Certifikáty od podporovaných certifikační autority pro CS OTE

Od 1. 10. 2017 bude umožněno pro elektronický podpis a přístup do webového prostředí CS OTE použít pouze kvalifikovaný certifikát. Od 1. 7. 2017 bude možné registrovat pro přístup do webového prostředí CS OTE a elektronické podepisování pouze kvalifikované certifikáty. Uživatelům CS OTE bude umožněno ve webovém prostředí CS OTE používat původní certifikáty (komerční certifikáty vč. OTECA) do 30. 9. 2017.

Změna přístupu vychází z nařízení evropského parlamentu a rady (EU) č. 910/2014 (eIDAS) a zákona č. 297/2016, o službách vytvářejících důvěru v elektronické transakce. Používání kvalifikovaných certifikátů v CS OTE respektuje stanovisko ministerstva vnitra, které je dostupné – zde.

Certifikáty OTECA a OTECA-TEST vydávané společností CGI IT Czech Republic s.r.o. nebudou od 1. 10. 2017 v CS OTE podporovány. Jejich vydávání a obnova nebude k 1.5.2017 zajištěna.

Pro **elektronický podpis v automatické komunikaci** (vytváření elektronické značky) bude možné od 1.7.2017 až do odvolání registrovat pouze **kvalifikované systémové certifikáty** a to až do doby, kdy budou dostupné kvalifikované certifikáty pro elektronické pečetě, které tyto systémové certifikáty nahradí. Od 1.10.2017 nebude možné použít komerční certifikáty k vytváření elektronické značky (automatizovanému podpisu).

Pro **účely zasílání šifrovaných zpráv do CS OTE** prostřednictvím zabezpečeného emailu operátor trhu nahradí původní certifikát OTECA **komerčním certifikátem.** Nový komerční certifikát OTE bude ke stažení umístěn na webových stránkách OTE, o čemž bude operátor trhu informovat uživatele v blízké době. Pro účely příjmu šifrovaných zpráv z CS OTE prostřednictvím zabezpečeného emailu účastníkem trhu, bude muset účastník trhu od 1.10.2017 disponovat komerčním certifikátem.

Pro aplikaci OTECOM bude muset účastník trhu pro přihlášení k aplikaci použít **komerční certifikát od 1.10.2017,** který uživatel používá jako za současného stavu. Pro elektronický podpis dat platí stejná pravidla jako v případě webového portálu, tzn. veškerá data musí být od 1. 10. 2017 podepsána pouze kvalifikovaným certifikátem.

Plánovaná změna se netýká uživatelů, kteří již pro komunikaci do webového prostředí CS OTE kvalifikovaný certifikát používají. Seznam certifikačních autorit vydávajících kvalifikované certifikáty pro elektronický podpis v CS OTE je uveden níže.

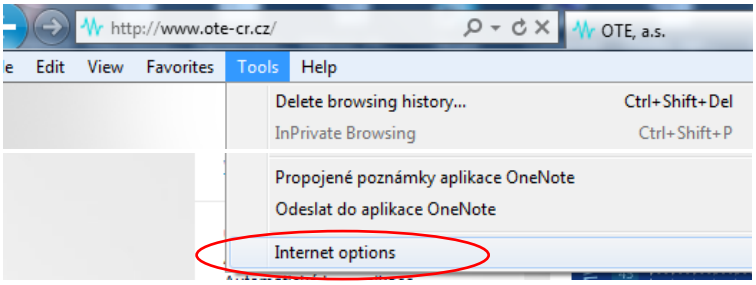
Seznam certifikátů je možné rozšířit na základě žádosti účastníka trhu o prověření dané autority operátorem trhu – kontaktujte prosím services@ote-cr.cz

