Certifikační autorita PostSignum

Instalace a použití aplikací Klíčník

Uživatelská dokumentace - verze 2.0.0

Obsah dokumentu

1. Informace o dokumentu

Cílem tohoto dokumentu je popsat všechny kroky vedoucí k úspěšné práci s certifikáty České pošty instalovanými do USB hardwarového šifrovacího klíče iKey 4000.

Dokument popisuje časový sousled činností, které je potřeba učinit:

- instalace aplikací Klíčník 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.

1.1. Systémové požadavky

Aplikace Klíčníka jsou v současné době podporovány těmito operačními systémy:

Podpora OS Windows	XP SP3*		Vista **		Windows 7 ***		Server 2003		Server 2008		Server 2008 R2
	32bit	64bit	32bit	64bit	32bit	64bit	32bit	64bit	32bit	64bit	64bit
SAC 8.0 †	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Klíčník 1.2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
BSec PKI 7.3.0.0006	✓	✗	✓	✗	✓	✗	✓	✗	✓	✗	✗

Proffesional; ** Business/Enterprise/Ultimate; *** Professional/Enterprise/Ultimate; † podpora i pro Home Basic/Premium Edition

1.2. Základní webová stránka

http://www.bezpecnyklic.cz

položka v levém menu „Postup pro získání Bezpečného klíče“

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

1.3. Tipy a rady

Na webových stránkách pod následujícím odkazem **http://www.t-soft.cz/klicnik** je k nalezení mnoho užitečných informací týkajících se práce s tokeny, instalace potřebných programů a použití certifikátů.

Stránky jsou určeny zejména pro uživatele, pro které problematika týkající se autentizačních tokenů nová. V sekcích „Časté otázky“ a „Tipy a rady“ uživatelé najdou řešení nejběžnějších problémů spojených s instalací či používáním, v sekci „Ke stažení“ najdou např. odkaz na stažení aktuálních ovladačů k tokenu aj.

2. Uživatelský software k USB tokenu

2.1. Poznámky k postupu

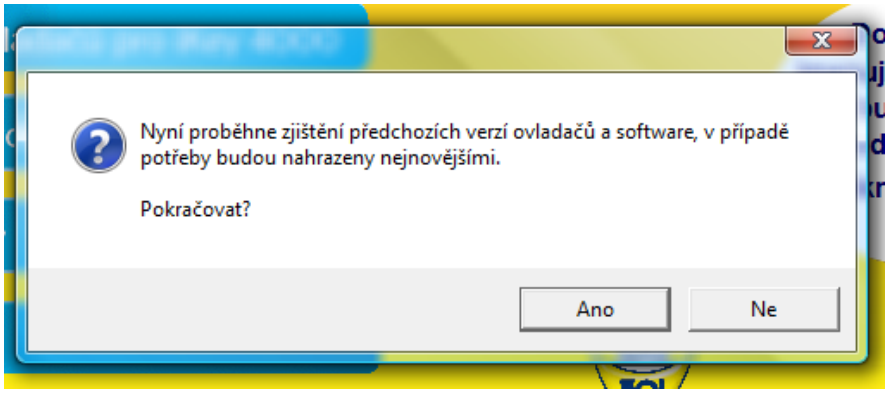
S instalací všech programů Vám pomůže interaktivní průvodce, který je součástí instalačního CD. Instalaci pomocí průvodce doporučujeme zejména uživatelům, kteří ještě nemají s tokeny a certifikáty dostatek zkušeností. Postup je následující:

2.2. Instalace aplikací Klíčníka pomocí průvodce

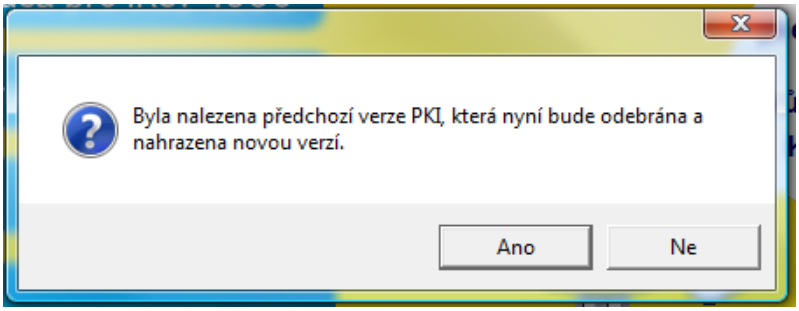
Před započetím instalace ukončete všechny aplikace. Po dokončení bude vyžadován restart počítače. Instalace bude vyžadovat přihlášení pod účtem správce či administrátora PC.

Vložte do mechaniky instalační CD Bezpeční klíč. Na hlavním menu klikněte kurzorem myši na bublinu u obrázku průvodce:

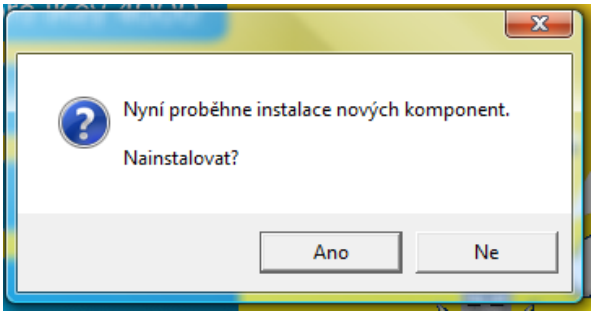
Instalátor zjistí zda, máte již některý z programů Klíčníka nainstalovaný:



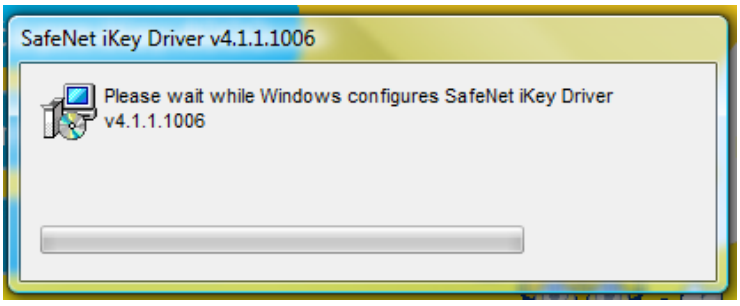
V případě nalezení starší verze ovladačů, SW BSec PKI nebo Klíčník Vám instalátor nabídne jejich odinstalaci a nahrazení starší verze za novou. Akci je třeba potvrdit:



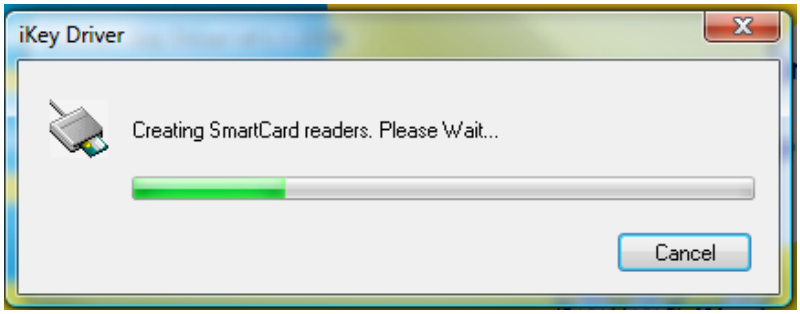
Po té již proběhne instalace všech nových komponent:



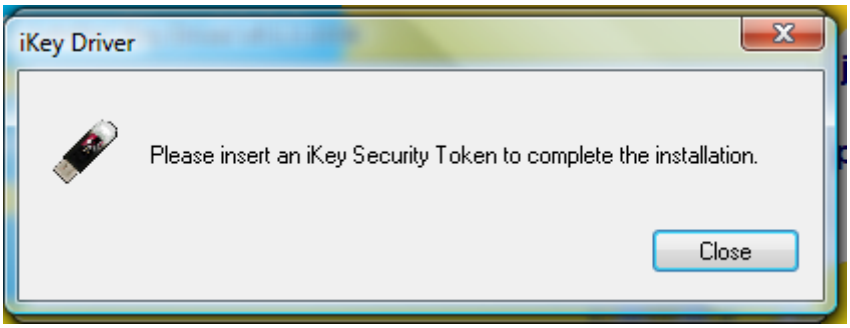
Nejdříve proběhne instalace ovladačů pro token iKey 4000:



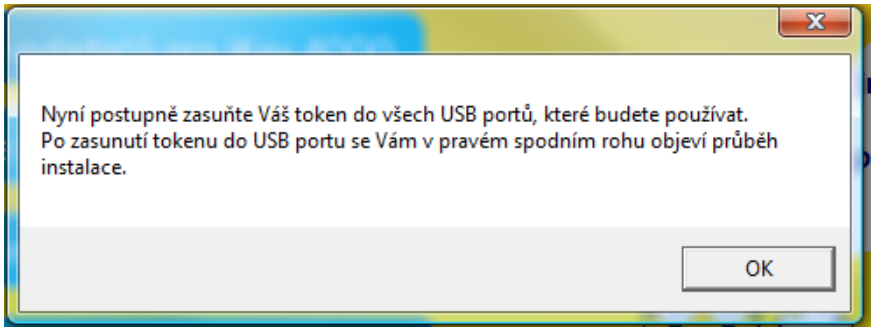
Do probíhající instalace nijak nezasahujte:



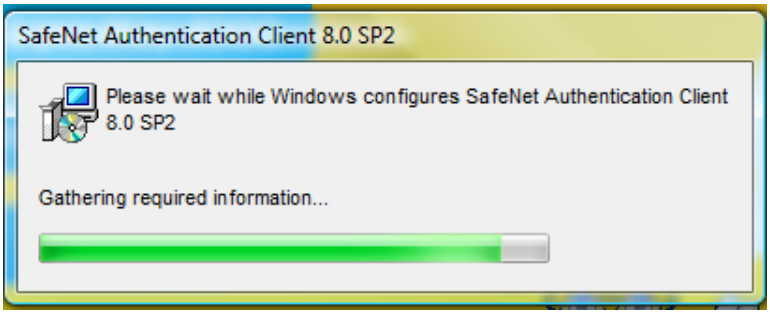
Teprve, až budete vyzváni, zasuňte svůj token iKey 4000 do USB portu v PC:



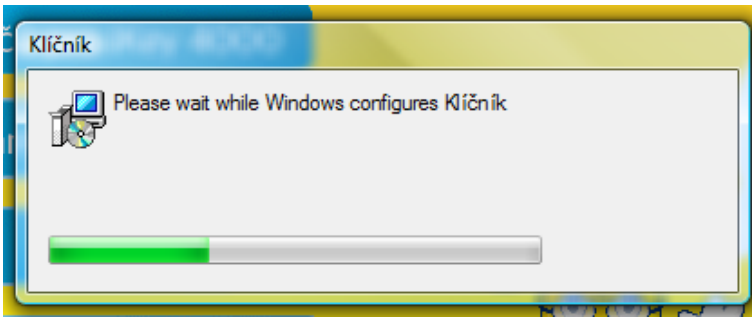
Jakmile bude USB port nakonfigurován, instalátor Vás vyzve, abyste podobně nakonfigurovali všechny USB porty, které chcete pro token iKey využívat:



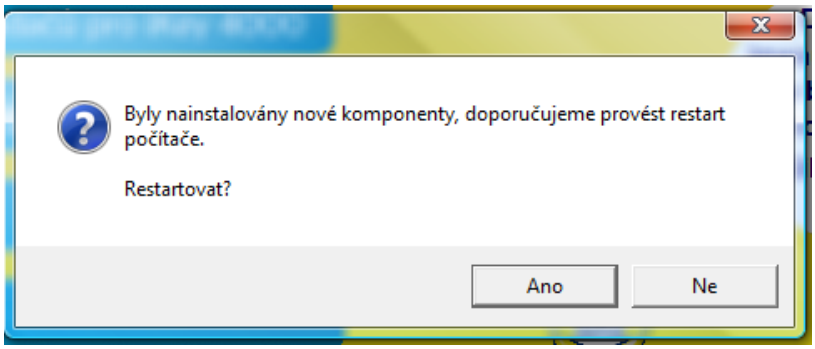
Po instalaci ovladačů bude nainstalován middleware SafeNet Authentication Client:



Nakonec bude spuštěna instalace personifikační utility Klíčník:



Po dokončení instalace programů Vám systém nabídne restart PC. Restartování PC důrazně doporučujeme:



2.3. Postup při ruční instalaci programů Klíčníka

- Pokud se rozhodnete pro ruční instalaci, doporučujeme následující postup:
  - Nejprve nainstalujte ovladače (drivery) k tokenu iKey 4000
  - Následně nainstalujte middleware SafeNet Authentication Client (v případě zpětné kompatibility s aplikacemi Borderless Security PKI (pro pokročilé uživatele a pro administrátory je určeno AMC, kde si sami určí bezpečnostní politiku a vytvoří .msi balíček – pouze pro program BSec PK)).
  - Nakonec nainstalujte program Klíčník, pomocí kterého provedete inicializaci tokenu

2.3.1. Instalace ovladačů k tokenu iKey 4000

Před započetím instalace ukončete všechny aplikace. Po dokončení bude vyžadován restart počítače. Instalace bude vyžadovat přihlášení pod účtem správce či administrátora PC.

