Uživatelská příručka informačního systému

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	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
26.2.2019	Doplnění možnosti jiného získání certifikační autority oteca.pem
26.4.2019	Kapitola o lokálním úložišti přesunutá z dokumentu Registrace
25.05.2019	Přechod z OTE PKI komponenty na Lokální Úložiště
26.06.2023	Revize konfigurace stanice a odstranění odkazu na download OTECOM
8.8.2024	Revize dokumentu
08.01.2026	Doplnění informace o aktuálnosti PKI komponent

Obsah

1 Konfigurace stanice a možnosti autentizace do CS OTE 3

2 OTE PKI klient pro přístup do CS OTE 4

2.1 Instalace komponenty OTE PKI 4

2.2 Poinstalační konfigurace 7
2.2.1 Import OTECA autority do prohlížeče Mozilla Firefox 7
2.2.2 Zákaz IPV6 DNS v prohlížeči Mozilla Firefox 9
2.2.3 Nastavení prohlížeče Microsoft Edge 9
2.2.4 Nastavení v CS OTE portálu 10
2.2.5 Smazání dříve inicializovaného lokálního úložiště SW certifikátů 11

3 Lokální úložiště certifikátů pro přístup do CS OTE 12

3.1 Výzva k vložení certifikátu do lokálního úložiště při pokusu o elektronický podpis 12

3.2 Správa lokálního úložiště 14

3.3 Vložení certifikátu do lokálního úložiště 15

3.4 Smazání certifikátu z lokálního úložiště 16

3.5 Odstranění expirovaných certifikátů z lokálního úložiště 17

3.6 Výběr primárního certifikátu 17

3.7 Změna hesla pro přístup do lokálního úložiště 18

3.8 Zapomenuté heslo pro přístup do lokálního úložiště 19

4 Registrace certifikátu po expiraci 21

4.1 Přístup na portál CS OTE po vypršení platnosti certifikátu s IČ 21

5 Nastavení přístupu do produkčního prostředí aplikace OTE-COM 22

5.1 Přístup přes aplikaci OTE-COM 22

5.2 Přístup přímo na AMQP server ze serveru účastníka trhu (Automatická komunikace) 23

1 Konfigurace stanice a možnosti autentizace do CS OTE

Kompatibilní webové prohlížeče:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge (bez kompatibilního režimu)

Kompatibilní operační systémy

- Windows 10
- Windows 11

Výše uvedená podporovaná prostředí by měla být aktualizována bezpečnostními update doporučenými MS na http://windowsupdate.microsoft.com.

Přihlášení do zabezpečeného portálu CS OTE je možné dvěma způsoby:

1) **OTE PKI Client** (umožňuje využití v počítači již nainstalovaných certifikátů)
   – kapitola *2 - OTE PKI klient pro přístup do CS OTE*

   Upozornění: 32bit verze již není aktivně udržována ani aktualizována.

   Doporučujeme používat 64bit verzi OTE PKI Client.

2) **Lokální úložiště certifikátů**
   - kapitola *3 - Lokální úložiště certifikátů*

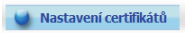
2 OTE PKI klient pro přístup do CS OTE

2.1 Instalace komponenty OTE PKI

Komponentu OTE PKI je možné nainstalovat po stažení z veřejného webu OTE – A) nebo z portálu CS OTE

A) Veřejný web http://www.ote-cr.cz/registrace-a-smlouvy/pristup-do-cs-ote/konfigurace-pc

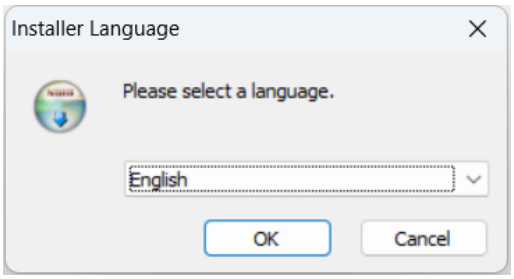
Tabulka *A) Přístup do CS OTE prostřednictvím webového prohlížeče*

B) Instalace z portálu CS OTE : portal.ote-cr.cz – na přihlašovací stránce zvolíme 

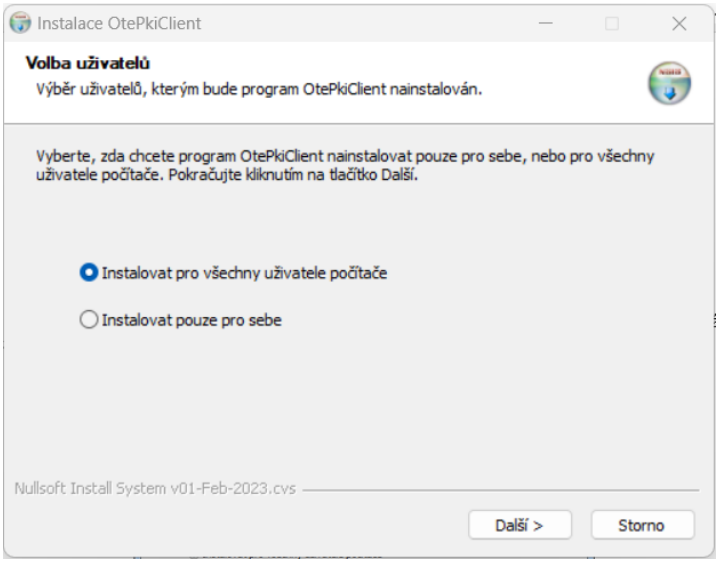
A na stránce Nastavení certifikátů vybereme možnost instalace:

Instalační proces Pki komponenty

1) Instalátor vyzve k volbě jazyka

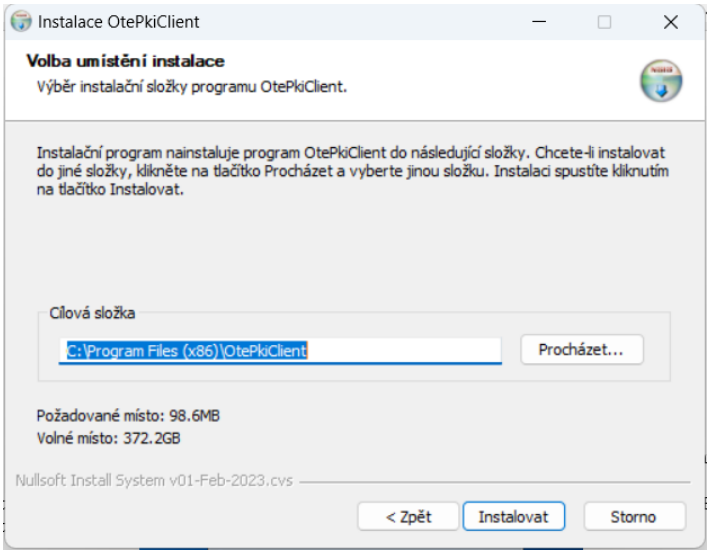


2) V dalším kroku, v závislosti na verzi prohlížeče, zvolíme zda-li nainstalována aplikace má být přístupná i ostatním uživatelům



