Uživatelská příručka informačního systému

Konfigurace klientských statnic

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	Aktializace 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
8.3.2018	Odstranění neaktuálních informací o certifikátech OTECA, OTECATEST
15.3.2018	Informace o komponentě OTE PKI Klient pro přístup do CS OTE
5.4.2018	Doplnění informací o Registraci certifikátu po expiraci
22.5.2018	Instalace nové podpisové komponenty PKI + nastavení v různých prohlížečích
20.9.2018	Aktualizace přístupu přes aplikaci OTE-COM
27.11.2018	Aktualizace nastavení Mozilla Firefox pro využívání PKI komponenty

Obsah

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)+ Outlook 2016 /x86

Windows 7 (64bit) + MS IE11.0(32bit)/FireFox(32bit) + Outlook 2016/ x64

Windows 10 (32bit) + MS IE11.0/Edge/FireFox/Chrome-poslední verze + Outlook 2016/ x86

Windows 10 (64bit) + MS IE11.0/Edge/FireFox/Chrome-poslední verze + Outlook 2016/ x64

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

http://windowsupdate.microsoft.com.

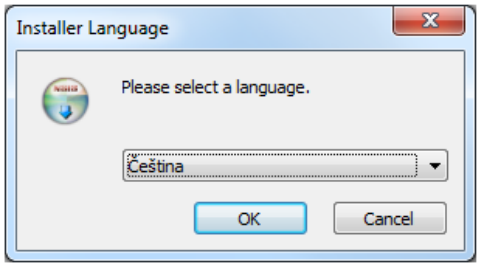
2 Prohlížeče Google Chrome, Mozilla Firefox a Microsoft Edge

2.1 Instalace komponenty OTE PKI klient pro přístup do CS OTE

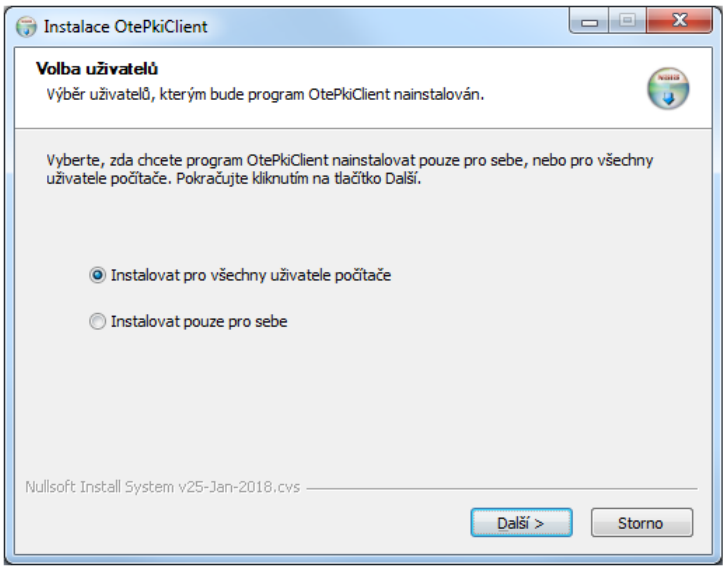
Odkaz na instalační soubor komponenty se nachází na stránce http://www.ote-cr.cz/registrace-a-smlouvy/pristup-do-cs-ote/konfigurace-pc - v *tabulce* ***A- Přístup do CS OTE prostřednictvím webového prohlížeče*** (instalace pro Internet Explorer a pro podporované prohlížeče pro 32-bit a 64-bit OS).

K zahájení instalace spustíme stažený soubor:

1) Instalátor vyzve k volbě jazyka

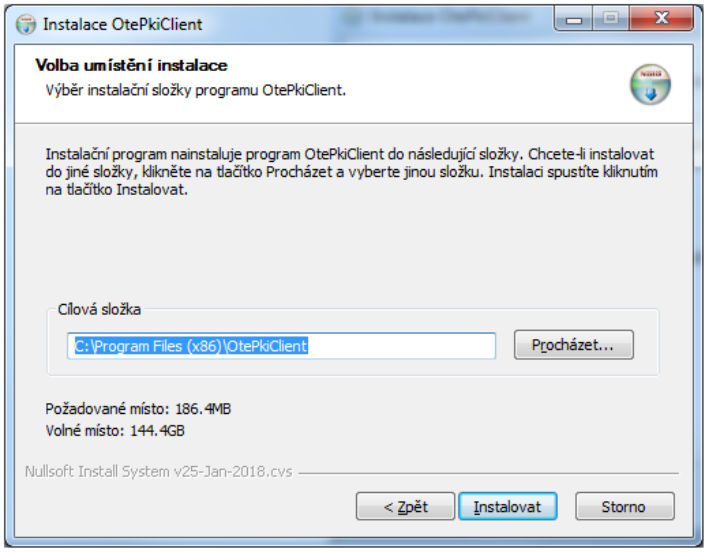


2) V dalším kroku, v závislosti na verzi prohlížeče, zvolíme zda-li nainstalována aplikace má být přístupná i ostatním uživatelům



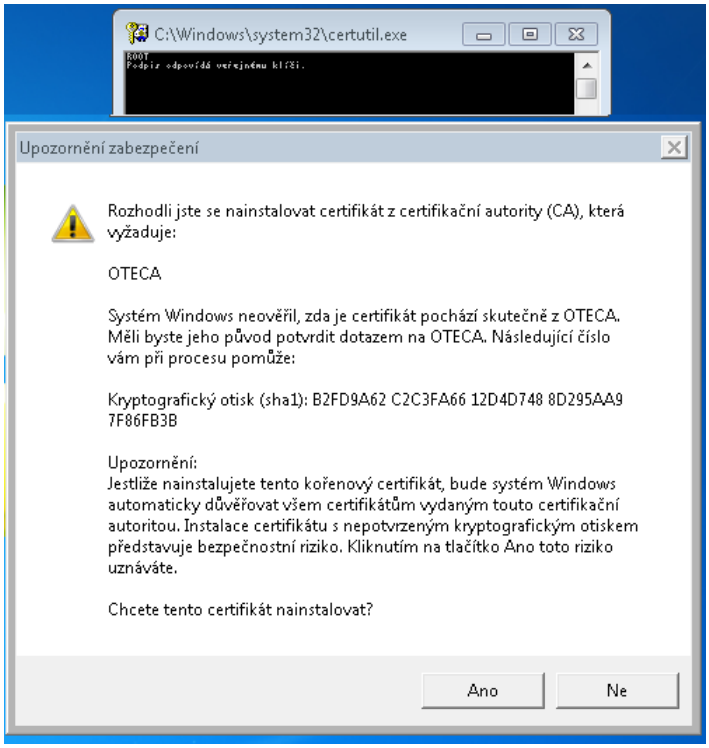
- při výběru pro všechny uživatele aplikace nabídne instalaci do Program Files
- v případě výběru pro daného uživatele aplikace nabídne instalaci do uživatelské složky

3) Následně je možné upravit umístění instalace



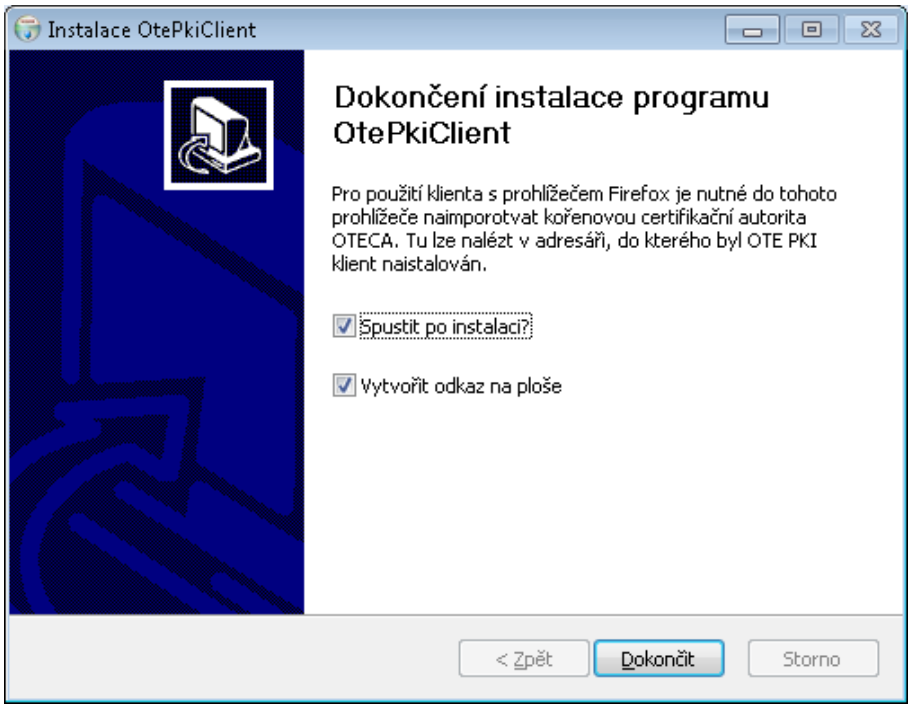
4) Je na PC nainstalovaná Certifikační Autorita OTECA nezbytná pro funkci OTE PKI klient ?

