

Certifikační autorita PostSignum

Generování klíčů pomocí programu PostSignum Tool Plus verze 2.0.1

Uživatelská dokumentace

Červenec 2011

1 Obsah

1 Obsah	2
2 Úvod	3
2.1 Informace o dokumentu.....	3
2.2 Kde využiji popsané postupy?.....	3
2.3 Chronologické pořadí uváděných postupů	3
3 Instalace programu	4
3.1 Spuštění instalátoru PostSignum Tool Plus.....	4
4 První spuštění programu	7
4.1 Poznámky k postupu	7
4.2 Bezpečnostní doporučení	7
4.3 Postup	7
5 Vygenerování klíčů a žádosti o certifikát	10
5.1 Poznámky k postupu	10
5.2 Postup	10
6 Instalace vydaného certifikátu	14
6.1 Poznámky k postupu	14
6.2 Instalace vydaného certifikátu do adresáře s klíči	14
6.3 Kontrola úspěšného provedení postupu.....	17
7 Export klíčů a certifikátu do souboru	18
7.1 Poznámky k postupu	18
7.2 Bezpečnostní doporučení	18
7.3 Postup	18
7.4 Kontrola úspěšného provedení postupu.....	21
7.5 Import klíčů a certifikátu ze souboru.....	21

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 do programu,
- export klíčů a certifikátu do souboru.
- popis práce s čipovou kartou a USB tokenem je v samostatném dokumentu CA_PSTool_Plus_device.pdf

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
- Po exportu klíčů a certifikátů do souboru lze tento soubor nainstalovat do operačního systému Windows. Poté lze používat elektronické podepisování dat v e-mailových klientech Outlook / Outlook Express, Internet Exploreru a dalších aplikacích používajících úložiště klíčů ve Windows (všechny relevantní aplikace od Microsoftu).
- Soubor s exportovanými klíči lze dále načíst do všech aplikací, které zvládnou zpracovat soubory ve formátu PKCS#12. Poté lze v těchto aplikacích používat elektronické podepisování dat. Příkladem těchto aplikací je Mozilla Firefox či Mozilla Thunderbird.

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.
- Spustíte opět program PostSignum Tool Plus a nainstalujete certifikát podle postupu v kapitole 6.
- Exportujete klíče a certifikát do souboru podle postupu v kapitole 7.
- Soubor, který vznikl exportem z PostSignum Tool Plus, importujete do cílové aplikace, ve které chcete klíče a certifikát používat. Způsob provedení importu byste měli najít v dokumentaci k vaší aplikaci.

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

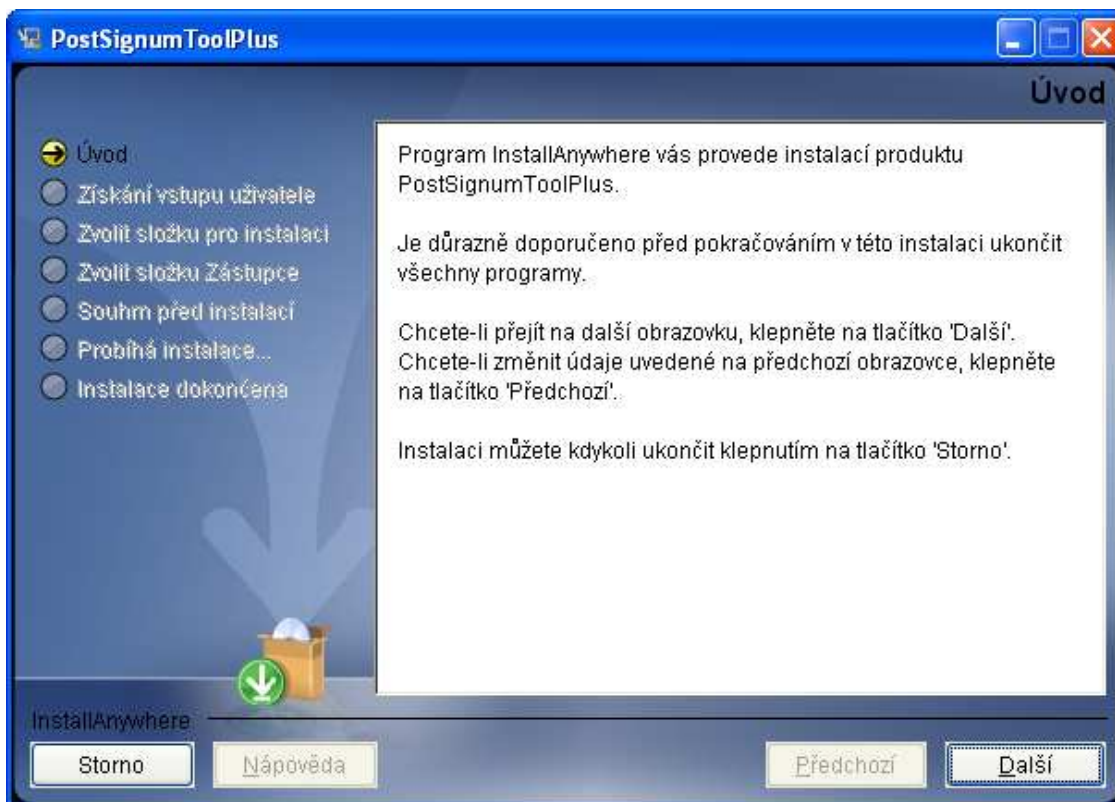
Poznámka pro operační systém Windows Vista a Windows 7:

Před spuštěním instalátoru je potřeba se přihlásit pod uživatelským účtem s administrátorskými právy. Nestačí spuštění pomocí funkce **Spustit jako správce**.

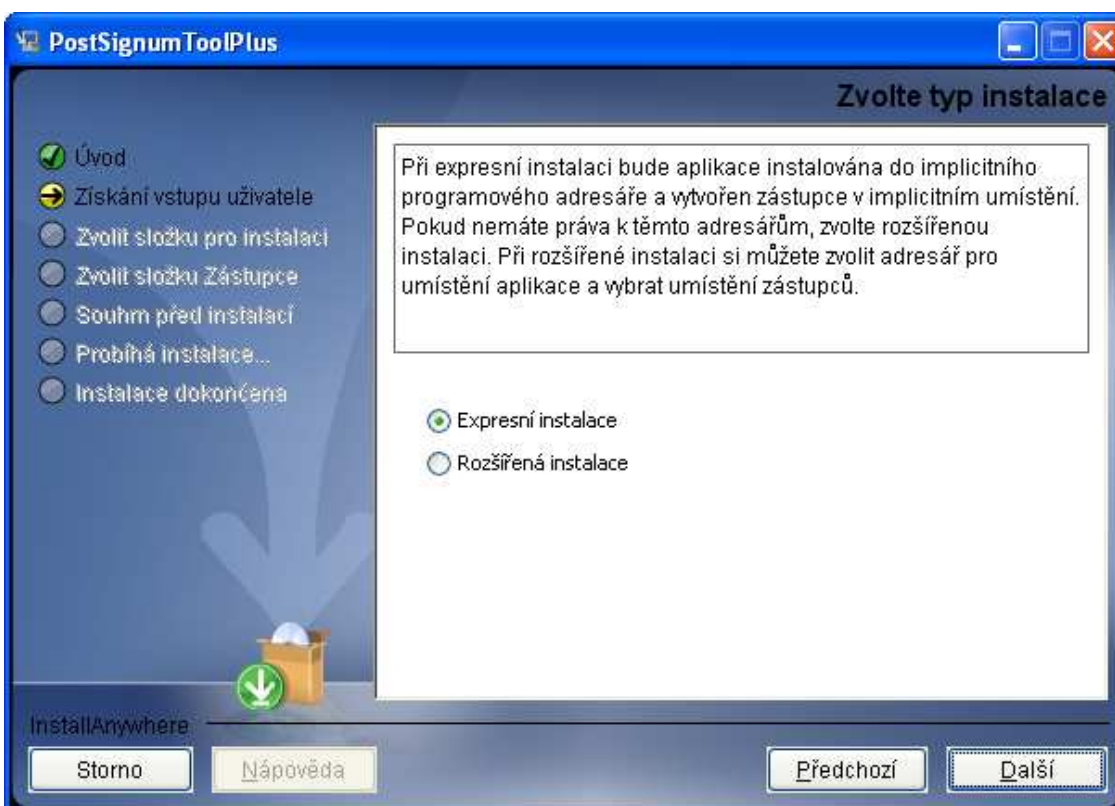
Spusťte stažený instalátor nástroje PostSignum Tool Plus. Po chvíli se zobrazí následující obrazovka:



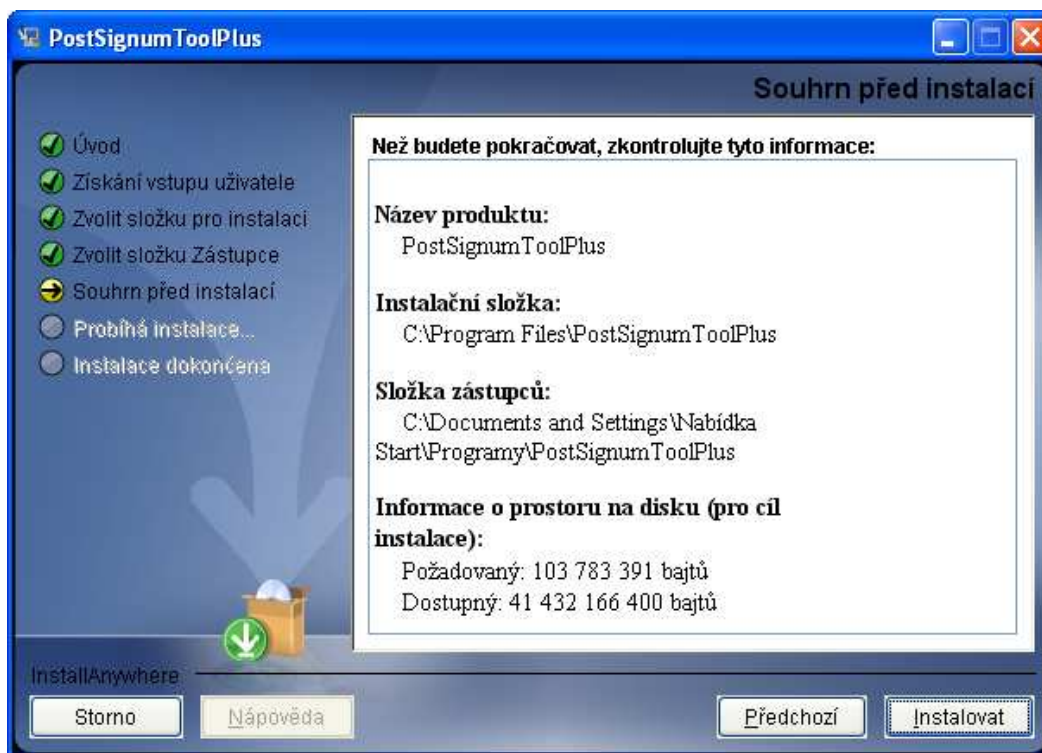
Pro instalaci můžete ponechat předvolený jazyk a stisknout tlačítko **OK**. Po chvíli se zobrazí další okno:



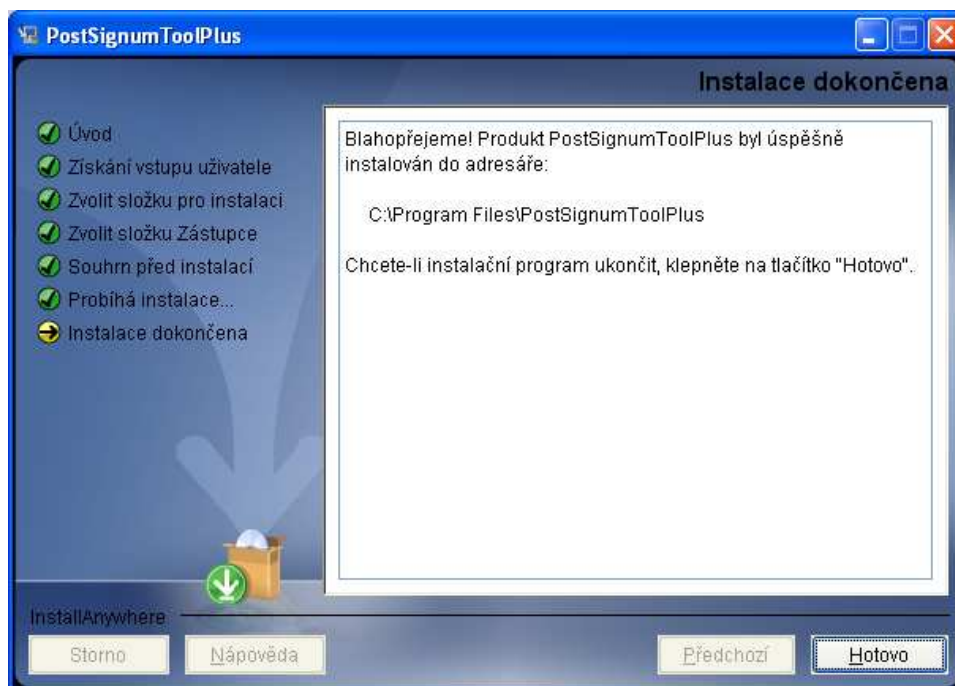
Pokračujte na další obrazovku stisknutím tlačítka **Další**.



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.
- Dejte si velký pozor, abyste si nesmazali obsah adresáře s klíči, minimálně dokud neprovedete export klíčů a certifikátu do souboru.
- 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.

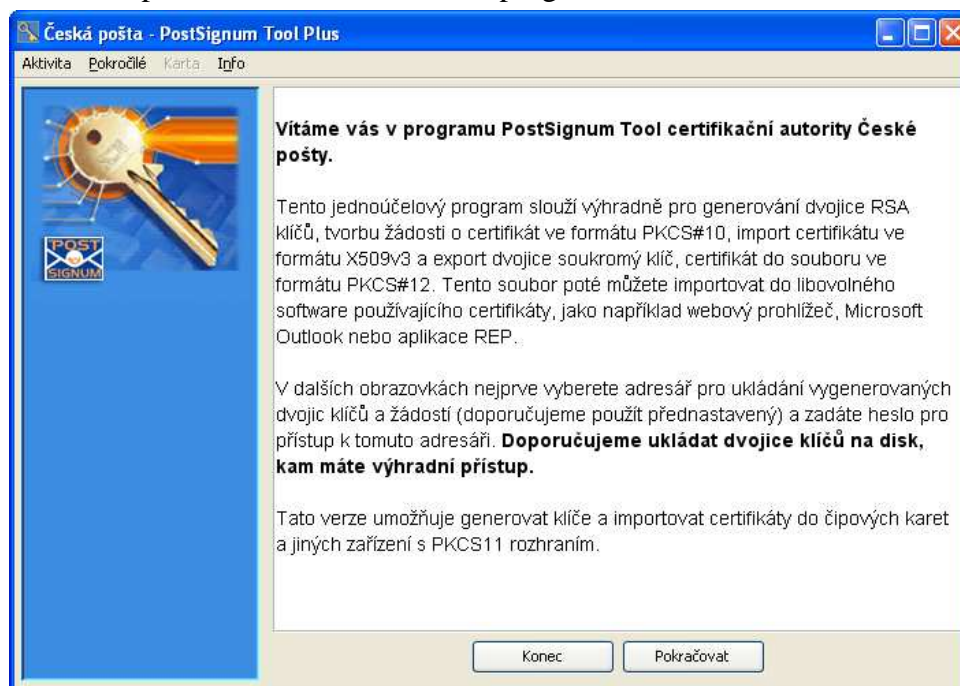
4.2 Bezpečnostní doporučení

- 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.