Autorita Odkaz	**Země**	**Komerční CA** **(autentizace a šifrování)**	**Kvalifikovaná CA** **(pouze el. podpis/značka/pečeť)**	**Pozn.**
První certifikační autorita, a.s. http://www.ica.cz/	CZ	**ANO** všechny komerční certifikáty	**ANO** I.CA Qualified 2 CA/RSA 02/2016 I.CA - Qualified Certification Authority, 09/2009 I.CA - Qualified root certificate	
Česká pošta, s.p. (PostSignum) http://www.postsignum.cz/	CZ	**ANO** všechny komerční certifikáty	**ANO** PostSignum Qualified CA PostSignum Qualified CA 2 PostSignum Qualified CA 3	
eIdentity a.s. http://www.eidentity.cz/app	CZ	**ANO** všechny komerční certifikáty	**ANO** ACAeID2.1 - Qualified Issuing Certificate (kvalifikovaný systémový certifikát vydávající CA)	
NetLock Ltd http://www.netlock.hu/	HU	**ANO** NetLock (Class B Legal) NETLOCK Trust Advanced CA	**ANO** NetLock (Class QA) NetLock (Class Q Legal) NetLock (Class Q) NetLock (Class Q Legal Spec.)	
GLOBALTRUST http://www.globaltrust.eu/	AU	**ANO** GLOBALTRUST ADVANCED 1 GLOBALTRUST CLIENT 1 A-CERT CLIENT (jen stávající) A-CERT ADVANCED (jen stávající)	**ANO** GLOBALTRUST QUALIFIED 1 GLOBALTRUST 2015 QUALIFIED 1	Dříve ARGE DATEN
QuoVadis https://www.quovadisglobal.com/	CH/BE	**ANO** QuoVadis Swiss Advanced CA G2	**ANO** QuoVadis Belgium Issuing CA G1 QuoVadis Belgium Issuing CA G2	
GeoTrust https://www.geotrust.com/	US	**ANO** GeoTrust SSL CA - G3	**NE**	
GoDaddy.com https://uk.godaddy.com/	US	**ANO** GD Root Certificate Authority - G2	**NE**	

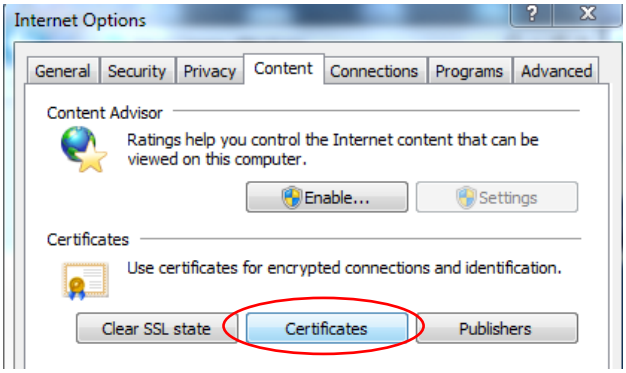
1. Kontrola certifikátu od podporované certifikační autority

- ✓ **Pro přístup do CS OTE prostřednictvím webového portálu a elektronický podpis** bude vyžadováno použití **kvalifikovaných certifikátů** od kvalifikovaných autorit.
- ✓ Pro **přístup do aplikace OTECOM a šifrování e-mailových zpráv** bude možné použít pouze **komerční certifikáty** od komerčních autorit.

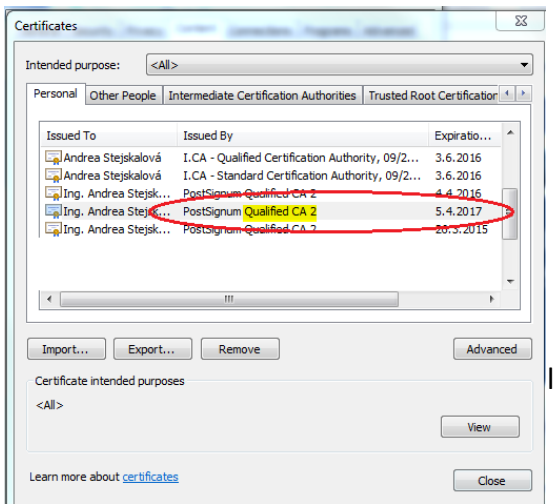
1. **Krok -** V Internet Explorer vyberte pole Tools a zvolte Internet Options



2. **Krok -** Na záložce Content zvolte pole Certificates

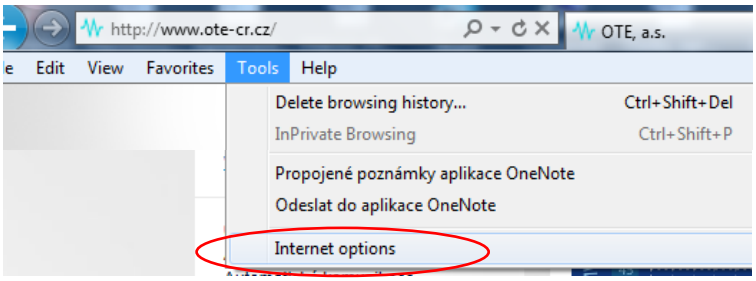


3. **Krok –** Zkontrolujte, zda máte kvalifikovaný certifikát.

