

informačního systému Uživatelská příručka



Konfigurace klientských statnic

Tento dokument a jeho obsah je důvěrný. Dokument nesmí být reprodukován celý ani částečně, ani ukazován třetím stranám nebo používán k jiným účelům, než pro jaké byl poskytnut, bez předchozího písemného schválení společností OTE, a.s.

Datum	Popis změny
31.12.2009	Vytvoření dokumentu
11.1.2011	Odstranění zastaralých informací
5.2.2011	Aktualizace pro nové konfigurace WIN7, Vista a MS Office
20.6.2011	Doplnění nastavení FireFox prohlížeče
1.11.2012	Aktualizace podporovaných konfigurací (IE v9, FireFox v12)
18.6.2013	Aktualizace konfigurací a podpisového balíčku
12.8.2014	Aktualizace podporovaných konfigurací (IE11, WIN8.1)
02.02.2015	Doplnění nové podpisové komponenty pro FireFox
16.03.2015	Aktualizace podpisového balíčku pro IE
23.03.2015	Konfigurace pro SSL/TLS konfigurace
19.12.2016	Aktualizace SafeNet a tokenů
24.1.2017	Aktualizace pro nové prohlížeče Google Chrome a Microsoft Edge

Obsah

1	Certifikované konfigurace stanice	3
2	Instalace přístupu k OTE prostřednictvím USB tokenu iKey 2032, eToken 5000 (dříve iKey 4000) a eToken 5100	4
2.1	<i>Instalace SW Packu Safenet Token Utilities v10.x pro USB token</i>	<i>4</i>
2.2	<i>Nastavení prohlížeče Internet Explorer.....</i>	<i>8</i>
2.2.1	Instalace kořenové autority OTECA	8
2.2.2	Nastavení důvěryhodných stránek	12
2.2.3	Kontrola povolení ActiveX komponent	14
2.2.4	Nastavení kompatibility IE prohlížeče	16
2.2.5	Kontrola nastavení zabezpečené komunikace	18
2.2.6	Instalace podpisového balíčku CGI PKI pro Internet Explorer.....	19
2.2.7	Ruční instalace podpisového balíčku CGI PKI pro Internet Explorer	22
2.3	<i>Nastavení prohlížeče FireFox</i>	<i>22</i>
2.3.1	Import certifikační autority	22
2.4	<i>Nastavení prohlížeče Google Chrome/Microsoft Edge</i>	<i>26</i>
2.4.1	Import certifikační autority	26

1 Certifikované konfigurace stanice

Klientská stanice pro provozování CS OTE je podporována v následující konfigurace operačních systémů:

Windows 7 (32bit) + MS IE11.0/FireFox(32bit)+ SAC 10.x + 3ks SafeNet USB tokenů (iKey 2032, eToken 5000 (dříve iKey 4000), eToken 5100) + Outlook 2016 /x86

Windows 7 (64bit) + MS IE11.0(32bit)/FireFox(32bit) + SAC 10.x + 3ks SafeNet USB tokenů (iKey 2032, eToken 5000 (dříve iKey 4000), eToken 5100) + Outlook 2016/ x64

Windows 10 (32bit) + MS IE11.0/Edge/FireFox/Chrome-poslední verze + SAC 10. x + 3ks SafeNet USB tokenů (iKey 2032, eToken 5000 (dříve iKey 4000), eToken 5100) + Outlook 2016/ x86

Windows 10 (64bit) + MS IE11.0/Edge/FireFox/Chrome-poslední verze + SAC 10. x + 3ks SafeNet USB tokenů (iKey 2032, eToken 5000 (dříve iKey 4000), eToken 5100) + Outlook 2016/ x64

Výše uvedená podporovaná prostředí by měla být aktualizována bezpečnostními update doporučenými MS na

<http://windowsupdate.microsoft.com>.

2 Instalace přístupu k OTE prostřednictvím USB tokenu iKey 2032, eToken 5000 (dříve iKey 4000) a eToken 5100

2.1 Instalace SW Packu Safenet Token Utilities v10.x pro USB token

Pro stažení instalačního balíčku Safenet Token Utilities v10.x je nutné vyplnit objednávkový formulář na odkaze níže

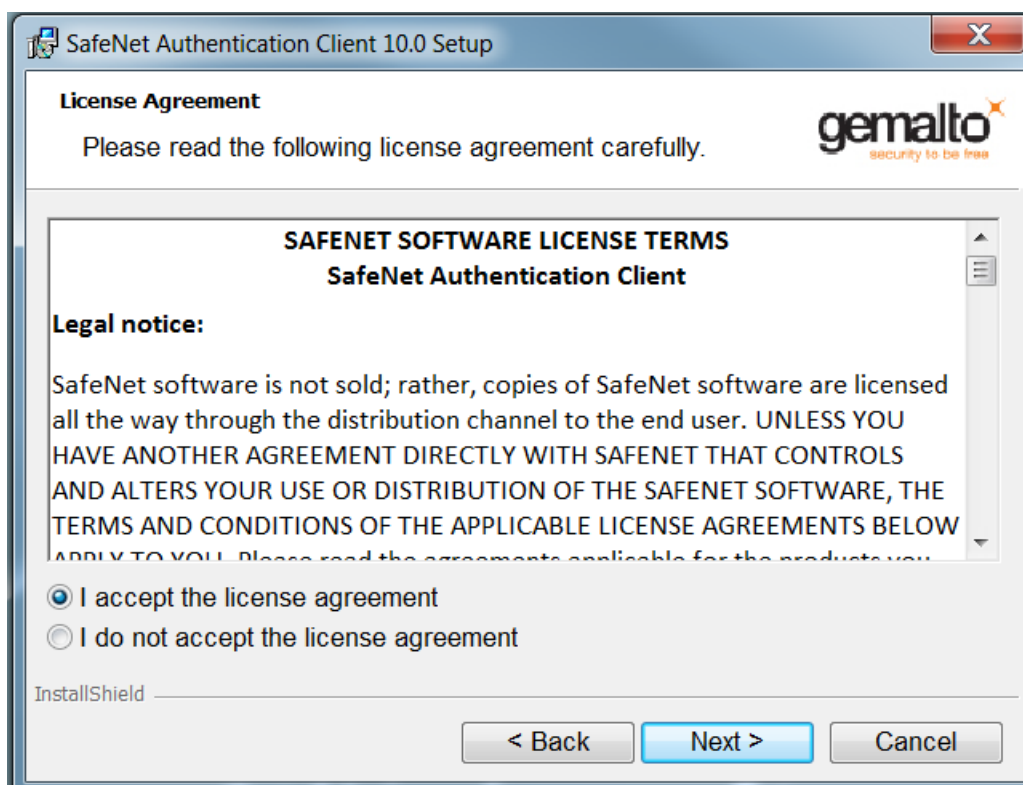
<http://www.ote-cr.cz/registrace-a-smlouvy/files-registrace-a-smlouvy/objednavka-bezpecnostni-prvky-cs-ote.pdf>

Instalaci proveďte **před připojením iKey tokenu!** Spustíte soubor SafeNetAuthenticationClient-x32-x64-10.0.exe (pro 32bit i 64bit OS)). Pokračujte dle postupu níže.



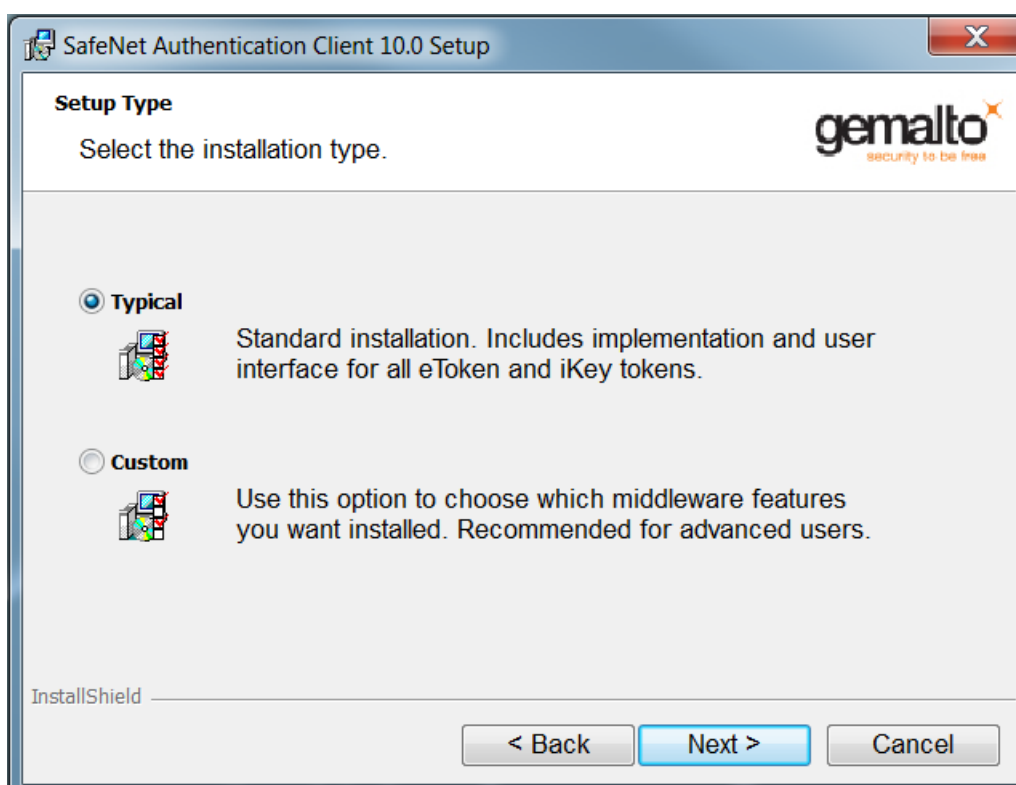


Je možné navolit i jazyk Čeština (Czech) v případě požadavku.





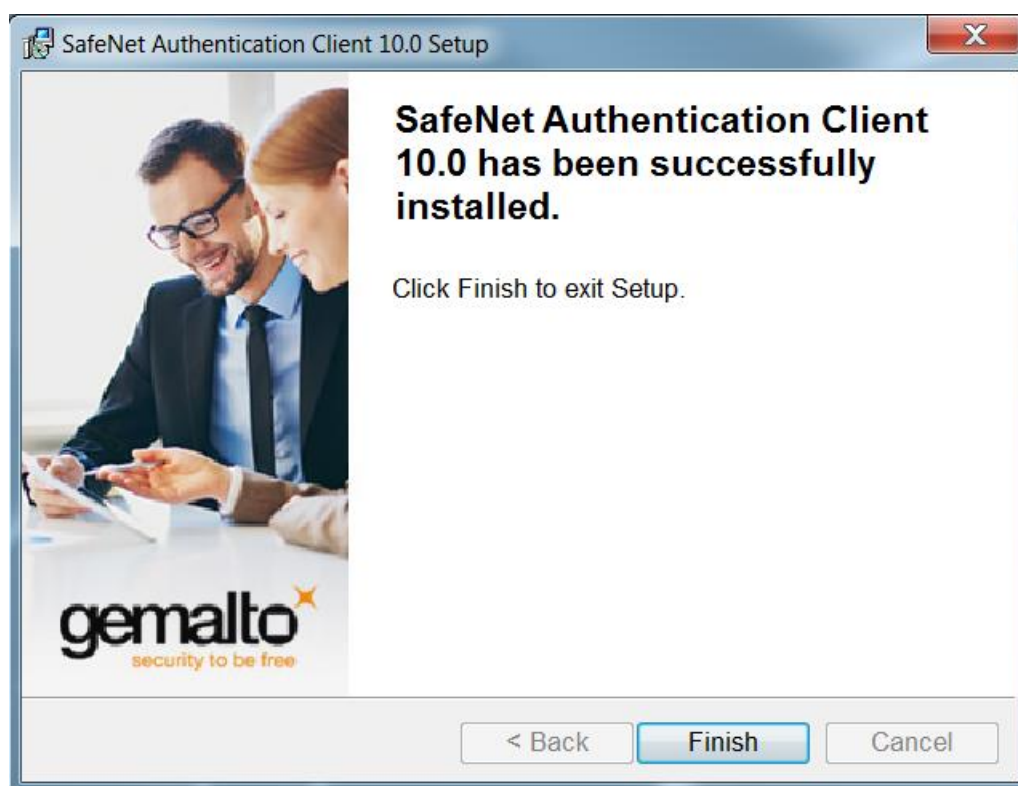
V případě potřeby je nainstalovat SW do vámi zvoleného adresáře.