Jestliže tato autorita není v systému přítomna, objeví se následující dialog – žádost o instalaci OTECA Autority :



Odsouhlasením uvedeného pokračujeme v instalaci. Autorita je nyní dostupná pro všechny podporované prohlížeče kromě Mozilla Firefox. Import pro tento prohlížeč je popsán v kap. 2.2.1.

5) Na závěr vybereme, jestli má být ikona aplikace přítomná na ploše.



2.2 Poinstalační konfigurace

V případě používání jiného webového prohlížeče než Mozilla Firefox, pokračujte na kapitolu **2.5**.

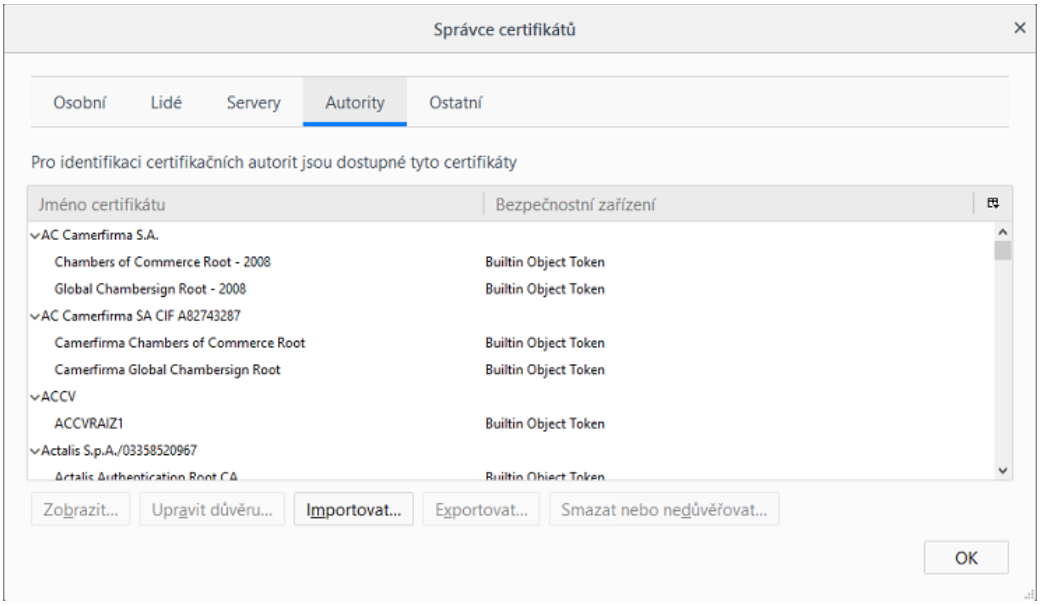
2.2.1 Import OTECA autority do prohlížeče Mozilla Firefox

V případě uživání OtePkiClient s tímto prohlížečem je nutné instalaci certifikační autority OTECA do prohlížeče provést ručně.

Níže uvedený text zkopírujeme do textového editoru a soubor uložíme s názvem OTECA.pem:

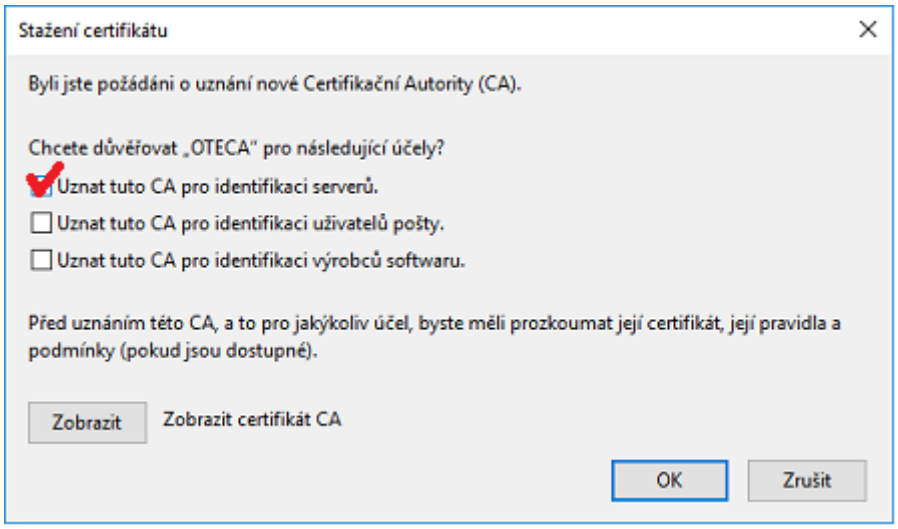
```
-----BEGIN CERTIFICATE-----
MIIFpDCCA4ygAwIBAgIKAq9tFwPoO3XI5TANBgkqhkiG9w0BAQsFADA/MQswCQYD
VQQGEwJDWjESMBAGA1UECgwJT1RFLCBhLnMuMQwwCgYDVQQLDANQS0kxDjAMBgNV
BAMMBU9URUNBMB4XDTE4MDMwNTE3NDgwM1oXDTI4MDMwNTE3NDgwM1owPzELMAkG
A1UEBhMCQ1oxEjAQBgNVBAoMCU9URSwgYS5zLjEMMAoGA1UECwwDUEtJMQ4wDAYD
VQQDDAVPVEVDQTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBANrqtnuv
5zS9byhArdH2sTE+dAGSYT85RT71+ElkoCwpYbOsGsR3/7LzbQT0R7dn8iSDPR5a
hh0B8mdcWLYXOV0croBFs0WpGUiOSiwpKLFr+aXMtVNBfX5qF+GZWRj+G+NfhYgr
zARTN2Ws0MnQGZbXY0GuIWOwYItj9EA15qTE3IN/ereSzwkSwx3Fd2AigxL7V6Yw
pxU+rWe39MFH8prTPw6TI0xvPconZwObaIoHG54P4wRqEeuKnzaW4vZeinGvIXpn
5MamU2tQrMUGCMOEeycASPMEubSK8z6IyJ35ZQ31aeUk3lwrzp0CJZVFsZtThn8T
9e1ZiPHxD3LbW5bGT7hSVqe7qe1qwdomYItQrRLJZ17YMBEA8vfgZHwjcjaO7QfX
ljYdUirnujTDgHqcu6RXVkhPvVbdFNcRe1o34+8TzmDXQOVOTSzjEOdGcB++Rvcp
+pxbbQUFM4ja3BH3Y9hV2GWSPtET/FhY028gG2KkFpXAz7HzpnLjm27dvSH4RU3S
AYKm+cd/btgDI2fGzaKtVt50+trB2Wjl+GipsRkw2VmOdBDO++T28NcrOu7HNVBF
xNzpvHchoVOonWLbghxzqVDux+BWEriOIJYSebBbQdn0Vic5xB0+kcGMHMfnJ6Dz
7sOhlZgH3h3rYg7G88JxGVGbxFGZHMTYyamhAgMBAAGjgaEwgZ4wDwYDVR0TAQH/
BAUwAwEB/zALBgNVHQ8EBAMCAQYwHQYDVR0OBBYEFOpk3trCPeD1gOlUhNgqi73M
7xMVMB8GA1UdIwQYMBaAFOpk3trCPeD1gOlUhNgqi73M7xMVMB4GA1UdEQQXMBWB
E290ZWNhLmN6QGxvZ2ljYS5jb20wHgYDVR0SBBcwFYETb3RlY2EuY3pAbG9naWNh
LmNvbTANBgkqhkiG9w0BAQsFAAOCAgEAXL8eTcjeG0Yb341YzErb+KGm6S2gWAqk
eBbrVtVJ6uq4lUYVuQ2radrN26ZMSedTyeCzmuq2bK3wLchBcQkeC/FY4gvDUVE5
nz3I0n4Ze6Ql4r6ZgcklDWEymO+OvHKaaLuheOkRTYx2+EVoTIWI/44zqZl5moQB
DKSdTENQNRSTxp1pRElTpCYxd28Ssv0S0fQpeX1vOP1fQZ363AUVr8FnKnMb3CHY
5ua45Chal3MzoiEIFz3AIo6o5AwMqs+vTTTzAM7Y5qEfurEOPWw08Pgv6IoxKIFv
5P7BEbwlOha8kJpncAnoLmhucZoPH774a4XHdVdT1678CWd0f+JCDGOFFVtaXkKV
aUBHuw5vojEiPXZ7VGysiApZ0EM1FJ5IuZYo3kjJ60q4Rj3I+436cdOk7PlSlBiQ
R0KrZmUPlChCwW42LVaIzh0//WlagXJ/2Il2bKI1qzTkixSYkOV3t+OewfLmBBM/
nmLoDdKfrmkWaEkURL8l911YhDgh2fwOn5cLwedq0XNzVGqnJW/knSjesfllt1Lv
79uUfXv6Yx3fXmG4Q6PVa++G4MXoccjEwndr83XrG7rTZlnF1qUrQGYjZduLiT8M
q7wCPGLXADYuDhV4ewN/SLlvfSR2oohcpbJ1f+a4eSXDbeq0jcN8YbT7+geY0tKc
iXTuTVuPZSI=
-----END CERTIFICATE-----
```

