

Certifikační autorita EET

Modelové postupy vytvoření souboru žádosti o certifikát

verze 1.0, 1.9.2016

OBSAH

1	Úvod	3
2	Sestavení souboru žádosti o certifikát ve Windows 7	4
	Přidání modulu snap-in Certifikáty do konzoly MMC pro uživatelský účet	4
	Vytvoření žádosti o certifikát	4
3	Vytvoření souboru žádosti o certifikát ve Windows 10	12
4	Sestavení souboru žádosti o certifikát pomocí OpenSSL	17
	Minimální požadavky	17
	Postup vytvoření souboru žádosti	17

1 ÚVOD

Uvedené postupy jsou označovány jako modelové, neboť konkrétní postup závisí vždy na konkrétním typu pokladního zařízení. Při práci s certifikáty pro evidenci tržeb doporučujeme postupovat podle instrukcí dodavatele či výrobce vašeho pokladního zařízení.

Uvedené postupy zahrnují práci se soukromým klíčem. Soukromý klíč musí být chráněn proti zcizení a zneužití, neboť právě soukromý klíč slouží k vytváření elektronických podpisů. Ochrana soukromých klíčů proti zneužití je dle zákona povinností poplatníka.

Z důvodů ochrany soukromého klíče obecně doporučujeme vytvářet žádost o certifikát na zařízení, ve kterém bude soukromý klíč používán.

Aby byl soubor žádosti o certifikát akceptován webovou aplikací CA EET, musí splňovat několik podmínek:

1. Žádost musí obsahovat **RSA klíč o velikosti 2048 bitů**
2. Žádost musí být **korektně podepsána** odpovídajícím soukromým klíčem.
3. Soubor žádosti musí být uložen ve **formátu PKCS#10**.

Jiné podmínky pro obsah žádosti nejsou.

Tento návod ukazuje obecné postupy sestavení souboru žádosti o certifikát na obvyklých platformách.

Vytvořený soubor žádosti (*typická přípona souboru žádosti je .req, .csr či .p10*) lze následně použít pro vydání nového certifikátu na základě souboru žádosti ve webové aplikaci CA EET.

2 SESTAVENÍ SOUBORU ŽÁDOSTI O CERTIFIKÁT VE WINDOWS 7

Obecný postup na zařízeních s Windows 7 a kompatibilními OS spočívá ve dvou krocích:

PŘIDÁNÍ MODULU SNAP-IN CERTIFIKÁTY DO KONZOLY MMC PRO UŽIVATELSKÝ ÚČET

- K provedení tohoto postupu je požadováno minimálně členství ve skupině Users nebo v místní skupině Administrators. Pro vytvoření žádosti o certifikát je nutné přidat modul snap-in do konzoly MMC. *Podrobné informace naleznete na stránkách [technické podpory společnosti Microsoft](#).*
- 1. Klikněte na tlačítko Start, do pole Prohledat programy a soubory zadejte **mmc** a stiskněte klávesu ENTER. *V případě zobrazení žádosti o povolení přístupu zvolte **Povolit***
- 2. V nabídce Soubor klikněte na příkaz **Přidat nebo odebrat modul snap-in**.
- 3. V seznamu *Moduly snap-in k dispozici* dvakrát klikněte na možnost **Certifikáty**.
- 4. Dále postupujte podle následujících pokynů:
 - Jste-li přihlášení jako správce, klikněte na položku **Můj uživatelský účet** a klikněte na tlačítko **Ok** nebo **Dokončit**.
 - Pokud jste přihlášení jako uživatel, otevře se automaticky modul snap-in Certifikáty.
- 5. Pro pozdější použití lze konzolu uložit kliknutím na příkaz **Uložit** v nabídce *Soubor*.

VYTVORENÍ ŽÁDOSTI O CERTIFIKÁT

1. Spusťte modul snap-in Certifikáty pro uživatele (pokud již není automaticky spuštěn po instalaci).
2. Ve stromu konzoly klikněte na položku **Certifikáty - aktuální uživatel** a vyberte úložiště certifikátů Osobní.
3. V nabídce *Akce* přejděte na příkaz *Všechny úkoly*, vyberte položku *Upřesnit operace* a potom kliknutím na položku **Vytvořit vlastní požadavek**
4. Spusťte Průvodce zápisem certifikátu kliknutím na tlačítko **Další**.
5. Na stránce *Vybrat zásady zápisu certifikátů* vyberte **Pokračovat se zásadami zápisu** a klepněte na tlačítko **Další**.
6. Na stránce *Vlastní žádost*:
 - vyberte šablonu (**Žádná šablona**) **Klíč CNG**
 - zaškrtněte políčko **Vynechat výchozí rozšíření**
 - vyberte formát žádosti **PKCS#10**
 - klikněte na **Další**
7. Na stránce *Informace o certifikátu*:
 - Rozbalte nabídku **Podrobnosti** a stiskněte tlačítko **Vlastnosti**
 - Na kartě *Obecné* lze vyplnit název a popis žádosti pro snazší orientaci v žádostech.

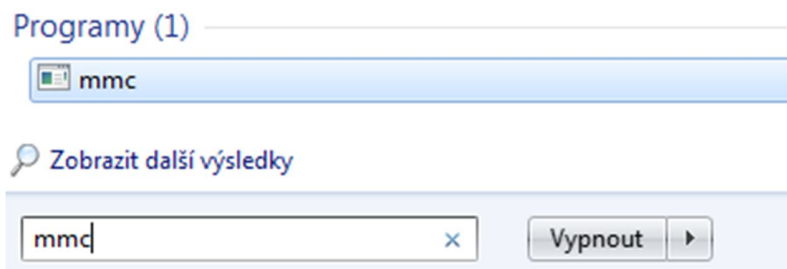
- Na kartě *Privátní klíč* rozbalte nabídku *Možnosti klíče* a nastavte **Velikost klíče** na hodnotu **2048**.
 - Stiskněte tlačítko **Použít** a vraťte se na stránku *Informace o certifikátu* stisknutím tlačítka **Ok** a zde pokračujte klepnutím na **Další**.
8. Vyberte formát souboru **Base 64**, zvolte **umístění a název souboru** žádosti a klikněte na tlačítko **Dokončit**.