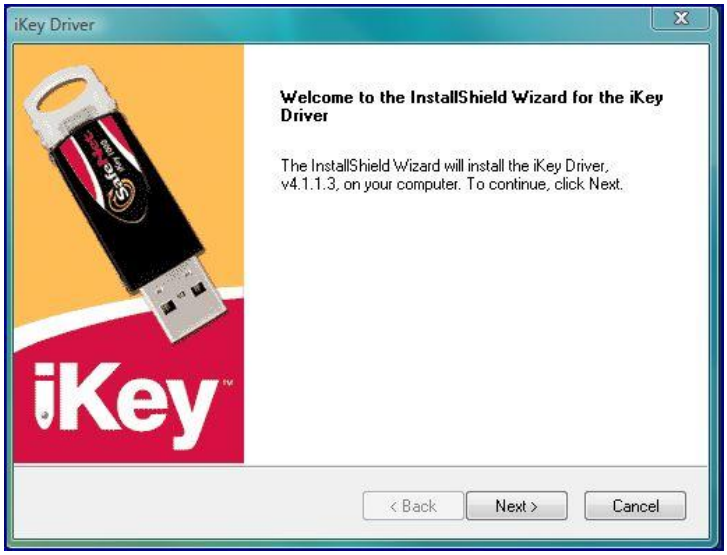
Vložte do mechaniky instalační CD Bezpeční klíč. Na hlavním menu instalačního CD zvolte odkaz "Instalace ovladačů pro iKey 4000". Po té vyberte odkaz dle operačního systému Vašeho PC:

- Windows 32 Bit OS 2000/XP/2003/Vista/2008 Server/Windows 7
- Windows 64 Bit OS XP/2003/Vista/2008 Server/2008 Server R2/ Windows 7

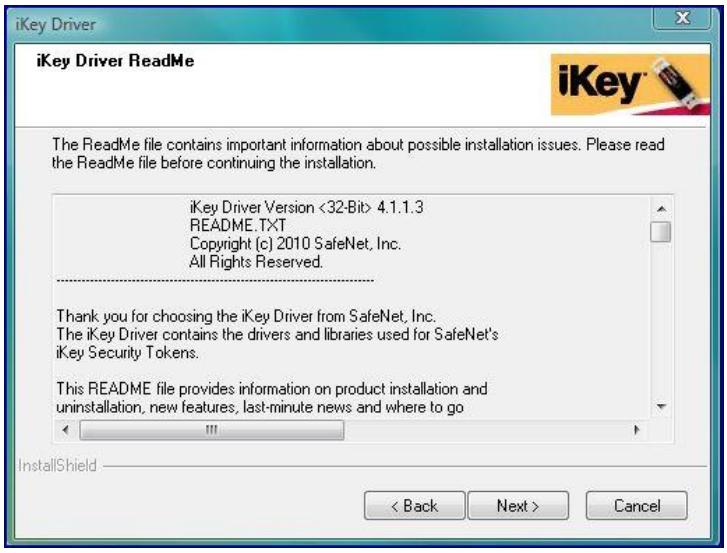
Odinstalace předchozích verzí:

Nejprve se ujistěte, že nemáte v PC nainstalované starší verze ovladačů pro iKey, pokud ano, ondinstalujte je. Rovněž zkontrolujte, zda nemáte starší verzi middlewaru Borderless Security PKI. Tu odinstalujte také.

Průběh instalace:



Pro další krok stiskněte tlačítko Next



Na této obrazovce si můžete zkontrolovat právě instalovanou verzi ovladače.
Pro další krok stiskněte tlačítko **Next** .

Zde je nutno přijmout licenční podmínky výrobce.
Pro další krok stiskněte tlačítko **Yes** .

Pro dokončení instalace je potřeba zasunout do USB portu token iKey.

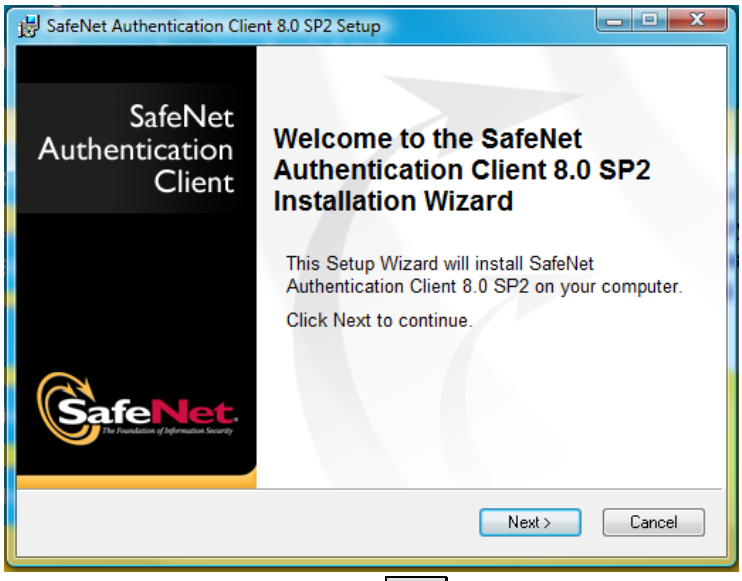
Pozn.: Doporučujeme toto zopakovat pro všechny porty, které máte na Vašem PC a které budete pro tento účel využívat.

Pro dokončení instalace stiskněte tlačítko **Finish** .

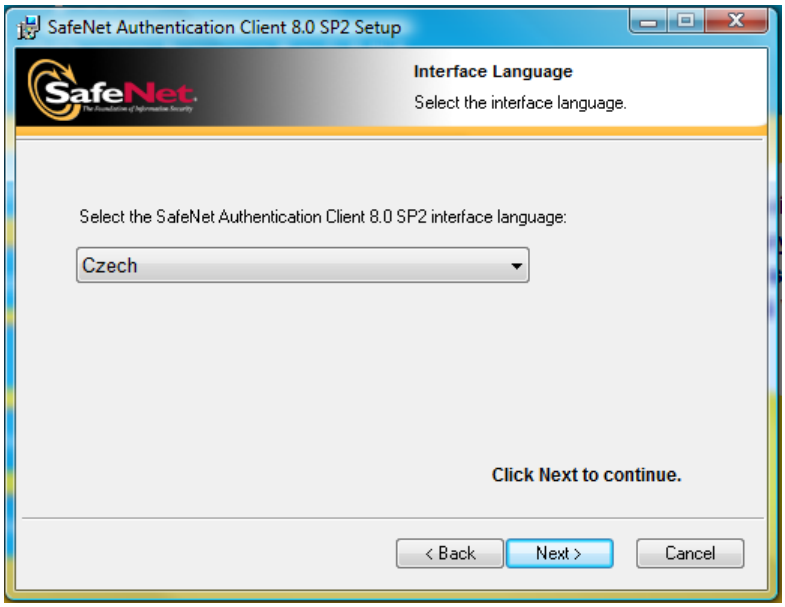
2.3.2. Instalace middlewaru SafeNet Authentication Client (SAC)

Vložte do mechaniky instalační CD **Bezpeční klíč**. Na hlavním menu instalačního CD zvolte odkaz "Instalace programů" a následně " SafeNet Authentication Client ".

Průběh instalace:



Pro další krok stiskněte tlačítko **Next** .
Na další obrazovce vyberte jazyk instalace:

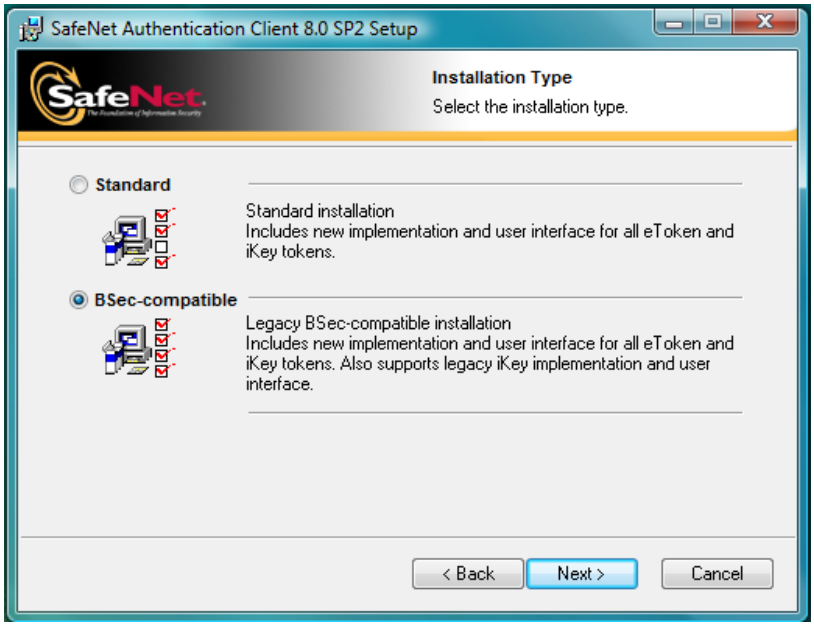


Pro další krok stiskněte tlačítko **Next** .

Po odsouhlasení licenčních podmínek, vyberte typ instalace:

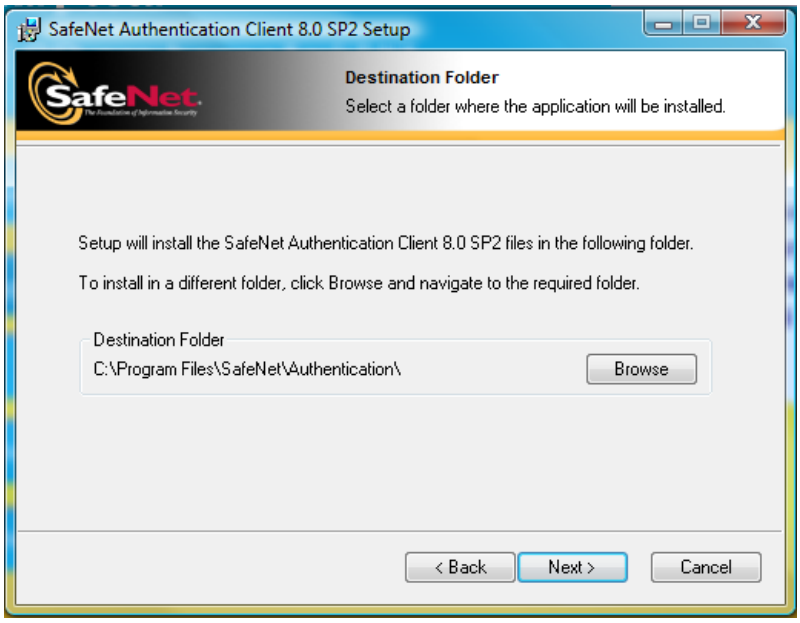
Standard – pro typickou instalaci podpory iKey a dalších autentizačních zařízení firmy SafeNet.

