OPERAČNÍ PROGRAM TECHNICKÁ POMOC

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

Principy práce s certifikáty v aplikaci MS 2014+

NÁRODNÍ ORGÁN PRO KOORDINACI

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Obsah

1 Úvod

Tento dokument popisuje možnosti použití soukromých klíčů a veřejných klíčů s certifikátem v systému MS 2014+ včetně popisu existujících omezení. Systém MS 2014+ využívá pro zabezpečení dat uživatelů i pro zajištění dokumentů z hlediska nepopiratelnosti dat v rámci systému asymetrické kryptografické funkce na bázi RSA.

Doplňkem k této příručce jsou ukázky postupů s práci s certifikáty a klíči.

2 Podporované certifikáty

V rámci systému jsou využívány typy certifikátů uvedené v následující tabulce.

ID	Význam	Použití	Využívá
C1	**Kvalifikovaný certifikát** vydaný akreditovaným poskytovatelem certifikačních služeb dle zákona č. 227/2000 Sb., o elektronickém podpisu, v platném znění. Certifikát si zajišťují a obnovují všichni uživatelé MS 2014+ na vlastní náklady u akreditovaného poskytovatele.	**Podepisování souborů a objektů**	**Uživatelé MS 2014+**

Tabulka 1 – Podporované certifikáty

3 Podporované způsoby uložení privátních klíčů a certifikátů

Systém MS 2014+ podporuje práci s privátními klíči, které mohou být uloženy následujícími způsoby:

- token (USB token, čipová karta, virtuální čipová karta, …)
- systémové úložiště Windows
- souborové úložiště počítače

Z hlediska zajištění maximální možné bezpečnosti je doporučováno zvolit pro uložení privátního klíče tokeny (USB tokeny, čipové karty). Dále je možné využít pro uložení soukromého klíče systémové úložiště Windows nebo virtuální čipovou kartu. Nejméně bezpečnou variantou uložení soukromého klíče je jeho uložení do souboru. Doporučuje se generovat klíče přímo v cílovém úložišti bez dodatečného importu.
Volba vhodného úložiště je volbou uživatele, resp. jeho organizace.

Níže uvedená tabulka shrnuje základní vlastnosti jednotlivých způsobů uložení privátního a veřejného klíče v návaznosti na vytvoření elektronického podpisu, šifrování a dešifrování dat.

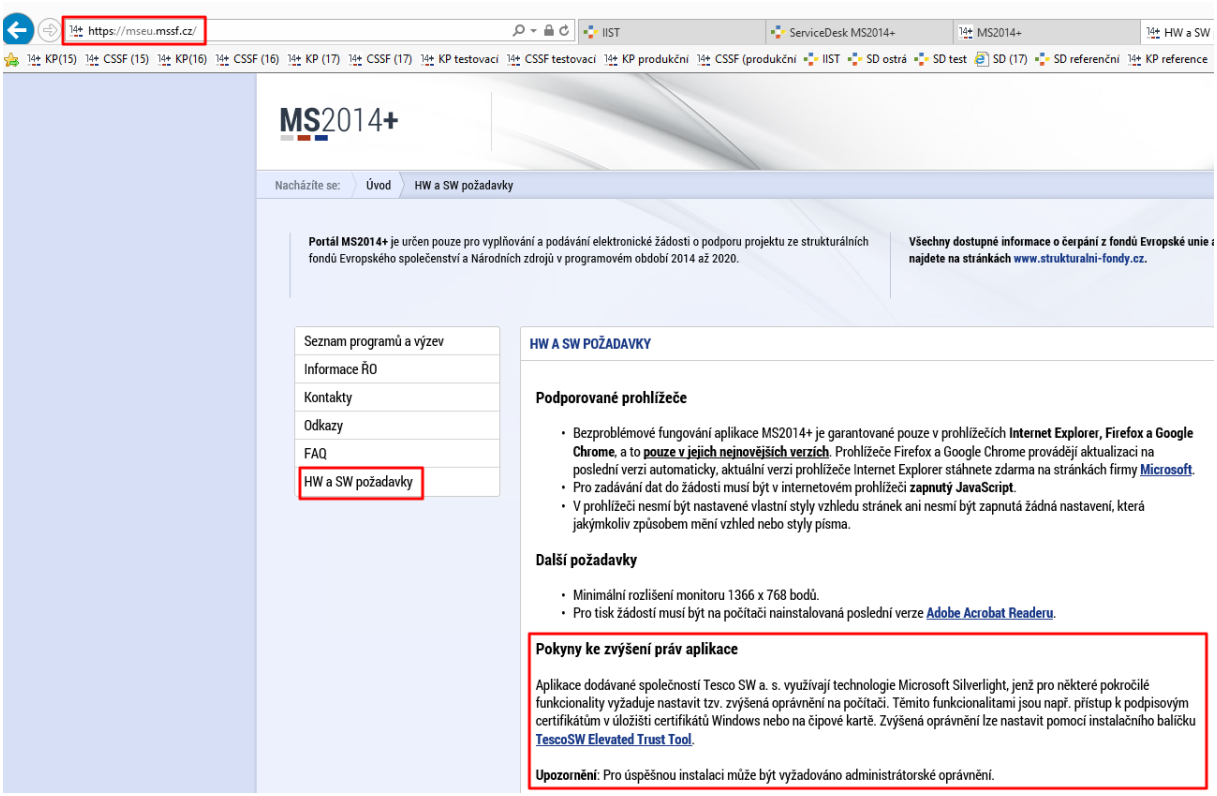
Varianta	Token	Systémové úložiště	Souborové úložiště
Místo uložení privátního klíče	USB token, čipová karta, virtuální čipová karta …	Systémové úložiště Windows	Soubor na diskovém úložišti
Princip	Privátní klíč a certifikát jsou uloženy na Vašem HW zařízení a nelze je přímo získat V případě virtuální čipové karty je soukromý klíč a certifikát uložen na Vašem počítači.	Privátní klíč je uložen do systémového úložiště Windows	Privátní klíč je uložen v souboru na disku vašeho počítače
Lze použít v MS 2014+ pro	Podepisování	Podepisování	Podepisování

Tabulka 2 – Základní vlastnosti jednotlivých způsobů uložení privátního klíče

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 odesílán na server.

Pro zpřístupnění ostatních způsobů je potřeba nastavit zvýšená oprávnění pro MS 2014+ dle návodu, který je uveden na následující URL adrese pod záložkou HW a SW požadavky

https://mseu.mssf.cz/



3.1 Privátní klíč uložen na tokenu

Uložení privátních klíčů na tokenech je všeobecně považováno za bezpečné. Privátní klíč není v tomto případě předáván do aplikace, neopouští token. Na těchto zařízeních mohou být rovněž uloženy i certifikáty s veřejným klíčem, nicméně tato skutečnost nemá žádný vliv na výslednou bezpečnost, jelikož certifikáty s veřejným klíčem představují veřejně dostupnou informaci.

Mezi tokeny se řadí:

- USB token
- čipová karta
- virtuální čipová karta

Při přístupu ke klíčům uloženým v tokenu je potřeba zadat PIN, který představuje další úroveň zabezpečení.

Pro využití tokenů ve spojitosti s aplikací MS 2014+ je potřeba provést následující úkony:

- Správně nainstalovat a zprovoznit token
- Nastavit zvýšená oprávnění pro aplikaci MS 2014+ a Silverlight
- Registrovat privátní klíč a certifikát s veřejným klíčem do systémového úložiště certifikátů[1]

Registrace privátního klíče a certifikátu s veřejným klíčem do systémového úložiště může být, v závislosti na použitém software a ovladačích dodávaných zpravidla s vaším tokenem, provedena automaticky. Pokud k automatickému zaregistrování nedojde, pak postupujte dle návodu *Jak zpřístupnit klíč uložený v tokenu v systémovém úložišti.* Pokud není registrace klíčů provedena, pak není možné pracovat se soukromým klíčem, který je uložen na tokenu.

[1] Možnost přístupu k soukromému klíči a certifikátu s veřejným klíčem bez nutnosti jejich registrace do systémového úložiště certifikátů není aktuálně dostupná

Tokeny je možné použít při samotném postupu získávání páru privátního a veřejného klíče a odpovídajícího certifikátu od certifikační autority. Postup je popsán v *Jak získat a nastavit token*.

3.1.1 USB tokeny a čipové karty

Ukázka postupu pro získání USB tokenu nebo čipové karty je popsána v *Jak získat a nastavit token* na příkladu získání USB tokenu „Bezpečný klíč“ od certifikační autority PostSignum.

První certifikační autorita poskytuje obdobnou službu pro zakoupení tokenu (http://www.ica.cz/Objednavka-Hardware). Certifikační autorita eIdentity takovouto službu v této chvíli neposkytuje.

Součástí dodávaného SW k tokenu „Bezpečný klíč“ je i možnost generování klíčů pro získání certifikátu od PostSignum přímo na samotném tokenu. Postup je popsán v *Jak získat pár privátního a veřejného klíče*.

Každý správně nainstalovaný token je možné obecně použít v rámci procesu získání páru privátního a veřejného klíče u každé podporované certifikační autority.

Všechny USB tokeny nebo čipové karty umožňují defaultně import soukromých klíčů do tokenu

Jak naimportovat klíč do tokenu. Nutnou prerekvizitou je získání privátního klíče a jeho uložení jako souboru na počítači. Privátní klíč je standardně, v rámci generování klíčového páru a žádosti o vystavení certifikátu určené pro certifikační autoritu, ukládán v systémovém úložišti. Privátní klíč je poté nutné vyexportovat.

Pokud máte již certifikát uložen v souboru a chcete jej naimportovat do tokenu, postupujte podle

Jak naimportovat klíč do tokenu.

3.1.2 Virtuální čipové karty

V nejnovějších operačních systémech Microsoft Windows je dostupná funkce **virtuální čipové karty**. V principu se jedná o zabezpečené uložení privátního klíče bez nutnosti vlastnictví USB tokenu nebo čipové karty. Tato možnost je dostupná od Windows 8 a rozšířena ve Windows 8.1. Virtuální čipové karty jsou realizovány prostřednictvím TPM, který umí do jisté míry totéž, co kryptografický procesor čipové karty.

TPM je HW komponenta, která slouží (mimo jiné) k bezpečné úschově kryptografických informací, zejména soukromých klíčů. V současné době je možné TPM nalézt ve stále se zvětšujícím počtu koncových zařízení (PC, notebook, tablet). S příchodem Windows 8.1 je nově podporována i firmware-based TPM komponenta, která již nemusí být samostatnou HW součástkou, ale může být obsažena v integrovaných obvodech procesoru.

Nevýhodou virtuálních čipových karet je uložení kontejneru se soukromým klíčem na daném zařízení bez možnosti jeho exportu. Při reinstalaci Windows nebo nutnosti použití jiného zařízení tedy není možné soukromý klíč přenést, jelikož je zabezpečen klíči uloženými v TPM čipu na daném zařízení.

Pro virtuální čipovou kartu platí stejné postupy jako pro ostatní čipové karty.

3.2 Privátní klíč uložen v systémovém úložišti Windows

Uložení privátních klíčů v systémovém úložišti Windows nelze považovat za bezpečný způsob uložení. Při infiltraci počítače malwarem nebo při přímém přístupu osoby existuje riziko zcizení klíčů zde uložených. Existují techniky, jak získat klíče uložené v systémovém úložišti, které byly označeny jako neexportovatelné.

Pokud přesto budete tuto variantu využívat, pak doporučujeme nastavit heslo, jež bude vyžadováno při každém přístupu ke klíčům, a nastavit příznak neexportovatelnosti privátních klíčů v rámci procesu importu. Neexportovatelnost nenastavujte, pokud budete privátní klíč potřebovat naimportovat do tokenu a máte jej uložen v systémovém úložišti. Postup exportu je popsán v *Jak exportovat privátní klíč do souboru*.

Veškeré operace s privátními klíči jsou prováděny na Vašem zařízení a systém získává pouze výsledek.

Postup pro získání páru privátního a veřejného klíče, které budou uloženy v systémovém úložišti Windows, je popsán v *Jak získat pár privátního a veřejného klíče*.

3.3 Privátní klíč uložen v souboru

Dalším podporovaným způsobem práce s privátními klíči je uložení klíče v souboru na souborovém úložišti. Tento způsob má značná bezpečnostní rizika. V aplikaci je podporován jako možnost „poslední záchrany“, pokud není možné využít žádný jiný způsob.

Hlavní nevýhodou je stav, kdy je privátní klíč uložen v souboru na zařízení uživatele, čímž je tedy lehce získatelný při infiltraci zařízení malwarem nebo fyzicky osobou. Při použití je potřeba PIN, ale i toto neposkytuje dostatečnou ochranu.

Při použití se soubor s privátním klíčem „nahrává“ do systému MS 2014+. V rámci systému MS 2014+ je i při tomto použití dbáno na bezpečnost a proto je zajištěno, že se privátní klíč fyzicky nenahrává až na servery, kde běží samotný systém. Technologicky se při první návštěvě systému MS 2014+ stáhne do paměti prohlížeče tzv. klientská část. Jednou z jejích funkcí je i provádění samotných kryptografických operací. Privátní klíč tedy fyzicky neopouští zařízení uživatele.

Postup pro získání privátního klíče uloženého v souboru závisí na zdroji, kde je privátní klíč uložen.

Pokud máte privátní klíč uložen v systémovém úložišti, musíte jej vyexportovat. Podmínkou je nastavení příznaku exportovatelnosti. Postup exportu je popsán v *Jak exportovat privátní klíč do souboru*.

Pokud máte privátní klíč uložen na tokenu, není možné jej vyexportovat do souboru.

3.4 Podporovaná zařízení

Systém MS 2014+ umí pracovat se všemi klíči na tokenech, které jsou zaregistrovány v systémovém úložišti. Jedná se o stejný princip, jaký využívá například Microsoft Outlook.

4 Použití certifikátů v systému

4.1 Ukázka podpisu

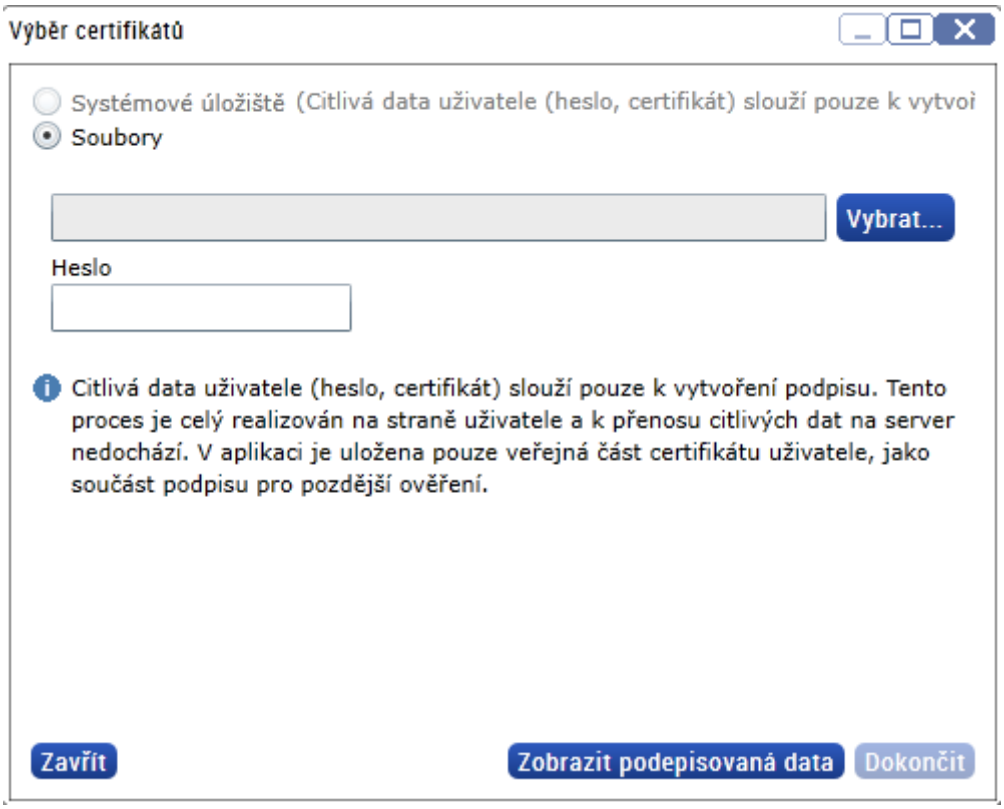
Podpis je možné v aplikaci použít v těchto situacích:

- Podpis souboru
- Podpis objektu

Každá operace je rozdílná a je inicializována rozdílným způsobem.

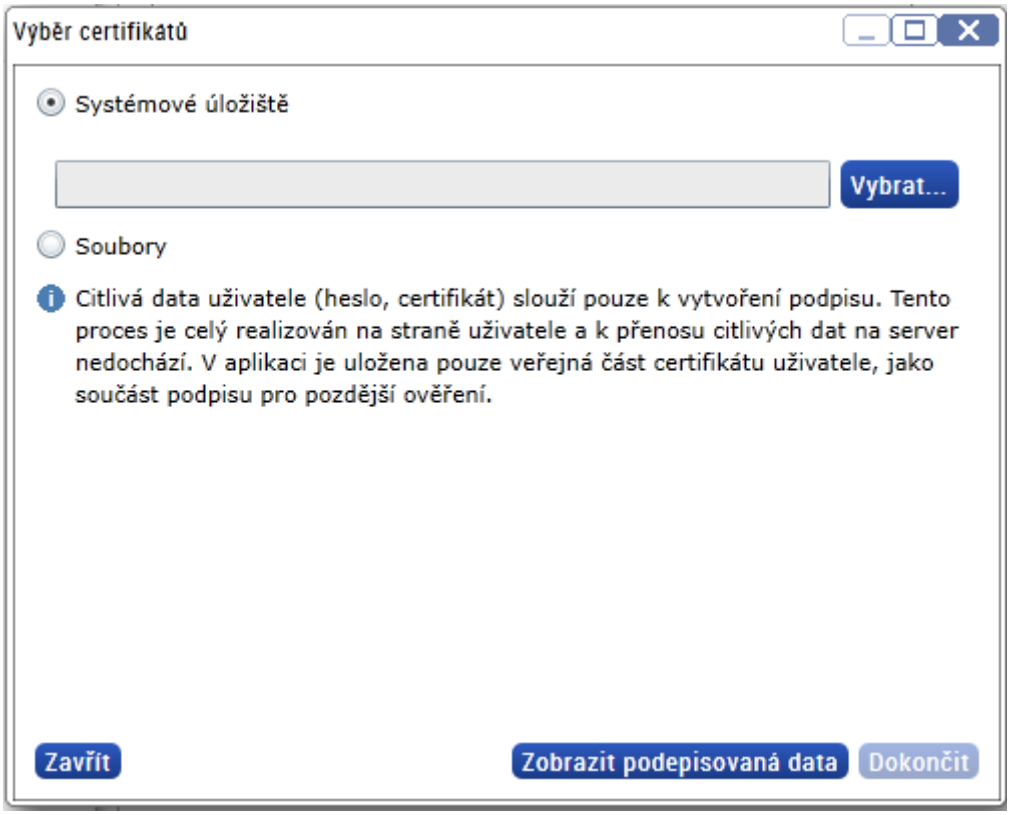
Samotné vytvoření podpisu je ale pro všechny varianty stejné a je vyobrazeno v této kapitole.

Pokud při použití podpisu nevidíte tlačítko „Úložiště“ a máte tedy možnost použít pouze soukromé klíče uložené v souboru, je potřeba provést postup podle návodu na formuláři HW a SW požadavky, ke kterému vede tento odkaz. Důrazně doporučujeme toto nastavení provést.



Obrázek 1 – Výběr certifikátu – bez zvýšených oprávnění

Po provedení potřebných úprav je již viditelné tlačítko „Úložiště“ a nyní máte možnost použít všechny podporované způsoby uložení klíčů.



Obrázek 2 – Výběr certifikátu – zvýšená oprávnění

Další ukázky již budou zachycovat situaci, kdy bylo úložiště systému MS 2014+ zpřístupněno. Je použit operační systém Microsoft Windows 8.1.

Celý postup podepsání se vždy skládá z výběru certifikátu a zadání PINu, pokud si jej aplikace vyžádá.

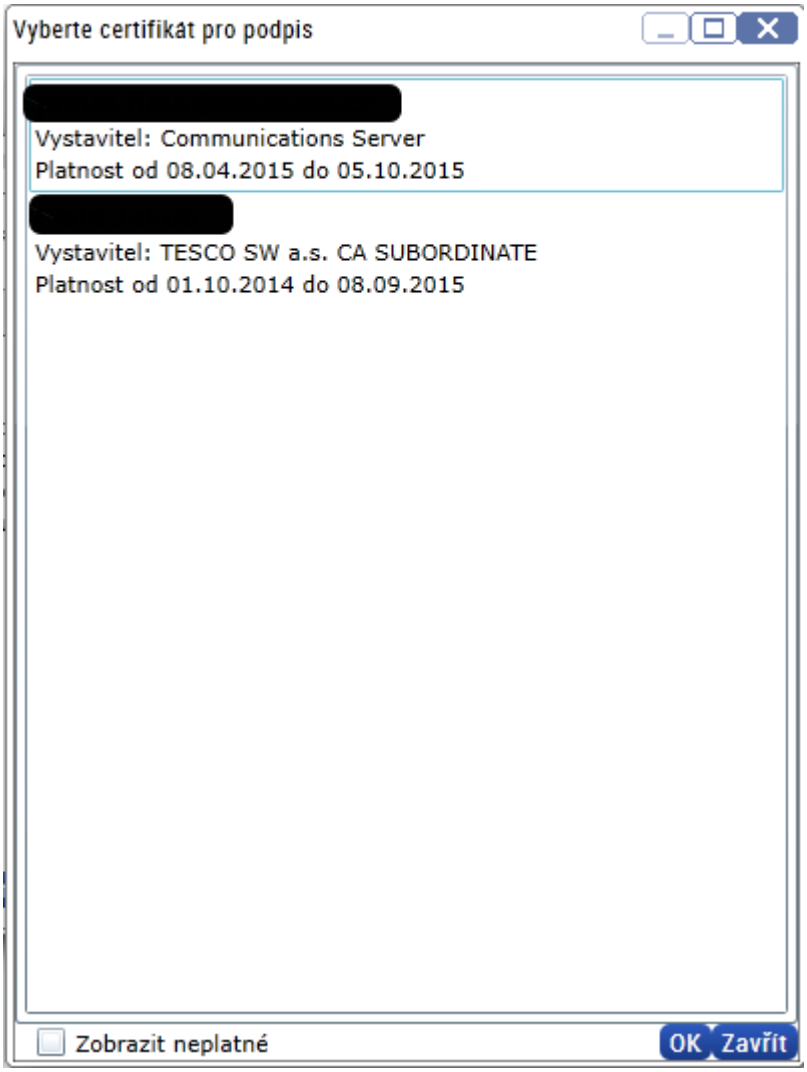
V otevřeném okně máte na výběr, které způsoby uložení privátního klíče využijete. Pokud chcete využít

- privátní klíč v tokenu, klikněte na „Systémové úložiště“[2] a volbu „Vybrat“, dále pokračujte postupem 4.1.1
- privátní klíč v systémovém úložišti, klikněte na „Systémové úložiště“ a volbu „Vybrat“, dále pokračujte postupem 4.1.1
- privátní klíč uložen v souboru, klikněte na „Soubory“ a volbu „Vybrat“, dále pokračujte postupem 4.1.2

4.1.1 Token, úložiště

Po výběru volby „Systémové úložiště“ a kliknutí na tlačítko „Vybrat“ se otevře dialogové okno s přehledem certifikátů. V seznamu se zobrazí jen ty privátní klíče, které je možné použít pro podpis, a zároveň jsou aktuálně platné. Vyberte certifikát, který chcete využít.

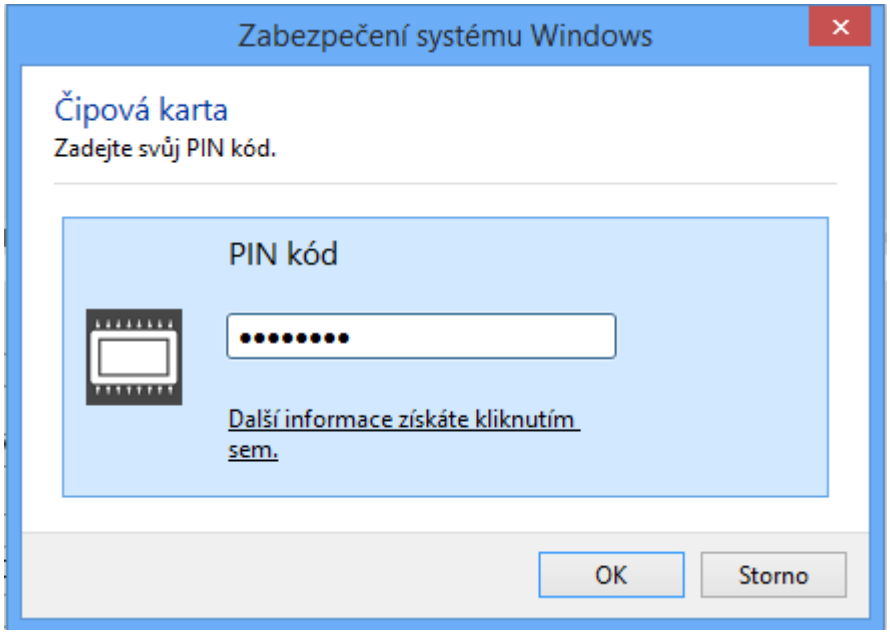
[2] Klíče budou viditelné za předpokladu zaregistrování klíče v úložišti. Více v kapitole „Privátní klíč uložen v tokenu“.