Ve zvoleném umístění na disku se nyní vytvořil pod zadaným názvem soubor žádosti, který je možno použít k vydání certifikátu ve webové aplikaci CA EET.

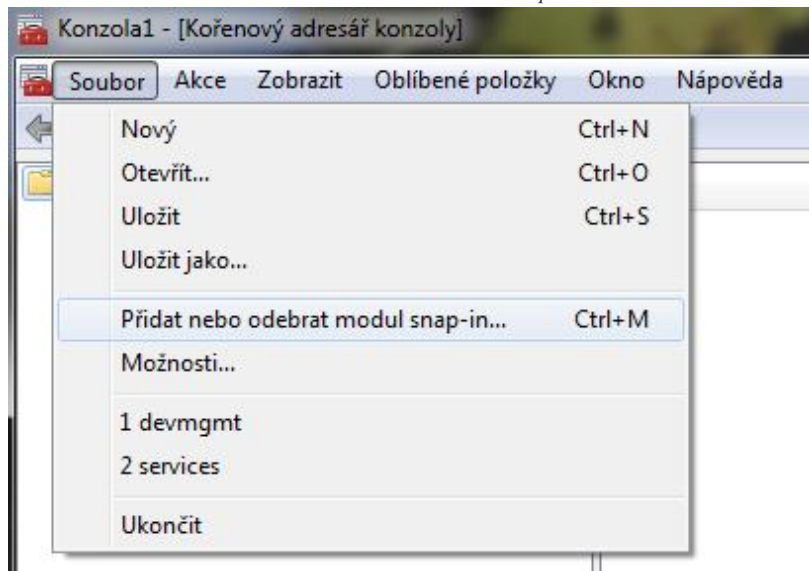
Pozn.: Žádost je možné zkontrolovat po znovuspuštění konzole v ovládacím panelu "Certifikáty pro uživatele" pod položkou "Požadavek na zápis certifikátu"/"Certifikáty".

