

# Národní elektronický nástroj

Principy práce s certifikáty v NEN

## Obsah

1	Úvod .....	3
2	Podporované certifikáty .....	4
3	Práce s privátními klíči importovanými v úložišti certifikátů nebo na čipové kartě.....	4
3.1	Praktická ukázka .....	6
4	Podporované tvary certifikátů.....	8
4.1	Certifikáty pro podepisování C1, C2 .....	8
4.1.1	Jak získat certifikát pro podepisování (C1,C2) .....	8
4.1.2	Export certifikátu C1,C2 do souboru s příponou .pfx .....	10
4.2	Klíče pro šifrování a dešifrování (C3) .....	17
4.2.1	Jak získat certifikát pro šifrování a dešifrování.....	17
4.2.2	Export soukromého klíče do souboru s příponou .pfx (dešifrovací) .....	18
4.2.3	Export veřejného klíče s certifikátem do souboru s příponou .cer (šifrovací) .....	18
4.2.4	Import veřejného klíče s certifikátem .....	24

# 1 Úvod

Tento dokument popisuje možnosti použití soukromých klíčů a veřejných klíčů s certifikátem v systému NEN ze strany zadavatelů i dodavatelů včetně jejich omezení. Obsahuje i možnosti získání podporovaných tvarů certifikátů.

V rámci systému NEN se postupuje dle níže popsanych pravidel,<sup>1</sup> není zcela aplikován soulad s Nařízením (EU) č. 910/2014 a zákonem č. 297/2016 Sb. V rámci systému NEN se nebude do 19. 9. 2018 (tj. po dobu přechodného ustanovení) postupovat dle pravidel uvedených v NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES a zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.

Aplikace NEN využívá certifikáty pro zabezpečení dat uživatelů i pro zajištění dokumentů z hlediska neodmítnutelné nepopíratelnosti dat v rámci systému. Možnosti zadavatelů a dodavatelů jsou

	zadavatel	dodavatel	systém	certifikát	Typ klíče
Podpis registrace	ano	ano	-	C1, C2	soukromý
Podpis souboru	ano	ano	-	C1, C2	soukromý
Podpis objektu (interní zpráva, podání,...)	ano	ano	-	C1, C2	soukromý
Zašifrování podání	-	ano	-	C3	veřejný
Dešifrování podání	ano	-	-	C3	soukromý
Elektronická značka NEN	-	-	ano	C4	soukromý

Aplikace umožňuje pracovat s různými úložišti certifikátů:

- Certifikát uložený na čipové kartě či tokenu
- Certifikát importovaný do systémového úložiště operačního systému
- Certifikát uložený jako soubor v souborovém úložišti (na disku počítače)

<sup>1</sup> Dle § 20 zákona č. 297/2016 Sb. byl sice zrušen zákon č. 227/2000 Sb., ale na základě přechodných ustanovení uvedených v § 19 odst. 1 zákona č. 297/2016 Sb. lze po dobu 2 let ode dne nabytí účinnosti tohoto zákona k podepisování podle § 5 použít rovněž zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis, a dle přechodného ustanovení uvedeného v § 19 odst. 2 zákona č. 297/2016 Sb. lze po dobu 2 let ode dne nabytí účinnosti tohoto zákona namísto zaručené elektronické pečeti založené na kvalifikovaném certifikátu pro elektronickou pečeť nebo namísto kvalifikované elektronické pečeti použít:

a) elektronickou značku podle zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění účinném přede dnem nabytí účinnosti tohoto zákona, založenou na systémovém certifikátu vydaném osobou, která byla přede dnem nabytí účinnosti tohoto zákona akreditovaným poskytovatelem certifikačních služeb a která je kvalifikovaným poskytovatelem služeb vytvářejících důvěru, nebo

b) zaručenou elektronickou pečeť založenou na certifikátu pro elektronickou pečeť vydaném kvalifikovaným poskytovatelem služeb vytvářejících důvěru.

Více o aktivaci a práci se soukromými klíči uloženými a importovanými v systémovém úložišti operačního systému naleznete v kapitole 3. Práce s privátními klíči importovanými v úložišti certifikátů nebo na čipové kartě).

## 2 Podporované certifikáty

Systém podporuje několik typů certifikátů

certifikát	Význam
<b>C1</b>	<b>Kvalifikovaný certifikát</b> vydaný akreditovaným poskytovatelem certifikačních služeb dle zákona č. 227/2000 Sb., o elektronickém podpisu, v platném znění. Certifikát si zajišťují a obnovují všichni uživatelé NEN na vlastní náklady u akreditovaného poskytovatele.
<b>C2</b>	<b>Kvalifikovaný systémový certifikát</b> vydaný akreditovaným poskytovatelem certifikačních služeb dle zákona č. 227/2000 Sb. Certifikát si zajišťují a obnovují všichni uživatelé NEN na vlastní náklady u akreditovaného poskytovatele.
<b>C3</b>	<b>Komerční certifikát zadavatele</b> není vydán v souladu se zákonem č. 227/2000 Sb. Certifikát si zajišťují a obnovují všichni zadavatelé využívající NEN na vlastní náklady.
<b>C4</b>	<b>Kvalifikovaný systémový certifikát</b> vydaný akreditovaným poskytovatelem certifikačních služeb dle zákona č. 227/2000 Sb. Certifikát zajišťuje a obnovuje správce NEN na vlastní náklady u akreditovaného poskytovatele.

## 3 Práce s privátními klíči importovanými v úložišti certifikátů nebo na čipové kartě

Aplikace má jako výchozí možnost pro práci s certifikáty nastavenou možnost vložení certifikátu ze souborového úložiště a zadání příslušného hesla. Aplikace pracuje s certifikátem a soukromým klíčem pouze v paměti prohlížeče na vašem zařízení, kde proběhne samotné vytvoření podpisu. Privátní klíč není odesílán na server.

Řada organizací svou bezpečnostní politikou neumožňuje používat certifikáty uložené jako soubory. Z toho důvodu aplikace podporuje používání certifikátů importovaných do systémového úložiště operačního systému. Technologie Microsoft Silverlight, která je pro účely podepisování využívána, nemá v základním nastavení povolen přístup k certifikátům. Provedením úprav podle postupu na <https://nen.nipez.cz/Help/ElevatedTrust/ElevatedTrust.aspx> se nastaví v aplikaci NEN přístup k vašim certifikátům.

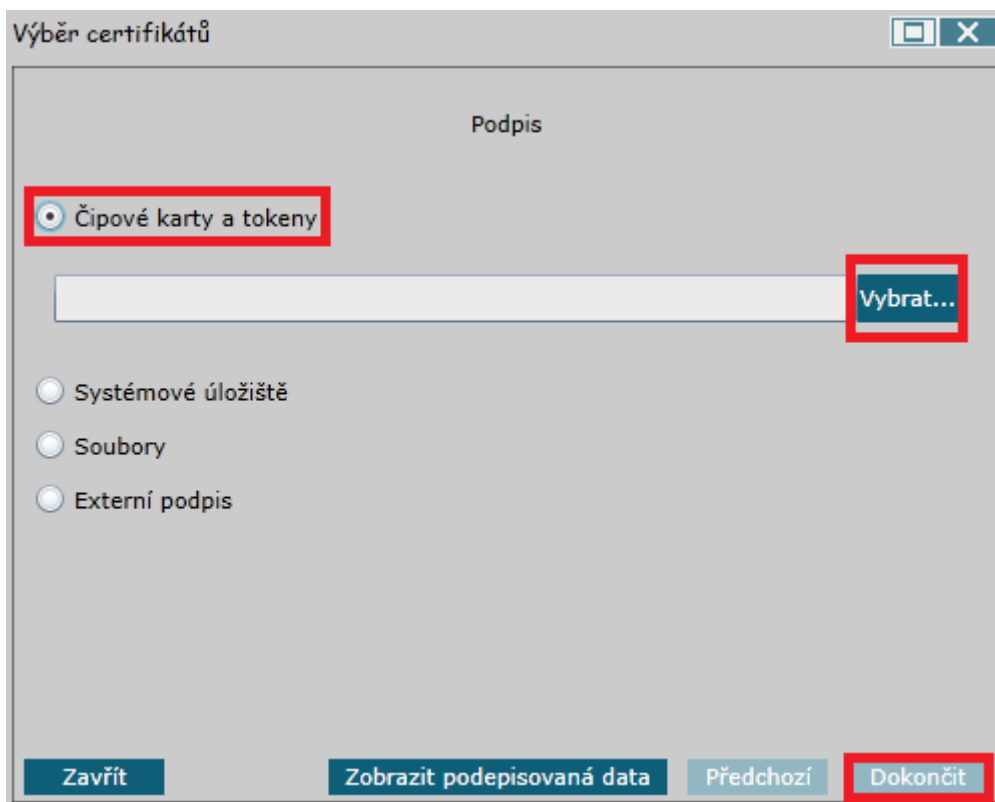
Aplikace NEN je elektronicky podepsána. Použitý certifikát, na kterém je založen elektronický podpis, má pouze omezenou dobu platnosti. Před jeho vypršením (nebo i dříve kvůli jiným důvodům) bude aplikace opatřena novým podpisem. Nový elektronický podpis vytvořený s využitím nového certifikátu se projeví nedostupností práce s certifikáty obsahujícími privátní klíče na čipové kartě nebo importovanými v úložišti certifikátů Windows. Proto bude nutné provést znovu postup odkazovaný výše. Při změně certifikátu budou uživatelé informováni.

Aplikace pro přístup k certifikátům importovaným v systémovém úložišti operačního systému nebo na čipové kartě aplikace využívá rozhraní operačního systému CryptoAPI, které má uživatel nastaveno v operačním systému. Aplikace nevyžaduje instalaci speciálního rozhraní. Z toho důvodu jsou zobrazeny pouze certifikáty, které rozhraní CryptoAPI aplikaci zpřístupní. Při správném nastavení jsou zpřístupněny certifikáty importované v systémovém úložišti operačním systémem (v části Osobní) a dále certifikáty na čipové kartě (pokud je připojena). Systém zobrazuje pouze platné certifikáty.