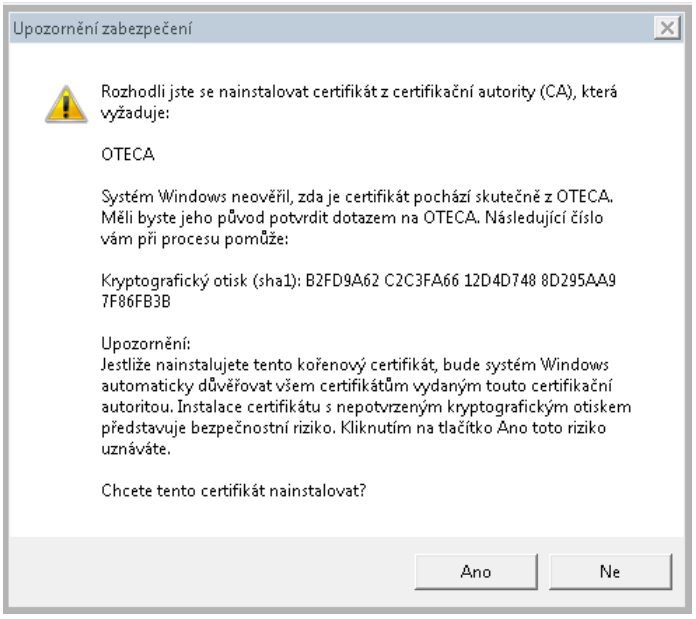
- při výběru pro všechny uživatele aplikace nabídne instalaci do Program Files
- v případě výběru pro daného uživatele aplikace nabídne instalaci do uživatelské složky

3) Následně je možné upravit umístění instalace



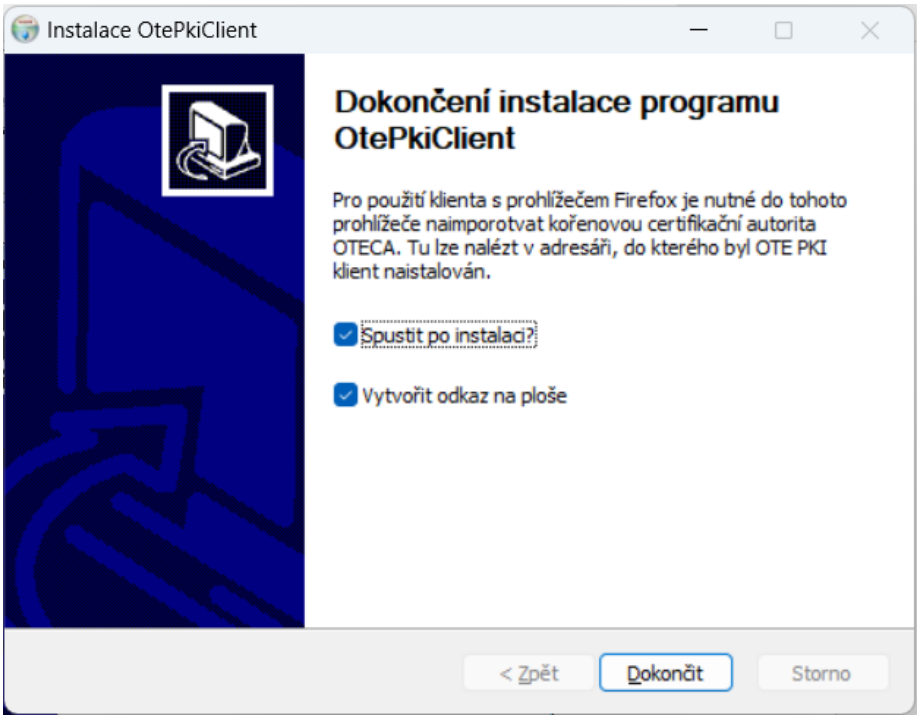
4) Je na PC nainstalovaná Certifikační Autorita OTECA nezbytná pro funkci OTE PKI klient ?

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



Odsouhlasením uvedeného instalace pokračuje. Autorita je nyní dostupná pro všechny podporované prohlížeče kromě Mozilla Firefox. Import pro tento prohlížeč je popsán v kapitole 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 **2.2.3**.

2.2.1 Import OTECA autority do prohlížeče Mozilla Firefox

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

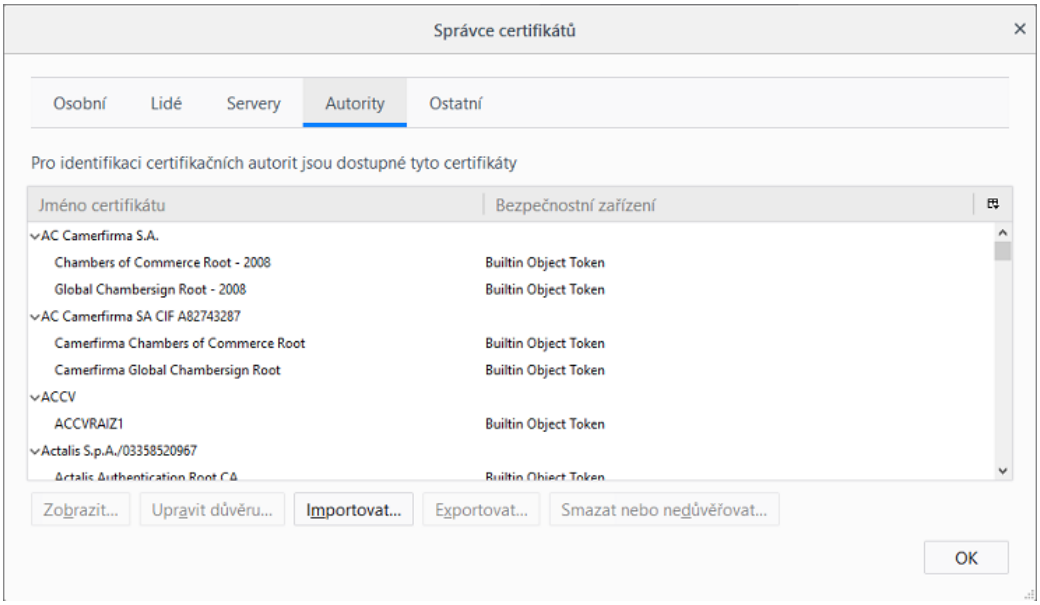
a) stažením souboru **oteca.pem** z odkazu https://www.ote-cr.cz/cs/registrace-a-smlouvy/pristup-do-cs-ote/files-konfigurace-pc/oteca.pem a jeho následná instalace do prohlížeče

b) zkopírováním níže uvedeného textu do textového editoru. Soubor uložíme s názvem OTECA.pem a nainstalujeme do prohlížeče…

```
-----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=
```