Obrazová příloha

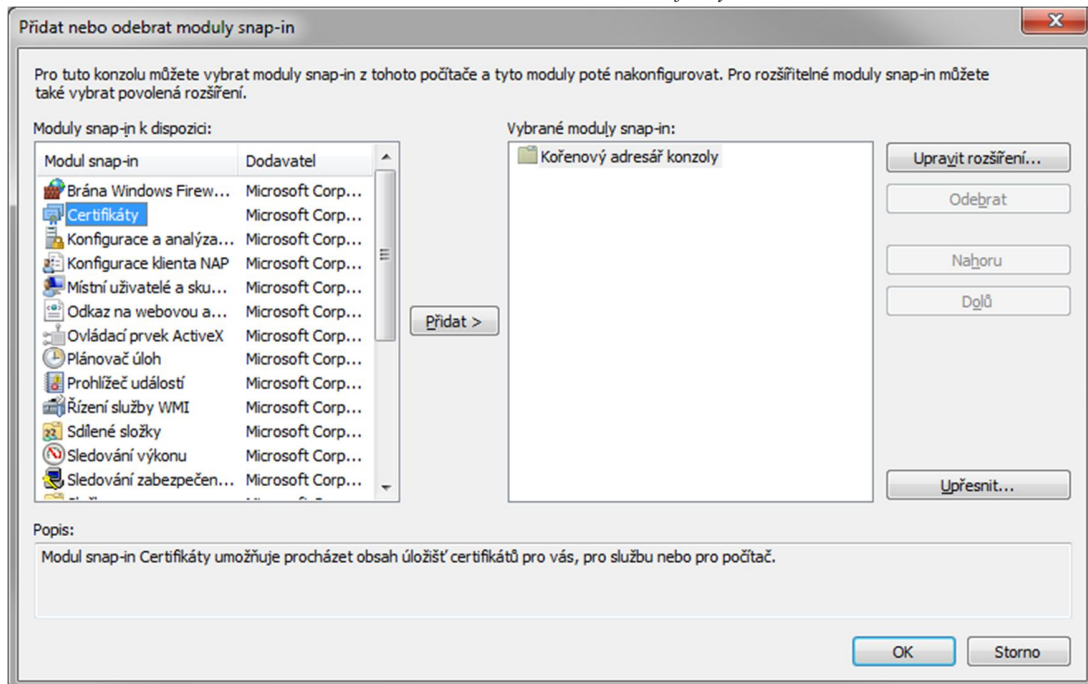
Obrázek 1 Spuštění konzole mmc



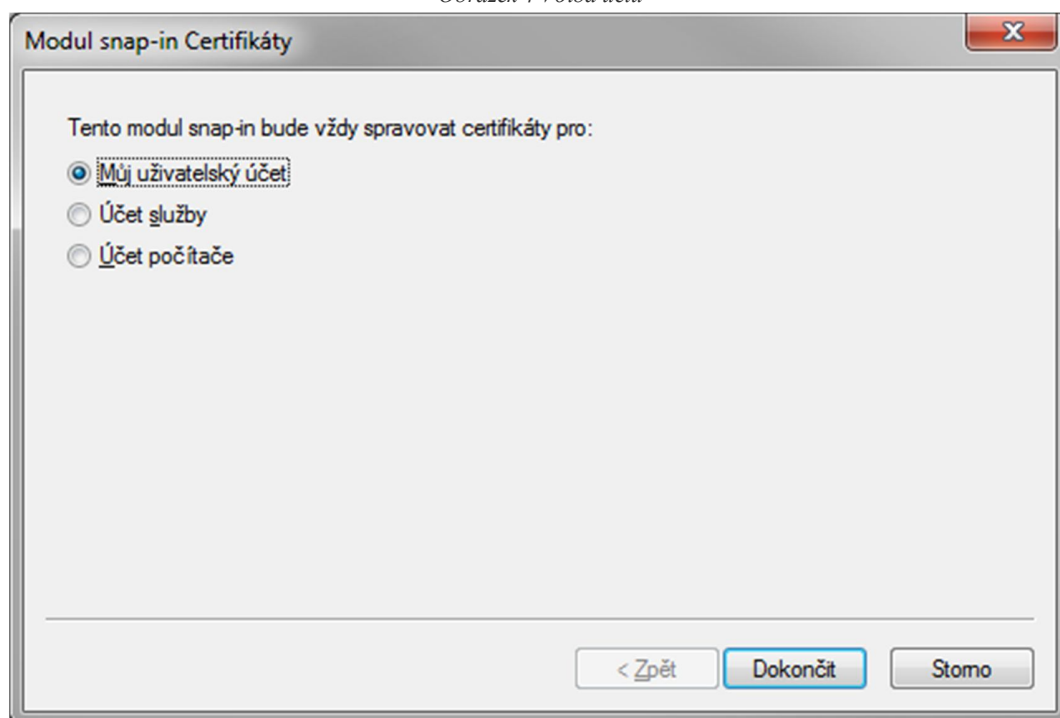
Obrázek 2 Přidání modulu snap-in



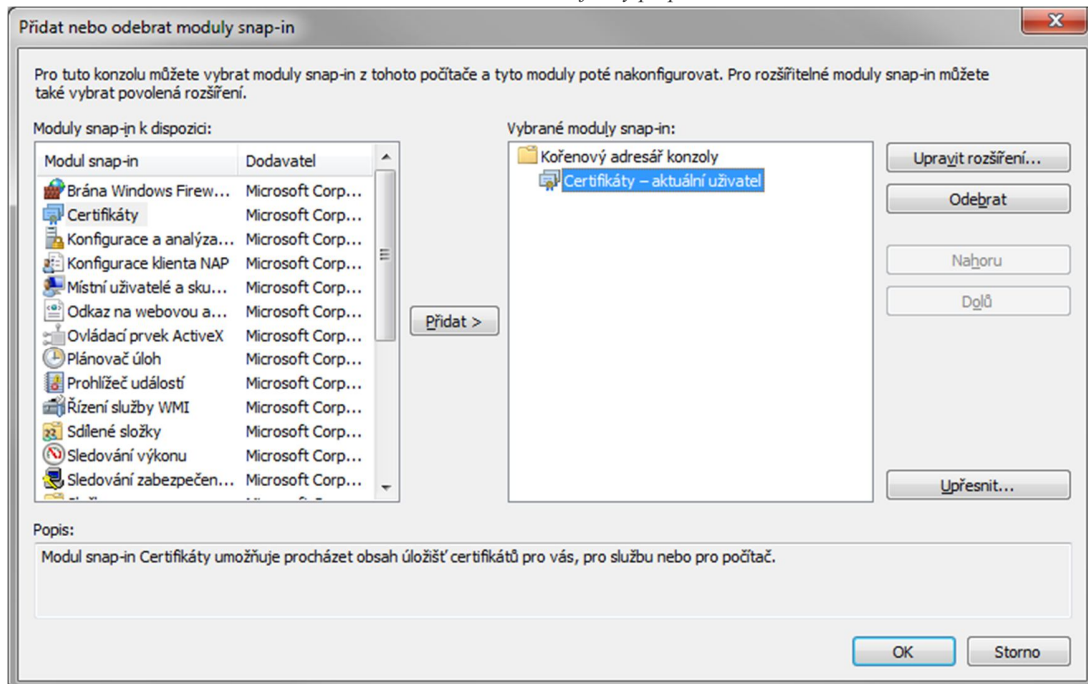
Obrázek 3 Přidání modulu Certifikáty



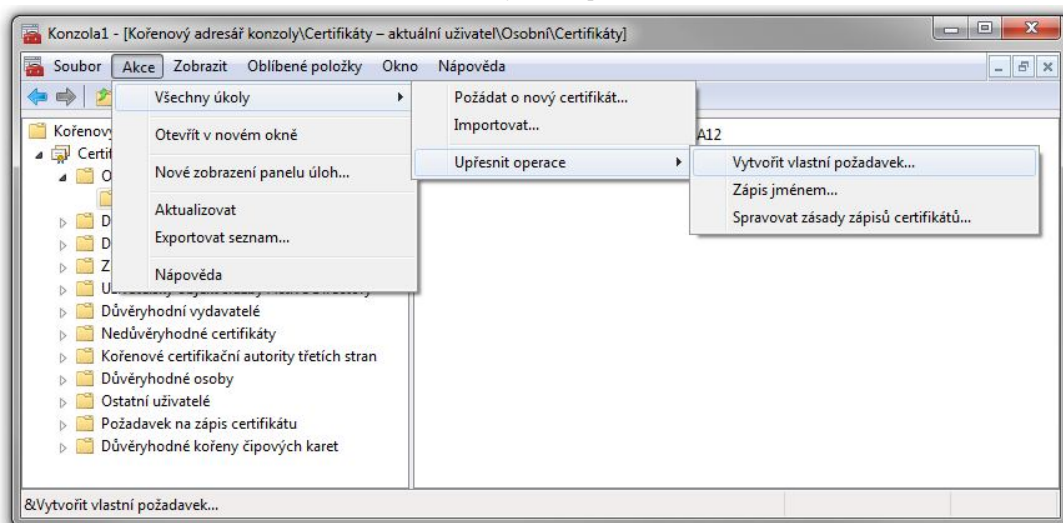
Obrázek 4 Volba účtu



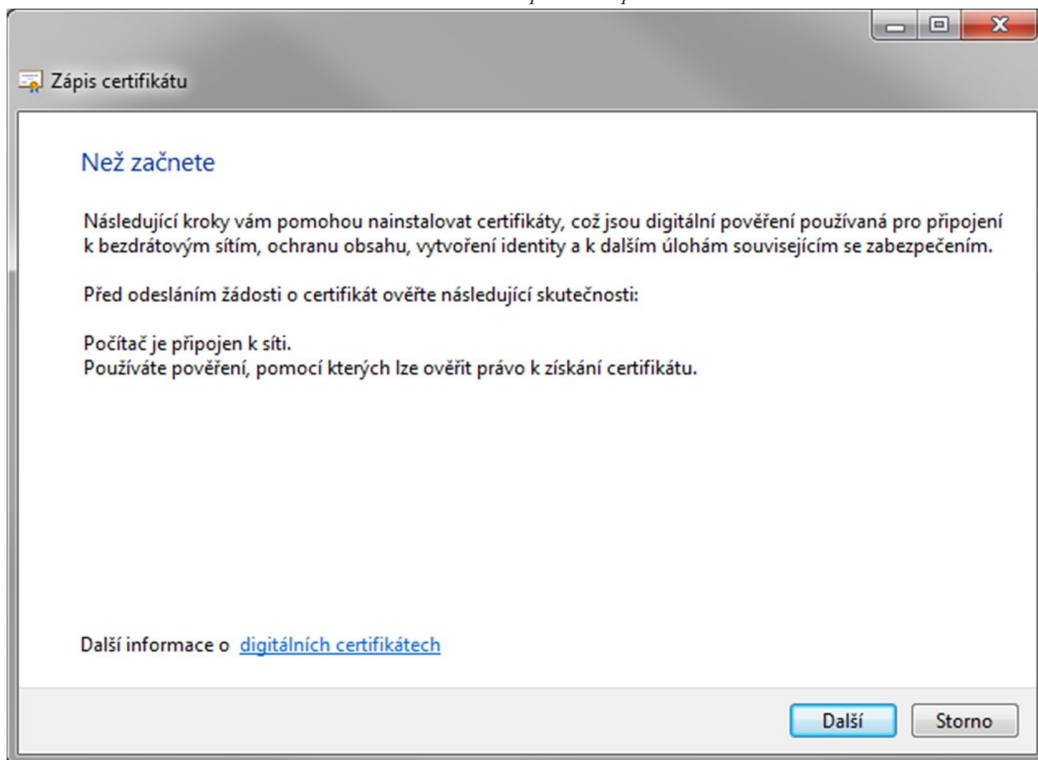
Obrázek 5 Modul Certifikáty po přidání



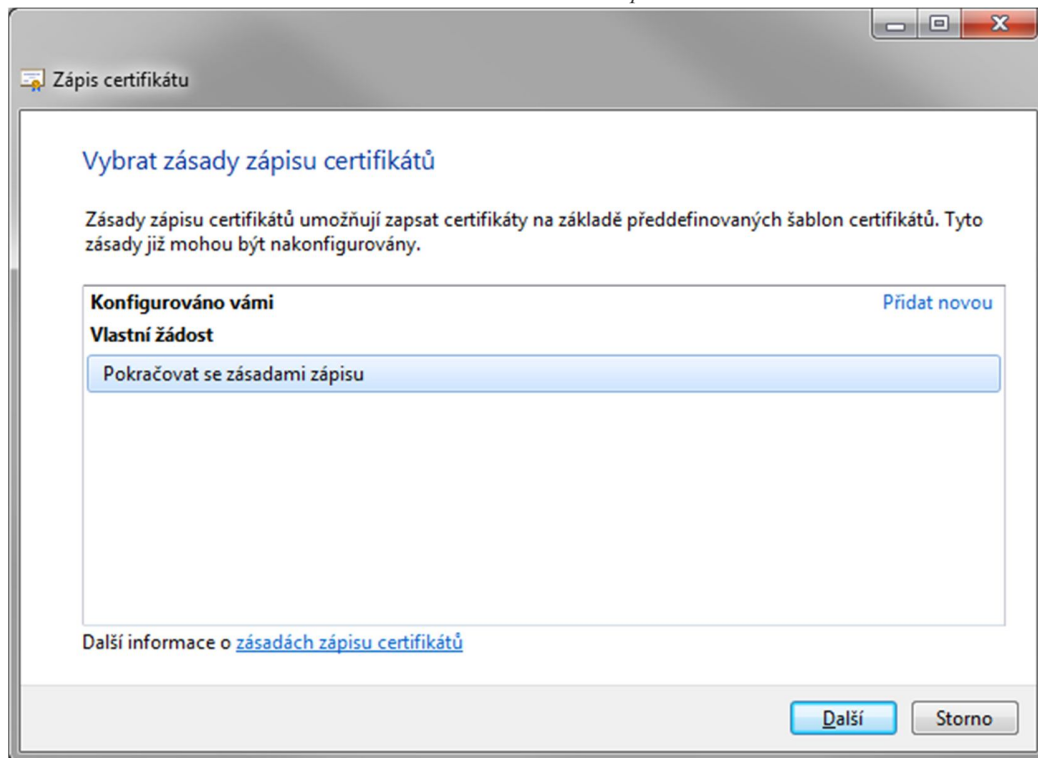
Obrázek 6 Vytvoření požadavku



Obrázek 7 Průvodce přidáním požadavku



Obrázek 8 Volba zásad zápisu



Obrázek 9 Výběr šablony

Zápis certifikátu

Vlastní žádost

Zvolte některou možnost z následujícího seznamu a podle potřeby nakonfigurujte možnosti certifikátu.

Šablona:

Vynechat výchozí rozšíření

Formát žádosti: PKCS #10
 CMC

Poznámka: Archivace klíče není k dispozici pro certifikáty založené na vlastní žádosti o certifikát, i pokud je tato možnost zadána v šabloně certifikátu.

