

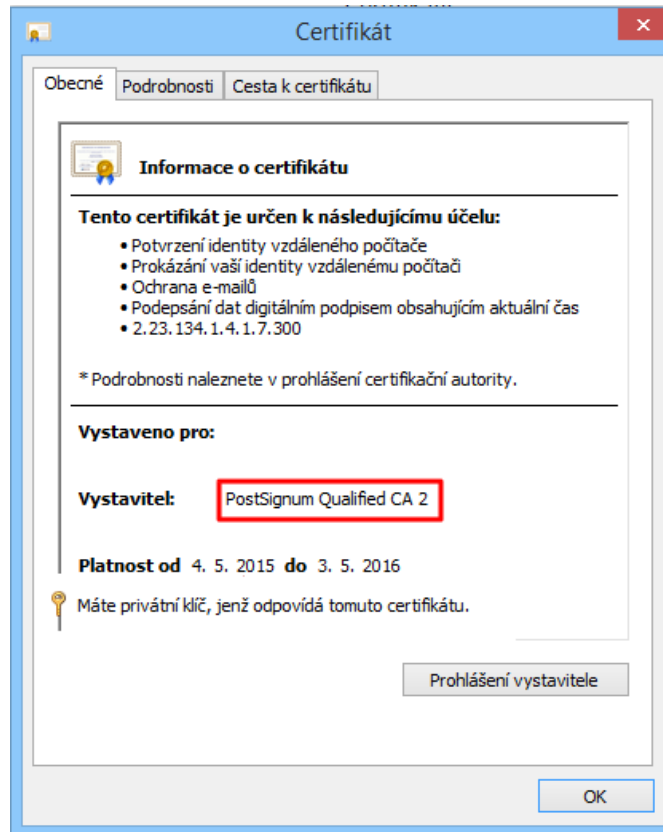


# Předcházení problémů s certifikátem pro podpis v aplikaci MS 2014+

26.5.2018 Verze 4

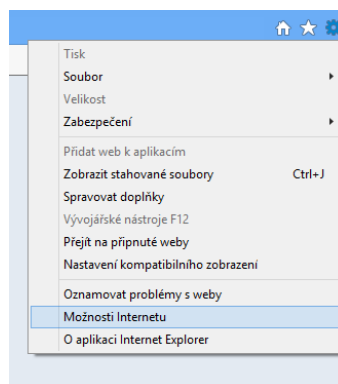


2. Je použitý certifikát kvalifikovaný, vydaný některou z podporovaných CA (Postsignum, I.CA, eidentity)? Jak zjistím platnost certifikátu?

