Certifikační autorita PostSignum

Generování klíčů a instalace certifikátu pomocí programu PostSignum Tool Plus na čipové kartě, USB tokenu

verze 1.0.0

Uživatelská dokumentace

Březen 2010

1 Obsah

2 Úvod

2.1 Informace o dokumentu

Cílem tohoto dokumentu je podrobně popsat

- instalaci a první spuštění programu PostSignum Tool Plus,
- vygenerování klíčů a žádosti o certifikát,
- instalaci vydaného certifikátu
- postup uvedený v tomto dokumentu je v použití USB tokenu iKey 4000

Součástí dokumentu jsou poznámky k uváděným postupům a bezpečnostní rady, jak dostatečně ochránit váš soukromý klíč před zcizením či zneužitím. Tyto informace jsou vždy uváděny před samotným postupem.

Obrázky v tomto dokumentu mohou být pouze orientační.
Uvedené postupy počítají s ovládáním myši pravou rukou. Leváci musí mačkat druhé tlačítko myši, než je uváděno v postupu.
Podobnost se jmény skutečných osob a organizací je čistě náhodná a neúmyslná.

2.2 Kde využiji popsané postupy?

- Všechny postupy v dokumentu lze aplikovat na libovolné verzi programu PostSignum Tool.Plus

2.3 Chronologické pořadí uváděných postupů

Tento dokument obsahuje několik postupů, které se provádějí v tomto pořadí:

- Stáhnete si a nainstalujete program PostSignum Tool Plus podle postupu v kapitole 3.
- Spustíte program podle postupu v kapitole 4.
- Provedete vygenerování klíčů a uložení žádosti o certifikát na přenosné médium podle postupu v kapitole 5.
- Na pracovišti České pošty si necháte vydat certifikát.
- Spusťte opět program PostSignum Tool Plus a nainstalujte certifikát podle postupu v kapitole 6.

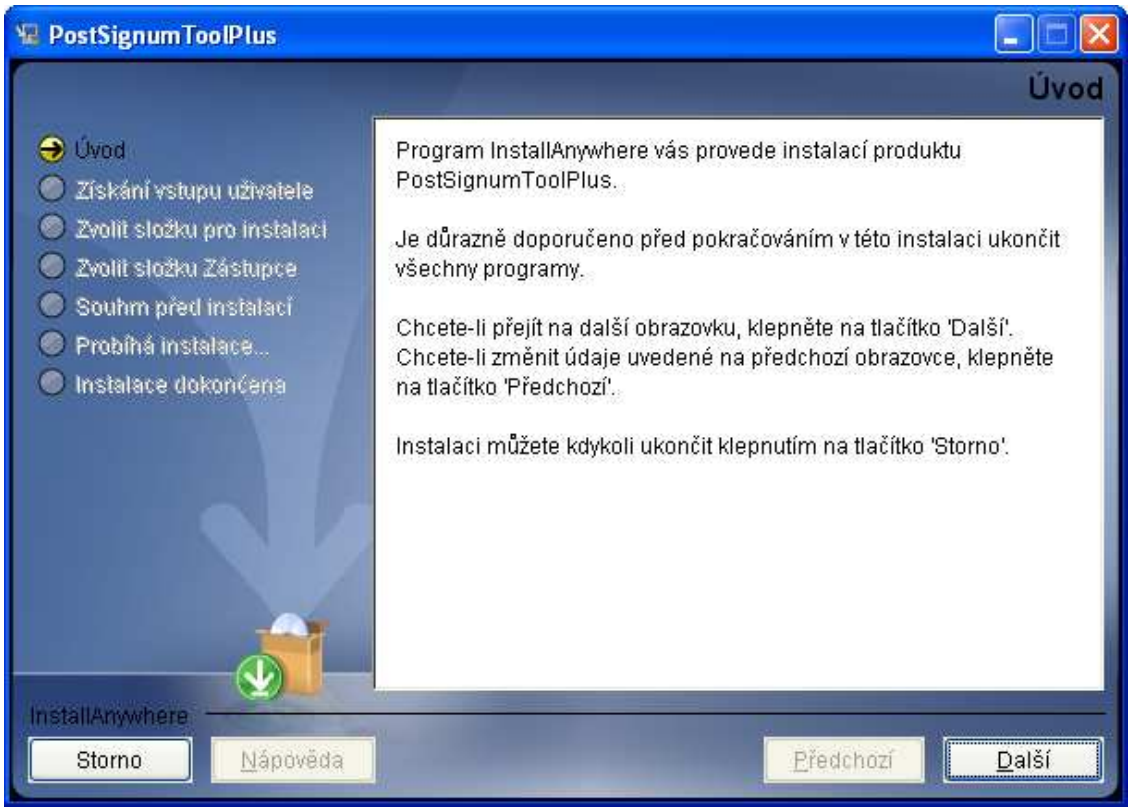
3 Instalace programu

Účel postupu	Pomocí tohoto postupu si nainstalujete program PostSignum Tool. Plus
Typ postupu	povinný
Předpoklady	stažené instalační soubory programu

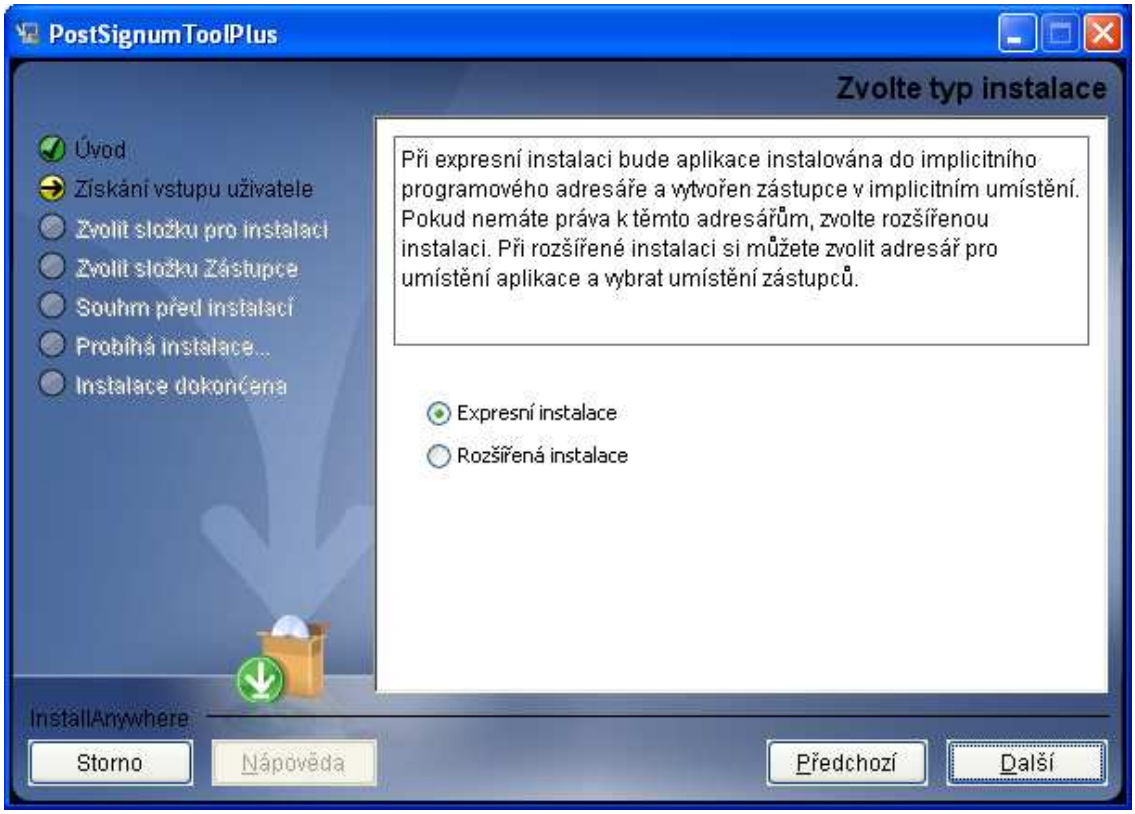
3.1 Spuštění instalátoru PostSignum Tool Plus

Poznámka pro operační systém Windows Vista a Windows 7:
Před spuštěním instalátoru je potřeba se přihlásit pod uživatelským účtem s administrátorskými právy. Nestačí spuštění pomocí funkce **Spustit jako správce**.
Spusťte stažený instalátor nástroje PostSignum Tool Plus. Po chvíli se zobrazí následující obrazovka:

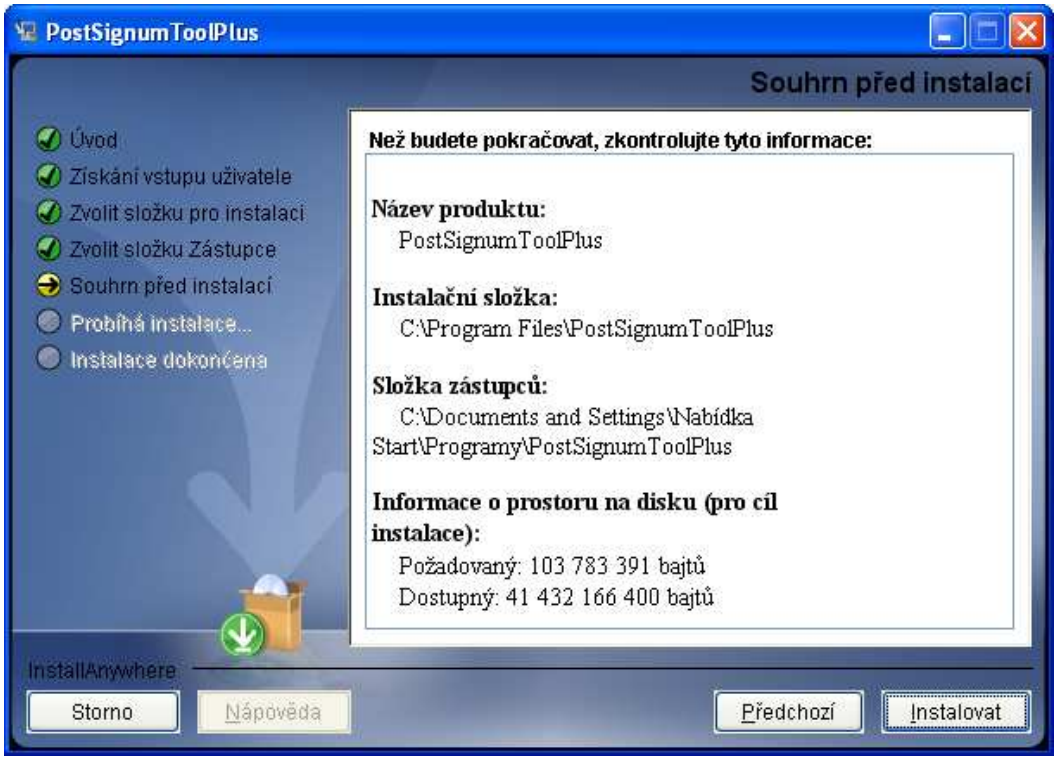
Pro instalaci můžete ponechat předvolený jazyk a stisknout tlačítko **OK**. Po chvíli se zobrazí další okno:



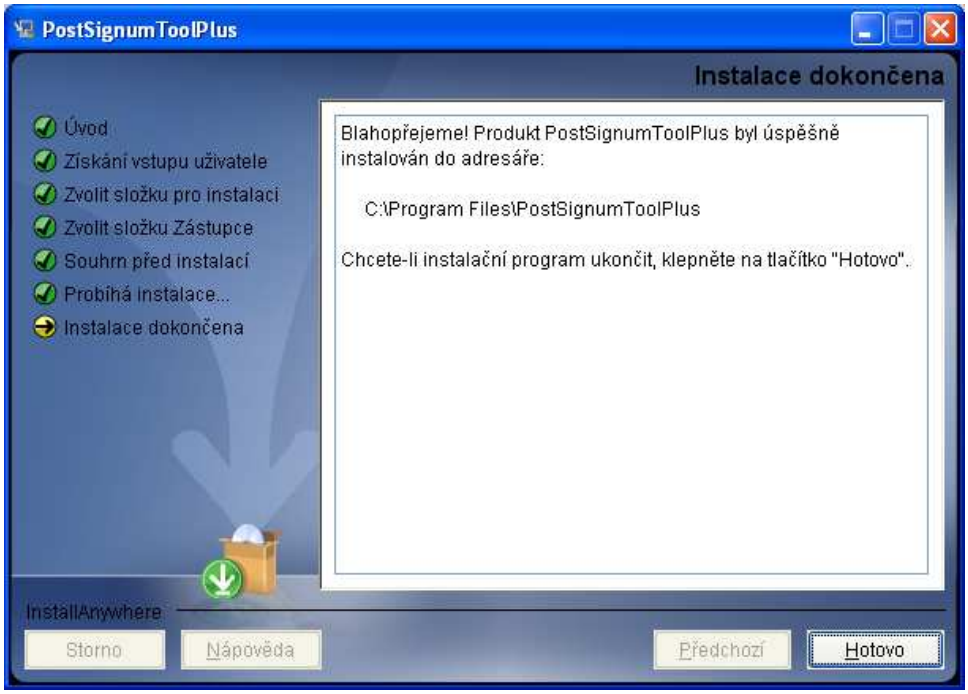
Pokračujte na další obrazovku stisknutím tlačítka **Další**.



