Certifikační autority PostSignum

Instalace a použití aplikace

SafeNet Borderless Security

USB token iKey 4000

verze 1.0.2

Uživatelská dokumentace

Srpen 2008

Verze	Datum	Autor	Poznámka
0.1	18.5.2008	Petr Huptich	pracovní verze
0.2	18.5.2008	Martin Šlancar	doplněny chybějící obrázky
0.3	21.5.2008	Bc. Miroslav Trávníček	finální úpravy dokumentu
1.0	22.5.2008	Bc. Miroslav Trávníček	verze schválená projektovým manažerem
1.0.1	25.7.2008	Martin Šlancar	varování o ztrátě dat po inicializaci tokenu přesunuto na začátek kapitoly 3
1.0.2	29.8.2008	Martin Šlancar	oprava kapitoly 2.2.1, instalátor software již nelze stáhnout z webových stránek

Schváleno:

Verze	Schválil	
1.0	Ing. Pavel Plachý	projektový manažer

1 Úvod

1.1 Informace o dokumentu

Cílem tohoto dokumentu je popsat instalaci a způsob práce s s aplikací SafeNet Borderless Security, která je dodávána společně s USB tokeny iKey 4000.

Dokument popisuje časový sousled činností, které je potřeba učinit:

- instalace aplikací k USB tokenu,
- inicializace USB tokenu
- instalace certifikátů certifikačních autorit
- vygenerování klíčů a žádosti o certifikát,
- instalace vydaného certifikátu.

Obrázky v tomto dokumentu mohou být pouze orientační. Uvedené postupy počítají s ovládáním myši pravou rukou. Podobnost se jmény skutečných osob a organizací je čistě náhodná a neúmyslná.

1.2 Systémové požadavky

Obslužný software SafeNet Borderless Security je určen **pouze pro operační systémy Windows**.

1.3 Základní webová stránka

Pro projekt Czech POINT byla zřízena www stránka s adresou:

http://qca.postsignum.cz/projects/czechpoint

V následujícím textu budeme tuto stránku označovat jako „Základní webová stránka“.

2 Uživatelský software k USB tokenu

Účel postupu

Instalace ovladače pro USB token a obslužný software.

2.1 Poznámky k postupu

- Nejprve nainstalujte ovladače a obslužný software, teprve poté připojte USB token k počítači.

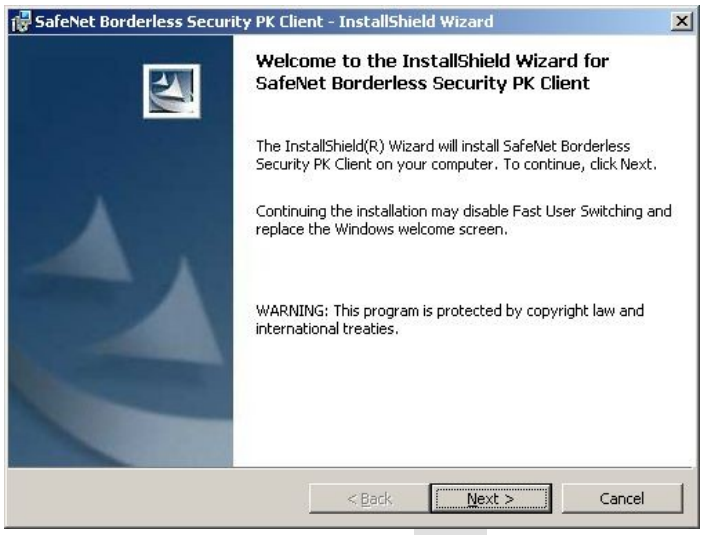
2.2 Postup

2.2.1 Instalace ovladačů a aplikací USB tokenu

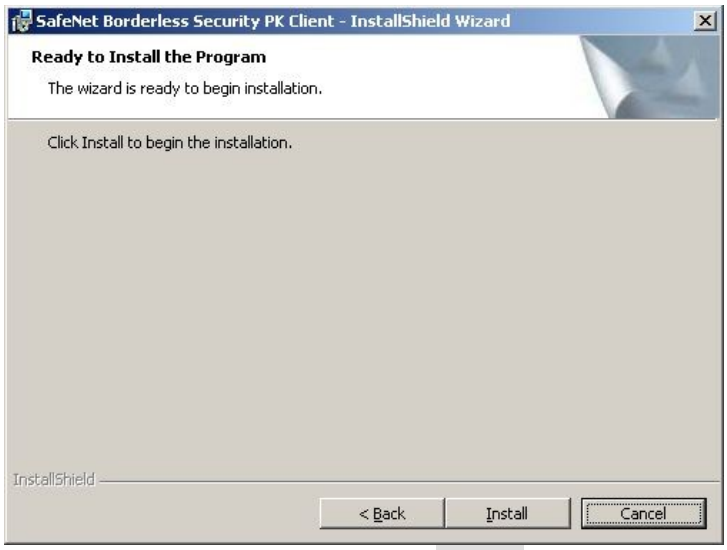
Před započetím instalace ukončete všechny aplikace. Po dokončení bude vyžadován restart počítače.

Vložte do mechaniky instalační CD **Borderless Security PK**. V adresáři **token_sw_instalator** spusťte soubor **setup.exe**. Tím zahájíte instalaci ovládacího SW a ovladače k USB tokenu iKey 4000.

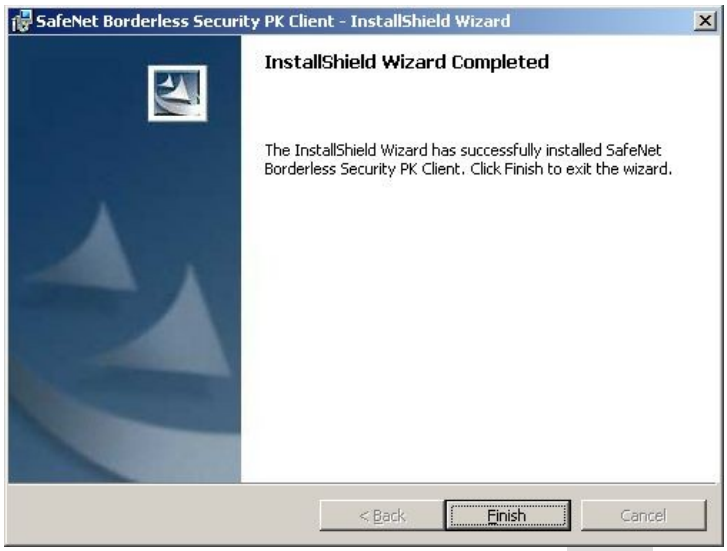
Průběh instalace:



Pro další krok stiskněte **tlačítko Next**.



Instalaci zahájíte stiskem tlačítka **Install.**



Instalace byla dokončena, stiskněte tlačítko **Finish.**

Po dokončení instalace je nutné restartovat počítač. Ukončete všechny aplikace a restartujte počítač stiskem tlačítka **Yes**.

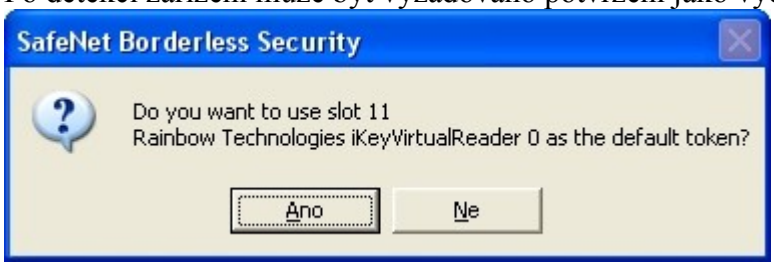
2.2.2 Připojení USB tokenu

Po instalaci a následném restartu počítače se u hodin v oznamovací oblasti hlavního panelu zobrazí nová ikona oznamující stav připojení USB tokenu.