Obrázek 3 – Přehled dostupných certifikátů

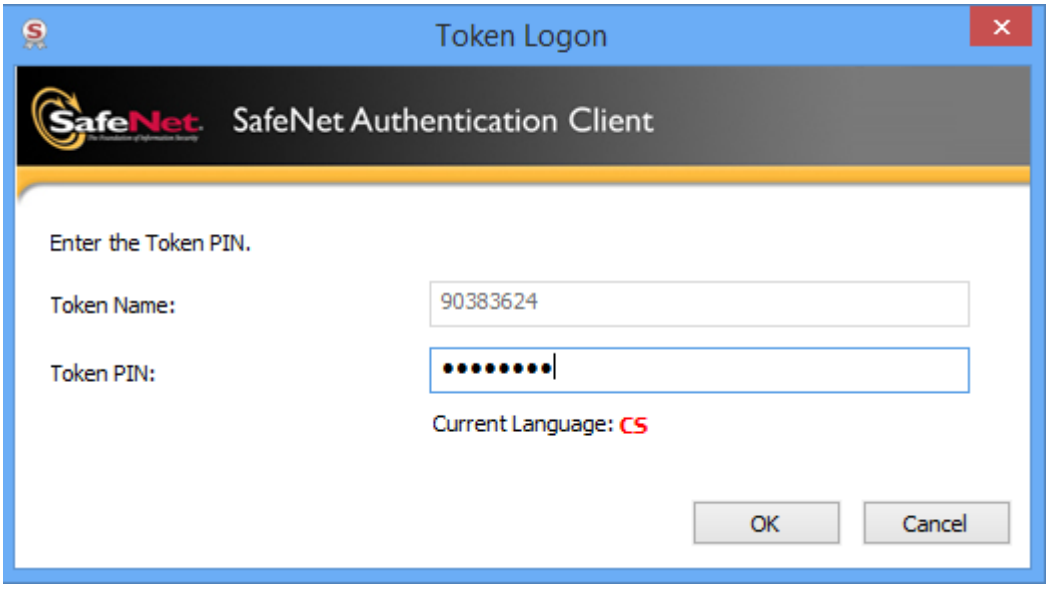
Vyberte záznam a stiskněte OK. Pokud bude vyžadováno zadání PINu k certifikátu, budete vyzváni ve vlastním vyskakovacím okně k jeho zadání. V okně se může zobrazit i ikona symbolizující místo uložení klíče.

Dialogové okno pro zadání PIN může být rozdílné. Například pokud je privátní klíč uložen v systémovém úložišti nebo na virtuální čipové kartě, objeví se dialogové okno systémového úložiště. Ale například při použití USB tokenu může vyskočit přímo dialogové okno obslužného programu tokenu.



Obrázek 4 – Dialogové okno pro zadání PIN – čipová karta

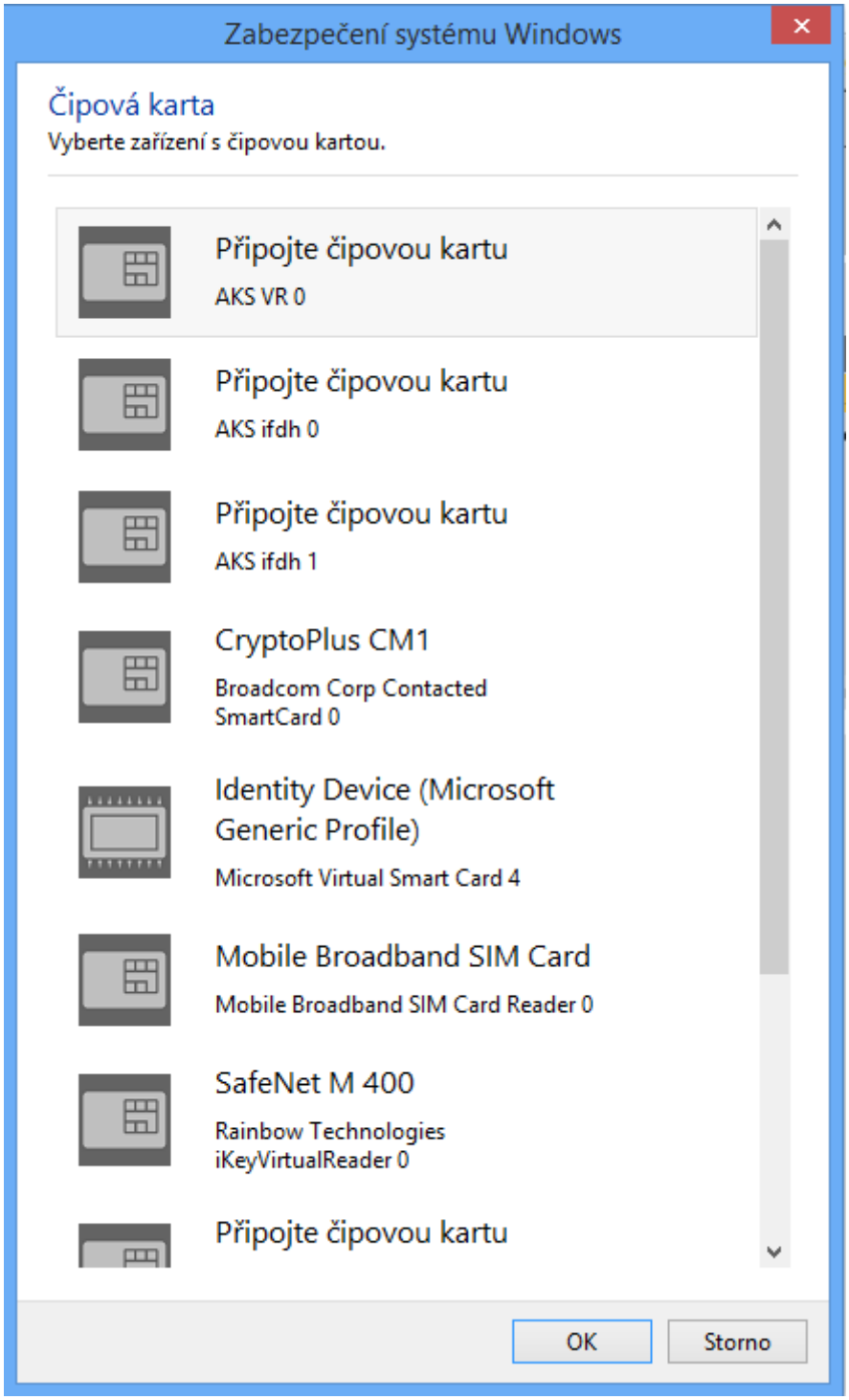
Příklad při použití USB tokenu iKey.



Obrázek 5 – Dialogové okno pro zadání PIN – USB token iKey

Po stisku tlačítka OK dojde k vytvoření podpisu. Pokud se vytvoření podpisu nepovede, budete informováni.

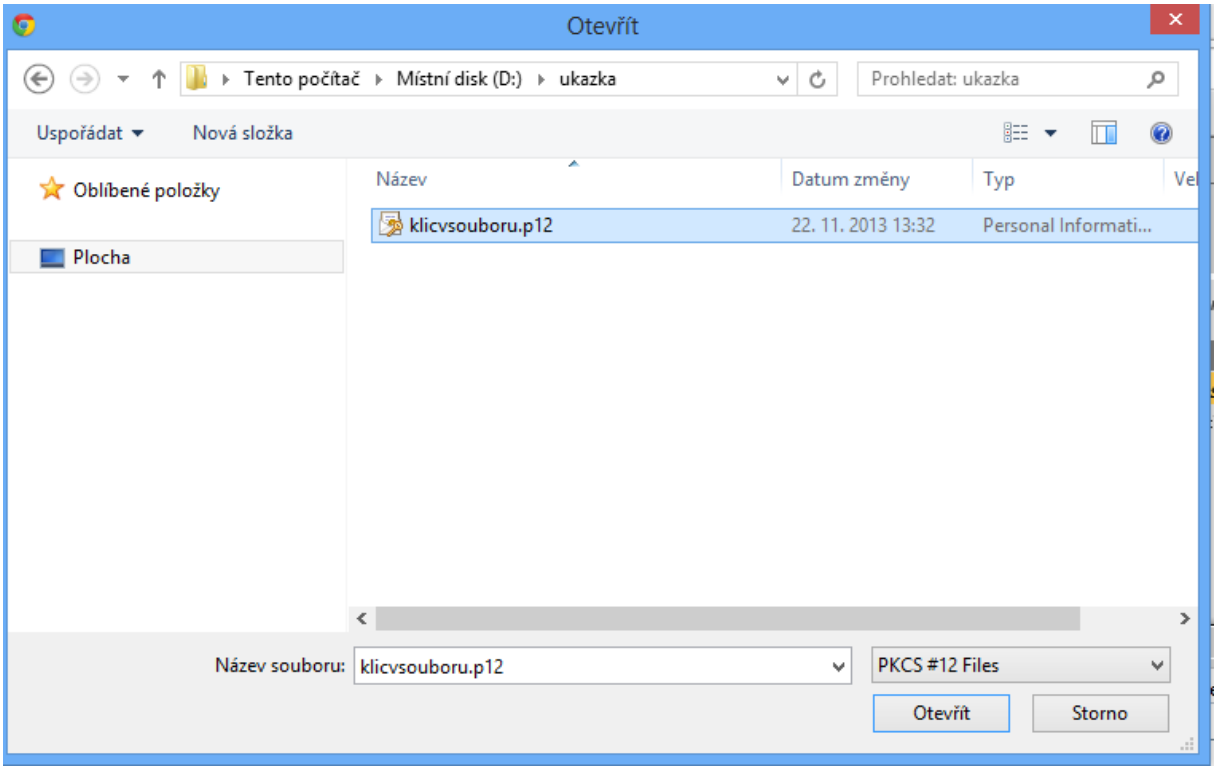
Pokud máte v systému více čipových karet a privátní klíč je uložen na čipové kartě, může se před otevřením dialogového okna pro zadání PIN objevit dialogové okno pro výběr správné čtečky čipových karet.



Obrázek 6 – Dialogové okno pro výběr čipové karty

4.1.2 Soubor

Po výběru volby „Soubory“ a kliknutí na tlačítko „Vybrat“ vyskočí dialogové okno pro vyhledání privátního klíče v souboru na disku zařízení. Systém vyhledává soubory ve formátu PKCS #12 (přípona .p12).



Obrázek 7 – Výběr certifikátu ze souborového úložiště

Po jeho výběru se okno zavře a uživatel vloží heslo ke klíči uloženému v souboru.

Obrázek 8 – Dialog pro zadání hesla k privátnímu klíči

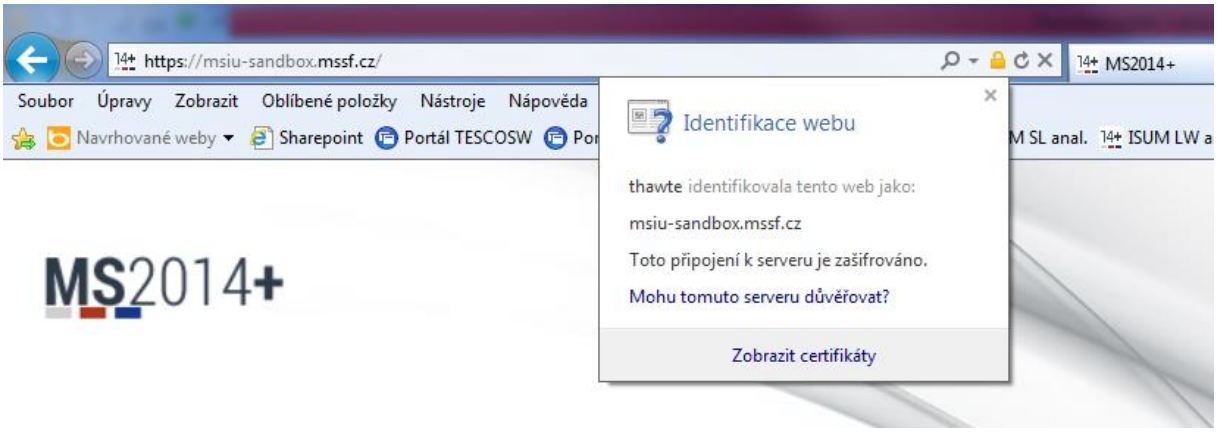
Zadejte odpovídající heslo. Po stisku tlačítka Dokončit dojde k vytvoření podpisu. Pokud se vytvoření podpisu nepovede, budete informováni.

4.2 Ověření identity

Systém MS 2014+ využívá výhradně zabezpečenou komunikace pomocí protokolu HTTPS. Ověření identity provádí samotný prohlížeč. V každém prohlížeči je možné zkontrolovat, zda certifikát souhlasí s adresou, kterou máte zadanou v prohlížeči.

Například v Internet Explorer 11 je vidět, že komunikace je zabezpečena a adresa aplikace odpovídá certifikátu.

Pro zabezpečení komunikace jsou a budou použity výhradně certifikáty certifikačních autorit, které jsou v programu Microsoft Root.



Obrázek 9 – Zabezpečení komunikace s aplikací MS 2014+

Samotná aplikace MS 2014+ je elektronicky podepsána. Právě certifikát s veřejným klíčem, jehož soukromý klíč byl použit pro podepsání aplikace, je instalován podle návodu na https://mseu.mssf.cz/ pod záložkou HW a SW požadavky. Na uvedené adrese je k dispozici ke stažení i instalační balíček ke zvýšení oprávnění práv aplikace. Přítomnost tohoto certifikátu je jedním z požadavků na zpřístupnění tokenů a systémového úložiště na Vašem zařízení.

Použitý certifikát, na kterém je založen elektronický podpis, má pouze omezenou dobu platnosti. Před jeho vypršením (nebo i dříve kvůli jiným důvodům) bude aplikace opatřena novým podpisem. Nový elektronický podpis vytvořený s využitím nového certifikátu se projeví nedostupností práce s klíči uloženými na tokenu nebo systémovém úložišti Windows. Uživatel musí opět provést postup odkazovaný výše. Při změně certifikátu budou uživatelé informováni. Tato obměna certifikátu souvisí s jeho platností, která je 1 až 2 roky.

Od 1.9.2014 je použit certifikát od „DigiCert EV Code Signing CA (SHA2)“ vystavený pro „TESCO SW, a.s.“ se sériovým číslem 25892533 a platností do 5.8.2016.

5 Prerekvizity pro práci s klíči a certifikáty v MS 2014+

5.1 Prerekvizity pro práci s privátními klíči pro podepisování (C1)

Po provedení příslušného nastavení počítače popsaného v nápovědě dostupné na následující adrese https://mseu.mssf.cz/ v záložce HW a SW požadavky, je možné použít privátní klíče uložené v systémovém úložišti Windows nebo na tokenu.

Pokud se neprovede předchozí postup, je možná pouze práce se soubory obsahujícími privátní klíč. Přípona souboru je „.PFX“.

6 Ukázky postupů

6.1 Jak získat pár privátního a veřejného klíče

Pro získání páru privátního a veřejného klíče doporučujeme obrátit se na své IT oddělení, které by mělo mít zkušenosti se získáváním certifikátů pro své pracovníky. Pokud to není možné, lze certifikát získat od jedné ze tří akreditovaných certifikačních autorit. Postup se může u každé certifikační autority lišit, proto je třeba se nejdříve s příslušným návodem seznámit na webových stránkách CA.

Pro certifikáty určené pro podpis

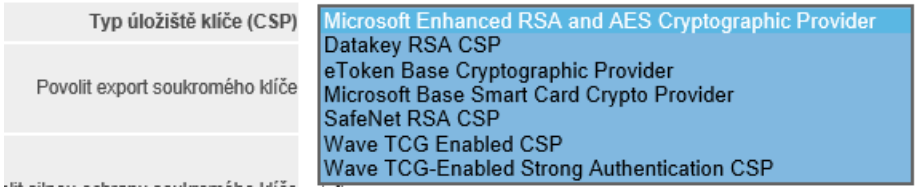
- PostSignum http://www.postsignum.cz/kvalifikovane_certifikaty.html
- První certifikační autorita https://www.ica.cz/Kvalifikovany-certifikat
- eIdentity http://www.eidentity.cz/

Dále popsaný postup popisuje příklad získání kvalifikovaného certifikátu od certifikační autority PostSignum. Získání komerčního certifikátu je procesně identické.

Pro získání prvního certifikátu od PostSignum je možné volit z několika způsobů. Zde je popsán způsob, kdy si žádost vygeneruje daná osoba na svém počítači a s ověřovacím kódem přijde na kontaktní místo PostSignum podepsat smlouvu, provést platbu a aktivovat certifikát:

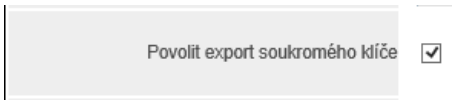
1. Na adrese https://www.postsignum.cz/online_generovani_zadosti.html, kterou otevřete v prohlížeči Internet Explorer, zvolte *On-Line generování žádosti o vydání certifikátu*.
2. Vyplňte své údaje (jméno a příjmení, email). Velikost klíče ponechejte co nejvyšší.
3. Podle zamýšleného uložení privátního klíče zvolte příslušnou volbu v „Umístění soukromého klíče“. Vaše volby mohou být odlišné z důvodu nainstalovaných jiných tokenů.
   Příklad PostSignum:

   Příklad I.CA:



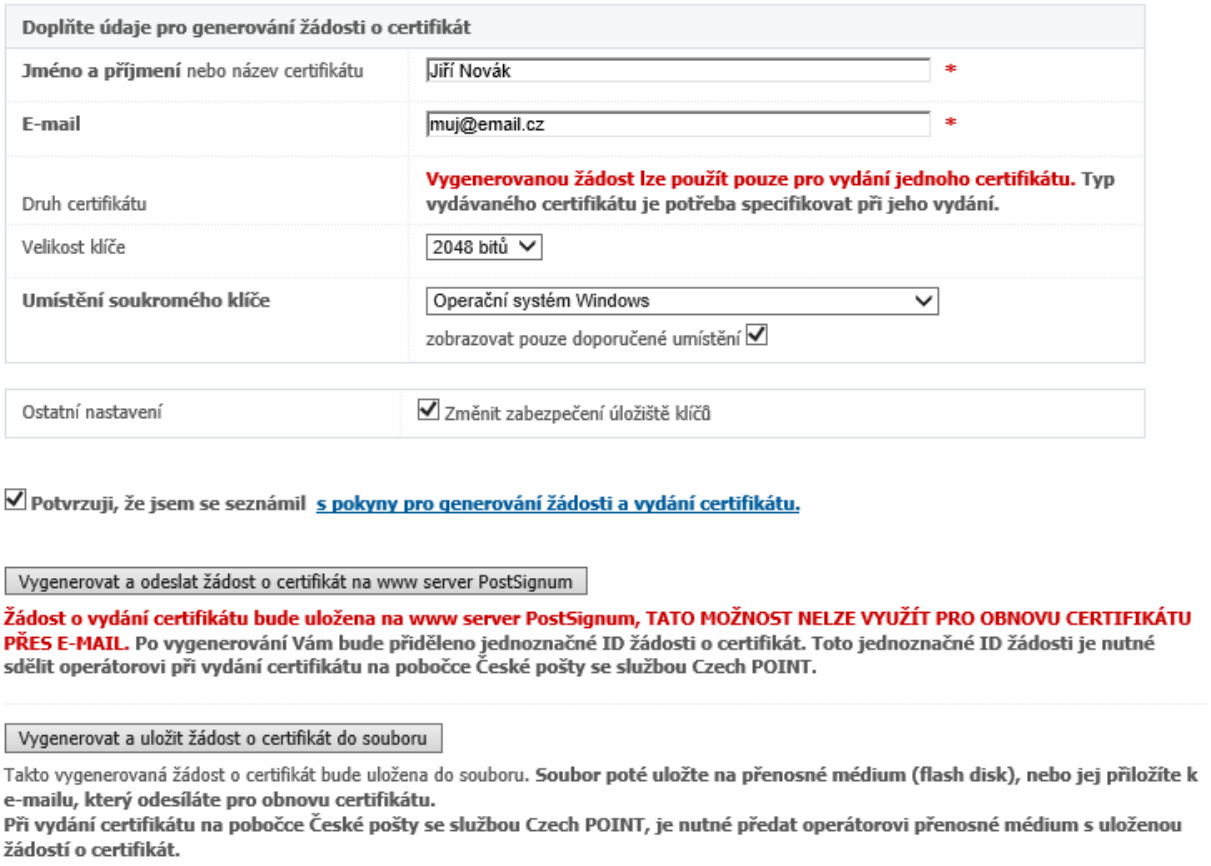
   a. Pokud chcete používat USB token (například iKey4000), zvolte „USB token iKey 4000“ (nebo SafeNet RSA CSP)
   b. Pokud chcete využívat čipovou kartu (včetně virtuální čipové karty), zvolte možnost obsahující „Microsoft Base Smart Card Crypto Provider“
   c. Pokud chcete využívat pouze systémové úložiště nebo chcete mít privátní klíč v souboru, zvolte Operační systém Windows (nebo „Microsoft Enhanced RSA and AES Cryptographic Provider“)
   d. Pokud máte jiný token, vyberte vhodný záznam.
4. Pokud máte zvolenu možnost c), zaškrtněte *Změnit zabezpečení úložiště klíčů*. Pokud budete chtít využívat privátní klíč uložený v souboru nebo jej budete chtít mít možnost exportovat

(například pro zálohu na bezpečné místo - na CD do trezoru) nebo pro následný import do virtuální čipové karty na jiný počítač nebo do jiného počítače a postup generování certifikátu u dané CA to umožňuje, povolte možnost Exportovat. Například u I.CA:

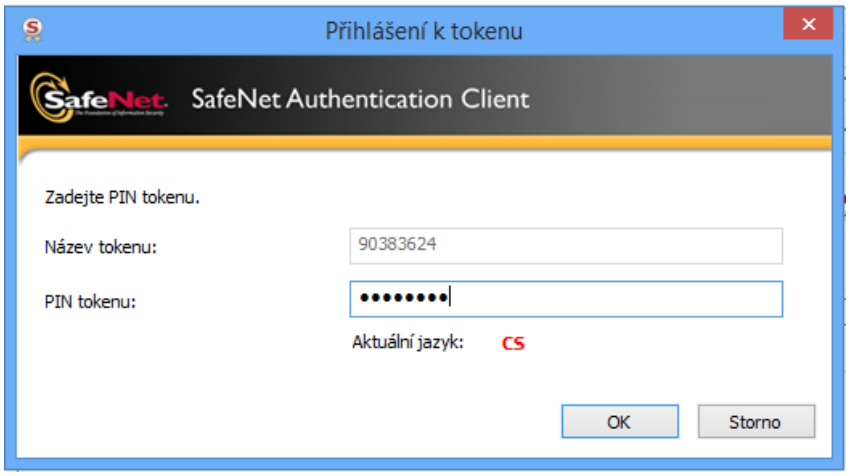


5. Po přečtení pokynů potvrďte jejich přečtení zaškrtnutím položky *„Potvrzuji, že jsem se seznámil…“*

Ilustrační stav je zobrazen na obrázku. Je zvoleno uložení privátního klíče v úložišti certifikátů.

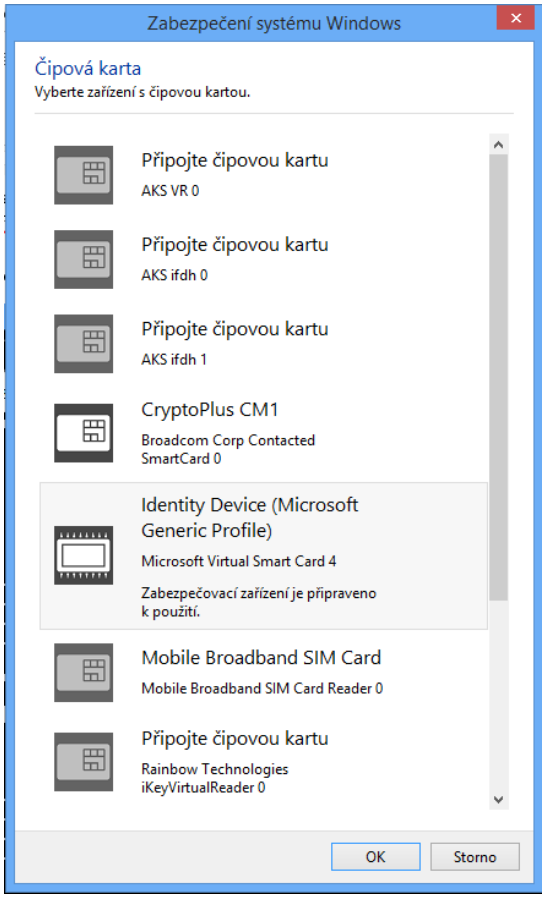


6. Zvolte *„Vygenerovat a odeslat žádost o certifikát na www server PostSignum“*.
7. Podle volby v bodě 3. postupujte:
    a. USB token, token
        i. Zadejte PIN (vzhled okna se může lišit v závislosti na použitém tokenu)

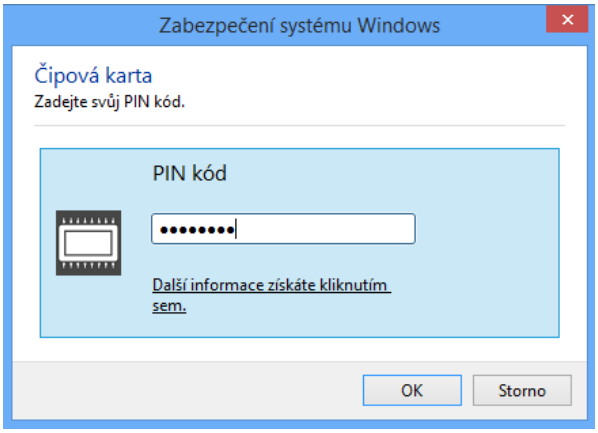


b. Čipová karta

i. Pokud máte na počítači více čipových karet, vyskočí dialogové okno pro vyběr přesného zařízení. V případě použití virtuální čipové karty se můžete i orientovat pomocí speciální ikony  .

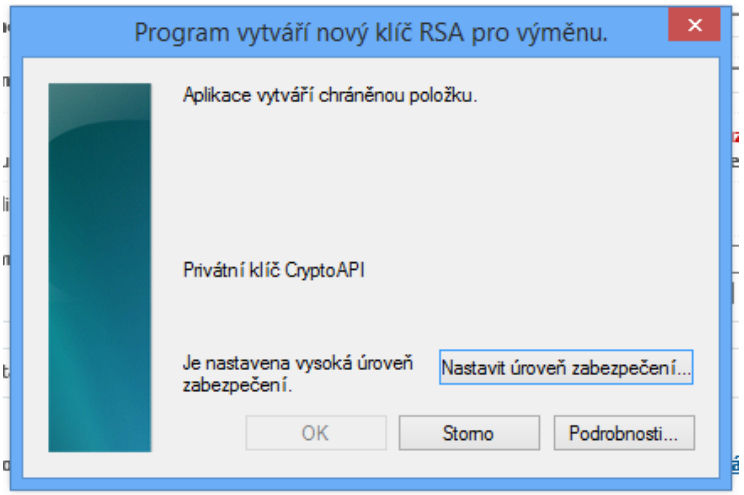


ii. Po stisku tlačítka OK vyskočí další dialogové okno pro zadání. Tento PIN budete zadávat vždy při požadavku o použití této čipové karty.