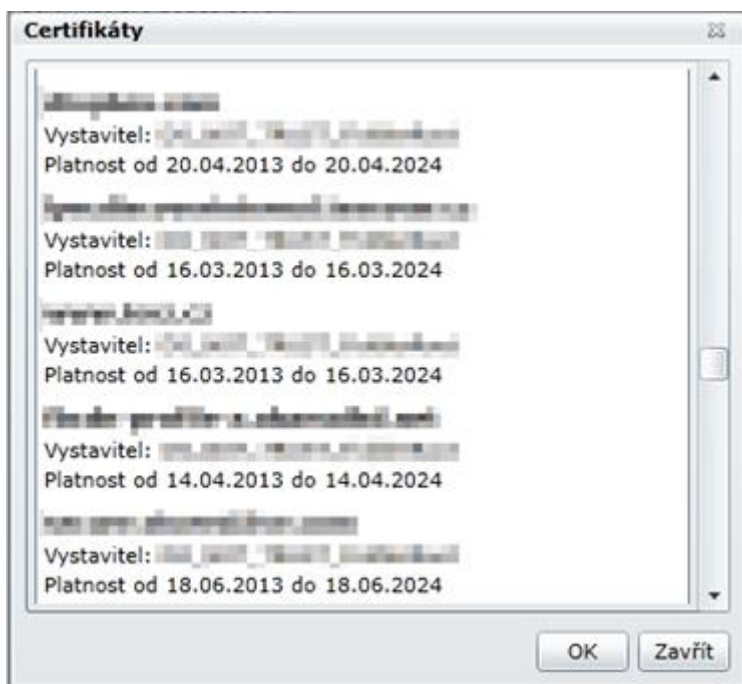
Aktuálně je v aplikaci zpřístupněna možnost práce s certifikáty uloženými v systémovém úložišti Windows. Práce s úložištěm certifikátů na MacOS není dostupná, protože tento operační systém nedisponuje potřebným rozhraním.

### 3.1 Praktická ukázka

Výběr certifikátu z „Čipových karet a tokenů“



Stiskem tlačítka „Vybrat“ se zobrazí seznam certifikátů, které je možno použít. Stejný seznam se zobrazí při výběru certifikátu ze systémového úložiště.



Výběr certifikátu ze „Systémového úložiště“

Výběr certifikátů

Podpis

☐ Čipové karty a tokeny

☒ Systémové úložiště

**Vybrat...**

☐ Soubory

☐ Externí podpis

**Zavřít** **Zobrazit podepisovaná data** **Předchozí** **Dokončit**

Výběr certifikátu uloženého do souboru (v případě použití certifikátu uloženého jako soubor bude případně nutné zadat heslo pro přístup k certifikátu)

Výběr certifikátů

Podpis

☐ Čipové karty a tokeny

☐ Systémové úložiště

☒ Soubory

**Vybrat...**

Heslo

☐ Externí podpis

**Zavřít** **Zobrazit podepisovaná data** **Předchozí** **Dokončit**

## 4 Podporované tvary certifikátů

Systém rozlišuje pro použití soukromé a veřejné klíče. Mimo šifrování jsou v systému vyžadovány soukromé klíče.

### 4.1 Certifikáty pro podepisování C1, C2

Po provedení příslušného nastavení počítače je možné použít certifikáty uložené v systémovém úložišti Windows nebo čipové kartě pomocí tlačítka „Úložiště“ (viz kapitola 3)

Pokud se nepoužije předchozí možnost, vkládá se soubor s příponou .PFX nebo .P12, který obsahuje soukromý klíč s certifikátem.

Při použití se může systém zeptat na heslo k soukromému klíči (toto heslo bylo zvoleno při exportu soukromého klíče).

#### 4.1.1 Jak získat certifikát pro podepisování (C1,C2)

Pro získání certifikátu se doporučujeme obrátit 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 certifikační autority.

- PostSignum [http://www.postsignum.cz/kvalifikovane\\_certifikaty.html](http://www.postsignum.cz/kvalifikovane_certifikaty.html)
- První certifikační autorita <https://www.ica.cz/Kvalifikovany-certifikat>
- eIdentity <http://www.eidentity.cz/>

Dále popsaný postup se týká certifikační autority PostSignum.

Pro získání prvního certifikátu od PostSignum je možné zvolit 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](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).
3. Zaškrtněte *Změnit zabezpečení úložiště klíčů*
4. Po přečtení pokynů potvrďte jejich přečtení zaškrtnutím položky „Potvrzuji, že jsem se seznámil...“

Ilustrační stav je zobrazen na obrázku.



Doplňte údaje pro generování žádosti o certifikát	
Jméno a příjmení nebo název certifikátu	<input type="text" value="Jiří Novák"/> *
E-mail	<input type="text" value="muj@email.cz"/> *
Druh certifikátu	<b>Vygenerovanou žádost lze použít pouze pro vydání jednoho certifikátu. Typ vydávaného certifikátu je potřeba specifikovat při jeho vydání.</b>
Velikost klíče	<input type="text" value="2048 bitů"/> ▼
Umístění soukromého klíče	<input type="text" value="Operační systém Windows"/> ▼ zobrazovat pouze doporučené umístění <input checked="" type="checkbox"/>
Ostatní nastavení	<input checked="" type="checkbox"/> Změnit zabezpečení úložiště klíčů

☒ Potvrzuji, že jsem se seznámil [s pokyny pro generování žádosti a vydání certifikátu.](#)

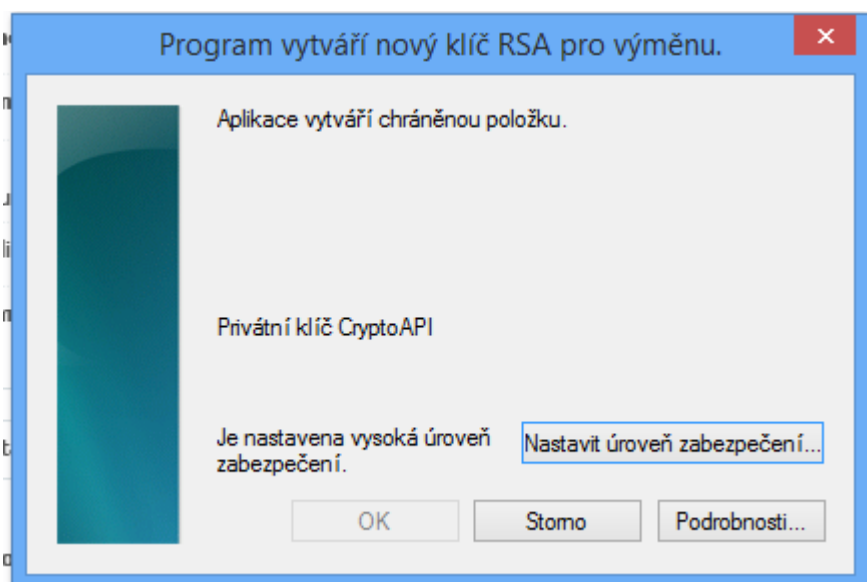
Vygenerovat a odeslat žádost o certifikát na www server PostSignum

**Žádost o vydání certifikátu bude uložena na www server PostSignum, TATO MOŽNOST NELZE VYUŽÍT PRO OBNOVU CERTIFIKÁTU PŘES E-MAIL.** Po vygenerování Vám bude přiděleno jednoznačné ID žádosti o certifikát. Toto jednoznačné ID žádosti je nutné sdělit operátorovi při vydání certifikátu na pobočce České pošty se službou Czech POINT.

Vygenerovat a uložit žádost o certifikát do souboru

Takto vygenerovaná žádost o certifikát bude uložena do souboru. Soubor poté uložte na přenosné médium (flash disk), nebo jej přiložte k e-mailu, který odesíláte pro obnovu certifikátu.  
Při vydání certifikátu na pobočce České pošty se službou Czech POINT, je nutné předat operátorovi přenosné médium s uloženou žádostí o certifikát.

5. Zvolte „Vygenerovat a odeslat žádost o certifikát na www server PostSignum“.
6. V zobrazeném okně klikněte na „Nastavit úroveň zabezpečení“



7. Zadejte heslo, které budete muset zadat při každém použití.

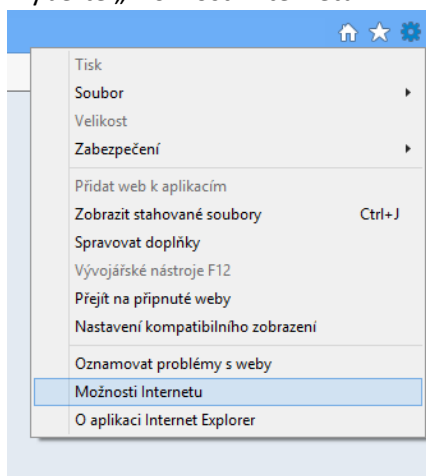
8. Stiskněte „Dokončit“ a poté „OK“
9. Na webové stránce se Vám zobrazí ID žádosti. Toto ID žádosti si zapište a zajděte s ním s potřebnými dokumenty na Kontaktní místo PostSignum. Jsou to všechny pobočky, na kterých je dostupná služba Czech Point. Odkaz na seznam poboček je umístěn zde: [http://www.postsignum.cz/pobocky\\_ceske\\_posty.html](http://www.postsignum.cz/pobocky_ceske_posty.html).  
Konkrétně: [http://www.ceskaposta.cz/documents/10180/282515/seznam\\_post\\_czechpoint.xls](http://www.ceskaposta.cz/documents/10180/282515/seznam_post_czechpoint.xls)
10. Po podepsání smlouvy dorazí na zadaný email odkaz na získání certifikátu.  
Pokud použijete jinou certifikační autoritu, postupujte podle jejich návodu a získejte svůj certifikát.
11.
  - a) Pokud budete využívat systémové úložiště operačního systému, zde skončete. Soukromý klíč s certifikátem by již měly být uloženy ve složce Osobní v systémové úložišti certifikátů operačního systému.
  - b) Pokud budete využívat k podpisu soubor uložený na disku, dále postupujte podle kapitoly „Export certifikátu C1,C2 do souboru s příponou .pfx“.
12. Doporučujeme si před uzavřením prohlížeče zálohovat soukromý klíč podle postupu, který je zobrazen pod ID certifikátu. Provedením zálohy soukromého klíče si zároveň vytvoříte požadovaný soubor s příponou PFX. V rámci provedení zálohy si zadejte heslo. Postupujte podle postupu na webových stránkách.