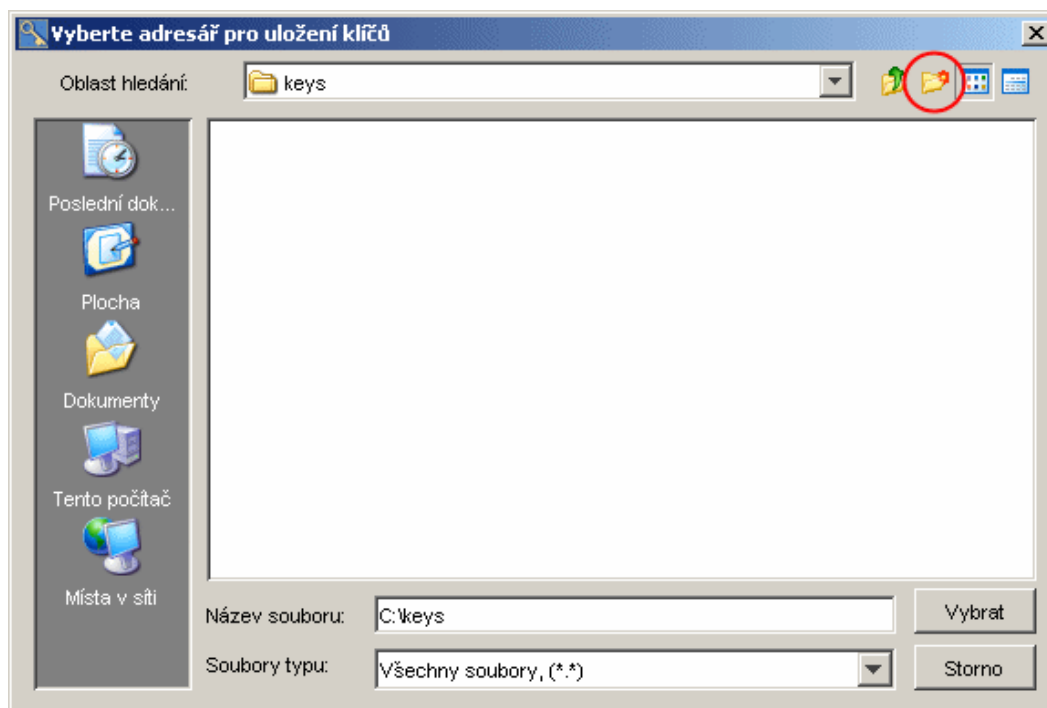
4.3 Postup

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:



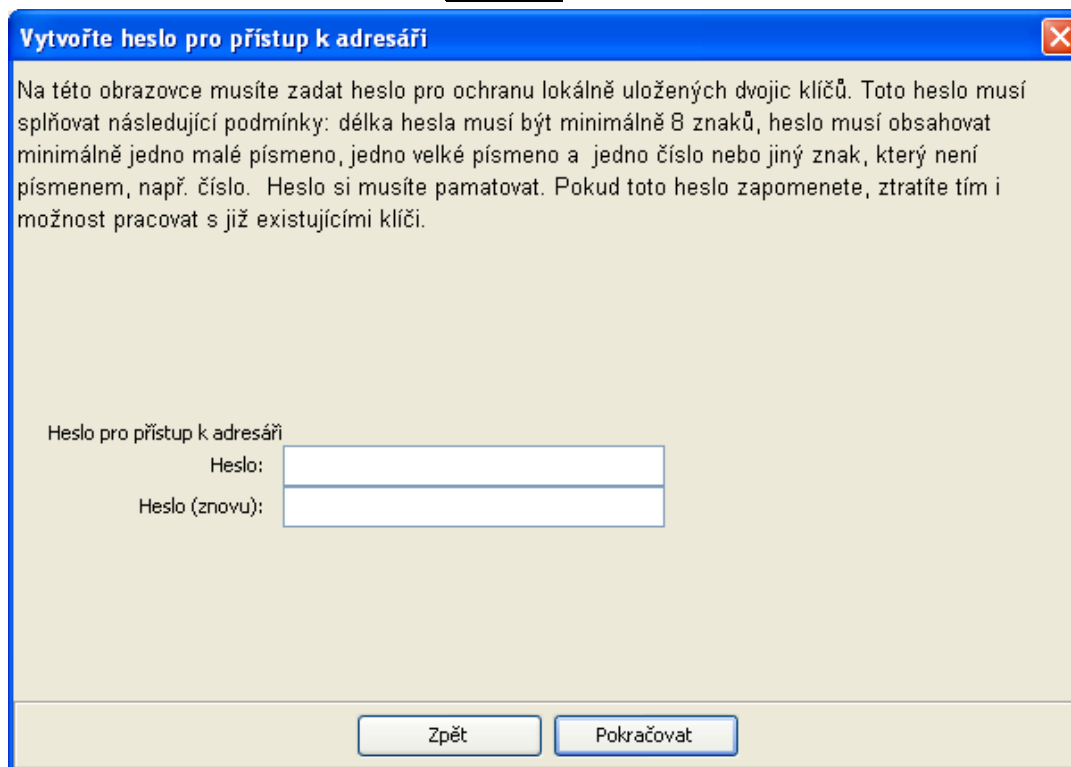
Po stisknutí tlačítka **Pokračovat** se zobrazí následující dialogové okno:



Zadáváte adresář, do něž 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.).

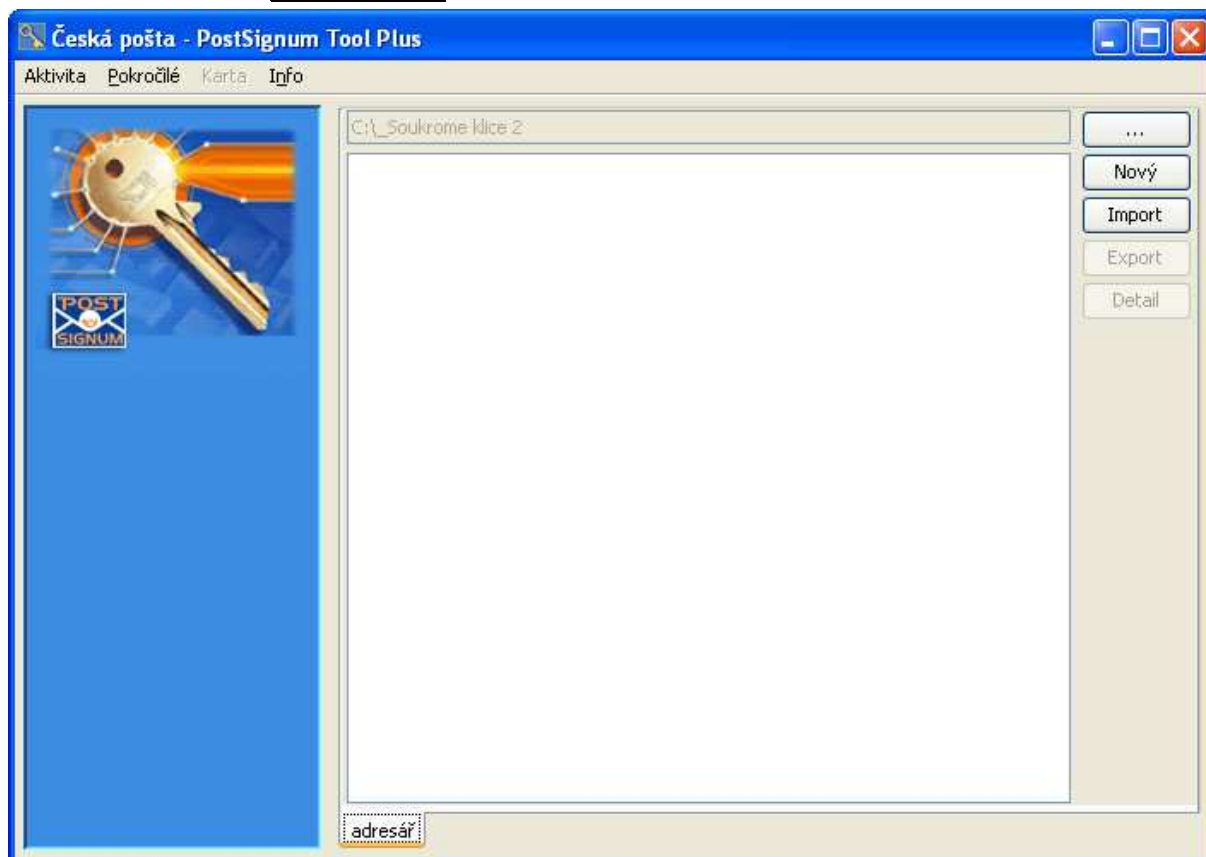
Po zadání adresáře klikněte na tlačítko **Vybrat**. Zobrazí se toto okno:



Generování klíčů pomocí programu PostSignum Tool Plus verze 2.0.1

Zadávaté 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:



Pochopitelně v tuto chvíli se zde ještě nenacházejí žádné klíče ani certifikáty.