V tomto případě není USB token připojen

Do volného USB portu připojte USB token iKey 4000. Dojde k automatické detekci nového hardware.

Po detekci zařízení může být vyžadováno potvrzení jako výchozí token.



3 Inicializace USB tokenu

Účel postupu
Nastavení PINu a PUKů USB tokenu iKey 4000

Inicializaci USB tokenu můžete provádět kdykoliv. Důrazně však upozorňujeme, že dochází ke ztrátě dat v USB tokenu při každé inicializaci. Pokud by na tokenu byly již uložené certifikáty a provedla se inicializace, budou certifikáty smazány. Kód PIN lze kdykoliv měnit (postup změny uveden v kapitole 6.2)**, kódy PUK se dají nastavit pouze při inicializaci tokenu.**

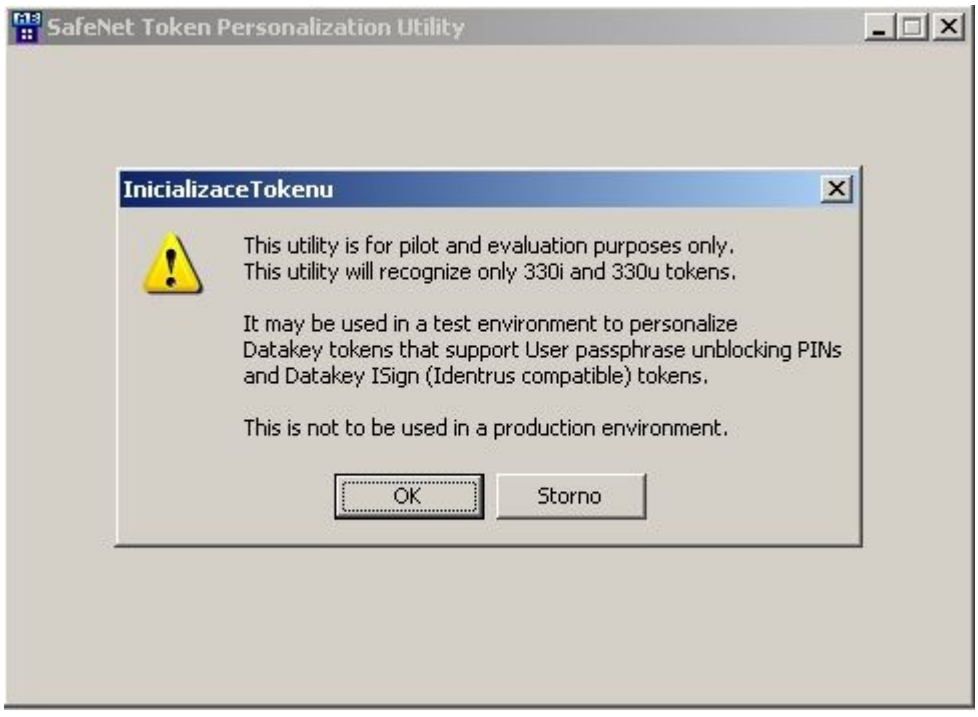
3.1 Spuštění aplikace

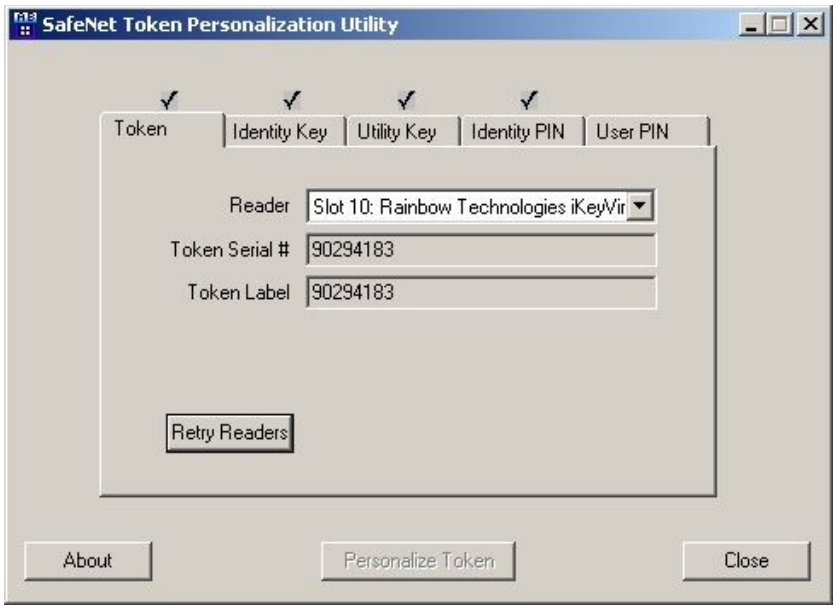
Vyhledejte soubor **InicializaceTokenu.exe,** který je nainstalován v adresáři **C:\Program Files\SafeNet\BsecClient,** nebo klikněte na následující odkaz:

C:\Program Files\SafeNet\BsecClient\InicializaceTokenu.exe

3.2 Inicializace USB tokenu

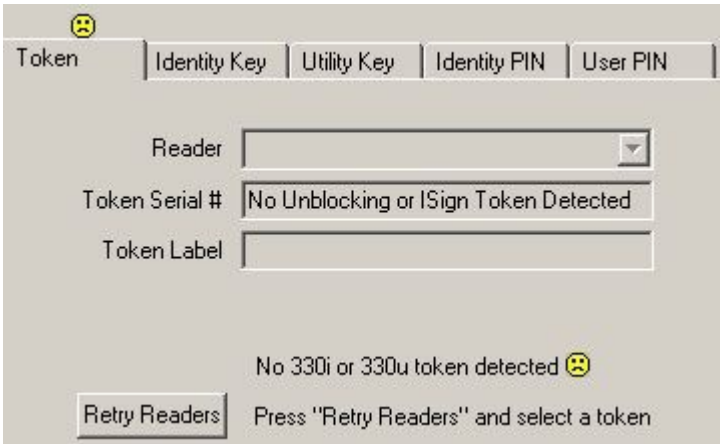
Při spuštění aplikace je vždy vyžadováno potvrzení informativní zprávy o použití programu. Zobrazený dialog vždy potvrďte tlačítkem **OK.** Po stisku tlačítka **Storno** dojde k ukončení aplikace.





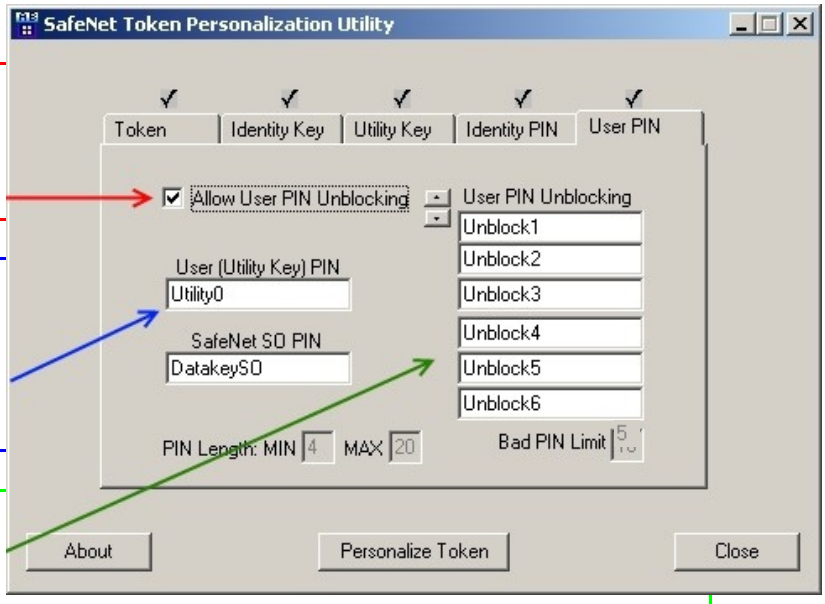
Při nalezení a rozpoznání USB tokenu iKey se zobrazí úvodní obrazovka aplikace **SafeNet Token Perzonalization Utility.** Na první zobrazené záložce jsou zobrazeny informace o vloženém USB Tokenu.