Zvolte standardní instalaci (Typical).



Pokračujte stisknutím tlačítka „Instalovat“. Vlastní instalace může, v některých případech, trvat i několik minut.



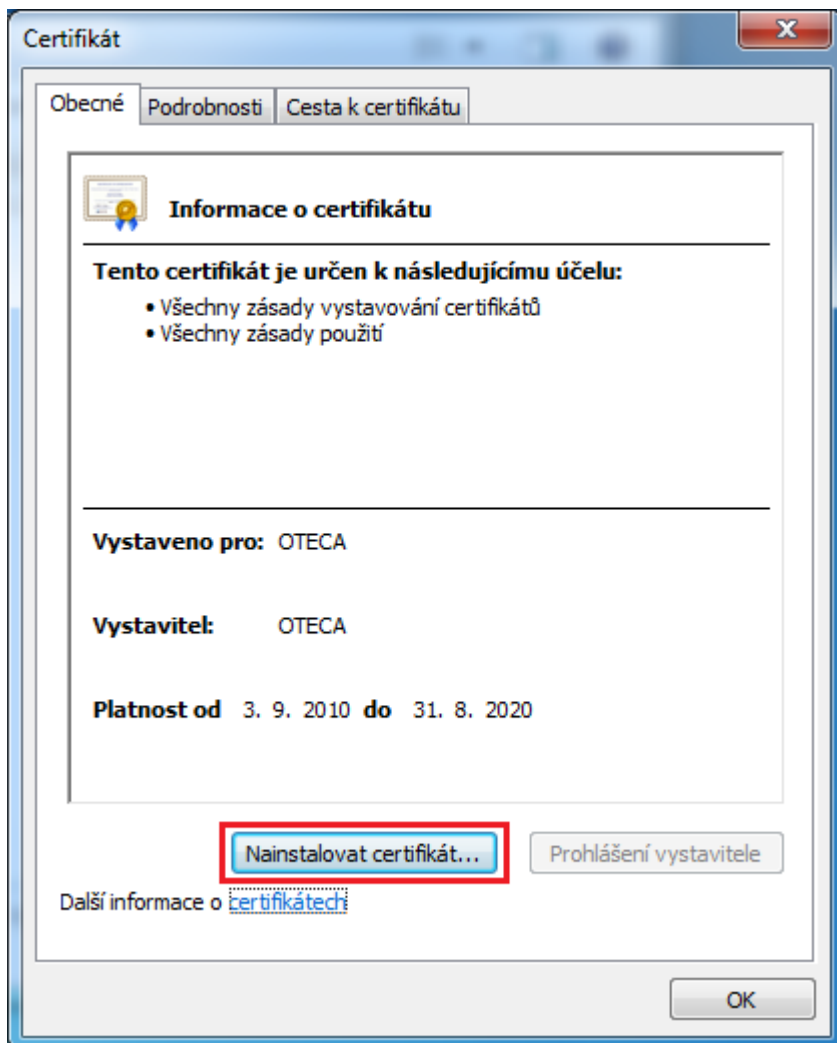
Po úspěšném provedení instalace se objeví následující okno.

2.2 Nastavení prohlížeče Internet Explorer

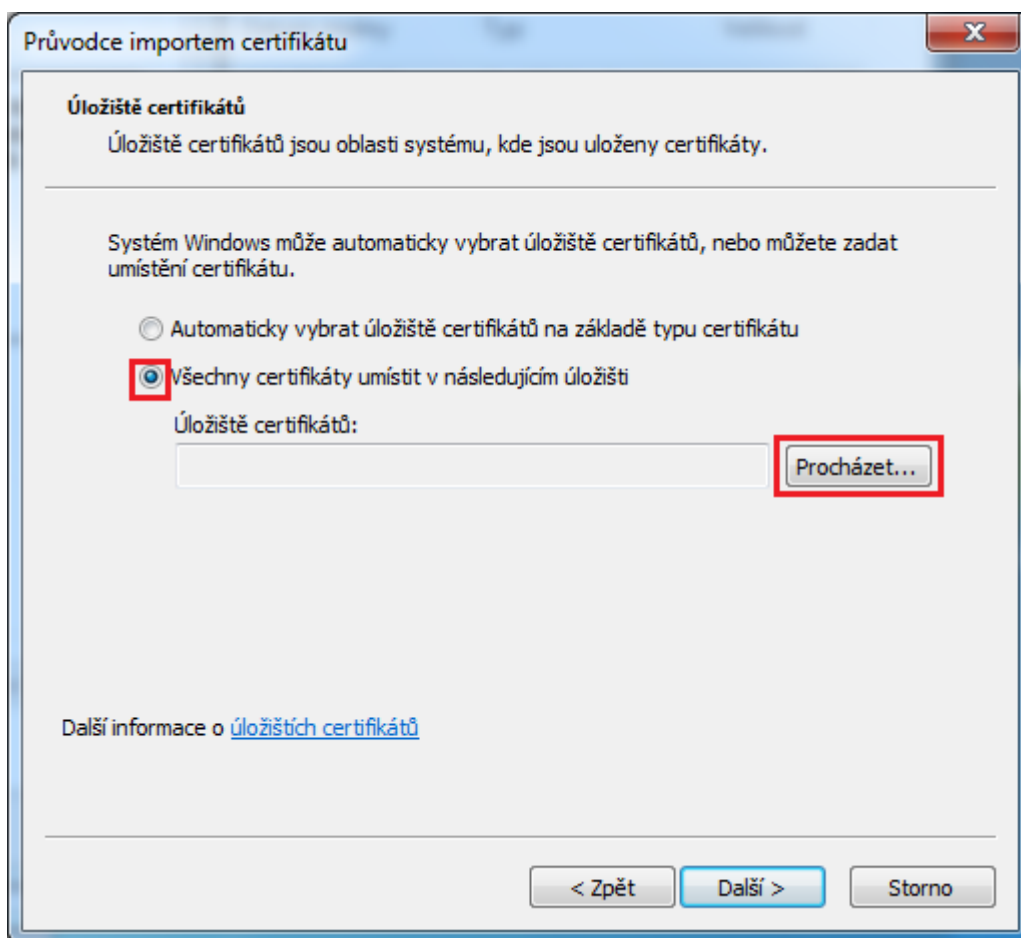
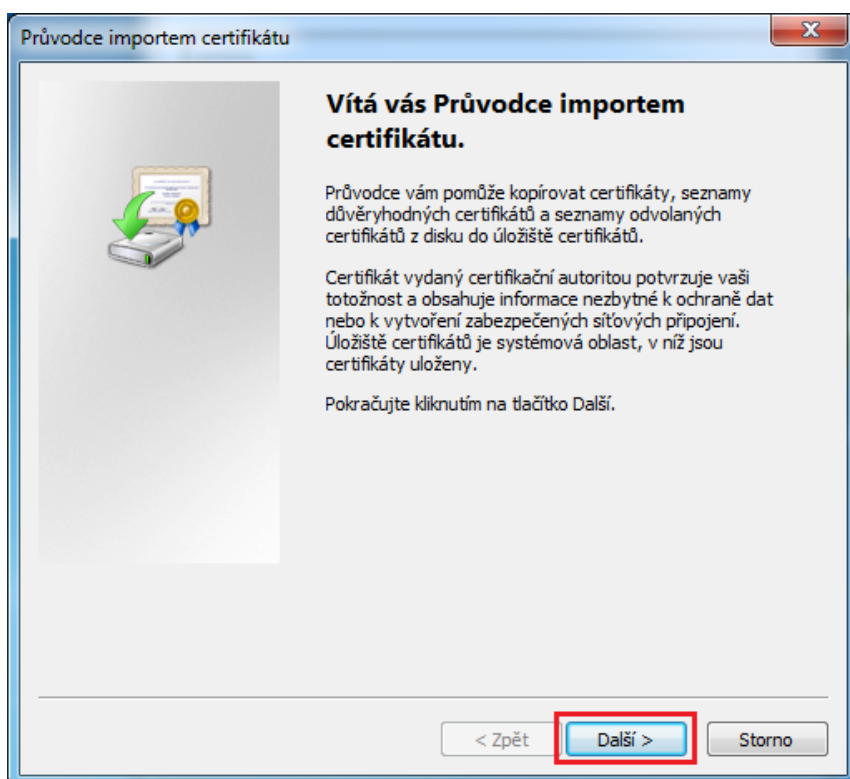
2.2.1 Instalace kořenové autority OTECA