BSec-compatible – v případě nutnosti zachování předchozích implementací tokenů iKey (tj. zejména, pokud používáte nadstavby – aplikace třetích stran, při jejichž vývoji bylo používáno BSec PKI SDK) **Tedy tento typ instalace je třeba zvolit v případě použití aplikací Klíčníka, zejména pokud budete využívat generování klíčů v samotném programu Klíčník.**



Pro další krok stiskněte **tlačítko** **Next**.

Instalace bude zahájena po výběru místa uložení:



Pro další krok stiskněte **tlačítko** **Next**.

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

Po dokončení instalace je doporučeno restartovat počítač. Ukončete všechny aplikace a restartujte počítač.

Pozn.: U SAC se vytváření vlastních balíčků s firemní politikou liší od předchozího middlewaru BSec PKI. Funkcionalita SAC, je závislá na hodnotách definovaných v registrech. Po instalaci SW SAC je možné ovlivnit vlastnosti chování SW pomocí konfigurace klíčů v jedné z níže uvedených větví registrů. Uplný seznam klíčů a jejich vlastnosti naleznete v „SAC_Admin_Guide_Windows_8.0_SP2_Rev_A.pdf“ str 99:

Chování SW se řídí následující prohledáváním hierarchie registrů:

- HKEY_CURRENT_USER\SOFTWARE\Policies\SafeNet\Authentication\SAC
  Vyžaduje administrátorské oprávnění.
- HKEY_CURRENT_USER\SOFTWARE\Policies\SafeNet\Authentication\SAC
  Vyžaduje administrátorské oprávnění
- HKEY_CURRENT_USER\SOFTWARE\SafeNet\Authentication\SAC
  Neyžaduje administrátorské oprávnění
- KEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC
  Neyžaduje administrátorské oprávnění
- Pokud není klíč uveden, chování SAC se řídí defaultním nastavením SW

Konfiguraci SW pomocí editace registrů je možné provést :

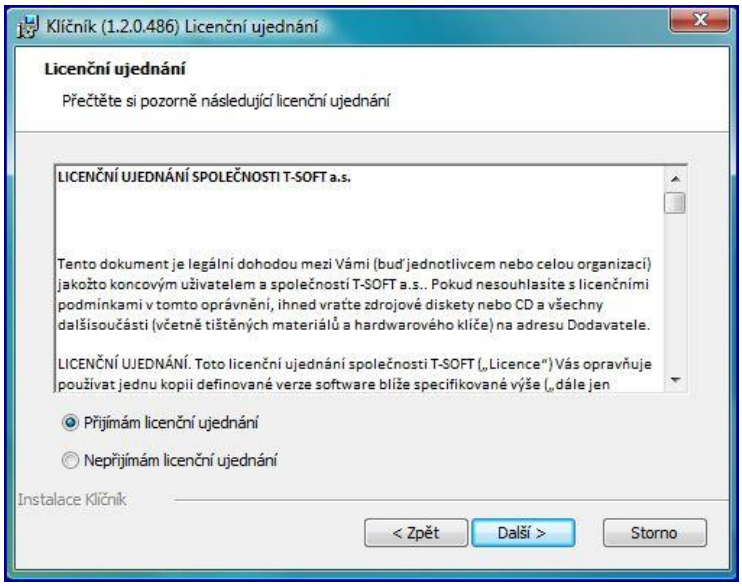
- Pomocí SafeNet Authentication Client Tools, které mohou konfigurovat pouze část registrů a hodnoty se zapisují do HKEY_CURRENT_USER.
- Pomocí Administrativních šablon (ADM/ADMX), pokud využijeme Group Policy Active Directory pro zprávu SW. Postup aktivace naleznete v Kapitole 7 „SafeNet Authentication Client Settings“ Administrativní příručky.
- Manuální Editací registrů. Pro manuální editaci se doporučuje Editovat registry ve větvi „KEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC“. Seznam klíčů a jejich hodnot naleznete v Administrativní příručce na str. 90 a vyšší.

2.3.3. Instalace personifikační utility Klíčník

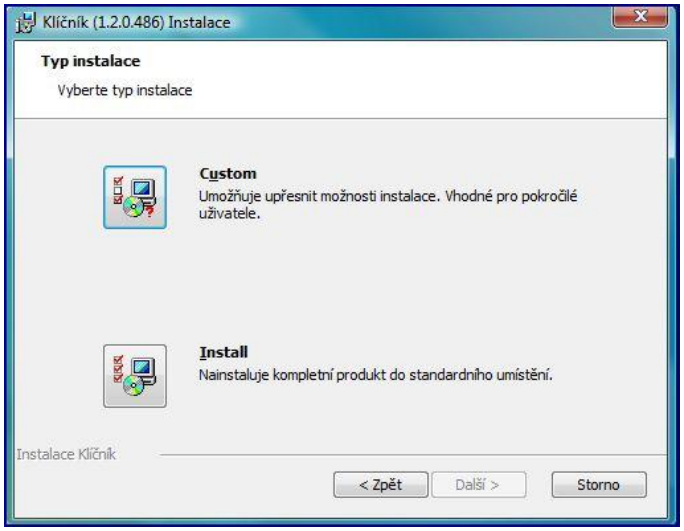
Vložte do mechaniky instalační CD **Bezpeční klíč**. Na hlavním menu instalačního CD zvolte odkaz "Instalace programů" a následně "Klíčník".

Průběh instalace:

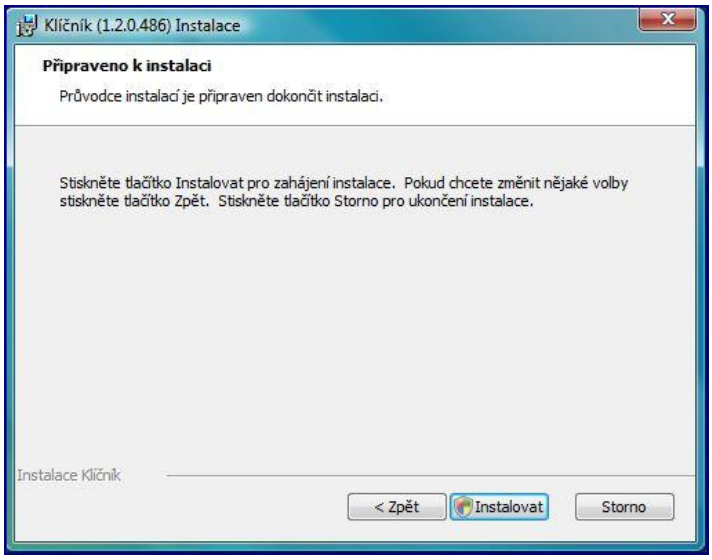
Pro další krok stiskněte **tlačítko Další**.



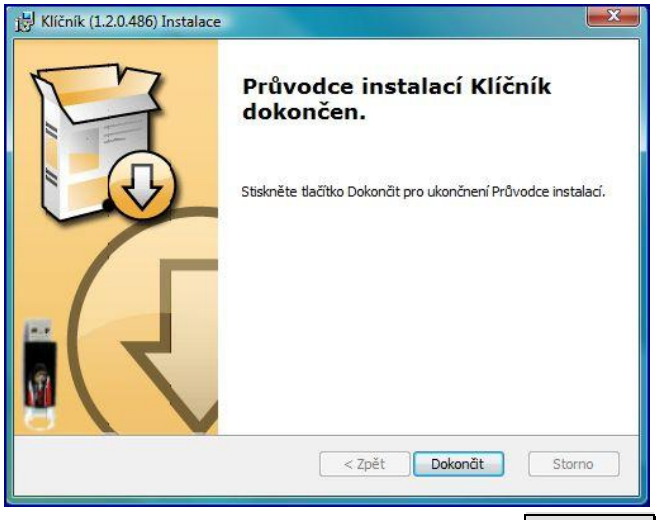
Pro další krok stiskněte **tlačítko Další**.



Pro další krok stiskněte **tlačítko** **Install**.



Instalaci zahájíte stiskem tlačítka **Instalovat**.

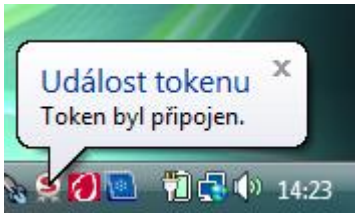


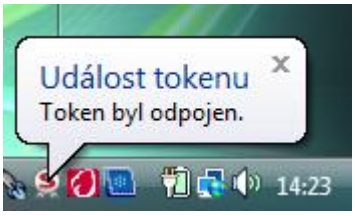
Instalace byla dokončena, stiskněte tlačítko **Dokončit**.

2.3.4. Připojení USB tokenu

Po instalaci a následném restartu počítače se u hodin v oznamovací oblasti hlavního panelu zobrazí nová ikona oznamující přítomnost middlewaru SAC:

Po vložení USB tokenu iKey 4000 do volného USB portu je uživatel informován o připojení / odpojení tokenu v pravé dolní části displeje:





3. Inicializace USB tokenu

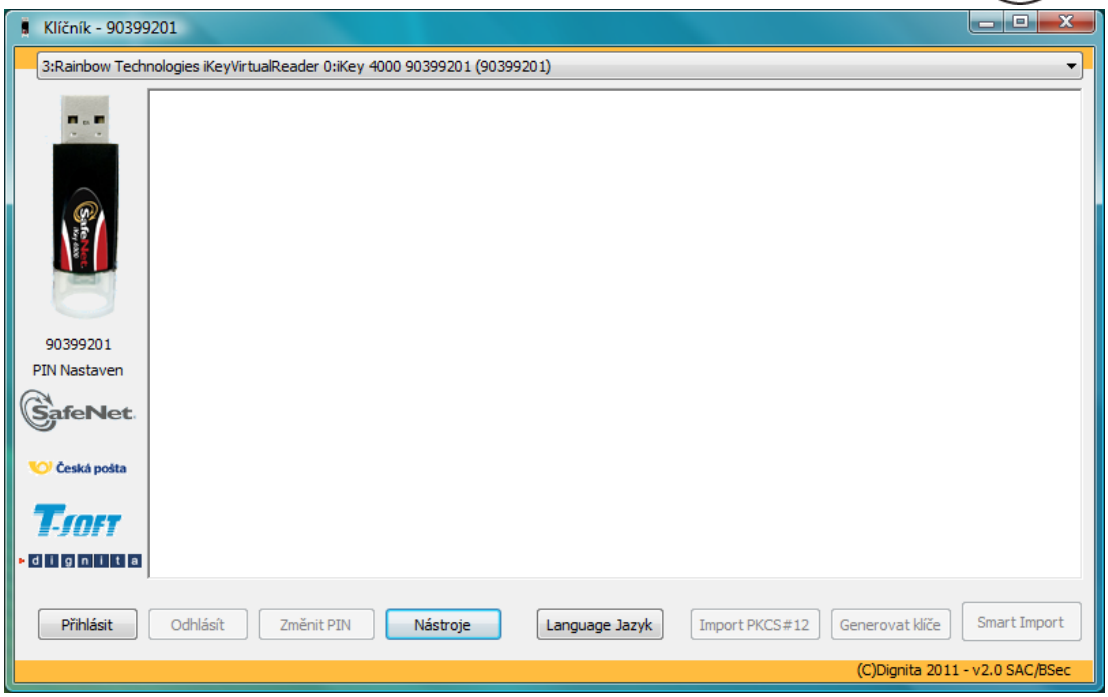
Inicializaci USB tokenu můžete provádět kdykoliv. Důrazně však upozorňujeme, že dochází ke ztrátě dat v USB tokenu při každé inicializaci. Pokud by na tokenu byly již uložené certifikáty a provedla se inicializace, budou certifikáty smazány. Kód PIN lze kdykoliv měnit (postup změny uveden v kapitole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

3.1. Spuštění aplikace

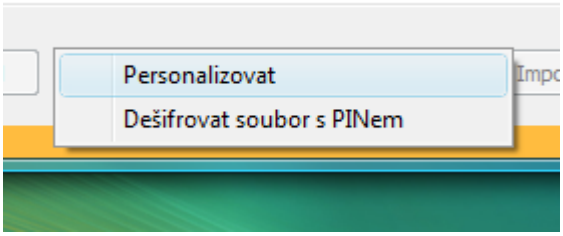
Inicializace tokenu se provádí pomocí programu Klíčník, který je součástí instalačního CD. Program spustíte prostřednictvím ikony na ploše anebo z nabídky *Start – Všechny programy – Klíčník*. Některé operace s Klíčníkem (jako např. Inicializace tokenu) je třeba provádět pod přihlášením k PS jako správce/administrátor.