Při nenalezení USB tokenu je zobrazena úvodní záložka bez informací o USB tokenu a zamračeným emotion symbolem. V tomto případě zkontrolujte připojení tokenu do USB zásuvky a zda na tokenu svítí zeleně led dioda. Poté stiskněte tlačítko **Retry Readers.**



Pro vlastní inicializaci tokenu je nutná pouze záložka **User PIN.** *Záložky Identity Key, Utility Key, Identity PIN jsou po vybrání zašedlé, neaktivní.*

Přepněte se na záložku **User PIN,** kde se nastavuje PIN a odblokovací kódy PUK.



Zaškrtněte položku **Alow User PIN Unblocking** pro zpřístupnění všech položek nutných pro inicializaci USB tokenu.

Zadejte PIN pro Váš USB token. PIN se zadává pouze jednou, pro Vaší kontrolu zadávání se zobrazuje skutečný text, nezobrazují se zástupné znaky (např.*)

Zadejte odblokovací kódy PUK. Doplňte všech šest políček pro zadání odblokovacích kódů. Zadávejte kódy odlišné, podobně jak je to uvedeno v příkladu**. V žádném případě nenechávejte přednastavené hodnoty.**

Položku SafeNet SO PIN nedoplňujte a nechte přednastavenou hodnotu. Toto heslo se v žádné aplikaci pro USB token nevyužívá. Může sloužit pouze jako servisní kód pro výrobce.

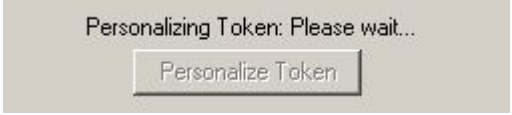
Všechny zapsané kódy PIN a PUK si pečlivě poznamenejte. Kód PIN budete vždy používat při jakékoliv operaci s USB tokenem. Kódy PUK slouží k odblokování USB tokenu, pokud 5x špatně zadáte kód PIN (viz kapitola 7 tohoto dokumentu)**.**

Po zadání všech nutných položek (PIN, PUK) pro inicializaci tokenu stiskněte tlačítko Personalize Token.

Tlačítko **About** zobrazí informace o aplikaci, tlačítko **Close** aplikaci ukončí.

Před vlastní inicializací je zobrazeno hlášení o smazání všech dat na tokenu. Pro pokračování stiskněte tlačítko **OK,** pro zrušení akce stiskněte tlačítko **Storno .**

Probíhající inicializace je zobrazena nad tlačítkem Personalize Token.



Po dokončení inicializace je zobrazena podobná informace.

4 Instalace certifikátů certifikačních autorit

Účel postupu

Instalace certifikátů certifikačních autorit PostSignum QCA, VCA do operační systému Windows.

Na základní webové stránce v části **3. Instalace certifikátů certifikačních autorit** klikněte na odkaz „Instalace certifikátů certifikačních autorit PostSignum“. Zobrazí se stránka:

4.1 Automatická instalace certifikátů autorit

Webová stránka nabídne možnost automatické instalace certifikátů jen v případě, že se jí podaří úspěšně detekovat potřebnou komponentu.

Po stisku tlačítka **Instalovat certifikáty** se zahájí proces instalace všech nezbytných certifikátů. Pokud instalace skončí s chybou proveďte ruční instalaci certifikátů autorit.

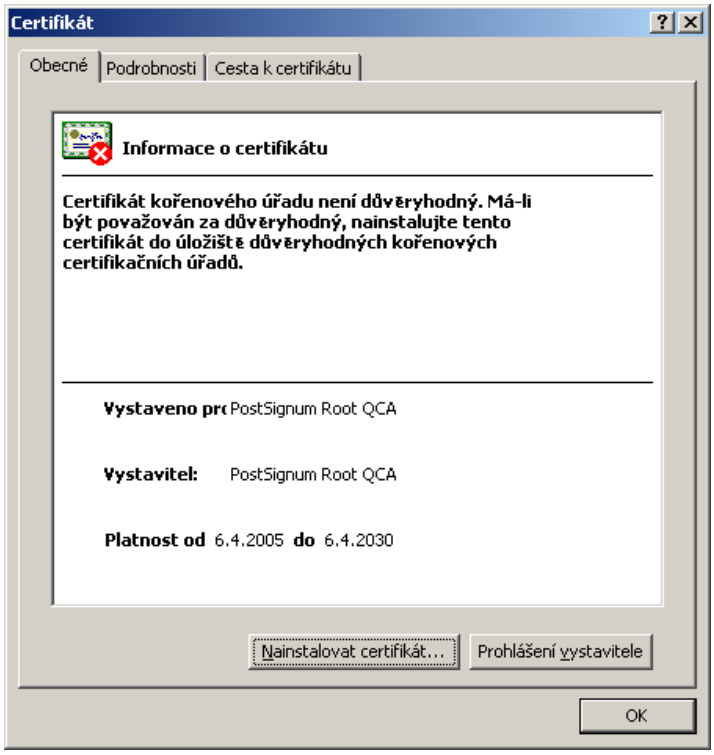
4.2 Ruční instalace certifikátů autorit

Následující postup proveďte postupně s každým ze souborů:

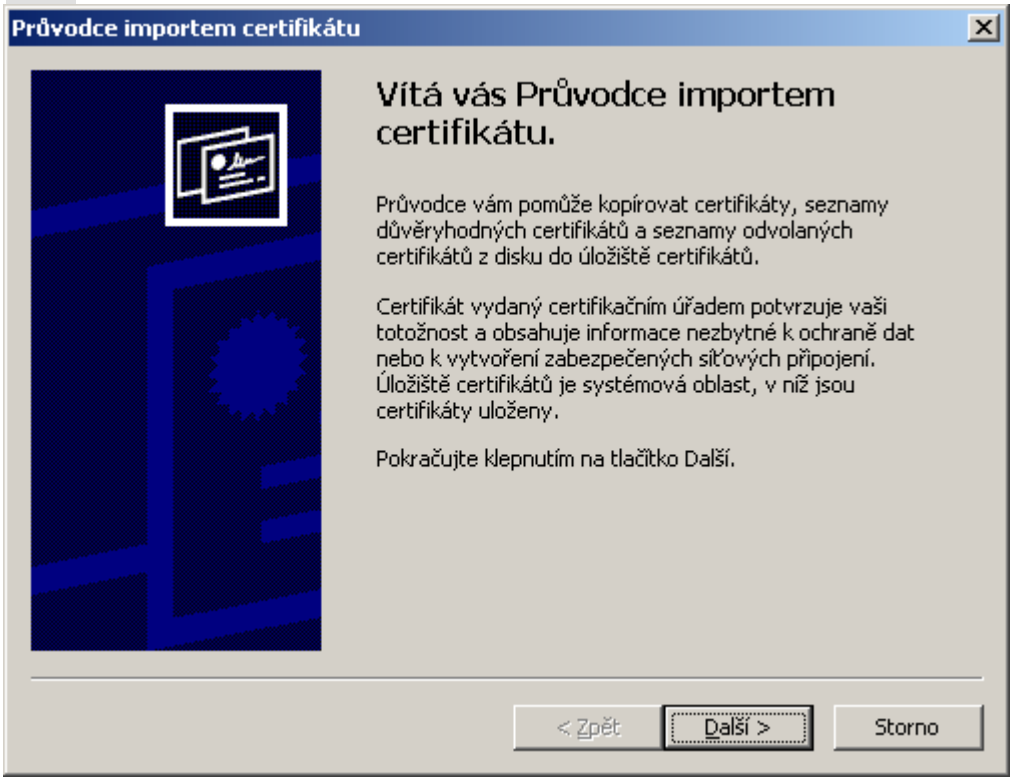
- **postsignum_qca_root.cer** .. soubor s certifikátem kořenové autority
- **postsignum_qca_sub.cer** .. soubor s certifikátem kvalifikované autority
- **postsignum_vca_sub.cer** .. soubor s certifikátem komerční autority

(Postup je rovněž uveden na webové stránce.)