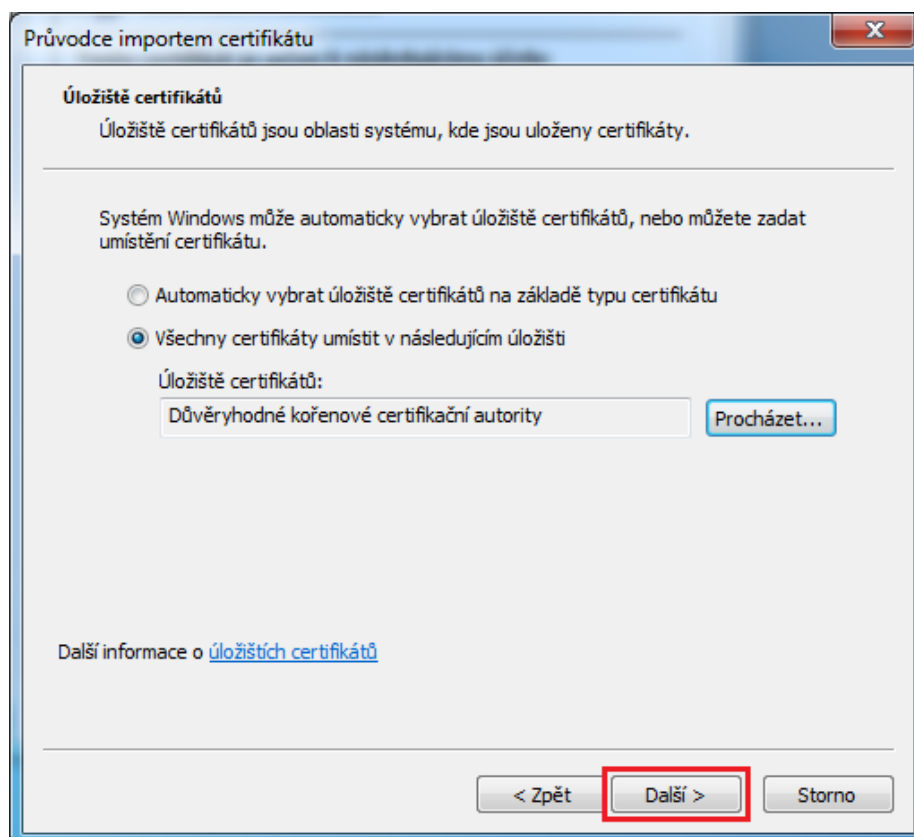
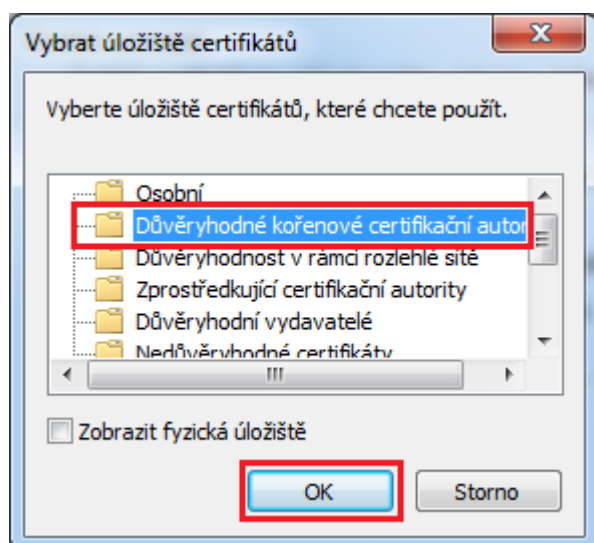
Pro přístup na stránky <https://portal.ote-cr.cz/otemarket> je nutné nainstalovat kořenový certifikát autority OTECA (pro přístup na testovací prostředí SAND je nutné nainstalovat kořenový certifikát OTECATEST). Tento certifikát je k dispozici ke stažení na veřejném webu OTE, resp. na přiloženém odkaze: <http://www.ote-cr.cz/registrace-a-smlouvy/pristup-do-cs-ote/konfigurace-pc>

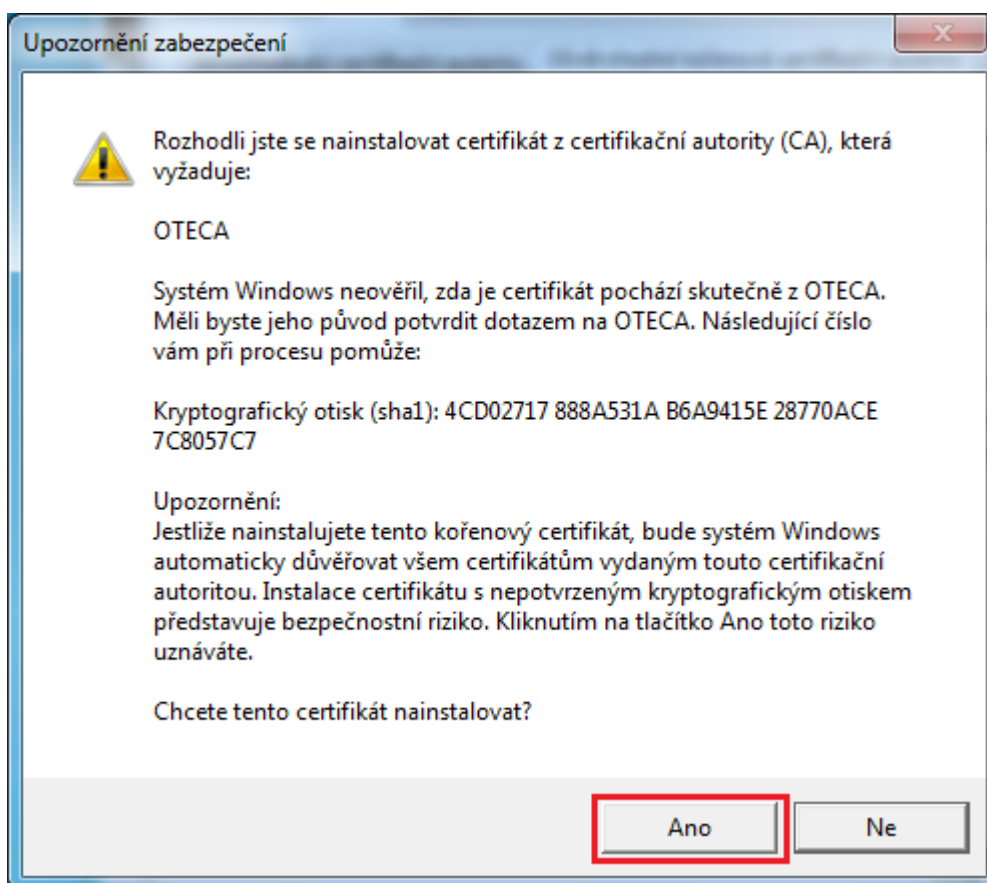
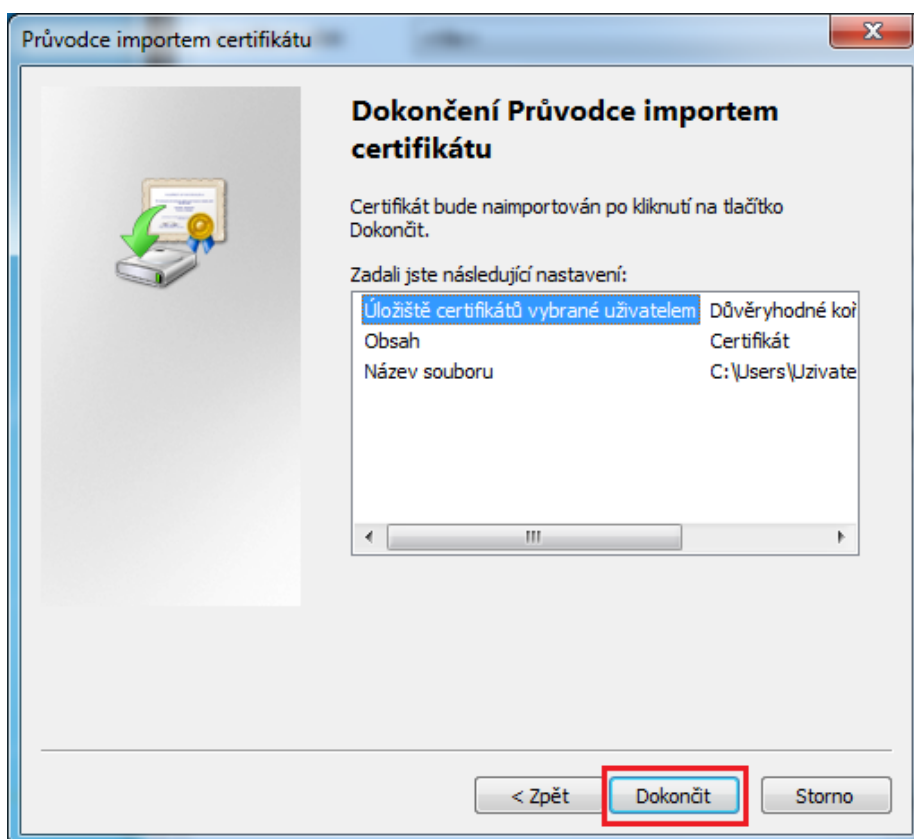
Dvojklikem na soubor OTECA.cer postupuje následovně:

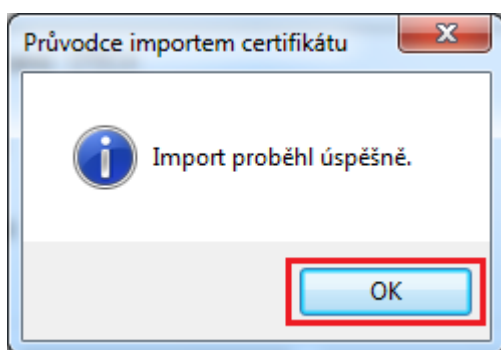


V okně s informacemi certifikátu OTECA je možné tento certifikát instalovat přímo stisknutím „Nainstalovat certifikát“.