Zde máte možnost vybrat expresní instalaci s předvolenými základními hodnotami (doporučujeme) nebo rozšířenou instalaci s možností nastavení vlastních možností instalace. Další postup instalace popisuje volbu typu Expresní instalace.
Pokračujte na další obrazovku stisknutím tlačítka **Další**.



Na této obrazovce jsou uvedeny informace o připravené instalaci. Stisknutím tlačítka **Instalovat** zahájíte instalaci programu:



Po stisknutí tlačítka **Hotovo** se ukončí instalátor programu.

4 První spuštění programu

Účel postupu	Nastavení programu PostSignum Tool Plus před prvním generováním klíčů.
Typ postupu	povinný
Předpoklady	byl nainstalován program PostSignum Tool Plus (kapitola 3)

4.1 Poznámky k postupu

- Další spuštění programu se od toho prvního liší jen tím, že se heslo k adresáři s klíči zadává jen jednou.
- Nesmíte zapomenout heslo k adresáři s klíči, bez něj nemůžete pracovat s klíči uloženými v daném adresáři. Pozor, nelze vytvořit nový adresář s klíči s jiným heslem a nakopírovat do něj soubory ze starého adresáře.

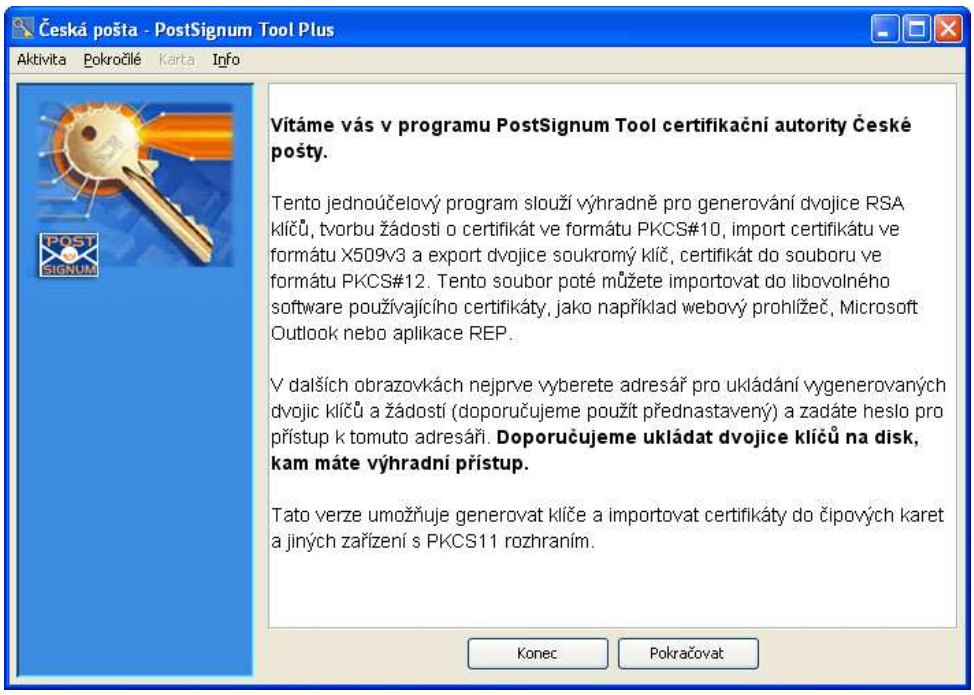
4.2 Bezpečnostní doporučení

- PostSignum Tool Plus automaticky vyžaduje silnější heslo pro ochranu adresáře s klíči. Pro heslo nepoužívejte známá jména a slova. Toto heslo si z bezpečnostních důvodů nikam nepište.

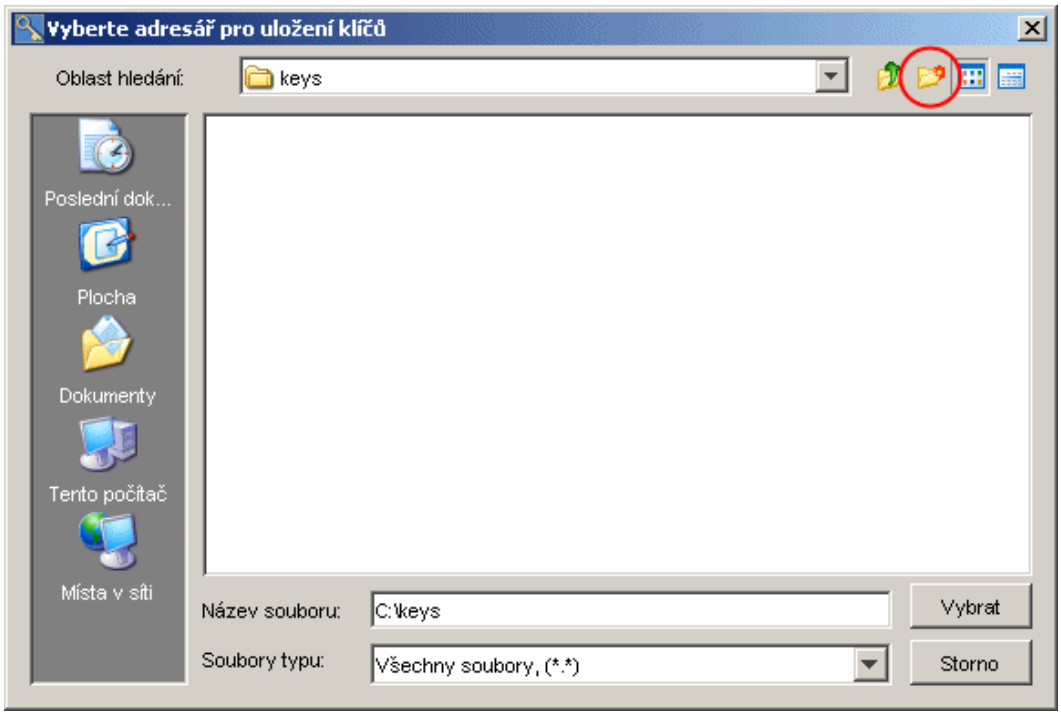
4.3 Postup

V nabídce Start vyhledejte zástupce **PostSignumTool Plus** pro spuštění programu (standardně se nachází ve skupině **PostSignum Tool Plus**).

Po kliknutí na zástupce se zobrazí úvodní okno programu:

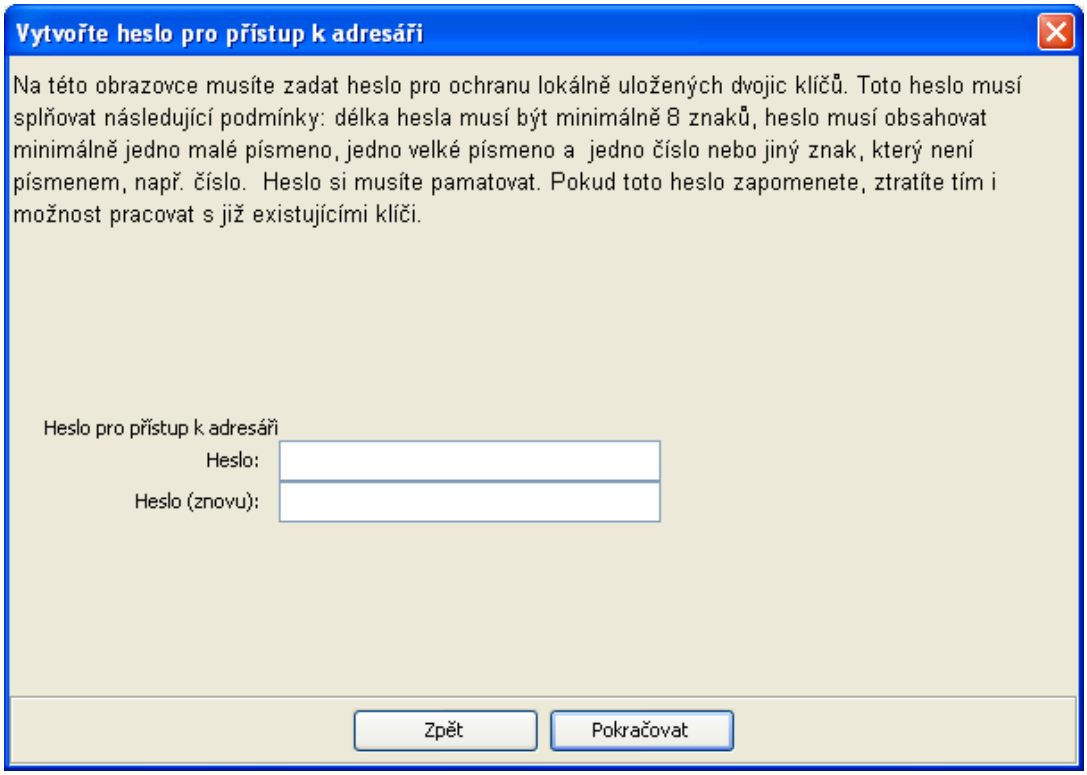


Po stisknutí tlačítka **Pokračovat** se zobrazí následující dialogové okno:



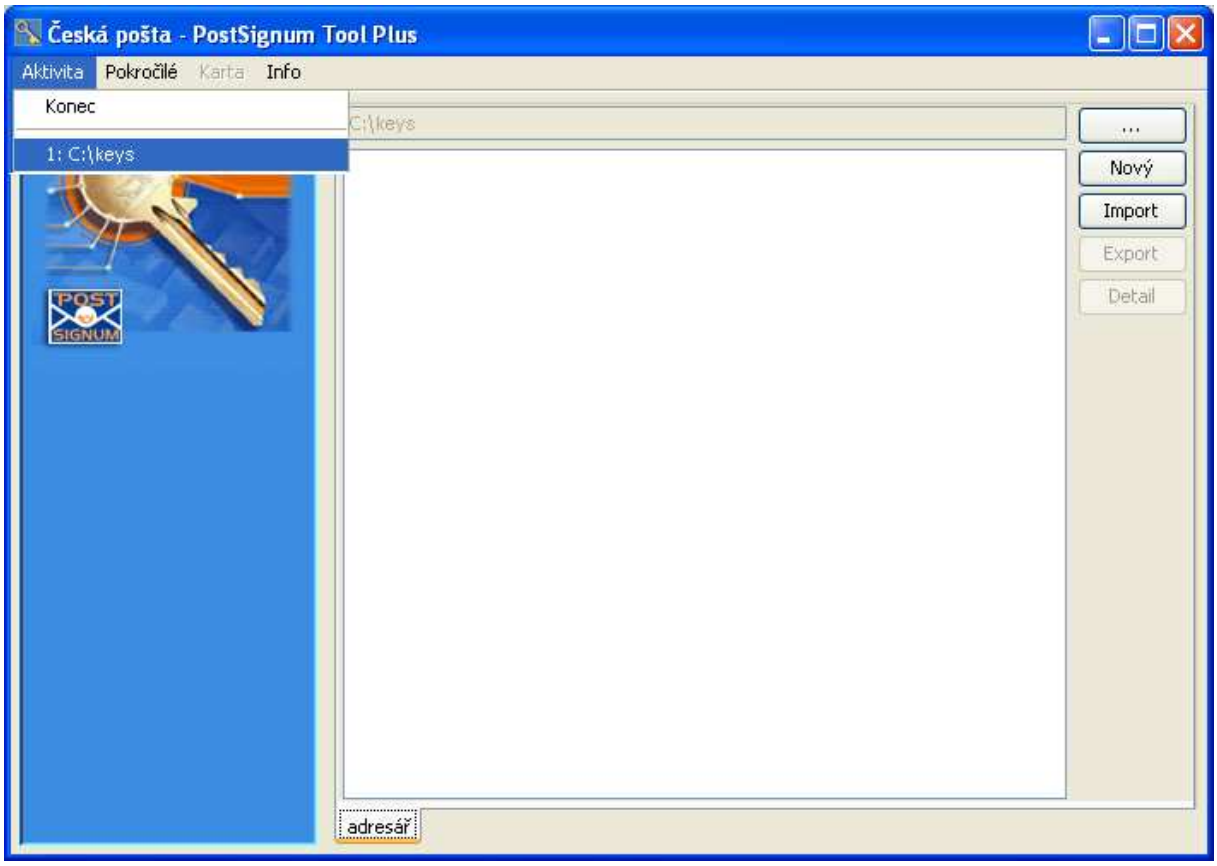
Zadáváte adresář, do nějž se budou ukládat klíče vygenerované programem. Můžete vytvořit nový adresář po stisknutí zvýrazněné ikony na obrázku (takto vytvořit nový adresář je možné pouze na operačním systému Windows) nebo ručně v Průzkumníku či jiném souborovém manažeru.
Jelikož bude adresář obsahovat soubory s citlivým obsahem, měli byste zvolit dostatečnou ochranu tohoto adresáře (omezení přístupu cizím osobám, uložení adresáře na přenosné médium, apod.).