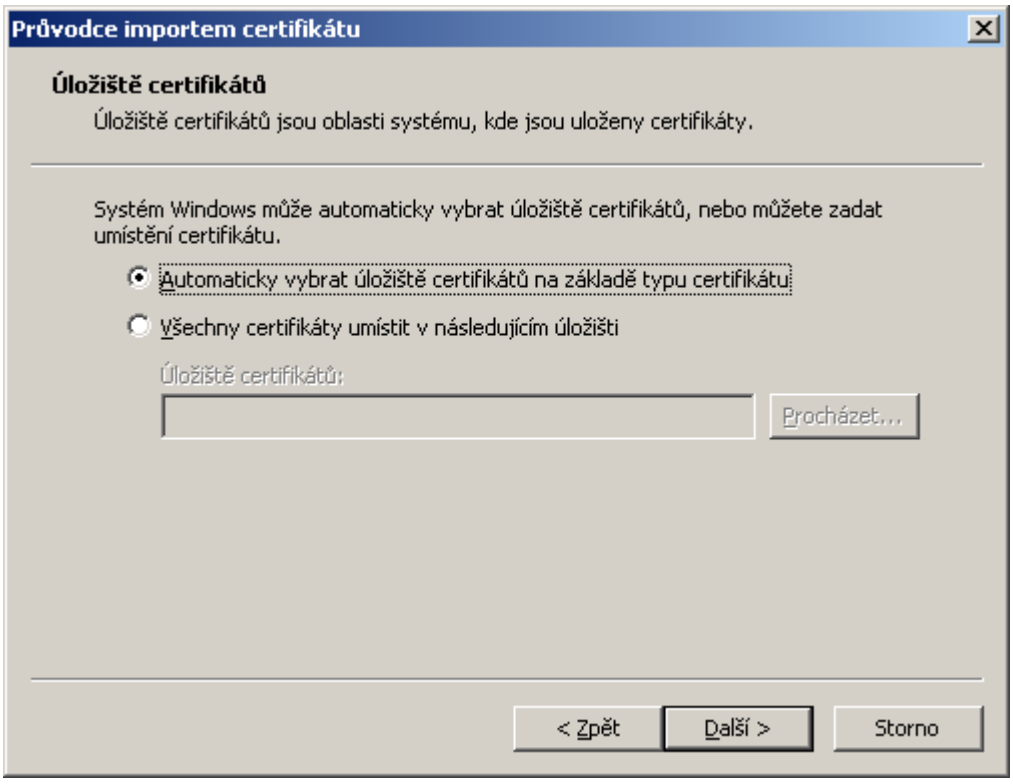
Klikněte myší na odkaz pro stažení souboru. Místo uložení souboru ale stiskněte tlačítko **Otevřít**. Po chvíli se zobrazí okno s informacemi o certifikátu.



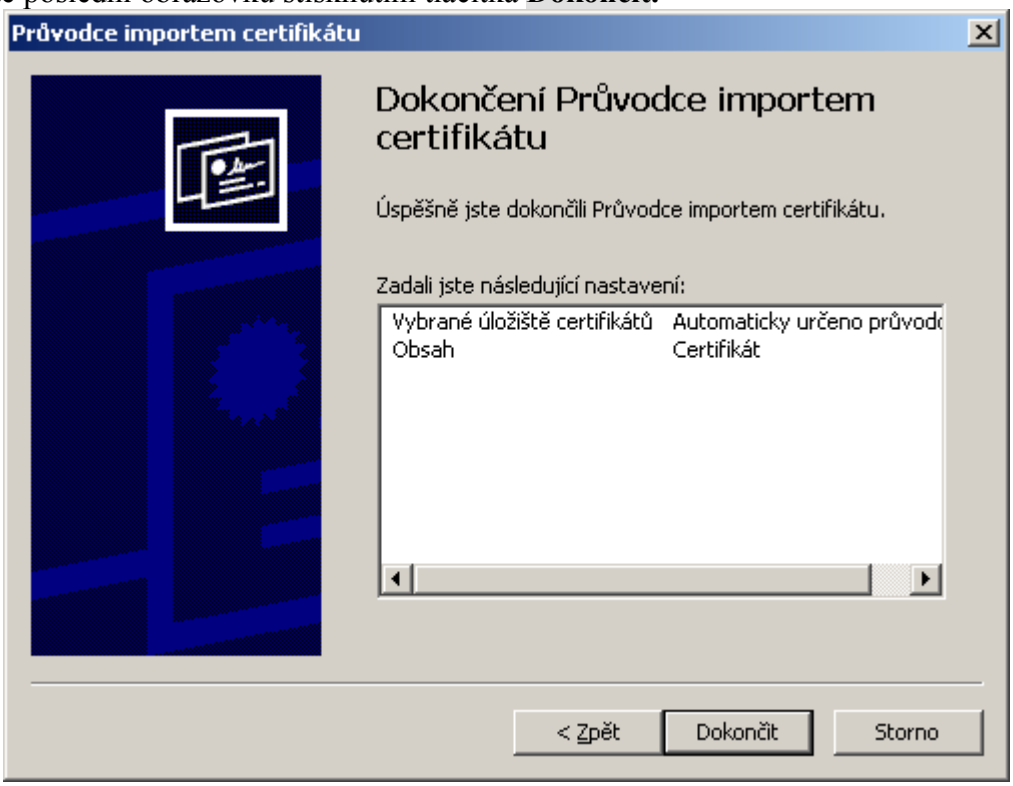
Stiskněte tlačítko **Nainstalovat certifikát.** Spustí se průvodce importem certifikátu. Stiskněte tlačítko **Další**.