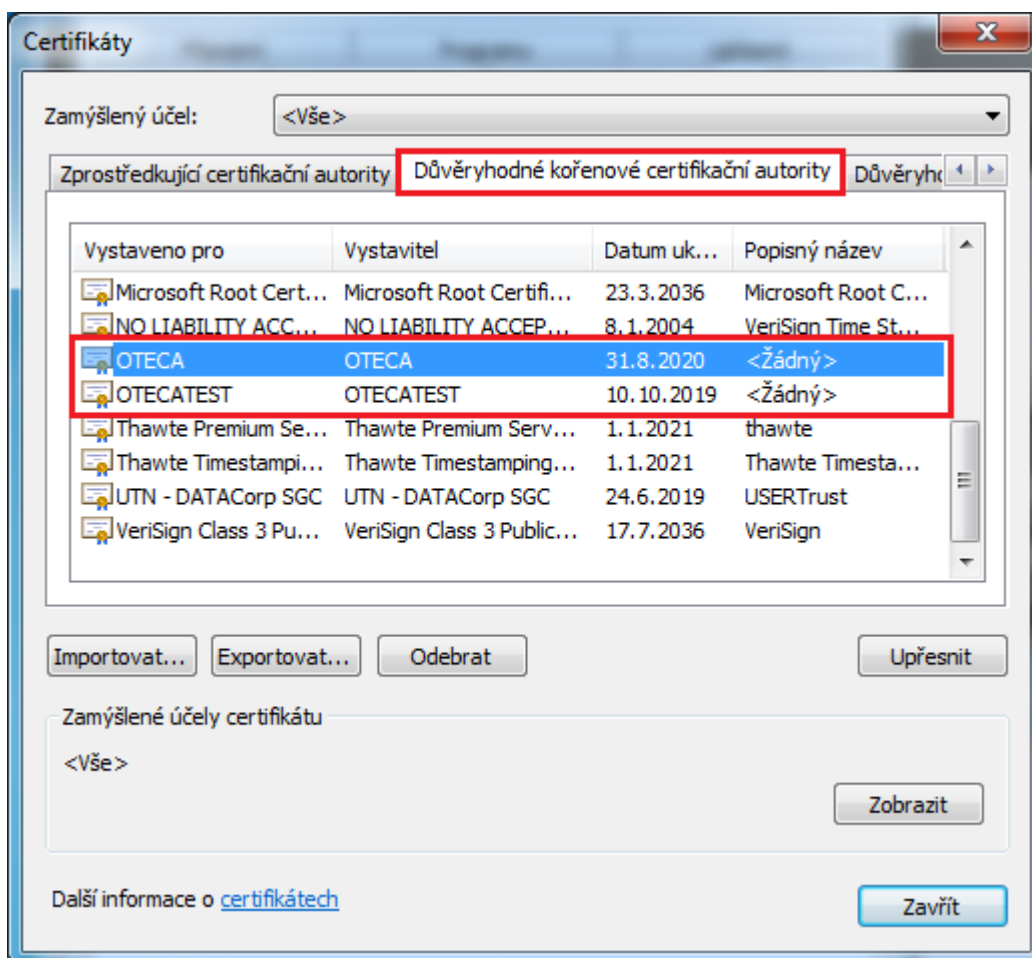






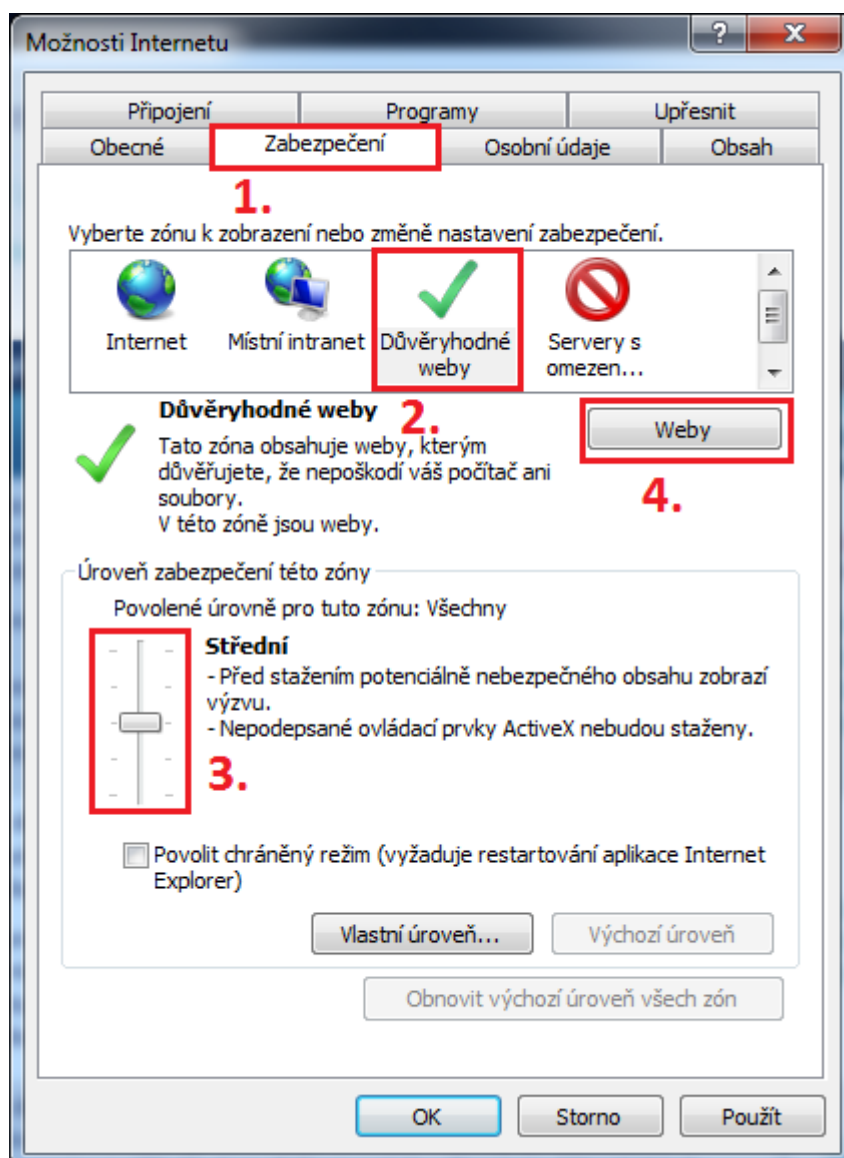


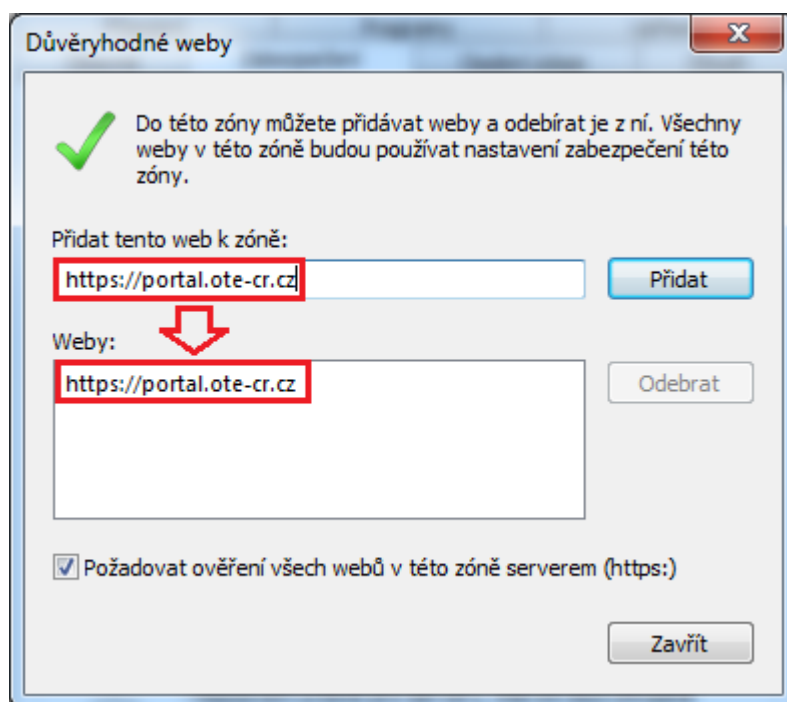
Po úspěšném naimportování kořenového certifikátu je certifikát vidět v seznamu „Důvěryhodných kořenových certifikačních autorit“.



2.2.2 Nastavení důvěryhodných stránek

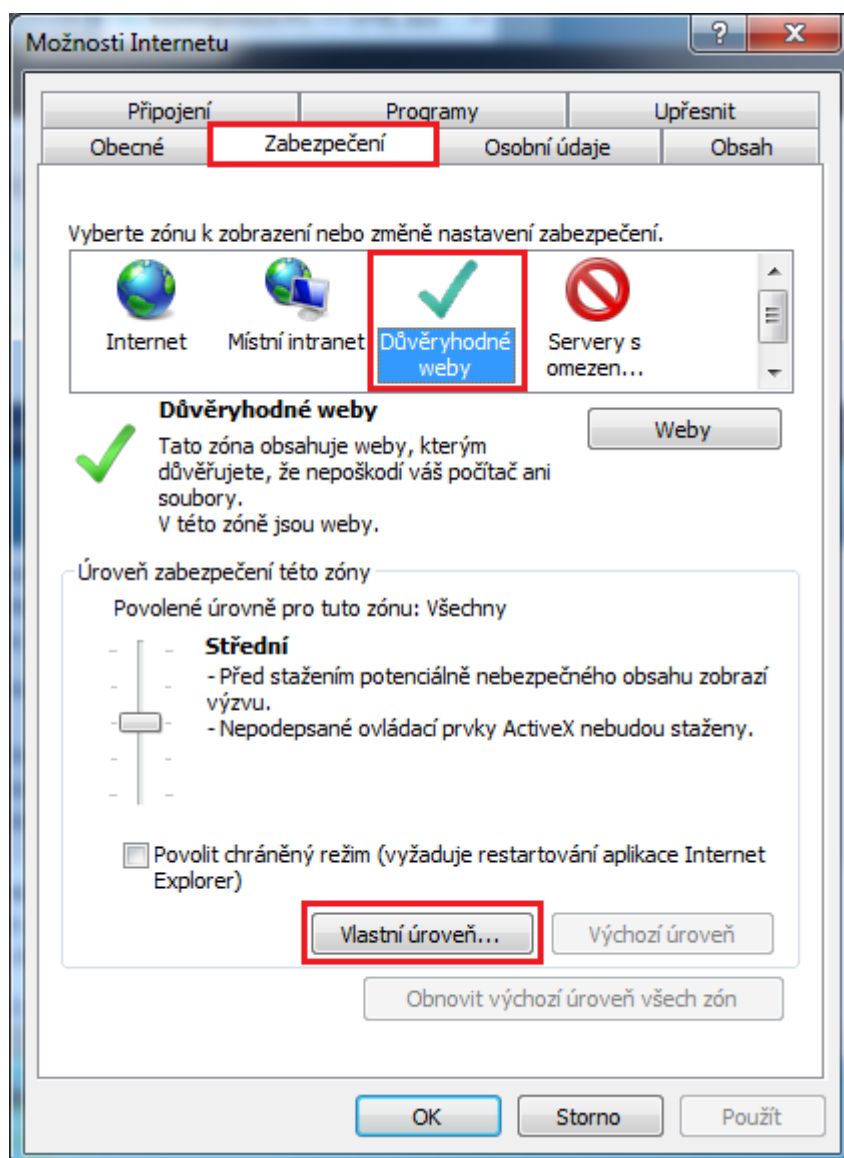
Všechna nastavení Internet Exploreru jsou ve standardním stavu, pouze pro některé funkce může být vyžadováno zařazení **https://portal.ote-cr.cz/otemarket** do „Trusted sites“, v menu Tools, Options jak je zobrazeno níže včetně kontroly úrovně zabezpečení.