#### 4.1.2 Export certifikátu C1,C2 do souboru s příponou .pfx

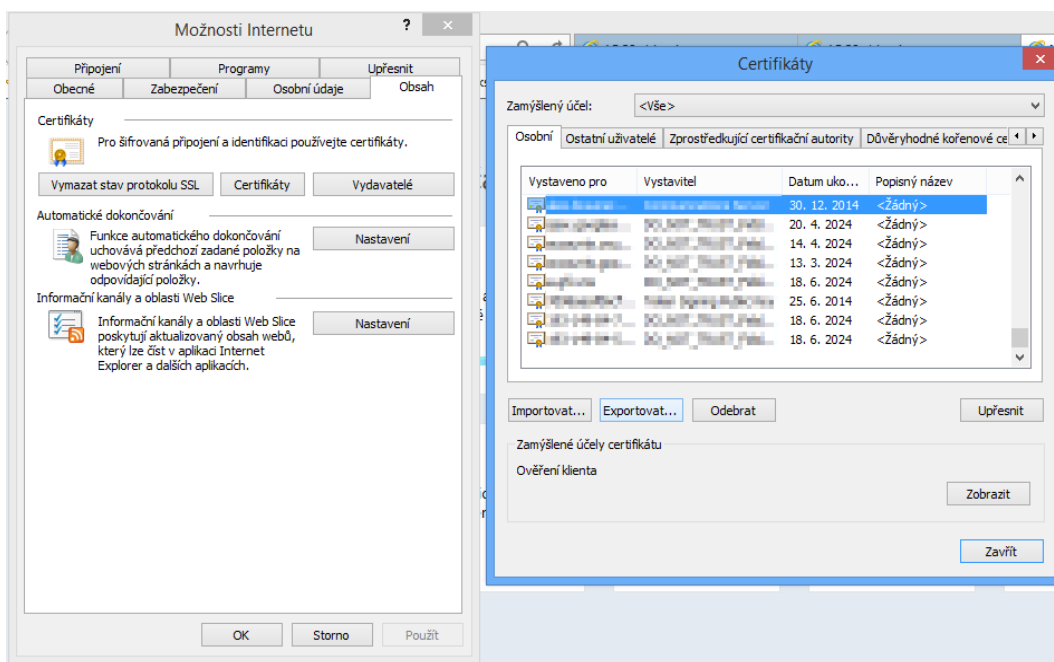
Export certifikátu, který je uložen v úložišti certifikátů ve Windows, je možné inicializovat více navzájem zaměnitelnými způsoby. Export nevyžaduje administrátorská oprávnění. Po spuštění samotného exportu jsou postupy totožné. Zobrazované ukázky jsou pro Windows 8.1 a prohlížeč Internet Explorer 11.

## 1. Postup pomocí prohlížeče.

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

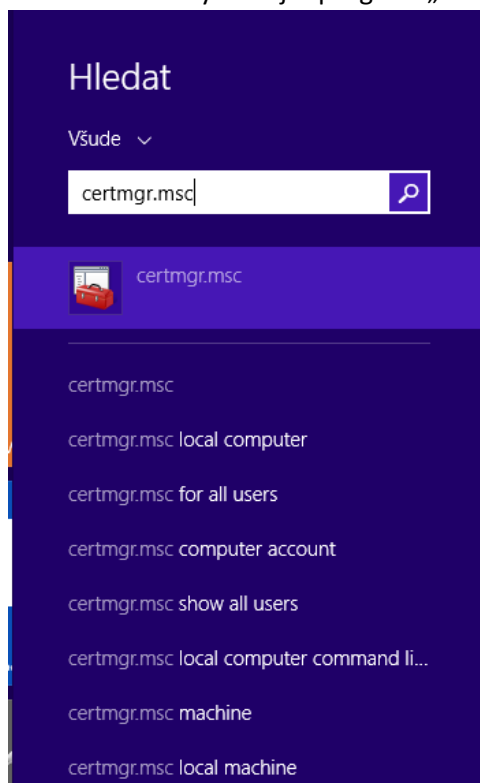


- 1.2. Na záložce „Obsah“ klikněte na tlačítko „Certifikáty“. Otevře se seznam certifikátů. Vyhledejte certifikát, který chcete exportovat. Typicky se bude nacházet na první záložce „Osobní“. Po jeho vybrání klikněte na tlačítko „Exportovat“ a pokračujte bodem 3.

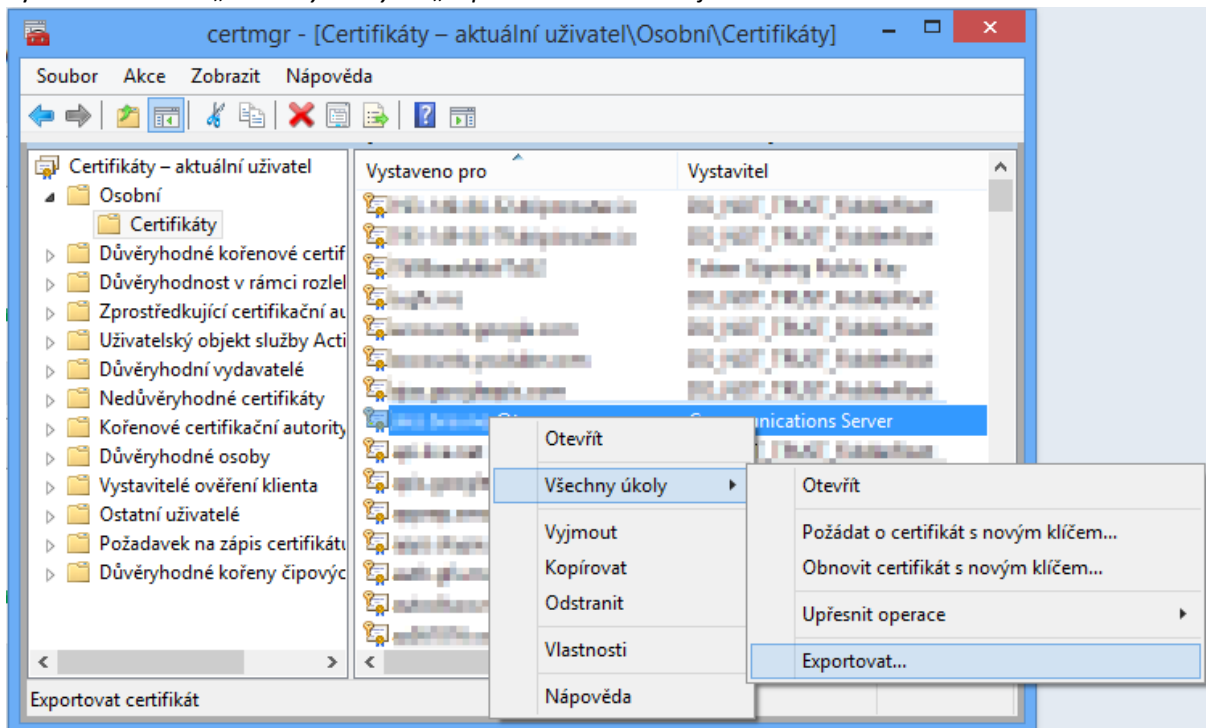


## 2. Postup přes konzoli

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

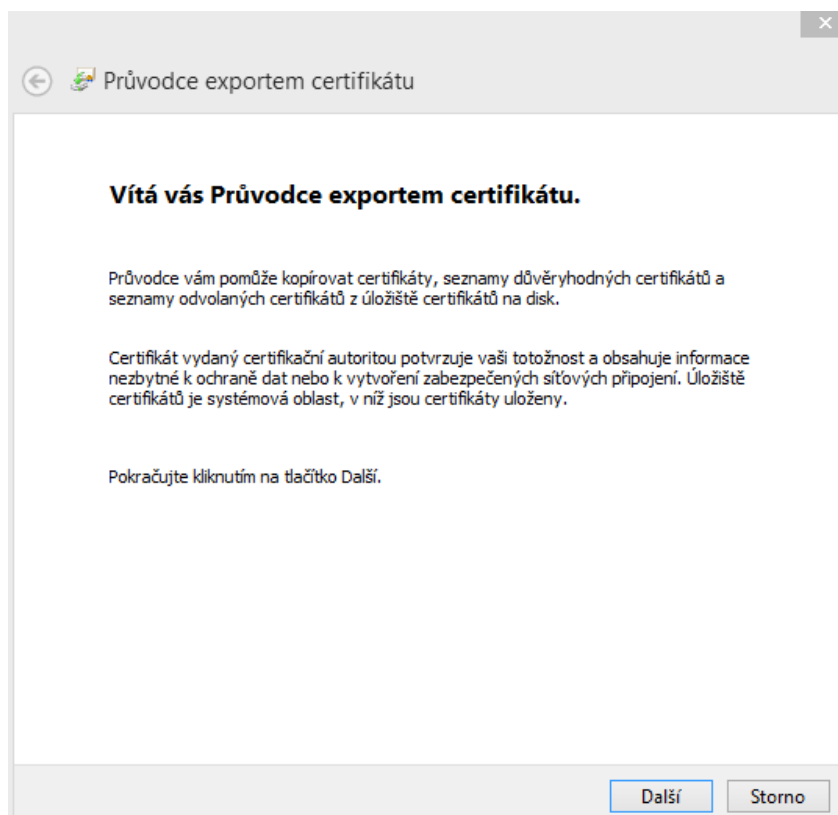


2.2. Otevře se seznam certifikátů. Vyhledejte certifikát, který chcete exportovat. Typicky se bude nacházet v první složce „Osobní“ -> „Certifikáty“. Klikněte pravým tlačítkem na certifikát, vyberte možnost „Všechny úkoly“ a „Exportovat“. Pokračujte bodem 3.





### 3. Export certifikátu do formátu .pfx

#### 3.1. První obrazovka po inicializaci exportu daného certifikátu.



- 3.2. Zvolte možnost exportování soukromého klíče. Pokud nemá soukromý klíč při vložení do systémového úložiště nastavenou možnost, že je exportovatelný, nebudete mít možnost si tuto volbu zvolit a dále není možné pokračovat. Můžete nadále využít soukromý klíč uložený v úložišti a přistupovat přímo k němu.



Průvodce exportem certifikátu

**Exportovat privátní klíč**  
Můžete se rozhodnout exportovat privátní klíč s certifikátem.

---



Privátní klíče jsou chráněny heslem. Chcete-li exportovat privátní klíč s certifikátem, musíte v pozdějším dialogu zadat heslo.

Chcete exportovat privátní klíč s certifikátem?