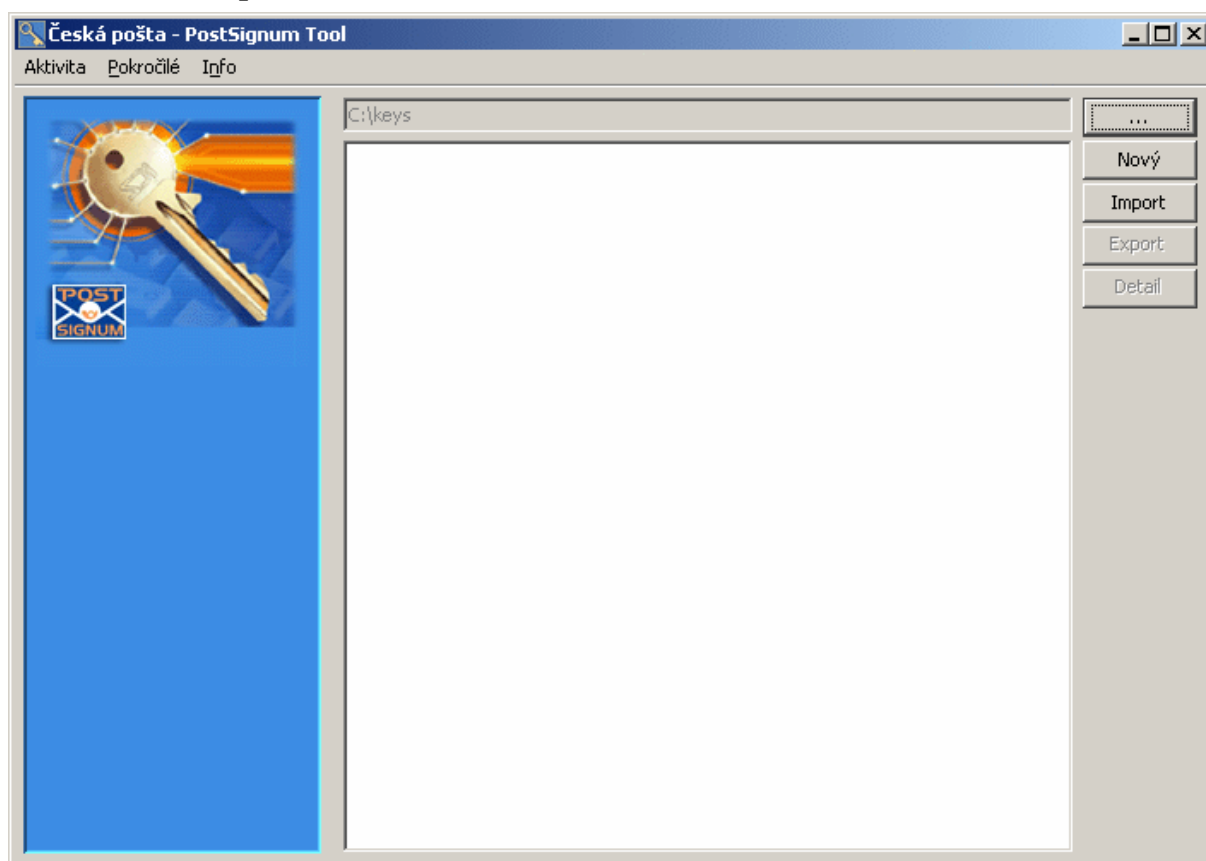
5 Vygenerování klíčů a žádosti o certifikát

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

- Žádost o certifikát lze kdykoliv znovu uložit do adresáře po stisknutí tlačítka **Export** v hlavní obrazovce programu; musíte mít pouze označenu položku se symbolem červeného klíče.
- 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:

Vyberte politiku pro novou žádost o certifikát

Kvalifikované certifikáty

- Certifikát zaměstnance
- Systémový certifikát organizace
- Certifikát fyzické osoby
- Systémový certifikát fyzické osoby

Komerční certifikáty

- Certifikát zaměstnance
- Certifikát technologické komponenty
- Certifikát skupiny osob
- Certifikát fyzické osoby
- Certifikát komponenty fyzické osoby
- Šifrovací certifikát fyzické osoby

Přerušit Zpět Pokračovat

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:

Nová žádost o certifikát zaměstnance

Stát* CZ IČ organizace* 85475236

Název organizace* PS Tool Plus Rozlišující org. jednotka

Jméno a příjmení* Jan Testovací Organizační jednotka

E-mail zaměstnance* testovaci@tool.cz Číslo zaměstnance* 1

E-mail zaměstnance Funkce zaměstnance

E-mail zaměstnance Jiné jméno

Žádost o certifikát: podpis SHA256 délka klíče 2048 bitů typ PEM

Místo uložení* C:_Soukrome klíče 2

* Hvězdička označuje povinný údaj.

Přerušit Zpět Pokračovat

Generování klíčů pomocí programu PostSignum Tool Plus verze 2.0.1

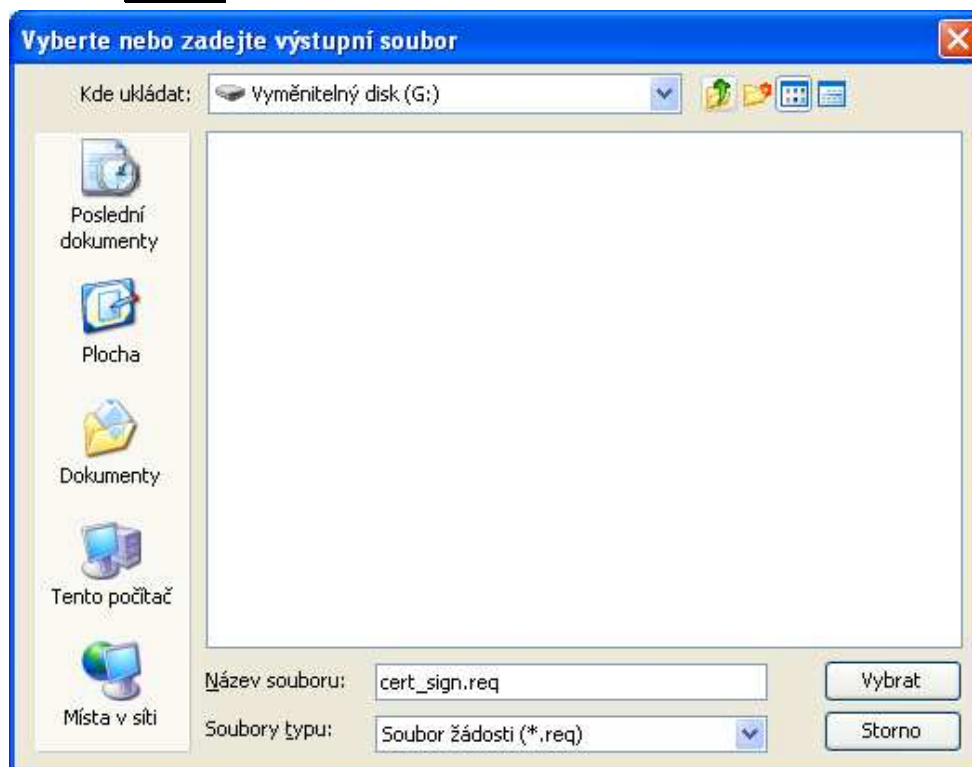
Obrazovka je odlišná na základě výběru z předchozí obrazovky. Povinně musíte vyplnit pouze pole označená hvězdičkou.

Po stisknutí tlačítka **Pokračovat** již bude zahájeno generování klíčů.