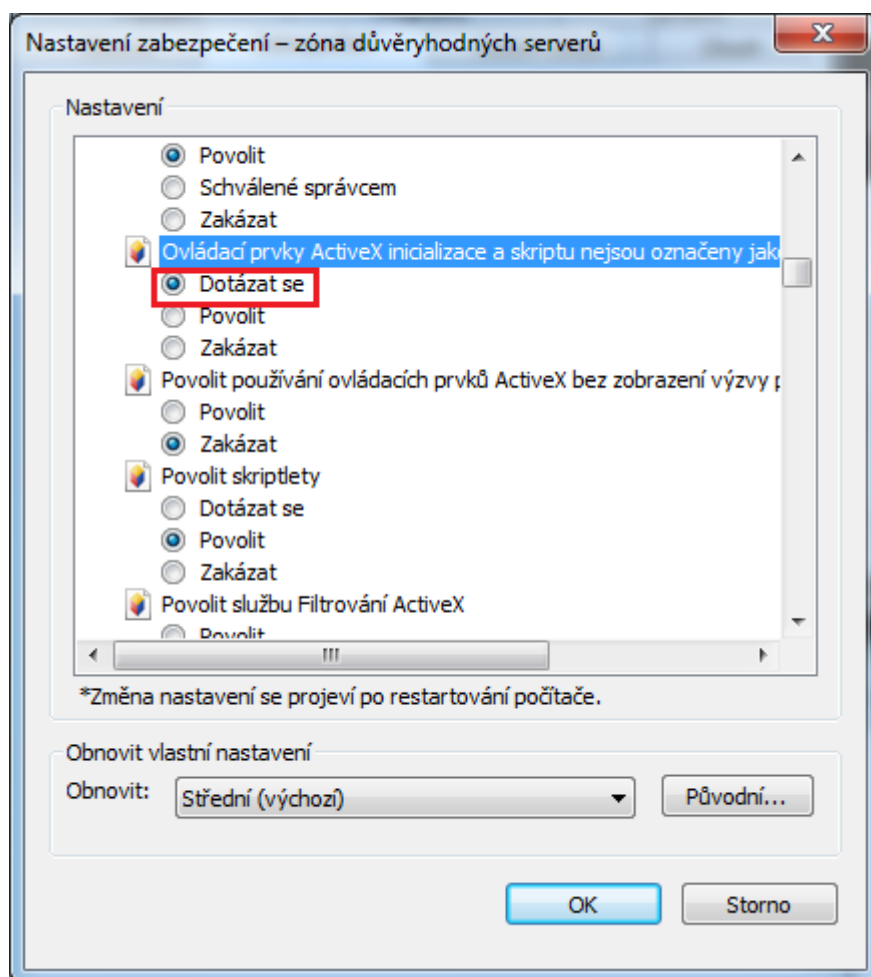




2.2.3 Kontrola povolení ActiveX komponent

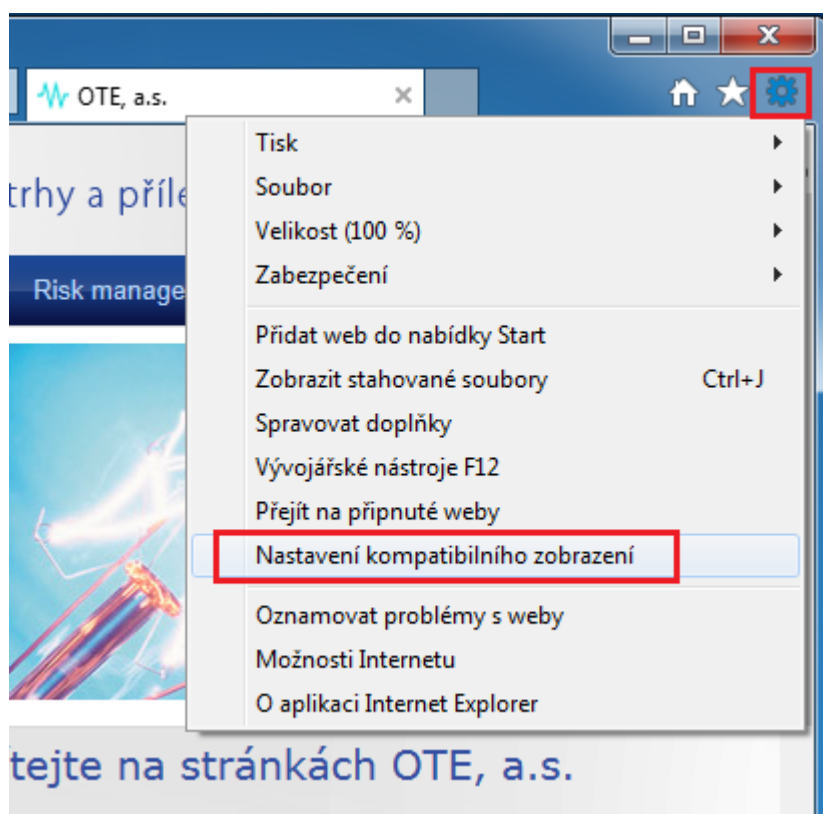
Pro korektní fungování v některých částech CS OTE je nutné zkontrolovat, popř. povolit stahování ActiveX komponent na klientskou stanici, dle postupu níže:



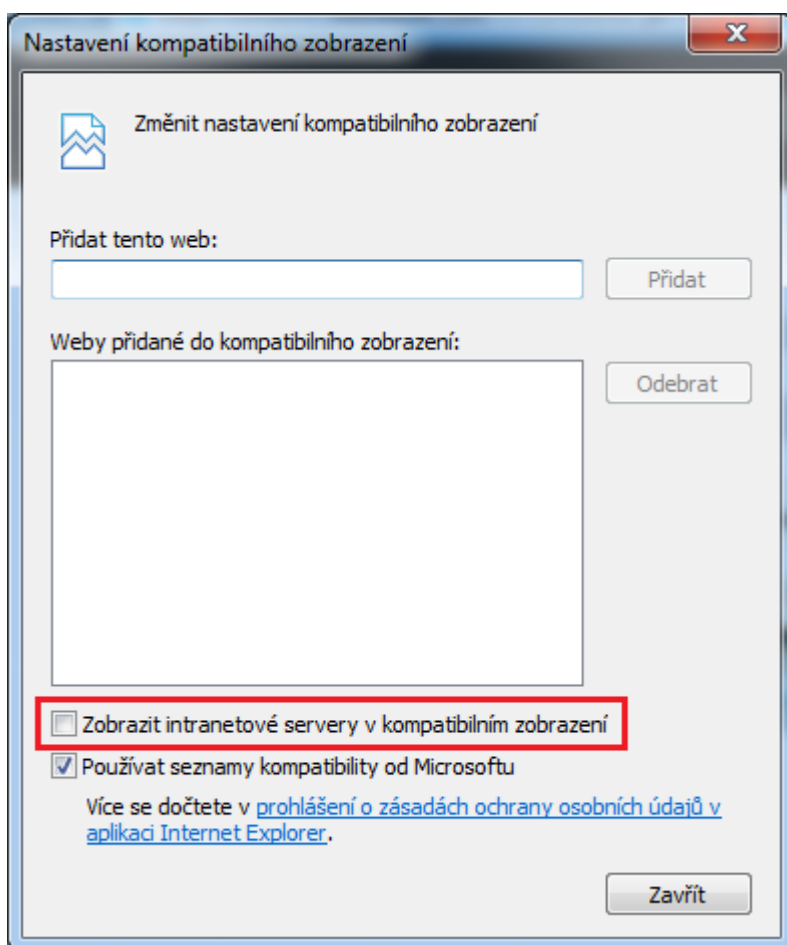


2.2.4 Nastavení kompatibility IE prohlížeče

Pro „korektní chování IEv11 je nutné odebrat implicitní nastavení kompatibility tohoto prohlížeče s předešlými verzemi prohlížeče. Je nutné zvolit v menu prohlížeče Tools/Nástroje – Internet options/Nastavení prohlížeče.



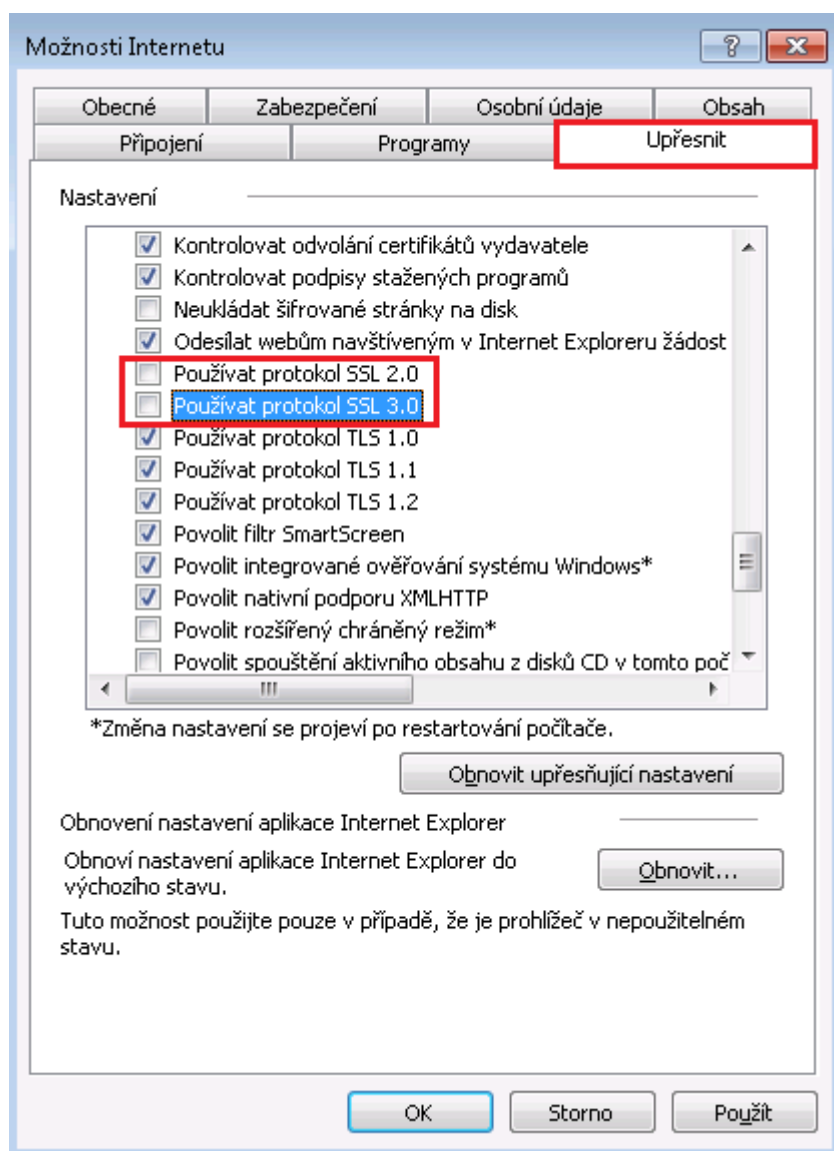
Z níže uvedené obrazovky odebrat implicitně nastavení „Zobrazit intranetové servery v kompatibilním zobrazení“, jak níže zobrazuje dialog.



A pak okno zavřít.

2.2.5 Kontrola nastavení zabezpečené komunikace

Bude nutné zkontrolovat, že v prohlížeči není vybrané již nepodporované nastavení SSL, tedy menu Možnosti Internetu – záložka Upřesnit, viz. screencopy níže.

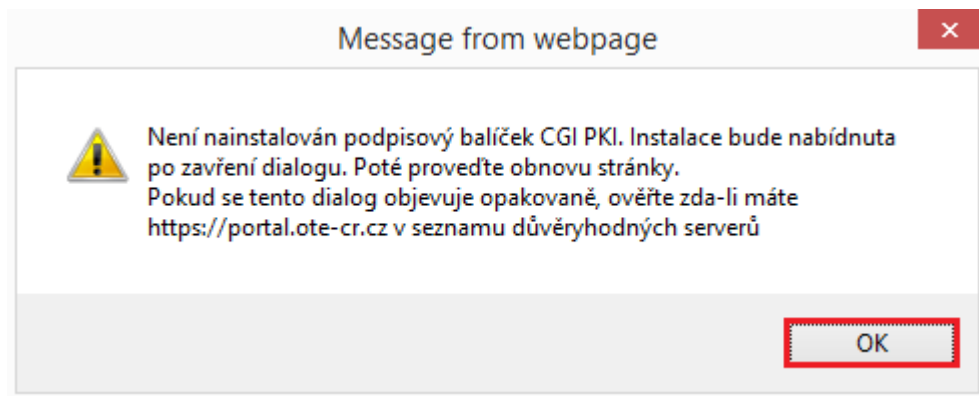


Ponechat jen TLS komunikaci a SSL odebrat a stisknout tlačítko OK.