Samotnou instalaci autority provedeme v prohlížeči Mozilla Firefox:
Menu -> Možnosti -> Soukromí a zabezpečení -> Certifikáty - Zobrazit certifikáty
a vybereme záložku *Autority* – ***Importovat*** (v různých verzích prohlížeče se cesta může odlišovat)



Objeví se dialogové okno, kde vybereme uložený certifikát.

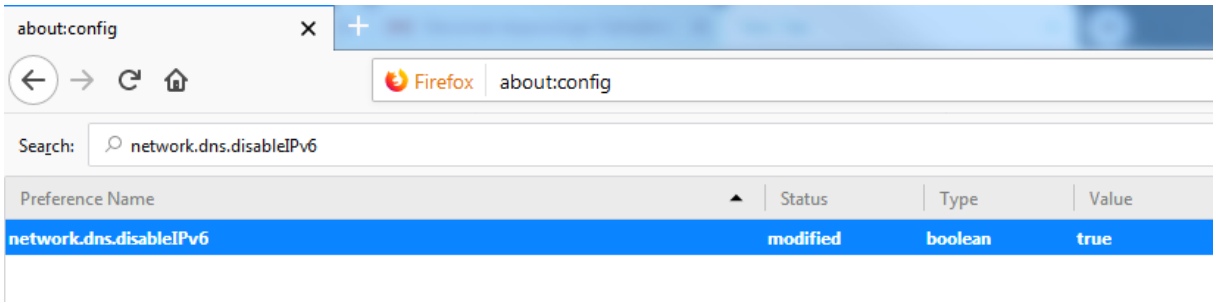
Dalším krokem je zobrazení okna pro stvrzení Certifikační autority



- zde zaškrtneme ***Uznání pro identifikaci serverů***, stiskneme OK a dokončíme import.

2.2.2 Zákaz IPV6 DNS v prohlížeči Mozilla Firefox

V některých specifických konfiguracích, např. v prostředí firemní sítě při využívání WPAD se může stát, že PKI komponenta v prohlížeči Firefox stále nefunguje. Tzn. ani po výše uvedeném importu autority se ji nedaří detekovat. Pak je potřeba změnit systémové nastavení prohlížeče a sice zakázat dohledávání IPv6 adres v DNS.
Postup je doporučován pouze pro zkušené uživatele, protože je třeba měnit nastavení v systémovém editoru Firefox:

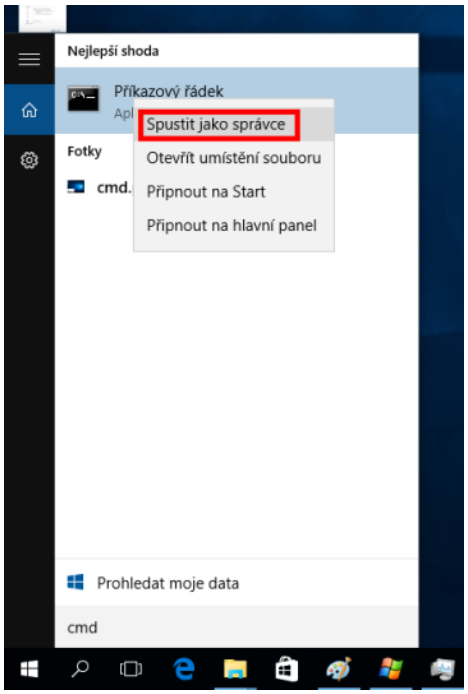


1) Do adresního řádku prohlížeče napíšeme ***about:config*** a stiskneme ***Enter***.
2) Přijmeme varování o vstupu určeném pouze pro zkušené uživatele
3) Vyhledáme „***network.dns.disableIPv6***“ a dvojklikem na tuto položku změníme *Hodnotu z* ***false*** *na* ***true.***
4) Záložku je možné uzavřít, nastavení je uloženo.

2.2.3 Nastavení prohlížeče Microsoft Edge

V případě problémů s detekcí nainstalované komponenty OTE PKi Klient v prohlížeči Microsoft Edge (zakázána komunikace webové aplikace s lokálními programy), spustťe příkazový řádek v Administratorském módu:

- v Menu Windows do řádku *Prohledat program a soubory* napíšeme cmd
- následně klikneme pravým tlačítkem myši na **cmd.exe / Příkazový řádek**



- z nabídnutého menu vybereme *Spustit jako správce/administrator*
- po zadání administrátorského jména a hesla se spustí příkazový řádek, kam je třeba zadat následující příkaz:

```
CheckNetIsolation LoopbackExempt -a -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"
```

- následný stisk Enter příkaz provede a prohlížeč je připraven k použití

2.2.4 Nastavení v CS OTE portálu

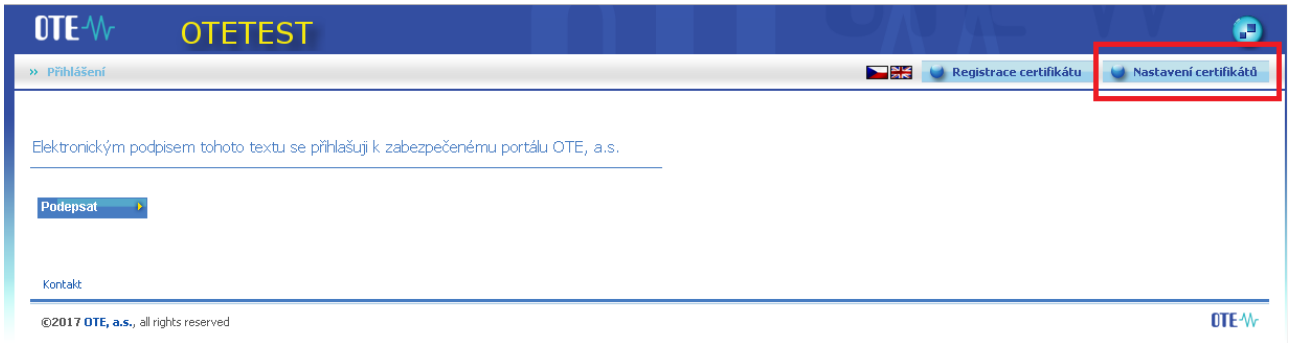
Portál CS OTE využívá lokální úložiště prohlížeče v daném profilu pro uložení nastavení určené pro práci s OTE PKI klientem. V případě, že není povoleno **ukládání Historie prohlížení** v nastavení používaného prohlížeče, je nutné všechny níže uvedené kroky vždy provádět při každém spuštění.

V případě, že je lokální úložiště inicializovano pro použití s certifikáty PKCS#12 (tzv. softwarové) je třeba napřed provést jeho dekonfiguraci.

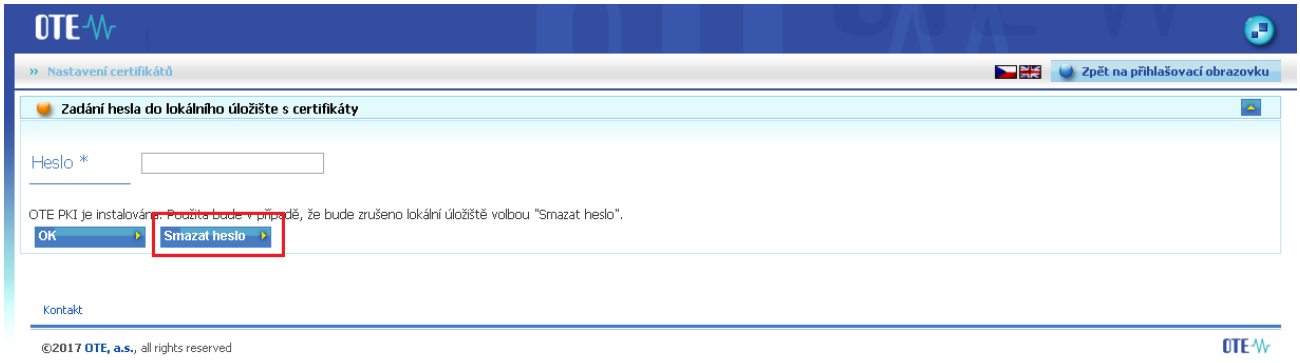
Veškerá níže uvedená nastavení se vždy provádí pro každý prohlížeč, resp. pro každý uživatelský profil operačního systému nebo prohlížeče.