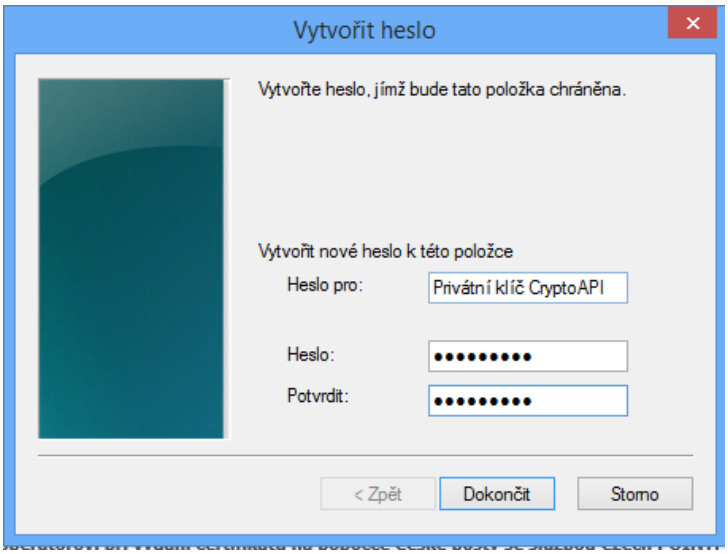


c. Systémové úložiště

i. vyskočí dialogové okno pro zadání PIN (v zobrazeném okně klikněte na *„Nastavit úroveň zabezpečení“*)



ii. Zadejte PIN, který budete muset zadat při každém použití



iii. Stiskněte *„Dokončit“* a poté *„OK“*

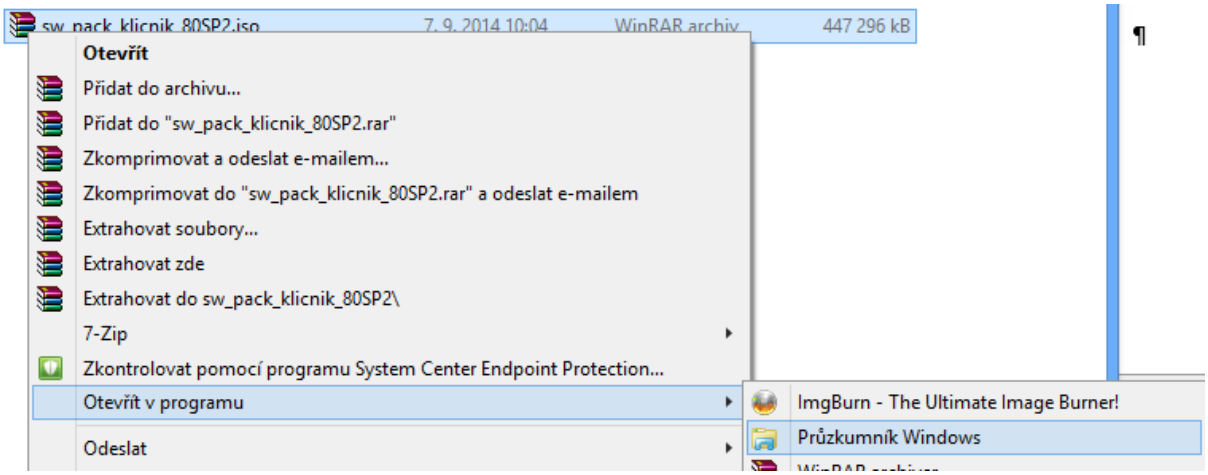
8. Na webové stránce se Vám zobrazí ID žádosti. Toto ID žádosti si zapište a zajděte s ním a s potřebnými dokumenty na Kontaktní místo PostSignum. Jsou to všechny pobočky, na kterých je dostupná služba Czech Point. Odkaz na seznam kontaktních míst je umístěn zde: http://www.postsignum.cz/pobocky_ceske_posty.html.
9. Po podepsání smlouvy dorazí na zadaný email odkaz na získání certifikátu. V rámci potvrzení vyberte odpovídající zařízení, na kterém je uložen privátní klíč.
10. Pokud použijete jinou certifikační autoritu, postupujte podle jejich návodu a získejte svůj certifikát. Postsignum a I.CA mají princip stejný. eIdentity má postup kroků lehce odlišný.
11.
    a) Pokud budete využívat systémové úložiště, čipovou kartu nebo USB token,… zde skončete. Privátní klíč s certifikátem by již měl být uložen ve složce Osobní v systémovém úložišti certifikátů operačního systému nebo zaregistrován v případě použití tokenu.
    b) Pokud jste zvolili možnost exportu privátního klíče, postupujte dále podle postupu *Jak exportovat privátní klíč do souboru*.

6.2 Jak získat a nastavit token

Ukázka je prováděna na Windows 8.1. Postup popisuje získání USB tokenu pod obchodním názvem Bezpečný klíč spolu s kupónem na získání certifikátu. Pro vytvoření virtuální čipové karty postupujte podle postupu *Jak vytvořit virtuální čipovou kartu*.

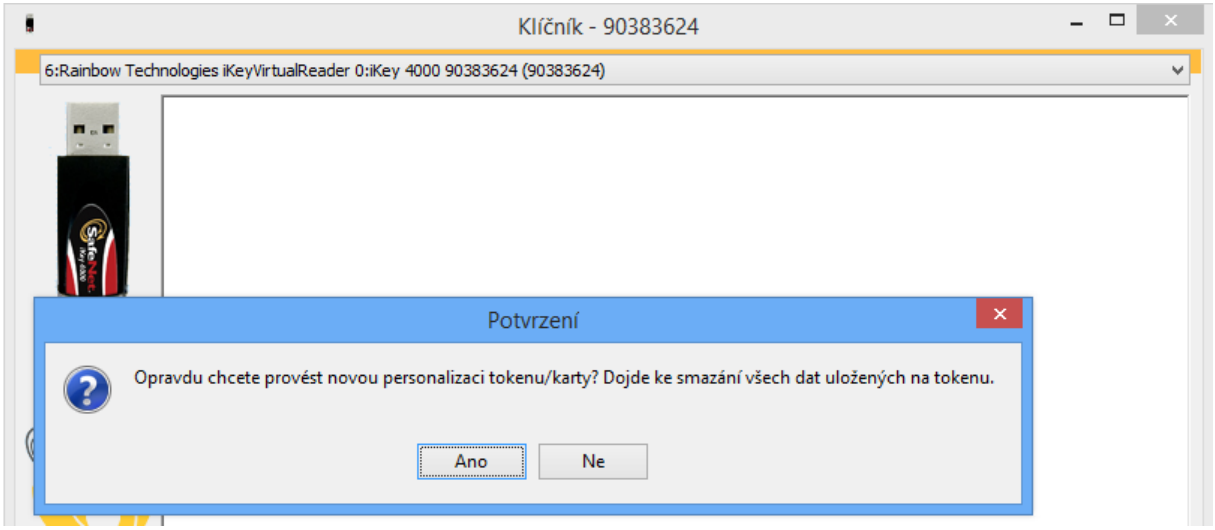
1. Na adrese http://www.postsignum.cz/bezpecny_klic_.html si přečtěte informace o tomto produktu a vyhledejte si požadovanou variantu.
2. Zakupte USB token, který bude dle varianty obsahovat i kupóny na nákup certifikátu/ů. Buď objednáním na internetu nebo osobní návštěvou některého kontaktního místa certifikační autority. Token nepřipojujte.
3. Pokud používáte Windows 8 a vyšší, aktuálně dodávaný SW u produktu na CD jej nepodporuje. Stáhněte si jej po zaregistrování (postup a kód pro registraci je součástí balení) a stáhněte aktuální verzi. Pro úspěšné provedení dalších kroků zvolte po registraci „větší“ variantu (sw_pack_klicnik_80SP2.iso).
   Pokud máte starší verzi Windows, postupujte bodem 5.

4. Stažený soubor vypalte dle návodu u odkazu nebo jej spusťte v průzkumníku Windows a otevře se jako CD.

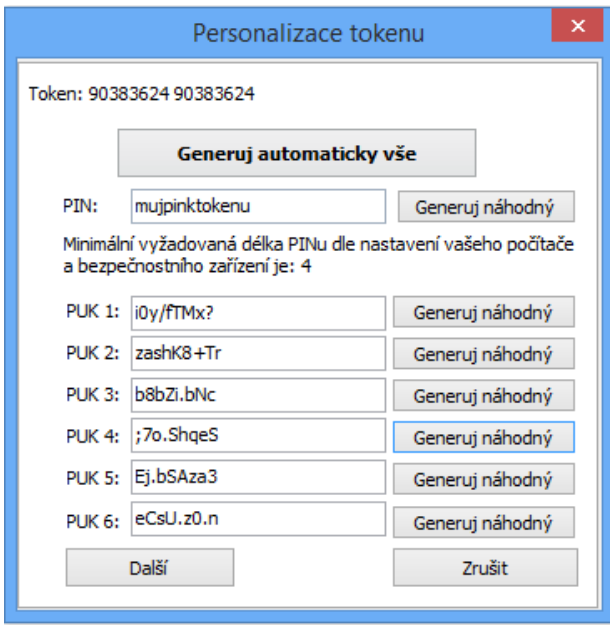


5. Před připojením USB tokenu nejdříve spusťte program na CD (pokud nemáte povoleno automatické spuštění, tak souborem „Spustme.exe"), prostudujte návody na přiloženém CD a poté pomocí průvodce token nainstalujte. Instalujte veškeré obslužné programy. Během instalace musíte minimálně 1x restartovat počítač a opětovně spustit instalaci. Během instalace budete vyzváni k připojení tokenu.

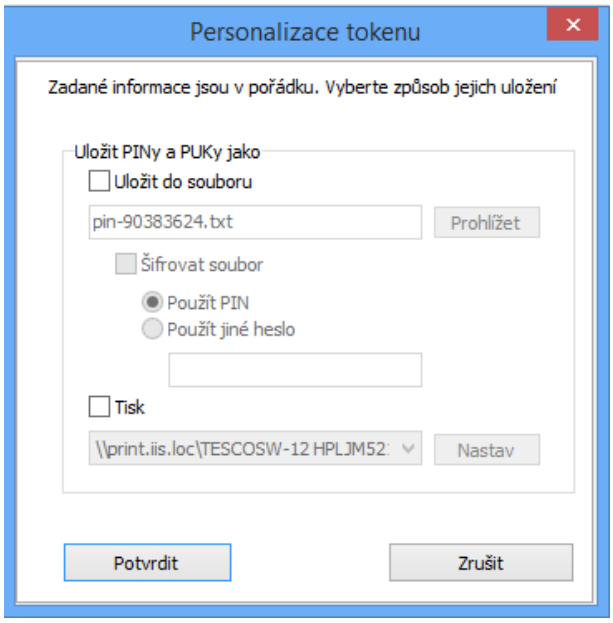
6. Spusťte nainstalovaný program Klíčník a proveďte nastavení tokenu– tzv. personalizace. Nachází se pod tlačítkem Nastavení – Personalizovat. Potvrďte zobrazenou hlášku.



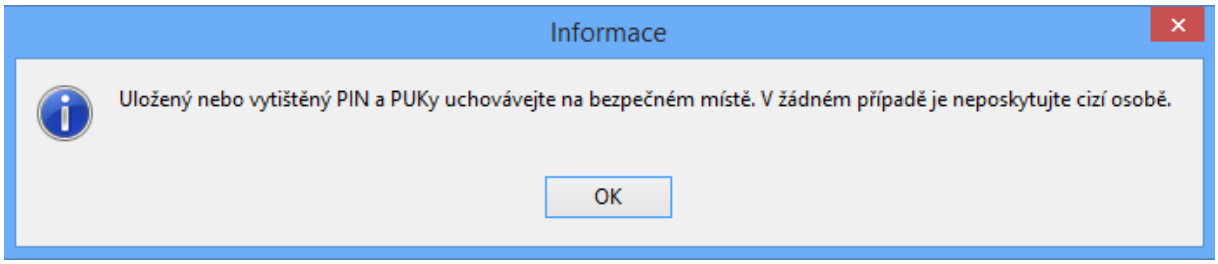
7. Personalizací dojde k nastavení PIN, který budete zadávat pro přihlášení se k tokenu nebo při použití klíče na USB tokenu uloženém. Dále PUK kódy sloužící k obnovení PIN, pokud dojde k jeho ztracení. Jako PIN doporučujeme zadat vlastní frázi. U PUK je možné použít i vlastní generátor.

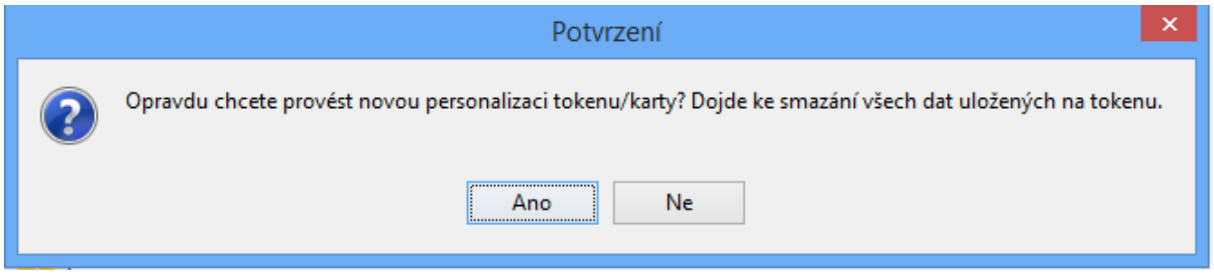


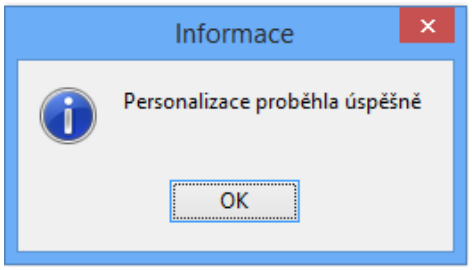
8. Klikněte na Další. Zde si můžete zvolit způsoby uložení PIN a PUK kódů. PIN ani PUK neuchovávatejte v otevřené podobě na zařízení, kde může dojít k jejich kompromitaci. Můžete a nemusíte vybrat nějakou z možností a klikněte na Potvrdit.



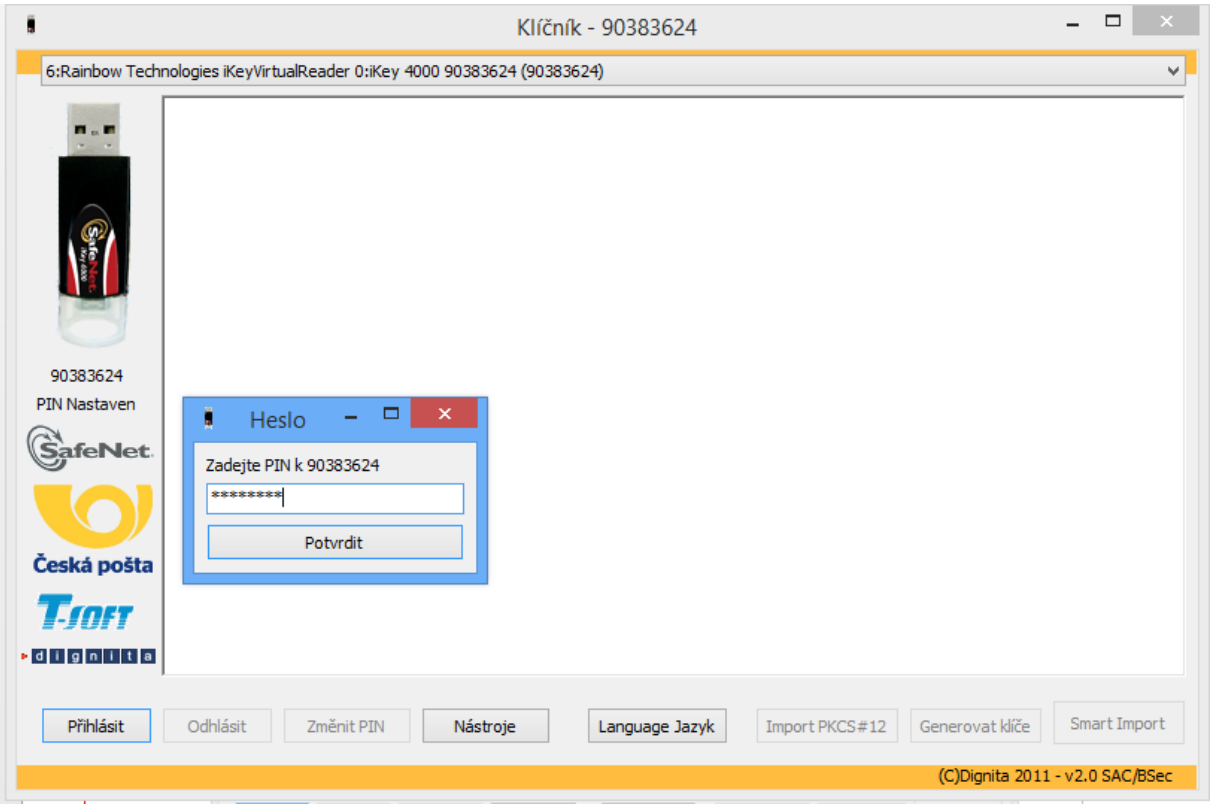
9. Vyskočí informační dialogové okno a za ním opět další potvrzovací okno. Potvrďte jej volbou Ano. Nyní je token připraven k použití.







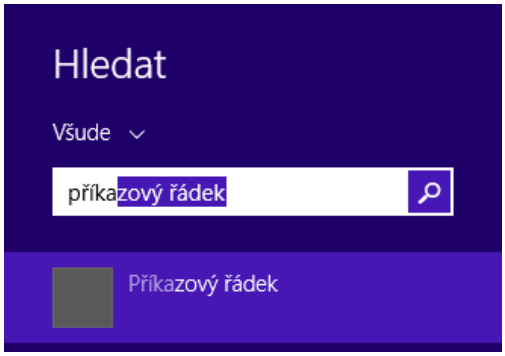
10. Pro přístup k tokenu v obslužném programu stikněte tlačítko Přihlásit a zadejte PIN. Poté se zpřístupní ostatní volby (změna PIN, import, generování).



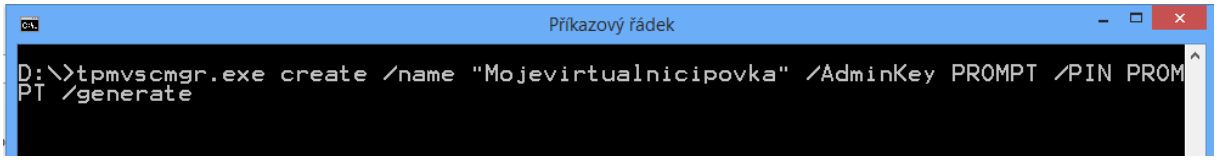
6.3 Jak vytvořit virtuální čipovou kartu

Ukázka je prováděna na Windows 8.1.

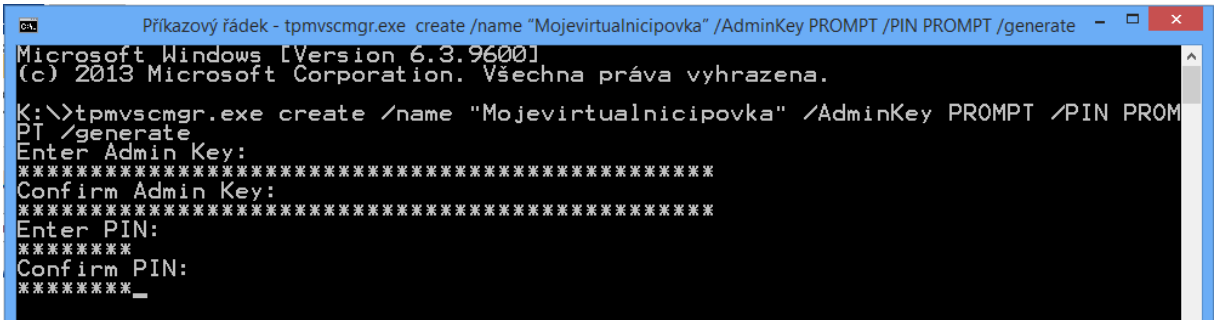
1. Spusťte příkazový řádek



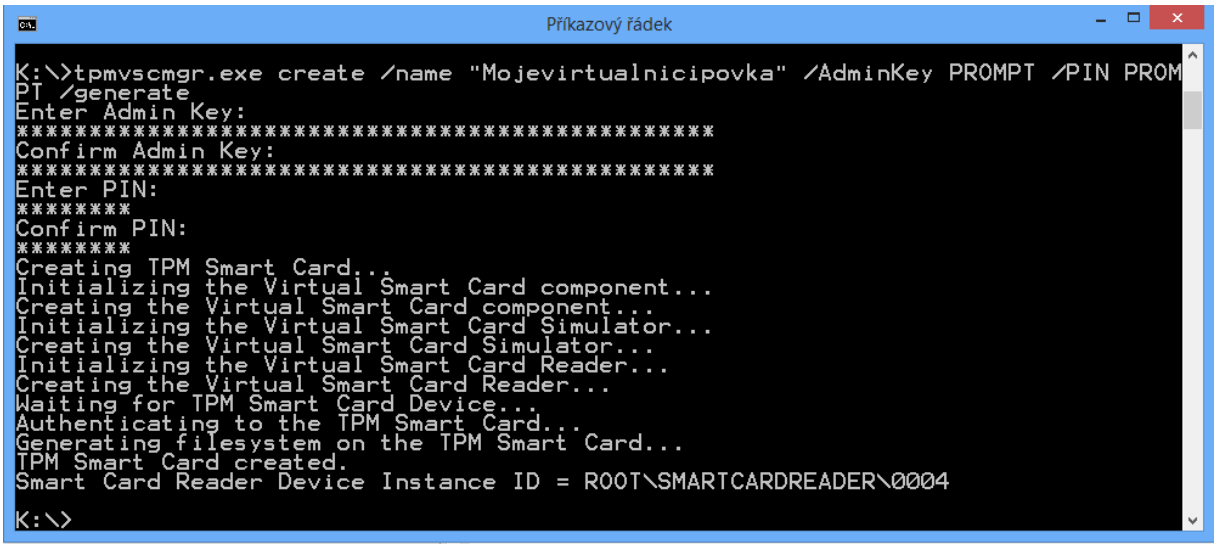
2. Spusťte v něm příkaz, kterým se vytvoří virtuální čipová karta. Například „tpmvscmgr.exe create /name “Mojevirtualnicipovka” /AdminKey PROMPT /PIN PROMPT /generate„.
   V příkazu specifikujete:
   - Name - název, pod jakým virtuální čipovou kartu uvidíte
   - PIN - PIN ke kartě, který budete zadávat při použití klíče na kartě uloženém. Zadáte jej po spuštění příkazu.
   - AdminKey pro zabezpečení administrace karty. Zadáte jej po spuštění příkazu. Musí být složen přesně ze 48 hexadecimálních znaků (číslic a písmen A až H).



3. Stiskněte Enter. Postupně zadejte AdminKey. Klíč si uložte na bezpečném místě. Rozhodně ne v otevřené podobě na stejném počítači. Dále zadejte PIN.



4. Po zadání údajů dojde k vytvoření virtuální čipové karty. Vytvoření trvá několik desítek sekund. Úspěšné vytvoření je zobrazeno na obrázku. Hodnota posledního řádku je závislá na vašem zařízení.



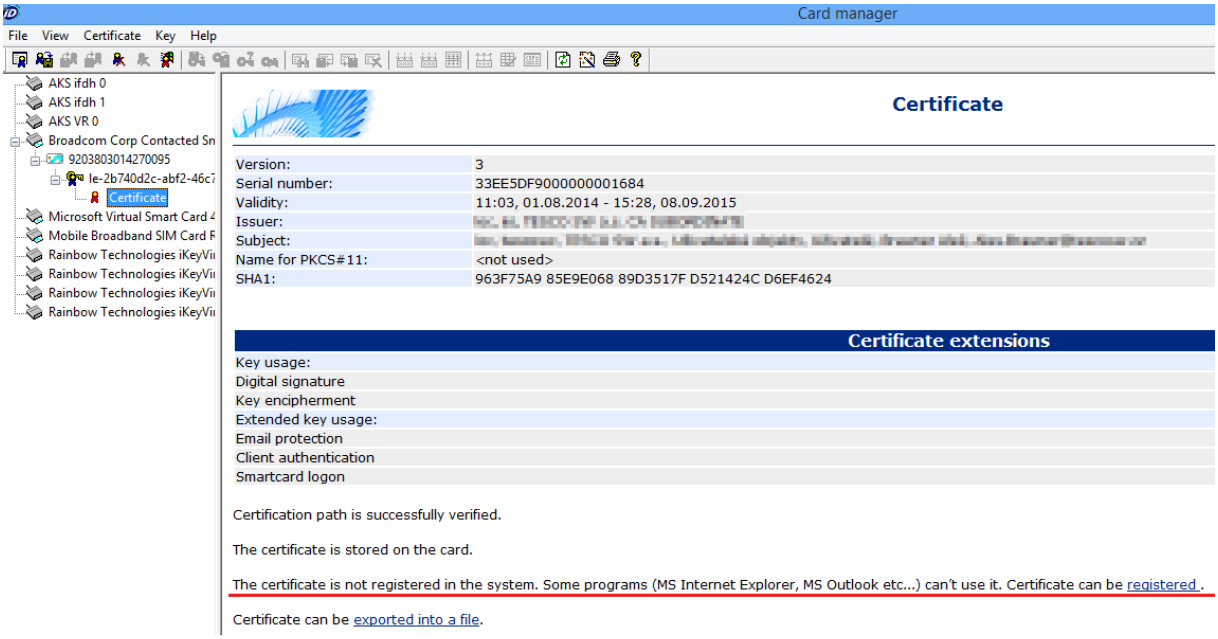
6.4 Jak naimportovat klíč do tokenu

Pokud jste negenerovali klíč přímo do tokenu, můžete jej dodatečně naimportovat. Podmínkou je existence klíče v souboru. Tímto postupem lze obecně importovat jak privátní klíče (pro podpis), tak i veřejné klíče (pro dešifrování).

1. Pro virtuální čipovou kartu postupujte podle samostatného postupu (podpora pouze privátních klíčů) *Jak zpřístupnit klíč uložený v tokenu v systémovém úložišti*

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.