Po zadání adresáře klikněte na tlačítko **Vybrat**. Zobrazí se toto okno:

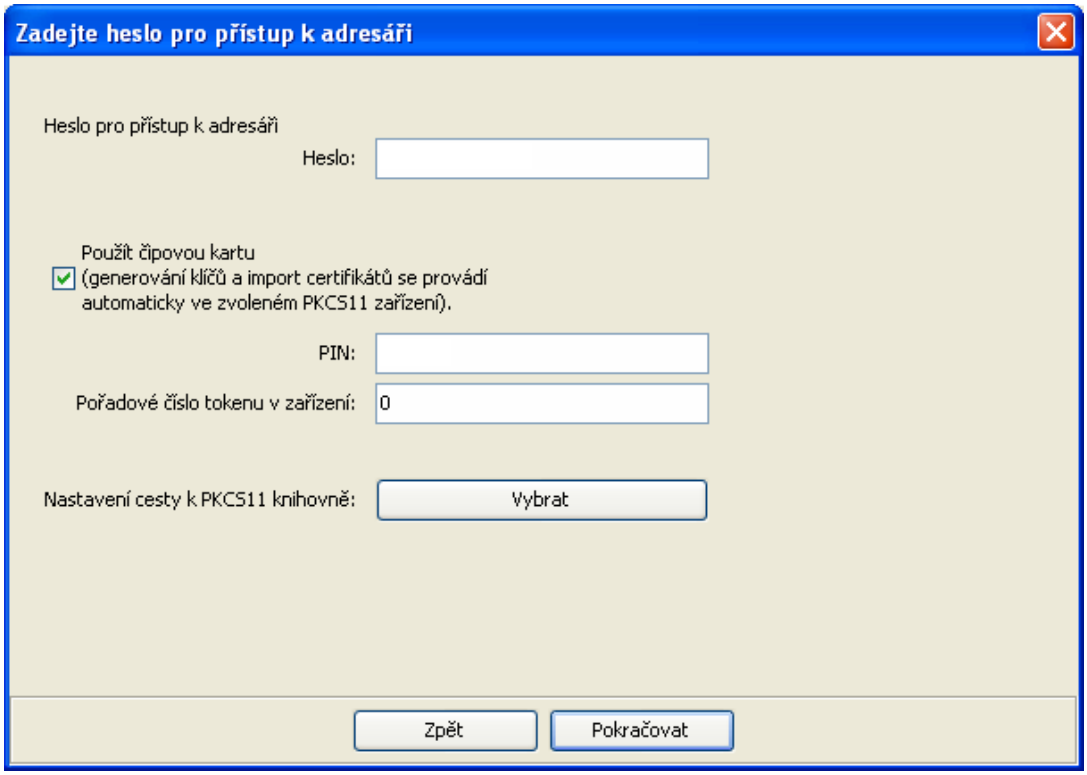


Zadáváte heslo, kterým budou chráněny klíče v adresáři. Aplikace vyžaduje zadání „silného“ hesla. Požadavky na heslo jsou uvedeny v textu okna.

Po stisknutí tlačítka **Pokračovat** se již zobrazí okno s obsahem adresáře s klíči:

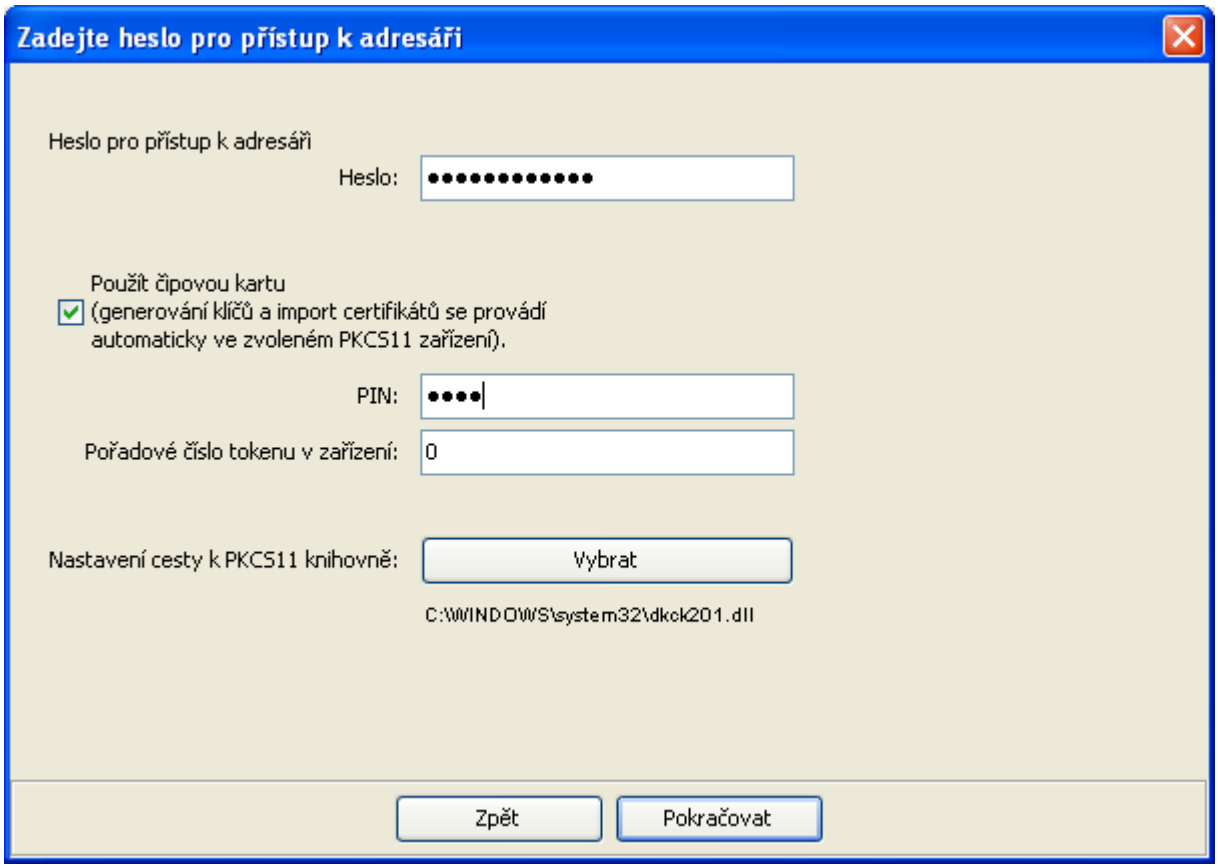


V levém horním rohu klikněte na položku **Aktivita** a dále klikněte na položku s názvem adresáře např **C:\keys**.

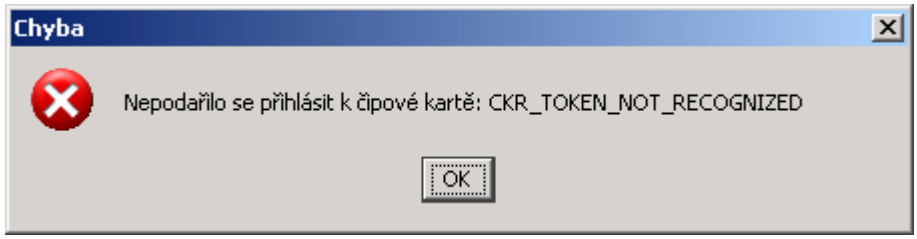


V tomto okně vyplňte heslo k adresáři, které jste zadali v předchozím kroku. Dále zaškrtněte volbu **Použít čipovou kartu** a do pole PIN zadejte **PIN k tokenu**. Pořadové číslo tokenu nechte přednastavené na 0. Dále je potřeba vybrat PKCS11 knihovnu. Stiskněte tlačítko **Vybrat**.

Postupně vyberte: Disk **C**, adresář **Windows**, dále adresář **system32** (načtení tohoto adresáře může trvat déle) a v něm vyhledejte soubor **dkck201.dll**, označte ho a stiskněte tlačítko **Vybrat**.



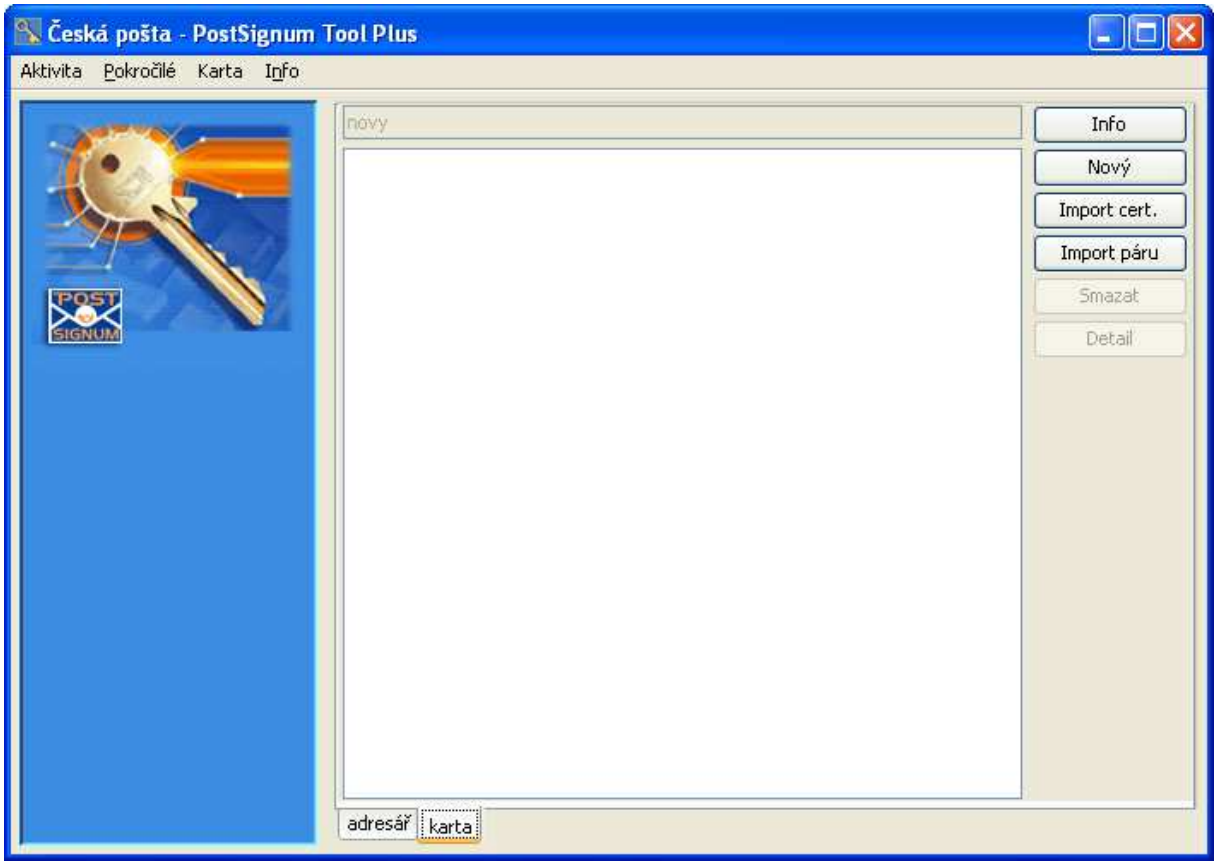
Cesta k vybrané knihovně *C:\Windows\system32\dkck201.dll* by se měla vypsat pod tlačítkem jako na obrázku. Pro pokračování stiskněte tlačítko **Pokračovat**.



Pokud se objeví následující chybová hláška, je v systému pravděpodobně přítomno ještě nějaké jiné zařízení, které umožňuje práci s certifikáty. Např. čtečka čipových karet, jiný token, apod.

V tomto případě potvrďte chybovou hlášku a změňte **Pořadové číslo tokenu v zařízení** na 1 a zvolte **Pokračovat**.

Pokud proběhne vše v pořádku, měl by se zobrazit následující obrázek:



Přepněte se na záložku **karta**.

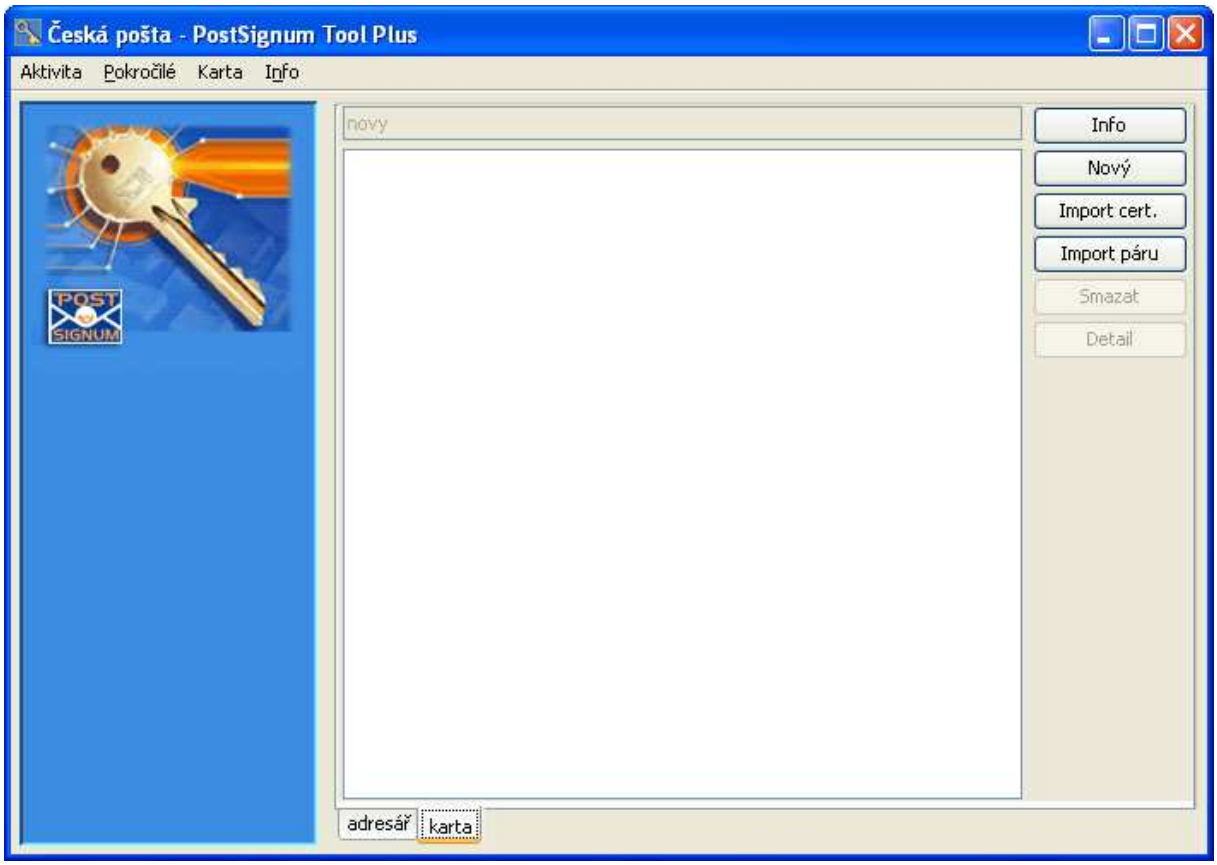
5 Vygenerování klíčů a žádosti o certifikát