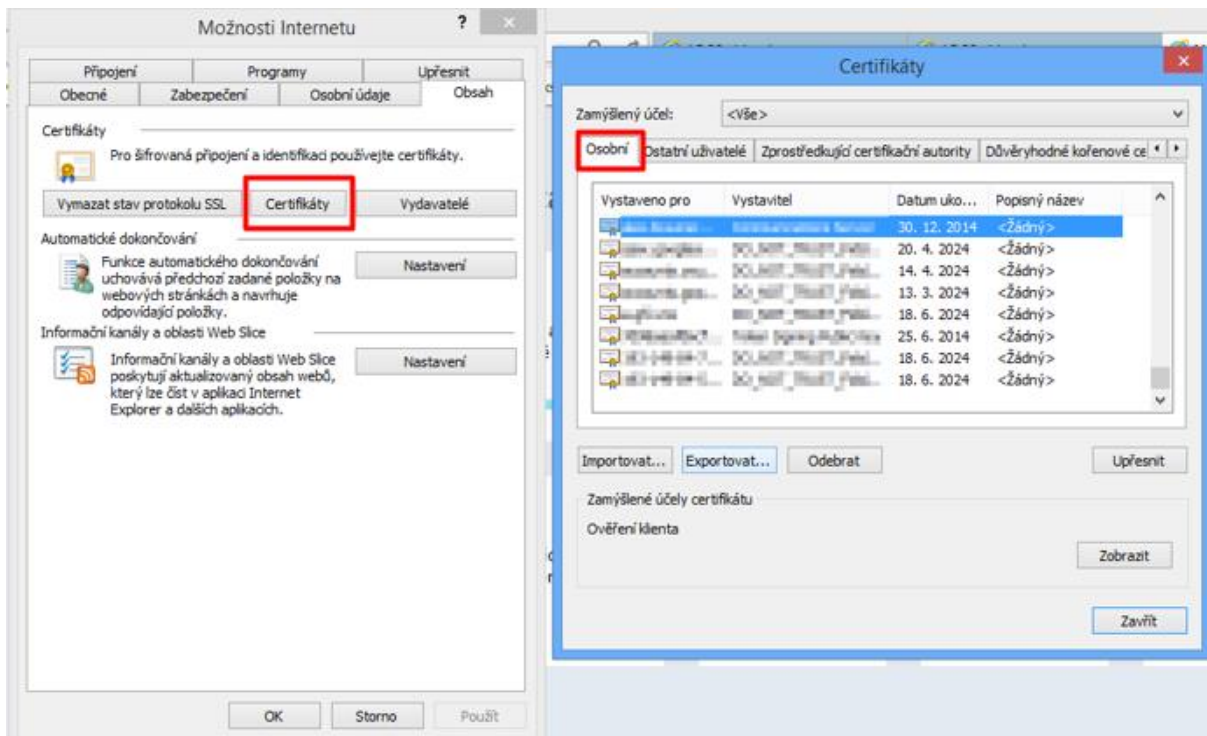


**Podrobnosti o Vašem certifikátu zjistíte následujícím způsobem:**

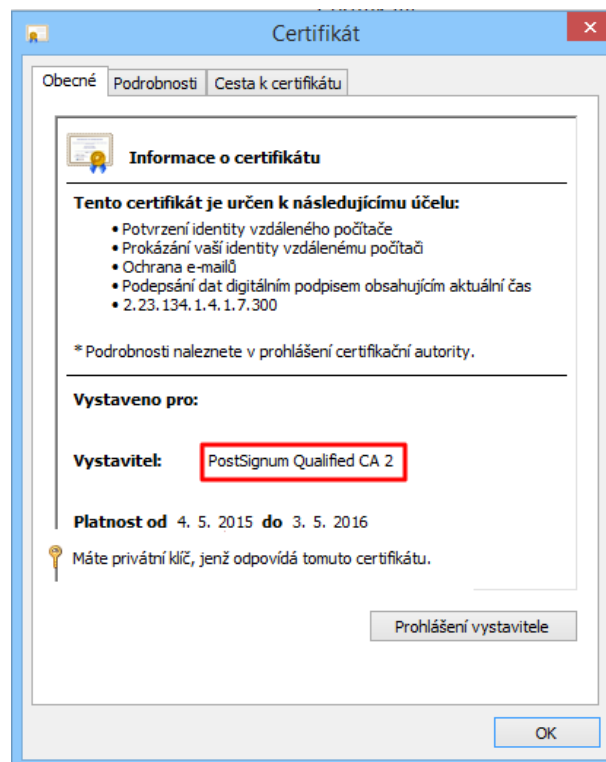
- a) V prohlížeči (Internet Explorer) otevřete nabídku pro nastavení (ozubené kolečko v pravém horním rohu) a v ní vyberte „Možnosti internetu“



- b) Na záložce „Obsah“ klikněte na tlačítko „Certifikáty“. Otevře se seznam certifikátů. Typicky se bude nacházet na první záložce „Osobní“.