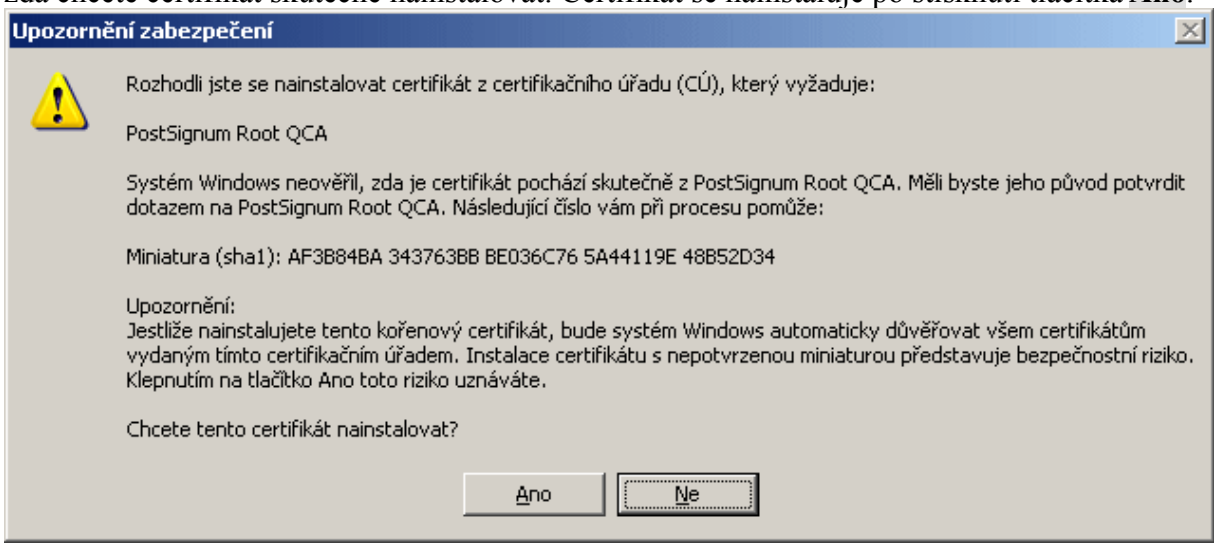
Na druhé obrazovce ponechte nastavenou položku **Automaticky vybrat úložiště certifikátů.** Stiskněte tlačítko **Další.**



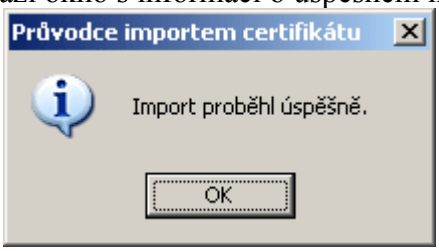
Potvrďte poslední obrazovku stisknutím tlačítka **Dokončit.**



Pokud instalujete certifikát ze souboru **postsignum_qca_root.cer**, zobrazí se okno s dotazem, zda chcete certifikát skutečně nainstalovat. Certifikát se nainstaluje po stisknutí tlačítka **Ano**.



Po dokončení importu se zobrazí okno s informací o úspěšném importu.



5 Generování klíčů a import certifikátu

5.1 Registrace certifikátu do Windows

Registrace certifikátů uložených na tokenu se provádí automaticky po vložení tokenu do USB. Po vyjmutí tokenu dojde k automatickému odmazání certifikátů ze systému.

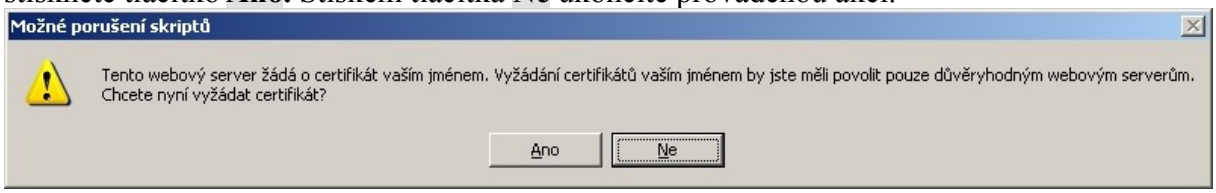
5.2 Generování klíčů a žádosti o certifikát

5.2.1 Generování klíčů a žádosti o certifikát

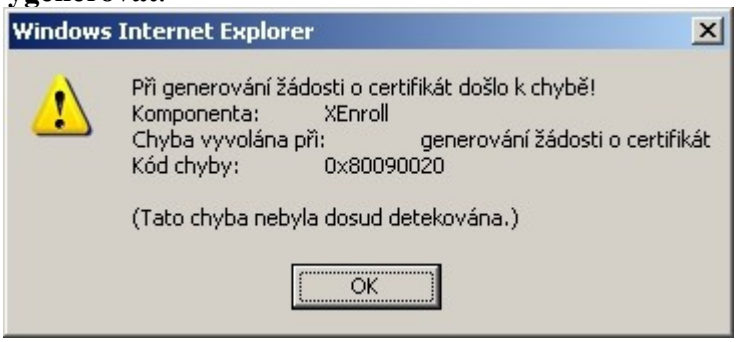
Na základní webové stránce klikněte na odkaz v části **4b. Generování klíčů a žádosti o certifikát.**
Zobrazí se následující stránka:

Doplňte všechny potřebné údaje pro vytvoření žádostí o certifikát, vyberte velikost generovaného klíče (standardní velikost je 1024 bitů, pro vyšší zabezpečení se používá 2048 bitů) a stiskněte tlačítko **Vygenerovat.**

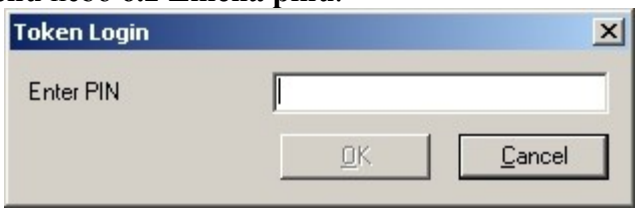
Před samotným generováním klíčů se zobrazuje následující varovné hlášení, Pro pokračování stiskněte tlačítko **Ano.** Stiskem tlačítka **Ne** ukončíte prováděnou akci.



Při zobrazení následující chyby nejspíše vznikl problém v komunikaci s USB tokenem. Vložte token do USB konektoru, nebo jej vyjměte a znovu vložte do USB konektoru. Znovu stiskněte tlačítko **Vygenerovat**.



Pro zápis klíčů na USB token je vyžadován PIN, který jste nastavili v kapitole **3.2 Inicializace USB tokenu** nebo **6.2 Změna pinu**.



Průběh generování klíčů je zobrazen v podobném okně.