3.2. Inicializace USB tokenu

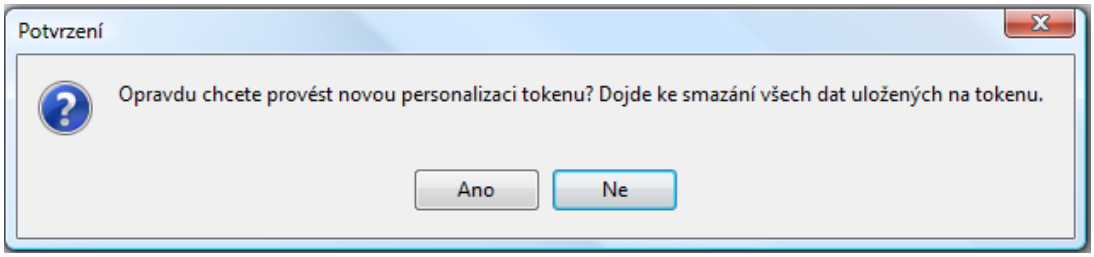
Vložte token do volného USB slotu. Po té spusťte aplikaci Klíčník. Na hlavní obrazovce aplikace –



vyhledejte tlačítko **Nástroje** a zvolte funkci **Personalizovat**:

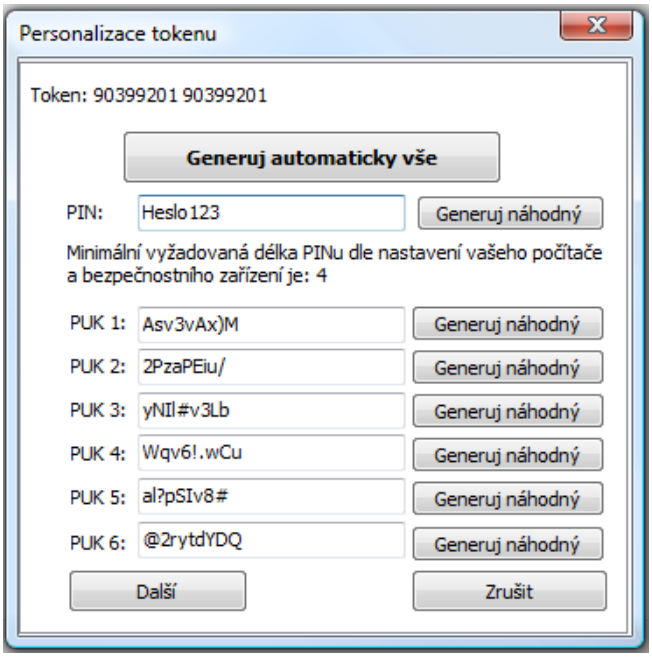


Potvrďte, zda chcete opravdu personalizovat Váš token (dochází k vymazání všech dat!):



Po té se Vám zobrazí obrazovka, kde si zvolíte PIN k tokenu a odblokovací PUK (až 6 odblokovacích PUKů):

V této fázi máte následující možnosti:



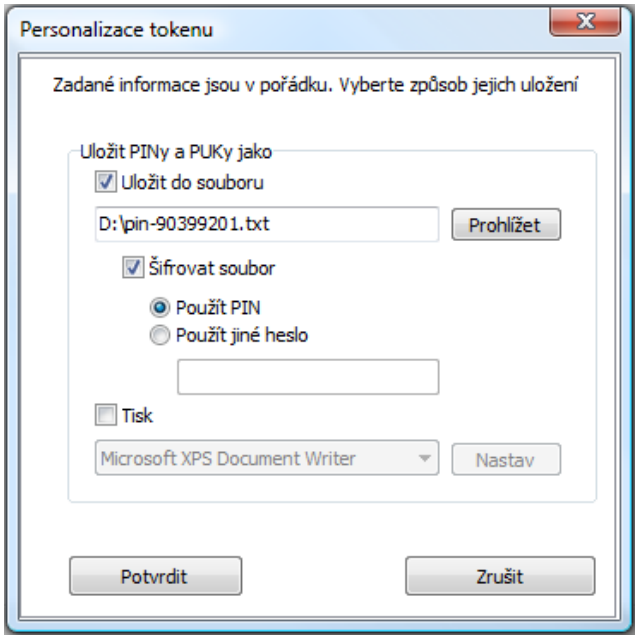
1/ vygenerovat PIN i PUKy pomocí tlačítka **Generuj** automaticky vše

2/ zadat do políčka vlastní PIN a vygenerovat až 6 náhodných PUKů

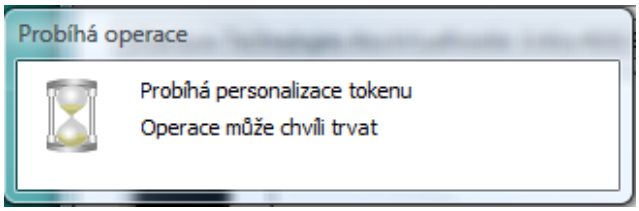
3/ zadat do příslušných políček PIN i PUK ručně

Zvolte jednu z možností generování a pokračujte stisknutím tlačítka **Další**.

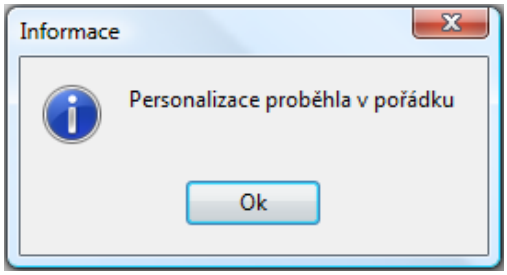
Na následující obrazovce máte možnost uložit PIN a PUK do souboru a vytisknout. Soubor je možné zašifrovat (přístup k souboru je chráněn PINem k tokenu nebo Vámi zvoleným heslem). Zašifrovaný soubor uložíte v PC na Vámi zvoleném místě, tlačítko **Prohlížet**.Tiskárnu, kterou chcete zvolit pro tisk PIN a PUK si rovněž můžete nastavit stisknutím tlačítka **Nastav**:



Pokračujte stisknutím tlačítka **Potvrdit**.



Do probíhající personalizace (trvá cca 20 sec) nijak nezasahujte a vyčkejte na zobrazení potvrzující úspěšnou operaci:



Pro dokončení stiskněte tlačítko **OK**.

Pozn.: Pokud budete chtít znovu nastavit odblokovací PUKy, bude nutné token znovu inicializovat!

4. Instalace certifikátů certifikačních autorit

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

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.

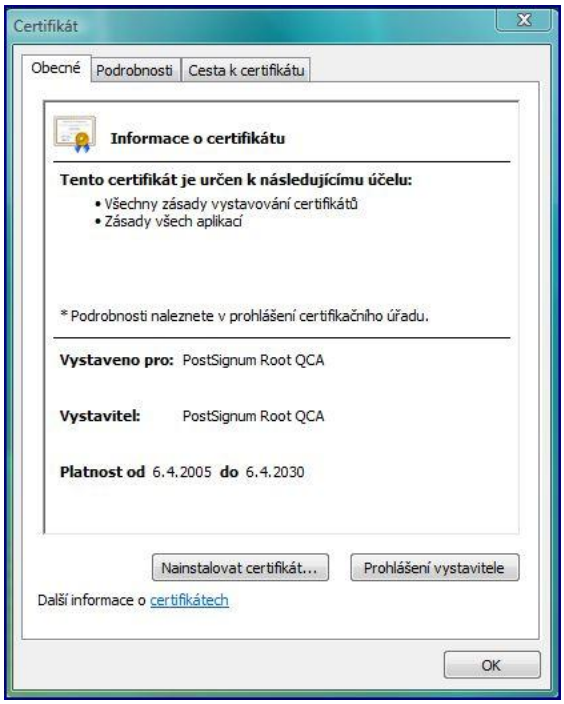
4.2. Ruční instalace certifikátů autorit

Následující postup proveďte postupně s každým ze souborů:

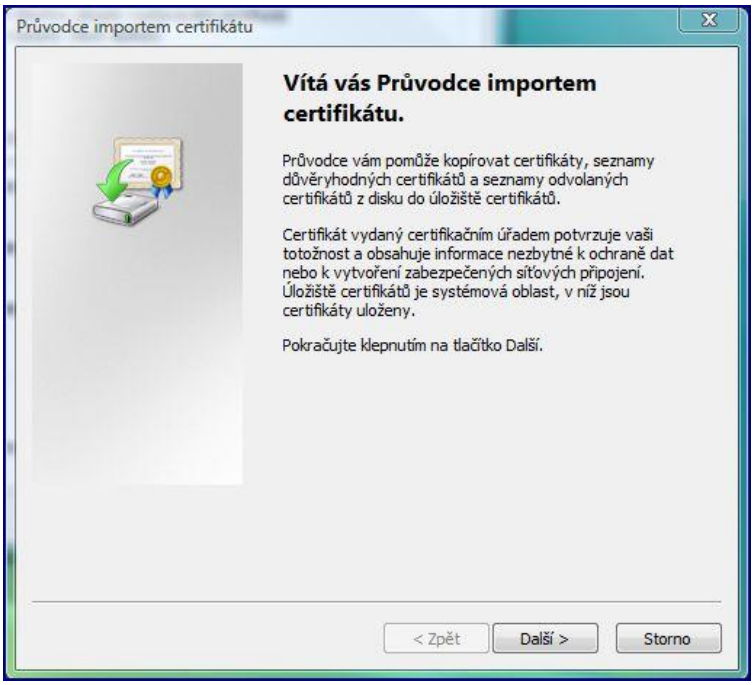
- **postsignum_qca2_root.cer** .. soubor s certifikátem kořenové autority
- **postsignum_qca2_sub.cer** .. soubor s certifikátem kvalifikované autority
- **postsignum_vca2_sub.cer** .. soubor s certifikátem komerční autority
- **postsignum_qca_root.cer** .. soubor s certifikátem kořenové autority
- **postsignum_qca_sub.cer** .. soubor s certifikátem kvalifikované autority
- **postsignum_vca_sub.cer** .. soubor s certifikátem komerční autority

(Postup je rovněž uveden na webové stránce.)