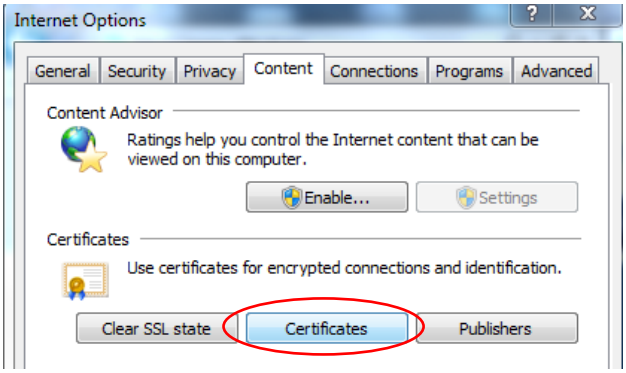


2. Vygenerování veřejné části certifikátu

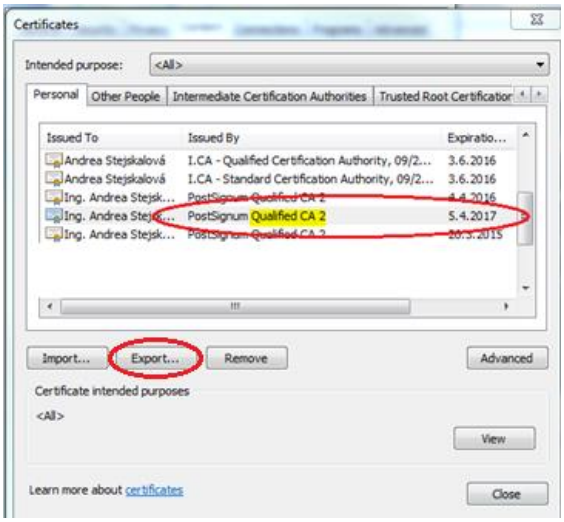
1. **Krok -** V Internet Explorer vyberte pole Tools a zvolte Internet Options



2. **Krok -** Na záložce Content zvolte pole Certificates

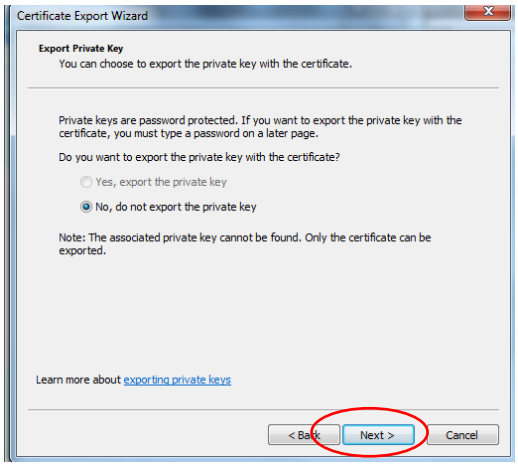


3. **Krok -** V seznamu certifikátů vyberete platný kvalifikovaný certifikát vydaný odpovídající certifikační autoritou a zvolíte tlačítko Export

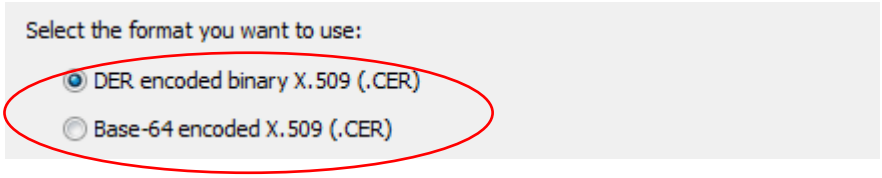


4. **Krok -** Zvolte pole **Next**

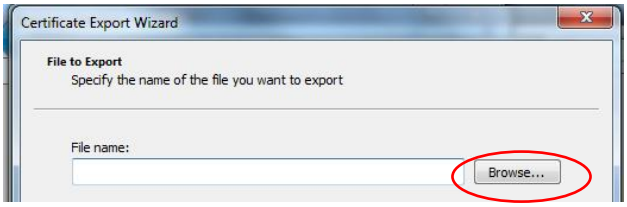
5. **Krok -** Ponechte nastavení a zvolte opět pole **Next**



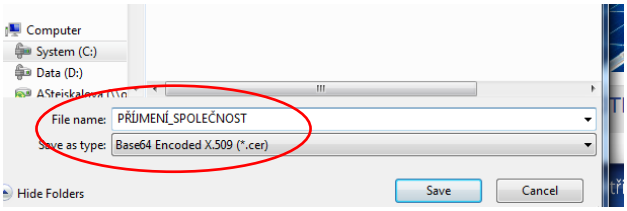
6. **Krok -** Zvolte formát **DER** nebo **Base-64 a stiskněte tlačítko Next.**
   Jiný formát veřejné části certifikátu není možné do systému OTE zaregistrovat.



