



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

Verze 2.0.



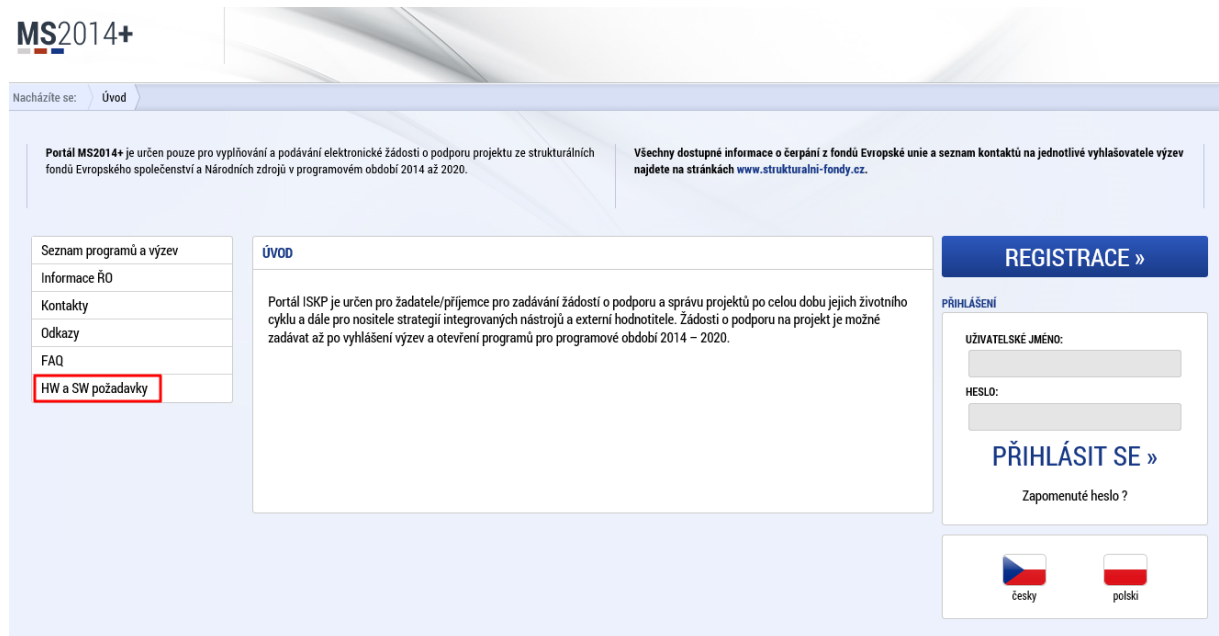
## 1. Má aplikace zvýšená oprávnění?

Aplikace dodávané společností Tesco SW a. s. využívají technologie Microsoft Silverlight, jenž pro některé pokročilé funkcionality vyžaduje nastavit tzv. zvýšená oprávnění na počítači. Těmito funkcionalitami jsou např. přístup k podpisovým certifikátům v úložišti certifikátů Windows nebo na čipové kartě. Zvýšená oprávnění lze nastavit pomocí instalačního balíčku **TescoSW Elevated Trust Tool**. Balíček si můžete stáhnout pod tímto odkazem:

<https://mseu.mssf.cz/help/TescoSwElevatedTrustToolCZ.msi>

**Upozornění:** Pro úspěšnou instalaci může být vyžadováno administrátorské oprávnění.

Další HW a SW požadavky naleznete pod odkazem: <https://mseu.mssf.cz/> pod záložkou HW a SW požadavky.



The screenshot shows the MS2014+ portal interface. At the top left, there is a navigation menu with the following items: "Seznam programů a výzev", "Informace ŘO", "Kontakty", "Odkazy", "FAQ", and "HW a SW požadavky" (highlighted with a red box). The main content area is titled "ÚVOD" and contains the following text: "Portál ISKP je určen pro žadatele/příjemce pro zadávání žádostí o podporu a správu projektů po celou dobu jejich životního cyklu a dále pro nositele strategií integrovaných nástrojů a externí hodnotitele. Žadosti o podporu na projekt je možné zadávat až po vyhlášení výzev a otevření programů pro programové období 2014 – 2020." To the right of the main content, there is a "REGISTRACE »" button and a "PŘIHLÁŠENÍ" section with input fields for "UŽIVATELSKÉ JMÉNO:" and "HESLO:", a "PŘIHLÁŠIT SE »" button, and a "Zapomenuté heslo ?" link. At the bottom right, there are language selection buttons for "česky" and "polski".