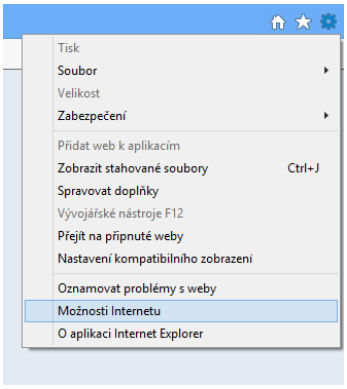


3. Pokud je certifikát nezaregistrovaný, program nabízí jeho zaregistrování. Klikněte na registraci. Nyní se klíč objevil v systémovém úložišti, složce osobní.

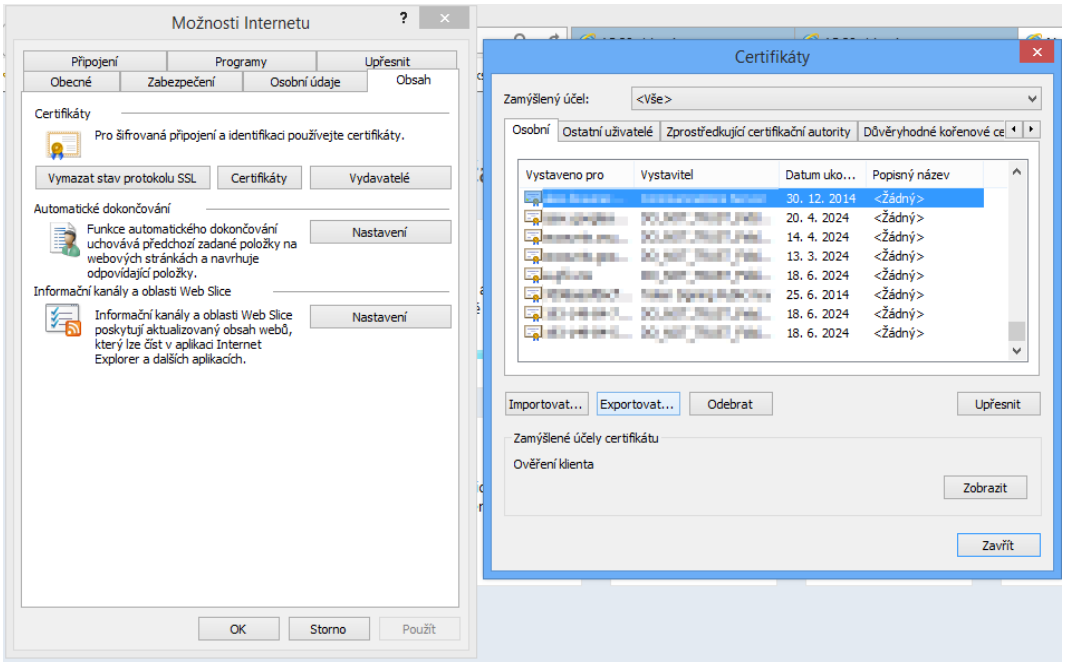
6.5 Jak exportovat privátní klíč do souboru

Export privátního klíče, který je uložen v úložišti certifikátů ve Windows a má nastaven příznak exportovatelnosti, je možné inicializovat více navzájem zaměnitelnými způsoby. Export nevyžaduje administrátorská oprávnění. Po spuštění samotného exportu jsou postupy totožné. Zobrazované ukázky jsou pro Windows 8.1 a prohlížeč Internet Explorer v.11.

1. Postup pomocí prohlížeče.
   1.1. V prohlížeči otevřete nabídku pro nastavení (ozubené kolečko v pravém horním rohu) a v ní vyberte „Možnosti internetu“

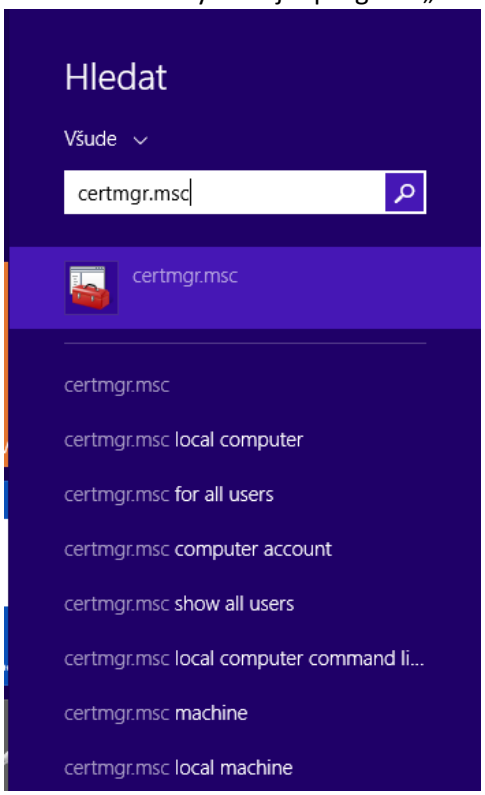


   1.2. Na záložce *„Obsah“* klikněte na tlačítko *„Certifikáty“*. Otevře se seznam certifikátů. Vyhledejte položku, kterou chcete exportovat. Typicky se bude nacházet na první záložce *„Osobní“*. Po jejím vybrání klikněte na tlačítko *„Exportovat“* a pokračujte bodem *3.Export klíče do souboru*.

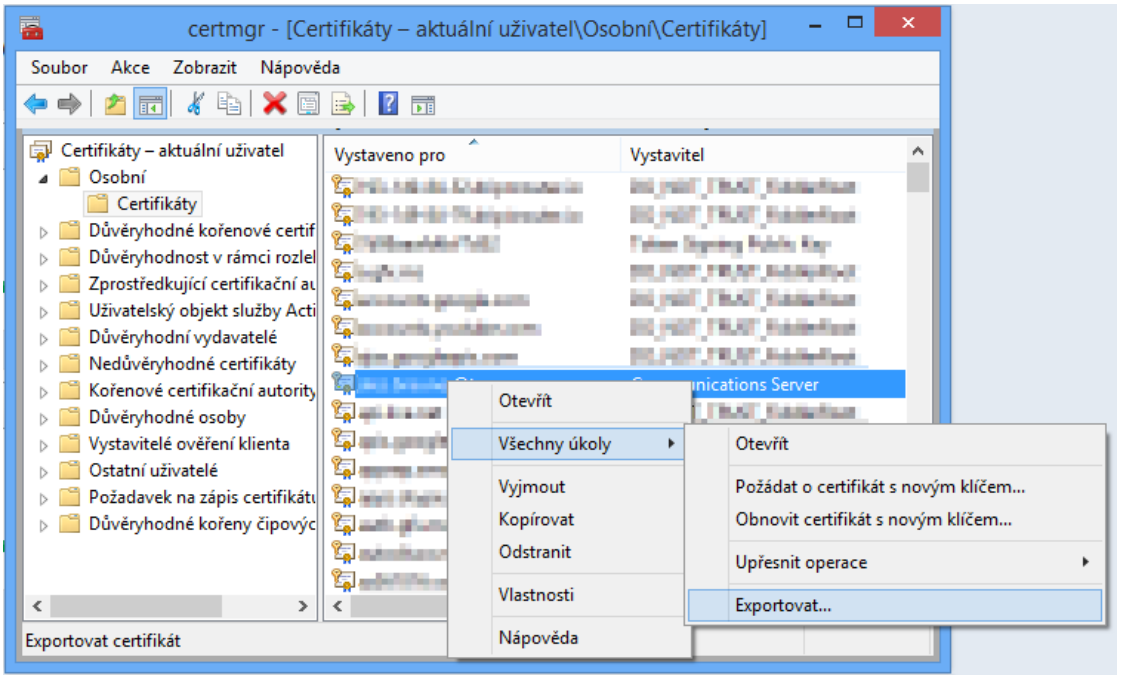


2. Postup přes konzoli

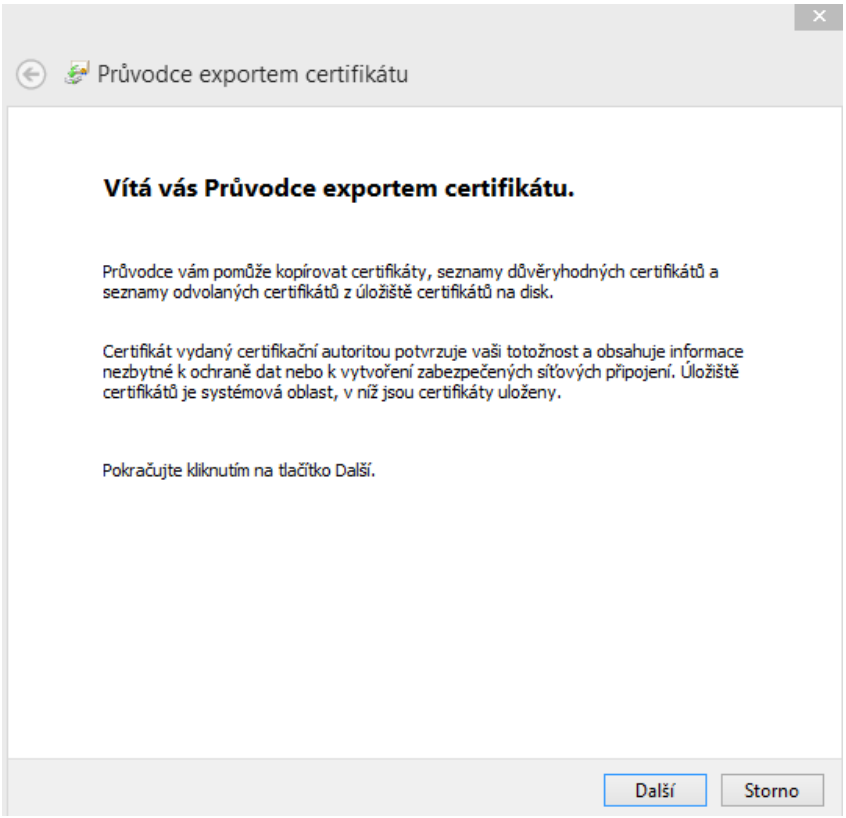
2.1. V nabídce start vyhledejte program „*certmgr.msc*“ a spusťte jej.



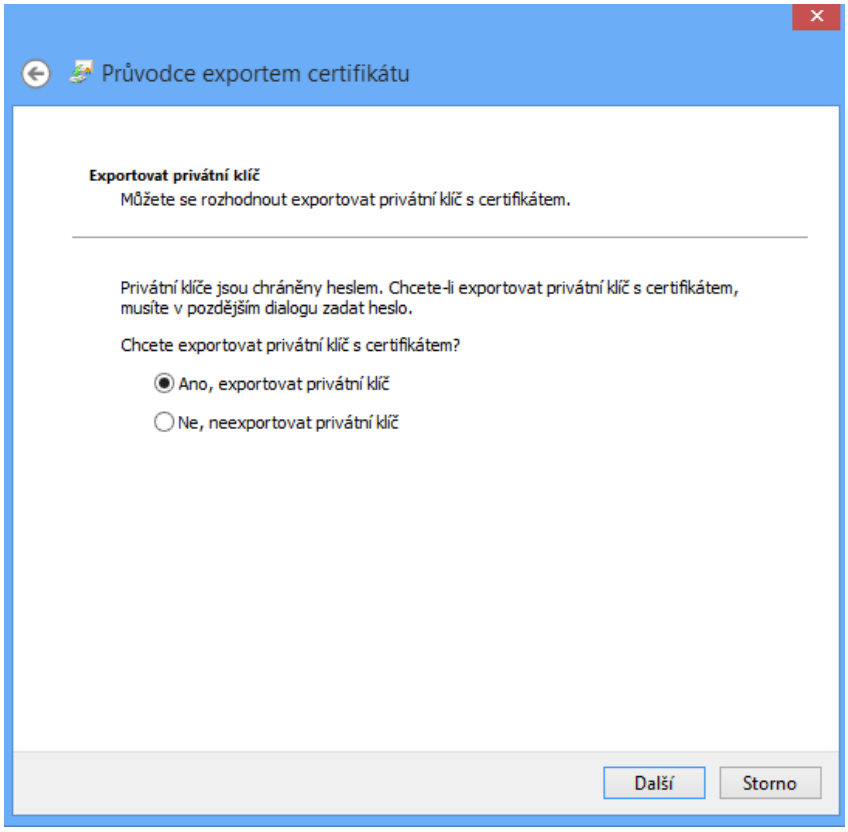
2.2. Otevře se seznam certifikátů. Vyhledejte položku, kterou chcete exportovat. Typicky se bude nacházet v první složce „*Osobní*“ -> „*Certifikáty*“. Klikněte pravým tlačítkem na položku, vyberte možnost „*Všechny úkoly*“ a „*Exportovat*“. Pokračujte bodem *3.Export klíče do souboru*.



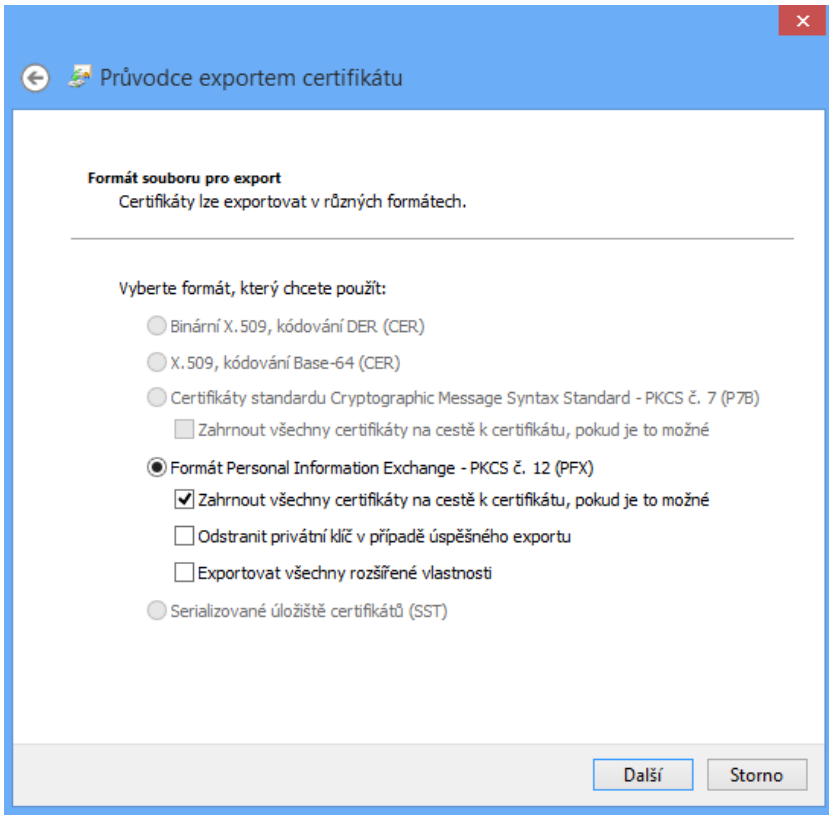
3. Export klíče do souboru
   3.1. První obrazovka po inicializaci exportu daného certifikátu:



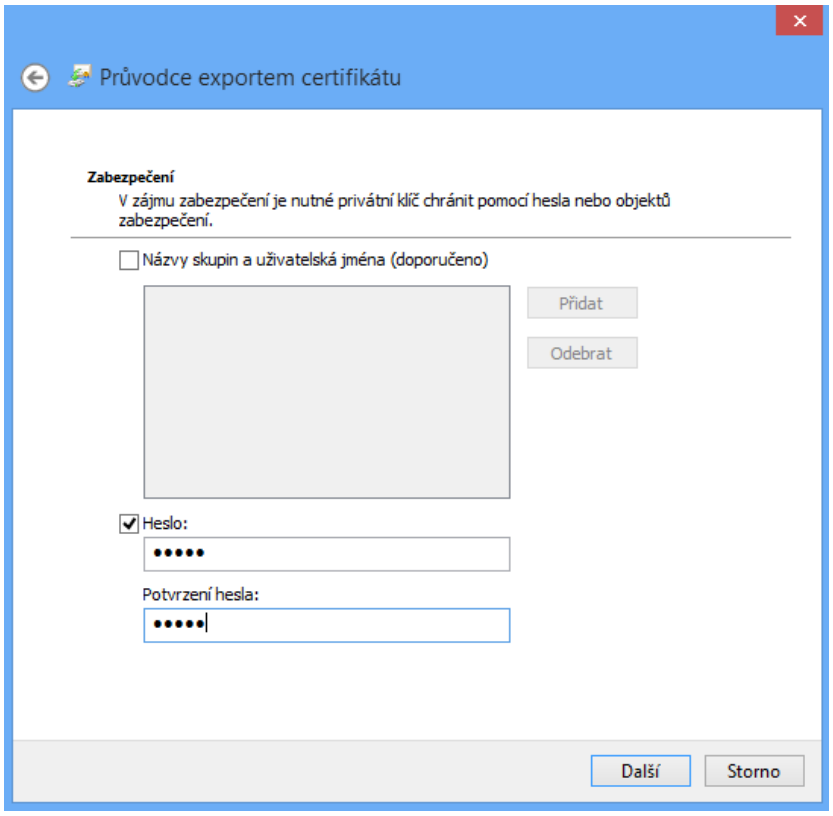
   3.2. Zvolte možnost exportování privátního klíče. Pokud nemá privátní klíč při vložení do systémového úložiště nastavenu možnost, že je exportovatelný, nebudete mít možnost si tuto volbu zvolit a dále není možné pokračovat.



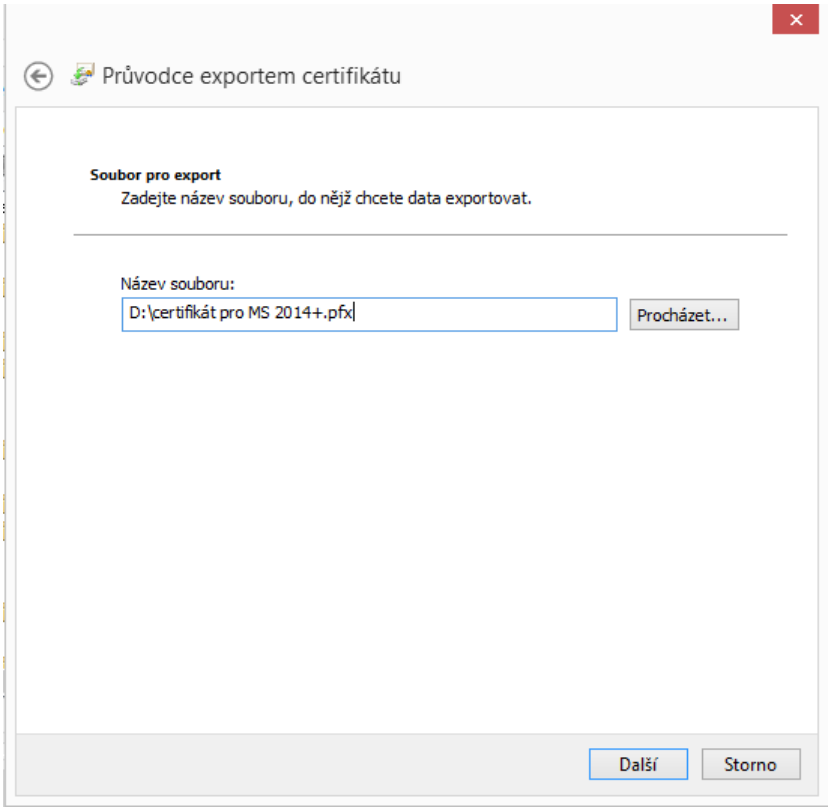
3.3. Ponechejte výchozí, nabízené nastavení. Pokud exportujete klíč z úložiště za účelem importu do bezpečnějšího způsobu uložení a nebudete chtít již dále mít tento klíč v úložišti, zvolte „Odstranit privátní klíč v případě úspěšného exportu“.



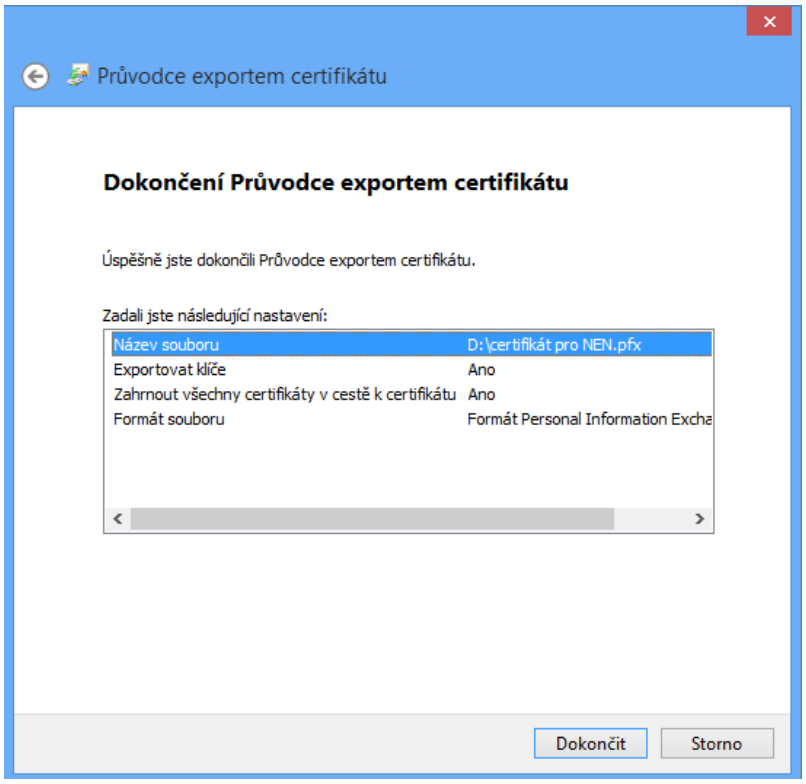
3.4. Zatrhněte možnost „*Heslo*“. Zadejte heslo. Při použití souboru s tímto klíčem budete muset zadat toto heslo. Zde zadané *Heslo* nemá žádnou souvislost s heslem zadaným během žádosti o generování certifikátu. Toto heslo se vztahuje pouze k tomuto souboru.



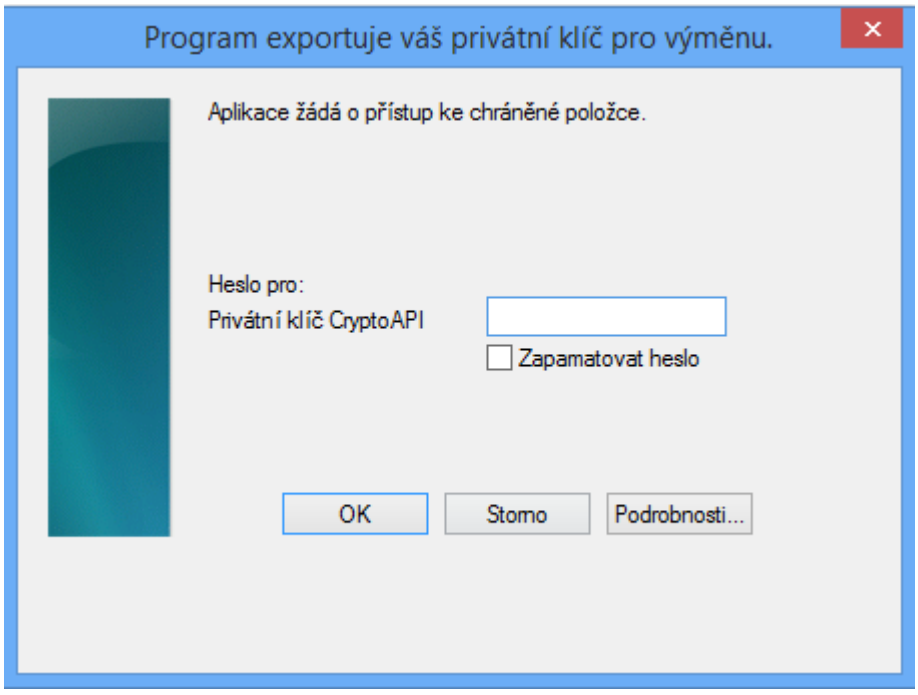
3.5. Zvolte umístění souboru.



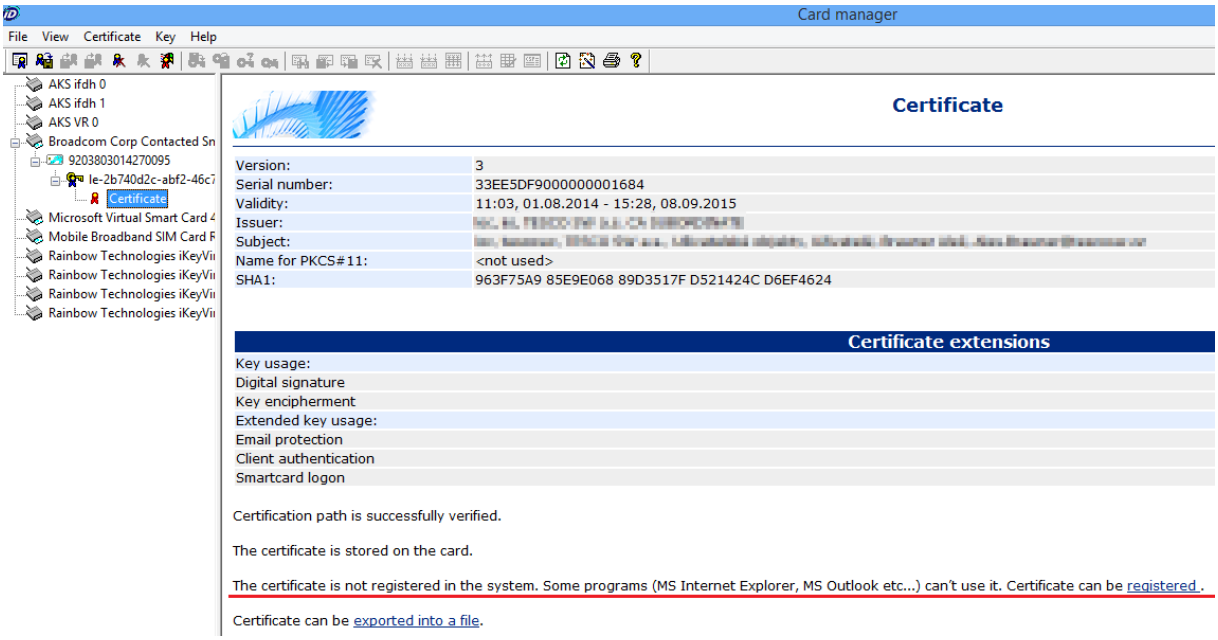
3.6. Stiskem tlačítka Dokončit se certifikát uloží na zadané úložiště a je možné jej použít.