☒ Ano, exportovat privátní klíč  
☐ Ne, neexportovat privátní klíč

Další
Storno

3.3. Ponechejte výchozí, nabízené nastavení.



Průvodce exportem certifikátu

**Formát souboru pro export**  
Certifikáty lze exportovat v různých formátech.

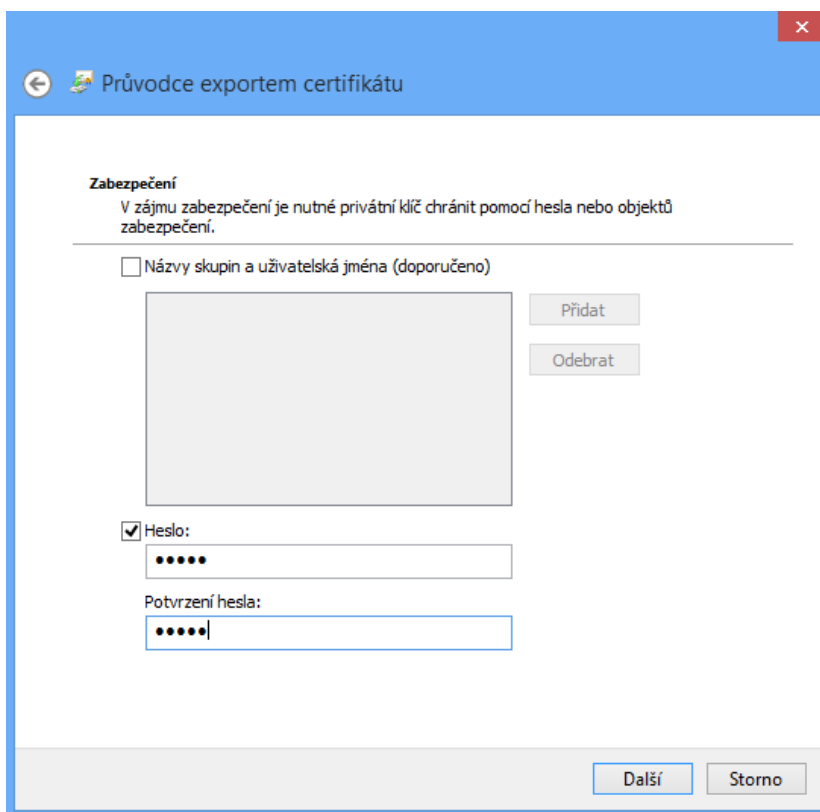
---

Vyberte formát, který chcete použít:

☐ Binární X.509, kódování DER (CER)  
☐ X.509, kódování Base-64 (CER)  
☐ Certifikáty standardu Cryptographic Message Syntax Standard - PKCS č. 7 (P7B)  
☐ Zahrnout všechny certifikáty na cestě k certifikátu, pokud je to možné  
☒ Formát Personal Information Exchange - PKCS č. 12 (PFX)  
☒ Zahrnout všechny certifikáty na cestě k certifikátu, pokud je to možné  
☐ Odstranit privátní klíč v případě úspěšného exportu  
☐ Exportovat všechny rozšířené vlastnosti  
☐ Serializované úložiště certifikátů (SST)

Další
Storno

- 3.4. Zatrhněte možnost „Heslo“. Zadejte heslo. Uživatel bude toto heslo zadávat v rámci podpisů. Systém nepodporuje použití soukromého klíče bez hesla. Zde zadané *Heslo* nemá žádnou souvislost s heslem zadaným během žádosti o generování certifikátu. Toto heslo se vztahuje pouze k exportovanému certifikátu.



**Zabezpečení**  
V zájmu zabezpečení je nutné privátní klíč chránit pomocí hesla nebo objektů zabezpečení.

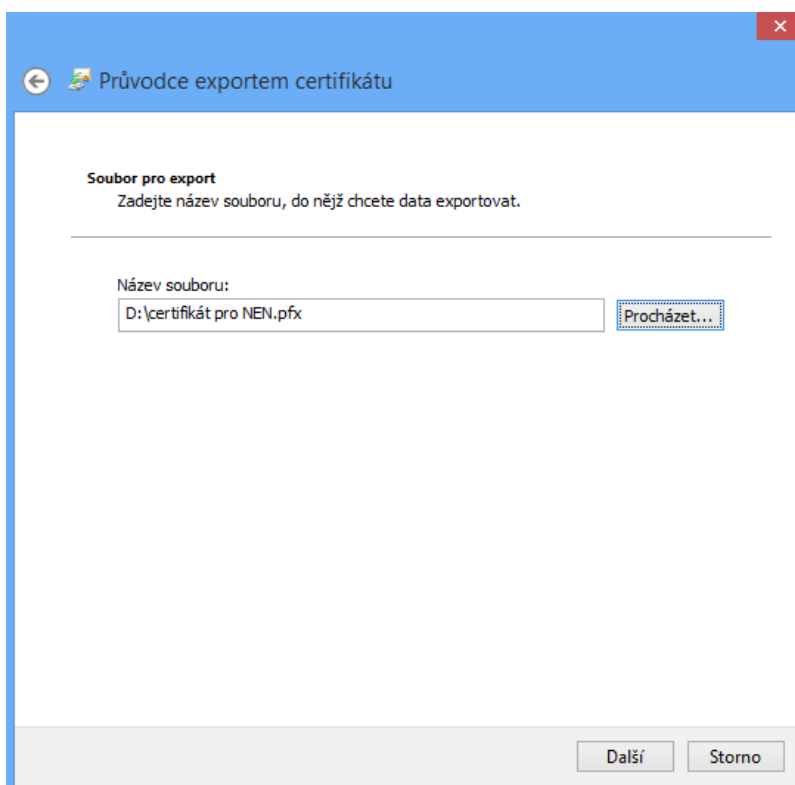
☐ Názvy skupin a uživatelská jména (doporučeno)

☒ Heslo:

Potvrzení hesla:

**Další** **Storno**

- 3.5. Zvolte umístění souboru.



**Soubor pro export**  
Zadejte název souboru, do nějž chcete data exportovat.

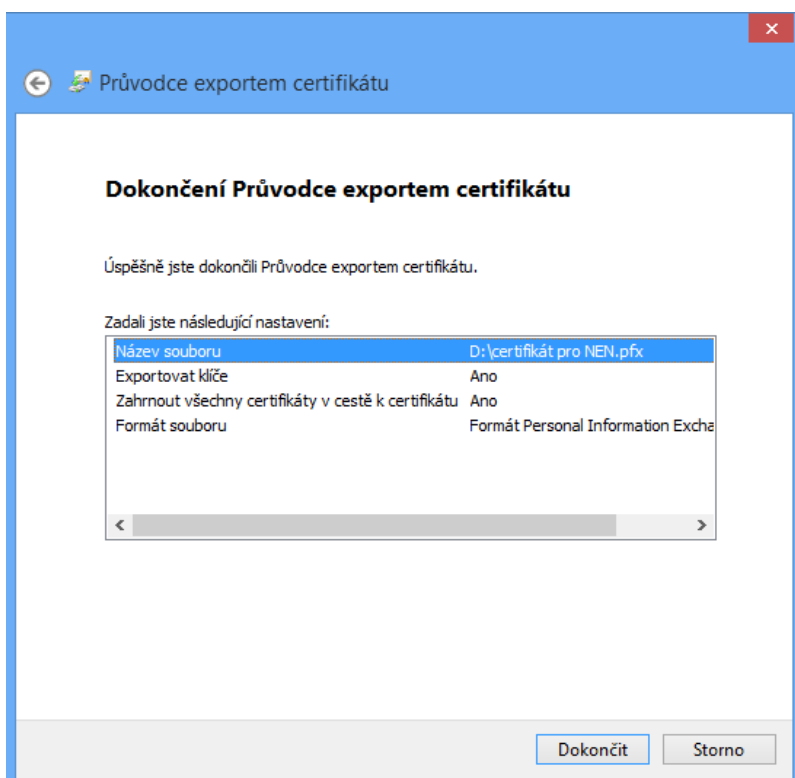
Název souboru:

D:\certifikát pro NEN.pfx

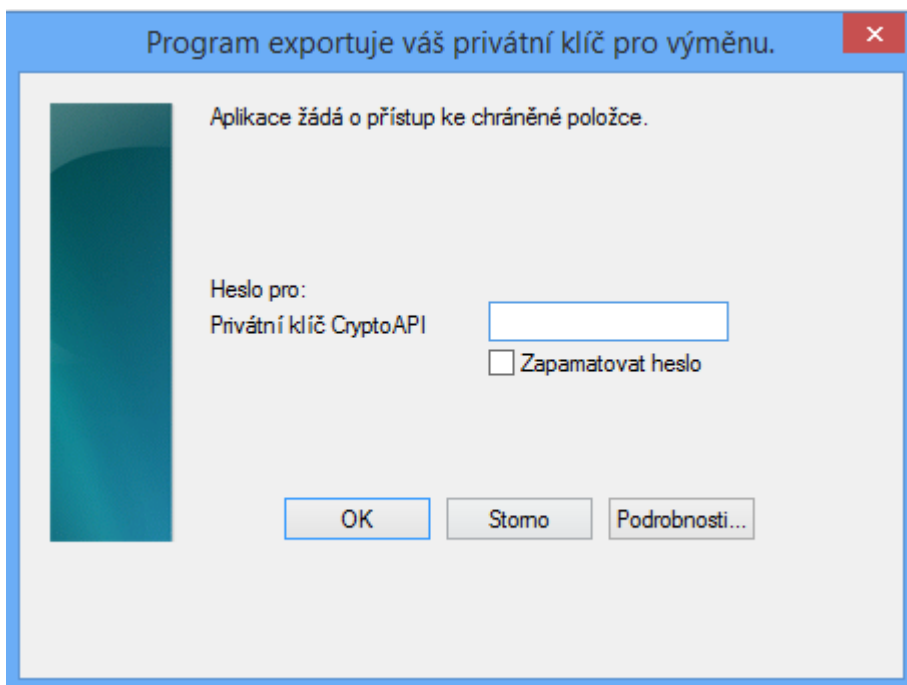
**Procházet...**

**Další** **Storno**

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



3.7. Pokud byla v žádosti o certifikát zaškrtnuta volba změny zabezpečení nebo u již uloženého certifikátu byla tato možnost nastavena, vyplňte na novém okně heslo, které jste zadali v rámci generování žádosti nebo které zadáváte pro jeho použití.





## 4.2 Klíče pro šifrování a dešifrování (C3)

Pro účely zabezpečení podání se využívá šifrování podání veřejným klíčem, který je součástí certifikátu zadavatele.

Zadavatel poskytne dodavatelům veřejný klíč s certifikátem. Dodavatelé zašifrují své podání tímto certifikátem. Zadavatel si svůj soukromý klíč uchovává v tajnosti a použije jej až v rámci dešifrování podání.

Pro účely **zašifrování dodavatelem** je možné použít:

- certifikát s veřejným klíčem uložený v systémovém úložišti Windows nebo na čipové kartě (viz kapitola 3)
- certifikát s veřejným klíčem ve vhodném formátu (viz níže)

Pro účely **dešifrování zadavatelem** je možné použít:

- soukromý klíč uložený v systémovém úložišti Windows nebo na čipové kartě (viz kapitola 3)
- soukromý klíč uložený v souboru s příponou .pfx

Akceptovaný formát certifikátu s veřejným klíčem pro zašifrování je Binární X.509 s kódováním DER a příponou výsledného souboru CER.

### 4.2.1 Jak získat certifikát pro šifrování a dešifrování

#### 4.2.1.1 Z pohledu zadavatele

**Získání klíčů a certifikátů odpovídá postupu pro získání certifikátu C1, C2. Vytváří se žádost o vydání komerčního certifikátu.** Jinak by postup neměl být rozdílný. Výsledkem je získání soukromého klíče, který slouží zadavateli pro dešifrování. Způsob jeho nastavení je popsán u certifikátů C1, C2.