## 2. Je adresa (stránka) <https://mseu.mssf.cz> zařazena mezi důvěryhodné weby?

Možnosti Internetu

Připojení: Obecné

Programy: Zabezpečení (2.), Osobní údaje, Upřesnit

Upřesnit: Obsah

Vyberte zónu k zobrazení nebo změně nastavení zabezpečení.

Internet, Místní intranet, Důvěryhodné weby (3.), Servery s omezen...

**Důvěryhodné weby**

Tato zóna obsahuje weby, kterým důvěřujete, že nepoškodí váš počítač ani soubory. V této zóně jsou 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

6. OK Storno Použít

Důvěryhodné weby

Do této zóny můžete přidávat weby a odebrat je z ní. Všechny weby v této zóně budou používat nastavení zabezpečení této zóny.

Přidat tento web k zóně:

https://mseu.mssf.cz 4. 5. Přidat

Weby:

http://sccm11.iis.loc Odebrat

Požadovat ověření všech webů v této zóně serverem (https:)

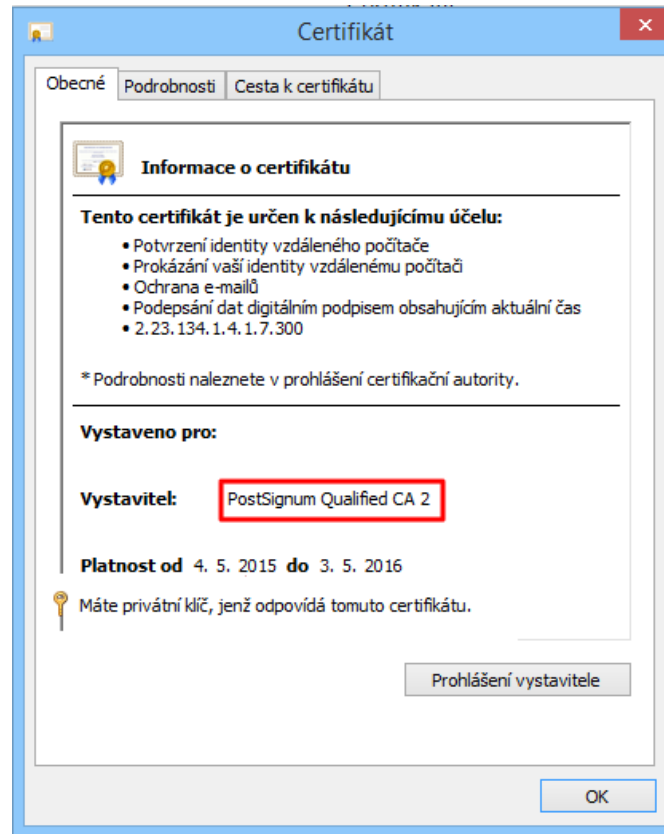
6. Zavřít

1. V Internetu Explorer kliknout na nástroje
2. Vybrat záložku Zabezpečení a položku Důvěryhodné weby
3. Kliknout na tlačítko Weby
4. Do pole pro přidání webu vložit url odkaz ISKP 2014+
5. Kliknout na tlačítko Přidat
6. Kliknout na tlačítko Zavřít a v Možnostech Internetu potvrdit tlačítkem OK



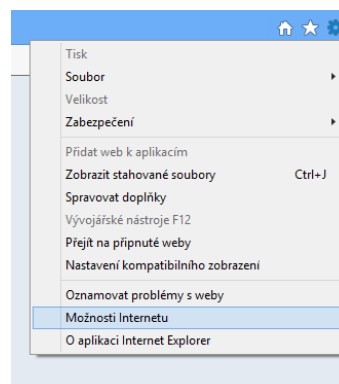
tů OPTP:

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

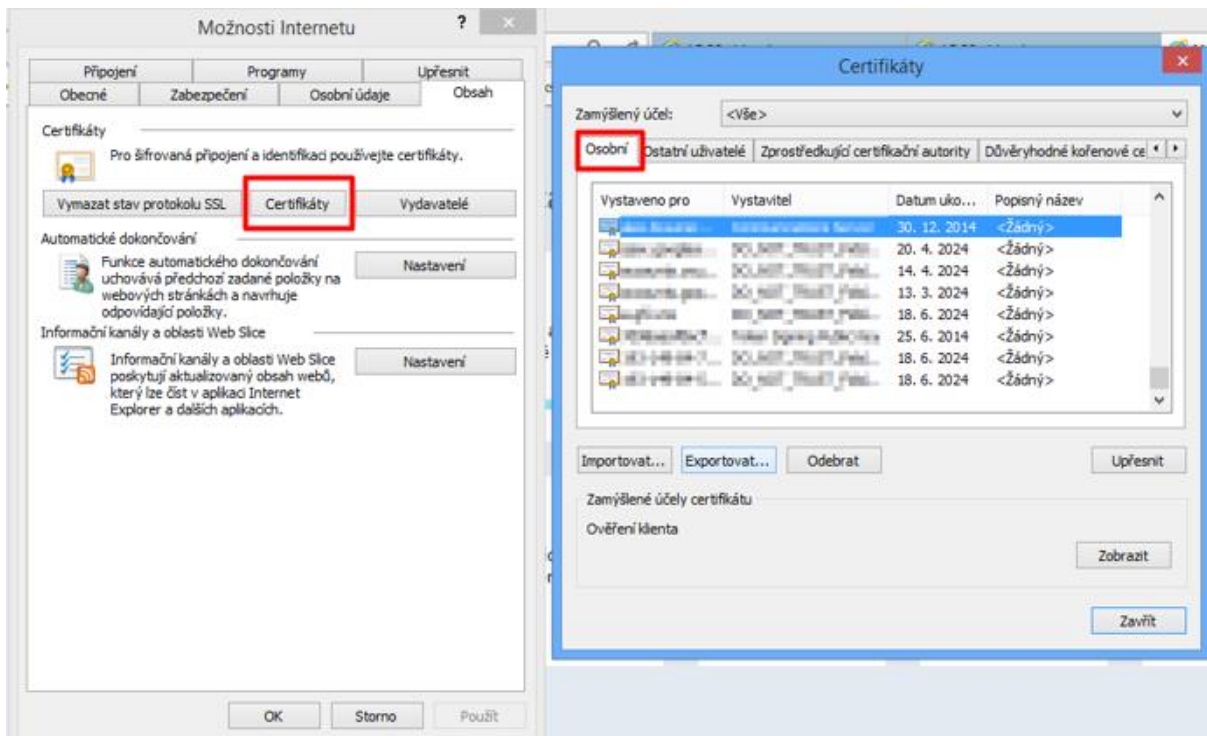


**Podrobnosti o Vašem certifikátu zjistíte následujícím způsobem:**

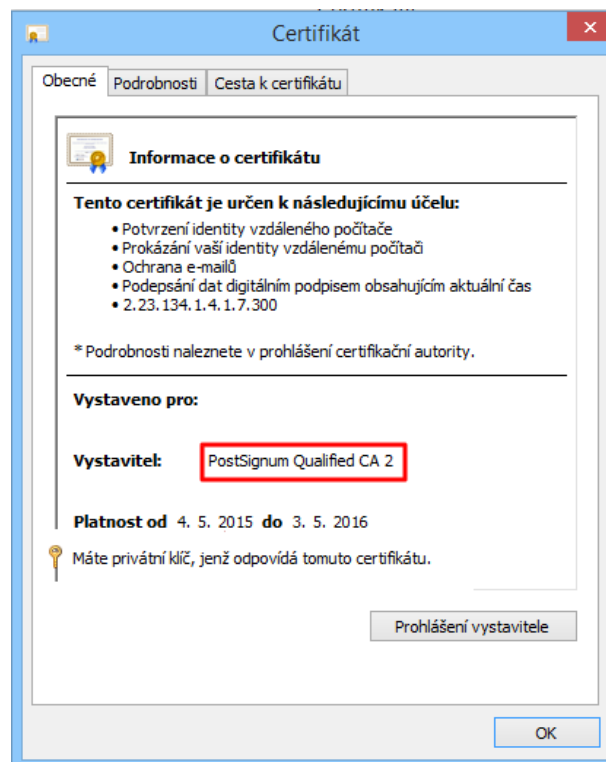
- a) V prohlížeči (Internet Explorer) otevřete nabídku pro nastavení (ozubené kolečko v pravém horním rohu) a v ní vyberte „Možnosti internetu“



- 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.



#### 4. Obsahuje certifikát privátní klíč?

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

**Informace o certifikátu**

**Tento certifikát je určen k následujícímu účelu:**

- Potvrzení identity vzdáleného počítače
- Prokázání vaší identity vzdálenému počítači
- Ochrana e-mailů
- Podepsání dat digitálním podpisem obsahujícím aktuální čas
- 2.23.134.1.4.1.7.300

\* Podrobnosti naleznete v prohlášení certifikační autority.

**Vystaveno pro:**

**Vystavitel:** PostSignum Qualified CA 2

**Platnost od 4. 5. 2015 do 3. 5. 2016**

Máte privátní klíč, jenž odpovídá tomuto certifikátu.

Prohlášení vystavitele

OK

## 5. 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.

The screenshot shows the Windows Card Manager application window titled "Card manager". The interface includes a menu bar (File, View, Certificate, Key, Help), a toolbar, and a tree view on the left showing a hierarchy of certificates. The main area displays the details of a selected certificate under the heading "Certificate".

Version:	3
Serial number:	33EE5DF9000000001684
Validity:	11:03, 01.08.2014 - 15:28, 08.09.2015
Issuer:	Microsoft Corporation
Subject:	...
Name for PKCS#11:	<not used>
SHA1:	963F75A9 85E9E068 89D3517F D521424C D6EF4624