2.2.5 Smazání dříve inicializovaného lokálního úložiště SW certifikátů

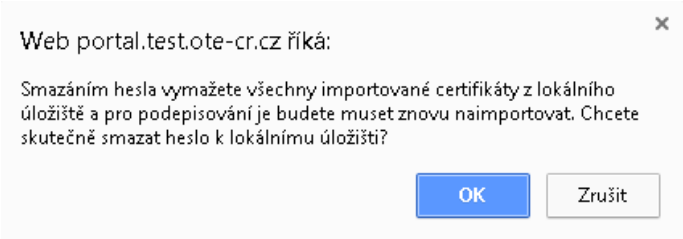
- na přihlašovací stránce do CS OTE zvolíme ***Nastavení certifikátů***



- na stránce Nastavení lokálního úložiště certifikátů zvolíme ***Smazat heslo***

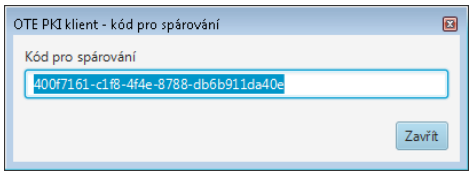


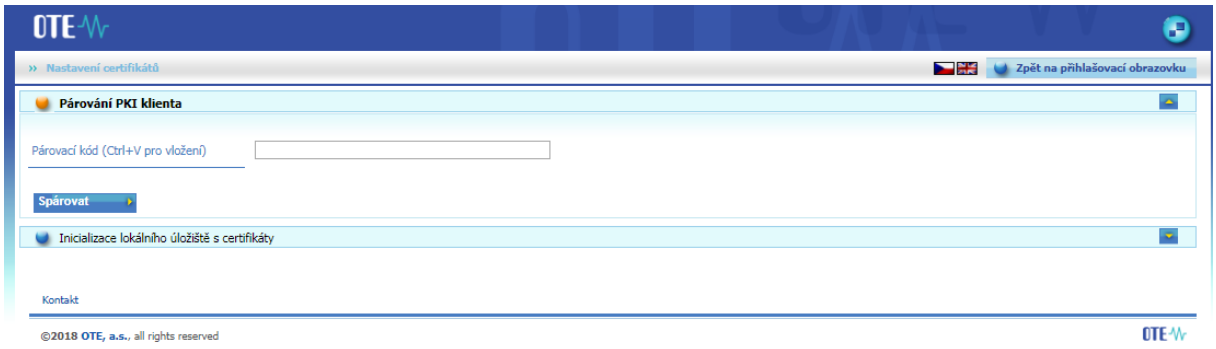
- následně, k dokončení instalace, potvrdíme možnost odstranění lokálního úložiště:



2.2.6 Párování web aplikace s komponentou

Pokud není lokální úložiště využíváno, tak při přístupu do Nastavení certifikátů se automaticky objeví dialogové okno OTE PKI klient s kódem pro spárovaní, který již je tímto okamžikem nakopírovaný do paměti *cache*. Webový portal CS OTE zobrazí sekci *Párování PKI klienta*, kam je třeba uvedený párovací kód stiskem Ctrl+V vložit:

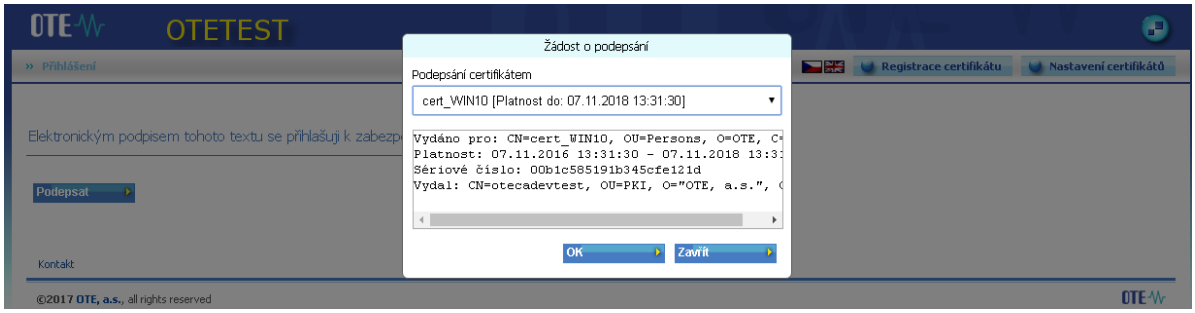




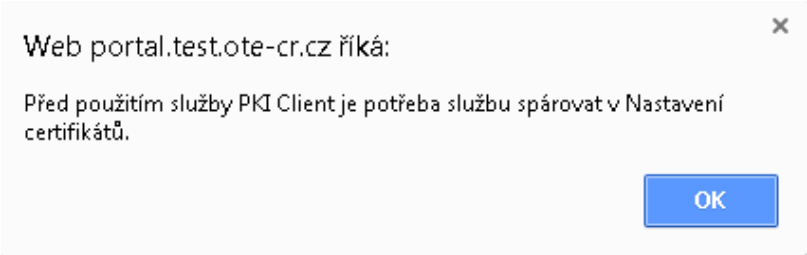
Po vložení uvedeného kódu a stisku ***Spárovat*** se zobrazí stránka s přehledem všech certifikátů v úložišti operačního systému. Aktivace OTE PKI klient je nyní dokončena.

V případě, že se se Dialog pro párování (OTE PKI klient) automaticky nezobrazí, je možné toto dialogové okno vyvolat stiskem pravého tlačítka myši na ikoně OTE PKI v seznamu rezidetních programů (v pravém dolním rohu obrazovky) a výběrem ***Otevřít dialog pro spárování****.*

Stiskem ***Zpět na přihlašovací stránku*** a ***Podepsat*** se nyní můžeme do portálu přihlásit.



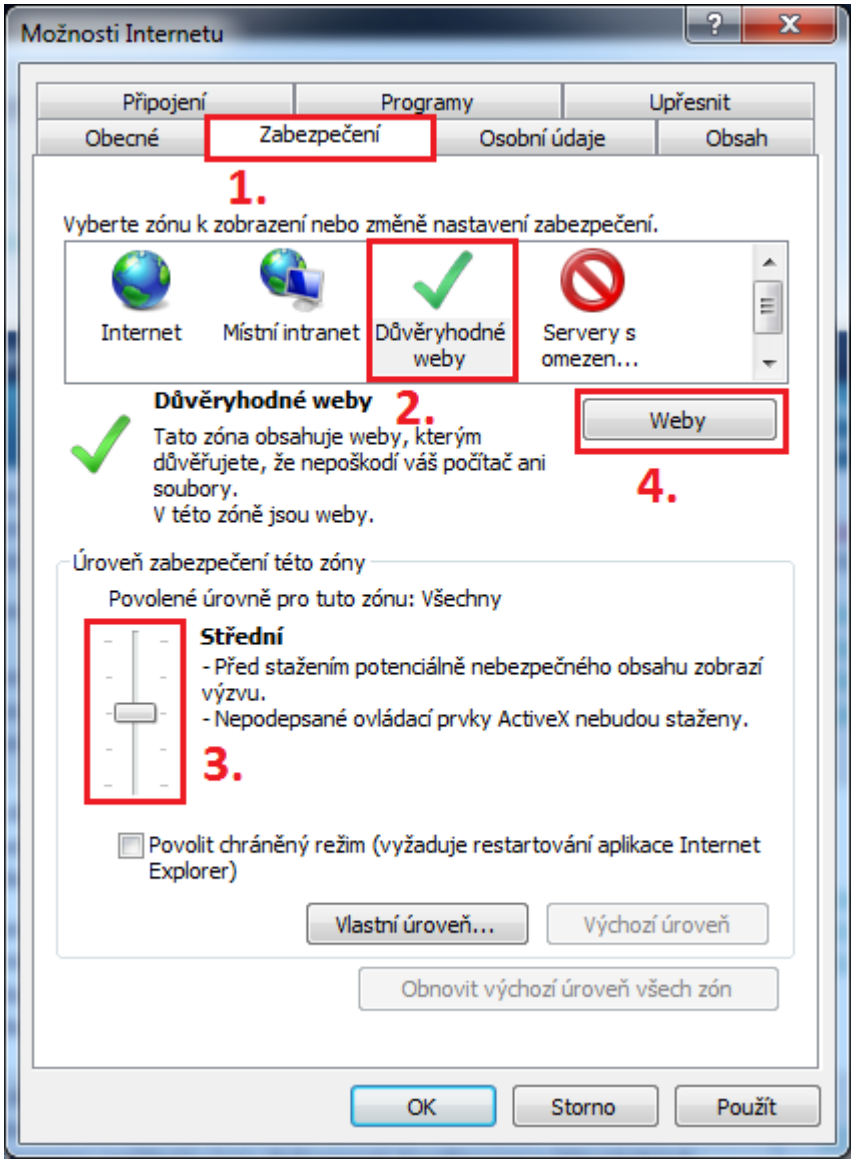
V případě, že není využíváno lokální úložiště pro softwarové certifkáty a je instalována OTE PKI komponenta, tak dokud není spárována, upozorňuje na tuto skutečnost CS OTE portál po stisku tlačítka Podepsat:

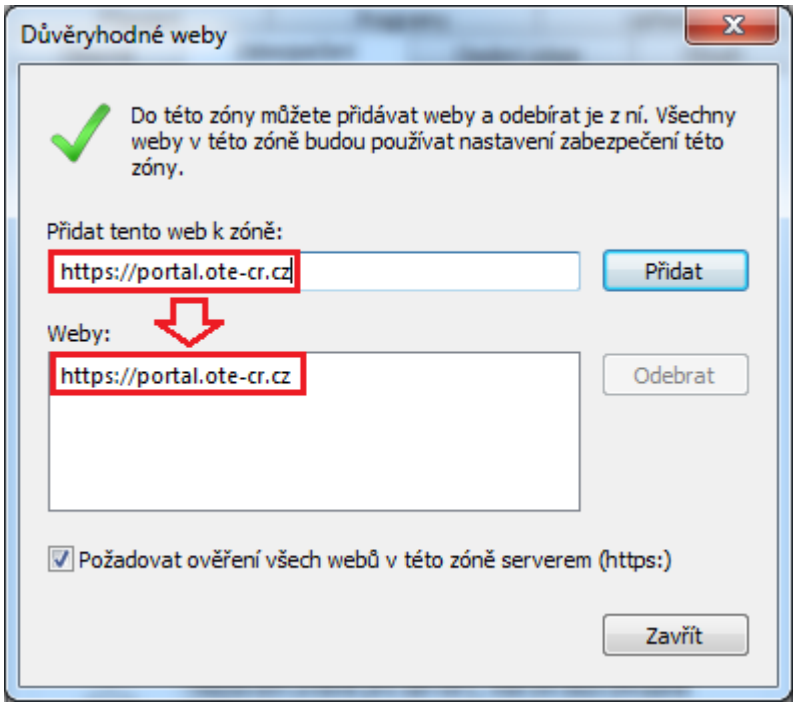

Web portal.test.ote-cr.cz říká:
Před použitím služby PKI Client je potřeba službu spárovat v Nastavení certifikátů.
OK

3 Prohlížeč Microsoft Internet Explorer

3.1 Nastavení důvěryhodných stránek

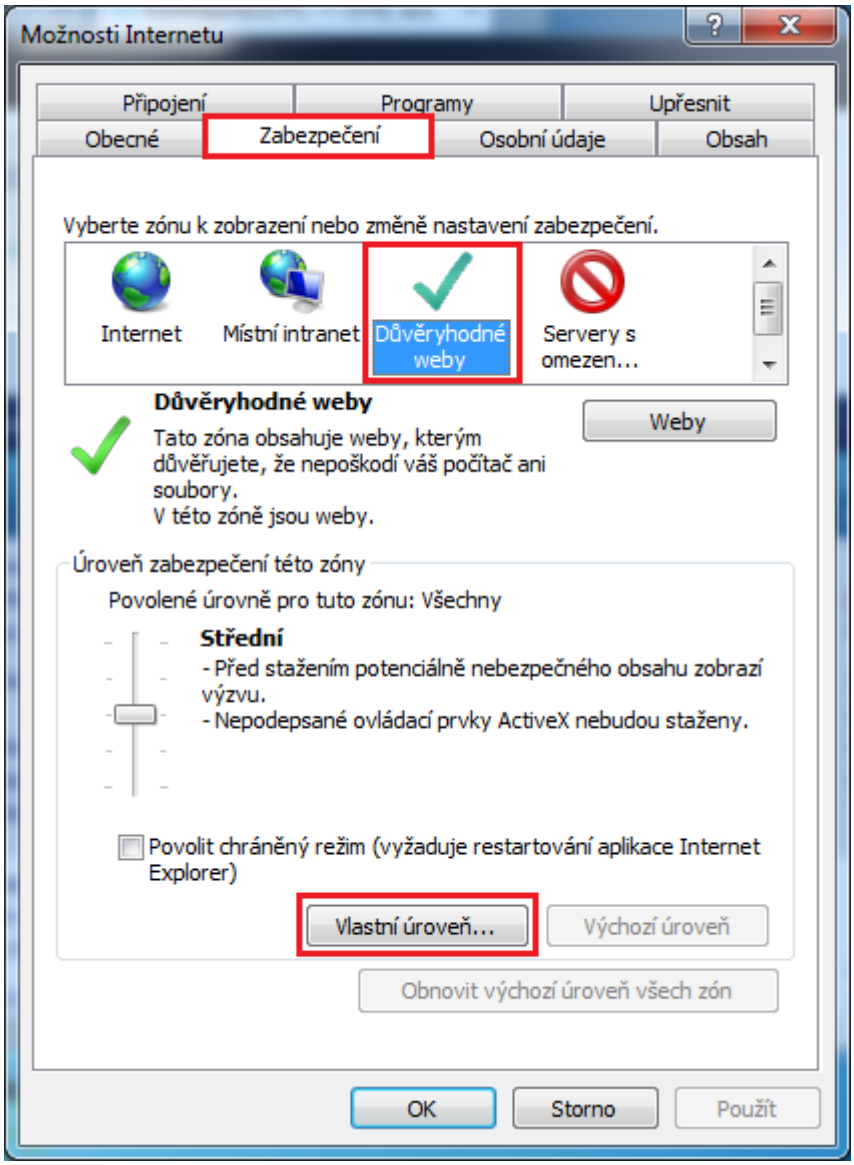
Všechna nastavení Internet Exploreru jsou ve standardním stavu, pouze pro některé funkce může být vyžadováno zařazení **https://portal.ote-cr.cz/otemarket do „Trusted sites“,** v menu Tools, Options jak je zobrazeno níže včetně kontroly úrovně zabezpečení.