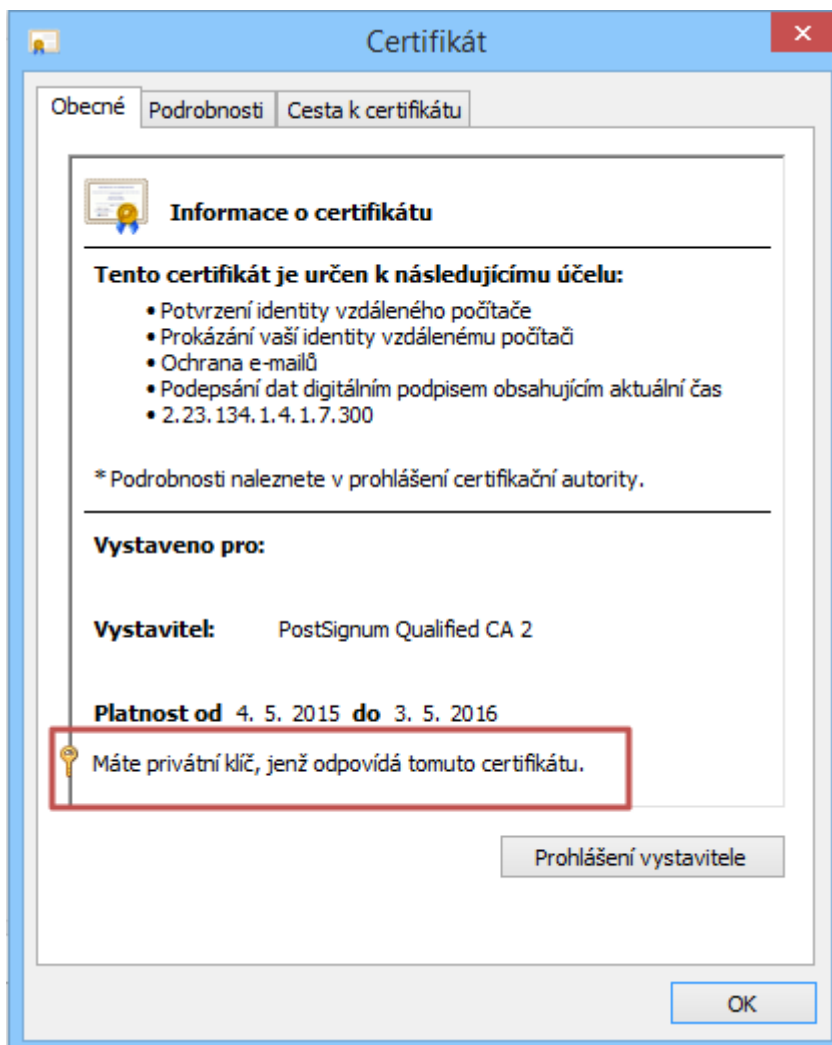


- c) Dvojitým kliknutím myši na daný certifikát se zobrazí detail certifikátu. V detailu je informace o vystaviteli certifikátu a platnosti.



### 3. Obsahuje certifikát privátní klíč?

Postup jak zjistit, zda certifikát obsahuje privátní klíč je popsán v předchozím bodu.



#### 4. Pokud jde o certifikát na čipové kartě/usb tokenu, je zaregistrován v systémovém úložišti?

Systém MS 2014+ má z technologických důvodů ve výchozím stavu dostupnou pouze možnost pro práci s certifikáty a privátními klíči, jenž jsou uloženy v souboru v rámci souborového úložiště. Vložení souboru vyžaduje zadání příslušného hesla, kterým je chráněn privátní klíč. V případě použití privátního klíče uloženého v souboru, pracuje MS 2014+ s tímto klíčem pouze a výhradně v paměti prohlížeče spuštěného na Vašem zařízení, kde je prováděno vytváření elektronických podpisů. Soukromý klíč není nikdy a za žádných okolností odeslán na server.

V případě, že obslužný SW neprovádí zaregistrování v úložišti automaticky, proveďte jej ručně. Příklad je ukázán na čipové kartě s obslužným programem „CryptoPlus CM“ na Windows 8.1. V případě klíče na virtuální čipové kartě je zaregistrování provedeno automaticky.

1. Otevřete Vás obslužný program k tokenu.
2. Vyhledejte v něm příslušný klíč.

3. Pokud je certifikát nezaregistrovaný, program nabízí jeho zaregistrování. Klikněte na registraci. Nyní se klíč objevil v systémovém úložišti, složce osobní.