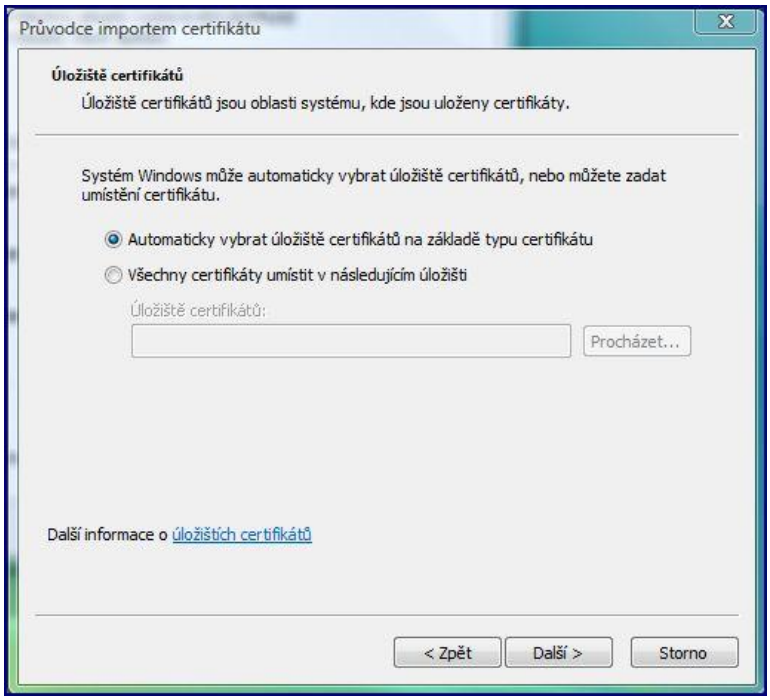
Klikněte myší na odkaz pro stažení souboru. Místo uložení souboru ale stiskněte tlačítko **Otevřít**. Po chvíli se zobrazí okno s informacemi o certifikátu.



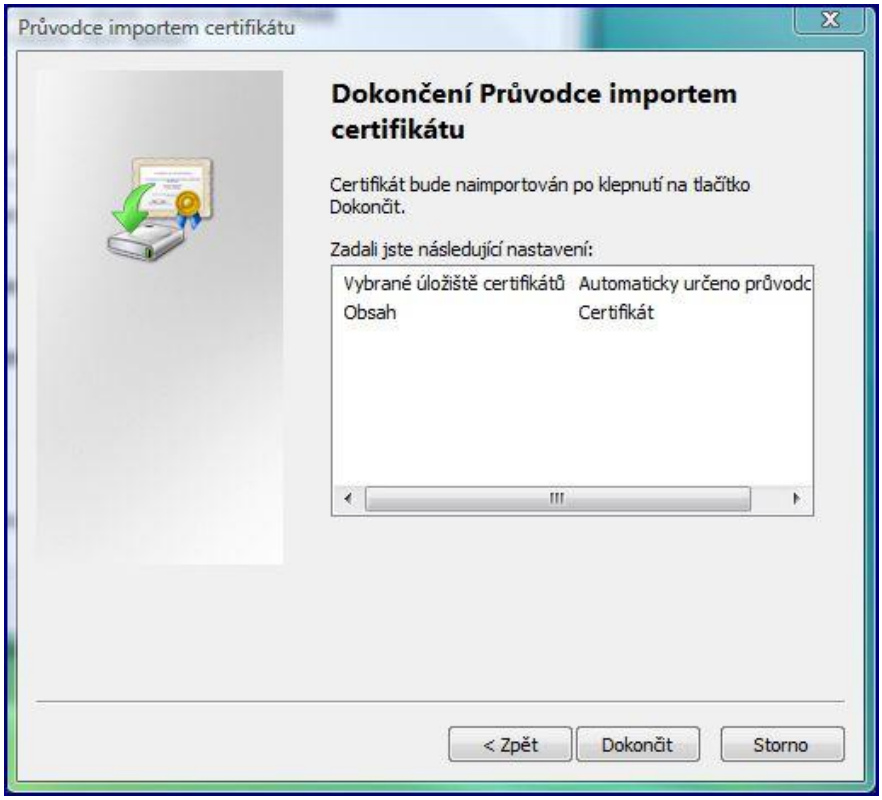
Stiskněte tlačítko **Nainstalovat certifikát.** Spustí se průvodce importem certifikátu. Stiskněte tlačítko **Další**.



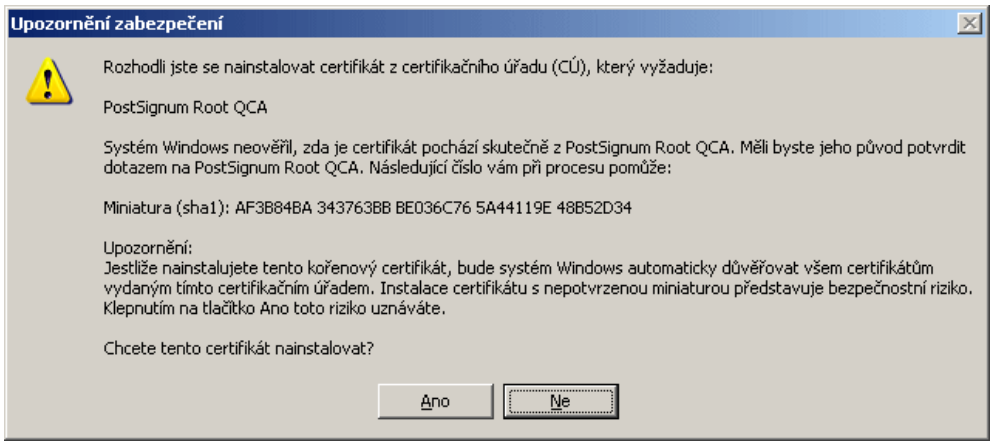
Na druhé obrazovce ponechte nastavenou položku **Automaticky vybrat úložiště certifikátů.** Stiskněte tlačítko **Další**.



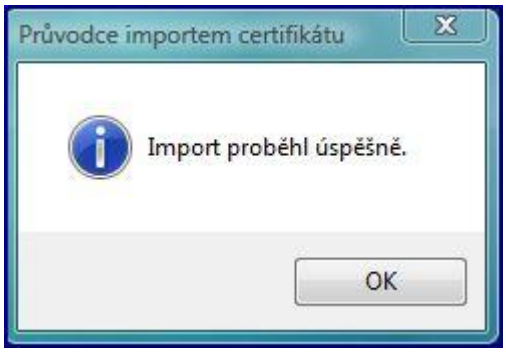
Potvrďte poslední obrazovku stisknutím tlačítka **Dokončit**.



Pokud instalujete certifikát ze souboru postsignum_qca_root.cer a postsignum_qca2_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.



4.3. Instalace certifikátů ve Windows Vista/7

Vzhledem ke zvýšeným bezpečnostním opatřením, není možné na OS Vista/7 nainstalovat odpovídající certifikáty pod běžným uživatelským účtem. Tyto certifikáty je třeba při instalaci umístit do specifického umístění, které pro běžného uživatele není dostupné. Pro instalaci těchto certifikátů do systému je třeba provézt následující kroky:

Odhlaste běžného uživatele a přihlaste se k danému počítači pod účtem s právy administrátora systému.

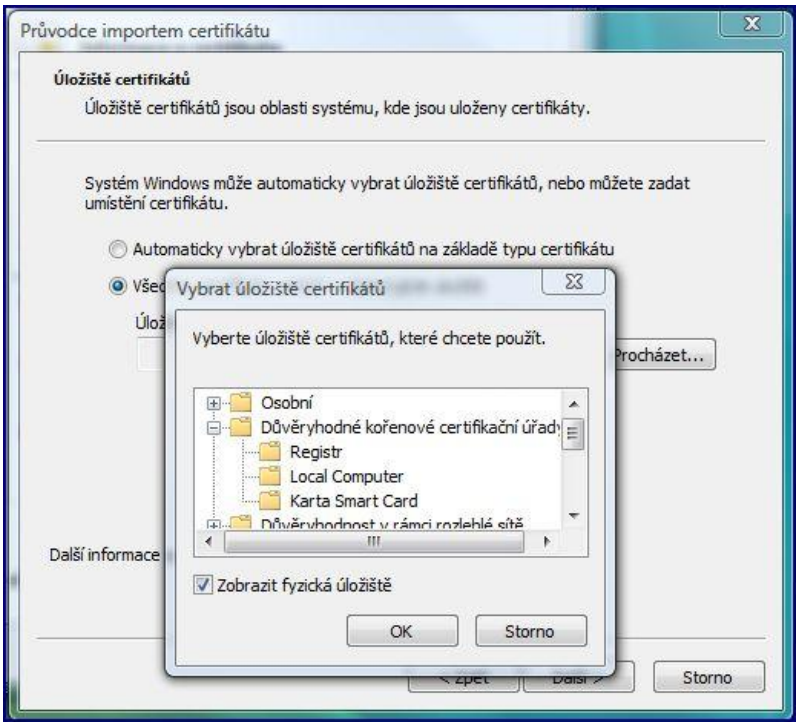
Ze základní webové stránky si stáhněte certifikáty kořenové a podřízené autority:

- **postsignum_qca2_root.cer** .. soubor s certifikátem kořenové autority
- **postsignum_qca2_sub.cer** .. soubor s certifikátem kvalifikované autority
- **postsignum_vca2_sub.cer** .. soubor s certifikátem komerční autority
- **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

Vypněte nástroj UAC administrátorského účtu (Ovládací panely – Uživatelské účty – účet s právy administrátora – zapnout nebo vypnout nástroj Řízení uživatelských účtů – k odebrání volby k zabezpečení počítače použijte nástroj Řízení uživatelských účtů - UAC).

Další postup je následující:

- V okně **Průvodce importem certifikátů** nastavte přepínač na položku **Všechny certifikáty umístit v následujícím úložišti.**
- Stiskněte tlačítko **Procházet**.
- V dialogu **Vybrat úložiště certifikátů** zaškrtněte políčko **Zobrazit fyzická úložiště**.
- Při instalaci souborů **postsignum_qca_root.cer** a **postsignum_qca2_root.cer** klepněte v seznamu úložišť na položku **Důvěryhodné kořenové certifikační úřady**.
- Při instalaci ostatních souborů klepněte v seznamu úložišť na položku **Zprostředkující kořenové certifikační úřady.**
- V rozvinuté podstruktuře klepněte na položku **Local Computer** a stiskněte tlačítko **OK**.



Dokončete instalaci certifikátu a stejným způsobem instalujte i ostatní certifikáty. Nakonec odhlaste uživatele s právy administrátora a přihlaste zpět výchozího uživatele.

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.

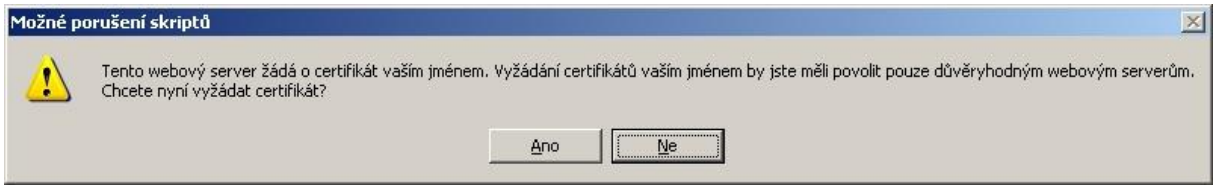
5.2. Generování klíčů a žádosti o certifikát

5.2.1. On-line generování klíčů a žádosti o certifikát

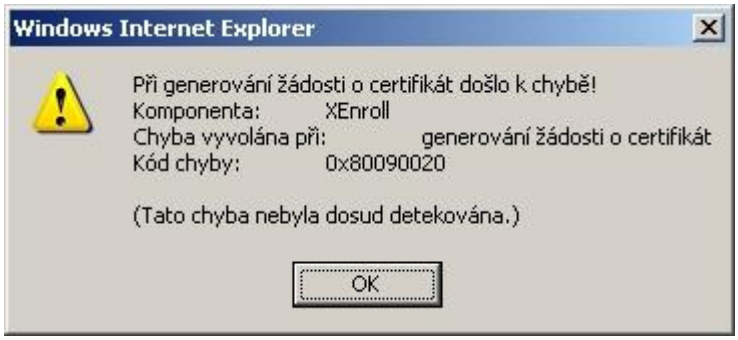
Na základní webové stránce klikněte na odkaz v části **5.1. Generování klíčů a žádosti o certifikát / On-line generování žádosti o certifikát.**

Doplňte všechny potřebné údaje pro vytvoření žádostí o certifikát a stiskněte tlačítko Vygenerovat a uložit žádost o certifikát do souboru nebo na www server PostSignum.