Účel postupu	Pomocí tohoto postupu si vygenerujete klíče a nezbytnou žádost o certifikát. Postup je nutné provést před vydáním certifikátu.
Typ postupu	povinný
Předpoklady	vytvořený adresář s klíči (kapitola 4)

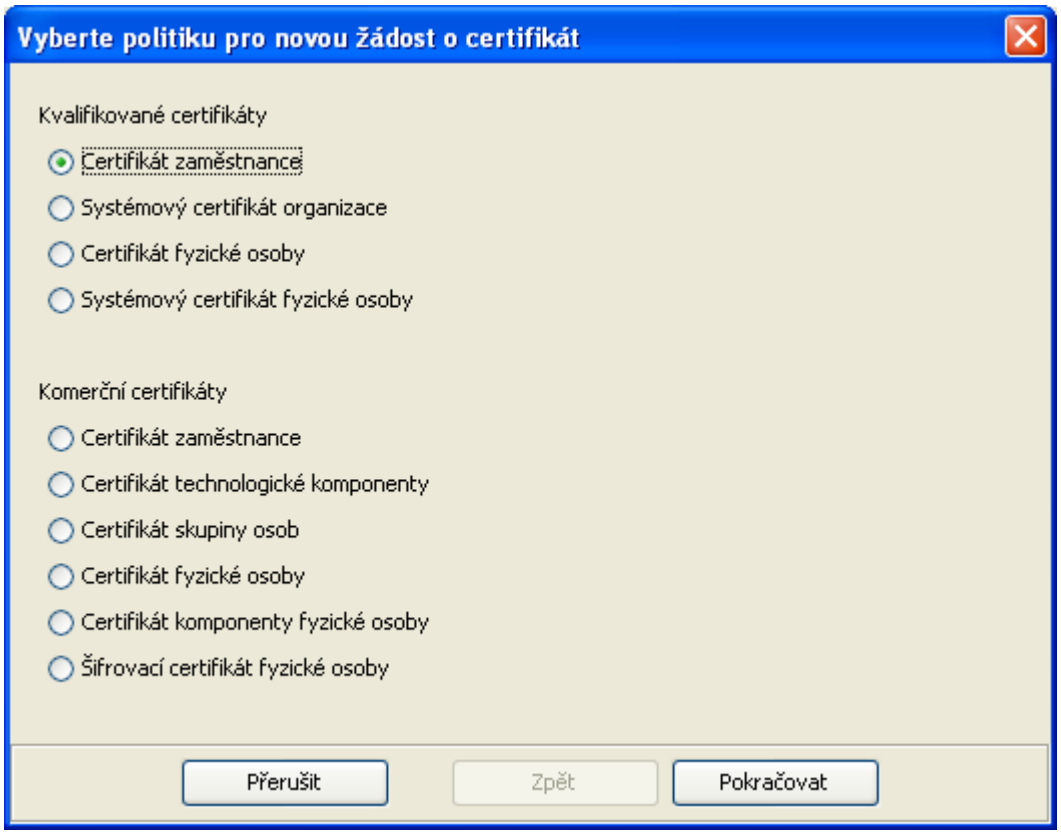
5.1 Poznámky k postupu

- Pomocí volby v menu „Pokročilé“ -> „Povolit další nastavení“ lze měnit parametry generované žádosti o certifikát. **Tuto možnost nedoporučujeme využívat méně zdatným uživatelům PC, vlastní vygenerovaná žádost o certifikát by nemusela jít využít pro vydání certifikátu.**

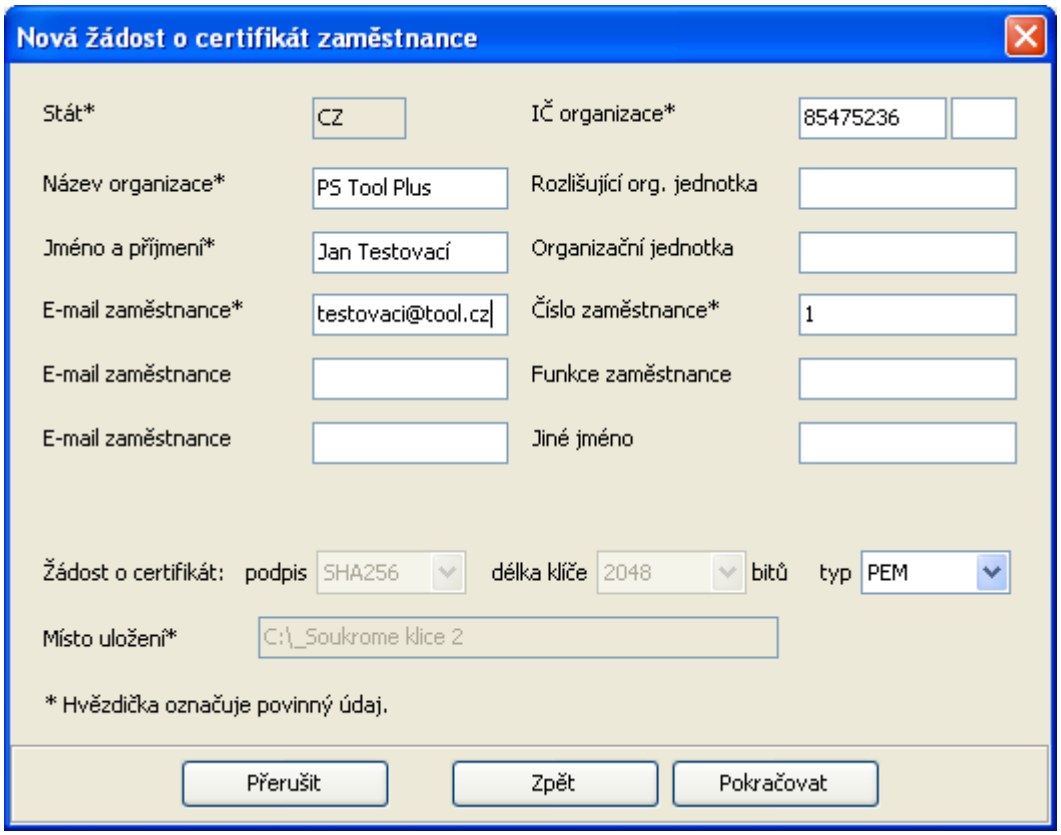
5.2 Postup



Ve spuštěné aplikaci se po kliknutí na tlačítko **Nový** se zobrazí toto okno:

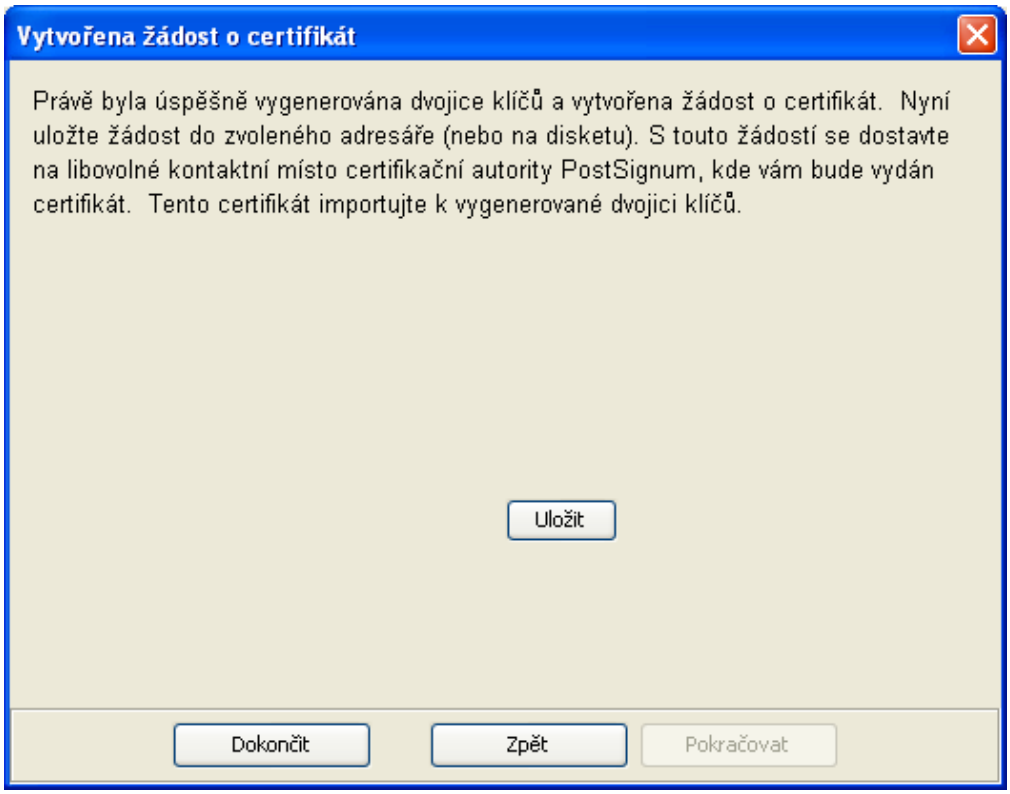


Program generuje klíče a žádosti o vydání komerčních i kvalifikovaných certifikátů.
Vyberte o jaký druh certifikátu budete žádat. Po stisknutí tlačítka **Pokračovat** se zobrazí další okno:

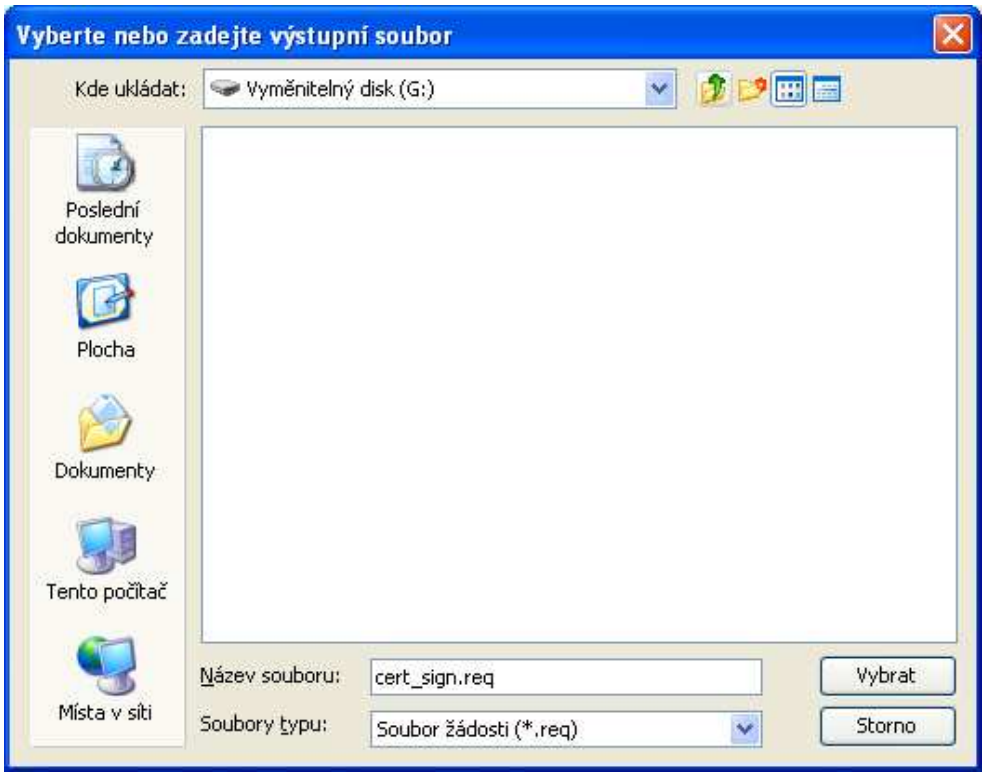


Obrazovka je odlišná na základě výběru z předchozí obrazovky. Povinně musíte vyplnit pouze pole označená hvězdičkou.