Pokud bude zadavatel pro dešifrování využívat soukromý klíč uložený v systémovém úložišti Windows, měl by mít tento klíč uložen v případě použití systémového úložiště ve složce Ostatní uživatelé.

Pokud bude zadavatel pro dešifrování využívat soukromý klíč uložený v souboru s příponou .pfx a nemá jej k dispozici, provede jeho export podle postupu 4.2.2 Export soukromého klíče do souboru s příponou .pfx (dešifrovací).

Získání certifikátu s veřejným klíčem je možné provést několika způsoby.

- Export certifikátu s veřejným klíčem z importovaného soukromého klíče. Soukromý klíč zadavatel získá v rámci jeho pořízení. Potom je tedy možné provést pouze export – viz kapitola 4.2.3 Export veřejného klíče s certifikátem do souboru s příponou .cer (šifrovací)
- Export certifikátu s veřejným klíčem z importovaného certifikátu s veřejným klíčem. Jedná se o alternativní postup podle 4.2.3 Export veřejného klíče s certifikátem do souboru s příponou .cer (šifrovací), kdy se v bodě 3.2 neumožní výběr.
- vyhledat a stáhnout od příslušného vydavatele. Každá certifikační autorita umožňuje vyhledání podle jiných údajů a poskytuje certifikát v jiných formátech. Tento způsob není předpokládán, ale je zde uveden z důvodu úplnosti.
  - PostSignum [http://www.postsignum.cz/certifikaty\\_uzivatelu.html](http://www.postsignum.cz/certifikaty_uzivatelu.html)
  - První certifikační autorita <http://www.ica.cz/Verejne-certifikaty>

#### 4.2.1.2 Z pohledu dodavatele

Dodavatel by měl obdržet certifikát od zadavatele způsobem, jakým si zadavatel v rámci zadávacího postupu zvolil.

Pokud bude pro šifrování používat certifikát s veřejným klíčem, který si naimportoval do systémového úložiště, musí si tento certifikát naimportovat podle kapitoly 4.2.4. Import veřejného klíče s certifikátem.

Pokud bude pro šifrování používat certifikát s veřejným klíčem uloženým v souboru a zároveň jej neobdrží v požadovaném tvaru, nebo jej aplikace odmítá, je řešením jeho import podle 4.2.4 Import veřejného klíče s certifikátem a poté export podle 4.2.3 Export veřejného klíče s certifikátem do souboru s příponou .cer (šifrovací).

#### 4.2.2 Export soukromého klíče do souboru s příponou .pfx (dešifrovací)

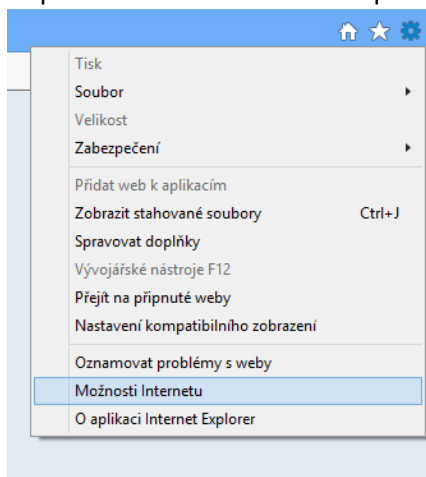
Postup odpovídá postupu pro získání soukromého klíče pro podpis (C1, C2).

#### 4.2.3 Export veřejného klíče s certifikátem do souboru s příponou .cer (šifrovací)

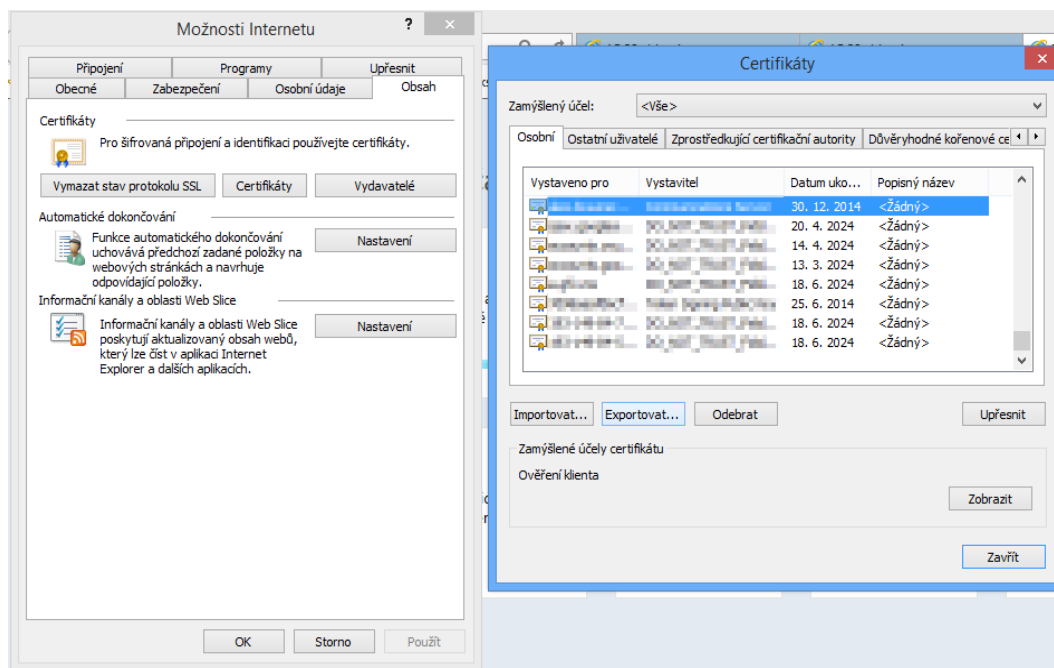
Postup je analogický jako kapitola 4.1.2 Export certifikátu C1,C2 do souboru s příponou .pfx. Inicializaci exportu je možné provést několika způsoby:

##### 1. Pomocí prohlížeče.

##### 1.1. V prohlížeči otevřete nabídku pro nastavení a v ní vyberte „Možnosti internetu“

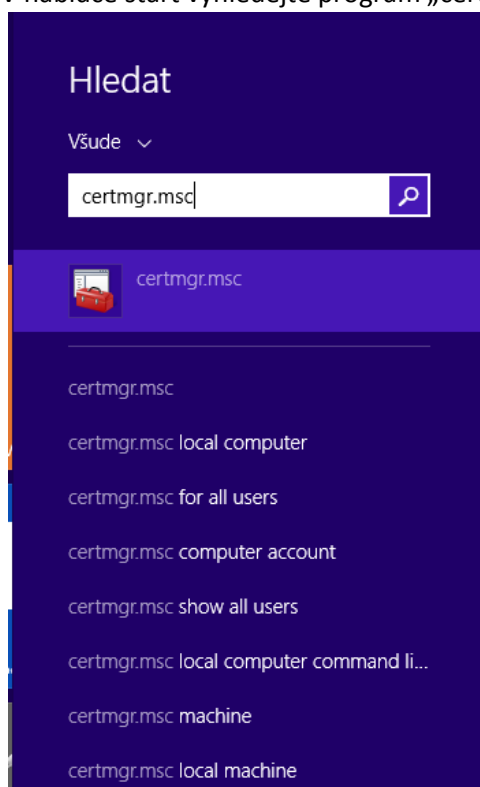


##### 1.2. Na záložce „Obsah“ klikněte na tlačítko „Certifikáty“. Otevře se seznam certifikátů. Vyhledejte certifikát, který chcete exportovat. Typicky se bude nacházet na první záložce „Osobní“. Po jeho vybrání klikněte na tlačítko „Exportovat“. Pokračujte bodem 3.