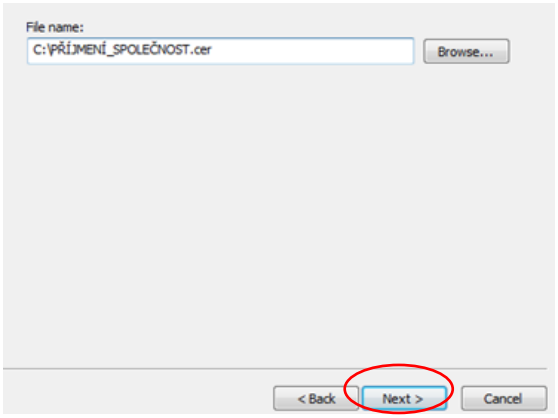
7. **Krok -** Vyberte místo pro uložení souboru na disku přes tlačítko Browse.



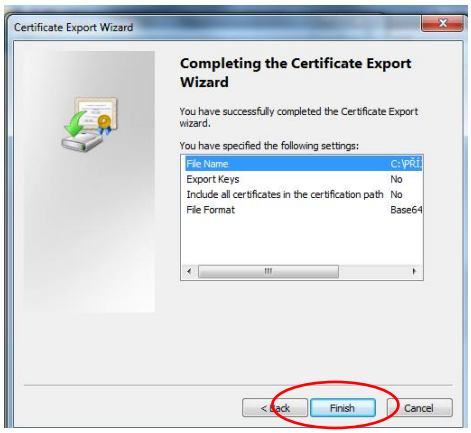
8. **Krok -** Zadejte název souboru (File name), např. Příjmení_název společnosti a soubor uložte (Save)



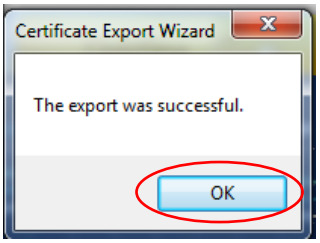
9. **Krok -** Zvolte pole Next



10. **Krok -** Zvolte pole Finish



11. Krok - Úspěšný export bude potvrzen následujícím dialogem.



3. Zaregistrování veřejné části certifikátu do CS OTE

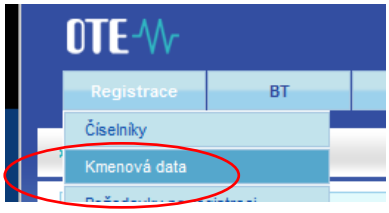
Veřejná část certifikátu musí být zaregistrována do CS OTE. Po jejím zaregistrování se uživatel může přihlašovat do CS OTE. Postup registrace veřejné části je následují:

A) Uživatel registruje do CS OTE nový certifikát (poprvé) nebo **platnost jeho původního certifikátu již vypršela**. V tomto případě se uživatel do systému nemůže přihlásit a jeho veřejnou část certifikátu do systému registruje Pověřená osoba, která má za danou společnost nastavena administrátorská práva. V CS OTE v seznamu uživatelů je Pověřená osoba zvýrazněna tučně. Pověřená osoba postupuje při registraci certifikátu dle níže uvedených kroků 1 - 6.

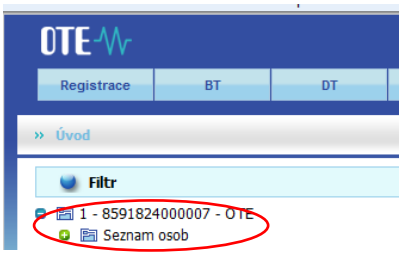
B) Uživatel registruje do CS OTE obnovený certifikát a **jeho původní certifikát je v CS OTE stále platný**. Veřejný klíč certifikátu zaregistruje do systému přímo uživatel. Uživatel může zaregistrovat certifikát pouze ke svému uživatelskému účtu. Uživatel postupuje při registraci certifikátu dle níže uvedených kroků 1 - 6.