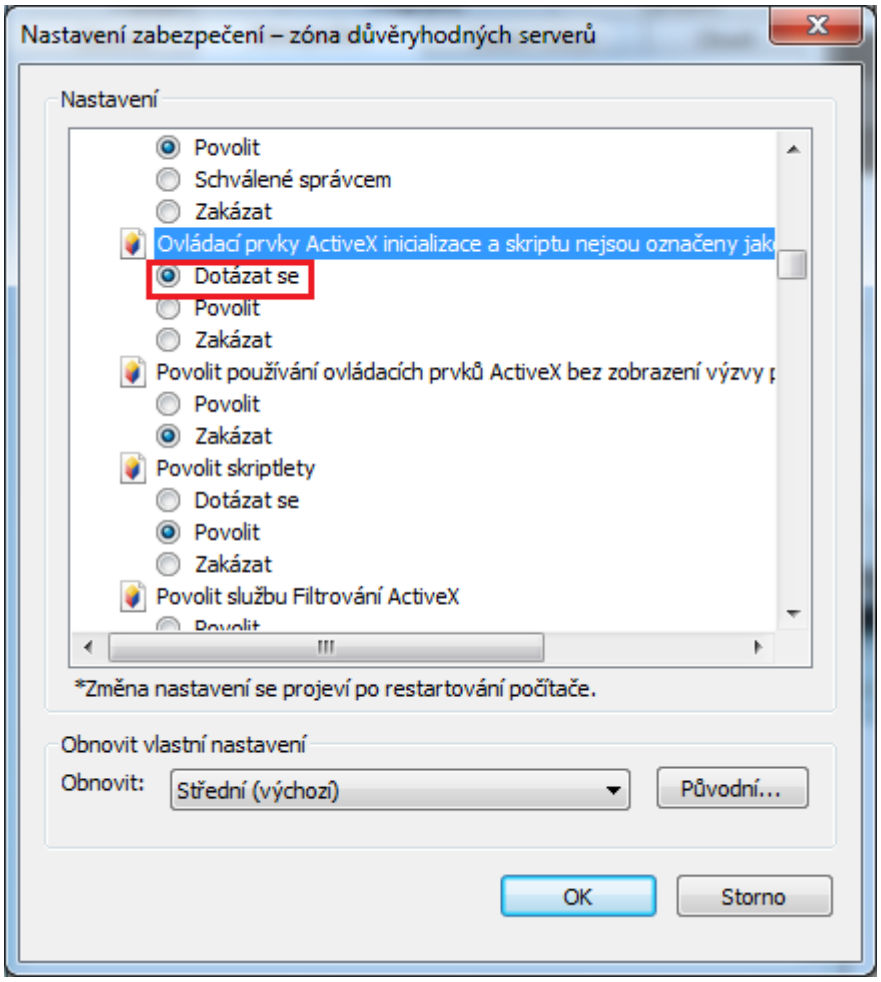




3.2 Kontrola povolení ActiveX komponent

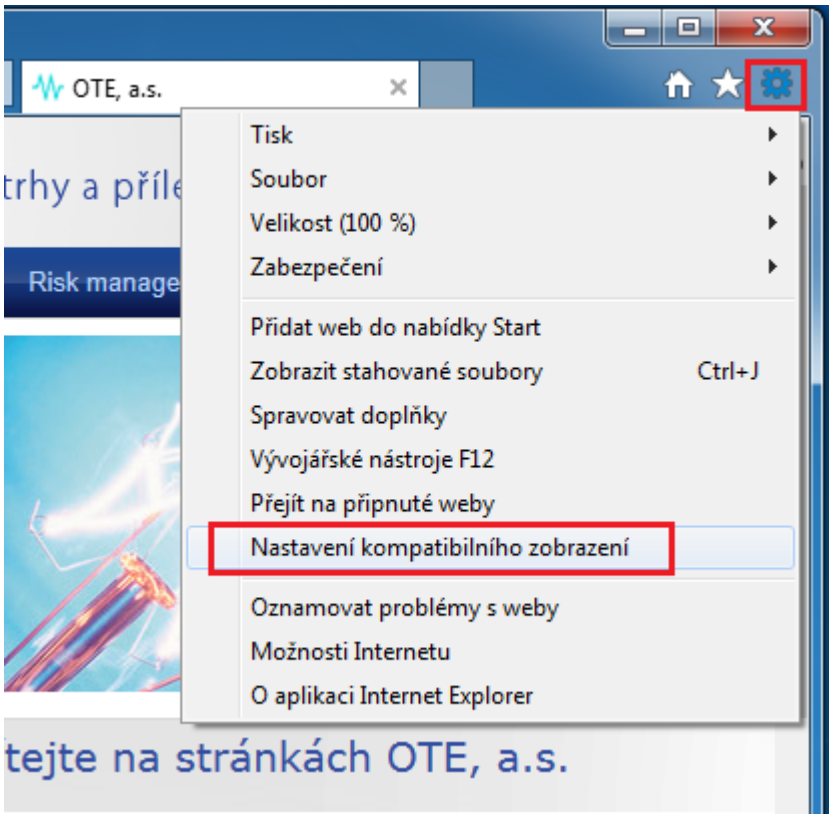
Pro korektní fungování v některých částech CS OTE je nutné zkontrolovat, popř. povolit stahování ActiveX komponent na klientskou stanici, dle postupu níže:


Možnosti Internetu
Připojení
Programy
Upřesnit
Obecné
Zabezpečení
Osobní údaje
Obsah
Vyberte zónu k zobrazení nebo změně nastavení zabezpečení.
Internet
Místní intranet
Důvěryhodné weby
Servery s omezen...
Důvěryhodné weby
Tato zóna obsahuje weby, kterým důvěřujete, že nepoškodí váš počítač ani soubory.
V této zóně jsou weby.
Weby
Úroveň zabezpečení této zóny
Povolené úrovně pro tuto zónu: Všechny
Střední
- Před stažením potenciálně nebezpečného obsahu zobrazí výzvu.
- Nepodepsané ovládací prvky ActiveX nebudou staženy.
Povolit chráněný režim (vyžaduje restartování aplikace Internet Explorer)
Vlastní úroveň...
Výchozí úroveň
Obnovit výchozí úroveň všech zón
OK
Storno
Použít