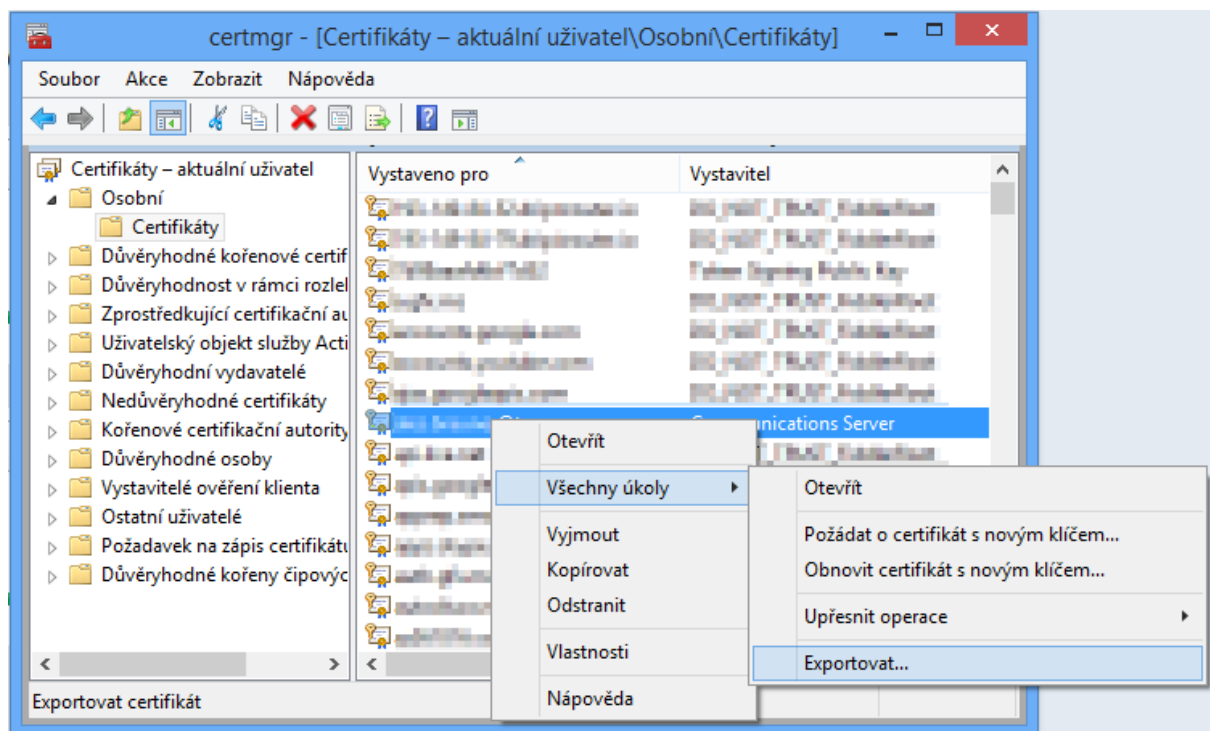


## 2. Přes konzoli:

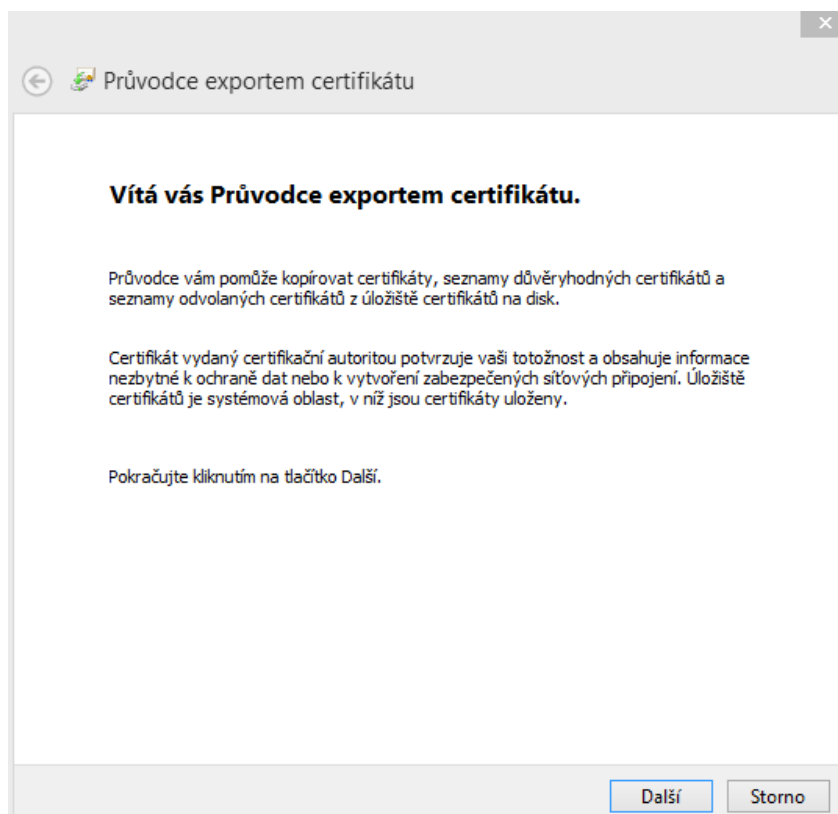
### 2.1. V nabídce start vyhledejte program „certmgr.msc“ a spusťte jej.



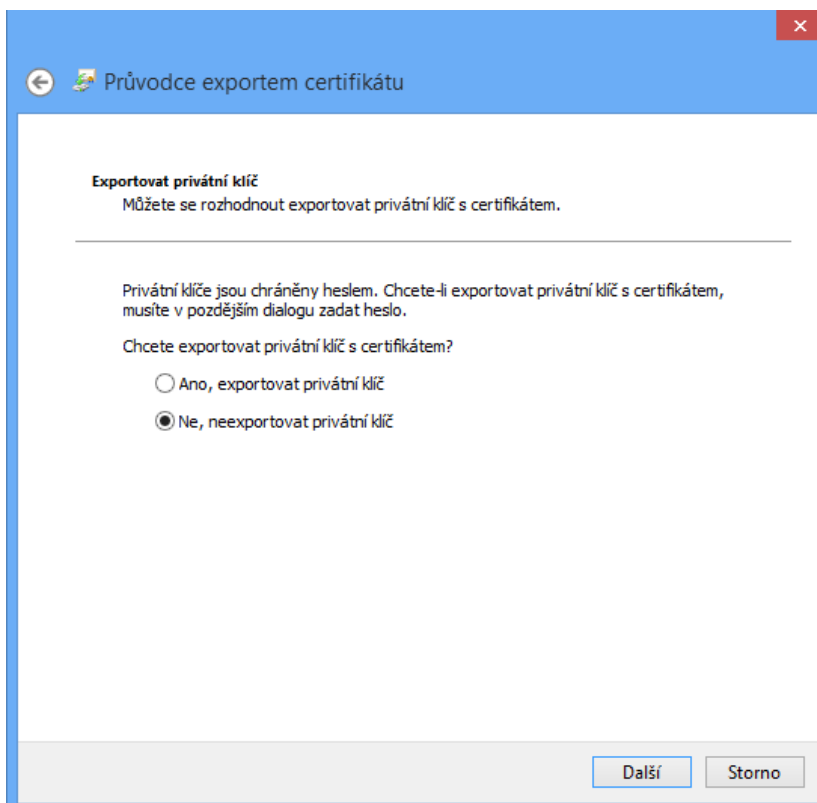
### 2.2. Otevře se seznam certifikátů. Vyhledejte certifikát, který chcete exportovat. Typicky se bude nacházet na první záložce „Osobní“, „Certifikáty“. Klikněte pravým tlačítkem na certifikát, vyberte možnost „Všechny úkoly“ a „Exportovat“. Pokračujte bodem 3.



3. Export certifikátu do souboru s přílohou .cer
  - 3.1. První obrazovka po inicializaci exportu daného certifikátu.



- 3.2. Tento formulář se objeví pouze v případě, že na počítači máte privátní klíč. Zvolte možnost NE, neexportovat privátní klíče



**Exportovat privátní klíč**  
Můžete se rozhodnout exportovat privátní klíč s certifikátem.

---

Privátní klíče jsou chráněny heslem. Chcete-li exportovat privátní klíč s certifikátem, musíte v pozdějším dialogu zadat heslo.

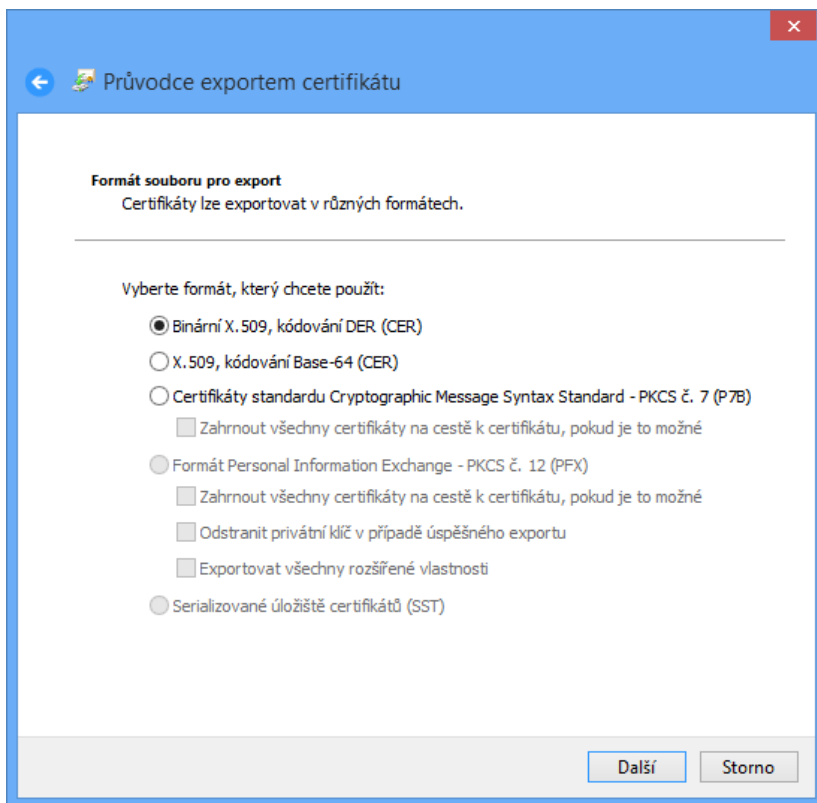
Chcete exportovat privátní klíč s certifikátem?

☐ Ano, exportovat privátní klíč

☒ Ne, neexportovat privátní klíč

Další Storno

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



**Formát souboru pro export**  
Certifikáty lze exportovat v různých formátech.

---

Vyberte formát, který chcete použít:

☒ Binární X.509, kódování DER (CER)

☐ X.509, kódování Base-64 (CER)

☐ Certifikáty standardu Cryptographic Message Syntax Standard - PKCS č. 7 (P7B)

☐ Zahrnout všechny certifikáty na cestě k certifikátu, pokud je to možné

☐ Formát Personal Information Exchange - PKCS č. 12 (PFX)

☐ Zahrnout všechny certifikáty na cestě k certifikátu, pokud je to možné

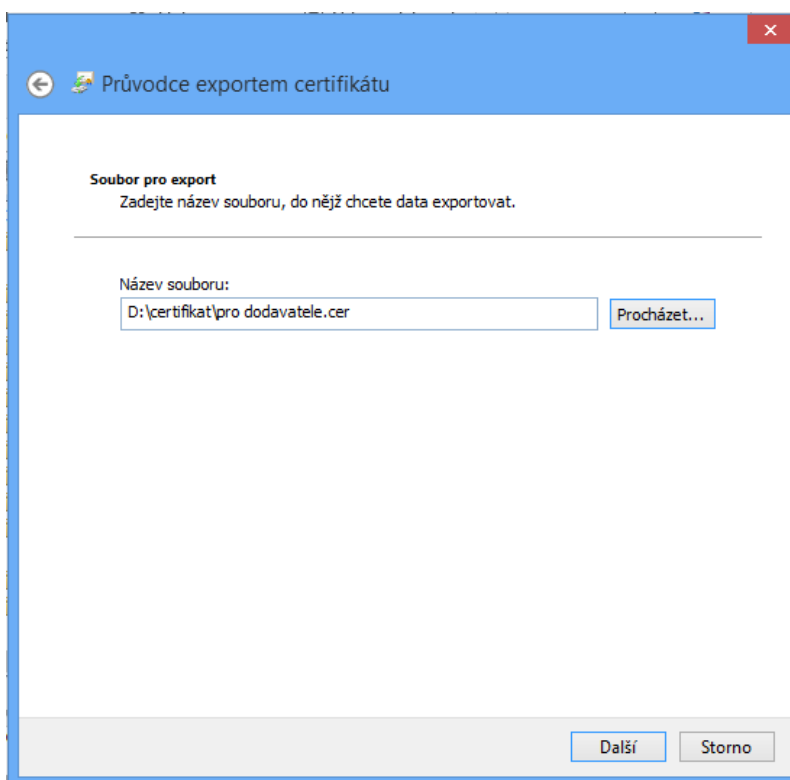
☐ Odstranit privátní klíč v případě úspěšného exportu

☐ Exportovat všechny rozšířené vlastnosti

☐ Serializované úložiště certifikátů (SST)