Po stisknutí tlačítka **Pokračovat** již bude zahájeno generování klíčů.
Po vygenerování klíčů se zobrazí obrazovka informující o úspěšném vygenerování klíčů:

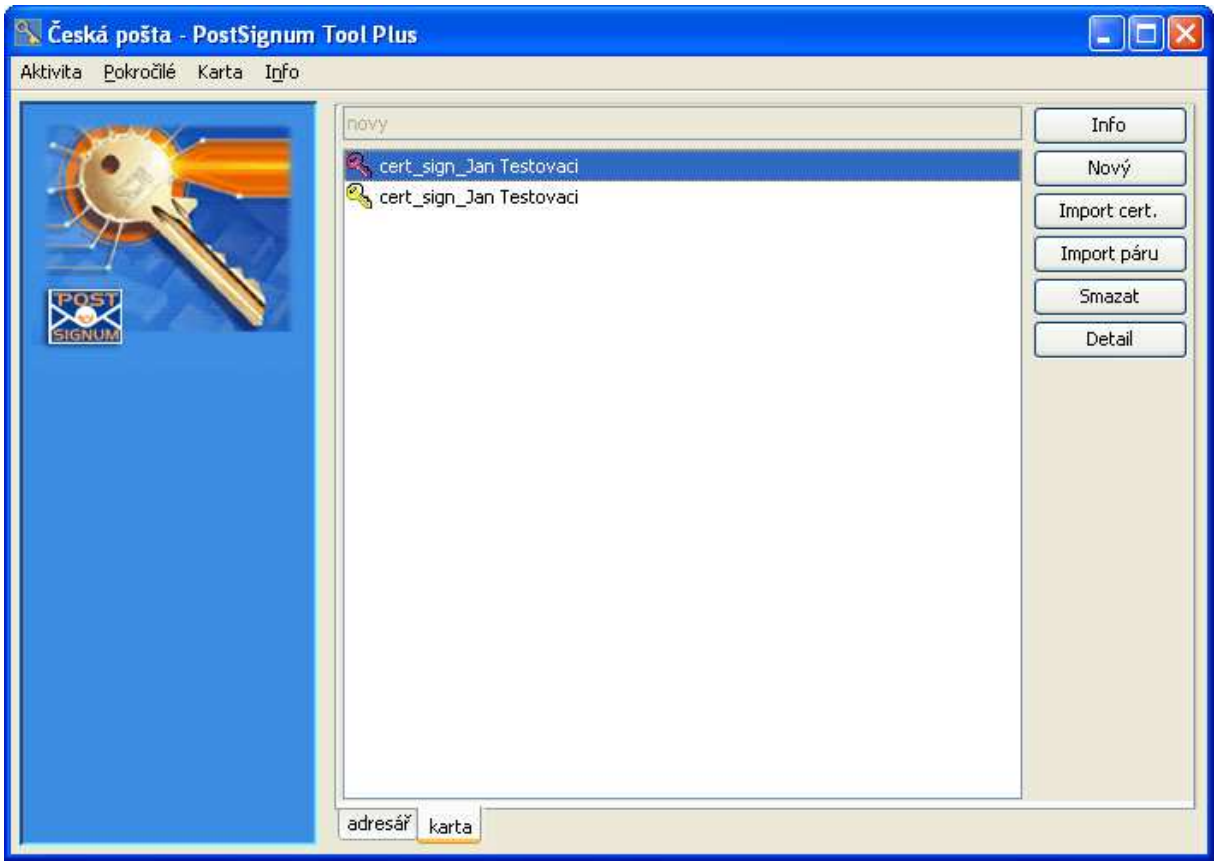


Stiskněte tlačítko **Uložit** a vyberte adresář, do kterého se uloží žádost o certifikát:



Zadejte jiný adresář než adresář s klíči. Můžete soubory uložit přímo na přenosné médium.

Po stisknutí tlačítka **Vybrat** se vrátíte do předešlého okna, v němž stiskněte tlačítko **Dokončit**. Vrátíte se do hlavního okna programu, ve kterém bude nyní již zobrazen vygenerovaný klíč:

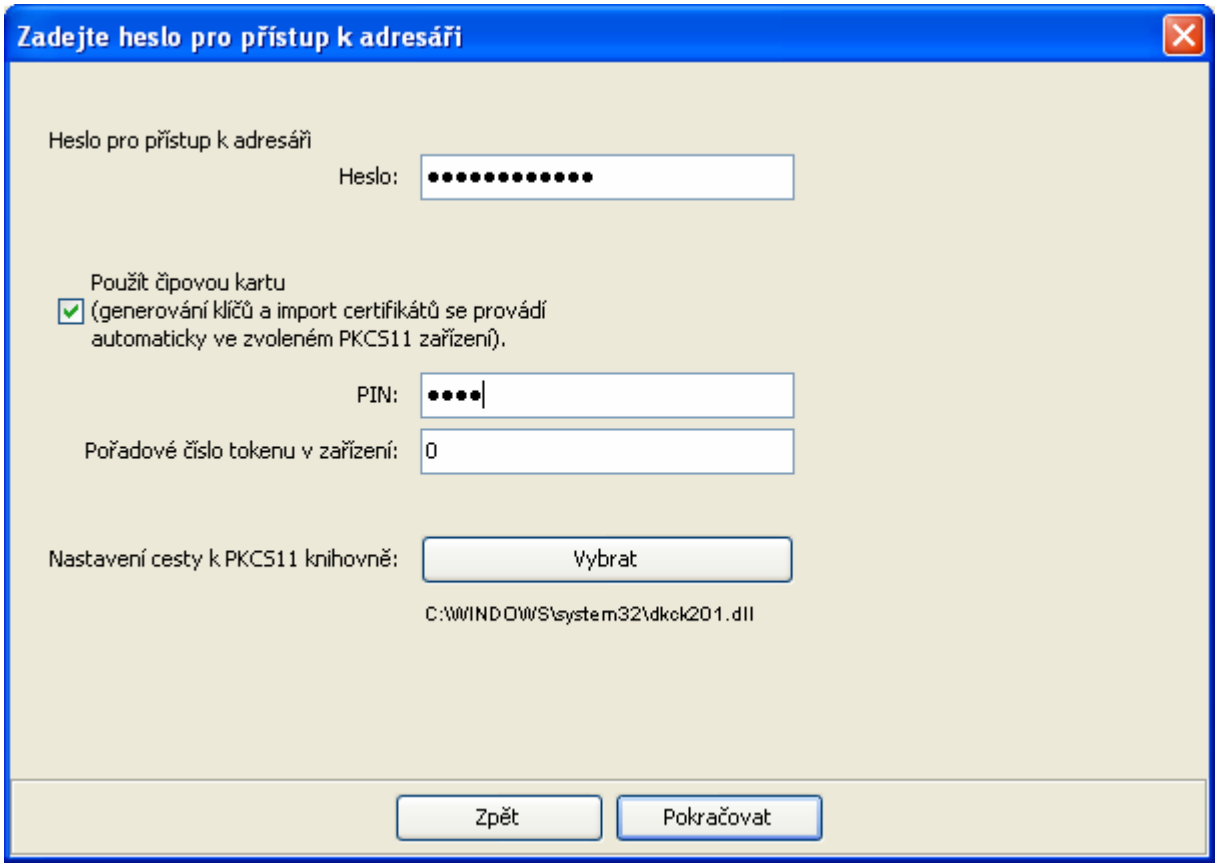


6 Instalace vydaného certifikátu

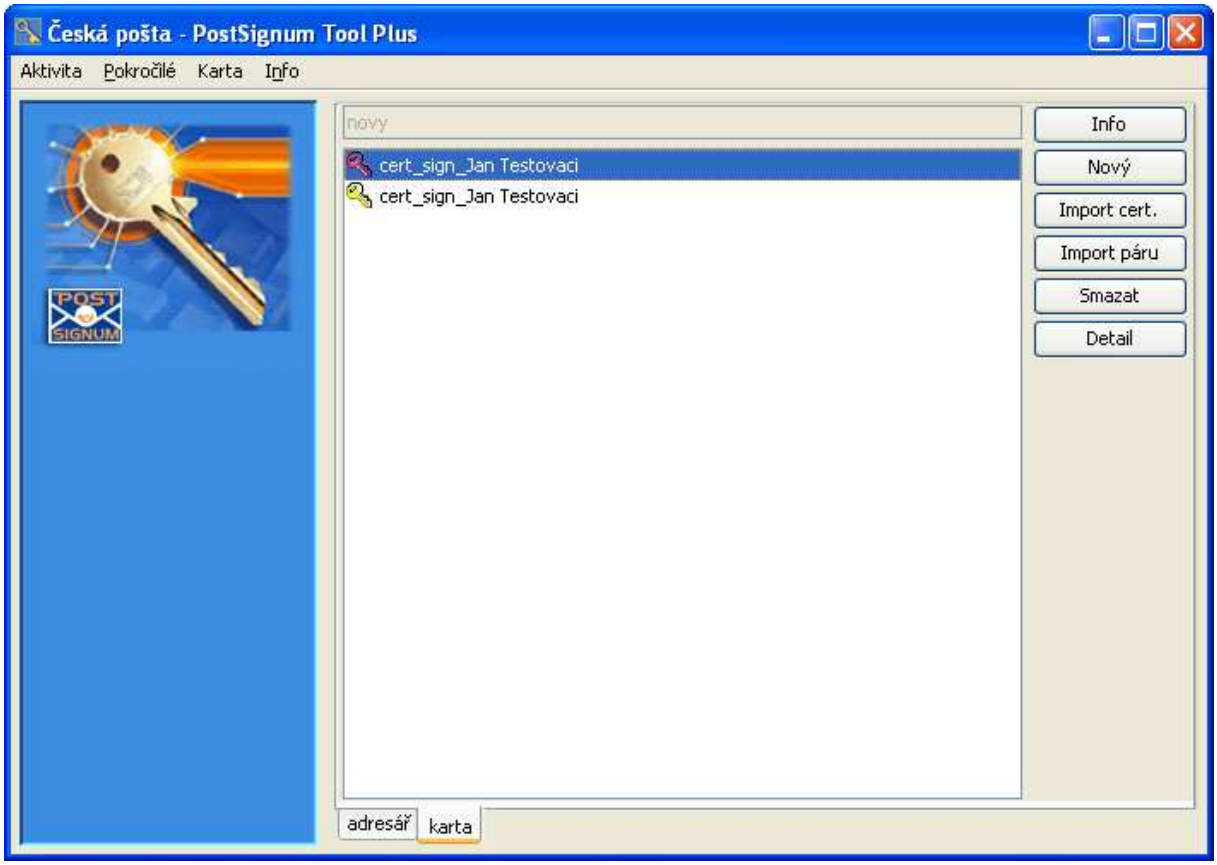
Účel postupu	Certifikát, který vám byl vydán na kontaktním místě České pošty, je potřeba nainstalovat do adresáře s klíči.
Typ postupu	povinný
Předpoklady	byl proveden postup vygenerování klíčů a žádosti o certifikát (kapitola 5)

6.1 Instalace vydaného certifikátu na čipovou kartu/USB token

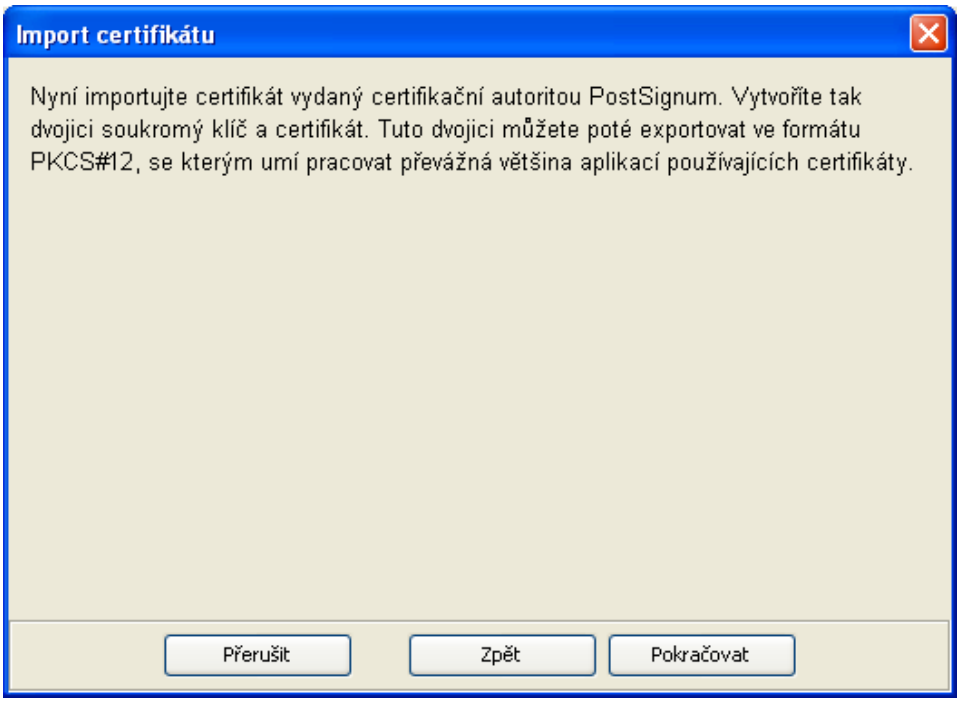
Spusťte program vyhledejte adresář se soukromými klíči kde probíhalo generování klíčů a zadejte heslo k tomuto adresáři (bylo zadáváno v kapitole 4.3) a zadejte PIN.



