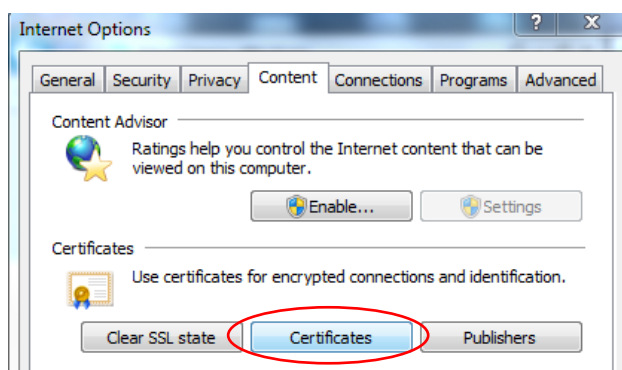
Pokud si nejste jistí, jaký typ certifikátu máte, obraťte se na Vaši certifikační autoritu, která Vám certifikát vydala. Kontrolu je možné rovněž provést manuálně v počítači podle následujícího postupu.

1. Kontrola certifikátu podporované certifikační autority v prohlížeči Internet Explorer

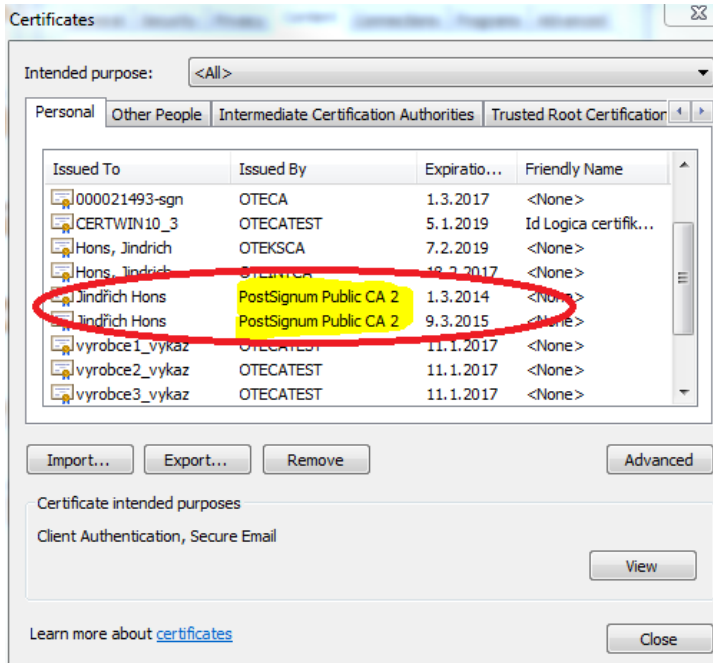
- 1. Krok** - V Internet Explorer vyberte pole Nástroje (Tools), pole Nástroje lze také nalézt pod symbolem ozubeného kolečka, vpravo nahoře. Dále zvolte Možnosti internetu (Internet Options)



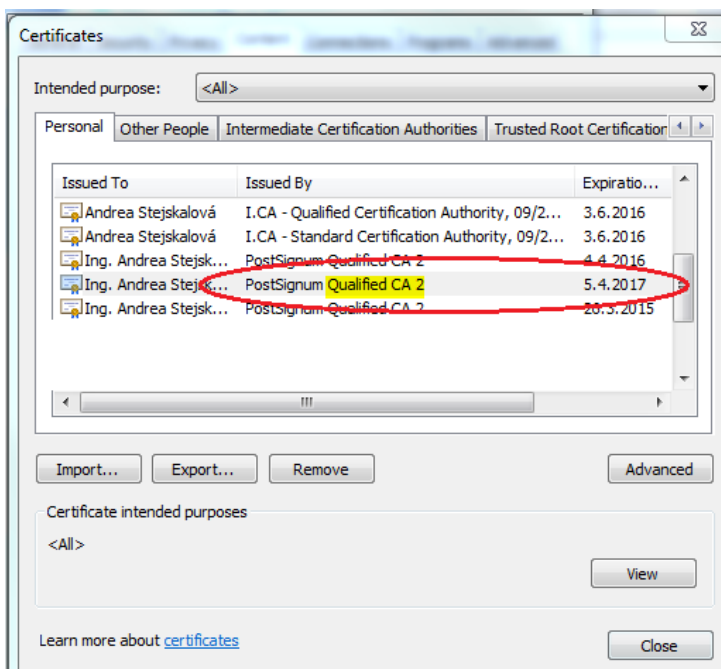
- 2. Krok** - Na záložce Obsah (Content) zvolte pole Certifikáty (Certificates)



3. Krok – Zkontrolujte, zda máte kvalifikovaný certifikát (např. PostSignum QCA)



ŠPATNĚ



SPRÁVNĚ

Pokud jste držitelem kvalifikovaného certifikátu, který je registrován v CS OTE, není třeba pro komunikaci s OTE cokoli měnit!!!!