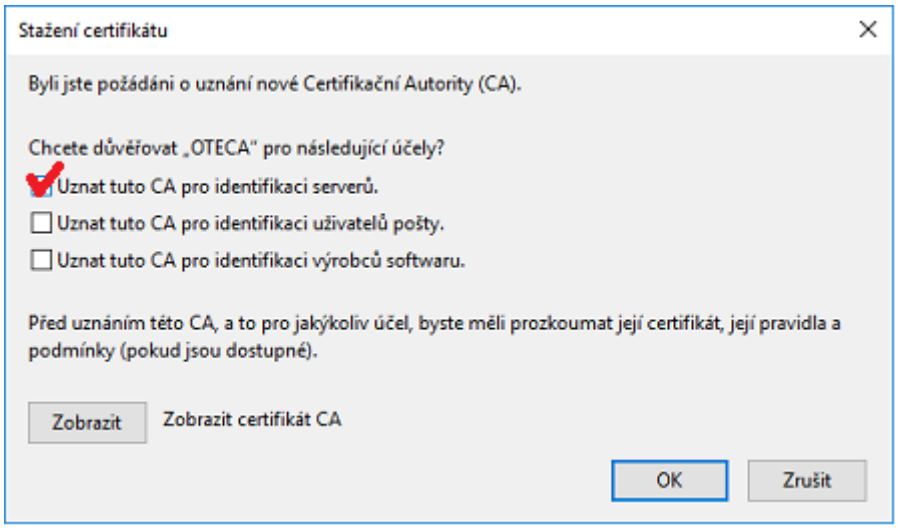
-----END CERTIFICATE-----

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.

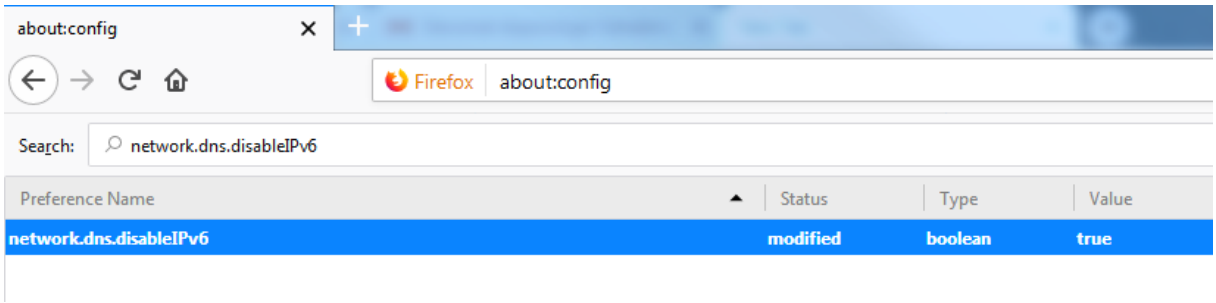
Dalším krokem je zobrazení okna pro stvrzení Certifikační autority



- 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:

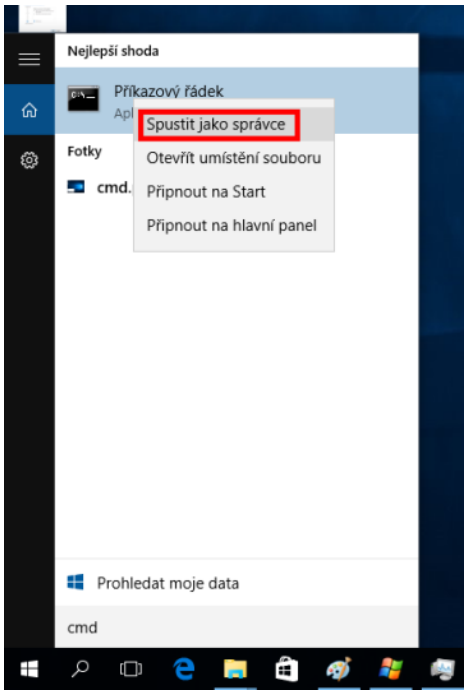


1) Do adresního řádku prohlížeče napíšeme ***about:config*** a stiskneme ***Enter***.
2) Přijmeme varování o vstupu určeném pouze pro zkušené uživatele
3) Vyhledáme „***network.dns.disableIPv6***“ a dvojklikem na tuto položku změníme *Hodnotu z* ***false*** *na* ***true.***
4) Záložku je možné uzavřít,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

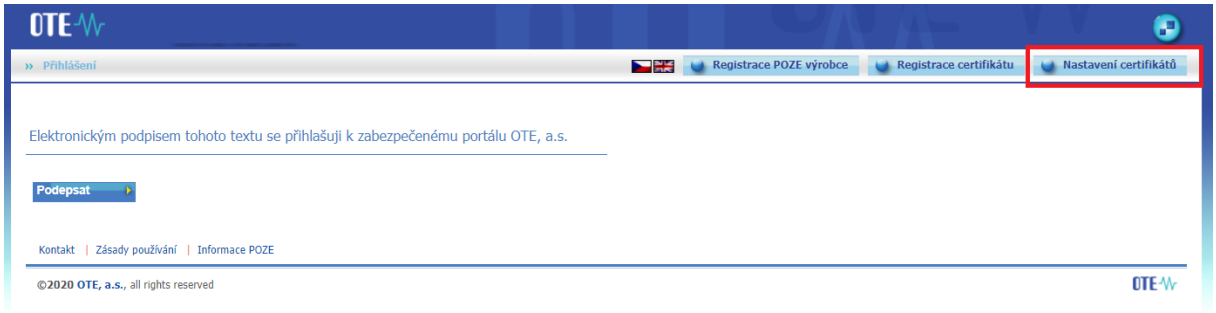
Portál CS OTE využívá lokální úložiště prohlížeče v daném profilu pro uložení nastavení určené pro práci s OTE PKI klientem. V případě, že není povoleno **ukládání Historie prohlížení** v nastavení používaného prohlížeče, je nutné všechny níže uvedené kroky vždy provádět při každém spuštění.

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

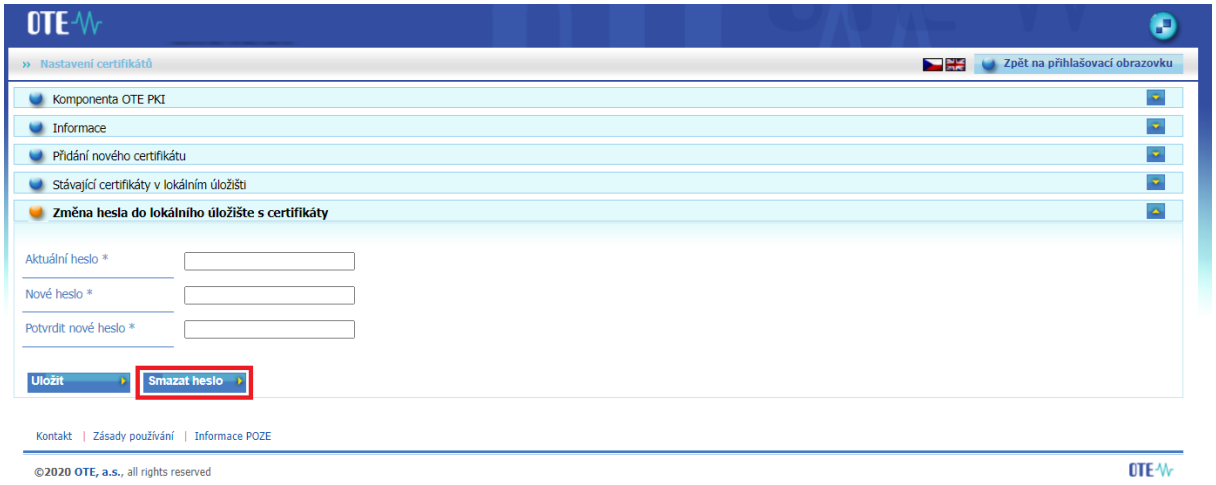
Veškerá níže uvedená nastavení se vždy provádí pro každý prohlížeč, resp. pro každý uživatelský profil operačního systému nebo prohlížeče.