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 PIN**.

Po zadání PINu dojde k vygenerování klíčů a žádosti o certifikát. Do operace generování klíčů nijak nezasahujte a neodpojujte samotný token, mohlo by dojít k jeho zničení. Samotná operace může trvat několik minut.

Poznámka pro uživatele Windows Vista:

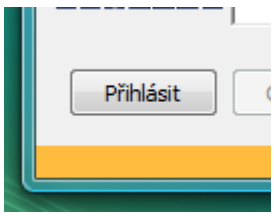
Uživatelé Windows Vista musí zařadit webový server PostSignum mezi důvěryhodné servery.
Dále je potřeba pro zónu Důvěryhodných serverů nastavit následující položce hodnotu Povolit nebo Dotázat se:
Ovládací prvky ActiveX inicializace a skriptu nejsou označeny jako bezpečné pro skriptování.

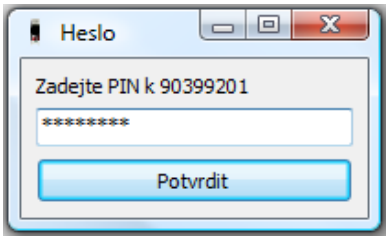
Jako alternativu pro generování klíčů můžete použít program **Klíčník**.

Pro vystavení certifikátu je nutné se dostavit na pobočku České pošty se službou Czech POINT. Detailní informace k návštěvě pobočky České pošty se službou Czech POINT naleznete na stránkách www.bezpecnyklic.cz

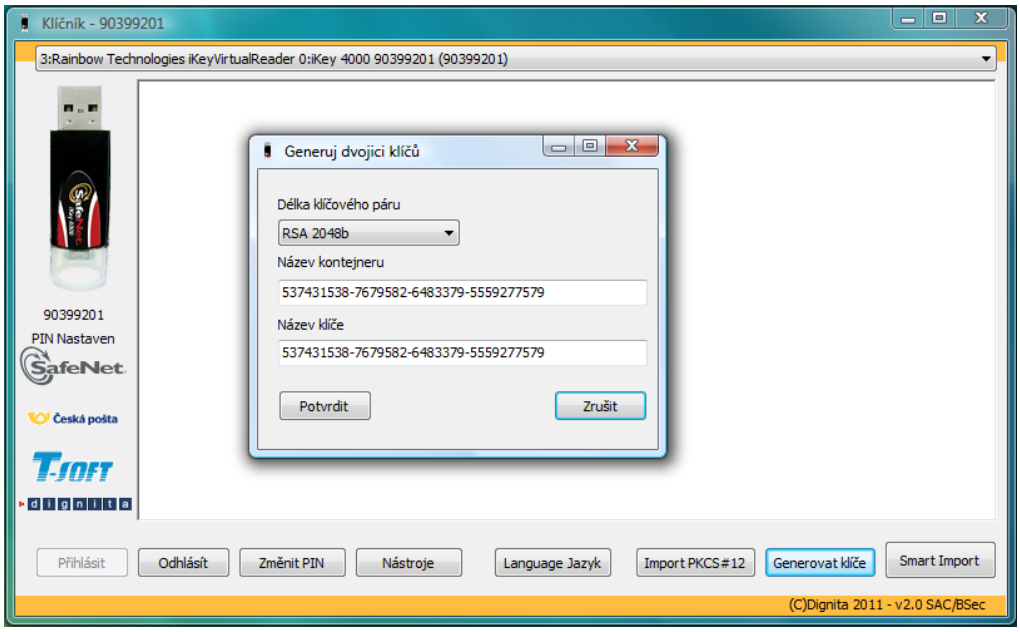
5.2.2. Generování klíčů a žádosti o certifikát pomocí programu Klíčník

- Spusťte aplikaci Klíčník na svém PC.
- Vložte token do USB slotu (token musí být již zinicializovaný viz kapitola 3 tohoto dokumentu).
- V aplikaci Klíčník proveďte přihlášení k tokenu:

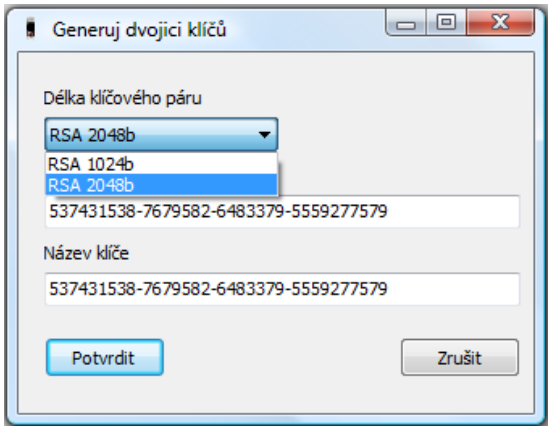




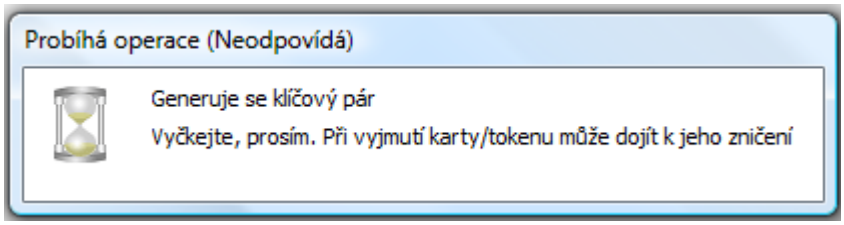
Na hlavním panelu aplikace Klíčník zvolte tlačítko **Generovat klíče**.



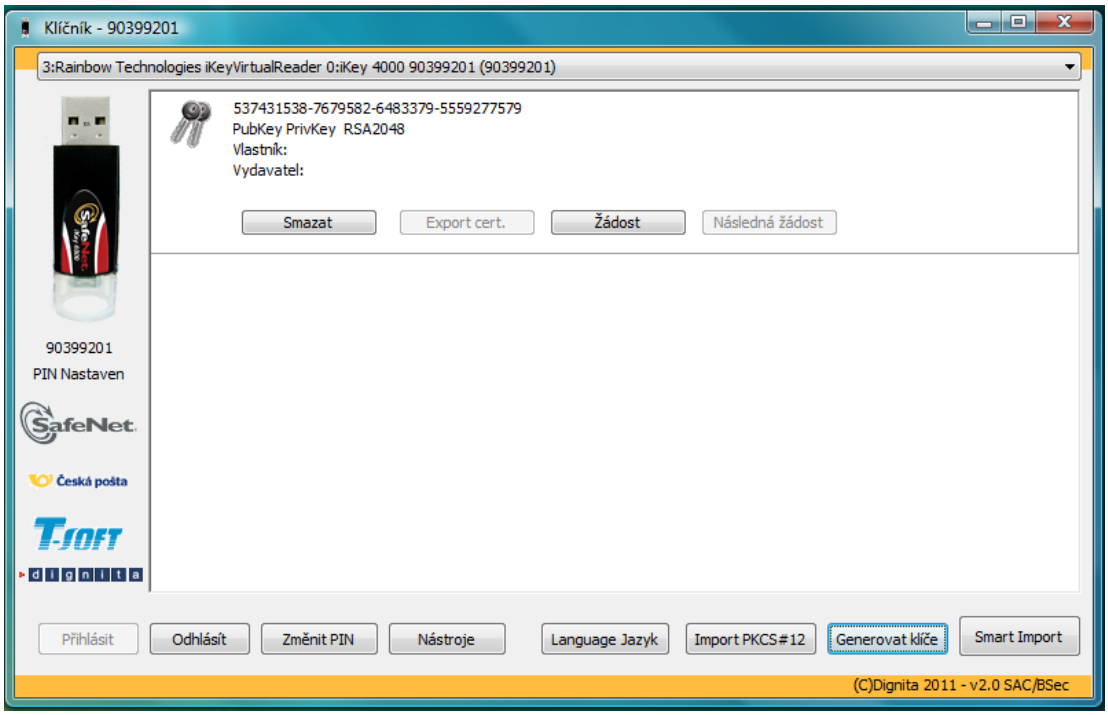
Zvolte délku klíčů (standardní velikost je 2048 bitů, pro vydání komerčního certifikátu lze nastavit velikost klíče 1024) a klikněte na tlačítko **Potvrdit**:



Do operace generování klíčů nijak nezasahujte a neodpojujte samotný token, mohlo by dojít k jeho zničení. Samotná operace může trvat několik minut.

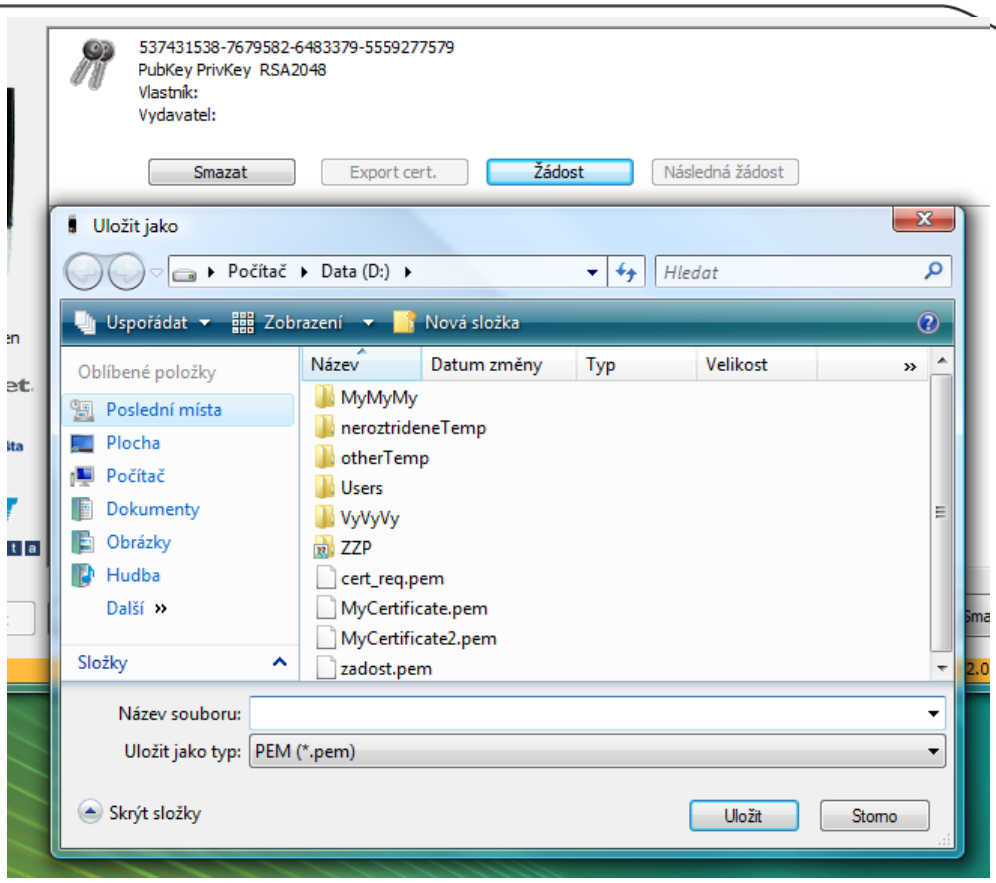


Vygenerovaný klíč se zobrazí na hlavní obrazovce aplikace Klíčník:

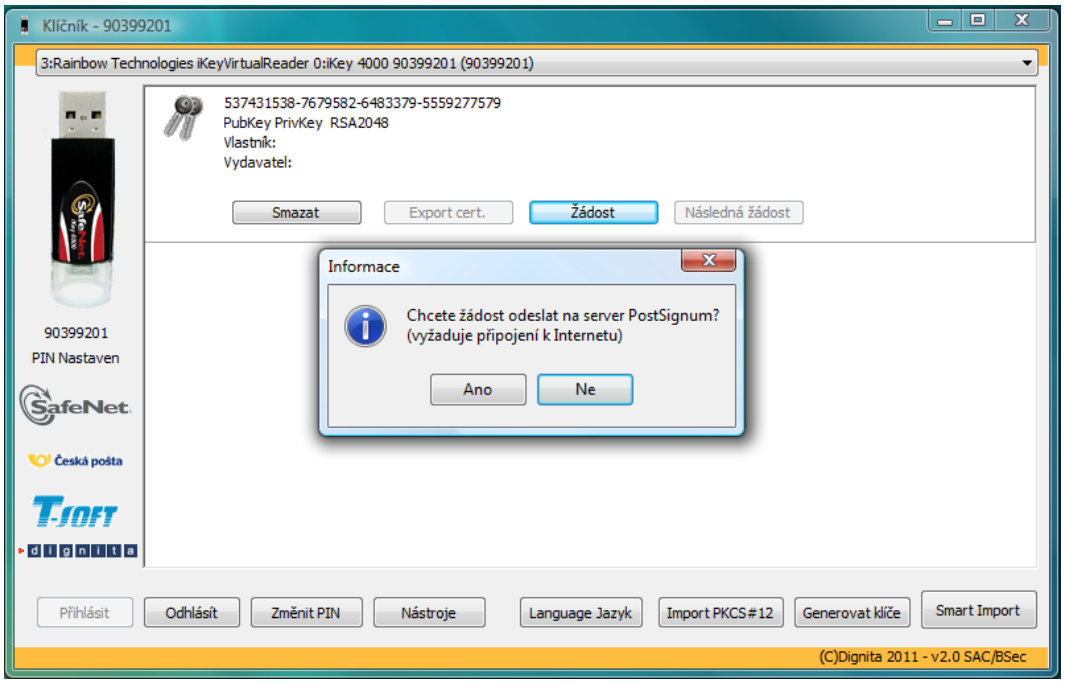


Pomocí tlačítka **Žádost** je možno vygenerovat žádost o certifikát dle normy PKCS#10. Na základě této žádosti pak certifikační autorita vystaví vlastní certifikát. Běžnou praxí je, že uživatel vygeneruje dvojici klíčů na tokenu, vystaví si žádost o certifikát (tato je podepsána privátním klíčem), požádá certifikační autoritu o vydání certifikátu a tento potom do kontejneru naimportuje.

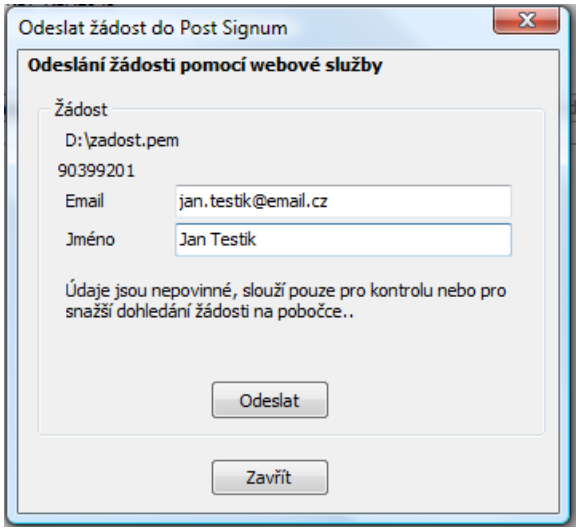
K vygenerování žádosti je potřeba být k tokenu přihlášen jako vlastník, protože žádost se podepisuje privátním klíčem. Vystavená žádost pak ale obsahuje pouze veřejný klíč, takže ani certifikační autorita nezná privátní klíč. Podpis žádosti je pak pro certifikační autoritu důkazem toho, že žadatel má k privátnímu klíči přístup.



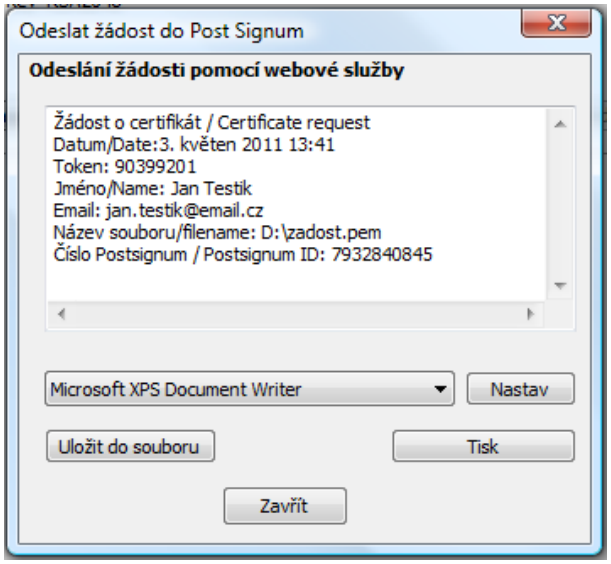
Aplikace Klíčník umožňuje vygenerovanou žádost rovnou odeslat na server PostSignum (tato akce vyžaduje připojení k internetu):



Pokud uživatel zvolí odeslání, bude vyzván k zadání jména a emailu. Tyto informace jsou nepovinné, ale mohou pomocí při vyhledání žádosti na pobočce České pošty se službou Czech POINT.



Po stisku tlačítka **Odeslat** dojde k odeslání žádosti na server Post Signum. Pokud vše proběhne bezchybně, aplikace Klíčník zobrazí okno s výsledkem operace. Zde je důležitý desetimístný kód, podle kterého se na pobočce žádost dohledává. Informace je možné vytisknout nebo uložit na disk.



Pro vystavení certifikátu je nutné se dostavit na pobočku České pošty se službou Czech POINT. Detailní informace k návštěvě pobočky České pošty se službou Czech POINT naleznete na stránkách www.bezpecnyklic.cz

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 5**.3. Instalace vydaného certifikátu**.
Na zobrazené stránce si můžete vybrat způsob načtení vašeho vydaného certifikátu.

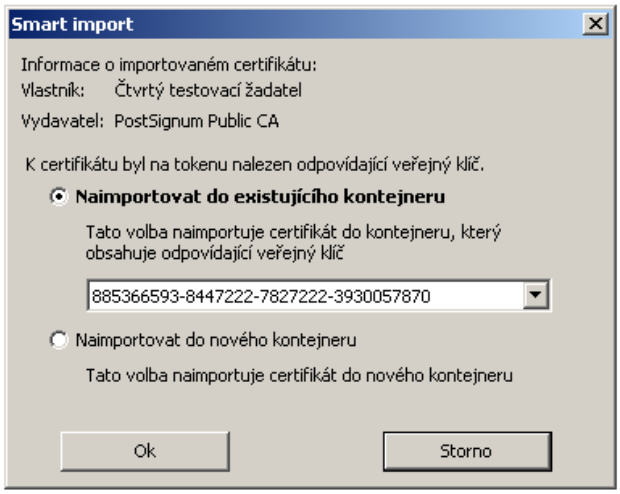
- Stažení z webu podle sériového čísla – vyplňte sériové číslo certifikátu, které naleznete na protokolu o vydání certifikátu. Tento dokument obdržíte na pracovišti České pošty při vydání certifikátu nebo je nabídnut ke stažení při přijmutí vydaného certifikátu na www stránkách www.postsignum.cz.
- Načtení 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 PIN**.

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

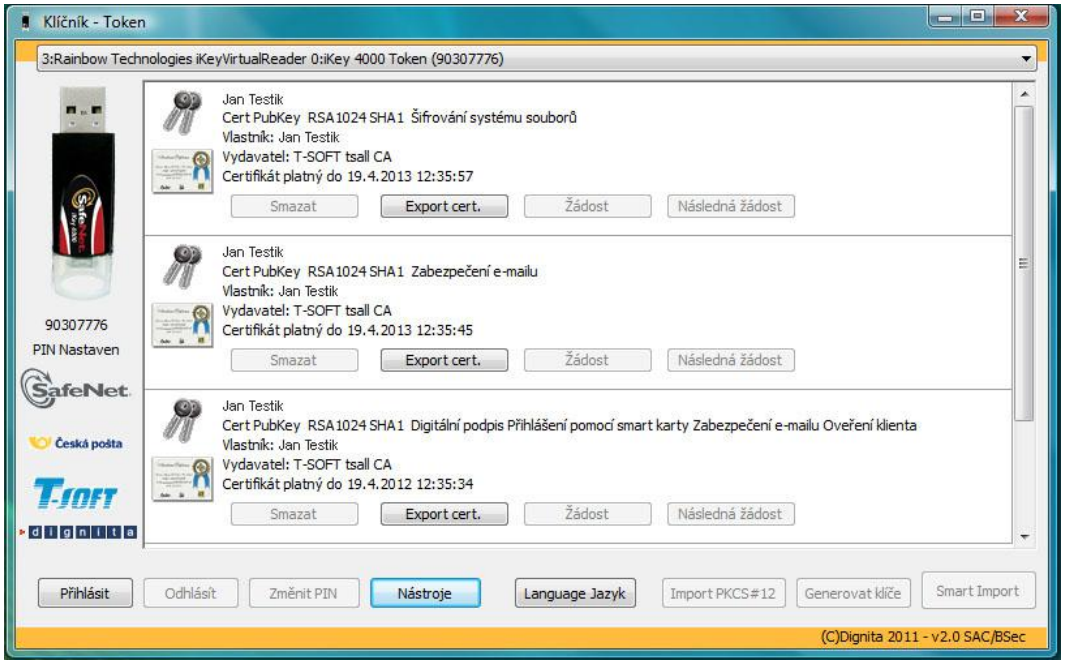
Jako alternativu pro import vydaného certifikátu můžete použít program **Klíčník**. Po spuštění aplikace a přihlášení k tokenu zvolením tlačítka **Smart import**:



6. Operace s USB tokenem

6.1. Spuštění aplikace

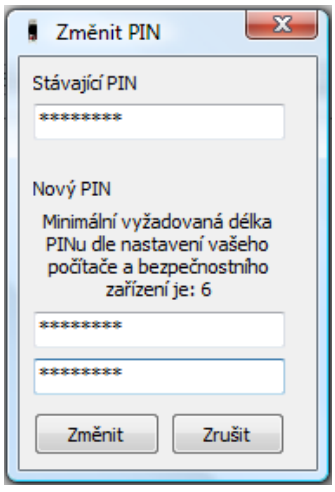
Pomocí zástupce na ploše nebo v nabídce Start (Programy→Klíčník) spusťte aplikaci **Klíčník**. Po té vložte token do USB portu a pomocí tlačítka **Přihlásit** se přihlaste ke svému tokenu.