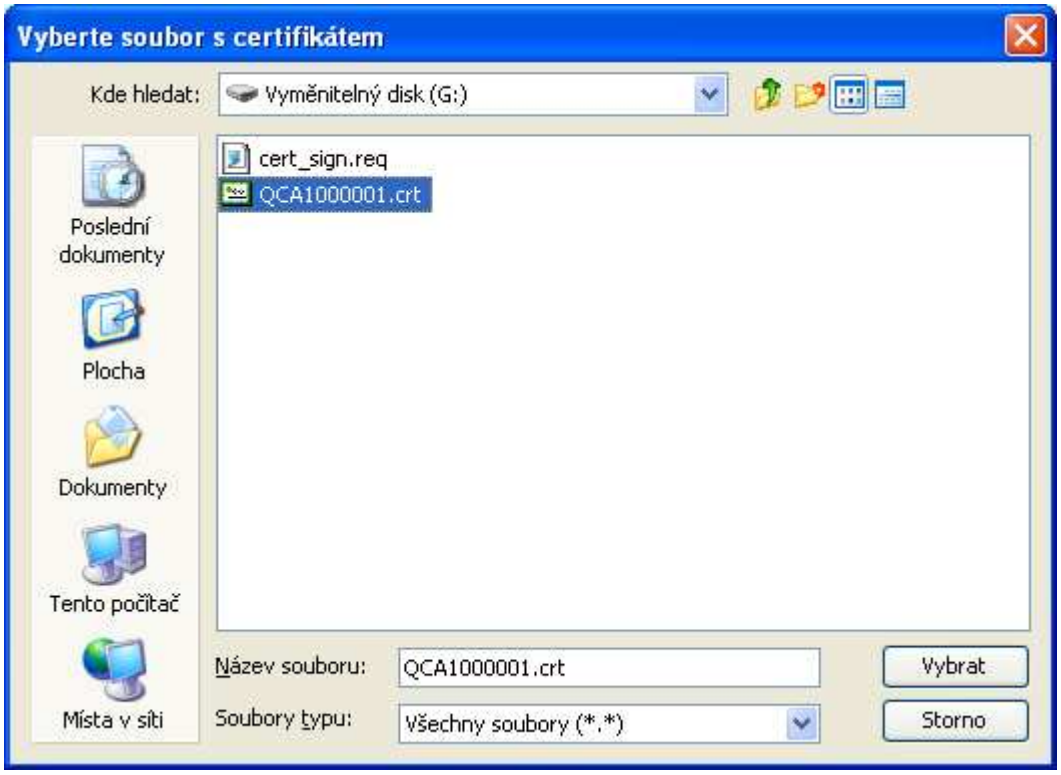
Zobrazí se tato obrazovka:



Stiskněte tlačítko **Import cert.**. Zobrazí se následující okno:

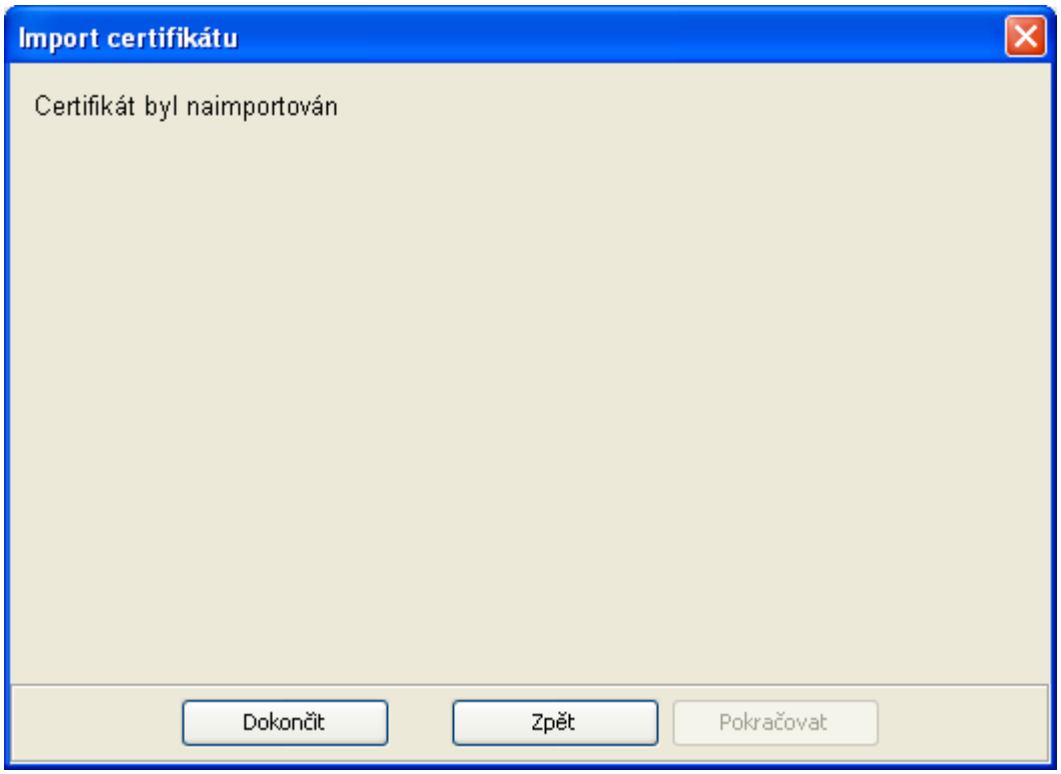


Stisknutím tlačítka **Pokračovat** zobrazíte další okno:

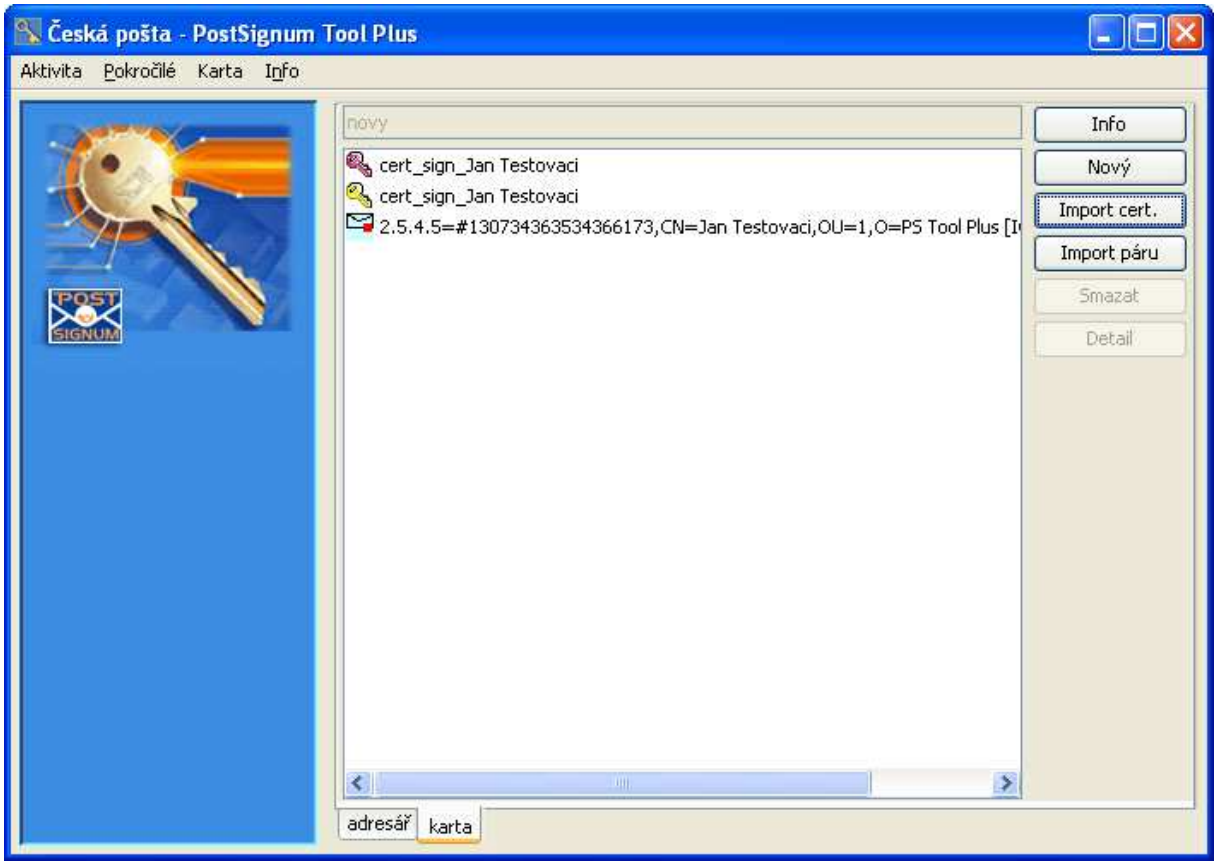


Zde zadáváte soubor s vydaným certifikátem, který máte uložen na přenosném médiu, nebo jste jej stáhli z www stránek.

Po zadání souboru stiskněte tlačítko **Vybrat**. Proběhne instalace certifikátu do čipové karty/USB tokenu a nakonec se zobrazí následující okno:



Po stisknutí tlačítka **Dokončit** se opět zobrazí hlavní okno programu:



6.2 Kontrola úspěšného provedení postupu

V hlavním okně programu se vytvořila nová položka se symbolem obálky.

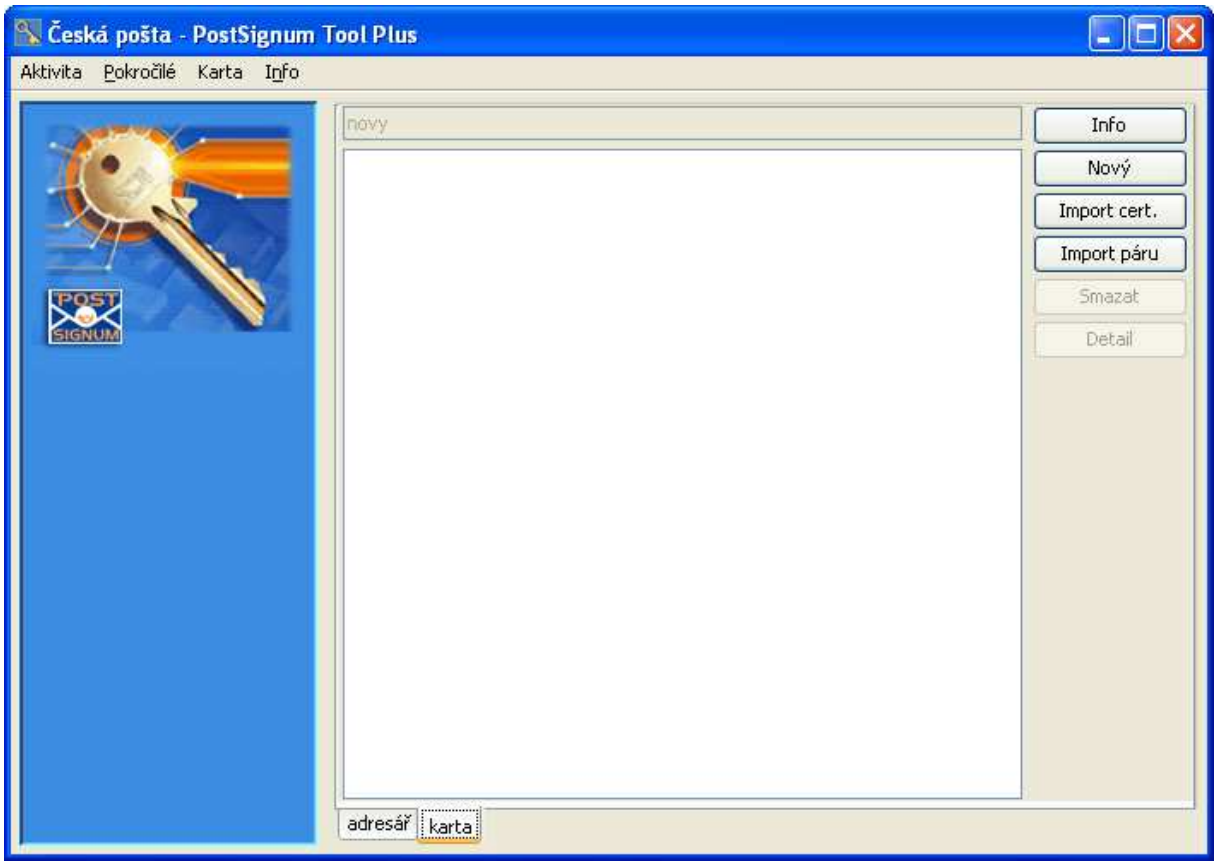
Po úspěšném importu certifikátu je nutné provést postup uvedený v kapitole 9 (platí pro USB token iKey 4000)