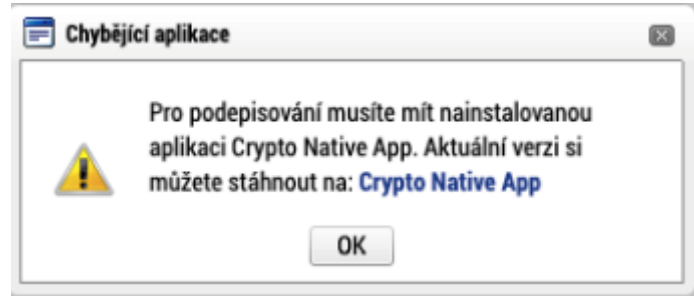
Pokud se Vám i přes výše uvedené nastavení stále nedaří vytvořit podpis Vaším certifikátem, pak nám zašlete:

- Vaše uživatelské jméno
- Datum a čas, kdy byl problém detekován

- O jaký typ certifikátu se jedná – název a vydavatel, např.: *ACAeID2.1 - Qualified Issuing Certificate (kvalifikovaný systémový certifikát vydávající CA)*
- Detailní popis jakým způsobem uživatel postupoval při podepisování, jak se chovala aplikace, zda došlo k nějaké chybě. Popis problému je velmi vhodné doplnit o screenshot.

**5. Pokud systém hlásí, že Crypto Native App (CNA) není nainstalován nebo přestal fungovat po aktualizaci a nemáte administrátorská oprávnění**

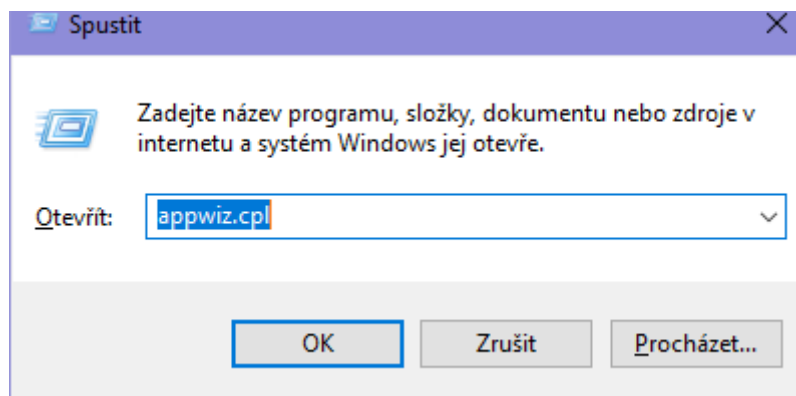
- Při podpisu vyskočí následující hláška



Nejčastější příčina je, že umístění aplikace není dostupné s nastaveným oprávněním uživatelského účtu. Řešením je změnit cestu instalace do uživatelské složky.

- Odinstalace již existující instalace CNA:

Zmáčknou klávesy WINDOWS + R zároveň na klávesnici. Vyskočí malé okno vlevo dole. Do okna napište **appwiz.cpl**



Otevře se vám nové okno (Programy a funkce), zde najít CNA. Pravý klik na CNA a kliknout na možnost odinstalovat.

	Crypto Native App verze 15.03.7158	TescoSW a.s.	17.10.2019	13,4 MB	15.0
	Crypto Web Extension for IE version 15.01.7046	TescoSW a.s.	26.04.2019	2,53 MB	15.0

- Nová instalace CNA:

Znovu stáhnout instalační soubory z adresy <https://download.tescosw.cz/crypto/?lang=cs> a spustit instalátor. Třetí krok, zvolení cesty. Kde přes procházet se ručně napíše, nebo nakliká cesta do uživatelské složky. Cesta bude vypadat následovně.

„C:\Users\VAŠE UŽIVATELSKÉ JMÉNO\Crypto Native App“

Dokončit instalaci a zkusit podepsat.