Podle následujících pokynů postupujte pouze v případě, že nejste držitelem kvalifikovaného certifikátu registrovaným v CS OTE!!!

2. Generování a instalace kvalifikovaného certifikátu

Generování a instalaci kvalifikovaného certifikátu provedete dle pokynů příslušné certifikační autority na příslušných web. stránkách :

Certifikační Autorita	Země	Odkaz
PostSignum (Česká pošta)	Česká republika	http://www.postsignum.cz/kvalifikovane_certifikaty.html
První certifikační autorita, a.s.	Česká republika	http://www.ica.cz/ziskat-kvalifikovany-certifikat-pro-ePodpis
eIdentity a.s.	Česká republika	https://www.eidentity.cz/registration/EasyRequest.html

3. Zaregistrování veřejné části certifikátu do CS OTE

Veřejný klíč certifikátu zaregistruje do systému:

- 1) přímo uživatel postupem uvedeným níže, tj. kroky 1-19, nebo
- 2) osoba s aktivní rolí „Správa vlastních údajů RÚT“ v případě, že sám uživatel nemá práva k přidání vlastního certifikátu, postupem uvedeným níže, tj. kroky 1-19.

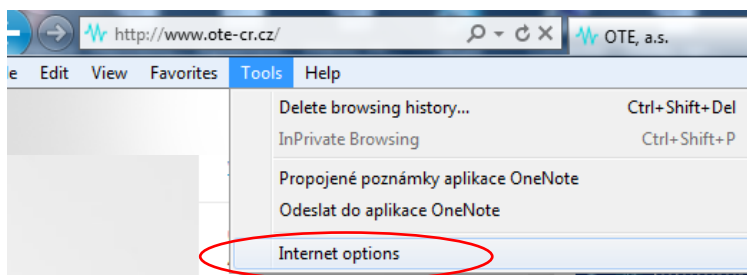
Upozorňujeme, že v případě, že má uživatel nahrán v portálu CS OTE v současné chvíli komerční osobní certifikát a nyní si vystaví certifikát kvalifikovaný, nedojde k automatickému nahrání veřejné části kvalifikovaného certifikátu do portálu CS OTE. Veřejnou část certifikátu je třeba nahrát do systému ručně.

Pokud uživateli nelze dohrát veřejnou část kvalifikovaného certifikátu ani pověřenou osobou s aktivní rolí „Správa vlastních údajů RÚT“, zašlete na e-mail Poze@ote-cr.cz platnou veřejnou část Vašeho kvalifikovaného certifikátu (soubor s příponou *.crt nebo *.cer), kterou požadujete do portálu CS OTE nahrát. Případně lze přeposlat e-mail od Postsignum (pokud se jedná o certifikát od Postsignum), ve kterém bude aktivní odkaz na veřejnou část kvalifikovaného certifikátu (e-mail s názvem „Upozornění na připravený certifikát“).

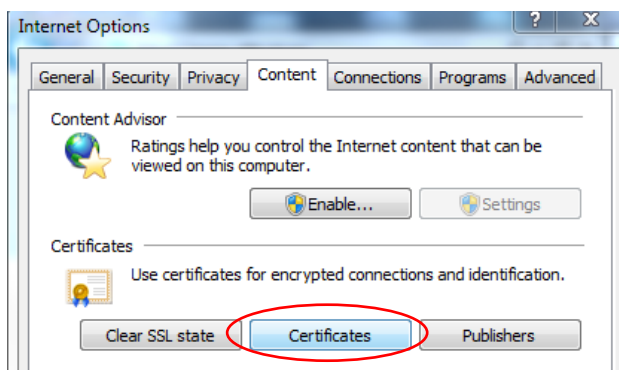
Certifikát může být uložen na hardwarovém zařízení (bezpečnostním tokenu) nebo může mít uživatel softwarový certifikát (uložený přímo v počítači) a to od výše uvedených certifikačních autorit.