2.2.5 Smazání dříve inicializovaného lokálního úložiště SW certifikátů

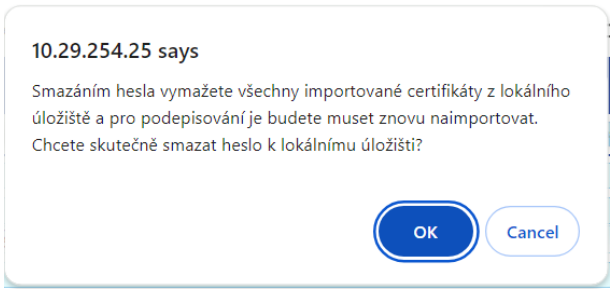
- na přihlašovací stránce do CS OTE zvolíme ***Nastavení certifikátů***



- na stránce Změna hesla do lokálního úložiště certifikátů zvolíme ***Smazat heslo***



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



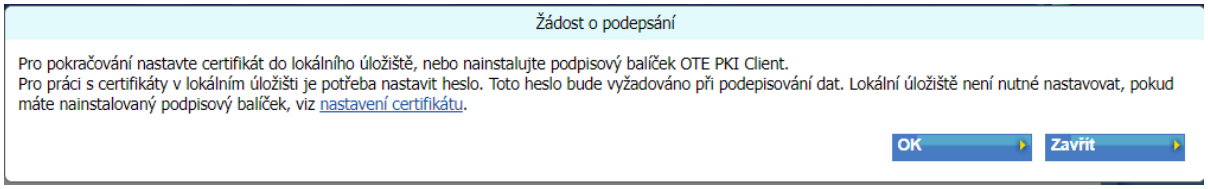
3 Lokální úložiště certifikátů pro přístup do CS OTE

Lokální úložiště umožňuje uchovávat certifikáty pro podepisování dat. Úložiště slouží především pro uživatele, kteří chtějí podepisovat data pomocí moderních webových prohlížečů (Google Chrome, Microsoft Edge) a nemají nainstalovanou podpisovou komponentu - kapitola 2.1 Instalace komponenty OTE PKI

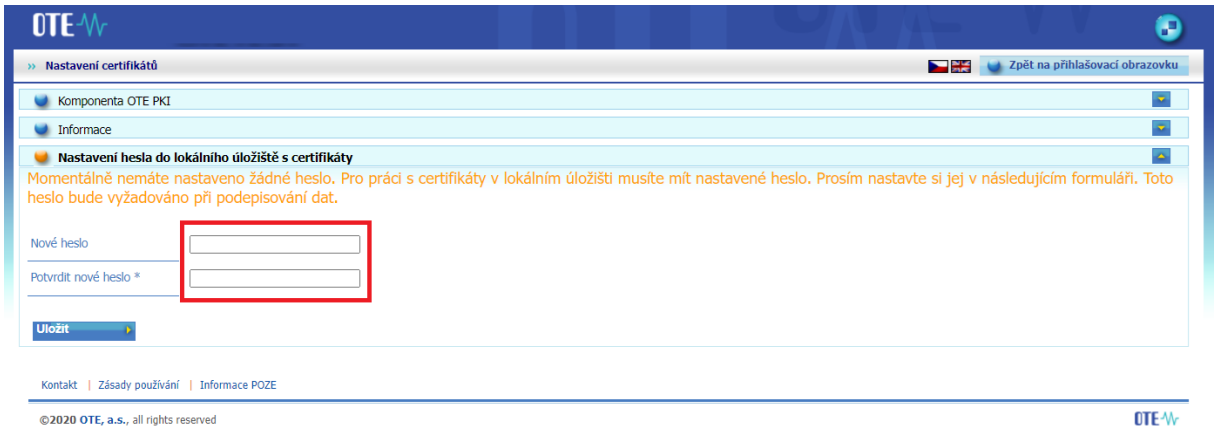
3.1 Výzva k vložení certifikátu do lokálního úložiště při pokusu o elektronický podpis

Při prvním pokusu o elektronický podpis v prohlížečích Google Chrome a Microsoft Edge se Vám zobrazí upozornění, že je nutno napřed vložit certifikát do lokálního úložiště certifikátů. Pokud používáte prohlížeč FireFox, zobrazí se Vám tato hláška, při prvním pokusu o elektronický podpis po aktualizaci FireFox na verzi 52 (aktualizace probíhá automaticky, nemusíte si tedy nemusí všimnout toho, že byla provedena).

Certifikát s privátním klíčem je importován pouze na Vaši lokální stanici do Vašeho uživatelského profilu do tzv. webového úložiště prohlížeče, které je určené jen pro konkrétní webovou aplikaci. Import provedený na adrese https://portal.ote-cr.cz není dostupný pro jinou adresu.



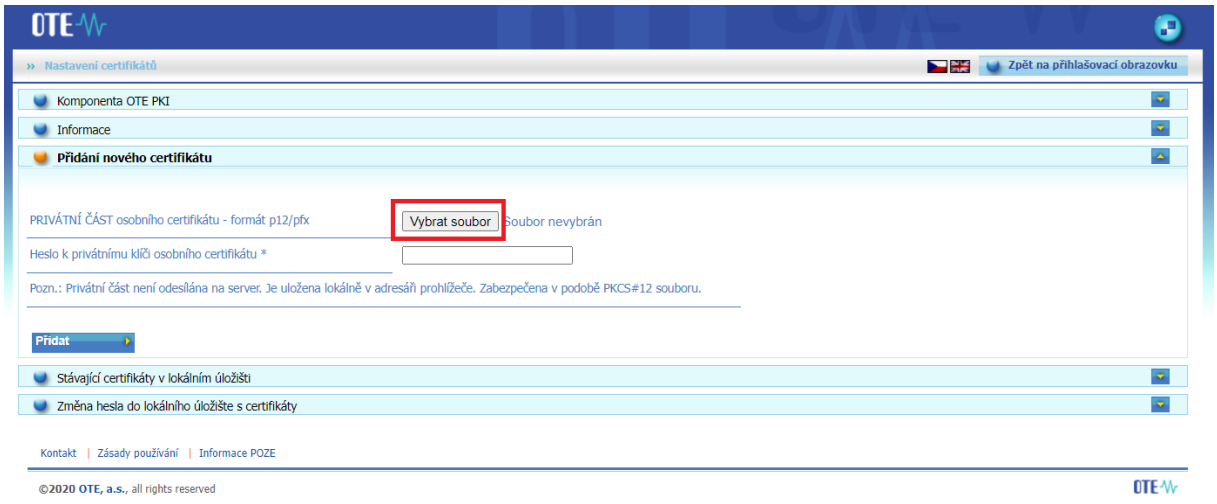
Po kliknutí na tlačítko OK budete přesměrováni do lokálního úložiště s certifikáty. Zde si musíte nastavit heslo, kterým bude úložiště chráněno. Po zadání hesla a jeho potvrzení klikněte na tlačítko Uložit.