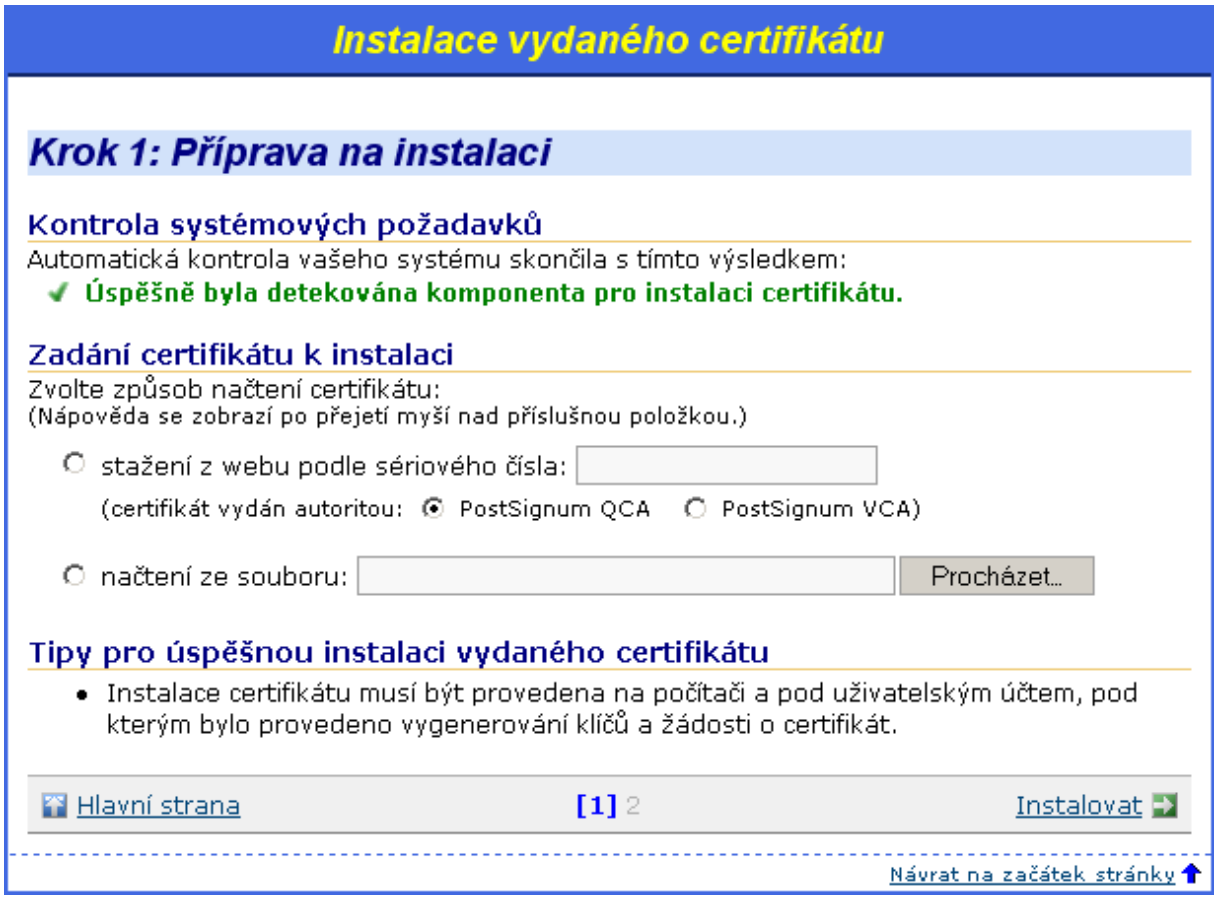
Generování klíčů probíhá dvakrát za sebou. Při úspěšném generování klíčů je zobrazena informace, že žádosti o certifikáty byly uloženy na server PostSignum.

5.3 Vydání certifikátu

Na základní webové stránce klikněte na odkaz v části **5. Vydání certifikátu,** kde jsou uvedeny podrobnější informace, jak probíhá vydání certifikátů. Na stránce je uveden rovněž seznam kontaktních míst, které vydávají certifikáty.

5.4 Instalace vydaného certifikátu

Na základní webové stránce klikněte na odkaz v části **6. Instalace vydaného certifikátu.**
Na zobrazené stránce si můžete vybrat způsob načtení vašeho vydaného certifikátu.



- Stažení z webu podle sériového čísla – vyplňte sériové číslo certifikátu, které naleznete na protokolu o vydání certifikátu. Tento dokument obdržíte na pracovišti České pošty při vydání certifikátu. Vyberte, jakou certifikační autoritou byl vydán certifikát (opět uvedeno na protokolu o vydání certifikátu).
- Načtení ze souboru – pokud máte vydaný certifikát uložený v souboru, zvolte tlačítko **Procházet** a vyberte soubor s certifikátem.

Kliknutím na odkaz **Instalovat** spustíte instalaci zvoleného certifikátu. Je zobrazeno upozornění, zda chcete opravdu instalovat certifikát, stiskněte tlačítko **Ano**.

Pro zápis klíčů na USB token je vyžadován PIN, který jste nastavili v kapitole **3.2 Inicializace USB tokenu** nebo **6.2 Změna pinu**.

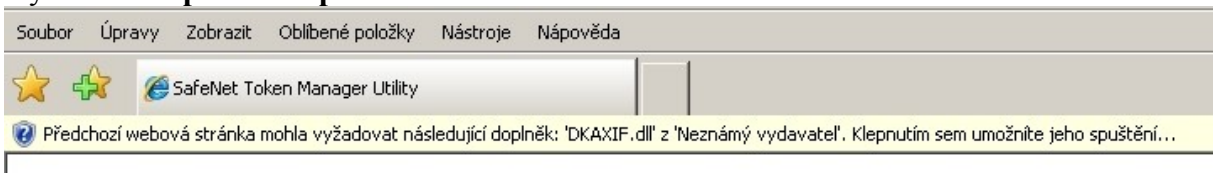
Nakonec se zobrazí **krok 2** průvodce s informací, že certifikát byl úspěšně nainstalován. Pokud během instalace došlo k chybě, je zobrazen popis chyby.

6 Operace s USB tokenem

6.1 Spuštění aplikace

Pomocí zástupce na ploše nebo v nabídce Start (Programy→SafeNet→Borderless Security PK) spusťte aplikaci **SafeNet Token Manager Utility**. Stiskněte tlačítko **Enrollment Update**. Operace v této aplikaci mohou být zdlouhavé, mějte prosím strpení při každé provedené akci.

Po kliknutí na tlačítko Enrollment Update se může zobrazit hlášení v horní části Internet exploreru. Pokud se hlášení zobrazí, klikněte na text s chybovým hlášením levým tlačítkem myši a zvolte **povolit doplněk**.

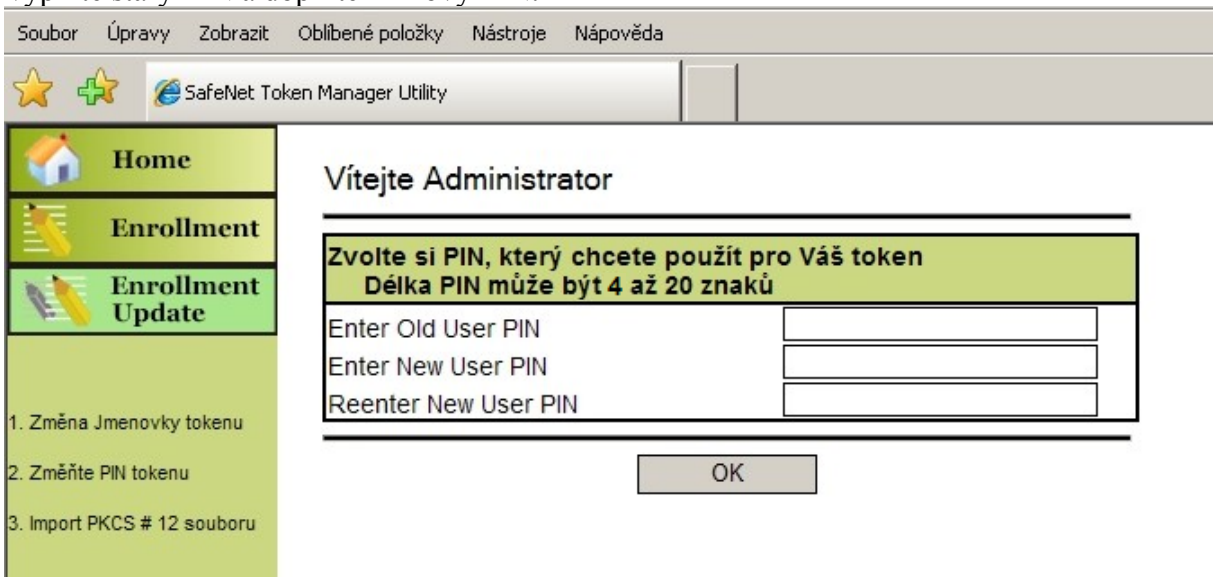


Při zobrazení tohoto dotazu prosím vložte USB token iKey 4000 a stiskněte tlačíto **OK**.