Vygenerování veřejné části certifikátu pomocí prohlížeče Internet Explorer

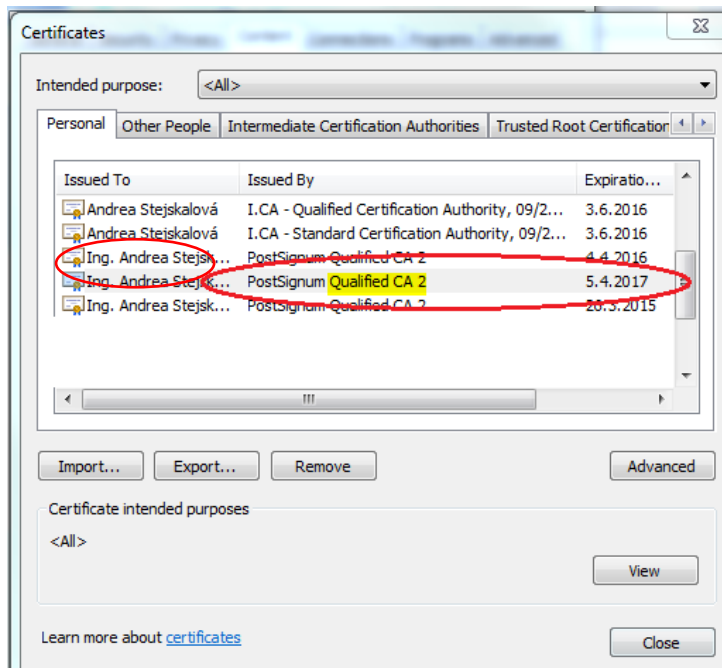
1. Krok - V Internet Explorer vyberte pole Nástroje (Tools) a zvolte Možnosti internetu (Internet options)



2. Krok - Na záložce Obsah (Content) zvolte pole Certifikáty (Certificates)



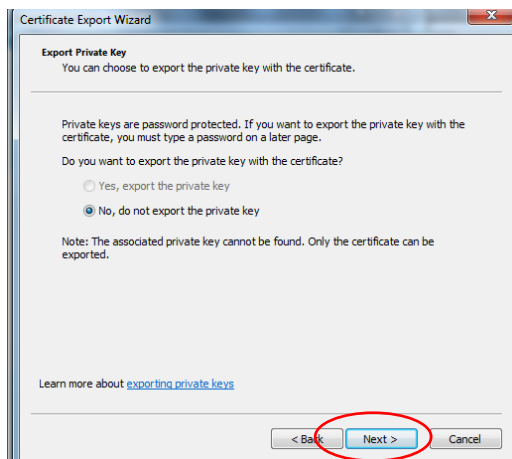
3. Krok - V seznamu certifikátů vyberete platný kvalifikovaný certifikát vydaný odpovídající certifikační autoritou a zvolíte tlačítko Export



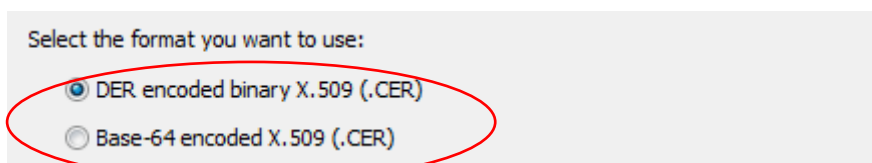
4. Krok - Zvolte pole Další (Next)



5. Krok - Ponechte nastavení a zvolte opět pole Další (Next)

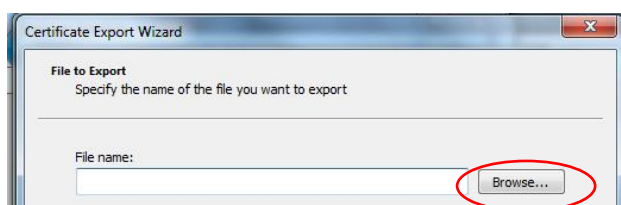


6. Krok - Zvolte formát **DER** nebo **Base-64** a stiskněte tlačítko Další (Next).
Jiný formát veřejné části certifikátu není možné do systému OTE zaregistrovat.