Po vygenerování klíčů se zobrazí obrazovka informující o úspěšném vygenerování klíčů:



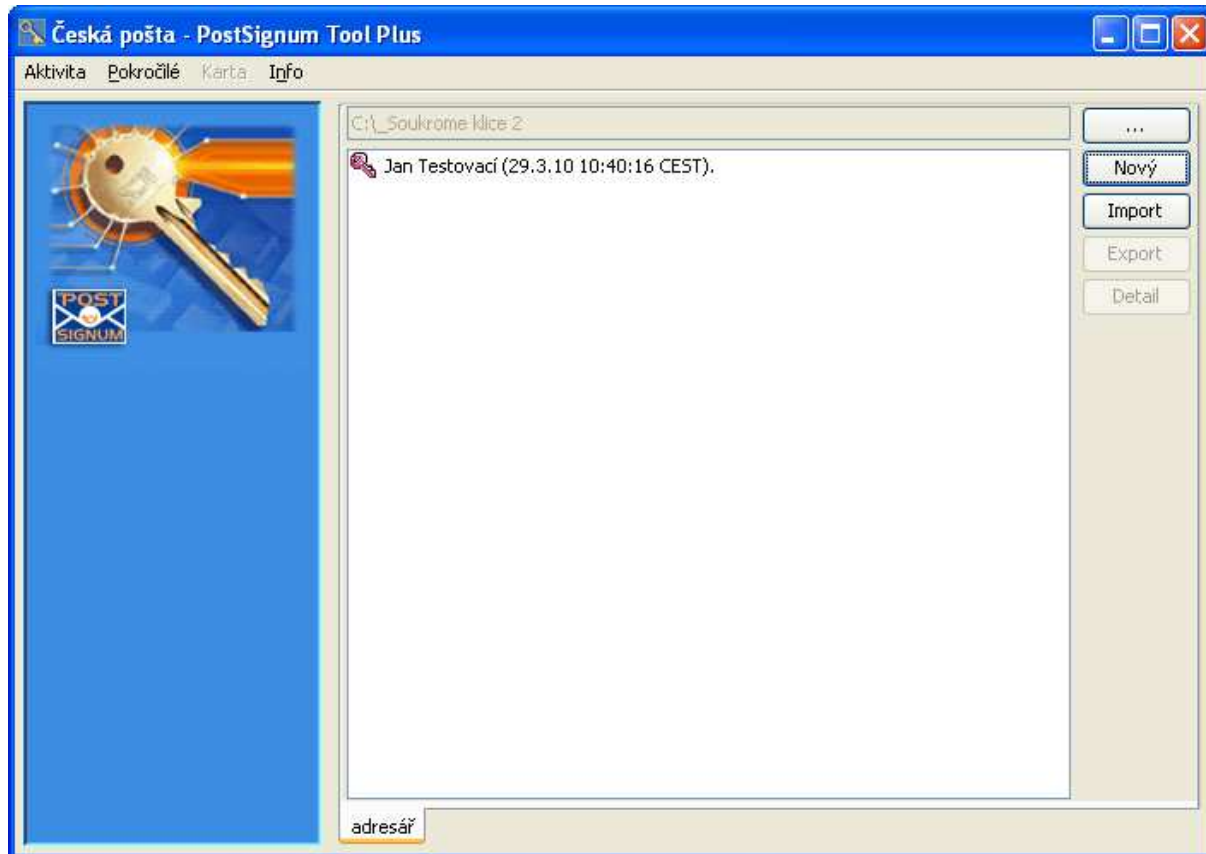
Stiskněte tlačítko **Uložit** a vyberte adresář, do kterého se uloží žádost o certifikát:



Generování klíčů pomocí programu PostSignum Tool Plus verze 2.0.1

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 stisknete tlačítko **Dokončit**. Vráťte 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 Poznámky k postupu

- Certifikát je nutné instalovat na počítači, kde došlo k vygenerování klíčů a žádosti o certifikát programem PostSignum Tool.Plus
- Pokud máte na počítači vytvořeno více adresářů s klíči, je potřeba načíst ten adresář, v němž probíhalo generování klíčů a žádosti o certifikát, podle níž byl certifikát vystaven.

6.2 Instalace vydaného certifikátu do adresáře s klíči

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

V přihlašovacím dialogu je možnost využít čipové karty nebo USB tokenu. Práce s čipovou kartou a USB tokenem je popsána v samostatném dokumentu CA_PSTool_Plus_device.pdf.

Zadejte heslo pro přístup k adresáři

Heslo pro přístup k adresáři
Heslo:

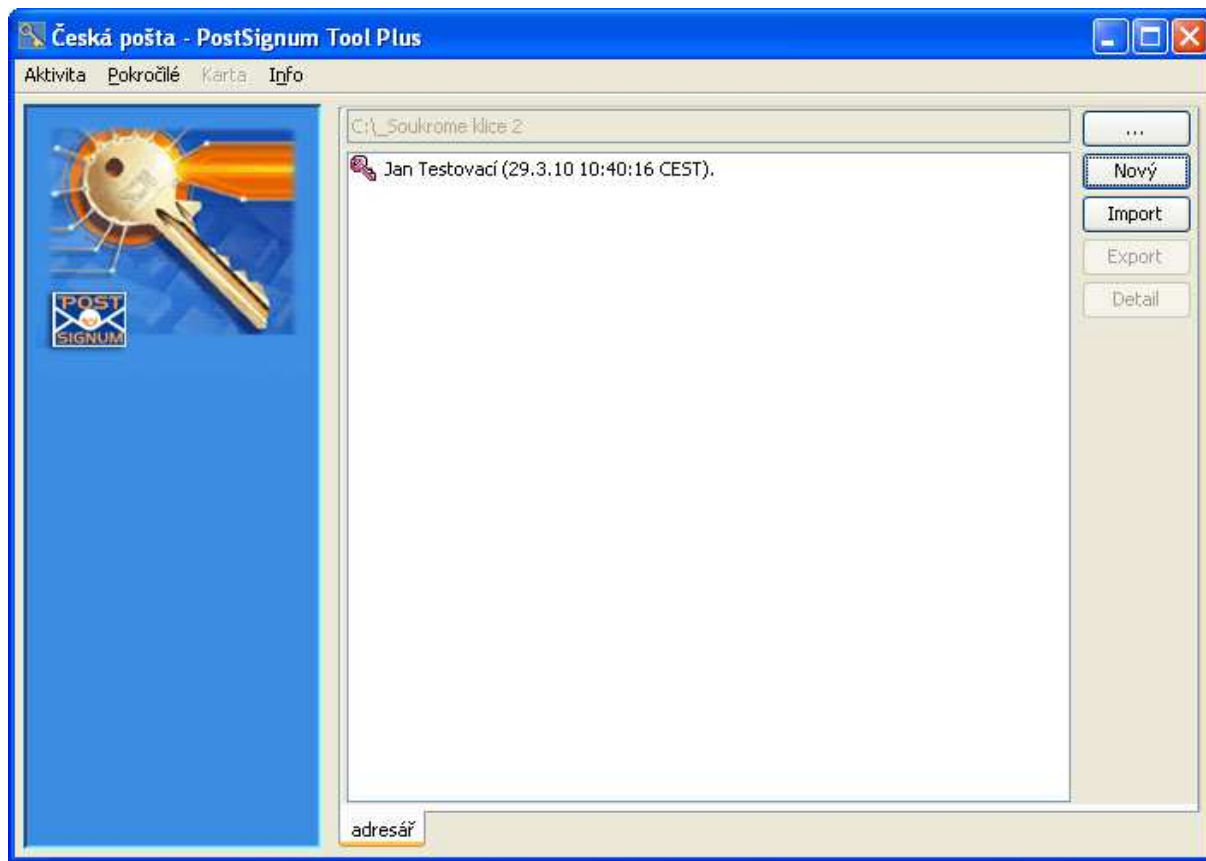
Použít čipovou kartu
(generování klíčů a import certifikátů se provádí automaticky ve zvoleném PKCS11 zařízení).