[Další informace o vlastní žádosti](#)

Obrázek 10 Podrobnosti žádosti

Zápis certifikátu

Informace o certifikátu

Klikněte na tlačítko Další, chcete-li použít již vybrané možnosti pro tuto šablonu, nebo na tlačítko Podrobnosti, pokud chcete přizpůsobit žádost o certifikát, a pak klikněte na tlačítko Další.

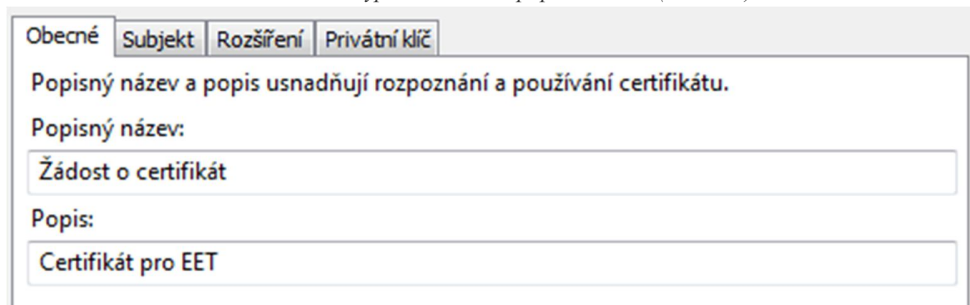
Vlastní žádost Stav: K dispozici Podrobnosti ^

Následující možnosti popisují možnosti použití a dobu platnosti, které platí pro tento typ certifikátu:

Použití klíče:
Zásady použití:
Doba platnosti (dny):

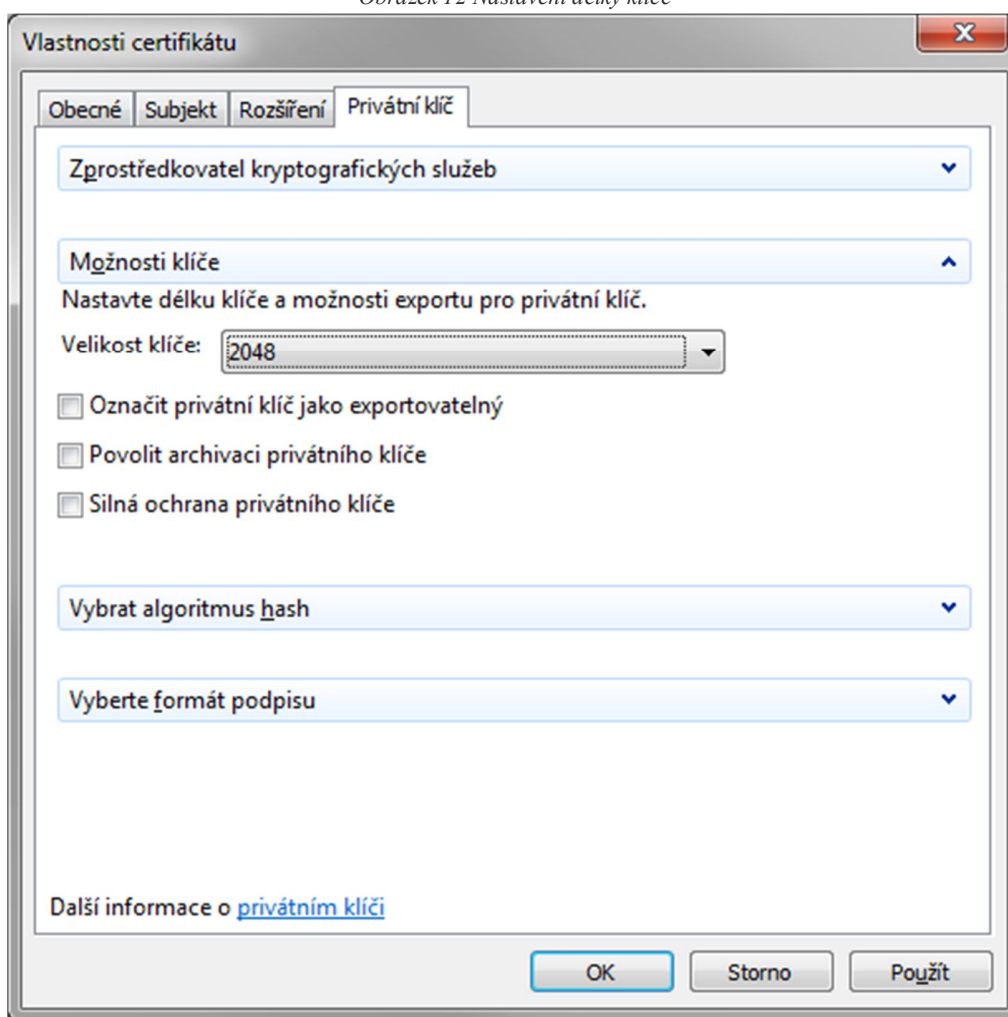
[Další informace o certifikátech](#)

Obrázek 11 Vyplnění názvu a popisu žádosti (volitelné)