3.7. Pokud to systém vyžaduje, vyplňte v novém okně heslo, které jste zadali v rámci generování žádosti nebo které zadáváte pro jeho použití.


Program exportuje váš privátní klíč pro výměnu.
Aplikace žádá o přístup ke chráněné položce.
Heslo pro:
Privátní klíč CryptoAPI
Zapamatovat heslo
OK
Storno
Podrobnosti...

2. Jak naimportovat privátní klíč v souboru do virtuální čipové karty 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.
   6.5. Otevřete vás obslužný program k tokenu.
   6.5. Vyhledejte v něm příslušný klíč.

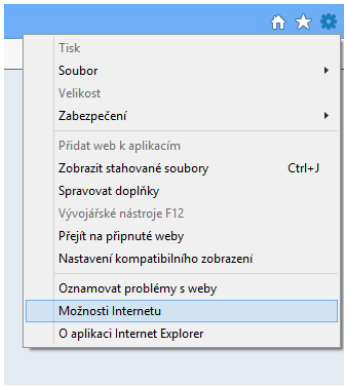


3. Pokud je certifikát nezaregistrovaný, program nabízí jeho zaregistrování. Klikněte na registraci. Nyní se klíč objevil v systémovém úložišti, složce osobní.

6.5 Jak exportovat privátní klíč do souboru

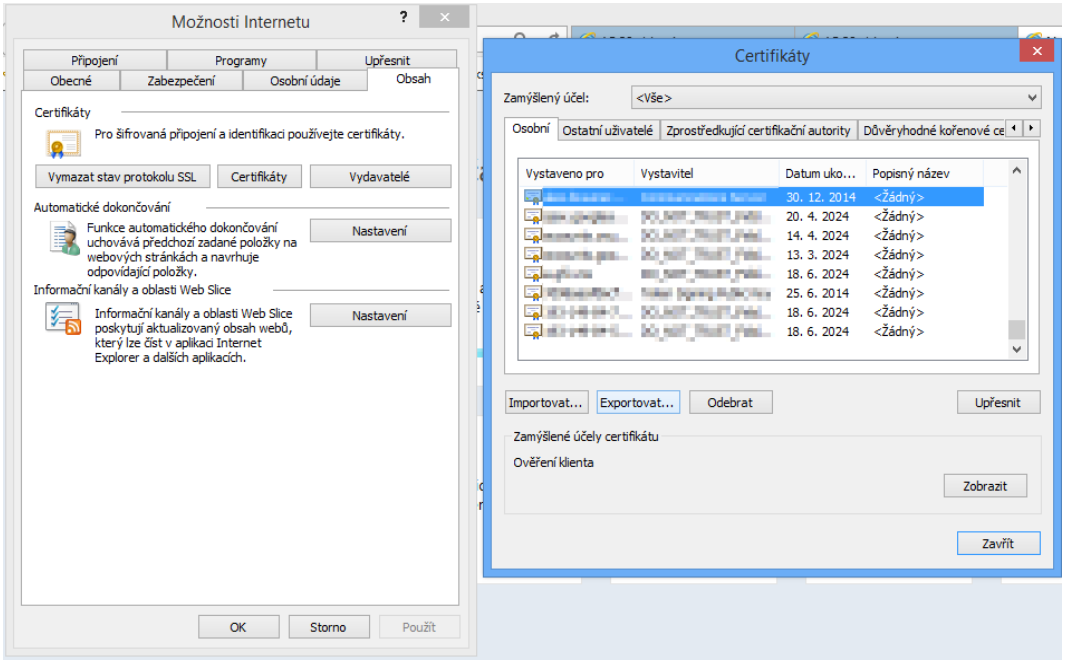
Export privátního klíče, který je uložen v úložišti certifikátů ve Windows a má nastaven příznak exportovatelnosti, je možné inicializovat více navzájem zaměnitelnými způsoby. Export nevyžaduje administrátorská oprávnění. Po spuštění samotného exportu jsou postupy totožné. Zobrazované ukázky jsou pro Windows 8.1 a prohlížeč Internet Explorer v.11.

1. Postup pomocí prohlížeče.
   1.1. V prohlížeči otevřete nabídku pro nastavení (ozubené kolečko v pravém horním rohu) a v ní vyberte „Možnosti internetu“

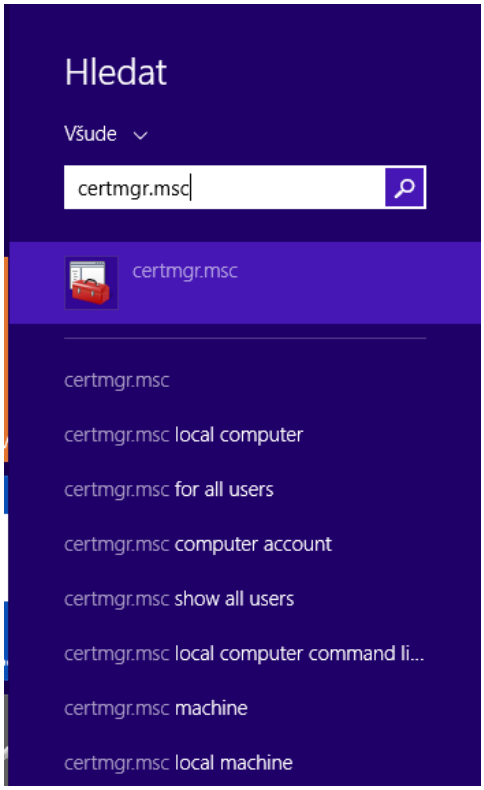


   1.2. Na záložce „*Obsah*“ klikněte na tlačítko „*Certifikáty*“. Otevře se seznam certifikátů. Vyhledejte položku, kterou chcete exportovat. Typicky se bude nacházet na první

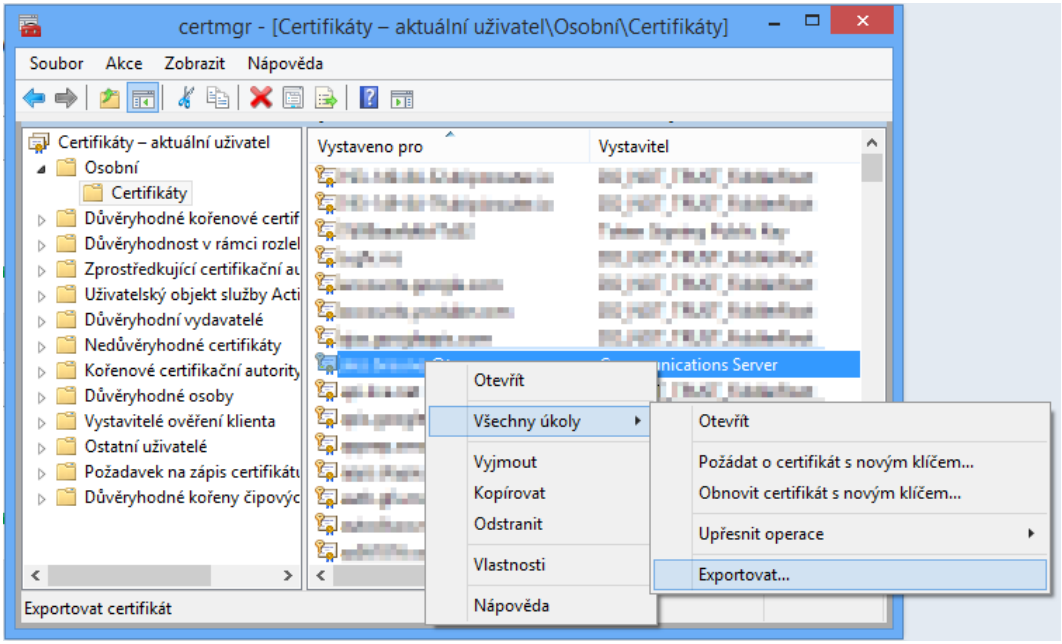
záložce „*Osobní*“. Po jejím vybrání klikněte na tlačítko „*Exportovat*“ a pokračujte bodem *3. Export klíče do souboru*.



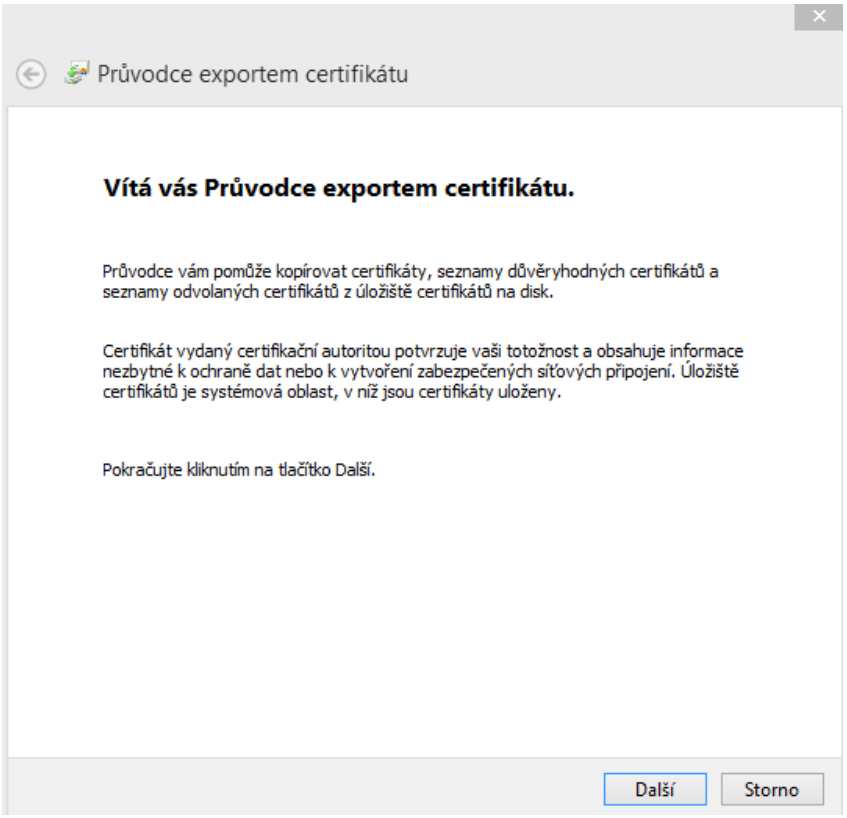
2. Postup přes konzoli
   2.1. V nabídce start vyhledejte program „*certmgr.msc*“ a spusťte jej.



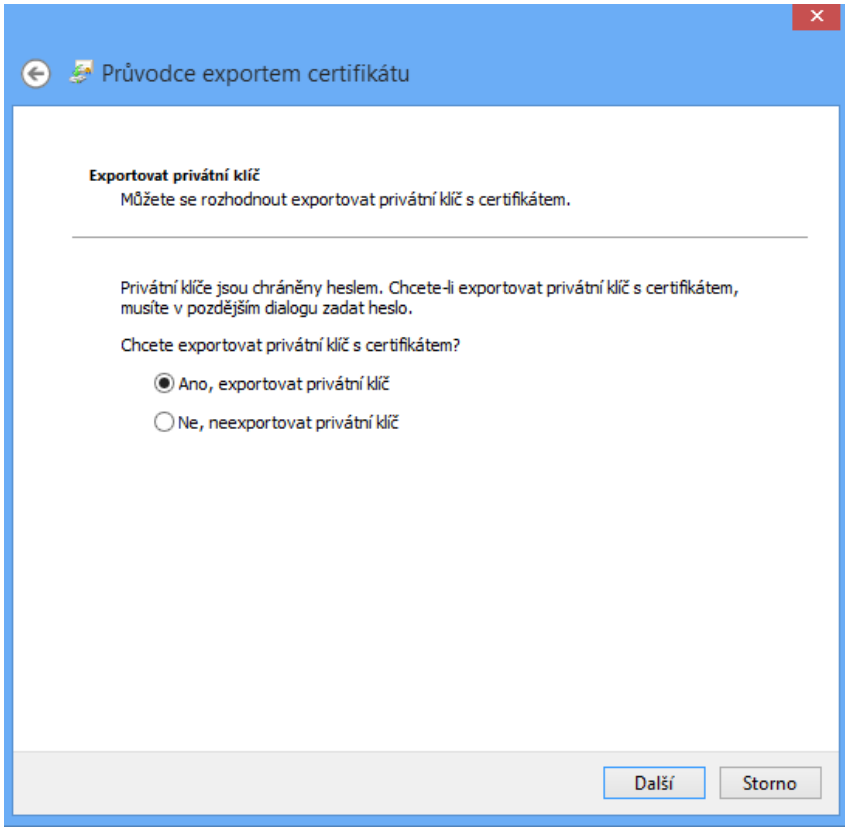
   2.2. Otevře se seznam certifikátů. Vyhledejte položku, kterou chcete exportovat. Typicky se bude nacházet v první složce „*Osobní*“ -> „*Certifikáty*“. Klikněte pravým tlačítkem na položku, vyberte možnost „*Všechny úkoly*“ a „*Exportovat*“. Pokračujte bodem *3. Export klíče do souboru*.



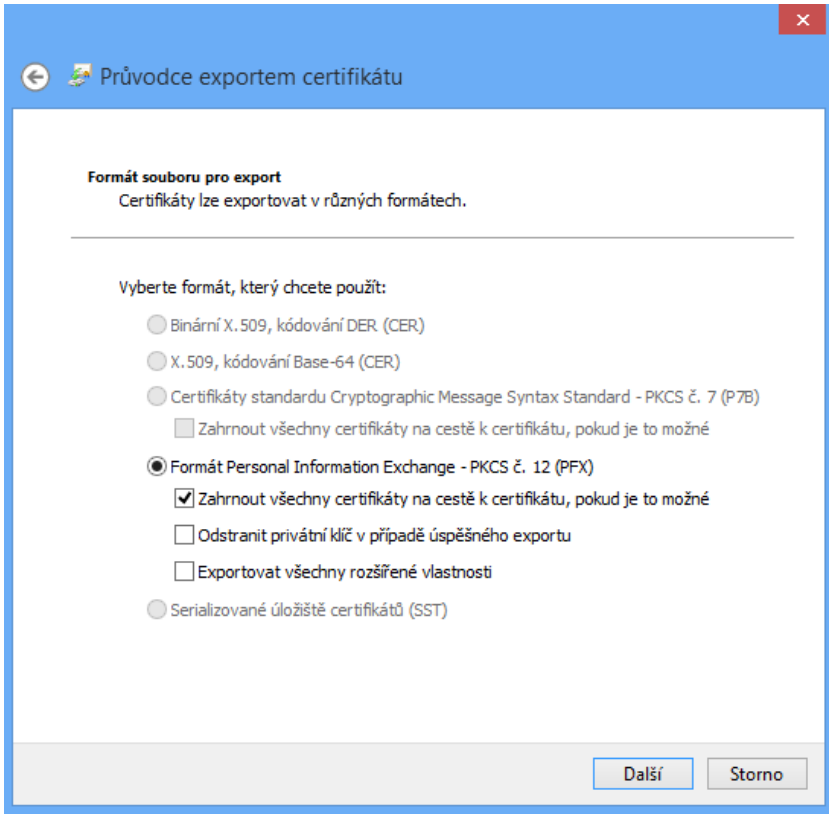
3. Export klíče do souboru
   3.1. První obrazovka po inicializaci exportu daného certifikátu:



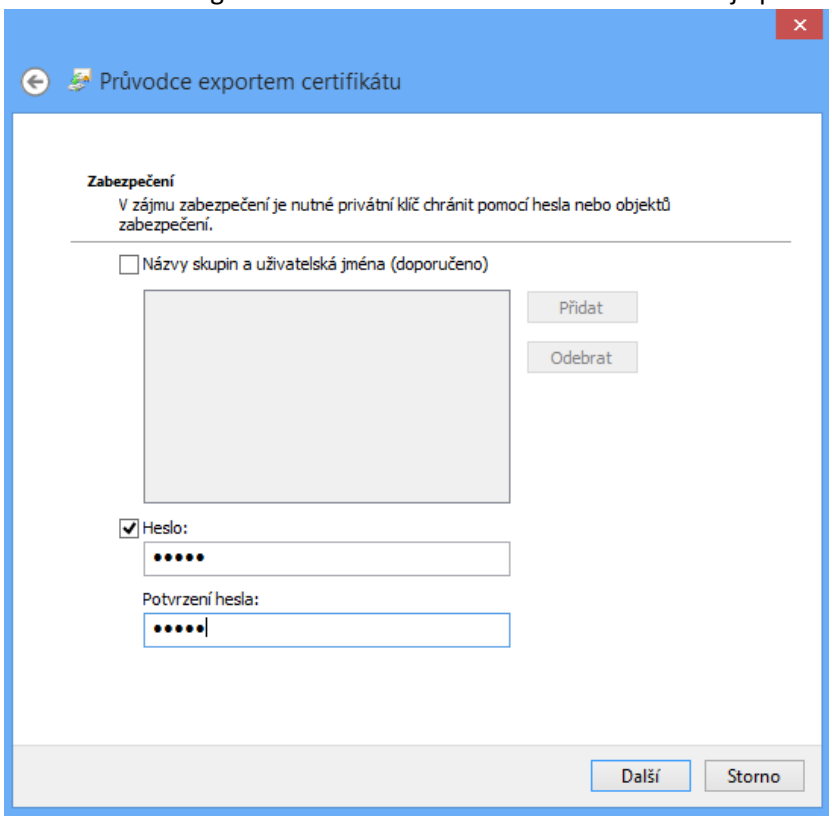
   3.2. Zvolte možnost exportování privátního klíče. Pokud nemá privátní klíč při vložení do systémového úložiště nastavenu možnost, že je exportovatelný, nebudete mít možnost si tuto volbu zvolit a dále není možné pokračovat.



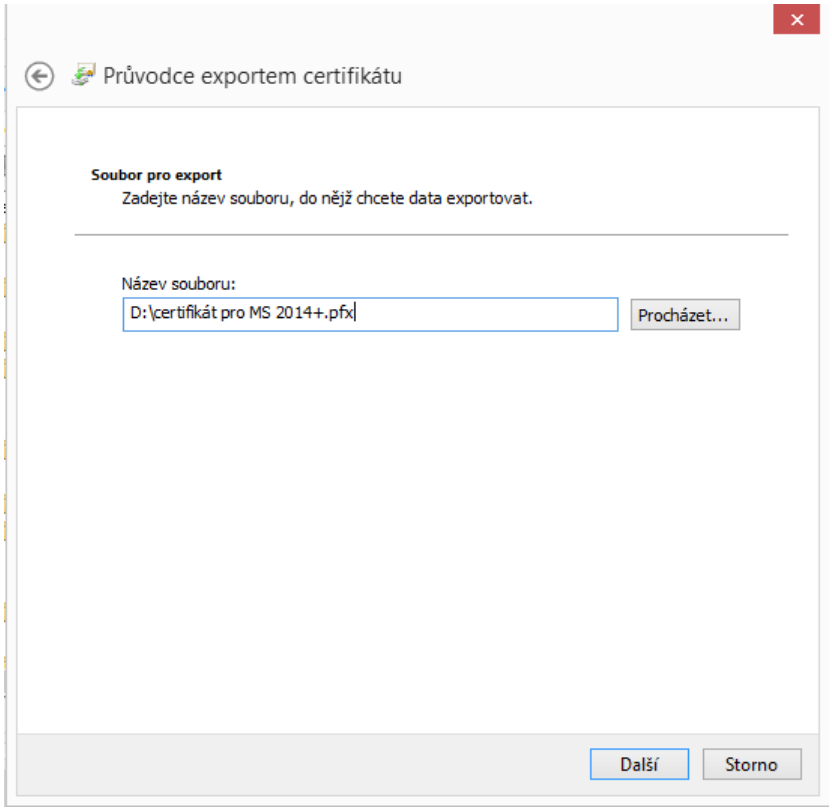
3.3. Ponechejte výchozí, nabízené nastavení. Pokud exportujete klíč z úložiště za účelem importu do bezpečnějšího způsobu uložení a nebudete chtít již dále mít tento klíč v úložišti, zvolte „Odstranit privátní klíč v případě úspěšného exportu“.



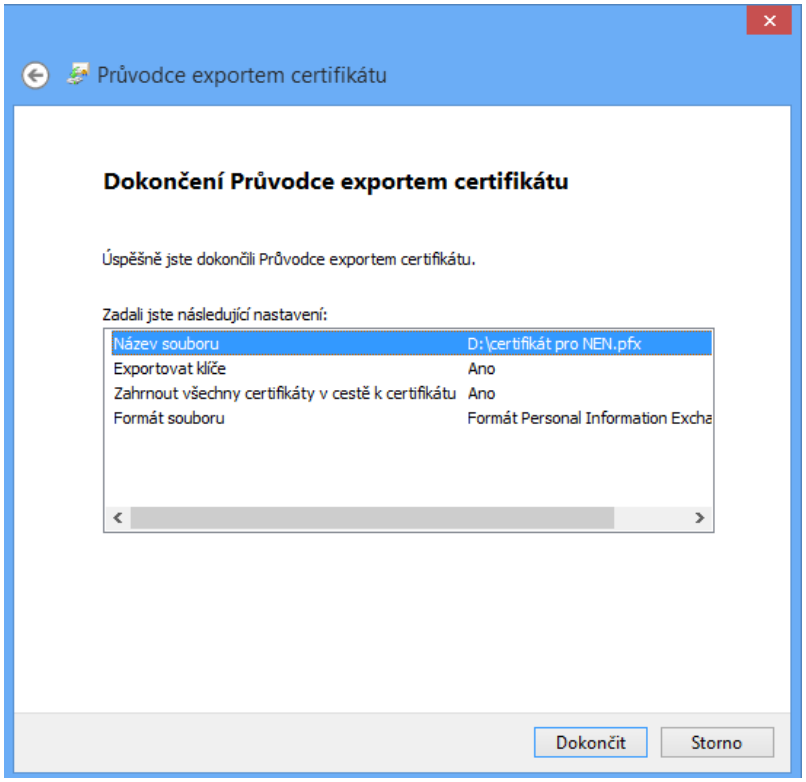
3.4. Zatrhněte možnost „*Heslo*“. Zadejte heslo. Při použití souboru s tímto klíčem budete muset zadat toto heslo. Zde zadané *Heslo* nemá žádnou souvislost s heslem zadaným během žádosti o generování certifikátu. Toto heslo se vztahuje pouze k tomuto souboru.



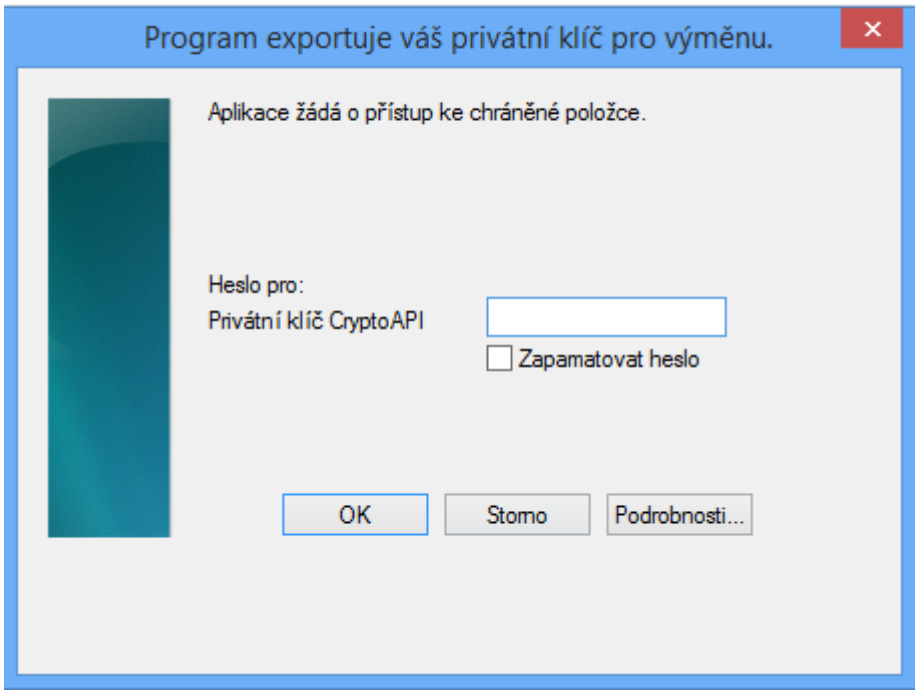
3.5. Zvolte umístění souboru.



3.6. Stiskem tlačítka Dokončit se certifikát uloží na zadané úložiště a je možné jej použít.



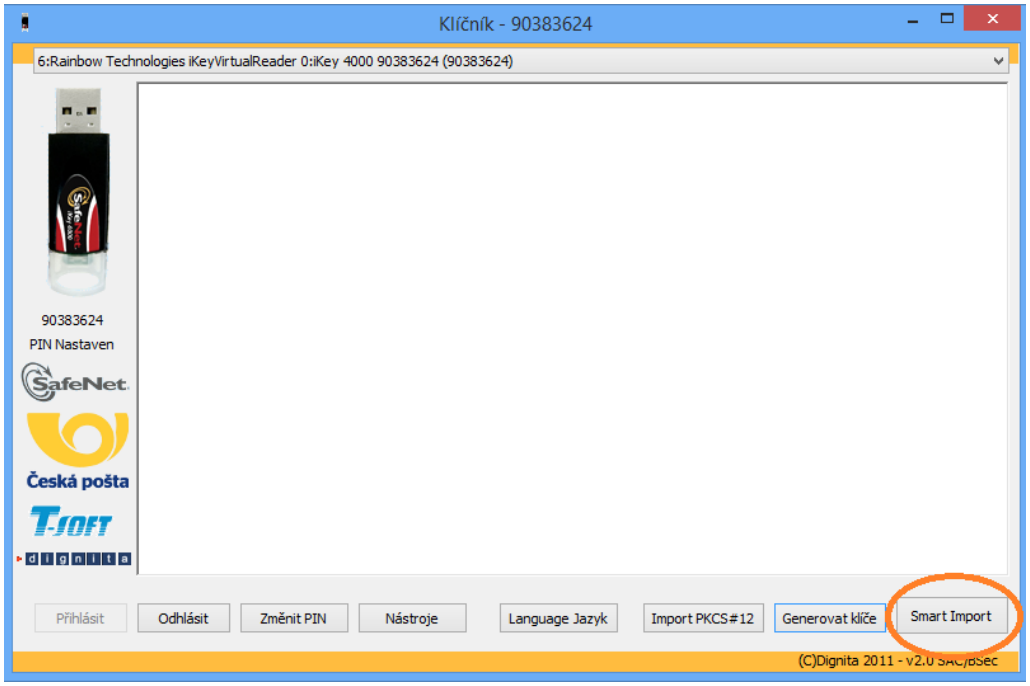
3.7. Pokud to systém vyžaduje, vyplňte v novém okně heslo, které jste zadali v rámci generování žádosti nebo které zadáváte pro jeho použití.