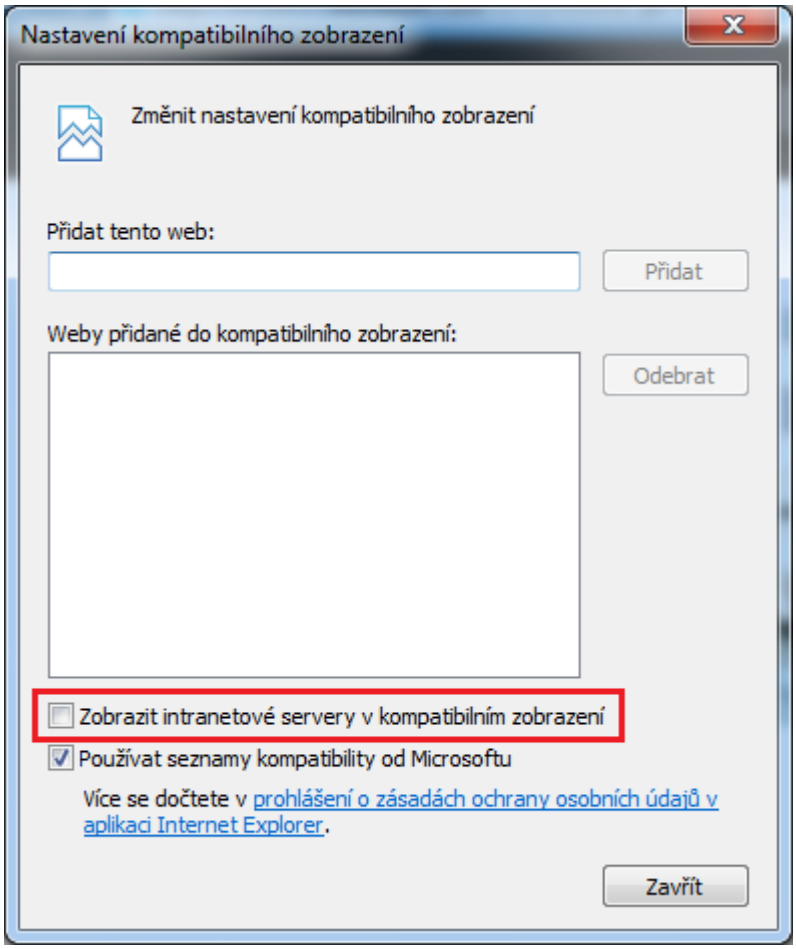


3.3 Nastavení kompatibility IE prohlížeče

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



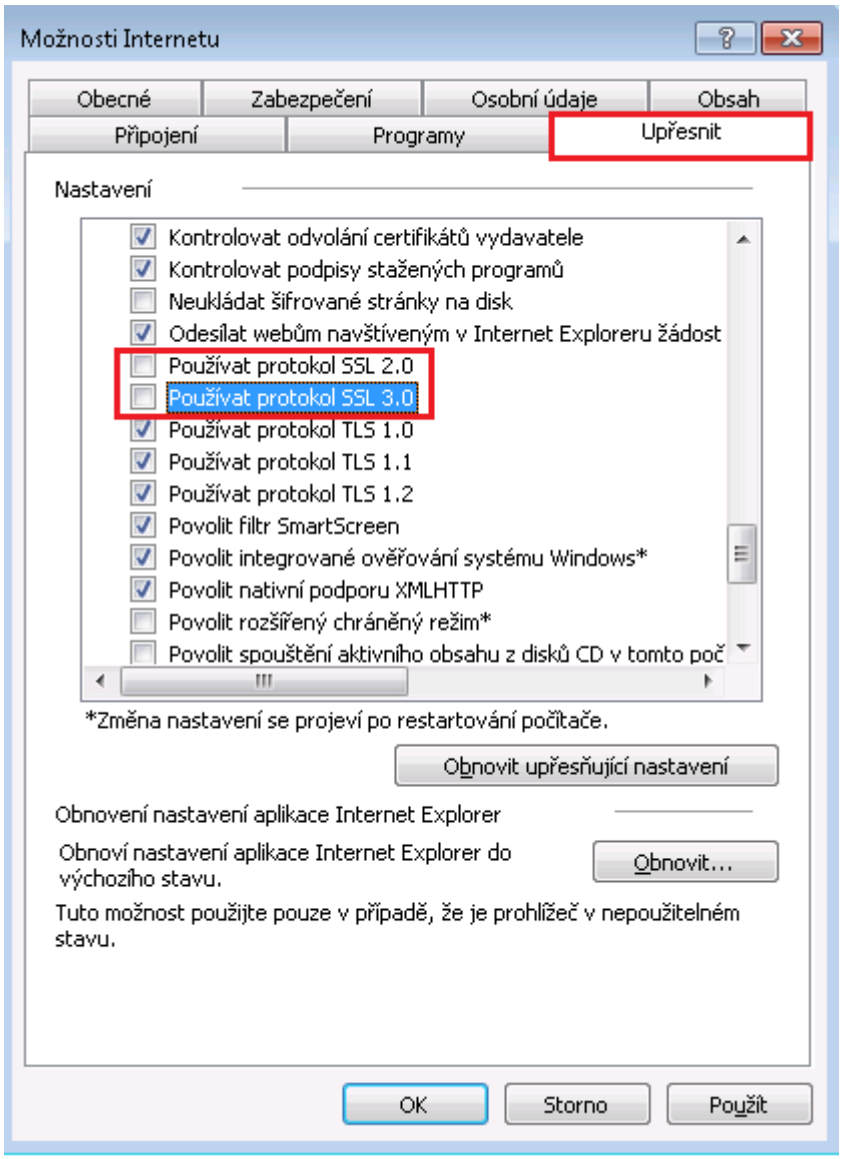
Z níže uvedené obrazovky odebrat implicitně nastavení „Zobrazit intranetové servery v kompatibilním zobrazení“, jak níže zobrazuje dialog.



A pak okno zavřít.

3.3.1 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.

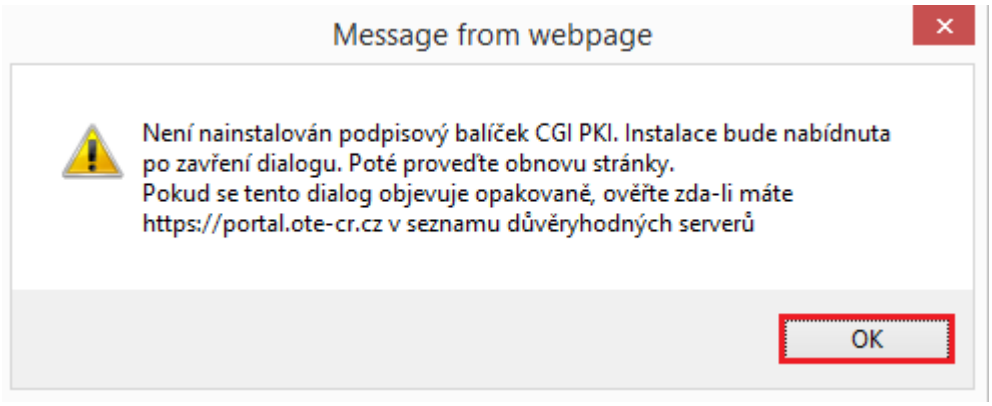


Ponechat jen TLS komunikaci a SSL odebrat a stisknout tlačítko OK.

3.3.2 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!**

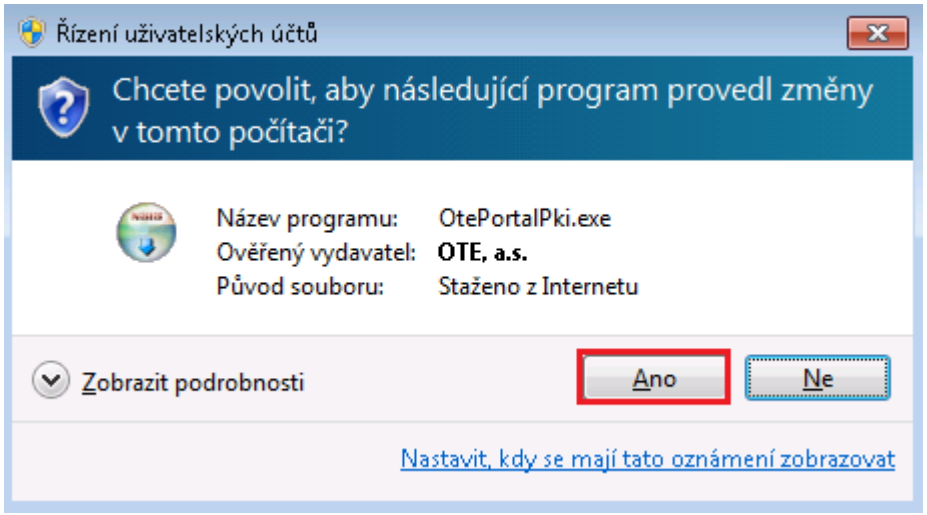
Po přihlášení na stránky https://portal.ote-cr.cz/otemarket a požadavku o elektronický podpis se objeví dialog o nutném stažení podpisového balíčku ActiveX.



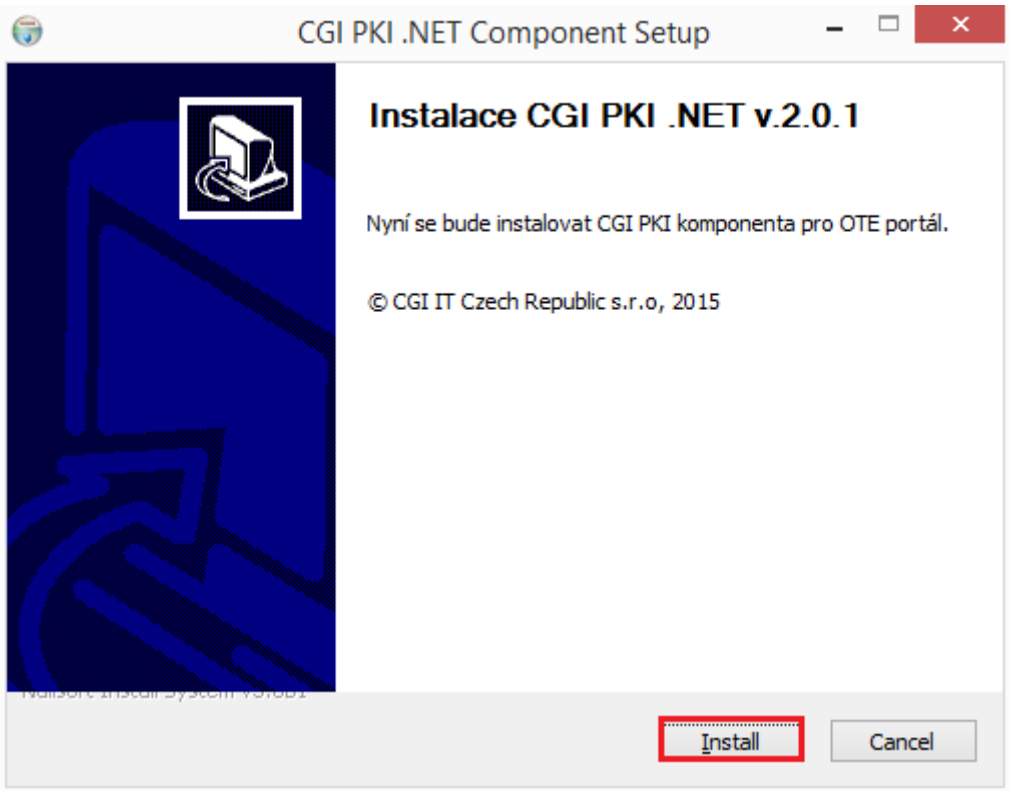
Stiskněte tlačítko „OK“.

V následujícím dialogu potvrďte volbu „Spustit“.