Další Storno

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



Průvodce exportem certifikátu

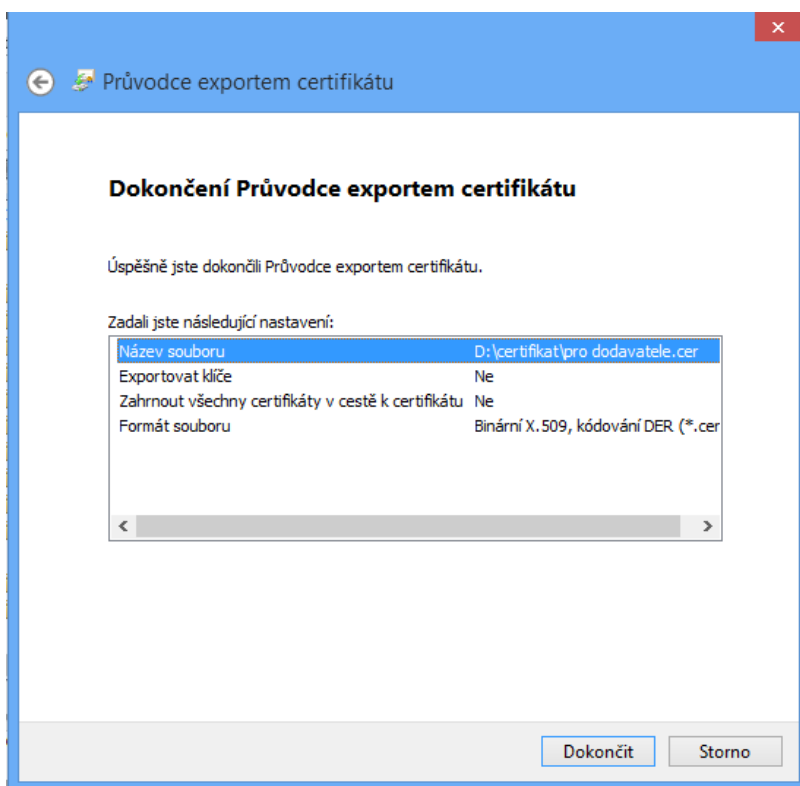
Soubor pro export  
Zadejte název souboru, do něž chcete data exportovat.

Název souboru:  
D:\certifikat\pro dodavatele.cer

Procházet...

Další Storno

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



Průvodce exportem certifikátu

**Dokončení Průvodce exportem certifikátu**

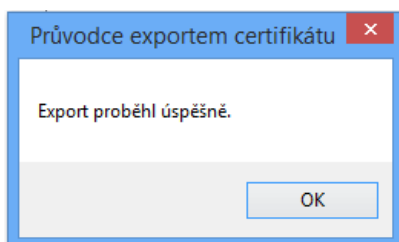
Úspěšně jste dokončili Průvodce exportem certifikátu.

Zadali jste následující nastavení:

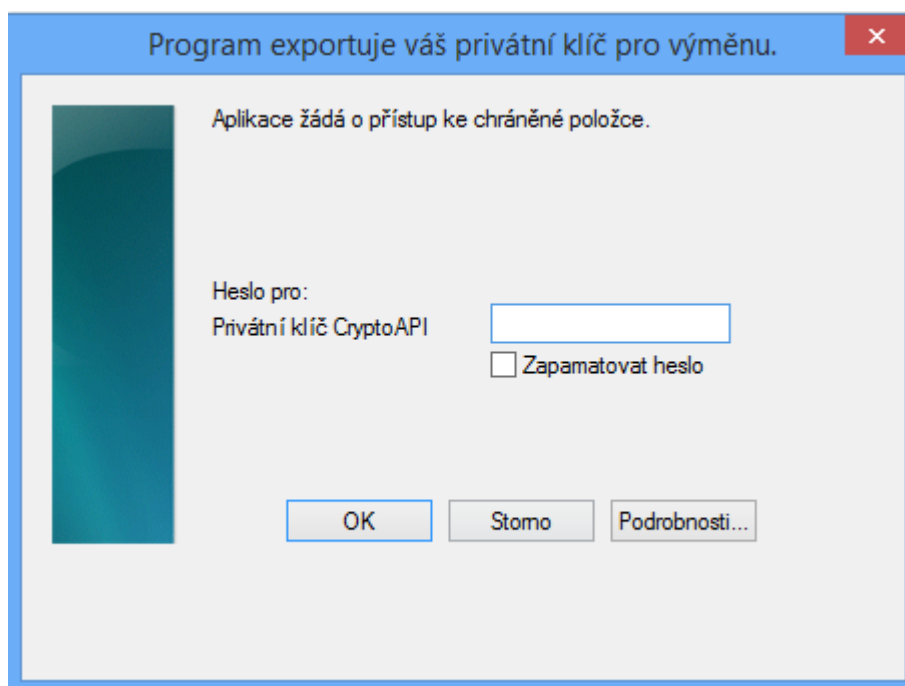
Název souboru	D:\certifikat\pro dodavatele.cer
Exportovat klíče	Ne
Zahrnout všechny certifikáty v cestě k certifikátu	Ne
Formát souboru	Binární X.509, kódování DER (*.cer)

Dokončit Storno

### 3.6. Zobrazí se potvrzení o exportu



- 3.7. Tento formulář se objeví pouze v případě, že na počítači máte uložen soukromý klíč a pokud byla v žádosti o certifikát zaškrtnuta volba změny zabezpečení nebo u již uloženého certifikátu byla tato možnost nastavena, vyplňte na novém okně heslo, které jste zadali v rámci generování žádosti nebo které zadáváte pro jeho použití.



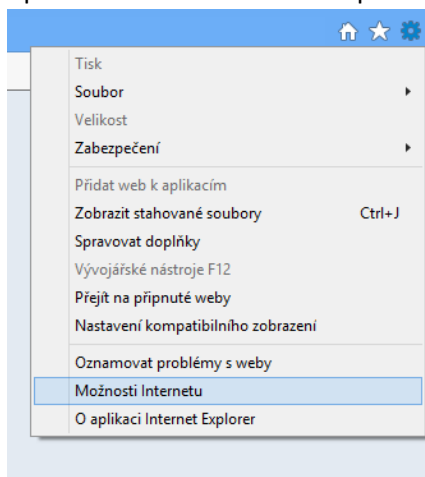
#### 4.2.4 Import veřejného klíče s certifikátem

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.

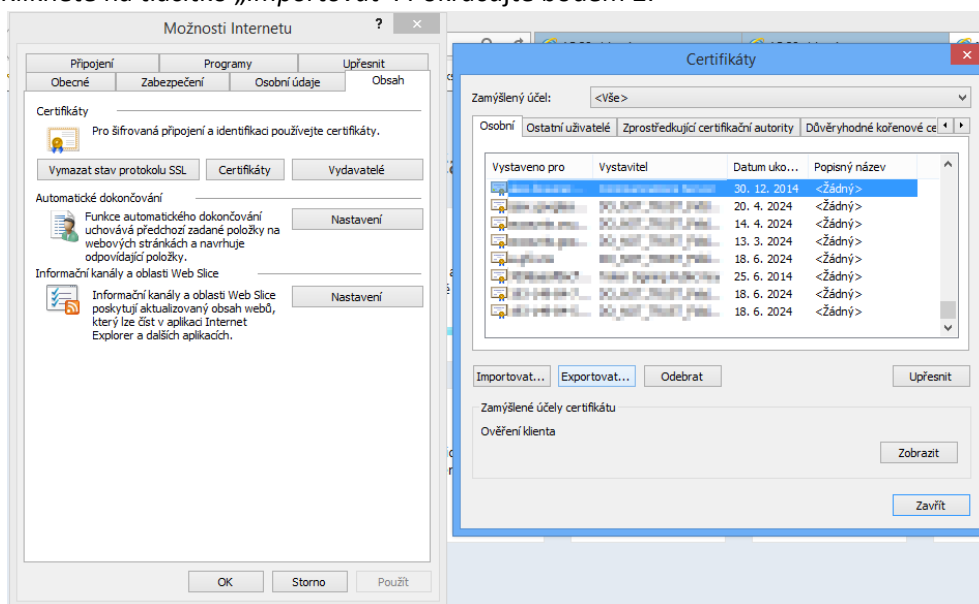
1. Inicializaci importu certifikátu je možné provést několika způsoby.

##### 1.1. Prohlížeč

##### 1.1.1. V prohlížeči otevřete nabídku pro nastavení a v ní vyberte „Možnosti internetu“



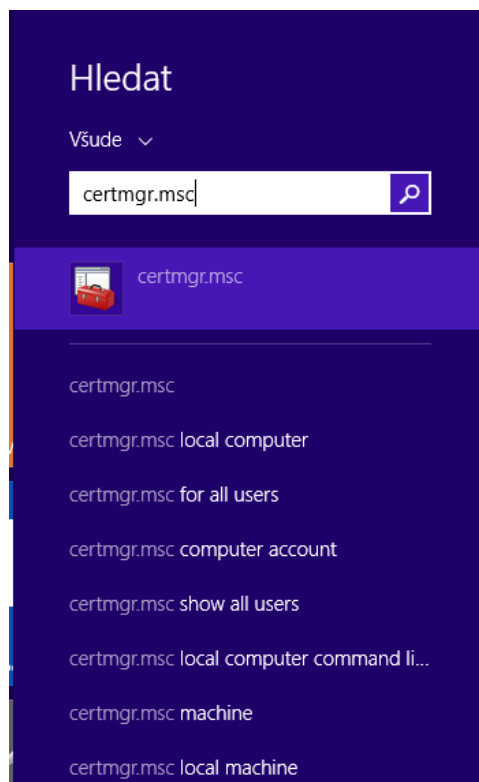
1.1.2. Na záložce „Obsah“ klikněte na tlačítko „Certifikáty“. Otevře se seznam certifikátů. Vyberte složku, kam chcete certifikát nainportovat. Například „Ostatní uživatelé“. Klikněte na tlačítko „Importovat“. Pokračujte bodem 2.