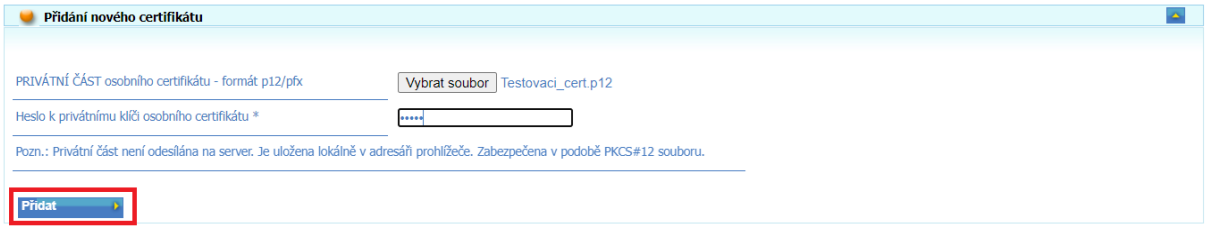
Dále klikněte na tlačítko „Procházet“ a vyhledejte zálohu vašeho certifikátu ve filesystému.

Je třeba naimportovat Váš certifikát včetně privátního klíče. K těmto účelům slouží soubor ve formátu p12 anebo pfx. Jedná se o tzv. zálohu soukromého klíče, která je doporučována externími certifikačními autoritami.

POZOR! Import certifikátu do lokálního úložiště je nutno provést po každé obnově certifikátu.



Po výběru certifikátu ve formátu p12 nebo pfx, zadejte heslo k privátnímu klíči osobního certifikátu (jedná se o heslo, které jste si nastavili při zálohování soukromého klíče do filesystému). Nakonec klikněte na tlačítko „Přidat“.



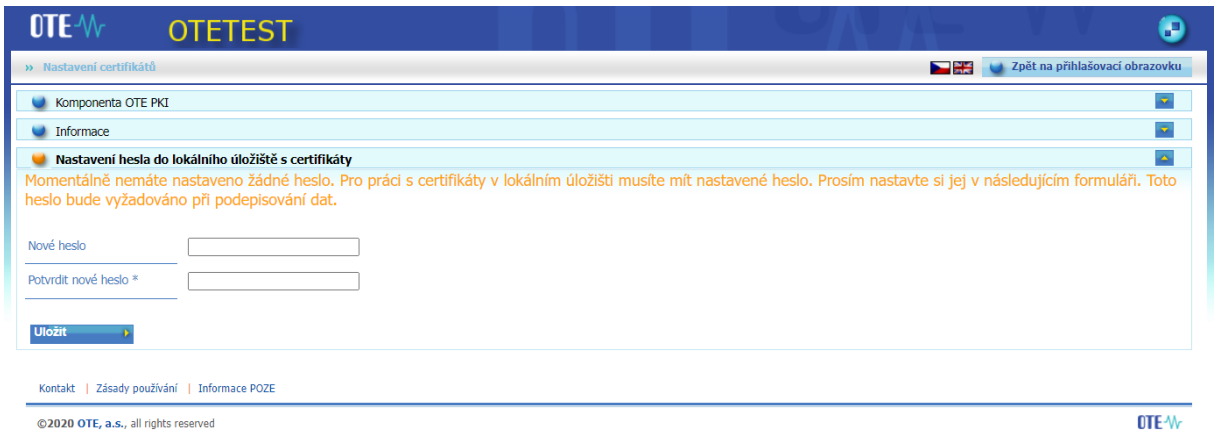
Po kliknutí na tlačítko se certifikát zobrazí v sekci „Stávající certifikáty v lokálním úložišti.

3.2 Správa lokálního úložiště

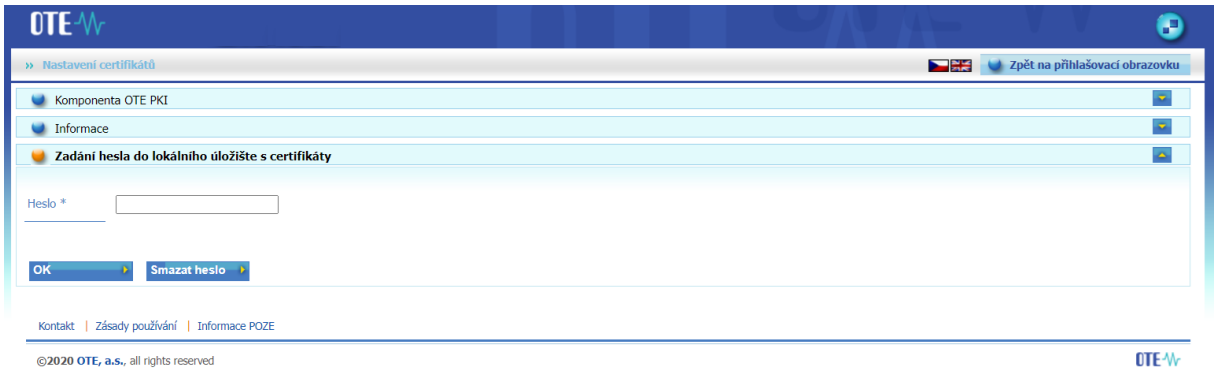
Výběrem *Správa certifikátů* v menu *Registrace* se zobrazí podmenu s položkou *Nastavení lokálního úložiště certifikátů*.

Následně vybereme záložku ***Inicializace lokálního úložiště s certifikáty***

Pokud se přihlašujete do lokálního úložiště poprvé, je nutné zadat heslo, které chcete používat pro přístup do lokálního úložiště. Pro kontrolu zopakujte a stiskněnte tlačítko Uložit. Následně budete přesměrování do lokálního úložiště.



V případě, že se nejedná o prvotní přihlášení, zadejte heslo a klikněte na tlačítko OK. Budete přesměrováni do lokálního úložiště.