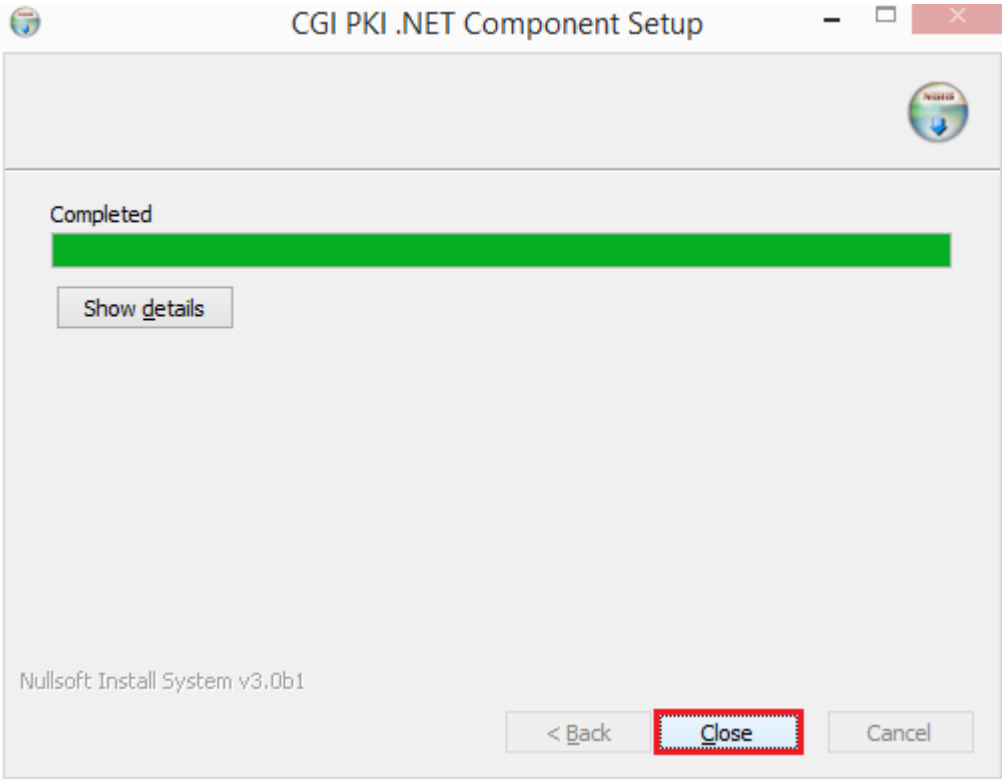
Stiskněte tlačítko „Ano“



Stiskněte tlačítko „Install/Instalovat“.

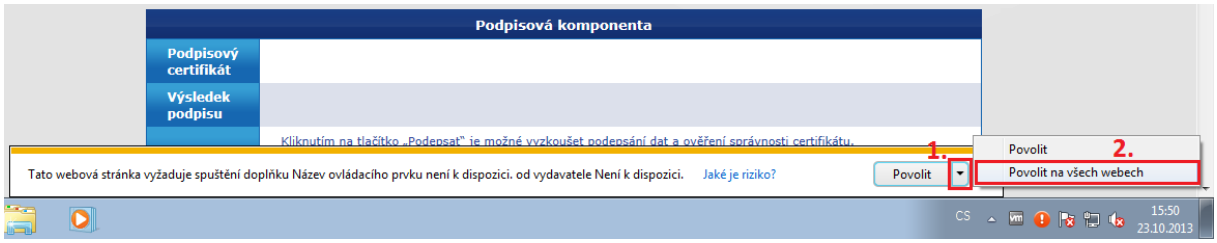


Stiskněte tlačítko „Close/Zavřít“.



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“.



3.3.3 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 baliček 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

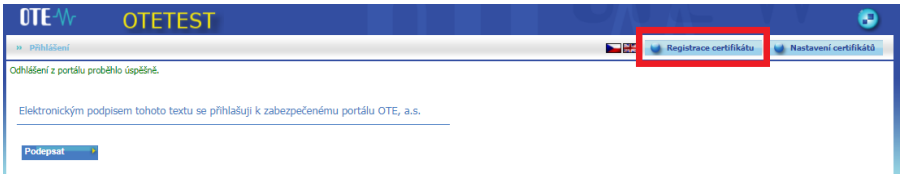
4 Registrace certifikátu po expiraci

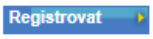
4.1 Přístup na portál CS OTE po vypršení platnosti certifikátu s IČ

1) Nový certifikát vydaný na stejné IČ, jako prošlý, vložíme do úložiště operačního systému, respektive do úložiště certifikátů používaného prohlížeče ***)**, aby bylo možné nový certifikát použít k podpisu.

) web. prohlížeč:** ***MENU – Nastavení – Certifikáty – Správce certifikátů – Osobní cert. **– vložíme nový certifikát**

2) Na přihlašovací stránce do portálu CS OTE zvolímo tlačítko ***Registrace certifikátu***:



- na následující stránce zvolíme ***Podepsat***
- zobrazí se „**Žádost o podepsaní**“ s nabídkou podpisových certifikátů – výběrem nově vloženého (se stejným IČ jako vypršelý) a stvrzením proběhne vyhledání v systému.
- zobrazí se stránka s Údaji o účastníkovi, o osobě a údaji o certifikátu
- pokud všechny zobrazené informace souhlasí potvrdíme stiskem 

Výpis hlášky ***Certifikát byl úspěšně zaregistrován*** informuje o jeho validním zaregistrování do systému a nyní je možné certifikát nadále běžně používat.

5 Nastavení přístupu do produkčního prostředí aplikace OTE-COM

Přístup do produkčního prostředí aplikace OTE-COM je možný dvěma následujícími způsoby:

1. Přes aplikaci OTE-COM
2. Přístup přímo na AMQP server ze serveru externího účastníka (Automatická komunikace)

5.1 Přístup přes aplikaci OTE-COM

- Nejdříve je nutné si stáhnout a nainstalovat OTE-COM Launcher Manager - elekřina (A) nebo OTE-COM Launcher Manager - plyn (B) (LM), který umožní spustit aplikaci OTE-COM.

  A) OTE-COM Launcher Manager - Elektřina

  - Pro 32bit verzi OS: http://www.ote-cr.cz/OTE-COM-POWER-PROD-windows-i586.exe
  - Pro 64bit verzi OS: http://www.ote-cr.cz/OTE-COM-POWER-PROD-windows-x64.exe

  B) OTE-COM Launcher Manager - Plyn

  - Pro 32bit verzi OS: http://www.ote-cr.cz/OTE-COM-GAS-PROD-windows-i586.exe
  - Pro 64bit verzi OS: http://www.ote-cr.cz/OTE-COM-GAS-PROD-windows-x64.exe

  - Instalační manuál OTE Launcher Manageru si můžete stáhnout zde.

- Komunikace LM probíhá prostřednictvím protokolu https, což v obvyklých případech nezpůsobuje žádné potíže. Mohou se však vyskytovat komplikace pokud je účastníkem využíván proxy server. V takovém případě je nutné v nastavení aplikace LM (kliknutím na tlačítko O) provést nastavení volby HTTP proxy a povolení přístupu na http://www.ote-cr.cz a https://portal.ote-cr.cz, popř. kontaktovat své IT oddělení a požádat je o nastavení.

- Upozorňujeme, že je potřeba, aby byl povolen přístup na URL amqp.ote-cr.cz (IP 91.209.101.43), port 5671 v infrastruktuře na straně účastníka.

- Každý účastník, který nyní přistupuje s osobním certifikátem do produkčního prostředí portálu CS OTE, bude mít pod stejným certifikátem přístup i do aplikace OTE-COM (prostřednictvím LM). Z hlediska osobních certifikátů se tedy na straně účastníků trhu nemusí nic měnit.

- Informace o instalaci kořenových certifikátů, které je třeba mít nainstalované pro přístup k aplikaci OTE-COM, naleznete v manuálu OTE Launcher Manageru.

5.2 Přístup přímo na AMQP server ze serveru účastníka trhu (Automatická komunikace)

- Komunikace probíhá na adrese (A-elekřina, B-plyn):

  A) amqp.ote-cr.cz (91.209.101.43), port 5671,virtualhost = market
  B) amqp.ote-cr.cz (91.209.101.43), port 5671,virtualhost = marketGAS

- Podporované TLS rozhraní: verze 1.2.

- Pro tento typ komunikace je nutné na straně účastníka trhu implementovat rozhraní, jehož specifikace je dostupná zde. Šablony zpráv pro OTE-COM aplikaci jsou dostupné zde. V tomto případě není využívána funkcionalita nastavení proxy.

- Pro tuto komunikaci je využíván AMQP protokol, který nemusí podporovat http/SOCKS proxy konfiguraci na straně účastníka trhu. V takovém případě je nutné, aby se účastník obrátil na své IT oddělení.

- Každý účastník, který nyní přistupuje s osobním certifikátem do produkčního prostředí portálu CS OTE, bude mít pod stejným certifikátem přístup i na AMQP server (prostřednictvím automatické komunikace). Z hlediska osobních certifikátů se tedy na straně účastníků trhu nemusí nic měnit.

- Informace o instalaci kořenových certifikátů, které je třeba mít nainstalované pro přístup k aplikaci OTE-COM, naleznete v manuálu OTE Launcher Manageru.