2.2.6 Instalace podpisového balíčku CGI PKI pro Internet Explorer

Pro elektronický podpis v IE je nutné mít na klientské stanici nainstalovaný podpisový balíček OtePortalPki, jež je společný pro 32 i 64bit verzi OS. Postup jeho instalace je popsán níže. Předpokladem je však přihlášení se na stránky <https://portal.ote-cr.cz/otemarket> s právy lokálního administrátora. Důvodem je instalace knihoven do úložiště, kam nemusí mít běžný uživatel přístup. **Bez administrátorských práv by instalace balíčku CGI PKI neproběhla úspěšně!**

Po přihlášení na stránky <https://portal.ote-cr.cz/otemarket> a požadavku o elektronický podpis se objeví dialog o nutném stažení podpisového balíčku ActiveX.

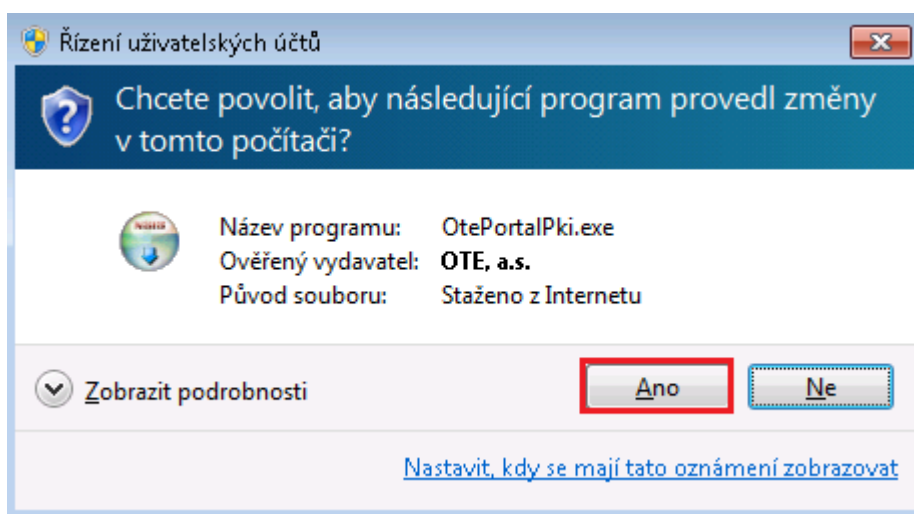


Stiskněte tlačítko „OK“.

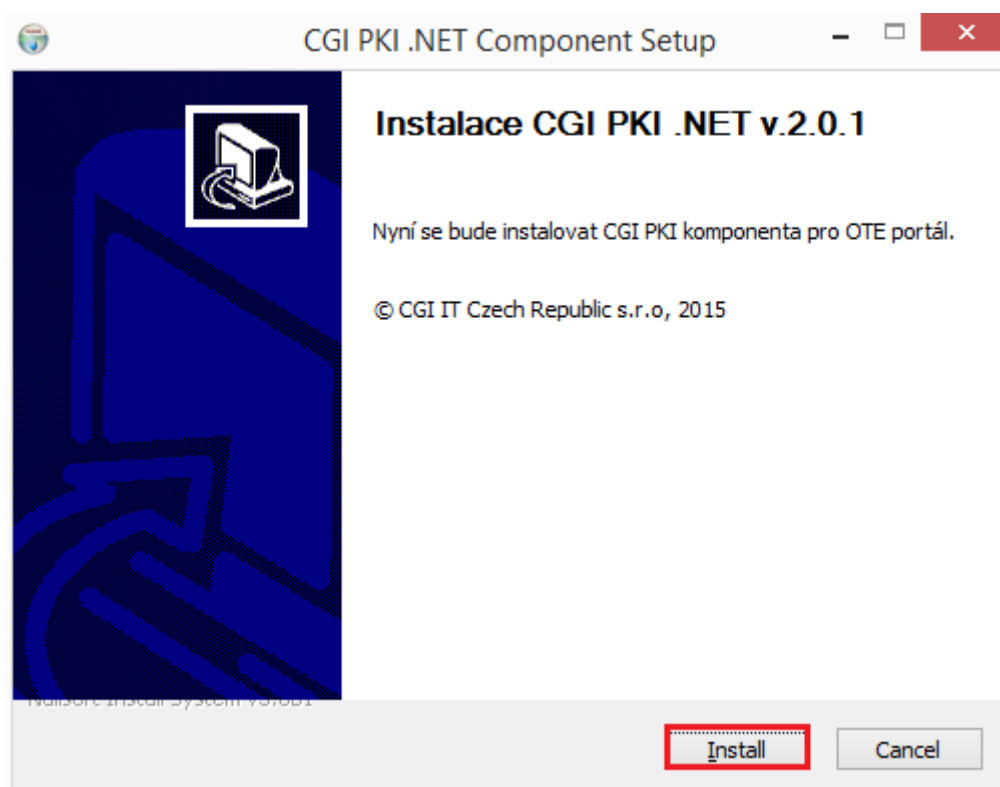
V následujícím dialogu potvrďte volbu „Spustit“.



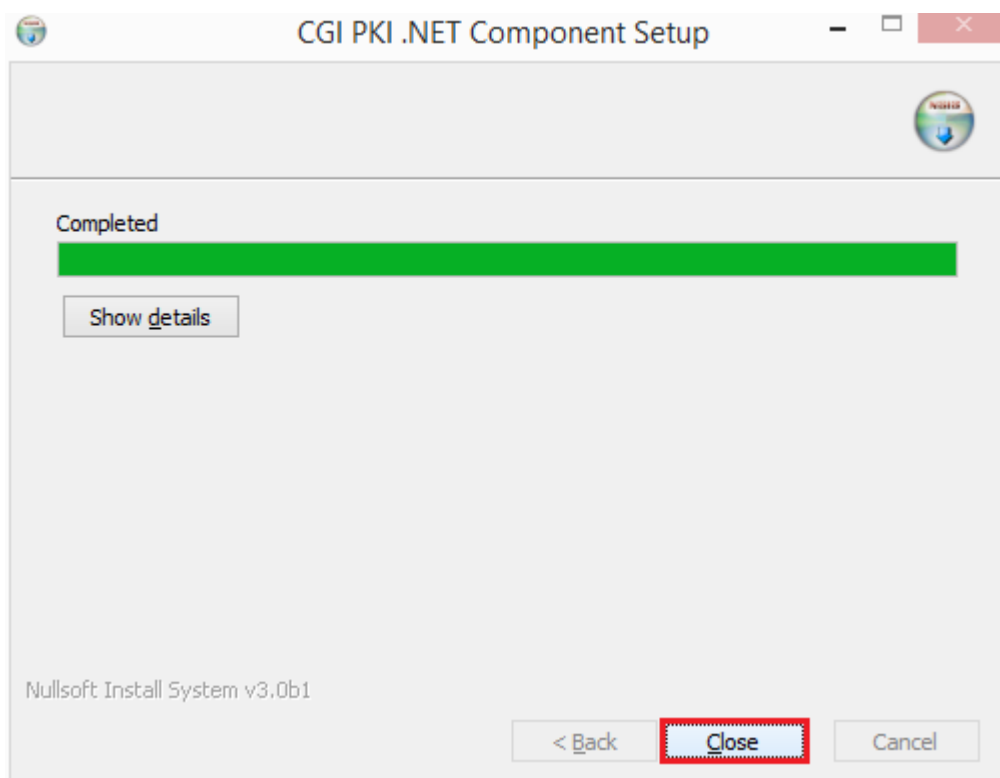
Stiskněte tlačítko „Ano“



Stiskněte tlačítko „Install/Instalovat“.

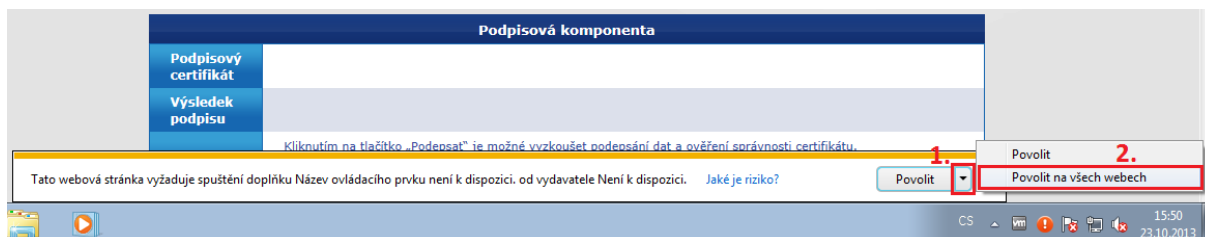


Stiskněte tlačítko „Close/Zavřít“.



Po tomto kroku by měl být podpisový balíček nainstalovaný na stanici a měl by jít používat elektronický podpis.

V případě, že vyskočí dialogové okno s žádostí o povolení doplňku, zvolte „Povolit na všech webech“.



2.2.7 Ruční instalace podpisového balíčku CGI PKI pro Internet Explorer

V případě, že se z nějakých technických důvodů nepodaří nainstalovat instalační podpisové balíčky přímo z portálu CS OTE, je nutné provést instalaci ručně dle níže uvedeného postupu:

- stáhnout instalační balíček z odkazu
<https://www.ote-cr.cz/registrace-a-smlouvy/pristup-do-cs-ote/files-konfigurace-pc/OtePortalPki.exe>
- zavřít všechna okna prohlížeče
- dvojklikem spustit či pravým tlačítkem myši zvolit instalovat
- postupovat podle instalačního průvodce
- spustit a ověřit elektronický podpis znovu