Below the certificate details, there is a section titled "Certificate extensions" with a list of usage options:

- Key usage:
- Digital signature
- Key encipherment
- Extended key usage:
- Email protection
- Client authentication
- Smartcard logon

Additional information at the bottom of the window:

- Certification path is successfully verified.
- The certificate is stored on the card.
- The certificate is not registered in the system. Some programs (MS Internet Explorer, MS Outlook etc...) can't use it. Certificate can be [registered](#).
- Certificate can be [exported into a file](#).

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.

## 6. Problém s přístupem do systémového úložiště certifikátů:

V ojedinělých případech je možné - i přes nainstalování balíčku TescoSW Elevated Trust Tool, zajišťujícího zvýšená a oprávnění aplikace a tudíž přístup k systémovému úložišti certifikátů, že není toto úložiště přístupné.

Je možné, že uživatel z bezpečnostních důvodů nemá mezi důvěryhodnými autoritami zařazeny v doméně (na PC, či v lokální síti) některé certifikační autority nezbytné pro bezchybný běh aplikace MS2014+.

Konkrétně se jedná o tyto certifikáty:

- DigiCert Assured ID CA-1, sha1 hash: 19A09B5A36F4DD99727DF783C17A51231A56C117
- DigiCert Assured ID Root CA, sha1 hash:0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43
- DigiCert EV Code Signing CA (SHA2), sha1 hash:60EE3FC53D4BDFD1697AE5BEAE1CAB1C0F3AD4E3
- DigiCert High Assurance EV Root CA, sha1 hash: 5FB7EE0633E259DBAD0C4C9AE6D38F1A61C7DC25

Pokud se tedy objeví problémy s přístupem do systémového úložiště certifikátů, je potřeba zkontrolovat existenci těchto certifikátů mezi důvěryhodnými certifikačními autoritami.