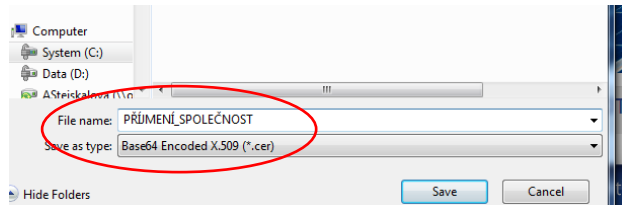


Zvolte tlačítko NEXT

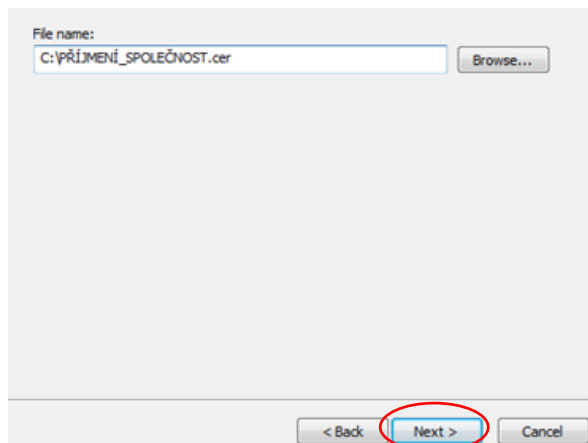
7. Krok - Vyberte místo pro uložení souboru na disku přes tlačítko Procházet (Browse).



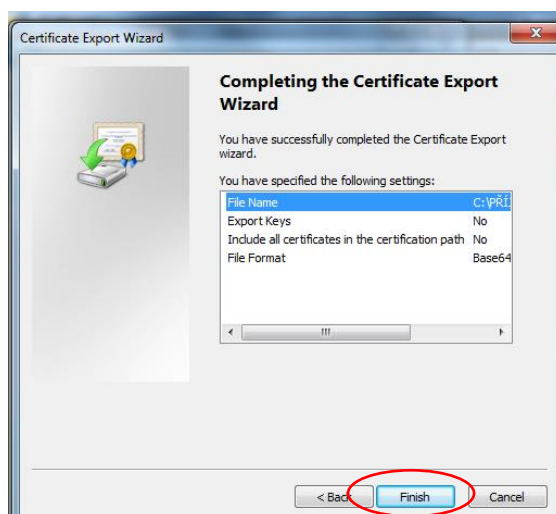
8. Krok - Zadejte libovolný název souboru (File name), např. Příjmení_název společnosti a soubor uložte (Save)



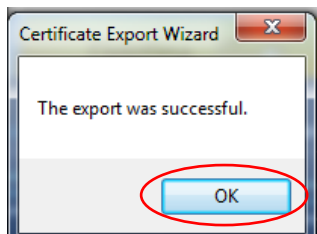
9. Krok - Zvolte pole další (Next)



10. Krok - Zvolte pole dokončit (Finish)

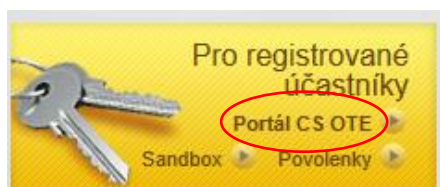


11. Krok - Úspěšný export bude potvrzen následujícím dialogem.

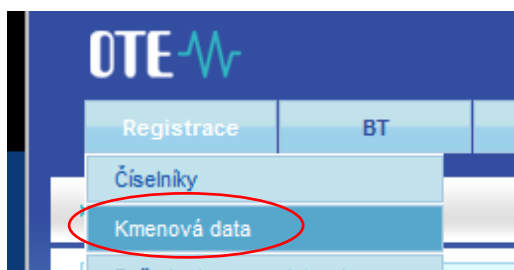


Nahrání veřejné části certifikátu do CS OTE

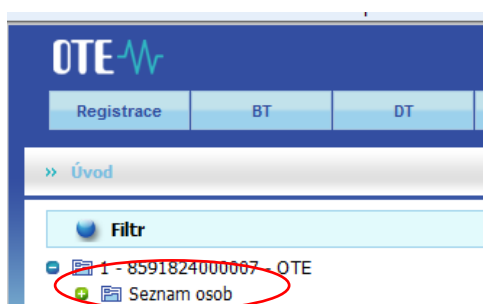
12. Krok – Přihlaste se do systému OTE přes svůj registrovaný platný certifikát.



13. Krok – Zvolte záložku Registrace a dále Kmenová data



14. Krok – Rozklikněte seznam osob a dále kliknete na jméno uživatele, ke kterému bude certifikát registrován



15. Krok – Na záložce Zabezpečený přístup zvolte pole Nový certifikát

The screenshot shows the 'Zabezpečený přístup' tab selected. Below the tabs is a toolbar with several icons, including a 'New' icon (a document with a plus sign) which is circled in red. Below the toolbar is a table with the following columns: Typ certifikátu, Certifikační autorita, Přihlášení, Odhlášení, DN, and Primární certifikát.