7 Import klíčů a certifikátu ze souboru

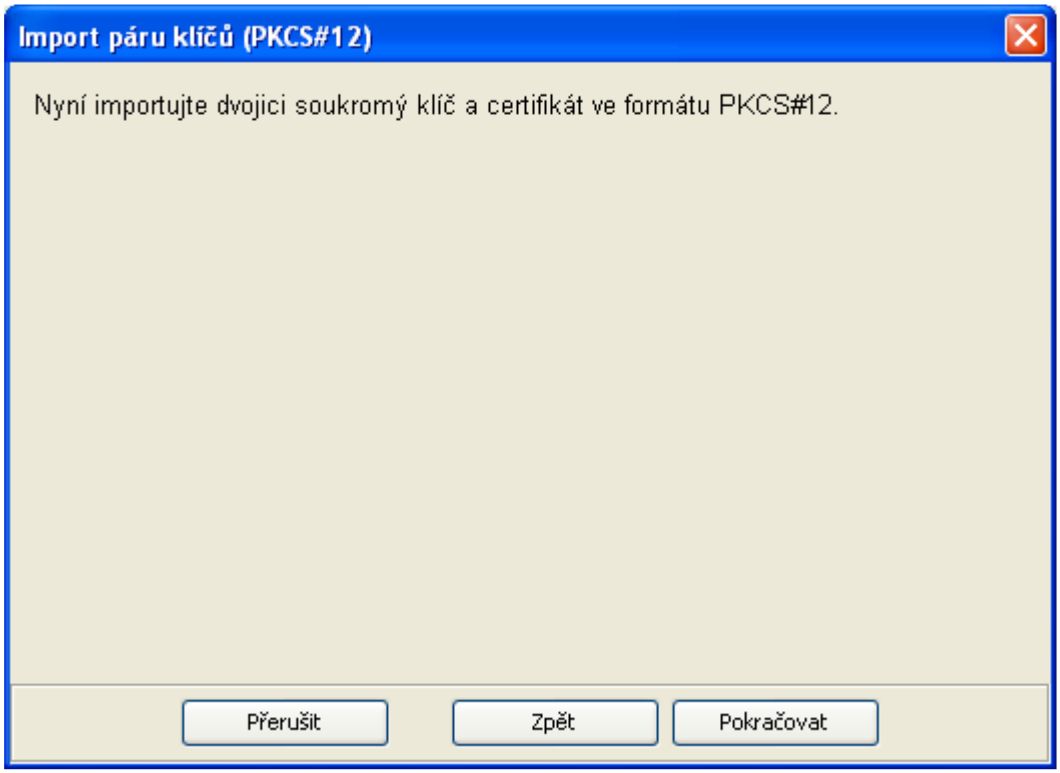
Účel postupu	Import zálohy certifikátu na čipovou kartu nebo USB token
Typ postupu	volitelný
Předpoklady	vytvořený adresář s klíči (kapitola 4)

7.1 Postup

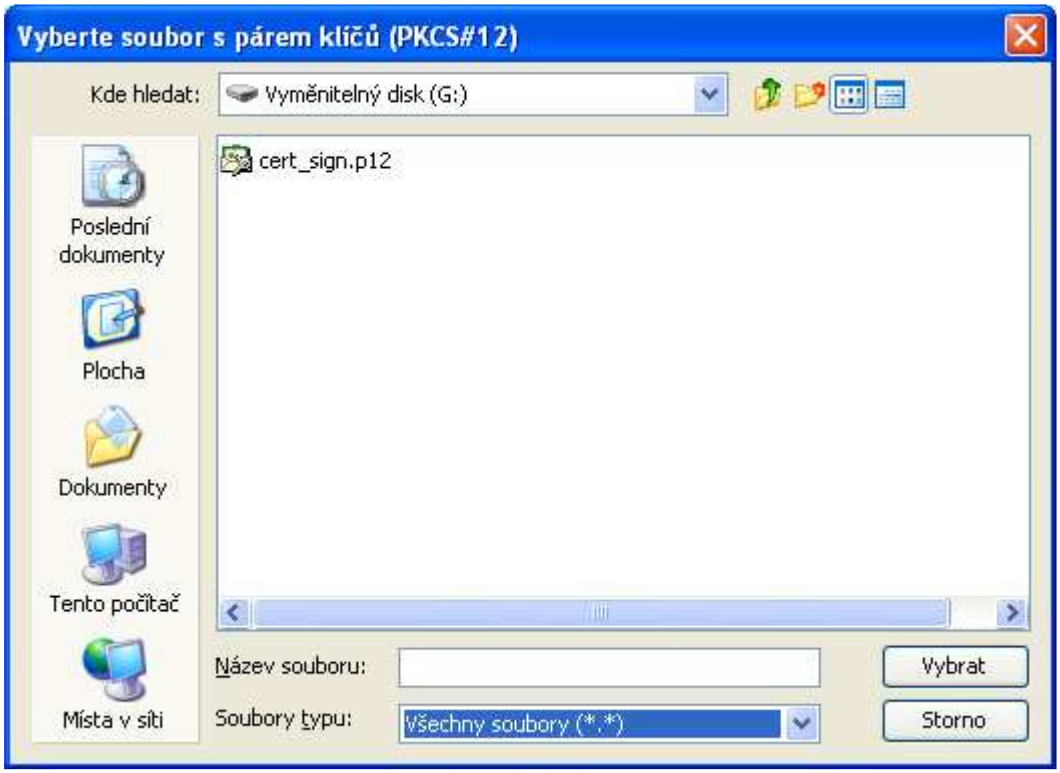
Spusťte program a „otevřete“ pomocí hesla adresář s klíči a pinu k čipové kartě, USB tokenu (viz kapitola 4.3) Zobrazí se tato obrazovka:



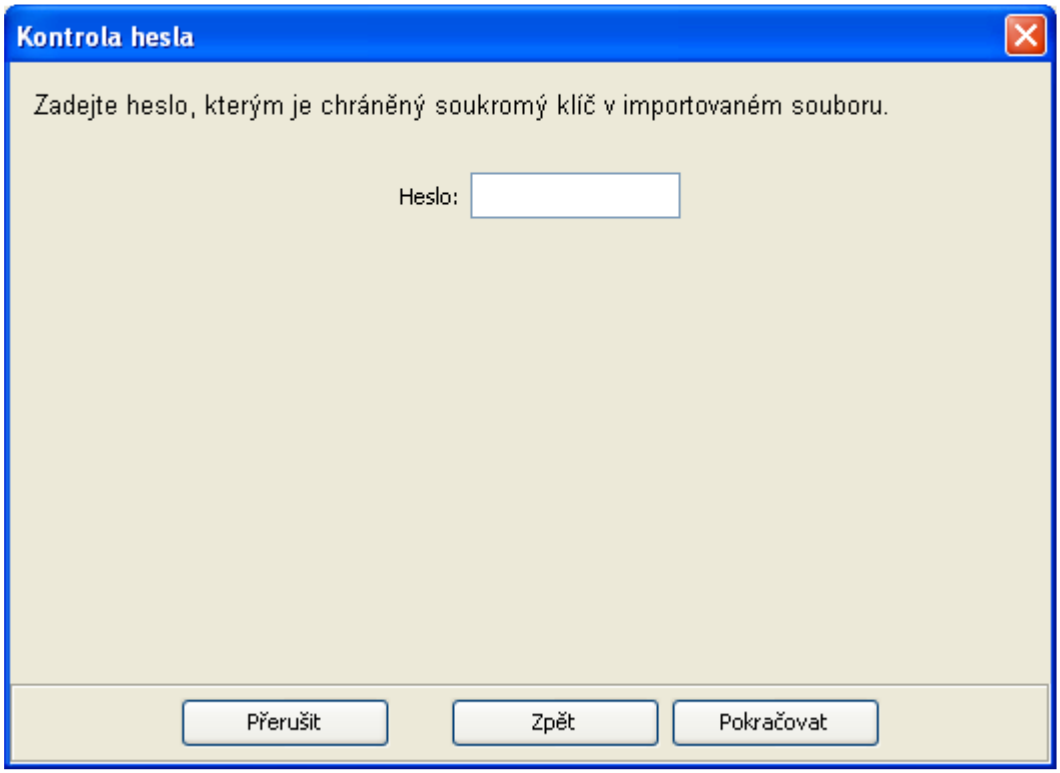
Stiskněte tlačítko **Import páru.** Zobrazí se následující okno:



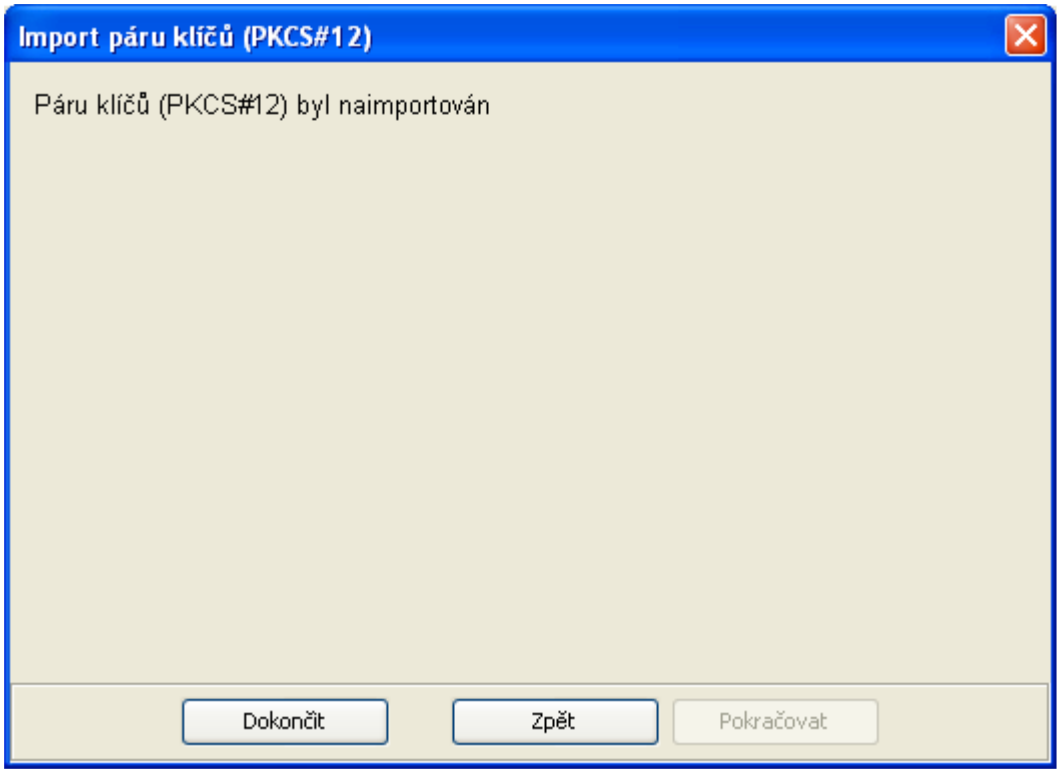
Stisknutím tlačítka **Pokračovat** zobrazíte další okno:



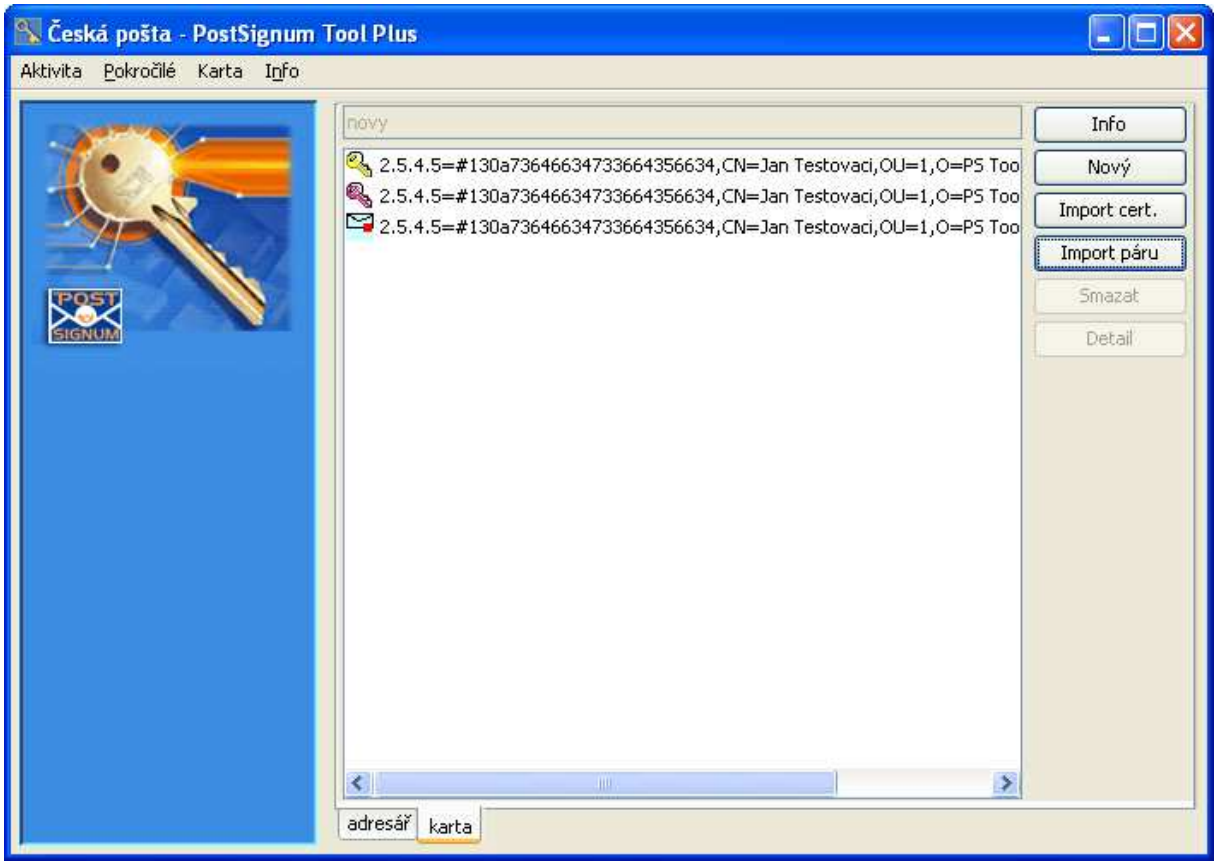
Po zadání souboru stiskněte tlačítko **Vybrat**.