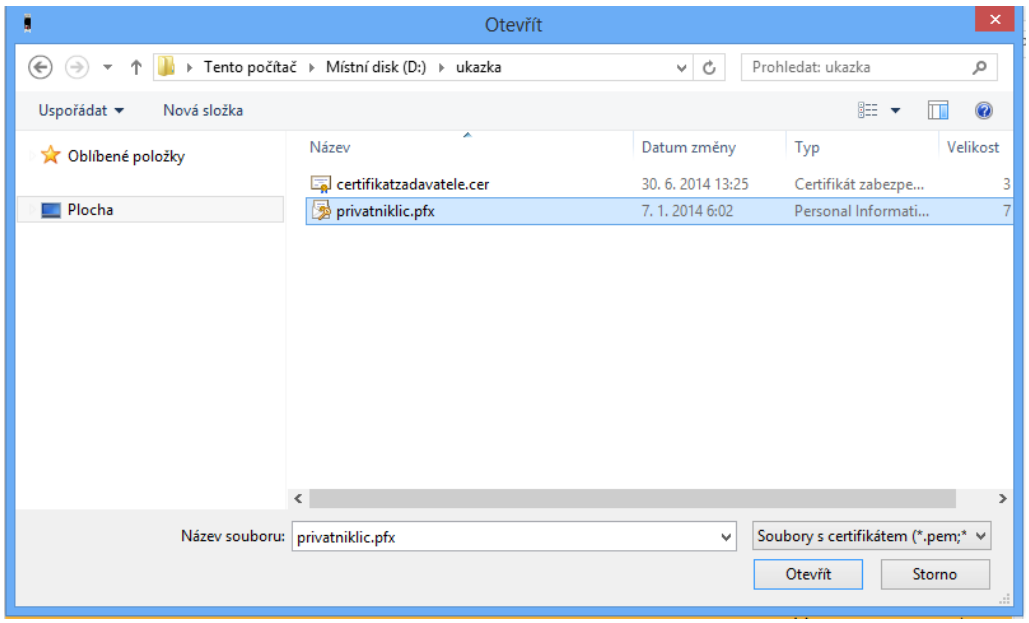
6.6 Jak naimportovat privátní klíč v souboru do virtuální čipové karty

Pro ostatní zařízení otevřete jejich obslužný program a vyhledejte možnost vložit (import). Princip importu spočítá v nalezení souboru s klíčem a zadání odpovídajícího hesla (pokud obsahuje privátní klíč). Například v programu Klíčník:

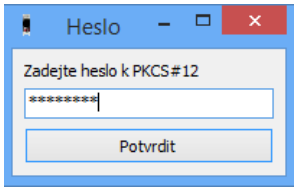
1. Zvolte možnost „Smart import“



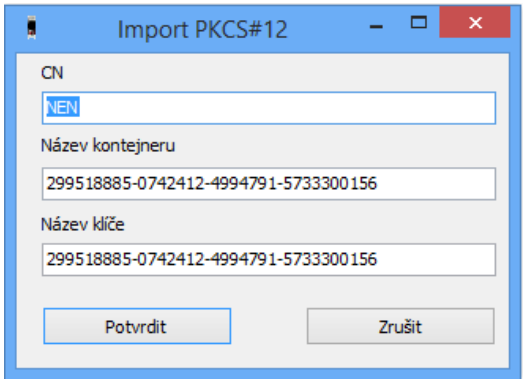
2. Vyhledejte soubor



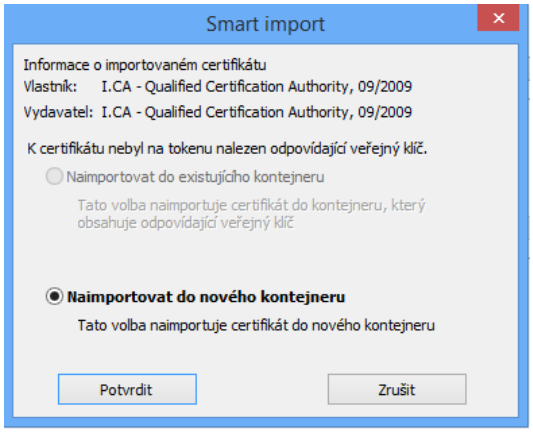
3. Pokud obsahuje privátní klíč
   3.1. vyskočí dialogové okno pro jeho zadání.



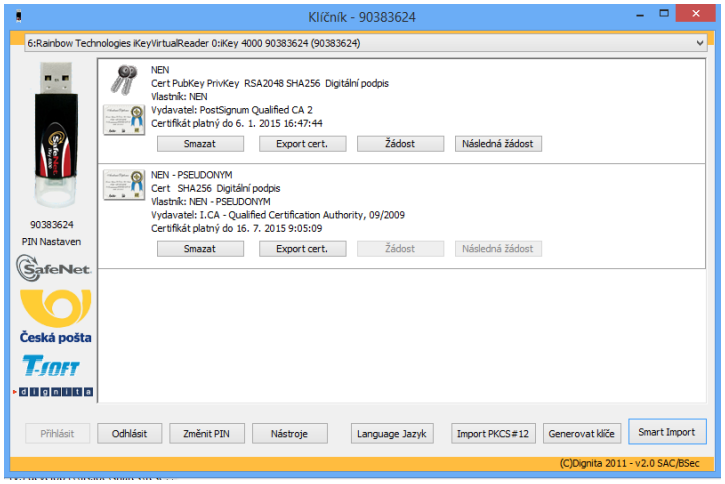
3.2. potvrďte následující dialogové okno.



4. Pokud neobsahuje privátní klíč, vyberte možnost „Naimportovat do nového kontejneru“ nebo v případě, že již je na tokenu privátní klíč, bude aktivní i první možnost (do existujícího kontejneru).



5. V tokenu se zobrazí příslušný záznam

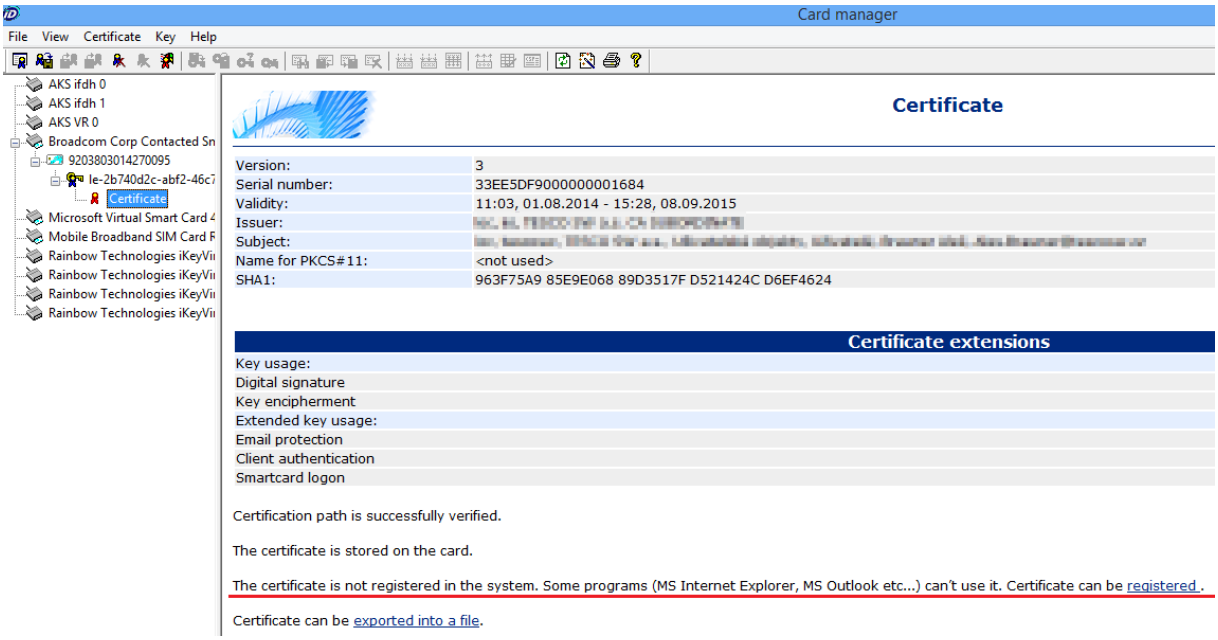


6. Soubor s privátním klíčem, pokud jej dále nepotřebujete, vymažte z počítače.

6.7 Jak zpřístupnit klíč uložený v tokenu v systémovém úložišti

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.

4. Otevřete Vás obslužný program k tokenu.
5. Vyhledejte v něm příslušný klíč.

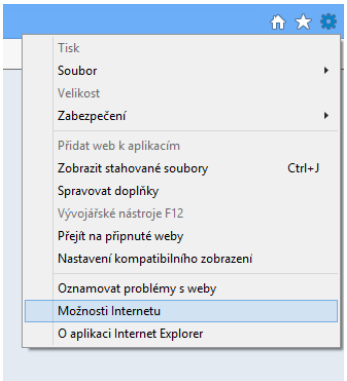


6. Pokud je certifikát nezaregistrovaný, program nabízí jeho zaregistrování. Klikněte na registraci. Nyní se klíč objevil v systémovém úložišti, složce osobní.

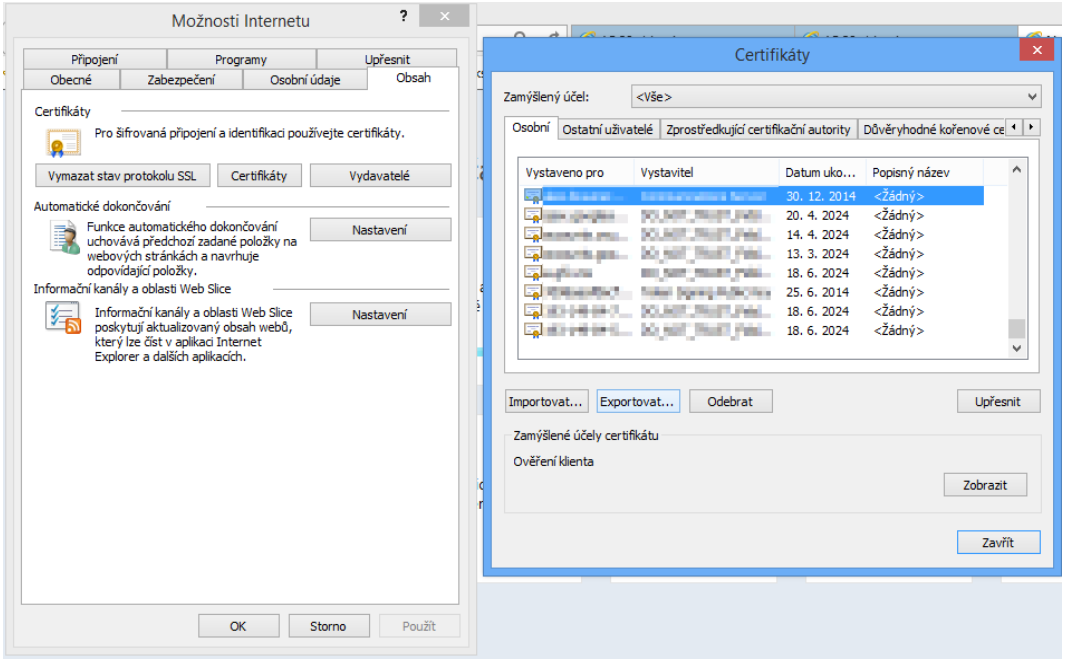
6.8 Jak exportovat privátní klíč do souboru

Export privátního klíče, který je uložen v úložišti certifikátů ve Windows a má nastaven příznak exportovatelnosti, je možné inicializovat více navzájem zaměnitelnými způsoby. Export nevyžaduje administrátorská oprávnění. Po spuštění samotného exportu jsou postupy totožné. Zobrazované ukázky jsou pro Windows 8.1 a prohlížeč Internet Explorer v.11.

4. Postup pomocí prohlížeče.
   4.1. V prohlížeči otevřete nabídku pro nastavení (ozubené kolečko v pravém horním rohu) a v ní vyberte „Možnosti internetu“

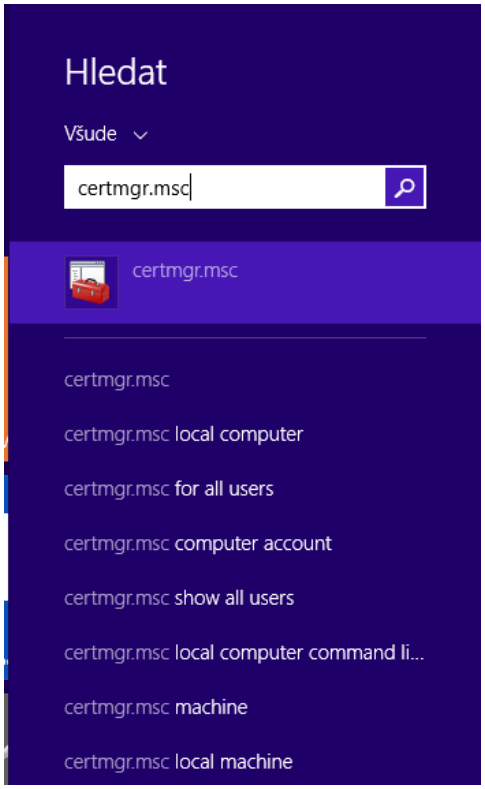


4.2. Na záložce „*Obsah*“ klikněte na tlačítko „*Certifikáty*“. Otevře se seznam certifikátů. Vyhledejte položku, kterou chcete exportovat. Typicky se bude nacházet na první záložce „*Osobní*“. Po jejím vybrání klikněte na tlačítko „*Exportovat*“ a pokračujte bodem *3.Export klíče do souboru*.



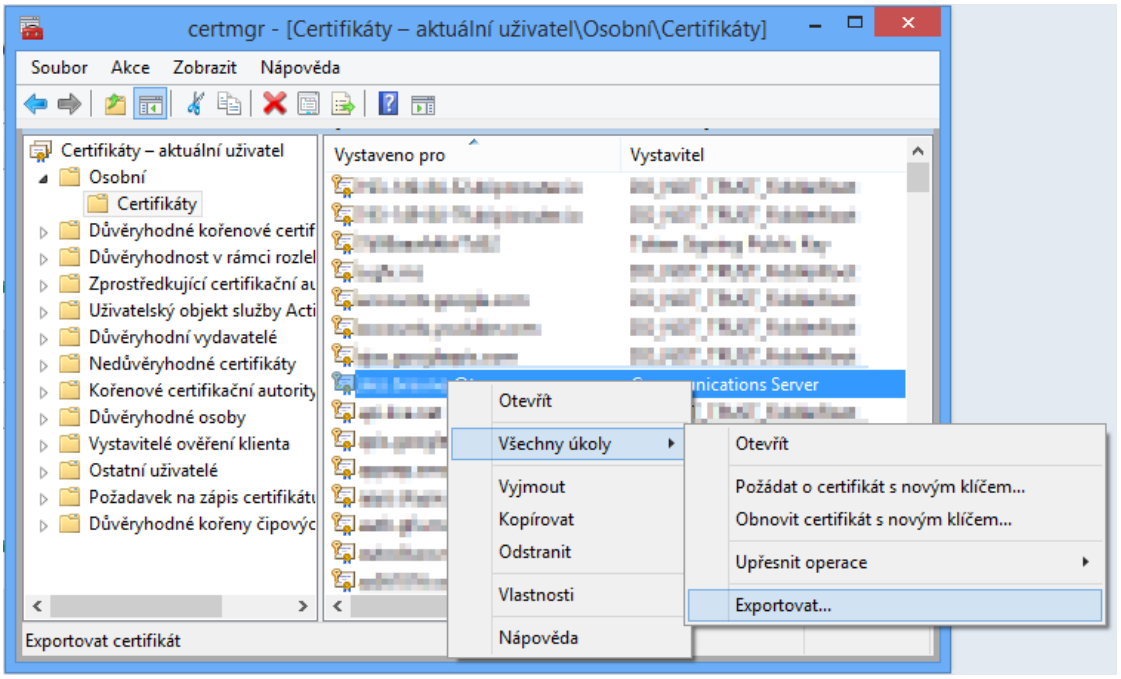
5. Postup přes konzoli

5.1. V nabídce start vyhledejte program „*certmgr.msc*“ a spusťte jej.

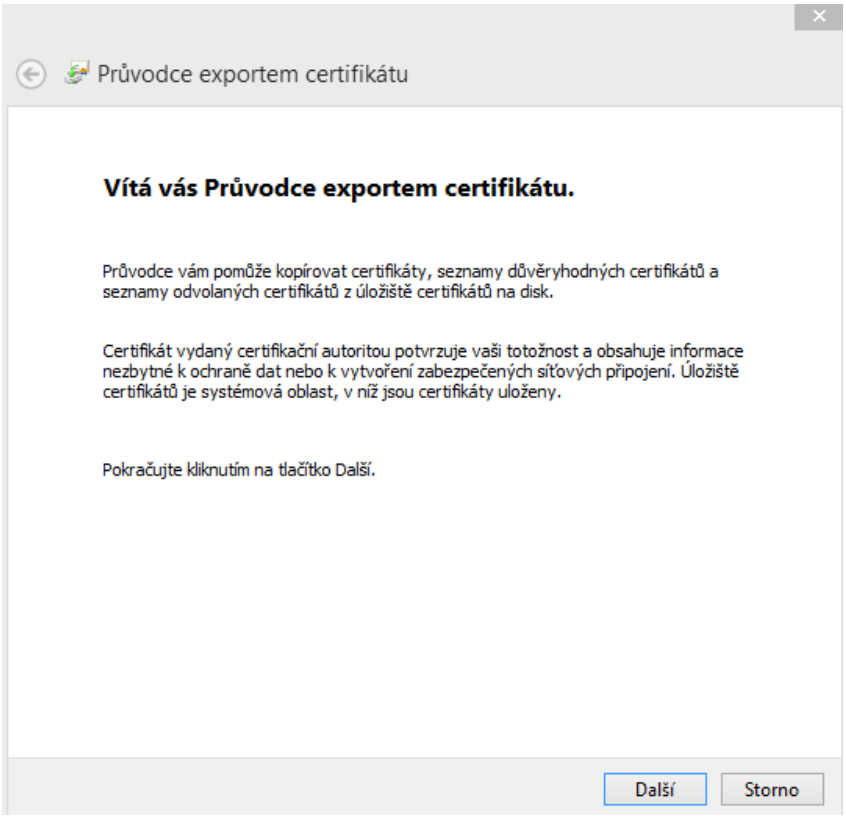


5.2. Otevře se seznam certifikátů. Vyhledejte položku, kterou chcete exportovat. Typicky se bude nacházet v první složce „*Osobní*“ -> „*Certifikáty*“. Klikněte pravým tlačítkem na položku,

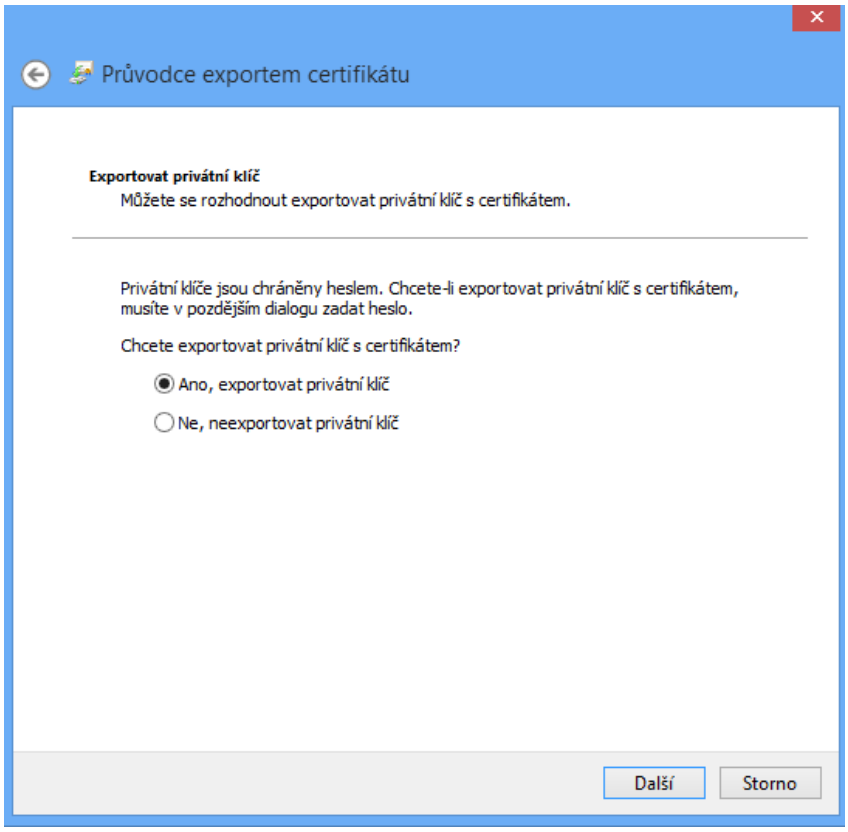
vyberte možnost *„Všechny úkoly“* a *„Exportovat“*. Pokračujte bodem *3.Export klíče do souboru*.



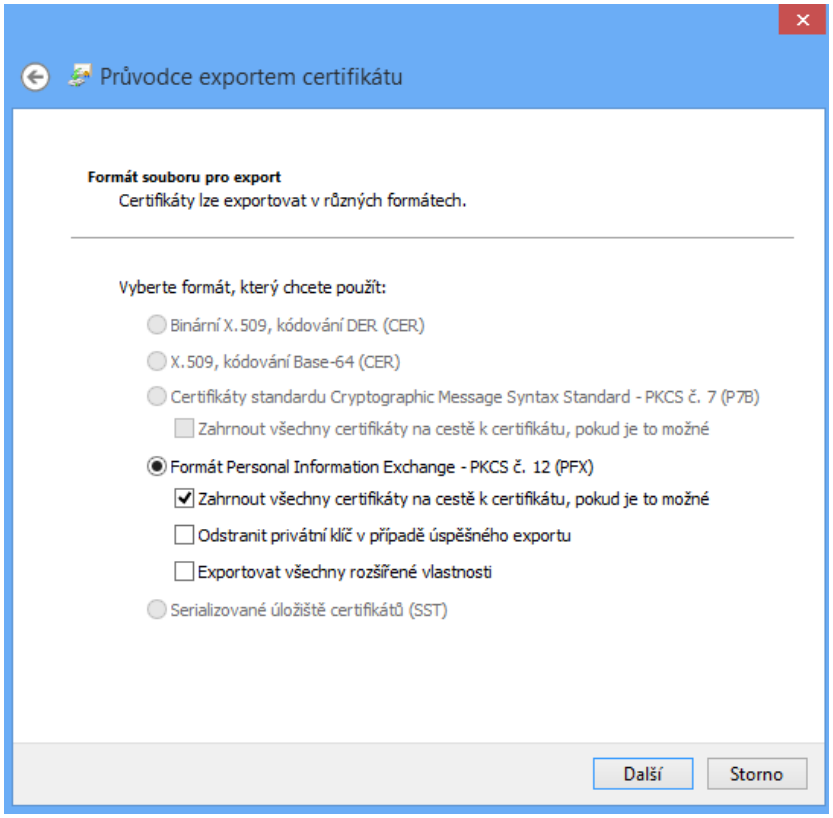
6. Export klíče do souboru
   6.1. První obrazovka po inicializaci exportu daného certifikátu:



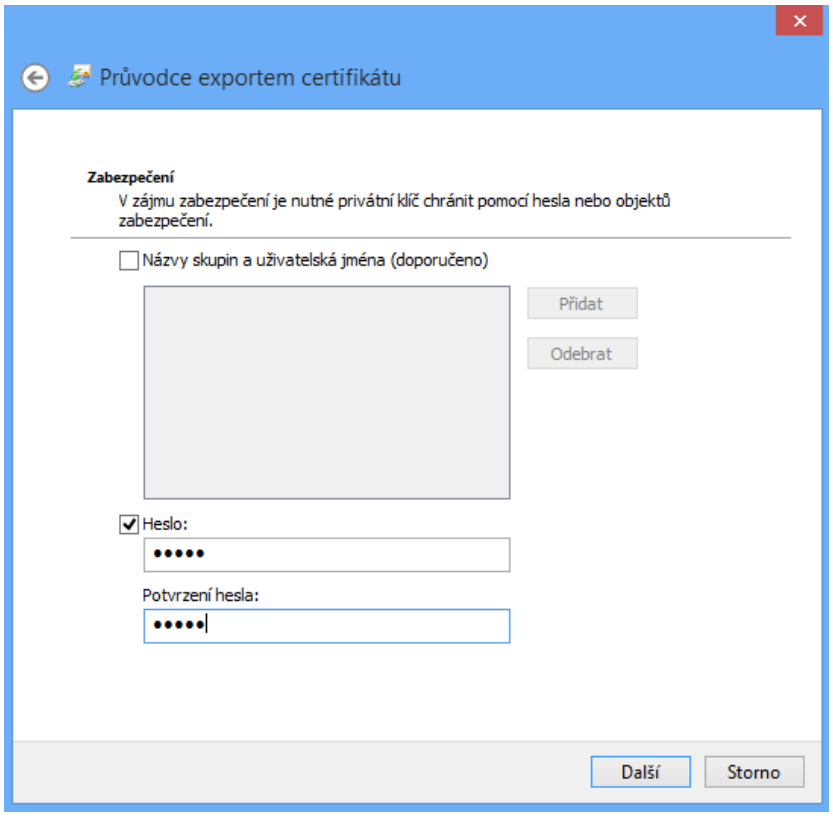
6.2. Zvolte možnost exportování privátního klíče. Pokud nemá privátní klíč při vložení do systémového úložiště nastavenu možnost, že je exportovatelný, nebudete mít možnost si tuto volbu zvolit a dále není možné pokračovat.