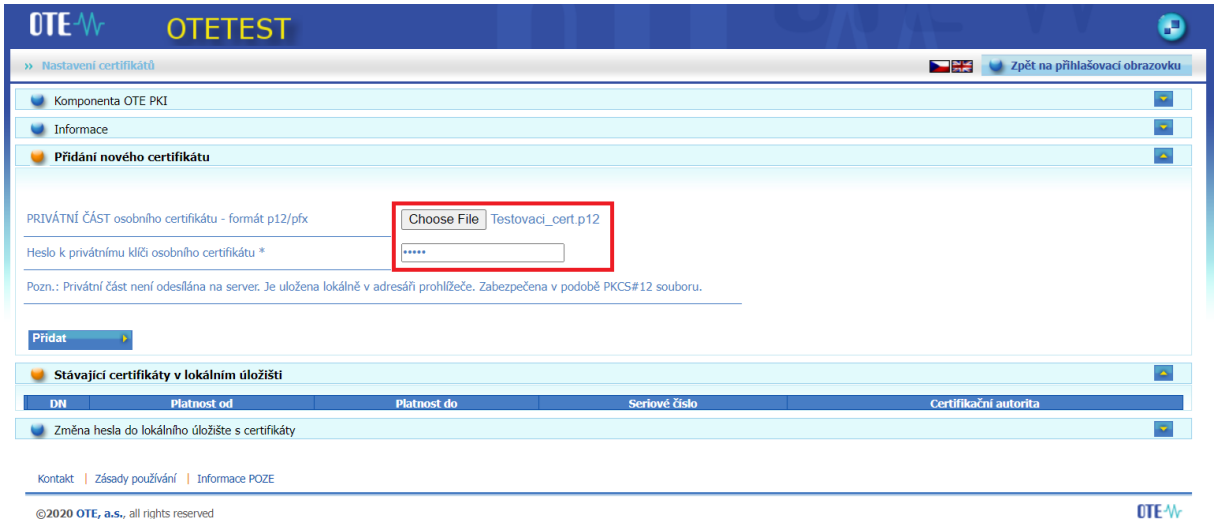


3.3 Vložení certifikátu do lokálního úložiště

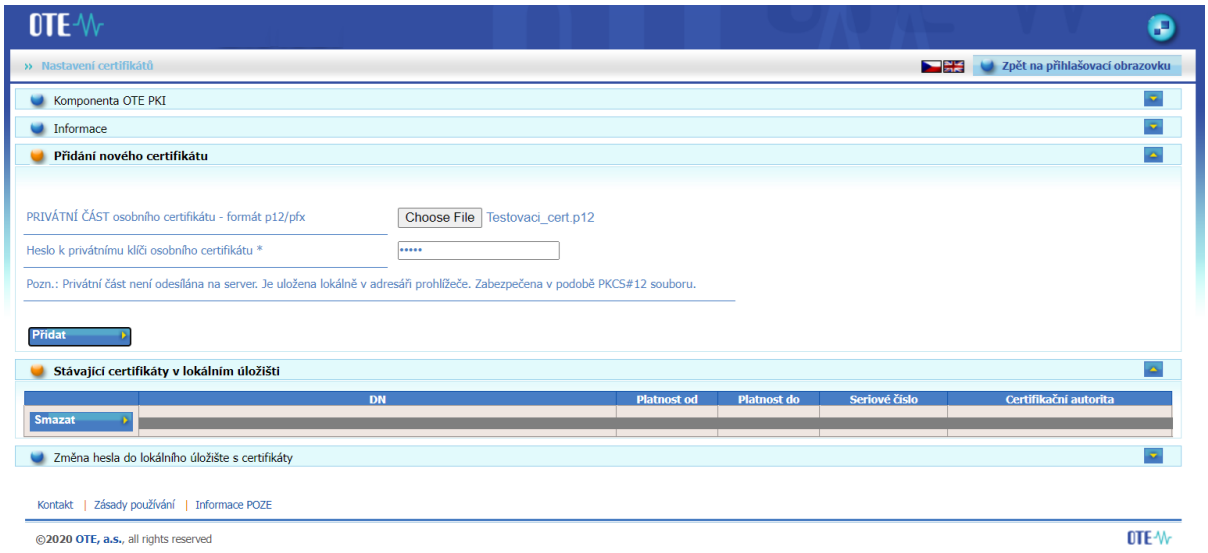
Klikněte na tlačítko Procházet a vyberte z filesystému certifikát, který chcete přidat do lokálního úložiště. Po vybrání certifikátu zadejte heslo, kterým je opatřený a klikněte na tlačítko Přidat.

Je třeba naimportovat Váš certifikát včetně privátního klíče. K těmto účelům slouží soubor ve formátu p12 anebo pfx. Jedná se o tzv. zálohu soukromého klíče, která je doporučována externími certifikačními autoritami.

POZOR! Import certifikátu do lokálního úložiště je nutno provést po každé obnově certifikátu.



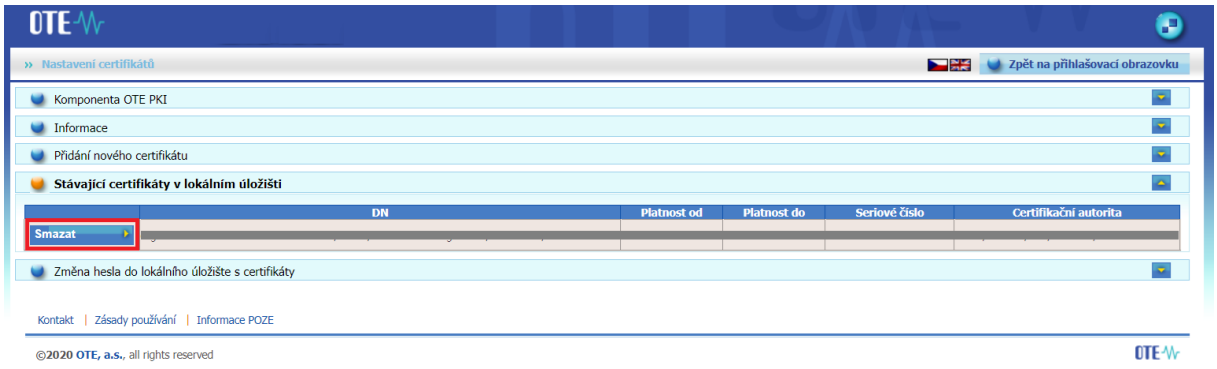
Po úspěšném přidání se certifikát zobrací v záložce Stávající certifikáty v lokálním úložišti.



Certifikáty s privátní klíčem jsou importovány pouze na lokální stanici do Vašeho uživatelského profilu do tzv. webového úložiště prohlížeče, které je určené jen pro konkrétní webovou aplikaci. Import provedený na adrese https://portal.ote-cr.cz není dostupný pro adresu jinou. Samozřejmě je chráněno heslem stejně jako samotný soubor p12/pfx.

3.4 Smazání certifikátu z lokálního úložiště

V záložce Stávající certifikáty v lokálním úložišti klikněte na tlačítko Smazat:

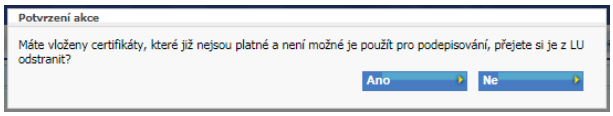


Vymazání je třeba potvrdit OK a v případě kladného provedení již certifikát nefiguruje v záložce *Stávající certifikáty v lokálním úložišti*.