2.3 Nastavení prohlížeče FireFox

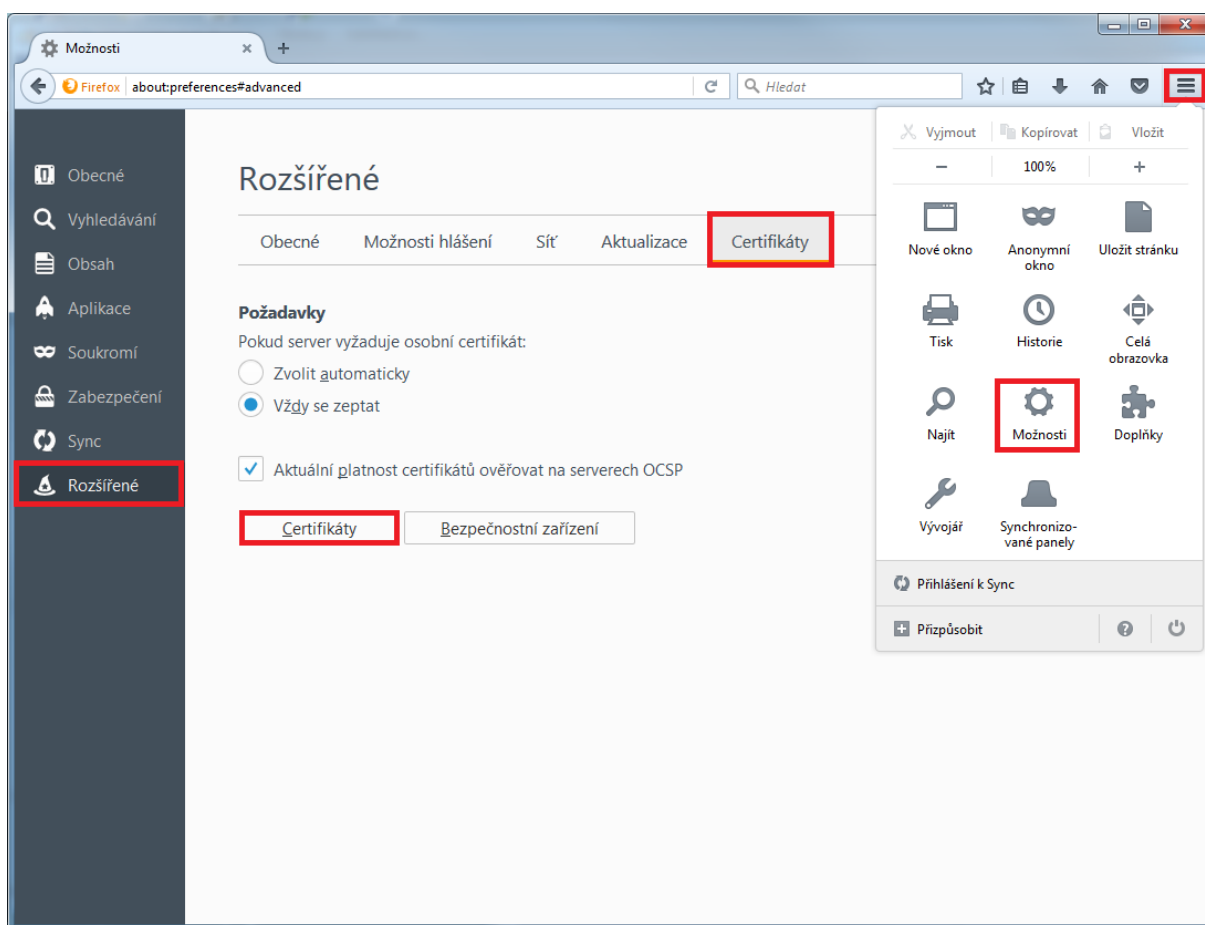
Nastavení přístupových prvků v prohlížeči FireFox je složeno z několika dílčích kroků.

2.3.1 Import certifikační autority

Pouze pro přístup na testovací prostředí SAND je nutné nainstalovat kořenový certifikát OTECATEST. Tento certifikát je k dispozici ke stažení na veřejném webu OTE, resp. na přiloženém odkaze: <http://www.ote-cr.cz/registrace-a-smlouvy/pristup-do-cs-ote/konfigurace-pc>.

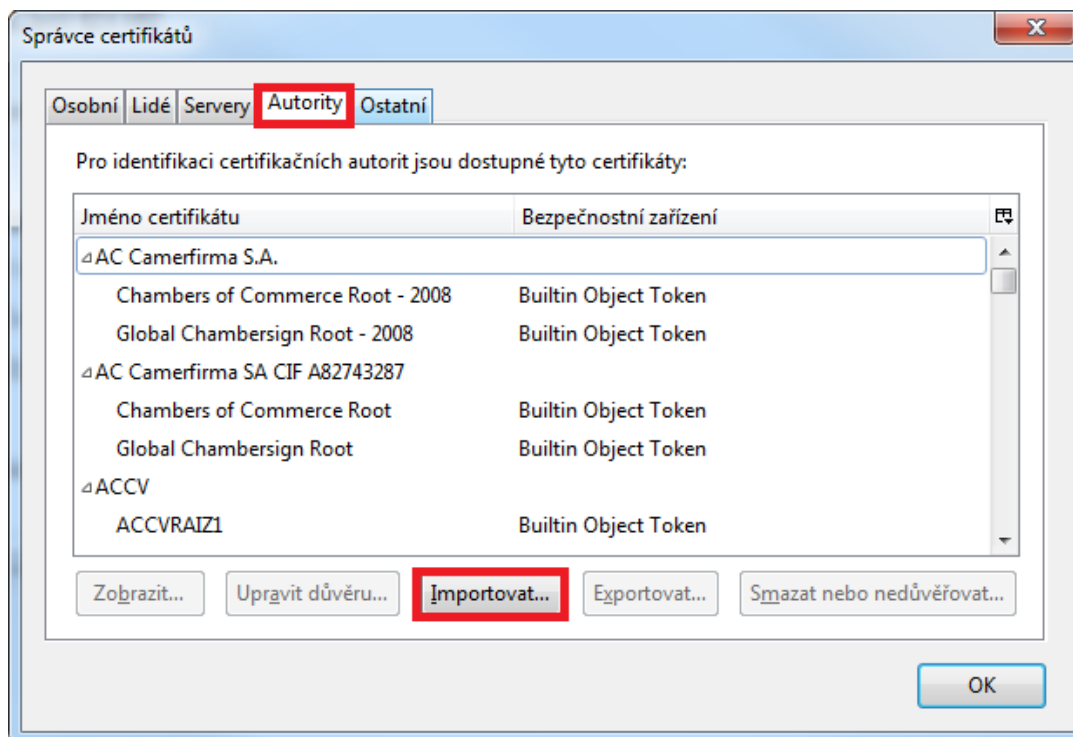
V menu klikněte na ikonu  zvolte Možnosti, sekce Rozšířené, podsekce Certifikáty.

Vyberte tlačítko „Certifikáty“.

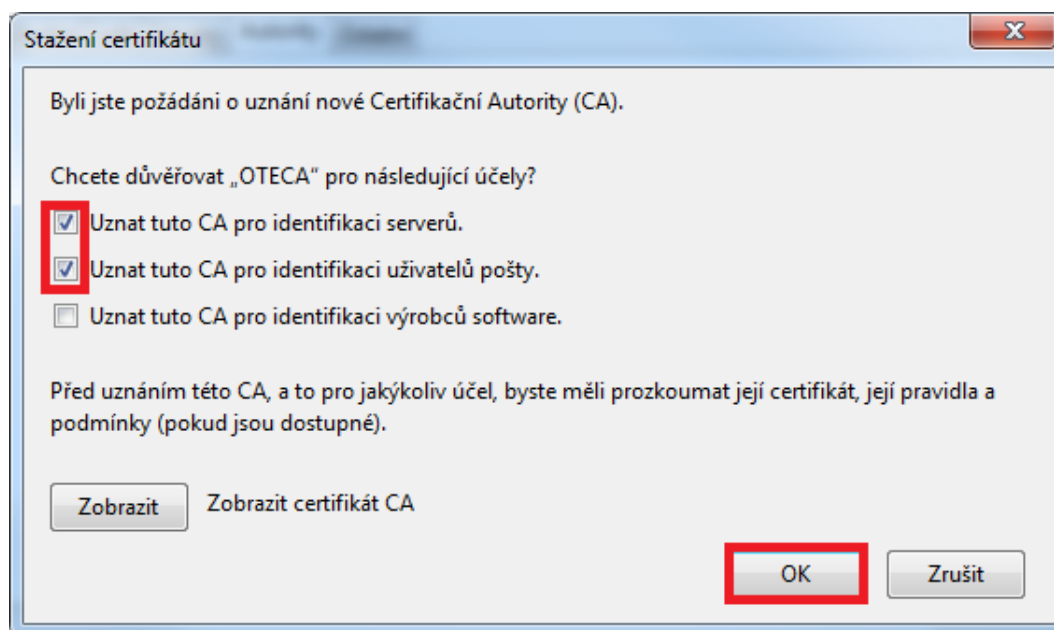


Zvolte záložku Autority a klikněte na tlačítko Importovat.

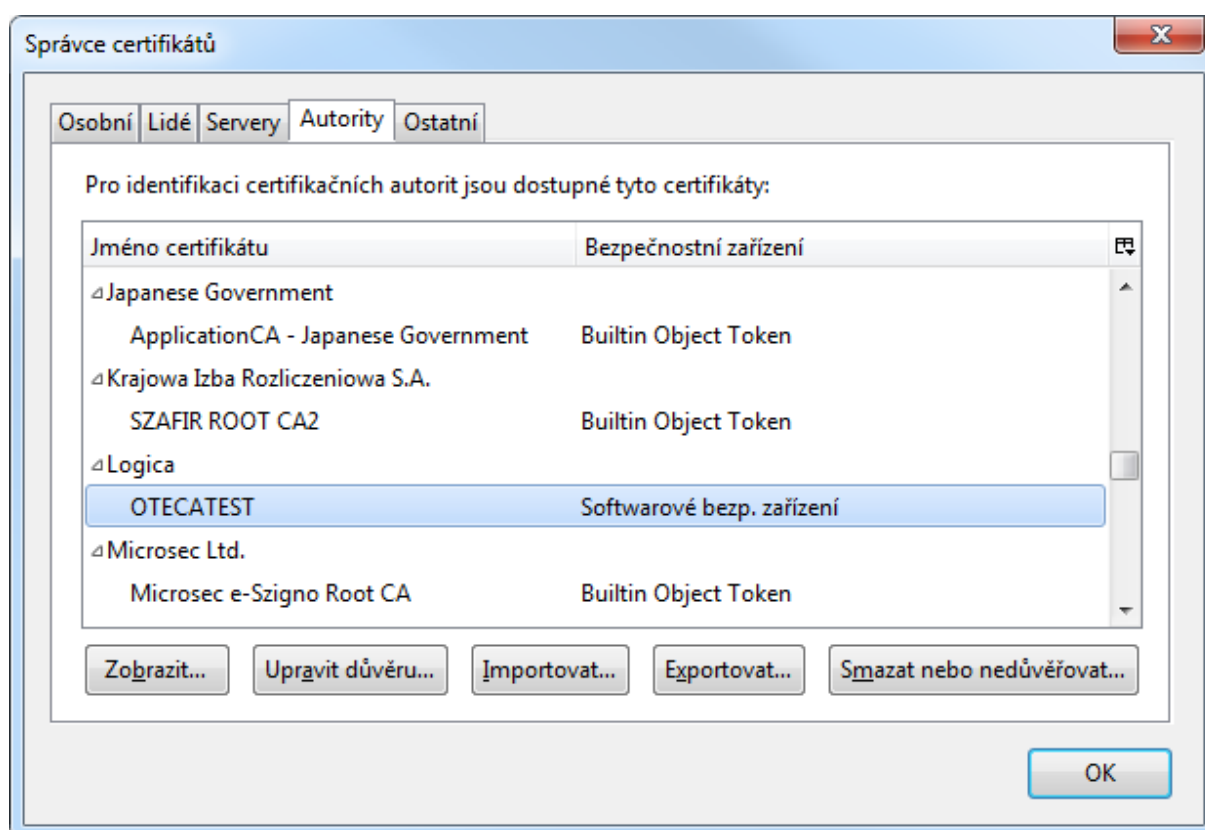
Prostřednictvím tlačítka „Importovat“ se dohledá ve filesystém soubor kořenové certifikační autority ve formátu *.pem, *.cer či *.der.



Zaškrtněte pole Uznat tuto CA pro identifikaci serverů a Uznat tuto CA pro identifikaci uživatelů pošty. Klikněte na tlačítko OK.