6.2 Změna pinu

V nabídce v levé části zvolte **Změňte PIN tokenu.**

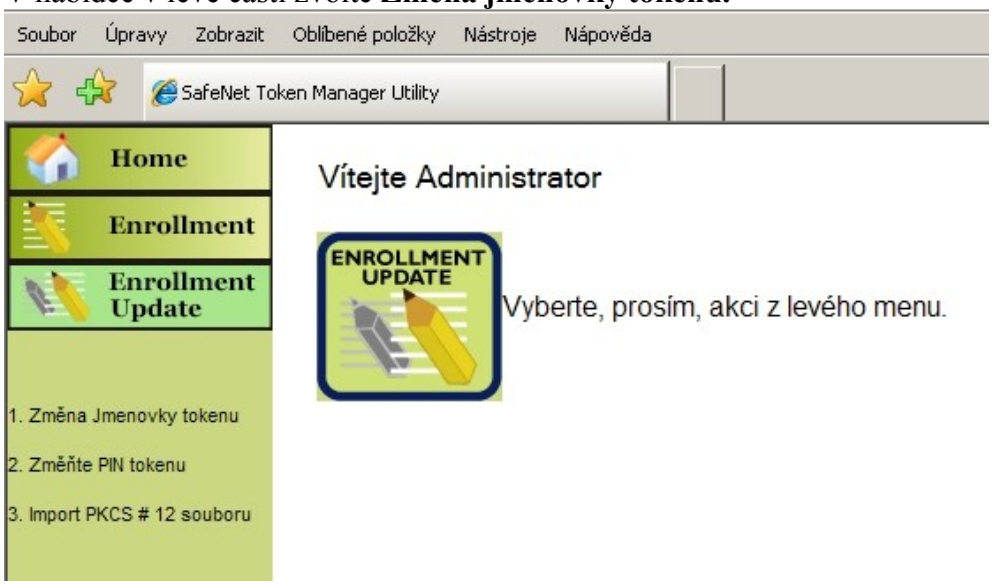
Vyplňte starý PIN a doplňte 2x nový PIN.



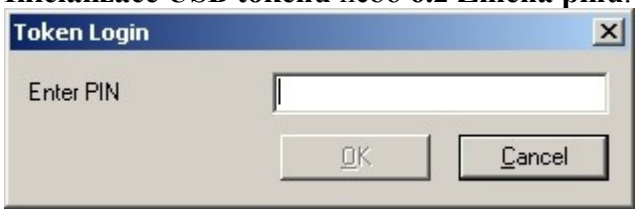
Při neúspěšném pokusu o změnu PINu jste upozorněni. Pokud je vše úspěšně provedeno, jste o tom informováni.

6.3 Změna jmenovky tokenu

V nabídce v levé části zvolte **Změna jmenovky tokenu.**



Při manipulaci s USB tokenem je vyžadován PIN, který jste nastavili v kapitole **3.2 Inicializace USB tokenu** nebo **6.2 Změna pinu**.



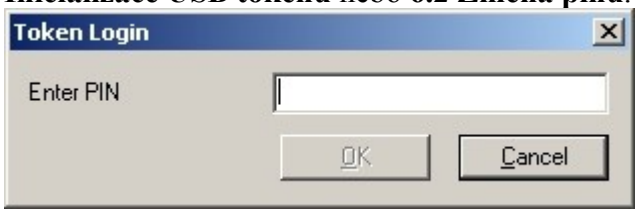
Zvolte název tokenu, prosíme nepoužívejte české znaky. Pro potvrzení zvolte **OK**.

Při neúspěšném pokusu o změnu jmenovky jste upozorněni. Pokud je vše úspěšně provedeno, jste o tom informováni.

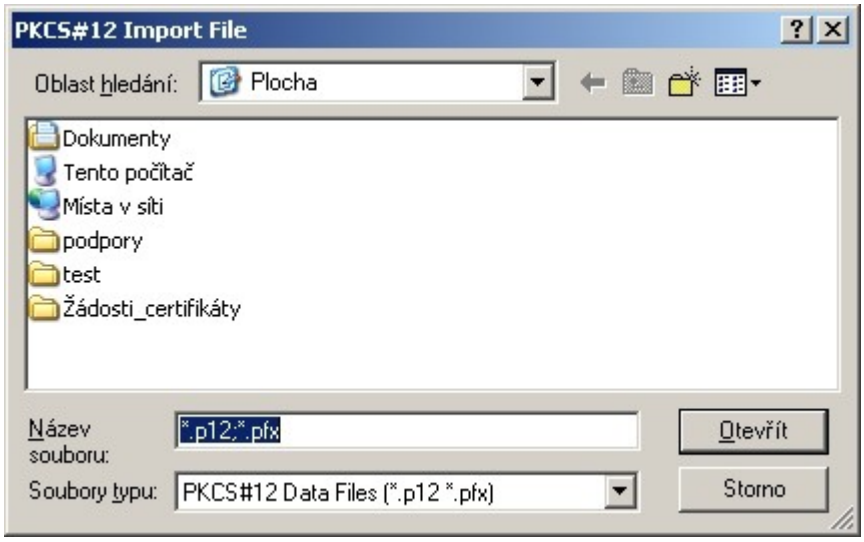
6.4 Import PKCS#12 souboru

V nabídce v levé části zvolte **Import PKCS#12 souboru**.

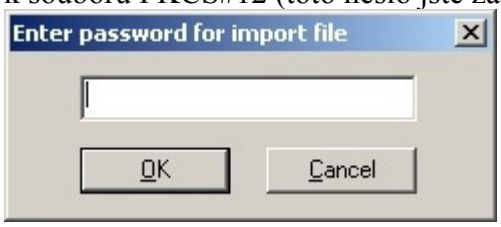
Stiskněte tlačítko **Import PKCS#12 souboru**.
Pro zápis klíčů na USB token je vyžadován PIN, který jste nastavili v kapitole **3.2 Inicializace USB tokenu** nebo **6.2 Změna pinu**.



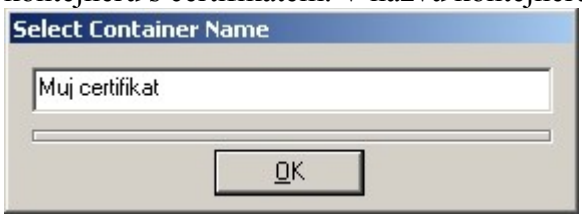
Po vložení PINu a stisku tlačítka **OK** se zobrazí okno pro vyhledání souboru se zálohou certifikátu.



Po vyhledání souboru a stisku tlačítka **Otevřít,** se zobrazí další okno požadující zadání hesla k souboru PKCS#12 (toto heslo jste zadávali při generování souboru):



Po zadání hesla a stisknutí tlačítka **OK** se zobrazí další okno požadující zadání názvu kontejneru s certifikátem. V názvu kontejneru prosím nepoužívejte české znaky.



Po zadání jména a stisknutí tlačítka **OK** se již zobrazí okno se zprávou, že obsah souboru PKCS#12 byl úspěšně importován do USB tokenu.

7 Odblokování USB tokenu

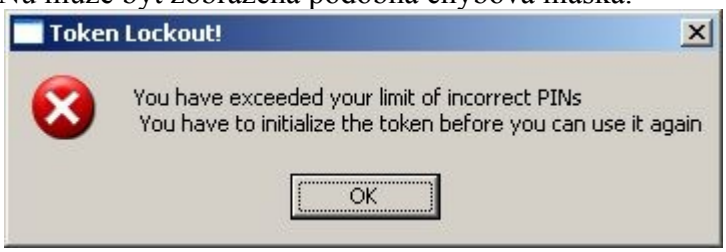
Účel postupu

Opětné zprovoznění USB tokenu po opakovaném chybném zadání PINu.

7.1 Proč k zablokování tokenu došlo?

K zablokování tokenu dojde, pokud se 5x zadá chybný PIN, který jste nastavili v kapitole **3.2 Inicializace USB tokenu** nebo **6.2 Změna pinu**.