Zadejte heslo, kterým je chráněn soubor se zálohou certifikátu. Po zadání hesla stiskněte tlačítko **Pokračovat**. Proběhne instalace certifikátu do čipové karty/USB tokenu a nakonec se zobrazí následující okno:



Po stisknutí tlačítka **Dokončit** se opět zobrazí hlavní okno programu:



7.2 Kontrola úspěšného provedení postupu

V hlavním okně programu se vytvořily nové položky.

8 Smazání objektu uloženého na čipové kartě/USB tokenu

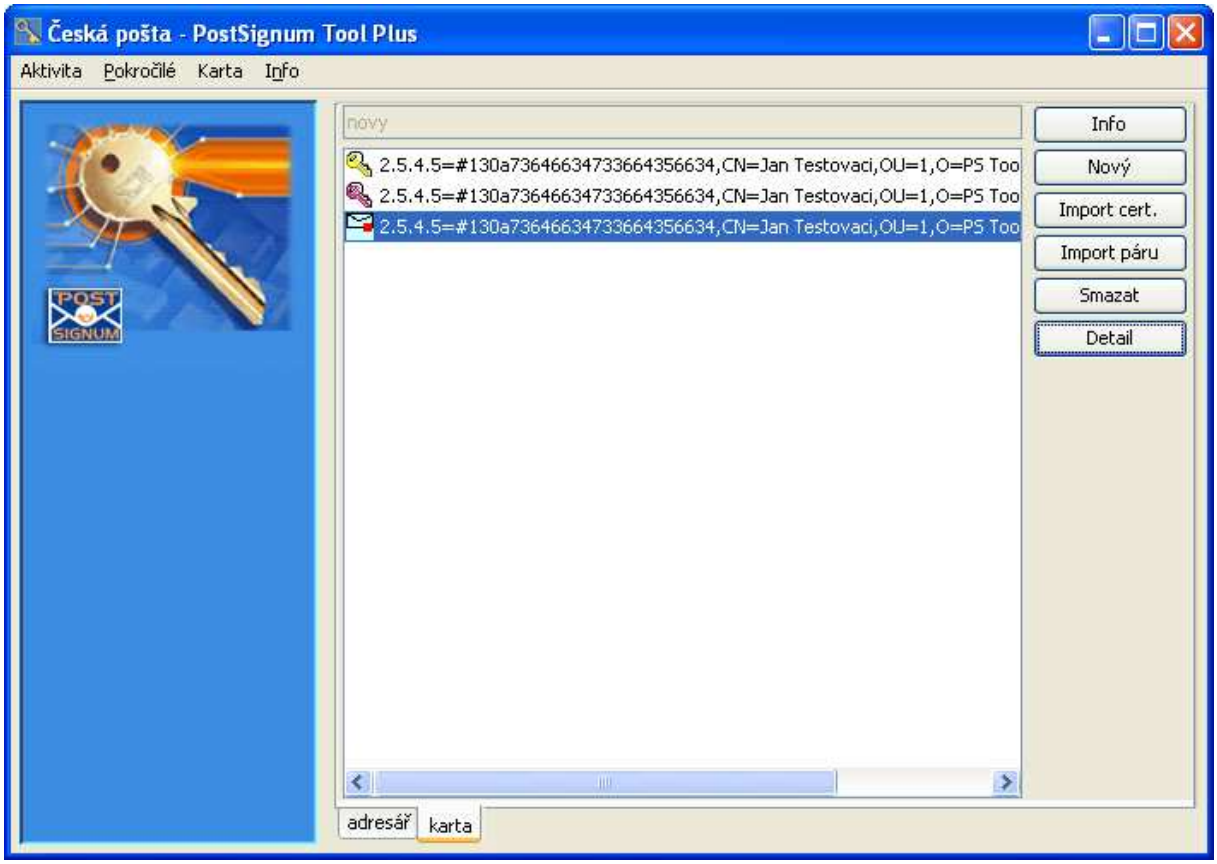
Účel postupu	Smazání nepotřebných certifikátů na čipové kartě/USB tokenu
Typ postupu	volitelný
Předpoklady	Existující objekt na čipové kartě/USB tokenu, Byl nainstalován program PostSignum Tool Plus (kapitola 3) Vytvořený adresář s klíči (kapitola 4)

8.1 Poznámky k postupu

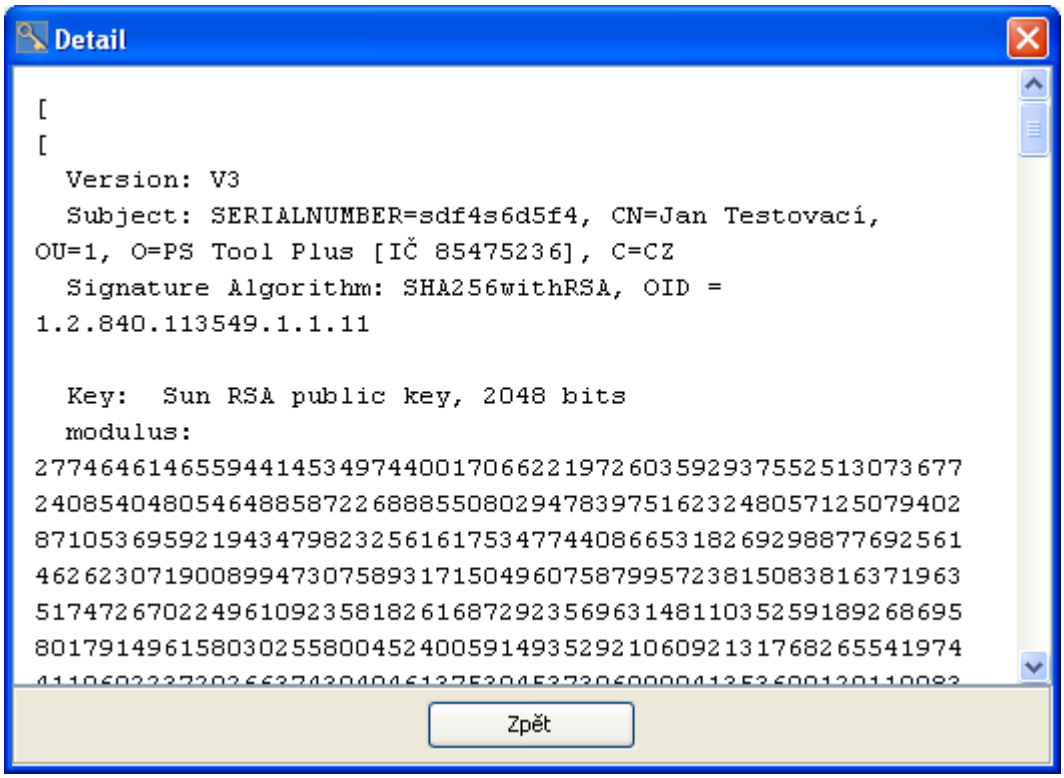
- Čipová karta/USB token se může po delším používání zaplnit již neplatnými certifikáty. V tomto postupu je uvedeno jak nepotřebné objekty smazat a uvolnit tak místo pro uložení dalších certifikátů.
- **Upozorňujeme, že smazaná data nelze nijak obnovit.**

8.2 Postup

Spusťte program a „otevřete“ pomocí hesla adresář s klíči a pinu k čipové kartě, USB tokenu (viz kapitola 4.3) Zobrazí se tato obrazovka:



Označte objekt, který chcete vymazat a stiskněte tlačítko **Smazat** .
Před vlastním vymazáním lze zkontrolovat o jaký certifikát v objektu se jedná. Označte objekt a stiskněte tlačítko **Detail** . Funkční certifikát na kartě či USB tokenu je složen vždy ze tří objektů stejně jako je vidět na předcházejícím obrázku.



9 Synchronizace certifikátů na USB tokenu

Účel postupu	Po instalaci certifikátů pomocí programu PSTool-Plus je potřeba provést ještě další krok, aby byly certifikáty na tokenu použitelné. Pokud se tento krok neprovede, certifikáty **nebudou funkční**.
Typ postupu	Povinný po instalaci certifikátu
Předpoklady	Instalovaný certifikát

9.1 Poznámky k postupu

- Při importu certifikátu přes aplikaci PSTool Plus může dojít k uložení certifikátu do USB tokenu na jiné místo, než je uložen privátní klíč k certifikátu. Níže uvedeným postupem tuto závadu odstraníte bez jakéhokoliv poškození dat na USB tokenu. **Prosíme o pečlivé dodržení uvedeného postupu.**

9.2 Postup

9.2.1 Stažení opravné utility

Z adresy **http://www.postsignum.cz/files/fixtoken.exe** si stáhněte samorozbalovací archiv.

9.2.2 Instalace opravné utility

Stažený soubor **fixtoken.exe** dvojklikem spusťte a stiskněte tlačítko **Unzip**

Hlášku potvrďte stiskem tlačítka **OK** a předchozí okno zavřete křížkem nebo stiskem tlačítka **Close**.

9.2.3 Spuštění opravné utility a vložení USB tokenu

Vložte USB Token do počítače. Přejděte do adresáře **C:\Program Files\SafeNet\BSecClient** a spusťte soubor „**Tknutils.exe**“

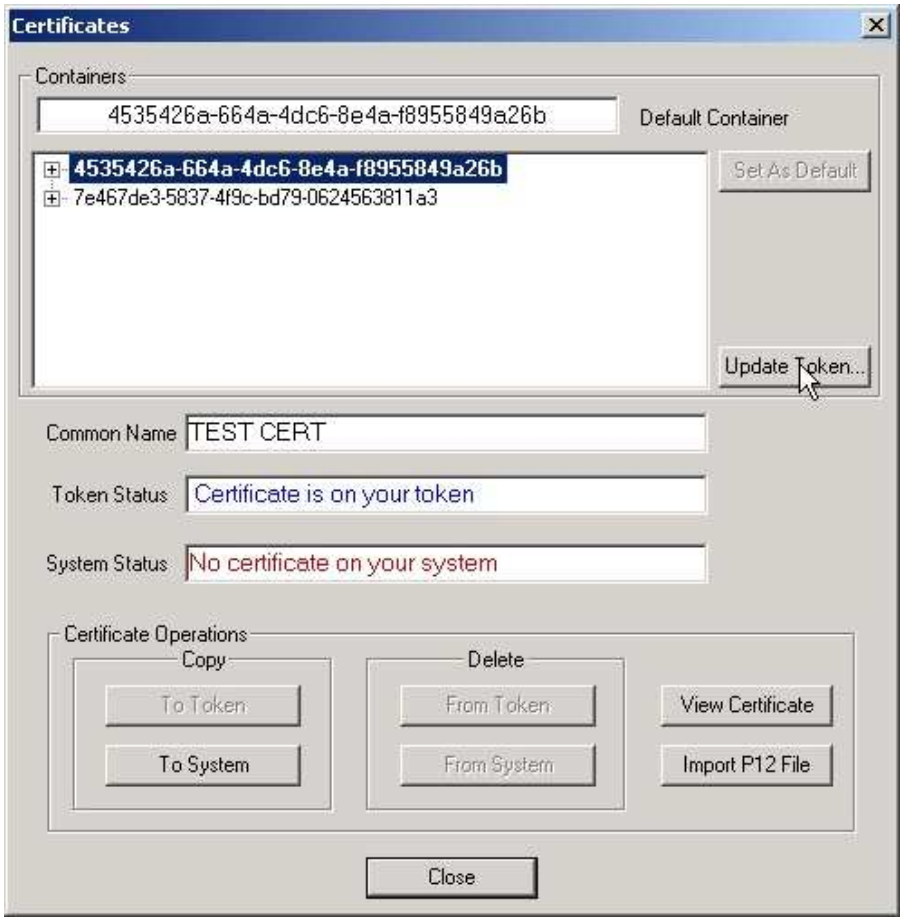
Pokud se objeví tato chybová hláška, je pravděpodobné, že v systému je ještě jiná čtečka čipových karet nebo jiný token.

Hlášku potvrďte stiskem **OK** a ze seznamu vpravo vyberte zařízení s názvem **Rainbow Technologies iKeyVirtualReader 0**.

9.2.4 Provedení opravy USB Tokenu

Ve spuštěné aplikaci **Token Utilities** stiskněte tlačítko **Certificates**.

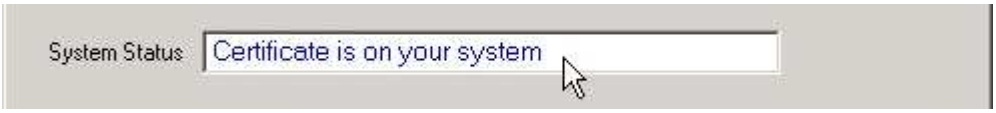
Budete požádání o zadání PINu. Zadaný PIN potvrďte stiskem tlačítka **OK**



Zobrazí se okno s názvy úložišť certifikátů. V tomto okně stiskněte tlačítko **Update Token**.

Zobrazí se upozornění, že proběhne synchronizace certifikátů na USB tokenu.
Hlášku potvrďte stiskem OK.

Po dobu synchronizace tokenu je zobrazen symbol přesýpacích hodin u kurzoru myši. Jakmile přesýpací hodiny u kurzoru myši zmizí je synchronizace ukončena.



Po úspěšné synchronizaci by se měl **Systém Status** změnit z původní hlášky „No certificate on your system“ na „Certificate is on your system“

Aplikaci **Token Utilities** je nyní možné ukončit. Buď stiskem tlačítka **Close** nebo křížkem v pravém horním rohu.
USB token z počítače vyjměte a znovu vložte. Tím se projeví všechny změny provedené v USB tokenu. Pokud tento krok neprovedete, nedojde k provedení změn.