Po úspěšném naimportování se osobní certifikát z úložiště prohlížeče spáruje s certifikační autoritou OTECATEST a to následovně:



2.4 Nastavení prohlížeče Google Chrome/Microsoft Edge

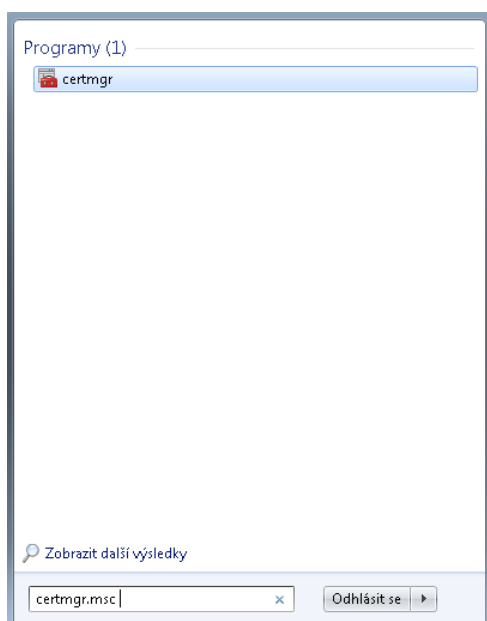
2.4.1 Import certifikační autority

Pouze pro přístup na testovací prostředí SAND je nutné nainstalovat kořenový certifikát OTECATEST. Tento certifikát je k dispozici ke stažení na veřejném webu OTE, resp. na přiloženém odkaze: <http://www.ote-cr.cz/registrace-a-smlouvy/pristup-do-cs-ote/konfigurace-pc>.

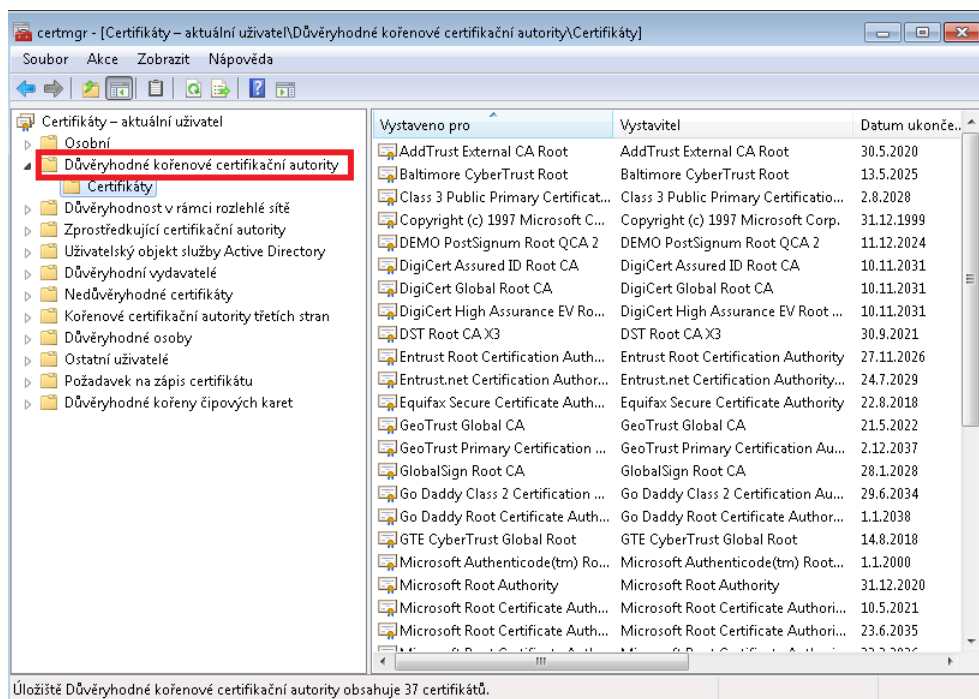
Klikněte na tlačítko Start.



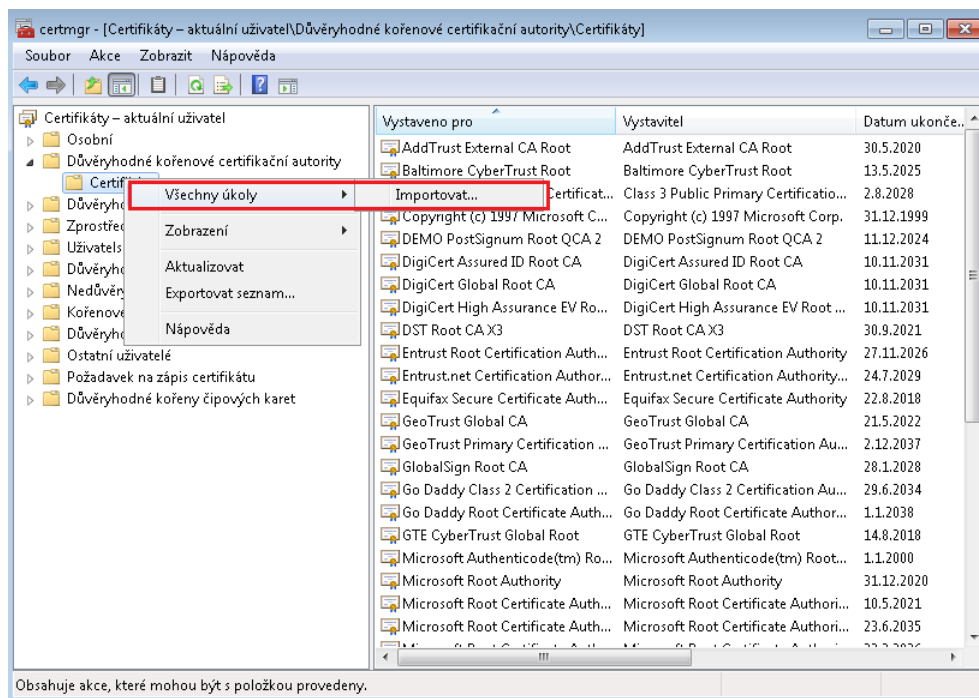
Do konzole zadejte příkaz certmgr.msc. Klikněte na ikonu programu certmgr.msc a poté zadejte Vaše přihlašovací údaje a heslo. Po zadání údajů se Vám zobrazí okno se správou certifikátů.



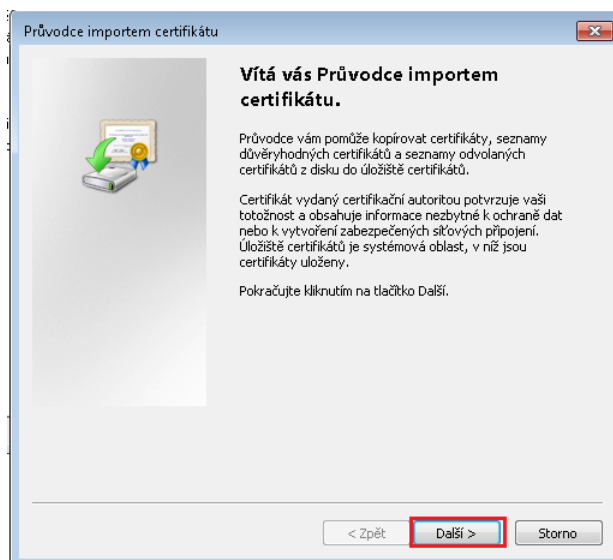
Klikněte na záložku Důvěryhodné kořenové certifikační autority, podzáložku Certifikáty.



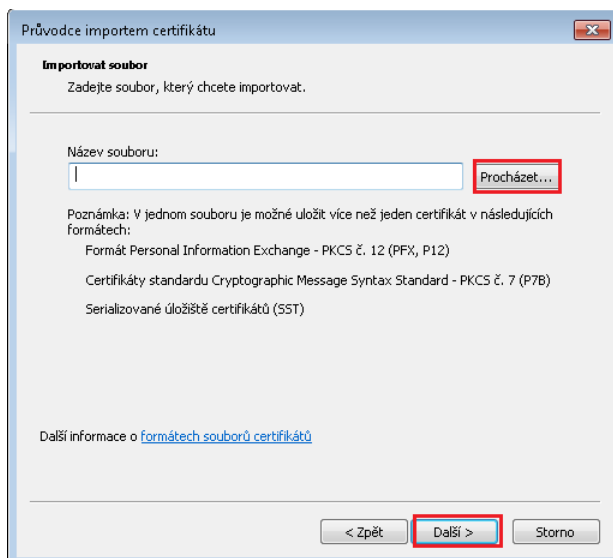
Klikněte pravým tlačítkem na myši na podzáložku Certifikáty, pokračujte klikem na Všechny úkoly, dále potom na Importovat.



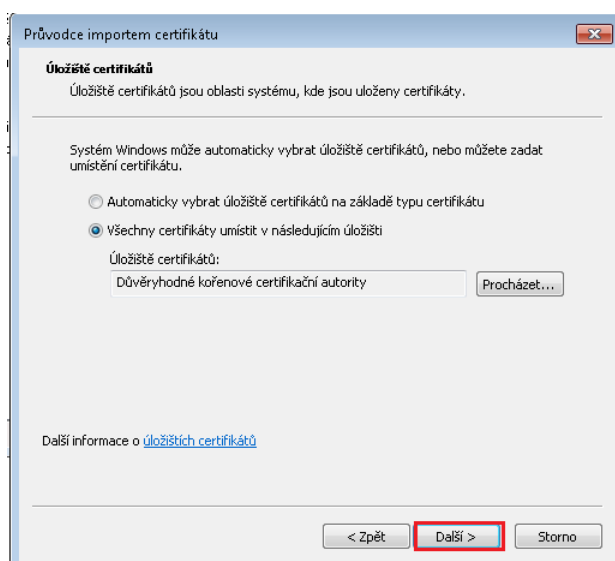
Klikněte na tlačítko Další.



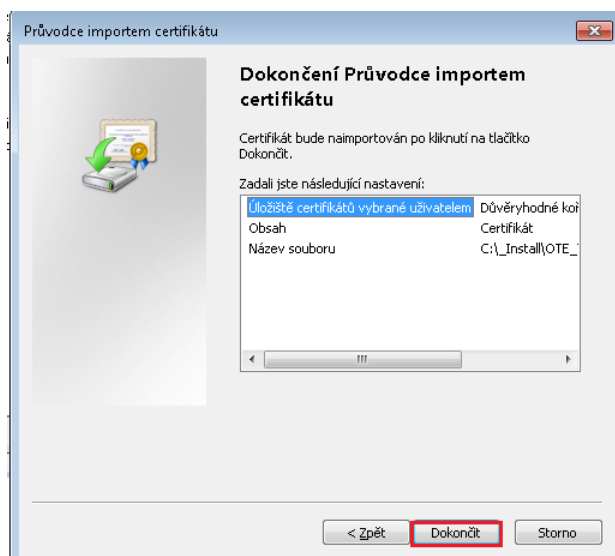
Prostřednictvím tlačítka „Procházet“ vyberte soubor kořenové certifikační autority OTECATEST.



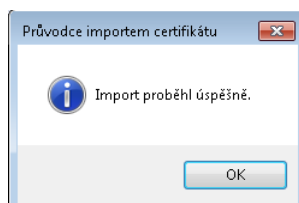
Zanechte nastavení ve výchozím stavu, tj. zaškrtnou možnost Všechny certifikáty umístit v následujícím úložišti.



Klikněte na tlačítko Dokončit.



Klikněte na OK.



Pokud proběhl import úspěšně, certifikát OTECATEST se zobrazí v seznamu certifikátů.