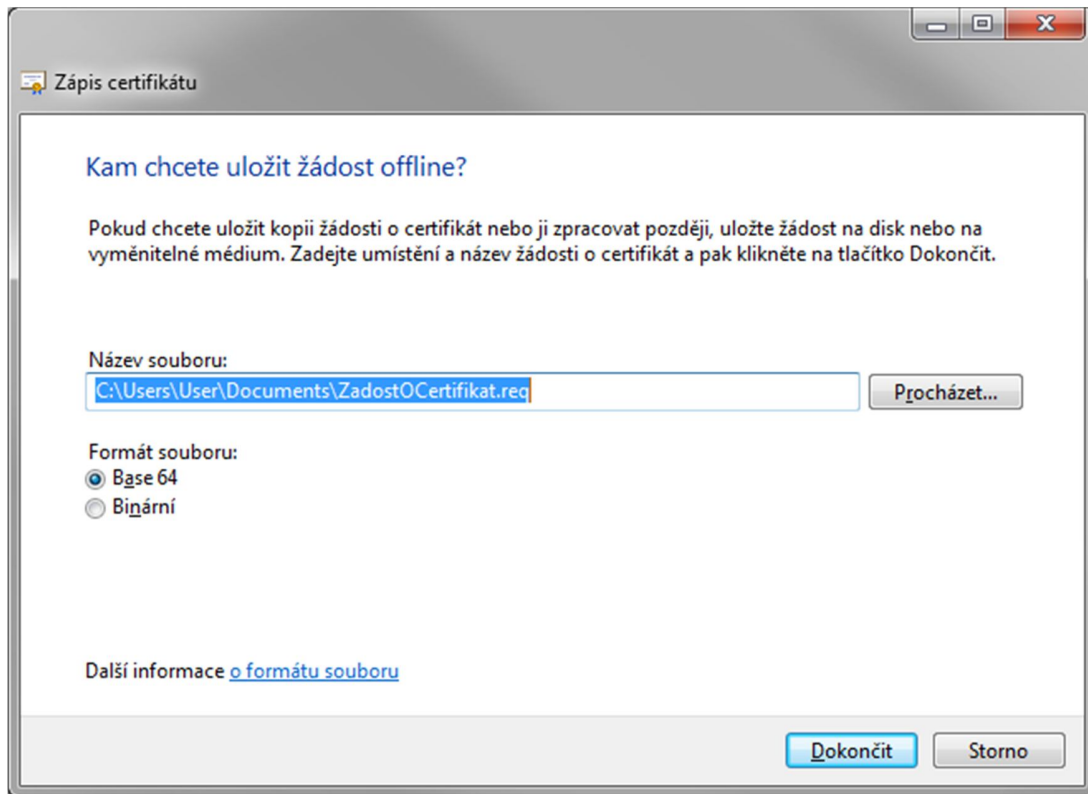
The screenshot shows a window with four tabs: 'Obecné', 'Subjekt', 'Rozšíření', and 'Privátní klíč'. The 'Obecné' tab is active. Below the tabs, there is a heading: 'Popisný název a popis usnadňují rozpoznání a používání certifikátu.' Below this heading, there are two text input fields. The first is labeled 'Popisný název:' and contains the text 'Žádost o certifikát'. The second is labeled 'Popis:' and contains the text 'Certifikát pro EET'.

Obrázek 12 Nastavení délky klíče



The screenshot shows a dialog box titled 'Vlastnosti certifikátu' with a close button (X) in the top right corner. It has four tabs: 'Obecné', 'Subjekt', 'Rozšíření', and 'Privátní klíč'. The 'Privátní klíč' tab is active. Below the tabs, there is a dropdown menu with the text 'Zprostředkovatel kryptografických služeb'. Below that is another dropdown menu with the text 'Možnosti klíče'. Below this is a heading: 'Nastavte délku klíče a možnosti exportu pro privátní klíč.' Below the heading, there is a label 'Velikost klíče:' followed by a dropdown menu showing '2048'. Below this are three checkboxes: 'Označit privátní klíč jako exportovatelný', 'Povolit archivaci privátního klíče', and 'Silná ochrana privátního klíče'. Below the checkboxes are two more dropdown menus: 'Vybrat algoritmus hash' and 'Vyberte formát podpisu'. At the bottom left, there is a link: 'Další informace o [privátním klíči](#)'. At the bottom right, there are three buttons: 'OK', 'Storno', and 'Použít'.

Obrázek 13 Uložení žádosti do souboru



3 VYTVOŘENÍ SOUBORU ŽÁDOSTI O CERTIFIKÁT VE WINDOWS 10

Obecný postup na zařízeních s Windows 10 a kompatibilními OS spočívá v následujících krocích:

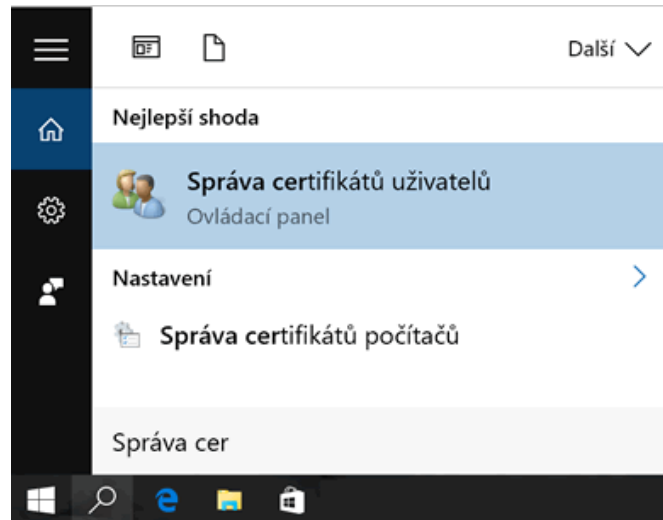
1. Vyhledejte a spusťte ovládací panel **Správa certifikátů uživatelů**. *Typické umístění tohoto panelu v systému Windows je c:32.msc.*
2. Ve stromu panelu dvakrát klikněte na položku **Osobní** a potom klikněte na položku **Certifikáty**.
3. V nabídce *Akce* přejděte na příkaz *Všechny úkoly*, vyberte položku *Upřesnit operace* a potom kliknutím na položku **Vytvořit vlastní požadavek**
4. Spusťte Průvodce zápisem certifikátu kliknutím na tlačítko **Další**.
5. Na stránce *Vybrat zásady zápisu certifikátů* vyberte **Pokračovat se zásadami zápisu** a klepněte na tlačítko **Další**.
6. Na stránce *Vlastní žádost*:
 - vyberte šablonu **(Žádná šablona) Klíč CNG**
 - zaškrtněte políčko **Vynechat výchozí rozšíření**
 - vyberte formát žádosti **PKCS#10**
 - klikněte na **Další**
7. Na stránce *Informace o certifikátu*:
 - Rozbalte nabídku **Podrobnosti** a stiskněte tlačítko **Vlastnosti**
 - Na kartě *Obecné* lze vyplnit název a popis žádosti pro snazší orientaci v žádostech.
 - Na kartě *Privátní klíč* rozbalte nabídku *Možnosti klíče* a nastavte **Velikost klíče** na hodnotu **2048**.
 - Stiskněte tlačítko **Použít** a vraťte se na stránku *Informace o certifikátu* stisknutím tlačítka **Ok** a zde pokračujte klepnutím na **Další**.
8. Vyberte formát souboru **Base 64**, zvolte **umístění a název souboru** žádosti a klikněte na tlačítko **Dokončit**.