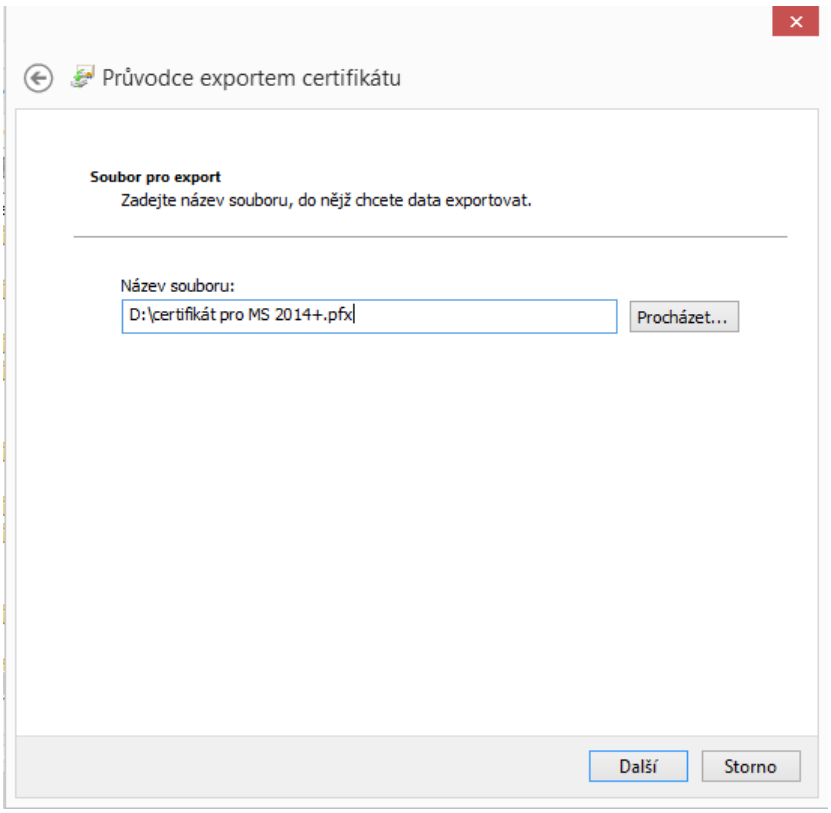
6.3. Ponechejte výchozí, nabízené nastavení. Pokud exportujete klíč z úložiště za účelem importu do bezpečnějšího způsobu uložení a nebudete chtít již dále mít tento klíč v úložišti, zvolte „Odstranit privátní klíč v případě úspěšného exportu“.



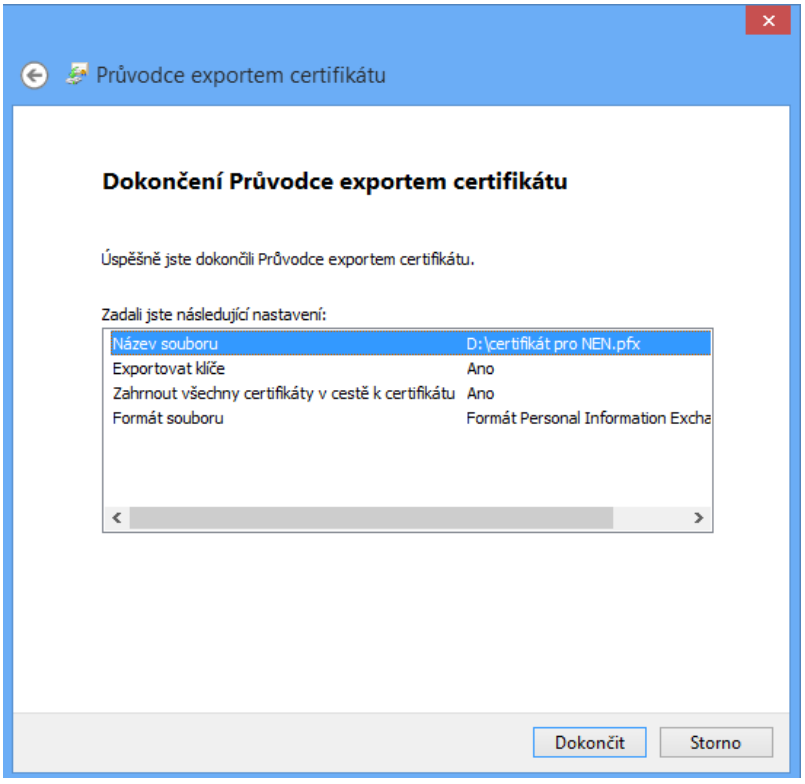
6.4. Zatrhněte možnost „*Heslo*“. Zadejte heslo. Při použití souboru s tímto klíčem budete muset zadat toto heslo. Zde zadané *Heslo* nemá žádnou souvislost s heslem zadaným během žádosti o generování certifikátu. Toto heslo se vztahuje pouze k tomuto souboru.



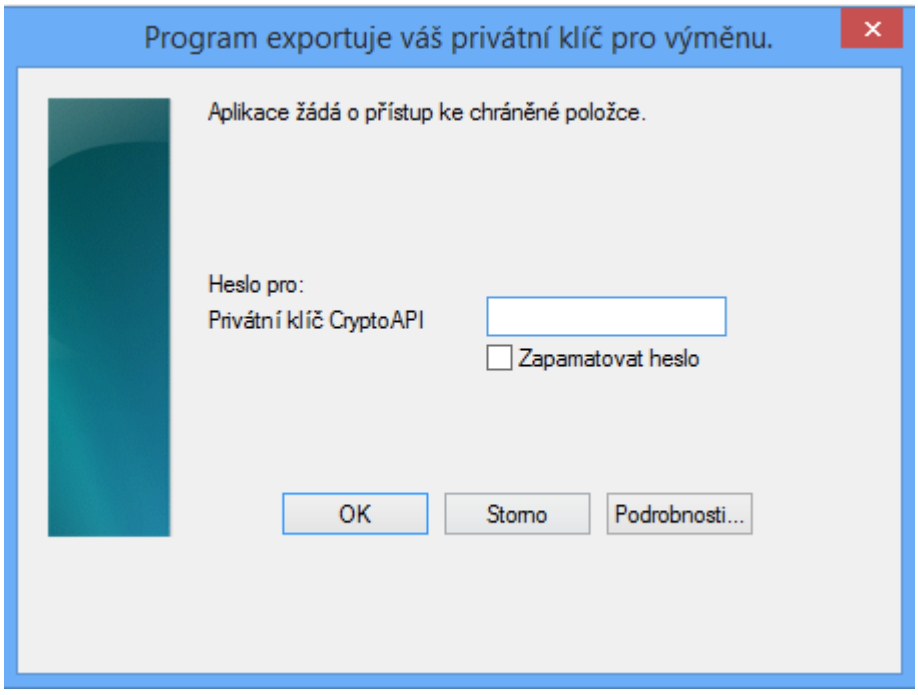
6.5. Zvolte umístění souboru.



6.6. Stiskem tlačítka Dokončit se certifikát uloží na zadané úložiště a je možné jej použít.



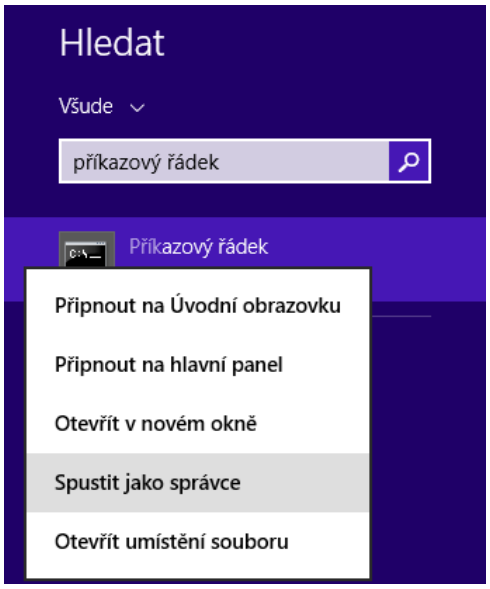
6.7. Pokud to systém vyžaduje, vyplňte v novém okně heslo, které jste zadali v rámci generování žádosti nebo které zadáváte pro jeho použití.


Program exportuje váš privátní klíč pro výměnu.
Aplikace žádá o přístup ke chráněné položce.
Heslo pro:
Privátní klíč CryptoAPI
Zapamatovat heslo
OK
Storno
Podrobnosti...

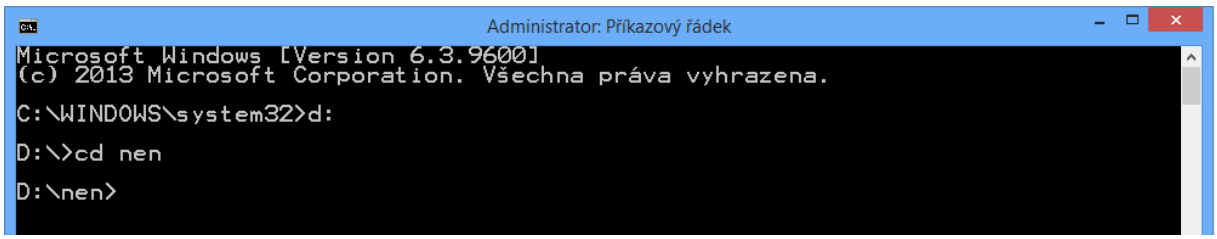
6.9 Jak naimportovat privátní klíč v souboru do virtuální čipové karty

Pokud jste negenerovali klíč přímo do virtuální čipové karty, můžete jej dodatečně naimportovat. Podmínkou je existenci privátního klíče v souboru.

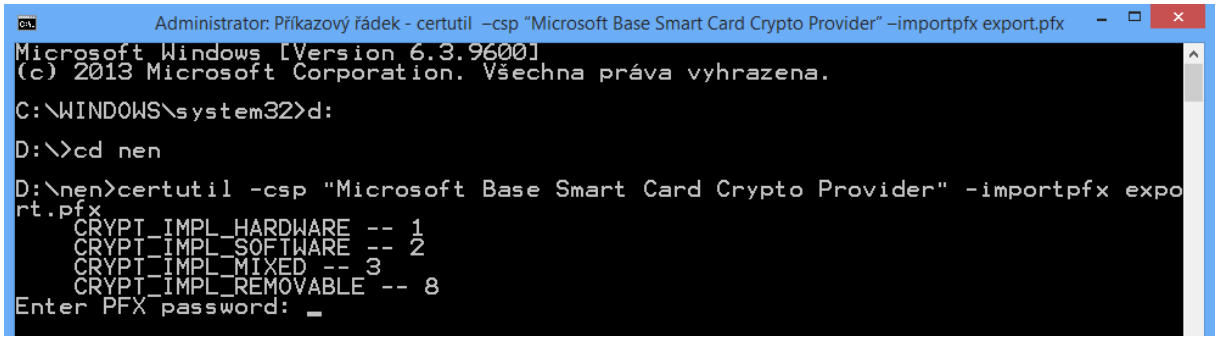
1. Doporučujeme si soubor uložit do snadno dostupné složky. V návodu se jedná o složku MS 2014+ na disku D (D:/MS 2014+/).
2. Spusťte příkazový řádek v administrátorském režimu. Po vyhledání klikněte pravým tlačítkem a vyberte „Spustit jako správce“.



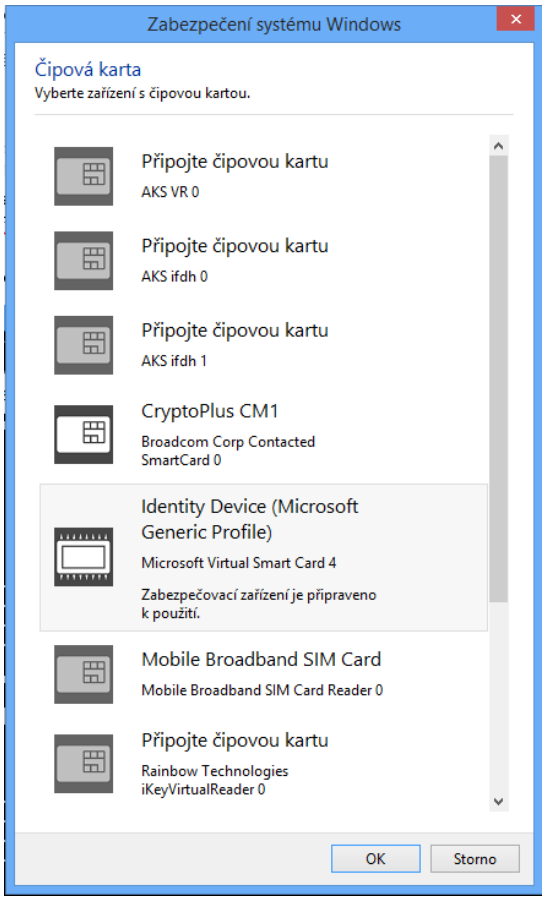
3. Pomocí příkazů příkazového řádku otevřete příslušnou složku na počítači, která obsahuje vyexportovaný soubor s privátním klíčem. V příkladu je uveden postup, jak přejít na jiný disk a otevřít složku.



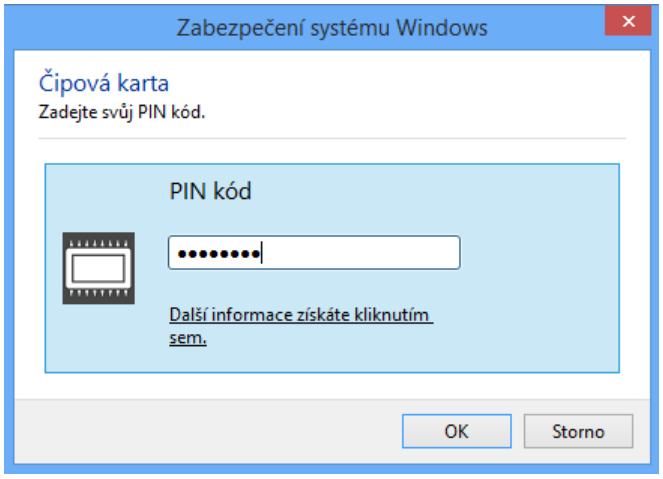
4. Spusťte příkaz *certutil –csp “Microsoft Base Smart Card Crypto Provider” –importpfx {PFXfile}*. Místo {PFXfile} zadejte skutečný název souboru. V příkladu se jedná o soubor „export.pfx“. Pokud je vypsáno, že požadovaná informace vyžaduje zvýšená oprávnění, neprovedli jste v bodu 3 všechny požadavky. Dále zadejte heslo k souboru, které jste zadali v rámci kroku 2.



5. Pokud máte na počítači jiné čipové karty nebo tokeny, vyskočí dialogové okno pro výběr správného tokenu. Virtuální čipová karta má svou unikátní ikonu, která pomůže v identifikaci.



6. Po stisku tlačítka OK vyskočí další dialogové okno pro zadání PIN virtuální čipové karty. Tento PIN budete zadávat vždy při požadavku o použití této virtuální čipové karty.



7. Certifikát je nyní zaregistrován v systémovém úložišti aktuálního uživatele, v části osobní. Vymažte z disku soubor s privátním klíčem!

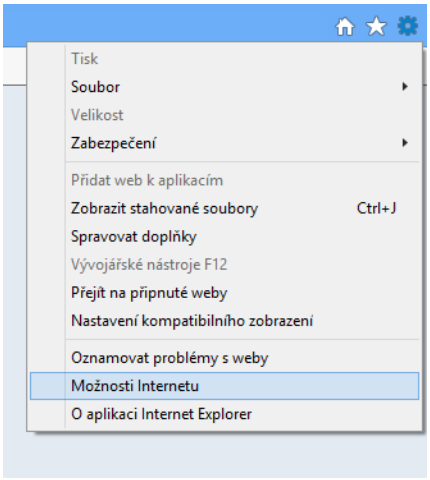
```
D:\nen>certutil -csp "Microsoft Base Smart Card Crypto Provider" -importpfx expo
rt.pfx
    CRYPT_IMPL_HARDWARE -- 1
    CRYPT_IMPL_SOFTWARE -- 2
    CRYPT_IMPL_MIXED -- 3
    CRYPT_IMPL_REMOVABLE -- 8
Enter PFX password:
Certificate "NEN - PSEUDONYM" added to store.

CertUtil: -importPFX command completed successfully.
```

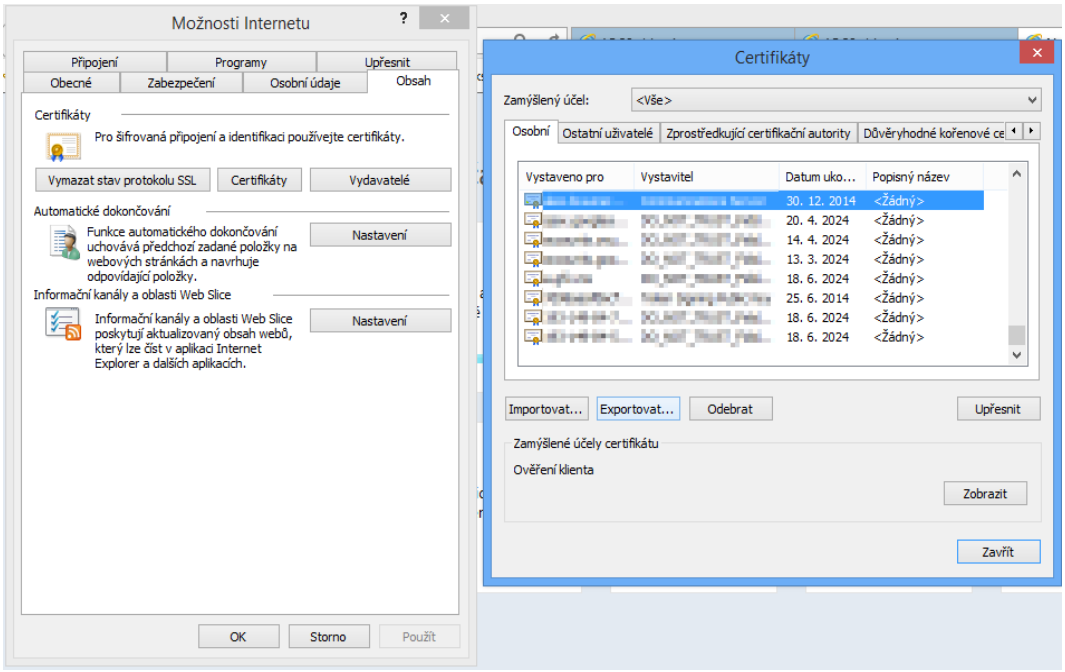
6.10 Jak exportovat veřejný klíč s certifikátem do souboru

Inicializaci exportu je možné provést několika způsoby:

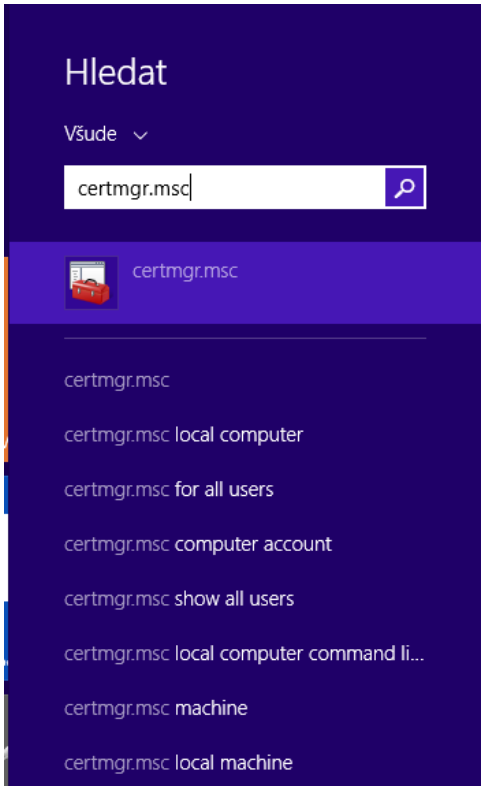
1. Pomocí prohlížeče.
   1.1. V prohlížeči otevřete nabídku pro nastavení a v ní vyberte „*Možnosti internetu*“



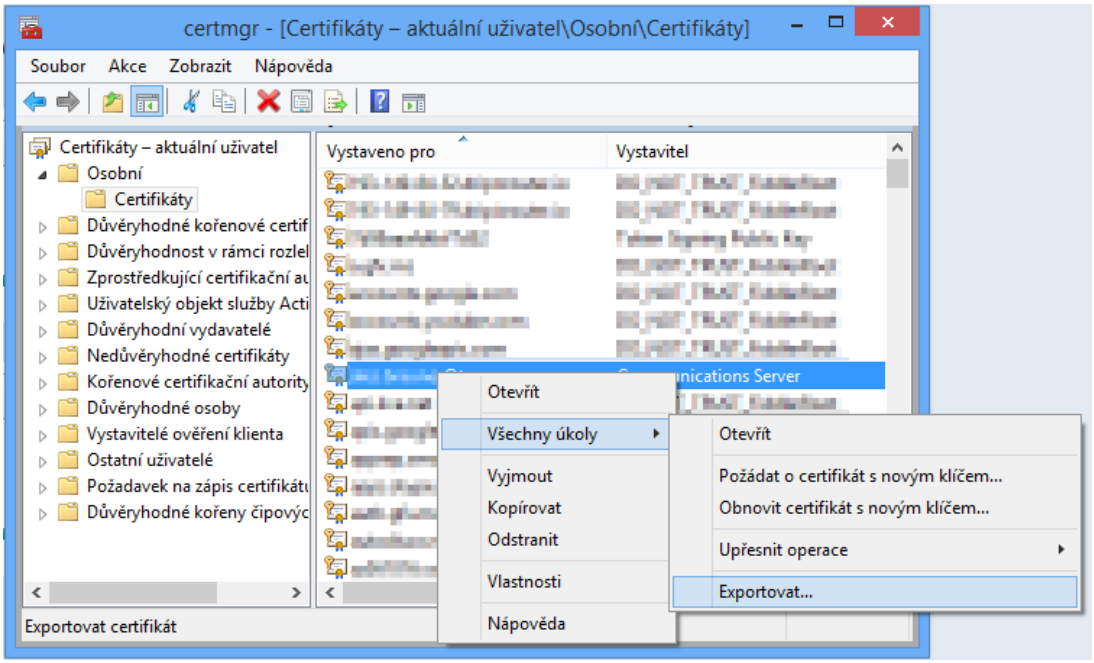
   1.2. Na záložce „*Obsah*“ klikněte na tlačítko „*Certifikáty*“. Otevře se seznam certifikátů. Vyhledejte položku, kterou chcete exportovat. Typicky se bude nacházet na první záložce „*Osobní*“. Po jejím vybrání klikněte na tlačítko „*Exportovat*“ a pokračujte bodem *3. Export certifikátu do souboru.*



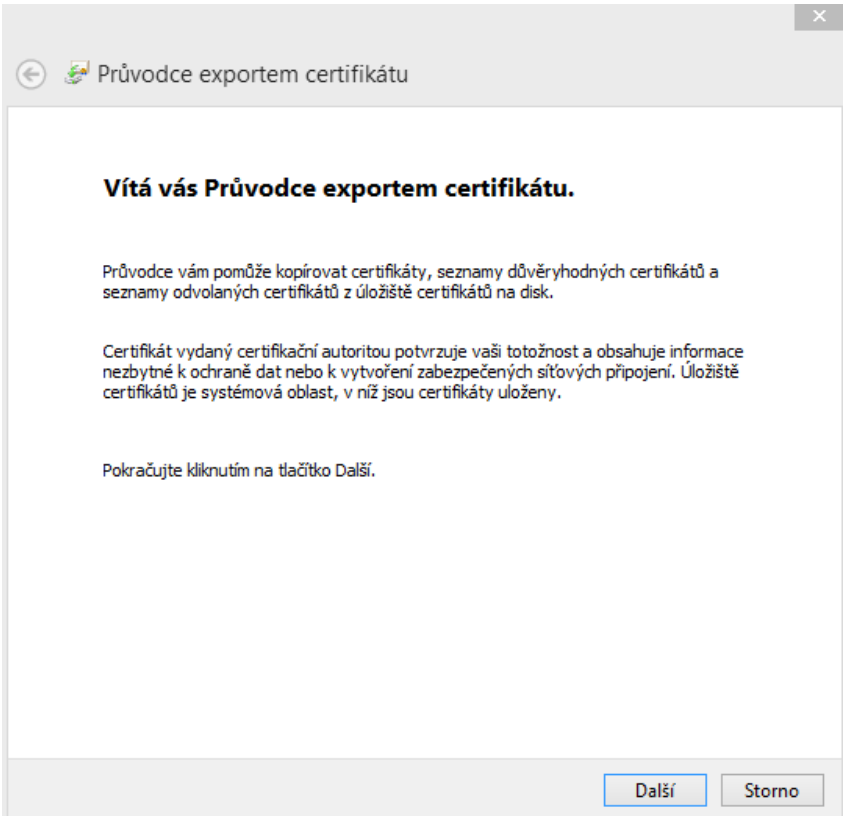
2. Přes konzoli:
   2.1. V nabídce start vyhledejte program „certmgr.msc“ a spusťte jej.