3.5 Odstranění expirovaných certifikátů z lokálního úložiště

Klikem na

na přihlašovací stránce do CS OTE se spustí automatická detekce vyexpirovaných certifikátů. V případě, že v lokálním úložišti se nějaký expirovaný nachází, zobrazí se dialogové okno:

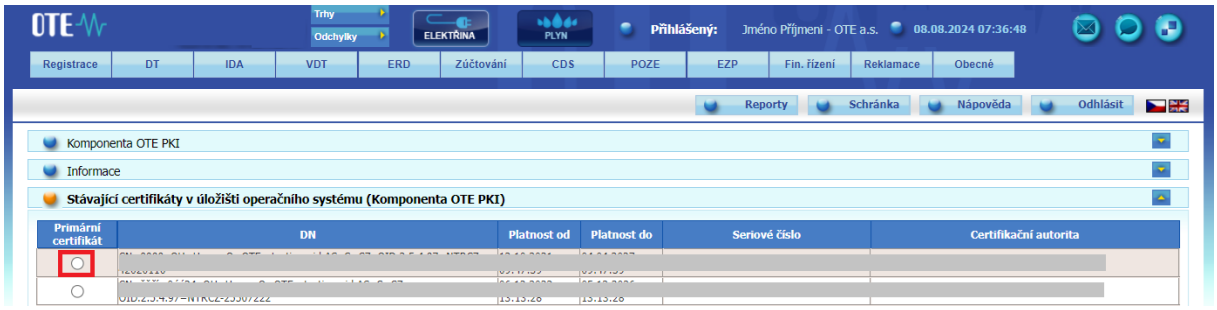


Klikem na „Ano“ můžeme rovnou neplatné certifikáty z lokálního úložiště smazat. Volbou „Ne“ nenastane v lokálním úložišti žádná změna.

Obsah lokálního úložiště je následně normálně zobrazen.

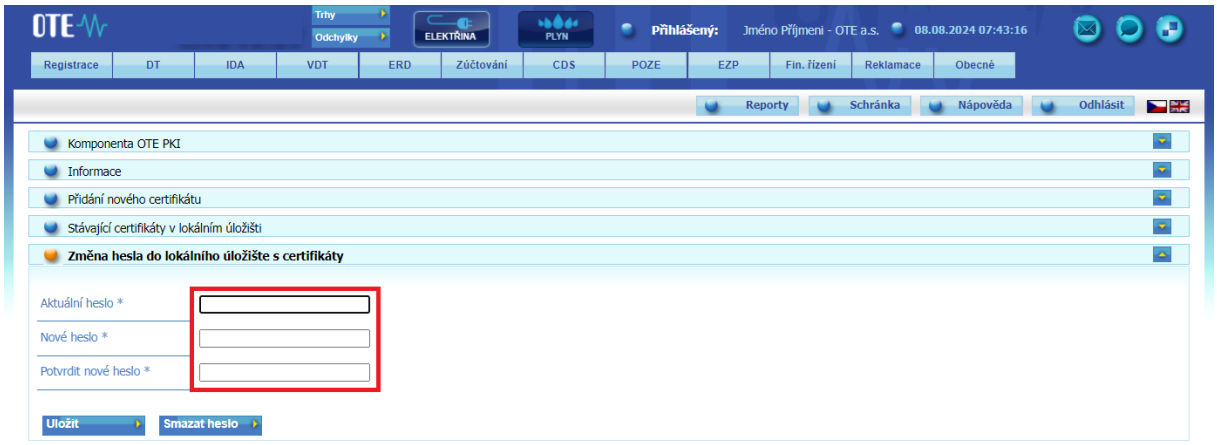
3.6 Výběr primárního certifikátu

Pokud máte v lokálním úložišti více jak 1 certifikát, můžete si zvolit primární certifikát. Tento certifikát pak bude použit jako výchozí pro podepsání dat, když v lokálním úložišti nebude zatrhnuto pole Zobrazit výběr certifikátu při podpisu.



3.7 Změna hesla pro přístup do lokálního úložiště

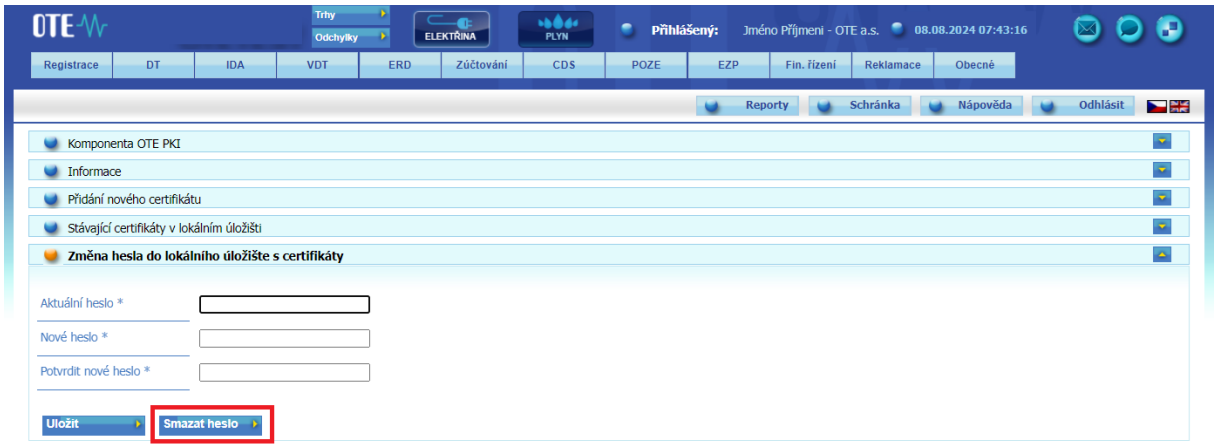
V záložce Změna hesla do lokálního úložiště s certifikáty zadejte Vaše Aktuální heslo, Nové heslo a nové heslo potvďte jeho znovu zadáním. Klikněte na tlačítko Uložit. Proběhne-li změna hesla úspěšně, zobrazí se hláška Heslo bylo úspěšně změněno.



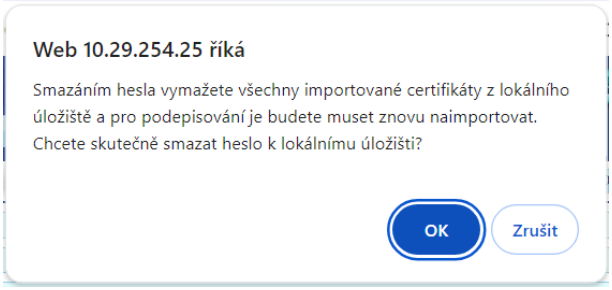
3.8 Zapomenuté heslo pro přístup do lokálního úložiště

Klikněte na Registrace. V menu vyberte Správa certifikátů, v podmenu potom Nastavení lokálního úložiště certifikátů.