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

2. Krok – Zvolte záložku Registrace a dále Kmenová data



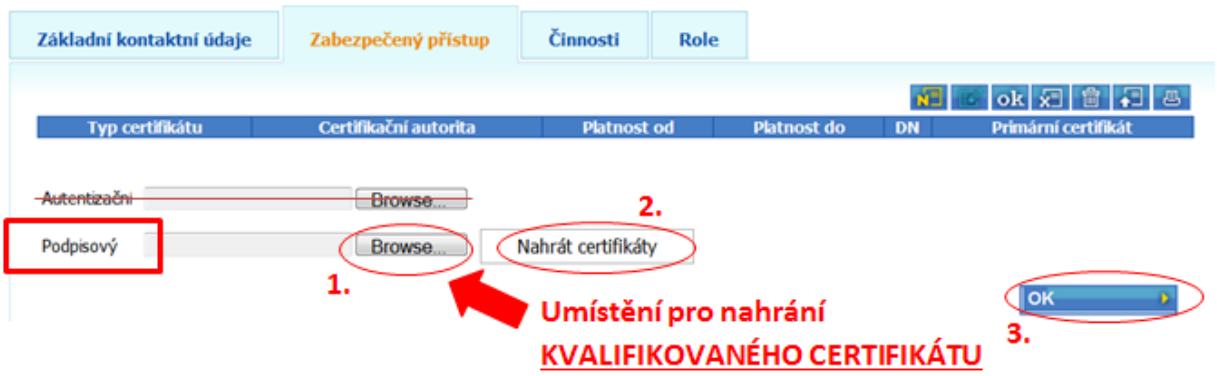
3. Krok – Rozklikněte seznam osob a dále kliknete na jméno uživatele, ke kterému bude certifikát registrován.



4. Krok – Na záložce Zabezpečený přístup zvolte pole „N“ - Nový certifikát

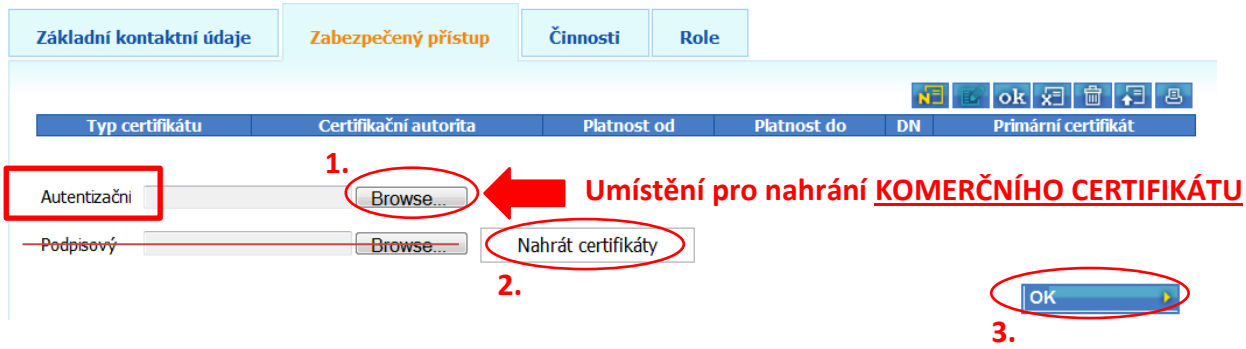
5. Krok – Nahrání veřejné části certifikátu provede uživatel přes tlačítko Browse. Příslušnou veřejnou část certifikátu nahrajte následovně:

✓ **Typ „Kvalifikovaný“ (do 1.7.2017 Podpisový) – slouží pro přístup do CS OTE prostřednictvím webového portálu a pro elektronické podepisování.**



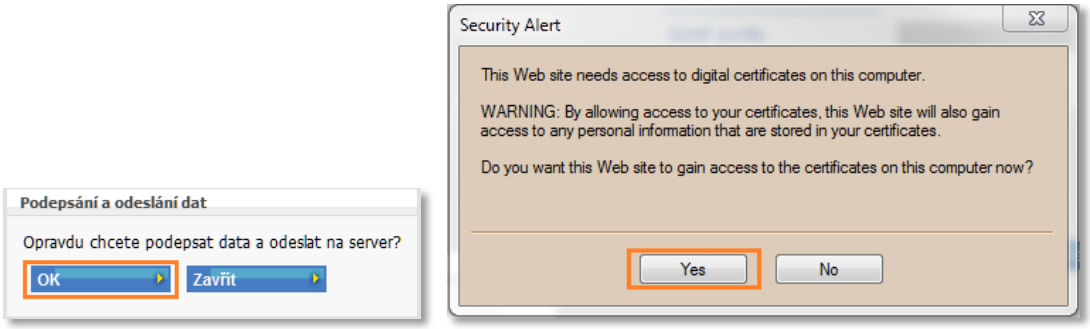
Od 1. 7. 2017 bude v CS OTE název rubriky změněn z „Podpisový“ na „Kvalifikovaný“.

- ✓ **Typ „Komerční“ (do 1.7.2017 Autentizační) – slouží pro účely přístupu OTECOM, TLS autentizace a šifrování e-mailových zpráv.**



Od 1. 7. 2017 bude název rubriky změněn z „Autentizační“ na „Komerční“.

6. Krok – Nahrání veřejné části certifikátu je potřeba potvrdit - podepsat původním certifikátem**.**



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