PIN:

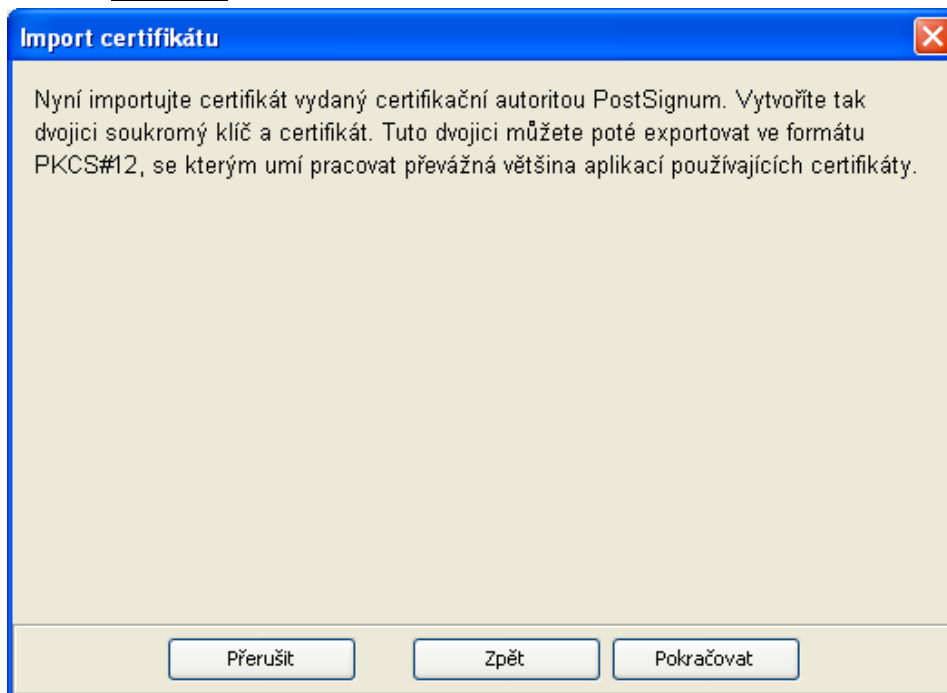
Pořadové číslo tokenu v zařízení:

Nastavení cesty k PKCS11 knihovně:
C:\WINDOWS\system32\proid11.dll

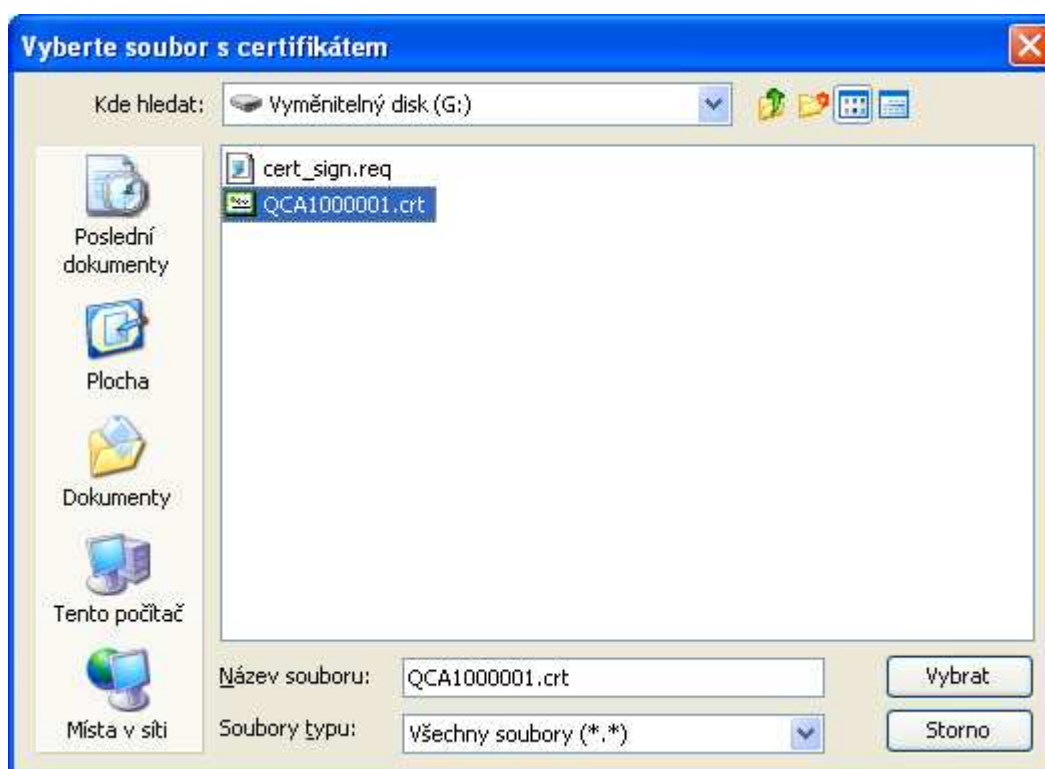
Zobrazí se tato obrazovka:



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



Stisknutím tlačítka **Pokračovat** zobrazíte další okno:

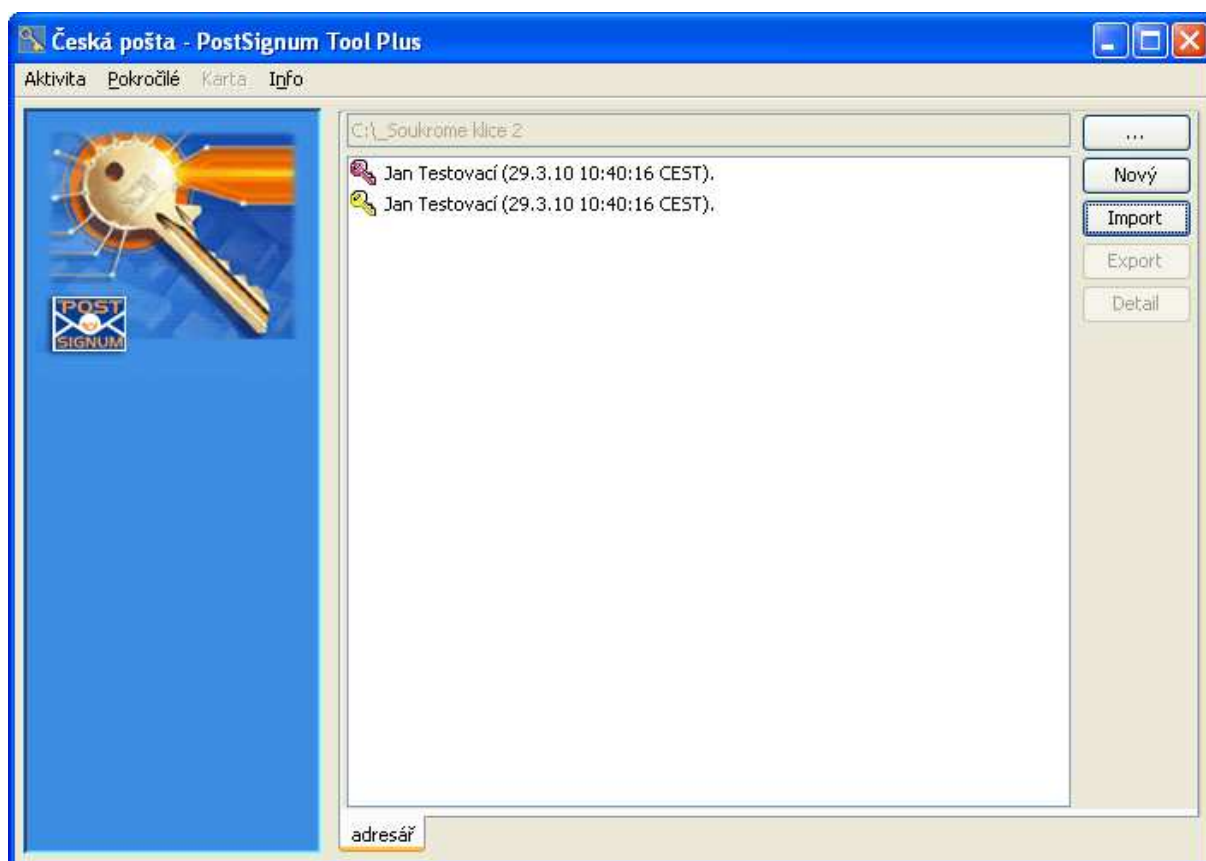


Zde zadáváte soubor s vydaným certifikátem, který máte uložen na přenosném médiu, nebo jste jej stáhli z www stránek.

Po zadání souboru stiskněte tlačítko **Vybrat**. Proběhne instalace certifikátu do adresáře s klíči a nakonec se zobrazí následující okno:



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



6.3 Kontrola úspěšného provedení postupu

V hlavním okně programu se vytvořila nová položka se symbolem žlutého klíče.