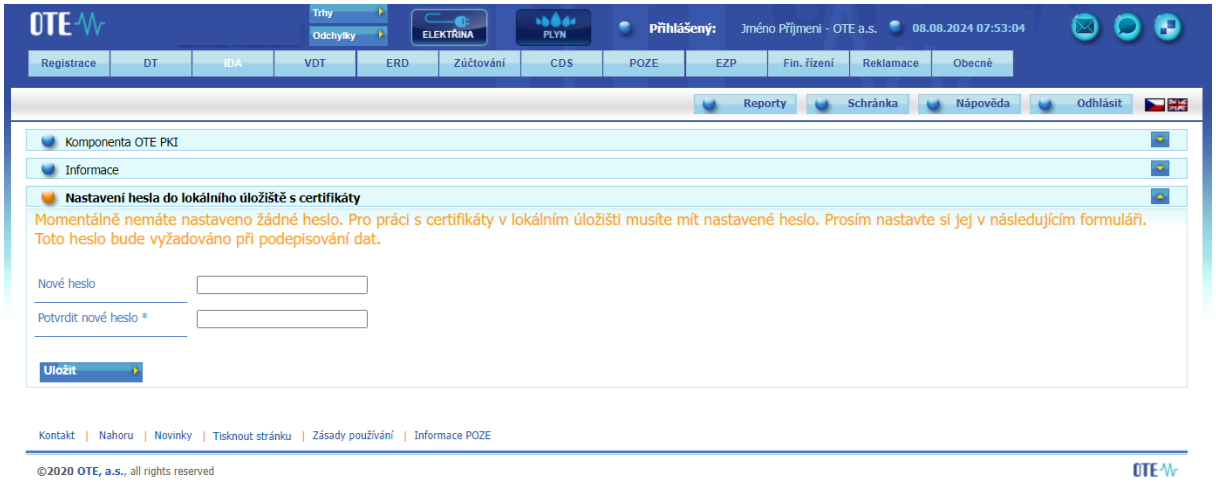
V záložce *Změna hesla do lokálního úložiště s certifikáty* klikněte na tlačítko Smazat heslo. **Smazáním hesla smažete všechny importované certifikáty!**



V zobrazeném dialogovém okně budete vyzváni k potvrzení smazání - OK.



Následně budete přesměrováni na obrazovku, kde si zvolíte Vaše nové heslo pro přístup do lokálního úložiště. Zadáte nové heslo, které potvrdíte jeho znovuzadáním a kliknete na tlačítko Uložit. Po kliknutí na tlačítko Uložit budete přesměrování do lokálního úložiště.


Trhy
Odchylky
ELEKTŘINA
PLYN
Přihlášený:
Jméno Příjmení - OTE a.s.
08.08.2024 07:53:04
Registrace
DT
iDA
VDT
ERD
Zúčtování
CDS
POZE
EZP
Fin. řízení
Reklamace
Obecné
Reporty
Schránka
Nápověda
Odhlásit
Komponenta OTE PKI
Informace
Nastavení hesla do lokálního úložiště s certifikáty
Momentálně nemáte nastaveno žádné heslo. Pro práci s certifikáty v lokálním úložišti musíte mít nastavené heslo. Prosím nastavte si jej v následujícím formuláři.
Toto heslo bude vyžadováno při podepisování dat.
Nové heslo
Potvrdit nové heslo *
Uložit
Kontakt | Nahoru | Novinky | Tisknout stránku | Zásady používání | Informace POZE
©2020 OTE, a.s., all rights reserved

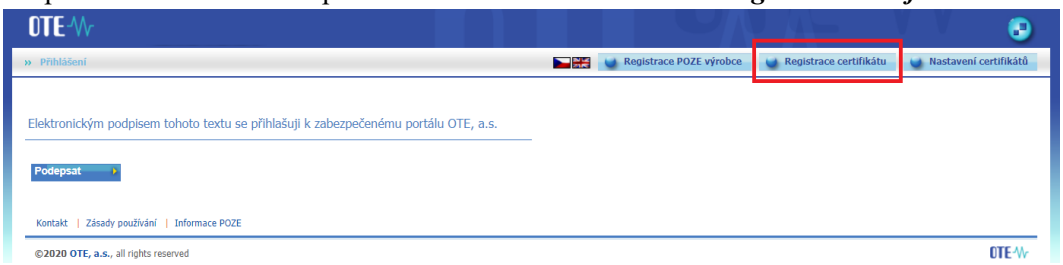
4 Registrace certifikátu po expiraci

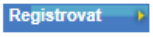
4.1 Přístup na portál CS OTE po vypršení platnosti certifikátu s IČ

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 certifikátu (s 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

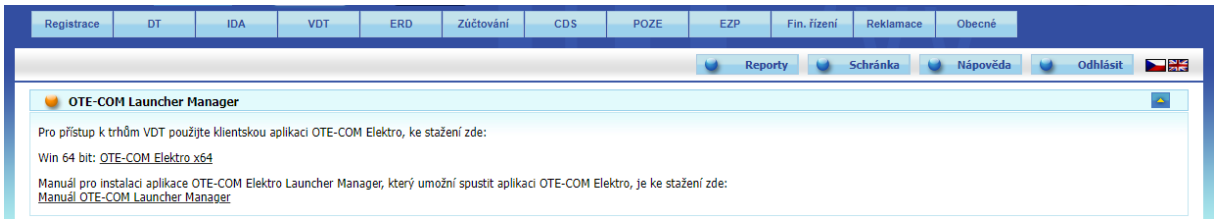
Přístup do produkčního prostředí aplikace OTE-COM je možný dvěma následujícími způsoby:

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

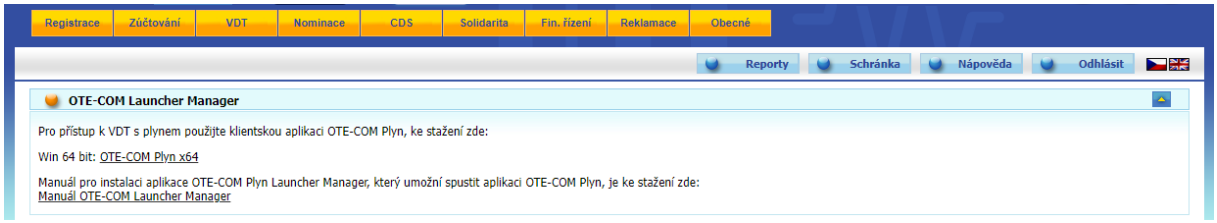
5.1 Přístup přes aplikaci OTE-COM

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.

OTE-COM elektro x64 je možno stáhnout v sekci VDT pod OTE-COM Launcher Manager:



OTE-COM plyn x64 je možno stáhnout v sekci VDT pod OTE-COM Launcher Manager



- 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 – A-elektřina, B-plyn. Šablony zpráv pro OTE-COM aplikaci jsou dostupné zde A-elektřina, B-plyn. 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.