Ve zvoleném umístění na disku se nyní vytvořil pod zadaným názvem soubor žádosti, který je možno použít k vydání certifikátu ze souboru ve webové aplikaci CA EET

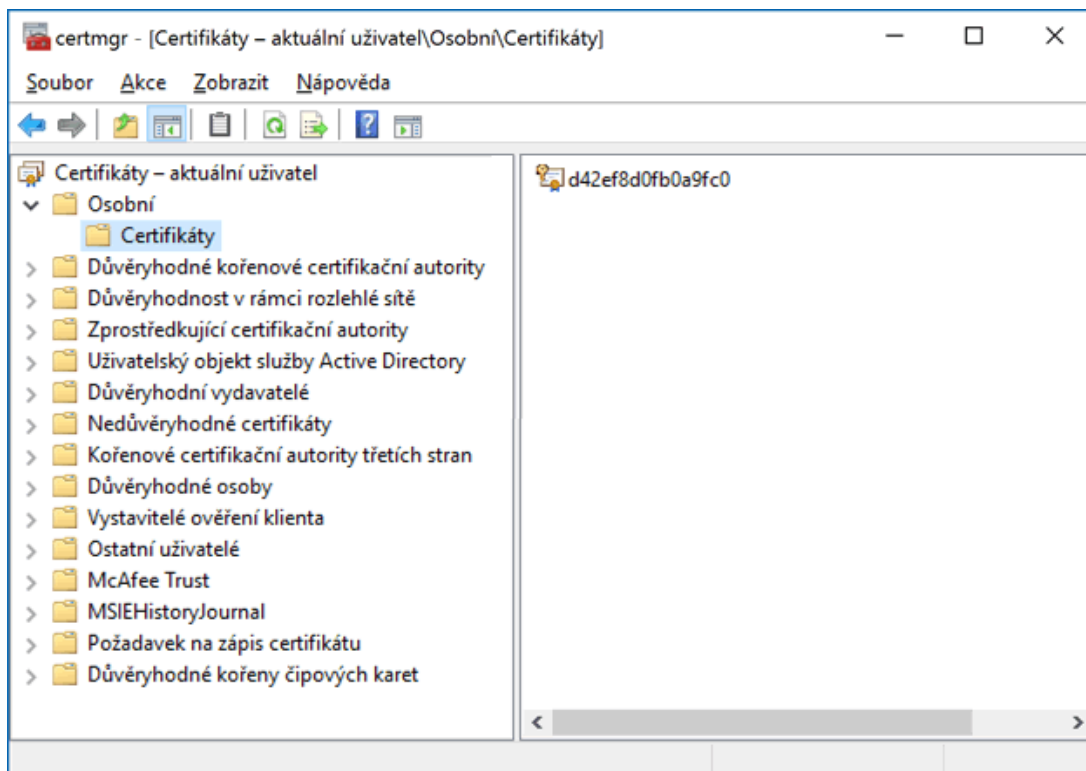
Pozn.: Žádost je možné zkontrolovat v ovládacím panelu "Certifikáty pro uživatele" pod položkou "Požadavek na zápis certifikátu"/"Certifikáty".

Obrazová příloha

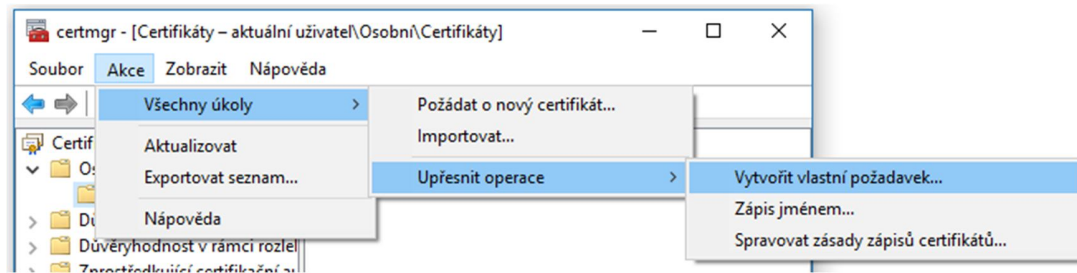
Obrázek 14 Spuštění ovládacího panelu pro správu certifikátů