16. Krok – Přes tlačítko procházet (Browse) a vyhledejte uloženou veřejnou část certifikátu. Stejný postup opakujte i pro Podpisovou část. Pokud používáte pouze jeden certifikát, zaregistruje stejnou veřejnou část k oběma polím (Autentizační i Podpisový).

The screenshot shows the 'Zabezpečený přístup' tab. Below the tabs is a toolbar with icons. Below the toolbar is a table with columns: Typ certifikátu, Certifikační autorita, Platnost od, Platnost do, DN, and Primární certifikát. Below the table are two input fields: 'Autentizační' and 'Podpisový'. Each field has a 'Browse...' button next to it, both of which are circled in red. There is also a 'Nahrát certifikáty' button and an 'OK' button at the bottom right.

17. Krok – Po vybrání certifikátů stiskněte pole Nahrát certifikáty.

The screenshot shows the 'Zabezpečený přístup' tab. Below the tabs is a toolbar with icons. Below the toolbar is a table with columns: Typ certifikátu, Certifikační autorita, Platnost od, Platnost do, DN, and Primární certifikát. Below the table are two input fields: 'Autentizační' and 'Podpisový'. Each field has a text box containing 'C:\Users\astejskalova\De' and a 'Browse...' button. Below these fields is a 'Nahrát certifikáty' button and an 'OK' button at the bottom right.

18. Krok – Zaregistrování veřejných částí certifikátů potvrďte tlačítkem OK.

Základní kontaktní údaje **Zabezpečený přístup** Činnosti Role

Typ certifikátu Certifikační autorita Platnost od Platnost do DN Primární certifikát

Autentizační Browse...

Podpisový Browse... Nahrát certifikáty

OK

19. Krok – Obnovu certifikátu je potřeba potvrdit - podepsat původním certifikátem!

Podepsání a odeslání dat

Opravdu chcete podepsat data a odeslat na server?

OK Zavřít

Security Alert

This Web site needs access to digital certificates on this computer.

WARNING: By allowing access to your certificates, this Web site will also gain access to any personal information that are stored in your certificates.

Do you want this Web site to gain access to the certificates on this computer now?

Yes No

Po úspěšném zaregistrování veřejné části certifikátu se pod původní certifikát zobrazí obnovený certifikát.

Základní kontaktní údaje Zabezpečený přístup Činnosti Role

Typ certifikátu	Certifikační autorita	Platnost od	Platnost do	DN	Primární certifikát
Autentizační	C=CZ,O=Česká pošta \, s.p. [IČ 47114983],CN=PostSignum Qualified CA 2	26.03.2013 15:39:41	26.03.2014 15:39:41	C=CZ,O=OTE \, a.s. [IČ 26463318],OU=1,CN=Ing. Andrea Stejskalová,SERIALNUMBER=P251225	<input checked="" type="radio"/>
Podpisový	C=CZ,O=Česká pošta \, s.p. [IČ 47114983],CN=PostSignum Qualified CA 2	26.03.2013 15:39:41	26.03.2014 15:39:41	C=CZ,O=OTE \, a.s. [IČ 26463318],OU=1,CN=Ing. Andrea Stejskalová,SERIALNUMBER=P251225	<input type="radio"/>
Autentizační	C=CZ,O=Česká pošta \, s.p. [IČ 47114983],CN=PostSignum Qualified CA 2	06.03.2014 14:54:41	26.03.2015 14:54:41	C=CZ,O=OTE \, a.s. [IČ 26463318],OU=1,CN=Ing. Andrea Stejskalová,SERIALNUMBER=P251225	<input type="radio"/>
Podpisový	C=CZ,O=Česká pošta \, s.p. [IČ 47114983],CN=PostSignum Qualified CA 2	06.03.2014 14:54:41	26.03.2015 14:54:41	C=CZ,O=OTE \, a.s. [IČ 26463318],OU=1,CN=Ing. Andrea Stejskalová,SERIALNUMBER=P251225	<input type="radio"/>

Informace „**Primární certifikát**“ nemá z pohledu účinnosti certifikátu význam a je vedena pouze jako technická informace pro správce systému.

Upozorňujeme, že změna v systému OTE není nikterak vázána na platnost komerčních certifikátů, které jsou aktuálně registrovány v CS OTE. Tyto certifikáty nebude po 1. 10. 2017 možné výrobci pro přístup do systému CS OTE ani pro zadávání dat použít.