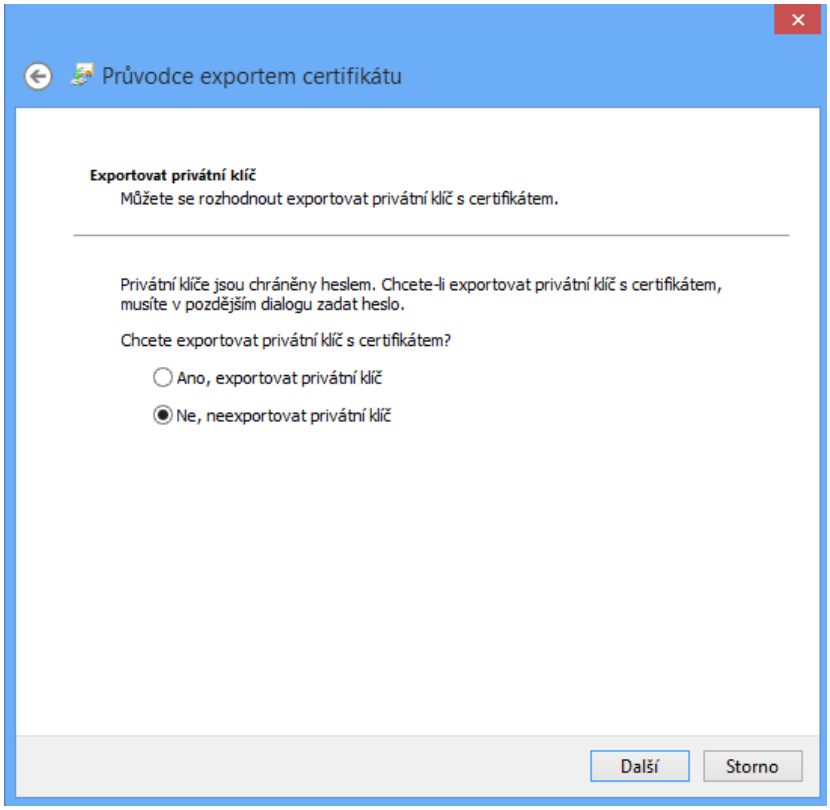
   2.2. Otevře se seznam certifikátů. Vyhledejte položku, kterou chcete exportovat. Typicky se bude nacházet v první složce „*Osobní*“ -> „*Certifikáty*“. Klikněte pravým tlačítkem na položku, vyberte možnost „*Všechny úkoly*“ a „*Exportovat*“. Pokračujte bodem *3. Export certifikátu do souboru.*


certmgr - [Certifikáty – aktuální uživatel\Osobní\Certifikáty]
Soubor
Akce
Zobrazit
Nápověda
Certifikáty – aktuální uživatel
Osobní
Certifikáty
Důvěryhodné kořenové certif
Důvěryhodnost v rámci rozlel
Zprostředkující certifikační au
Uživatelský objekt služby Acti
Důvěryhodní vydavatelé
Nedůvěryhodné certifikáty
Kořenové certifikační autority
Důvěryhodné osoby
Vystavitelé ověření klienta
Ostatní uživatelé
Požadavek na zápis certifikátu
Důvěryhodné kořeny čipových
Vystaveno pro
Vystavitel
Otevřít
Všechny úkoly
Vyjmout
Kopírovat
Odstranit
Vlastnosti
Nápověda
Otevřít
Požádat o certifikát s novým klíčem...
Obnovit certifikát s novým klíčem...
Upřesnit operace
Exportovat...
Exportovat certifikát

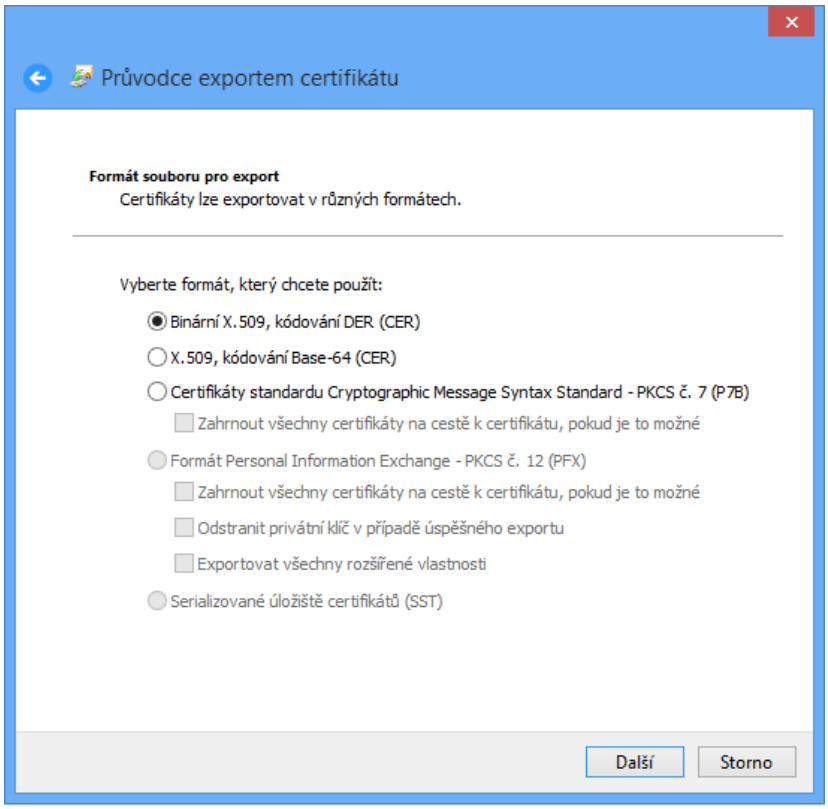
3. Export certifikátu do souboru
   3.1. První obrazovka po inicializaci exportu daného certifikátu:



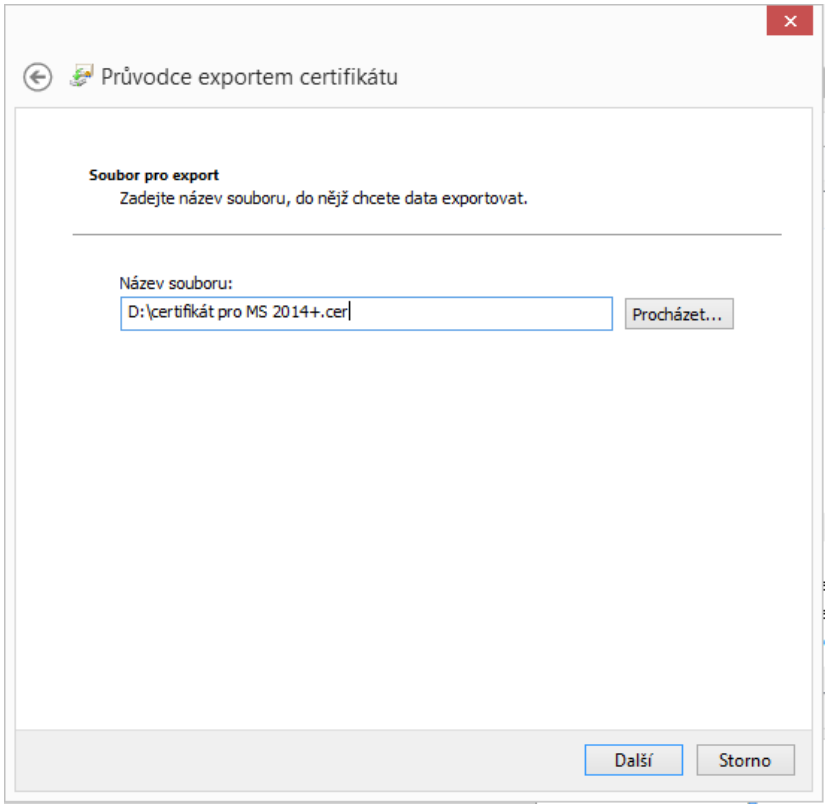
   3.2. Tento formulář se objeví pouze v případě, pokud v úložišti máte i privátní klíč. Zvolte možnost NE, neexportovat privátní klíč.



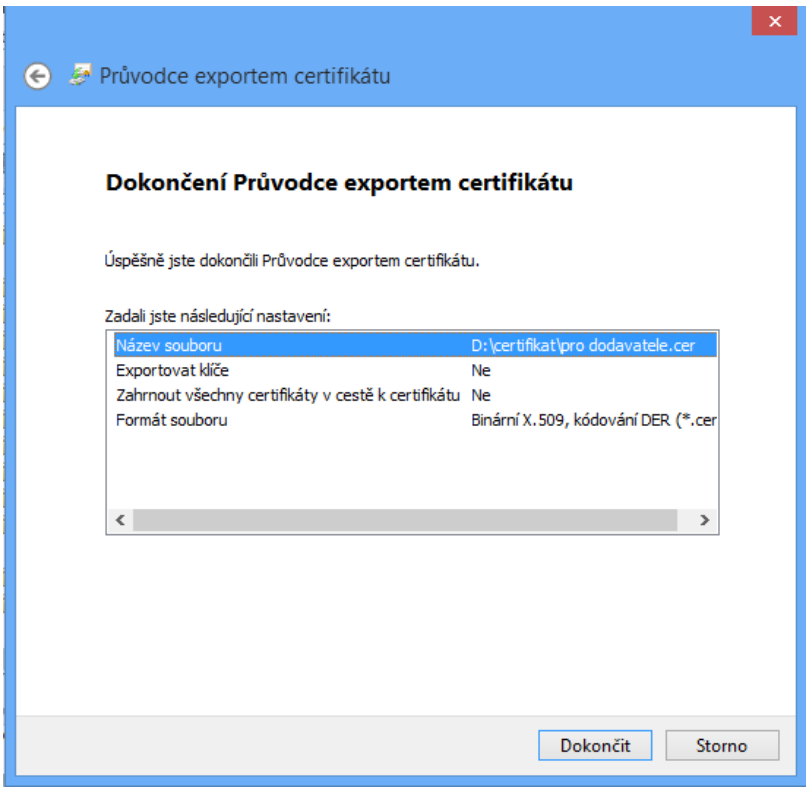
3.3. Ponechejte výchozí, nabízené nastavení Binární X.509, kódování DER (CER).



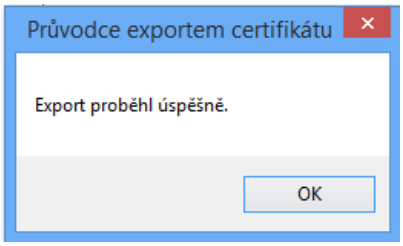
3.4. Zvolte název a umístění certifikátu. Zkontrolujte, že má certifikát příponu .cer


Průvodce exportem certifikátu
Soubor pro export
Zadejte název souboru, do nějž chcete data exportovat.
Název souboru:
D:\certifikát pro MS 2014+.cer
Procházet...
Další
Storno

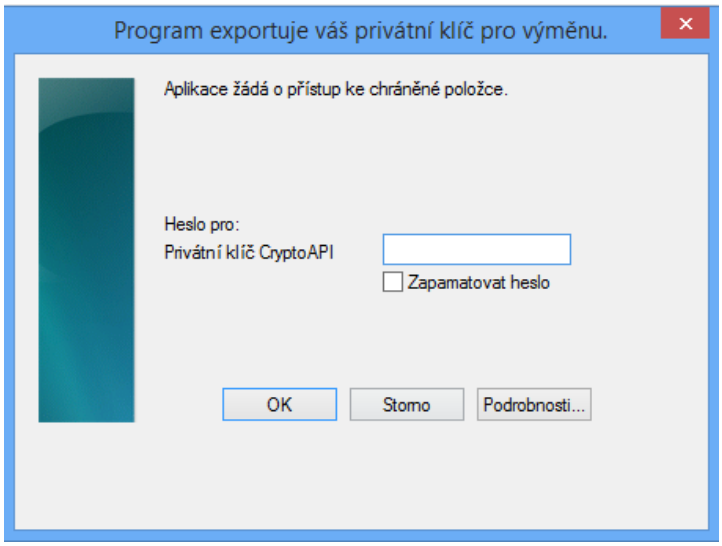
3.5. Stiskem tlačítka Dokončit se certifikát uloží a je možné jej použít.



3.6. Zobrazí se potvrzení o exportu



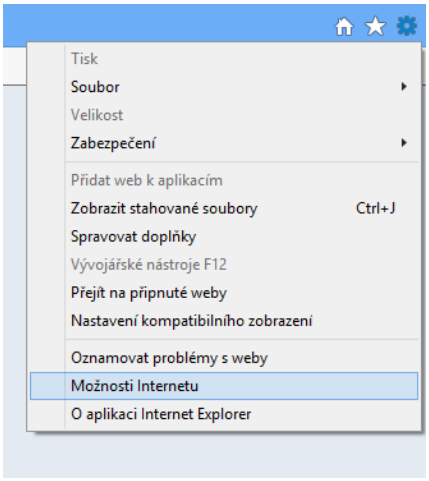
3.7. Tento formulář se objeví pouze v případě, že na počítači máte uložen privátní klíč a pokud byla v žádosti o certifikát zaškrtnuta volba změny zabezpečení nebo u již uloženého certifikátu byla tato možnost nastavena.


Program exportuje váš privátní klíč pro výměnu.
Aplikace žádá o přístup ke chráněné položce.
Heslo pro:
Privátní klíč CryptoAPI
Zapamatovat heslo
OK
Storno
Podrobnosti...

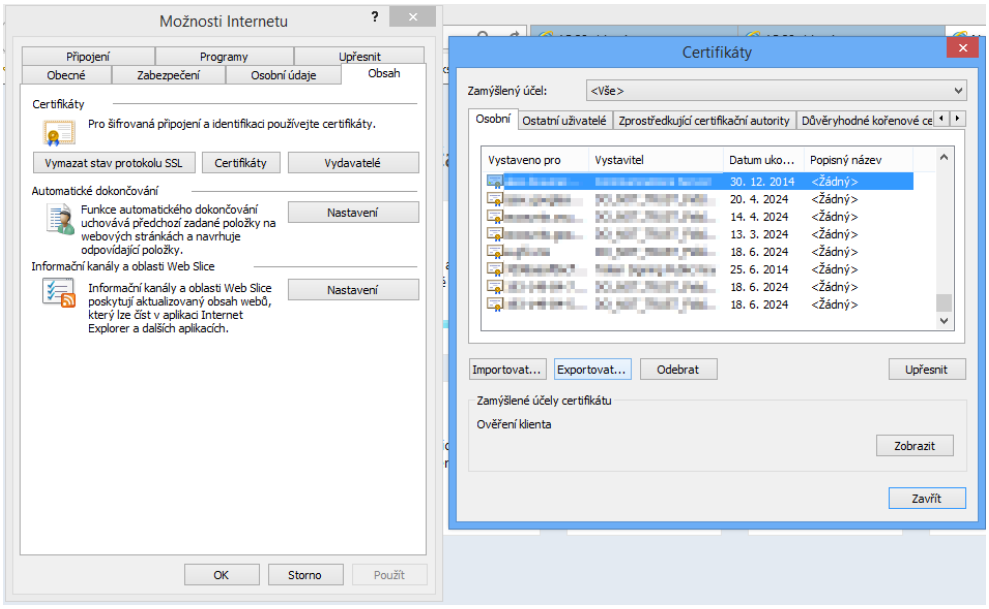
6.11 Jak importovat veřejný klíč s certifikátem do systémového úložiště

Tuto činnost by měl provádět zadavatel a dodavatelům by měl poskytovat certifikát ve tvaru, který aplikace požaduje. Je možné jej použít při importu certifikátu pro účely konverze do požadovaného formátu nebo pro účely uložení do úložiště operačního systému.

1. Inicializaci importu certifikátu je možné provést několika způsoby.
   1.1. Prohlížeč
      1.1.1. V prohlížeči otevřete nabídku pro nastavení a v ní vyberte „*Možnosti internetu*“

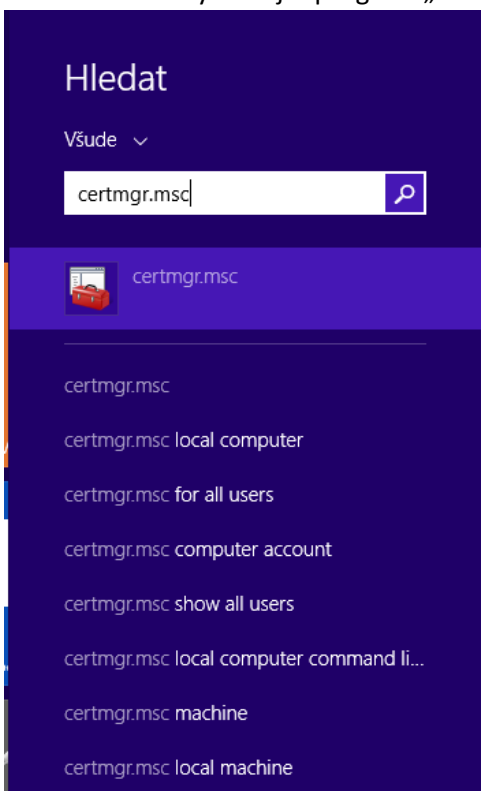


      1.1.2. Na záložce „*Obsah*“ klikněte na tlačítko „*Certifikáty*“. Otevře se seznam certifikátů. Vyberte složku, kam chcete certifikát naimportovat. Například „*Ostatní uživatelé*“. Klikněte na tlačítko „*Importovat*“. Pokračujte bodem *2. Samotný import*.

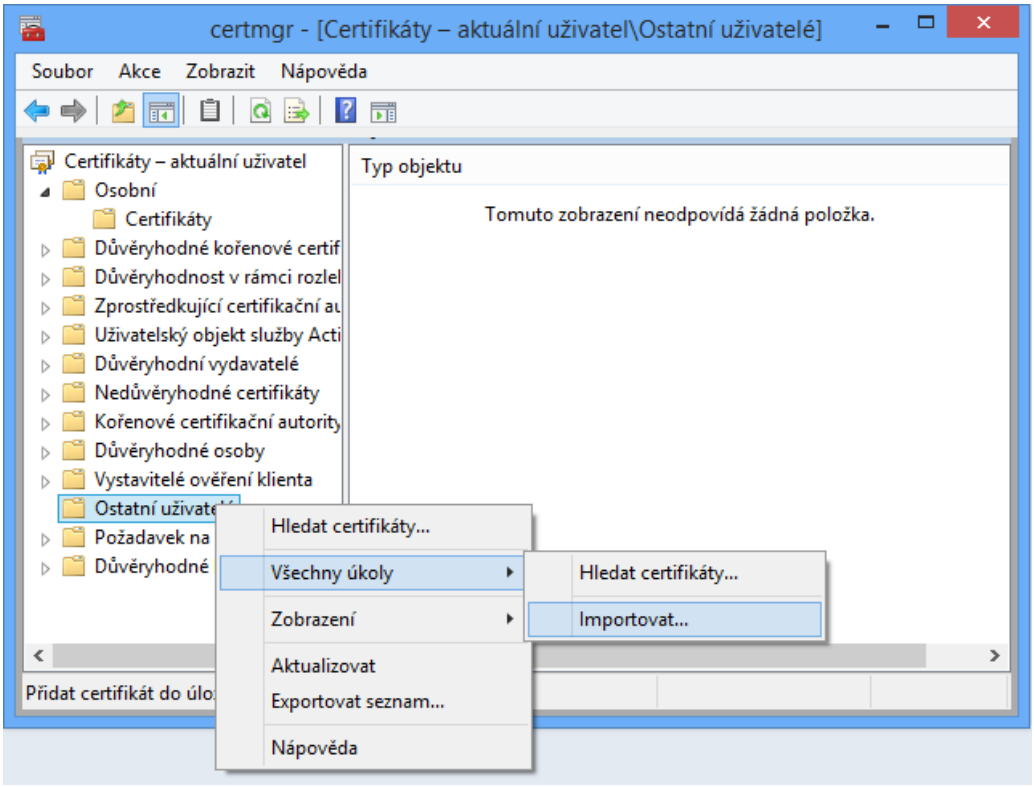


1.2. Přes konzoli

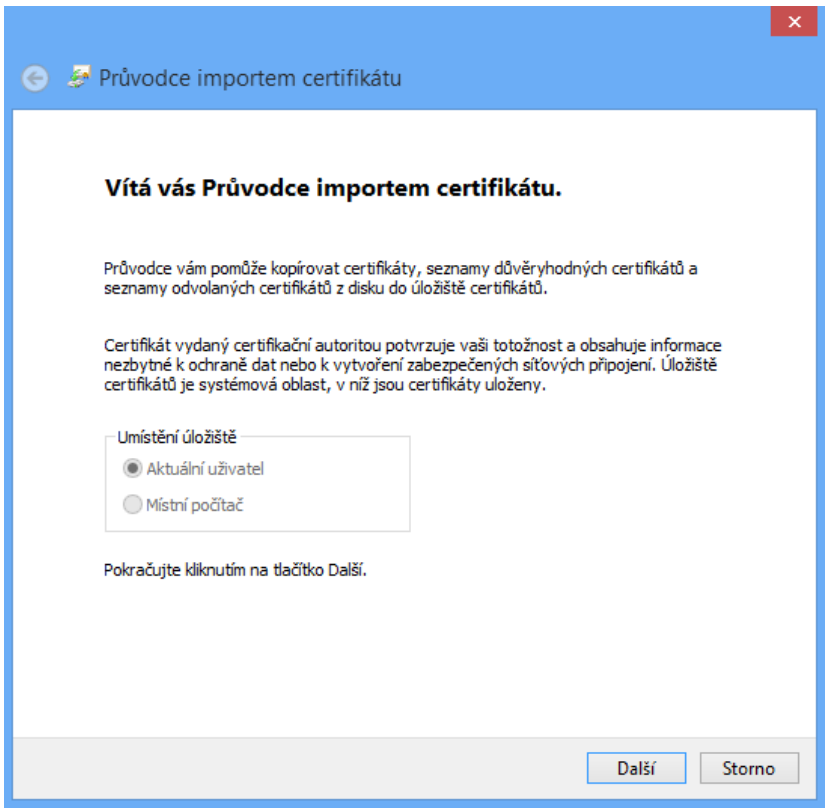
1.2.1. V nabídce start vyhledejte program „certmgr.msc“ a spusťte jej.



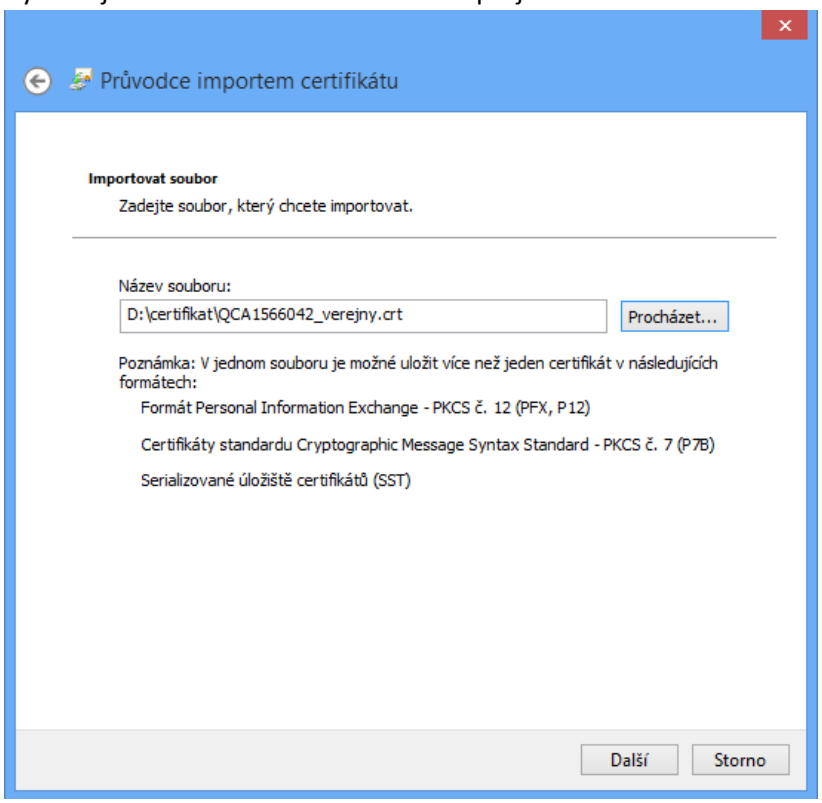
1.2.2. Otevře se seznam certifikátů. Vyberte složku, kam chcete certifikát naimportovat. Vyberte *„ostatní uživatelé“*. Klikněte pravým tlačítkem na tuto složku a přes volbu *„Všechny úkoly“* a *„Importovat“* spusťte import. Pokračujte bodem *2. Samotný import***Chyba! Nenalezen zdroj odkazů.**.



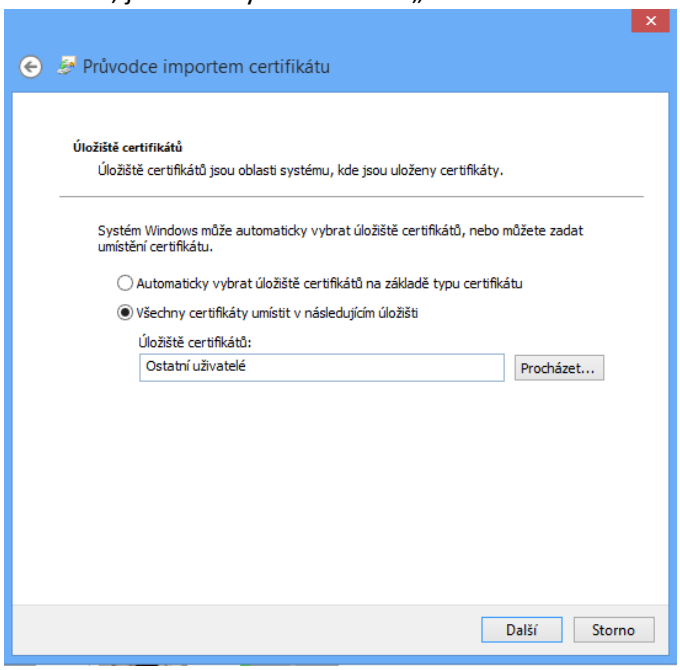
2. Samotný import
   2.1. Otevře se průvodce importem certifikátu. Nechejte možnost *„Aktuální uživatel“* a pokračujte dále.



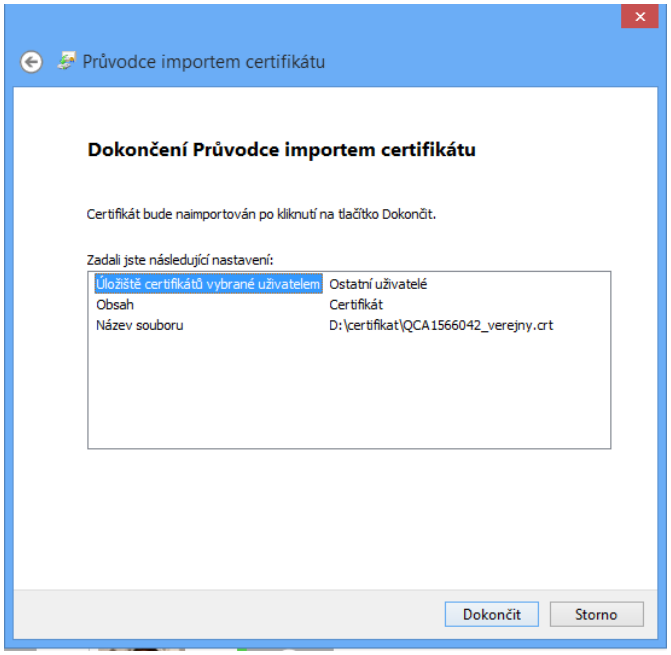
2.2. Vyhledejte certifikát na disku zařízení a přejděte dále.



2.3. Ponechte možnost, kterou jste zvolili výše a pokračujte dále. Máte zde možnost změnit složku, kam chcete certifikát uložit. Pokud budete pro šifrování používat naimportovaný certifikát, je nutné vybrat úložiště „ostatní uživatelé“



2.4. Stiskněte dokončit.



2.5. Po několika sekundách se objeví potvrzovací hláška o úspěšném importu.