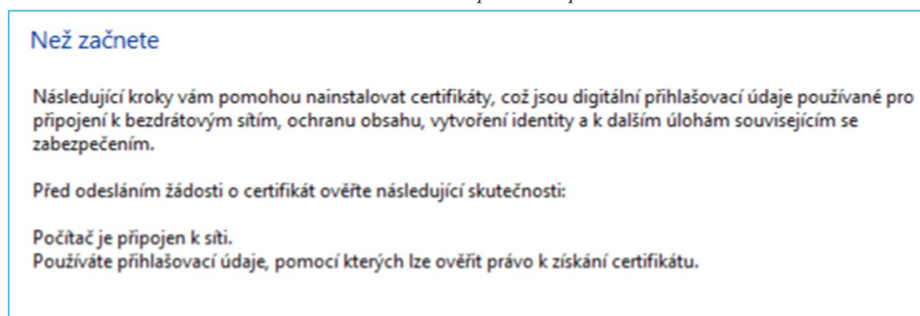
Obrázek 15 Výběr kategorie certifikátů



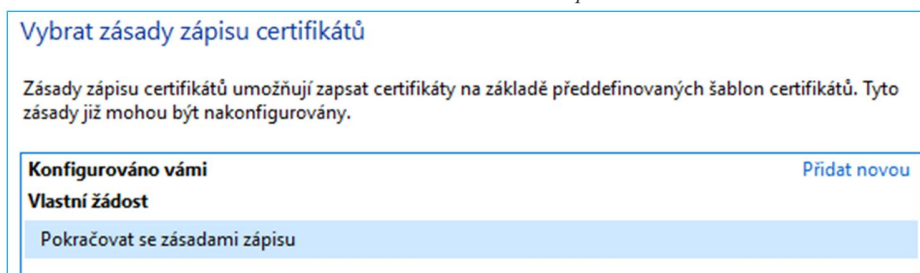
Obrázek 16 Vytvoření požadavku



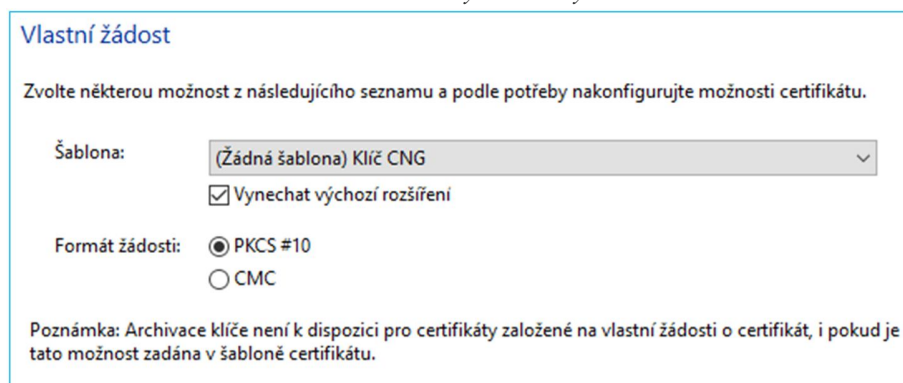
Obrázek 17 Průvodce přidáním požadavku



Obrázek 18 Volba zásad zápisu



Obrázek 19 Výběr šablony



Obrázek 20 Vlastnosti žádosti

Informace o certifikátu

Klikněte na tlačítko Další, chcete-li použít již vybrané možnosti pro tuto šablonu, nebo na tlačítko Podrobnosti, pokud chcete přizpůsobit žádost o certifikát, a pak klikněte na tlačítko Další.

Vlastní žádost Stav: K dispozici Podrobnosti ^

Následující možnosti popisují možnosti použití a dobu platnosti, které platí pro tento typ certifikátu:

Použití klíče:
Zásady použití:
Doba platnosti (dny):

Vlastnosti

Obrázek 21 Vyplnění popisu

Vlastnosti certifikátu ✕

Obecné **Subjekt** Rozšíření Privátní klíč

Popisný název a popis usnadňují rozpoznání a používání certifikátu.

Popisný název:

Popis:

Obrázek 22 Nastavení délky klíče

Vlastnosti certifikátu ✕

Obecné **Subjekt** Rozšíření **Privátní klíč**

Zprostředkovatel kryptografických služeb

Možnosti klíče

Nastavte délku klíče a možnosti exportu pro privátní klíč.

Velikost klíče:

Označit privátní klíč

Povolit archivaci klíče

Silná ochrana klíče

Vybrat algoritmus hash

Vyberte formát podpisu

Obrázek 23 Uložení žádosti do souboru

Kam chcete uložit žádost offline?

Pokud chcete uložit kopii žádosti o certifikát nebo ji zpracovat později, uložte žádost na disk nebo na vyměnitelné médium. Zadejte umístění a název žádosti o certifikát a pak klikněte na tlačítko Dokončit.

Název souboru:
C:\Users\Josef\Documents\ZadostOCertifikat.req Procházet...

Formát souboru:
 Base 64
 Binární

4 SESTAVENÍ SOUBORU ŽÁDOSTI O CERTIFIKÁT POMOCÍ OPENSSL

MINIMÁLNÍ POŽADAVKY

- Tento postup vyžaduje alespoň základní znalosti práce s příkazovou řádkou.
- Pro vygenerování žádosti o certifikát v prostředí operačního systému OS X je nutné:
 - Nejméně Apple Mac OS X verze 10.8 Mountain Lion (včetně aktualizací na 10.8.2).
 - OpenSSL 1.0.1c 10 May 2012 a vyšší.
- Pro vygenerování žádosti o certifikát v prostředí operačních systémů unixového typu je zapotřebí OpenSSL v aktuální verzi v závislosti na distribuci systému.

POSTUP VYTVOŘENÍ SOUBORU ŽÁDOSTI

1. Spustíte Terminál a přesuňte se do adresáře, kde budete chtít žádost o certifikát uložit.
2. Ve vybraném adresáři spustíte následující příkaz:

```
openssl req -out request.req -new -newkey rsa:2048 -keyout privatekey.key
```

 - **request.req** - soubor vygenerované žádosti o certifikát.
 - **privatekey.key** - soukromý klíč (*Pro oba tyto soubory lze zvolit libovolný název*). Soubor soukromého klíče si uschovejte a ujistěte se, že k němu máte přístup pouze vy, popřípadě oprávněná osoba, budete ho potřebovat při instalaci certifikátu.
 - **rsa:2048** - nastavení algoritmu RSA a velikosti klíče na 2048 bitů.
3. Po zadání příkazu budete vyzváni k zadání hesla k soukromému klíči a jeho potvrzení. **Heslo si dobře zapamatujte**, není možné ho dodatečně zjistit, změnit ani odstranit!. Ostatní požadované údaje není nutné vyplňovat, do certifikátu je doplní webová aplikace CA EET.

Vytvořený soubor request.req je možno použít k vydání certifikátu ze souboru ve webové aplikaci CA EET.