7 Export klíčů a certifikátu do souboru

Účel postupu	Exportem si vytvoříte soubor s klíči a certifikátem, který poté nainstalujete do operačního systému Windows nebo do jiných aplikací, ve kterých hodláte elektronicky podepisovat data.
Typ postupu	povinný
Předpoklady	byl proveden postup instalace vydaného certifikátu (kapitola 6)

7.1 Poznámky k postupu

- Klíče a certifikáty se exportují do souboru, jenž odpovídá standardu (formátu) PKCS#12.
- V exportovaném souboru se nenacházejí certifikáty certifikačních autorit; musíte je do Windows nebo příslušné aplikace nainstalovat ručně.

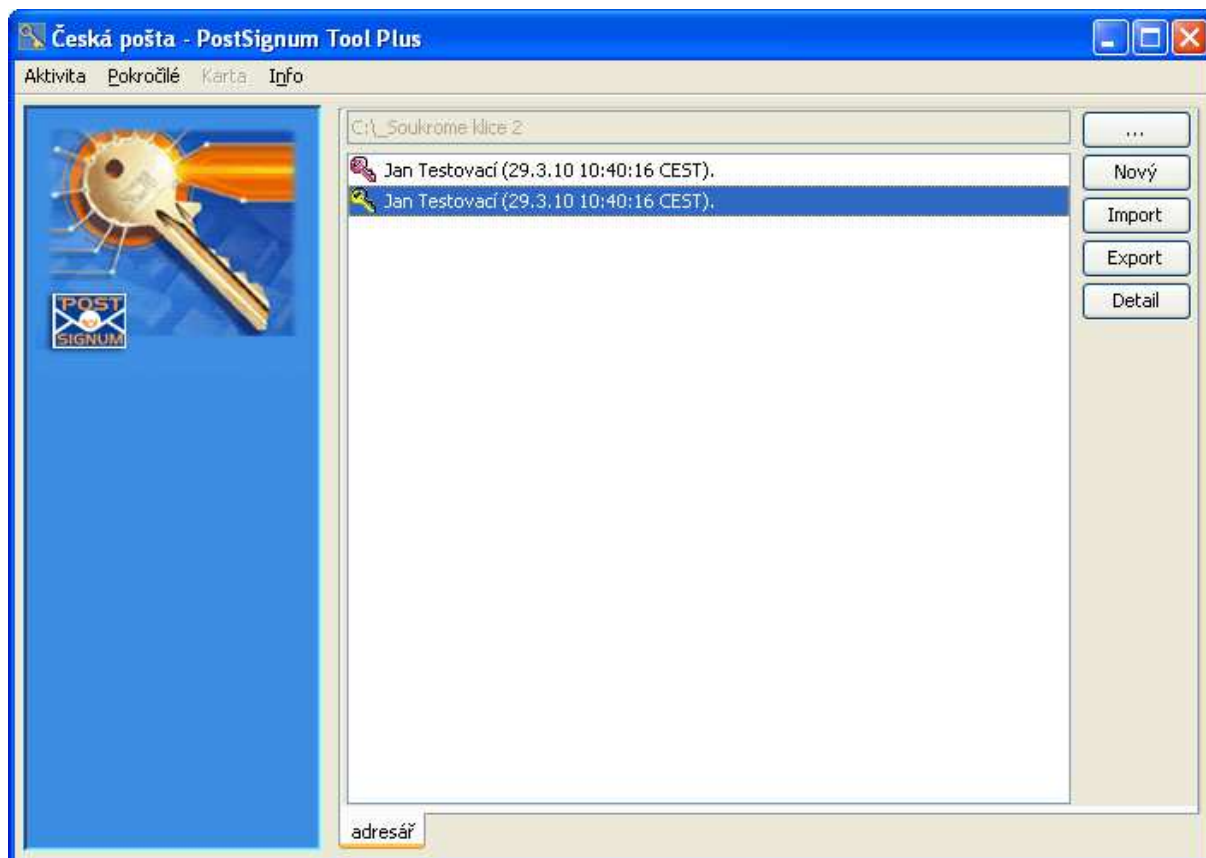
7.2 Bezpečnostní doporučení

- Uvědomte si, že stejným postupem si může stáhnout vaše klíče i cizí osoba, pokud k nim získá přístup.
- PostSignum Tool Plus vyžaduje zadání „silného“ hesla na ochranu klíčů v exportovaném souboru (alespoň 8 znaků, kombinace malých a velkých písmen, číslic a neabecedních znaků; nepoužívejte známá jména a slova). Heslo si nikam nezapíšíte, rozhodně je nenechávejte na jednom místě s vytvořeným souborem.
- Exportovaný soubor uložte na více přenosných médií, abyste nemuseli řešit problém s fyzickým poškozením média. Získáte tak zálohu klíčů, kterou lze použít v případě havárie počítače.

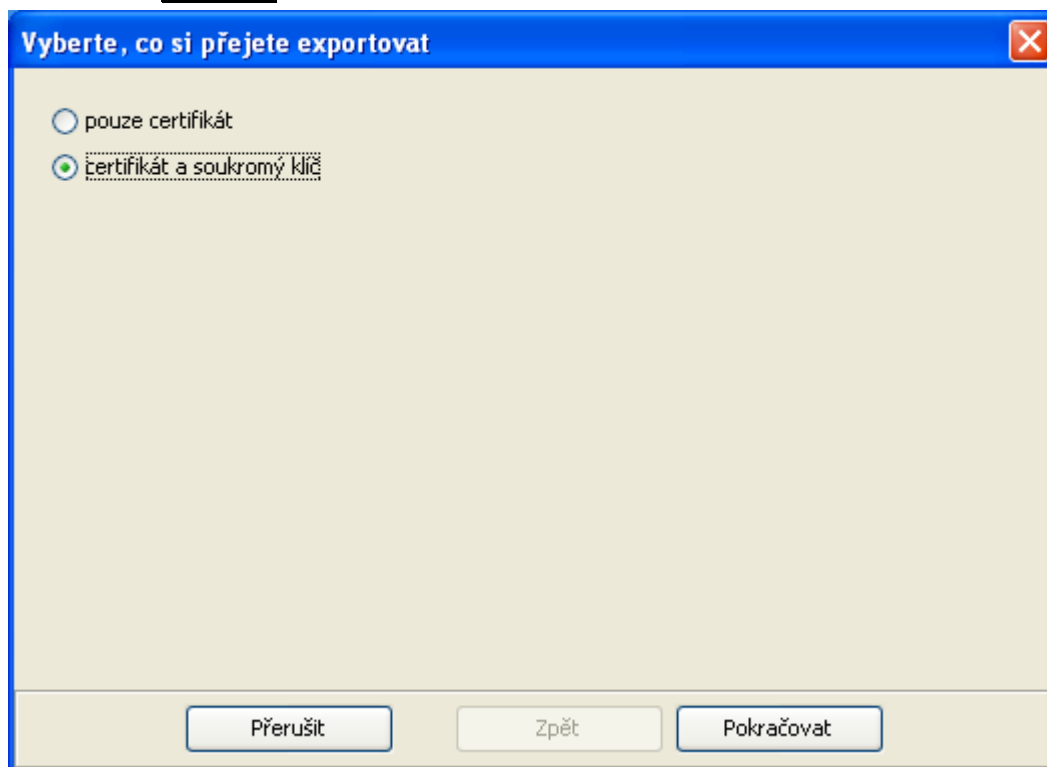
7.3 Postup

Spusťte program a „otevřete“ pomocí hesla adresář s klíči. Zobrazí se tato obrazovka:

Generování klíčů pomocí programu PostSignum Tool Plus verze 2.0.1

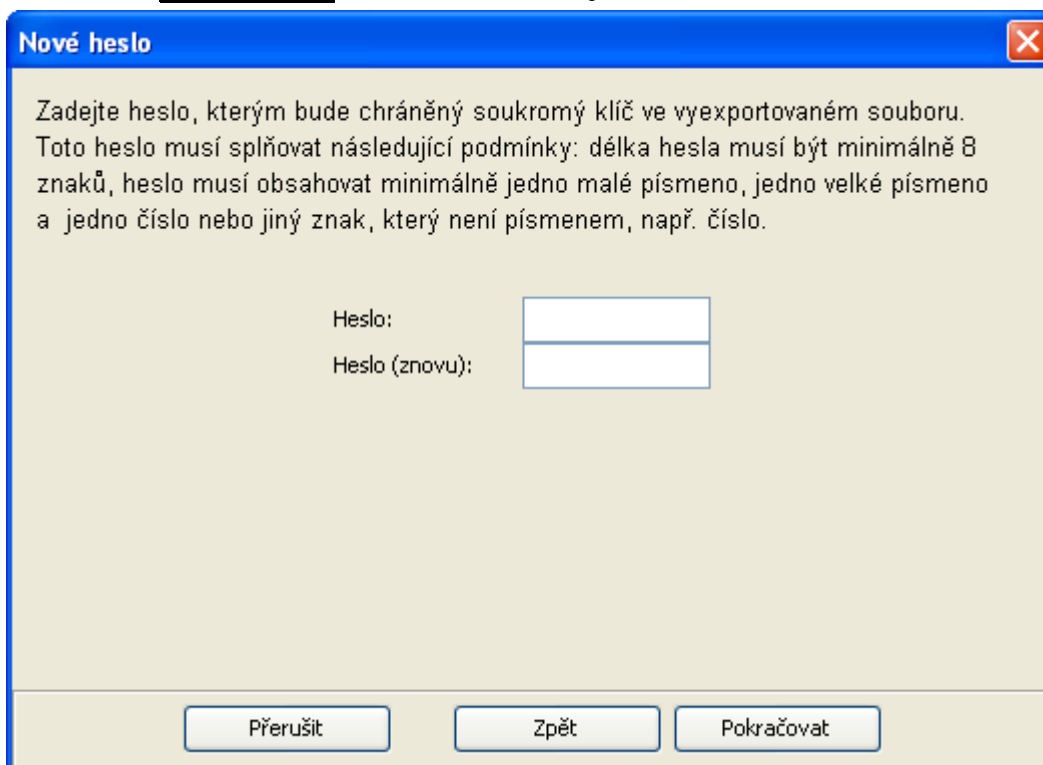


Vyberte položku, kterou chcete exportovat. Vždy zvolte položku se symbolem žlutého klíče. Stiskněte tlačítko **Export**. Zobrazí se následující okno:



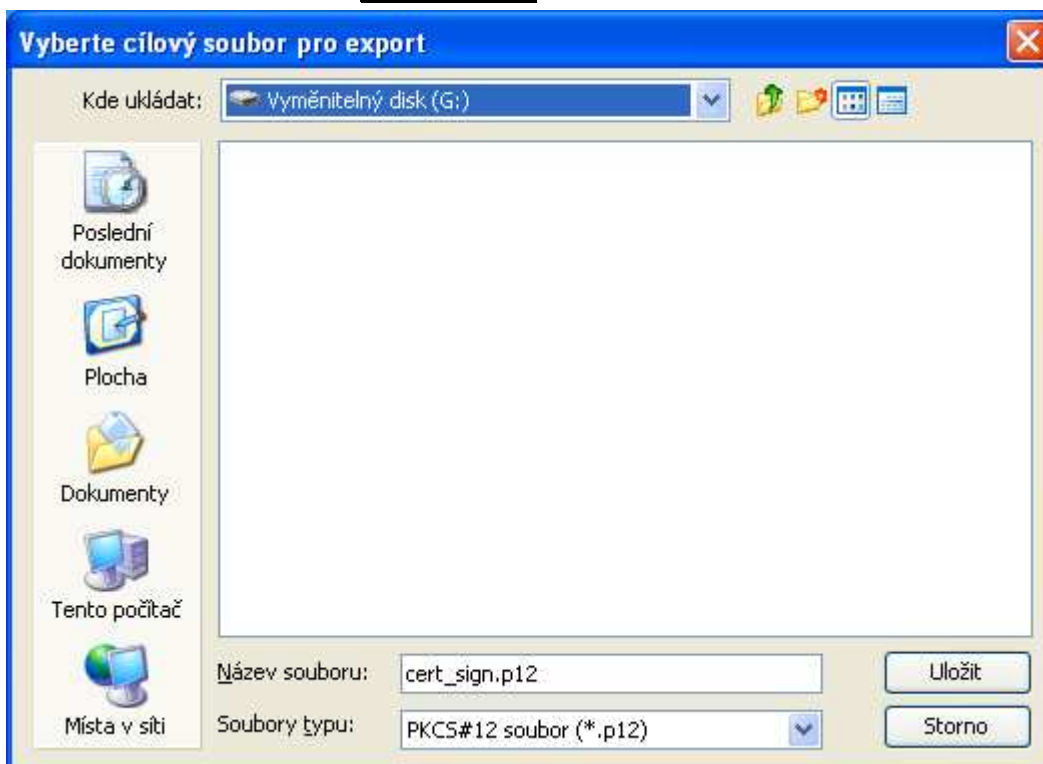
Zvolte, že chcete exportovat certifikát a soukromý klíč.

Stiskněte tlačítko **Pokračovat**. Zobrazí se následující okno:



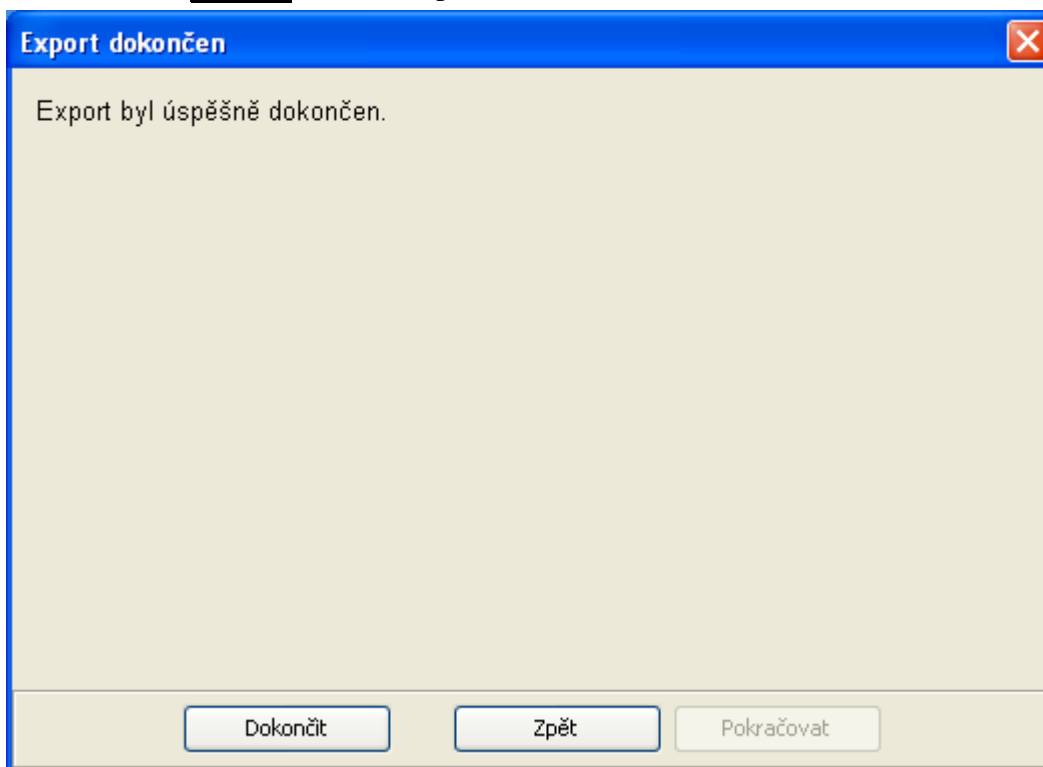
Zadejte heslo, kterým bude chráněn exportovaný obsah v souboru. Pro „složitost“ hesla platí stejná pravidla jako pro heslo chránící adresář s klíči.

Po zadání hesla stiskněte tlačítko **Pokračovat**. Zobrazí se toto dialogové okno:



Zadejte umístění a jméno souboru, do kterého se mají exportované klíče a certifikát uložit.

Po stisknutí tlačítka **Uložit** se zobrazí poslední okno:



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

7.4 Kontrola úspěšného provedení postupu

Zkontrolujte, zda byl úspěšně vytvořen vámi specifikovaný soubor.

7.5 Import klíčů a certifikátu ze souboru

Program PostSignum Tool Plus neumožňuje importovat klíče a certifikát ze souboru typu PKCS#12.