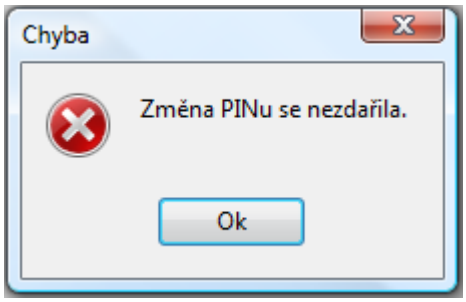
Na hlavní obrazovce vidíte přehled všech Vašich certifikátů. Informace o práci s certifikáty a další funkcionality, které nabízí SW Klíčník, naleznete v dokumentaci k této utilitě. Dokumentace je součástí této instalace. V následujících kapitolách popíšeme jen základní funkce podporující práci s USB tokenem iKey.

6.2. Změna PIN

V nabídce v dolní části aplikace klikněte na tlačítko **Změnit PIN**.

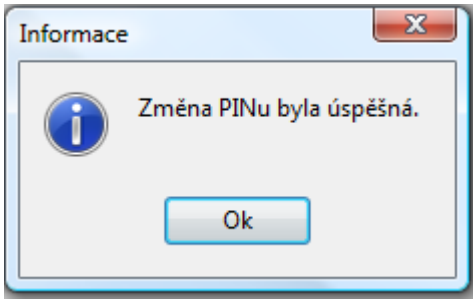


Vyplňte stávající PIN a doplňte 2x nový PIN.



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

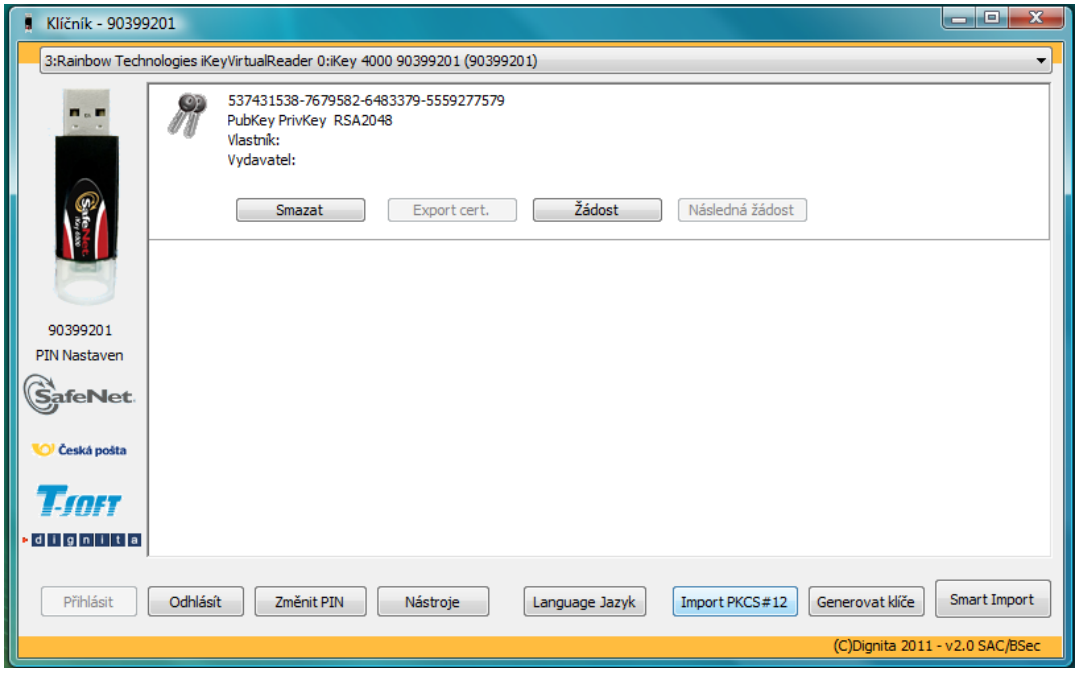
Parametry nového PINu musí odpovídat nastavení na tokenu nebo aplikace Safenet Authentication Client.



Pro dokončení stiskněte tlačítko **OK**

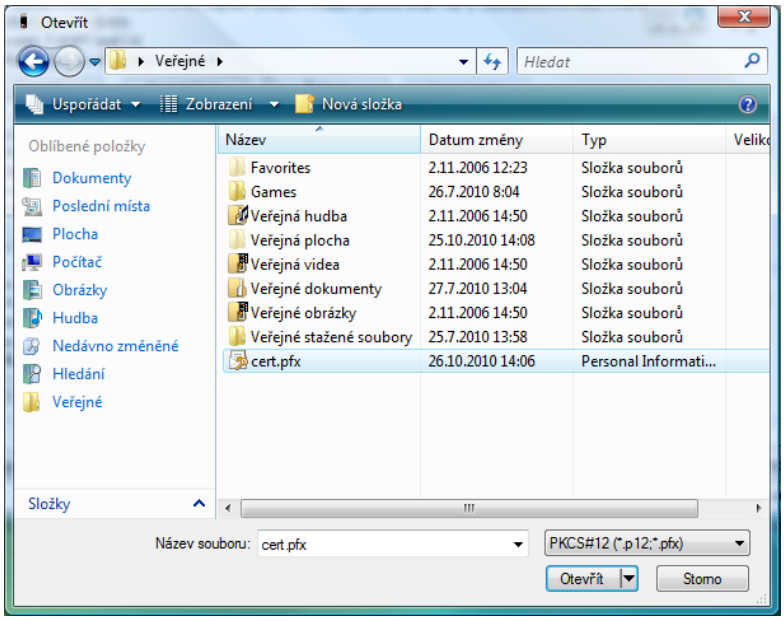
6.3. Import PKCS#12 souboru

Do tokenu je možno vložit balíček podle normy PKCS#12. Ten většinou obsahuje dvojici klíčů a související certifikát. Balíček je většinou chráněn heslem.

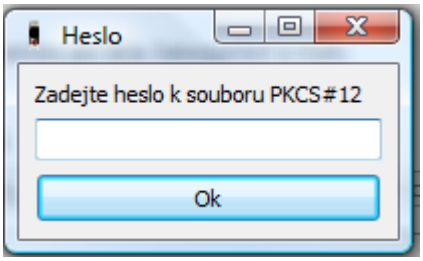


V nabídce v dolní části aplikace klikněte na tlačítko **Import PKCS#12**.

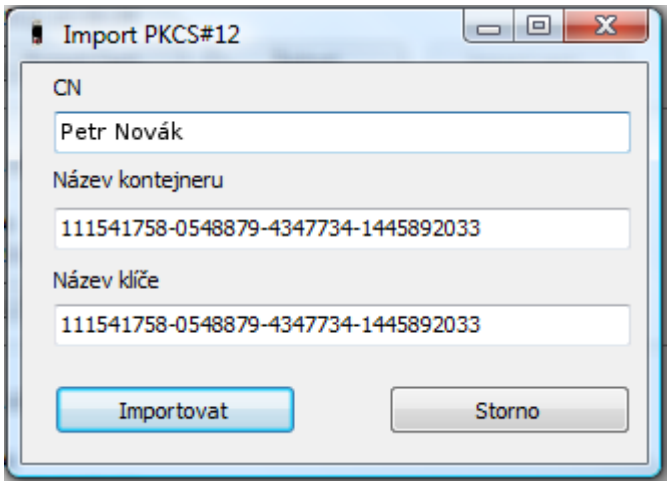
Po vložení PINu a stisku tlačítka **OK** se zobrazí okno pro vyhledání souboru se zálohou certifikátu.



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 s názvem certifikátu a názvem klíče.



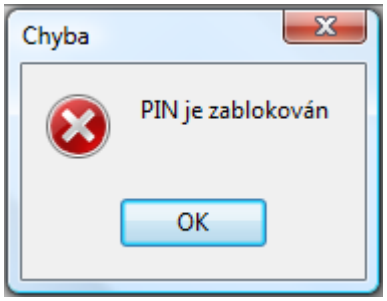
Po stisknutí tlačítka **Importovat** se obsah souboru PKCS#12 nahraje do USB tokenu. Importovaný certifikát se zobrazí v seznamu certifikátů.

7. Odblokování USB tokenu

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 PIN**.

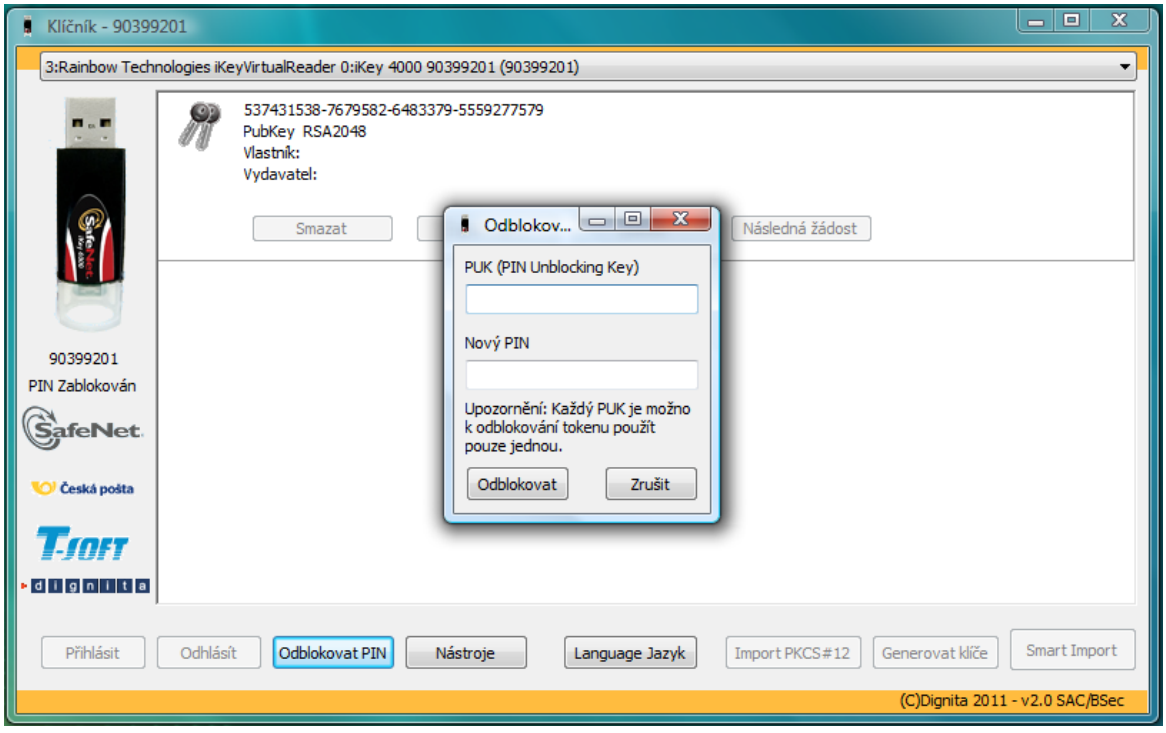
Při zablokování PINu může být zobrazena podobná chybová hláška.



7.2. Spuštění aplikace a odblokování tokenu

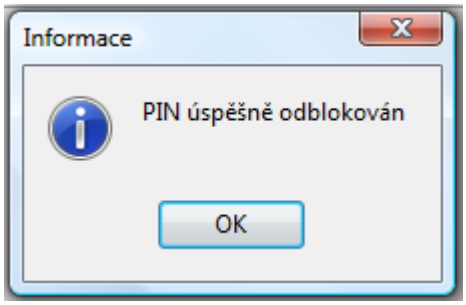
Pomocí zástupce na ploše nebo v nabídce Start (Programy→Klíčník) spusťte aplikaci **Klíčník**. Stiskněte tlačítko **Odblokovat PIN**.

Pro tuto operaci je nutné vložit token do volného USB portu.



Doplňte jeden z kódů PUK, který jste zadávali v kapitole **3.2 Inicializace USB tokenu**. Dále doplňte 2x nový PIN a stiskněte tlačítko **Odblokovat.**

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.