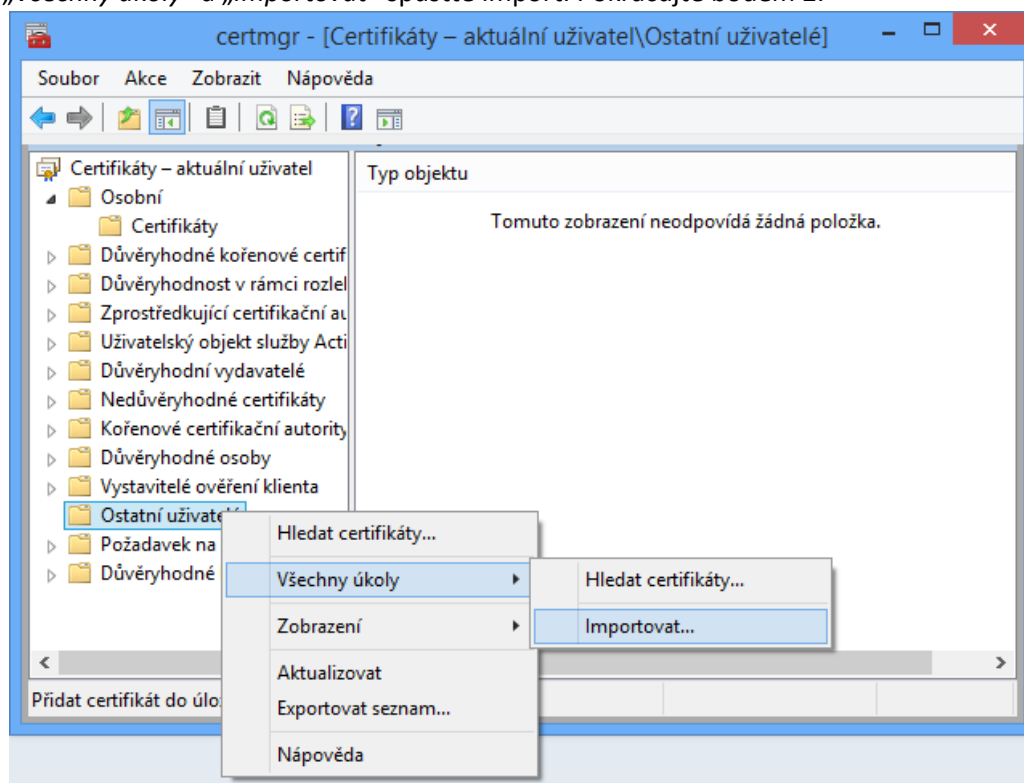
##### 1.2. Přes konzoli

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



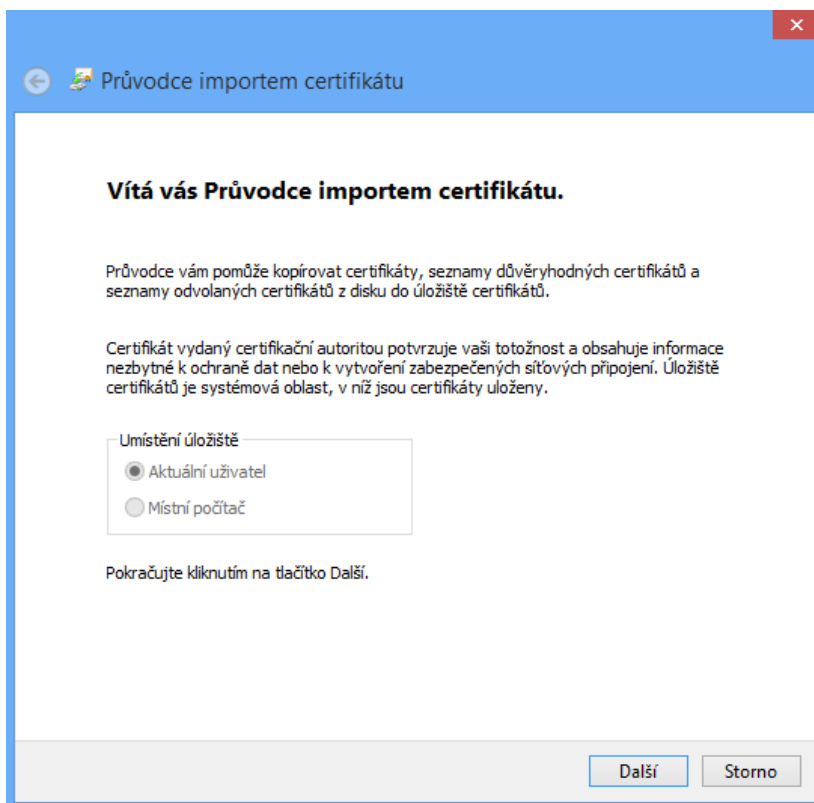


1.2.2. Otevře se seznam certifikátů. Vyberte složku, kam chcete certifikát nainportovat. Vyberte „ostatní uživatelé“. Klikněte pravým tlačítkem na tuto složku a přes volbu „Všechny úkoly“ a „Importovat“ spusťte import. Pokračujte bodem 2.

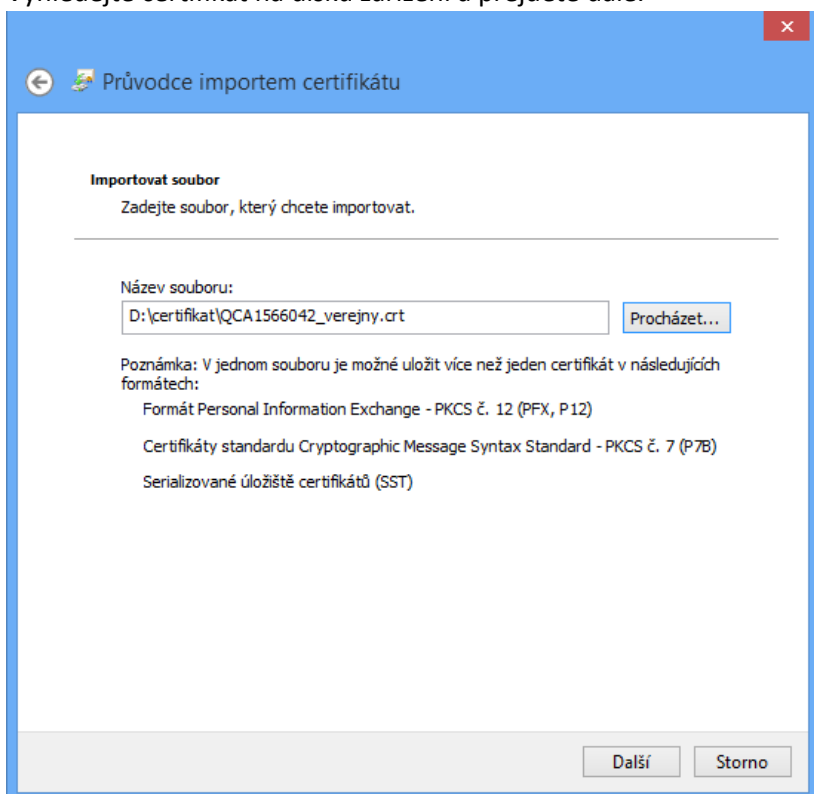


## 2. Samotný import

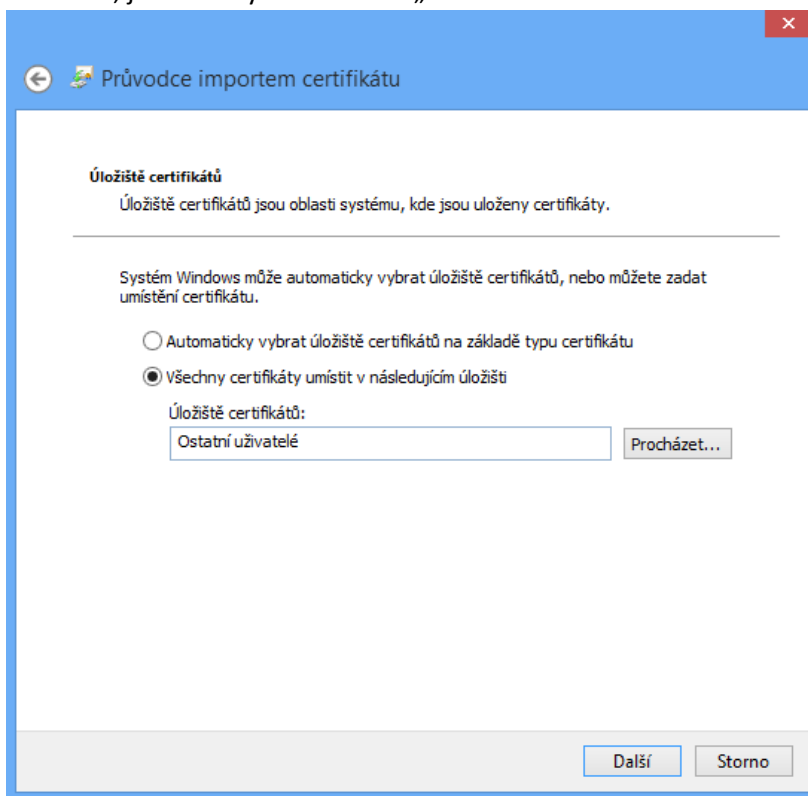
- 2.1. Otevře se průvodce importem certifikátu. Nechejte možnost „Aktuální uživatel“ a pokračujte dále.



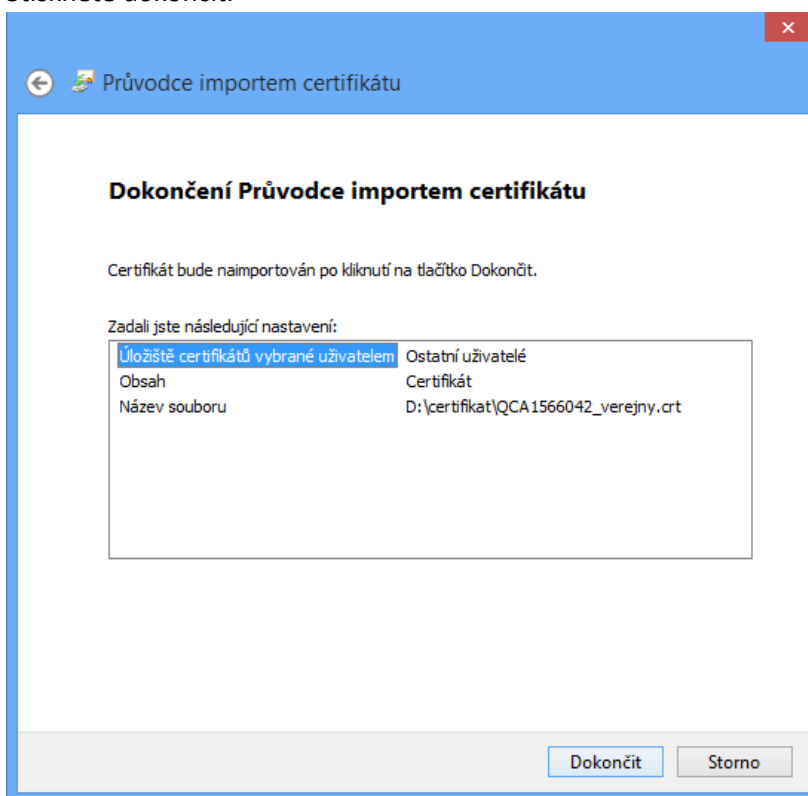
- 2.2. Vyhledejte certifikát na disku zařízení a přejděte dále.



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



- 2.4. Stiskněte dokončit.



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