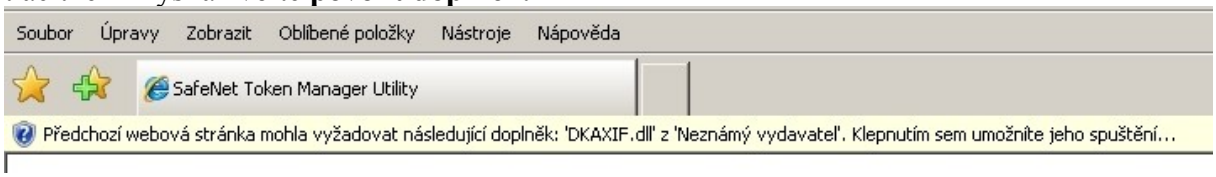
Při zablokování PINu může být zobrazena podobná chybová hláška.



7.2 Spuštění aplikace pro odblokování tokenu

Pomocí zástupce na ploše nebo v nabídce Start (Programy→SafeNet→Borderless Security PK) spusťte aplikaci **SafeNet Token Manager Utility**. Stiskněte tlačítko **Enrollment Update**. Operace v této aplikaci mohou být zdlouhavé, mějte prosím strpení při každé provedené akci.

Po kliknutí na tlačítko **Enrollment Update** se může zobrazit hlášení v horní části Internet Exploreru. Pokud se hlášení zobrazí, tak na text s chybovým hlášením klikněte levým tlačítkem myši a zvolte **povolit doplněk.**

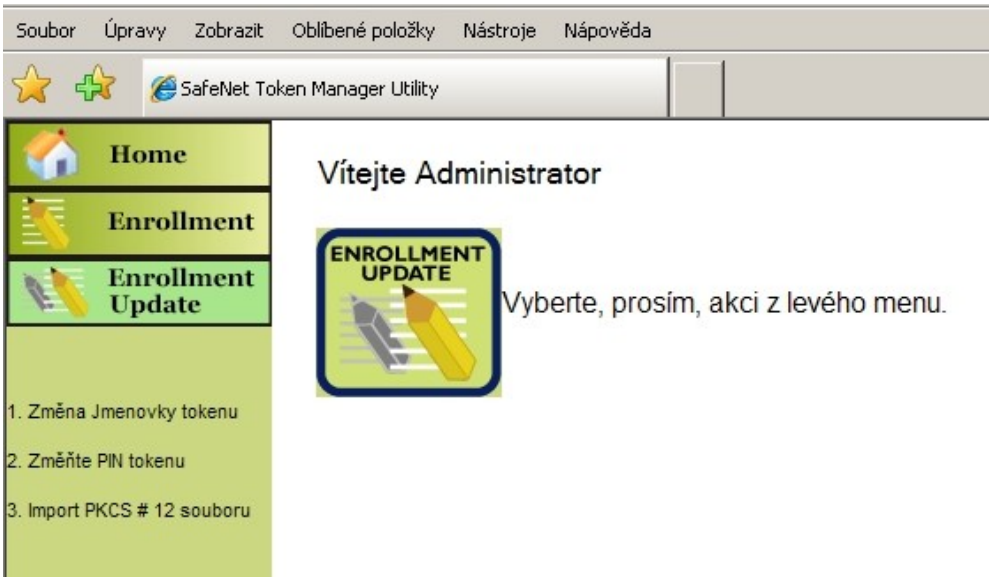


Při zobrazení tohoto dotazu prosím vložte USB token iKey 4000 a stiskněte tlačíto **OK**.

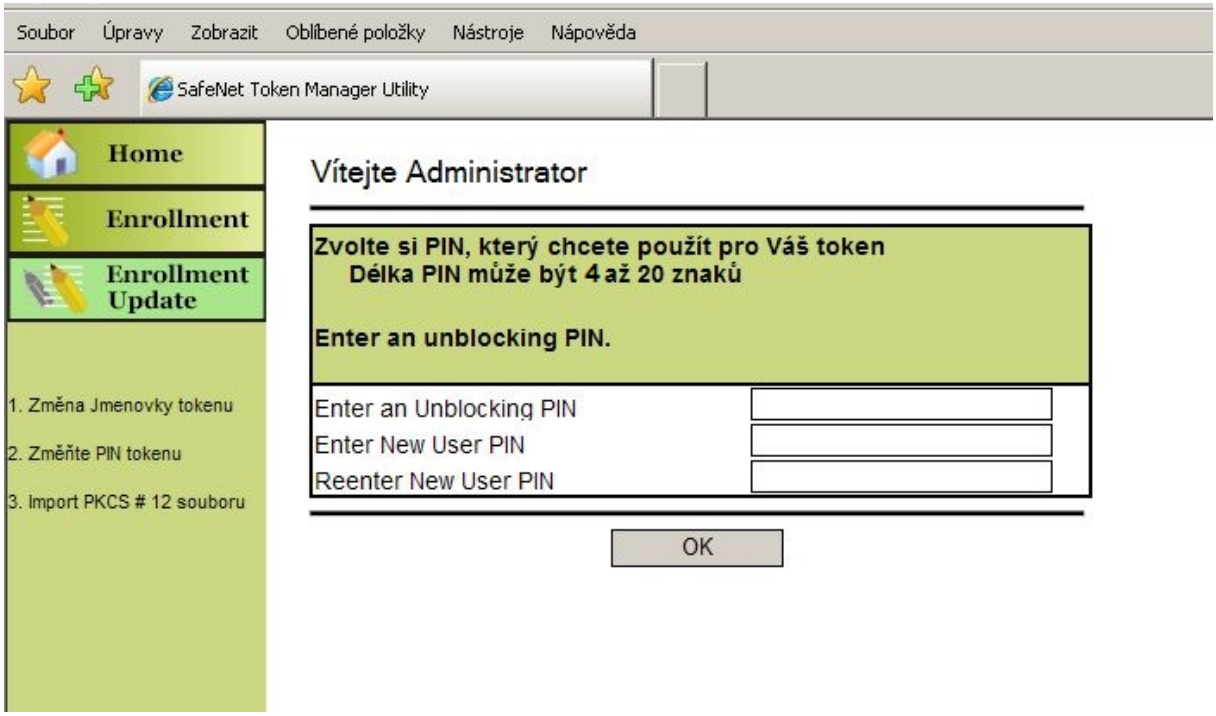
Při spuštění aplikace se zablokovaným tokenem bude zobrazena tato informativní hláška.

7.3 Odblokování USB tokenu

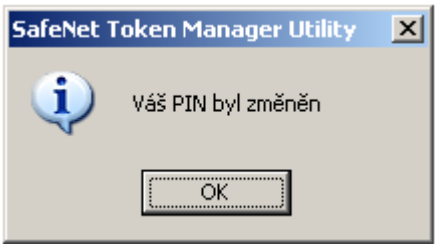
V nabídce v levé části zvolte **Změňte PIN tokenu.**



Doplňte jeden z Unblocking PINů (PUK), který jste zadávali v kapitole **3.2 Inicializace USB tokenu**. Dále doplňte 2x nový PIN a stiskněte tlačítko **OK.**



Při neúspěšném pokusu o změnu PINu jste upozorněni. Pokud je vše úspěšně provedeno, jste o tom informováni.



Důležité upozornění:
Po zadání Unblocking PINu (PUKu) již tento použitý PUK nelze použít. Pokud vyčerpáte všechny Unblocking PINy, nelze již token odblokovat, ale pouze znovu inicializovat (viz kapitola 3). **Při inicializaci tokenu ale dochází ke ztrátě dat uložených v tokenu.**