SOFTIDEA

Šifrovanie elektronickej pošty

Príručka administrátora

(AN101012)

December 2011

Obsah

Táto príručka popisuje implementáciu systému zabezpečenia poštovej komunikácie umožňujúceho šifrovať a digitálne podpisovať správy elektronickej pošty. Systém zabezpečenia využíva hardvérové kryptografické zariadenia ***GNT USB Token*** od spoločnosti ***SoftIdea*** a poštový klient ***Thunderbird***. Je tu popísaný proces vytvorenia siete dôvery založenej na koreňovej certifikačnej autorite pomocou programu ***XCA*** a generovanie certifikátov jednotlivým užívateľom. Samotné nastavenie poštového klienta je potrebné vykonať podľa príručky [***2***].

1 Systémové požiadavky

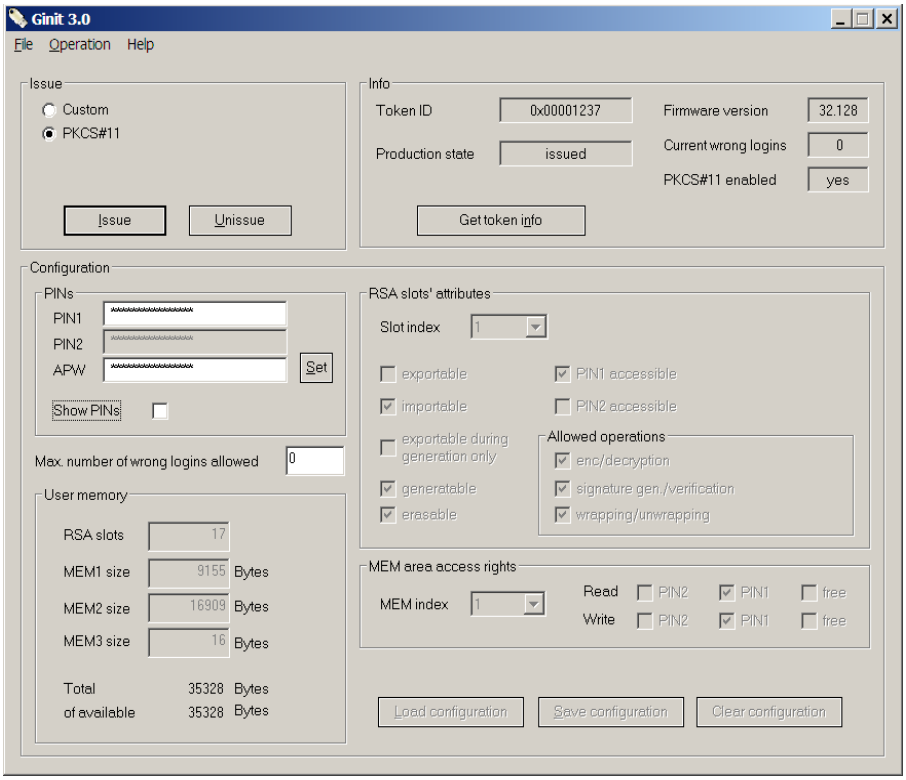
1. Operačný systém: Microsoft Windows XP, Vista, 7, 8.
2. Tokeny (zariadenia ***GNT USB Token***) účastníkov systému zabezpečenej poštovej komunikácie.
3. Nástroj pre správu certifikačnej autority ***XCA***. Podporovaná verzia programu ***XCA*** je súčasťou štandardnej inštalácie produktu ***GNT USB Token*** s podporou administrácie.
4. Nástroj pre administráciu ***Ginit***.
5. Bezpečnostný modul SIPKCS.

Implementáciu systému vykonajte na dobre zabezpečenom počítači ! Vylúčte prítomnosť škodlivých softvérov.

---

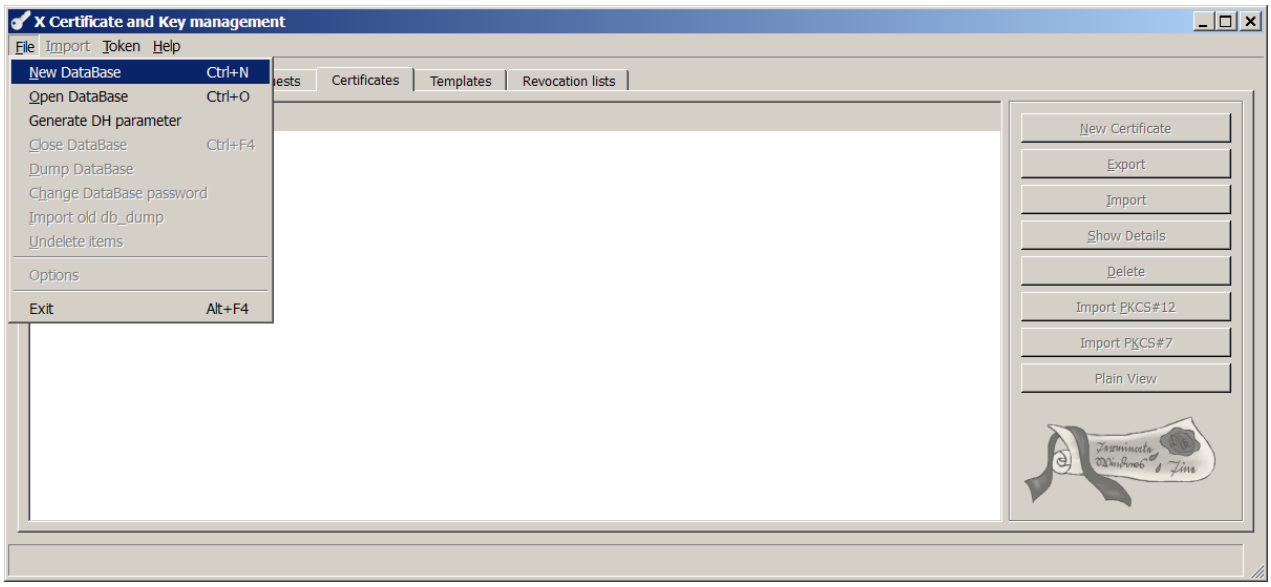
2 Inicializácia Tokenu

Pomocou nástroja ***Ginit*** inicializujte token užívateľa pre rozhranie SIPKCS. V poli PIN1 nastavte dočasné heslo účastníka.

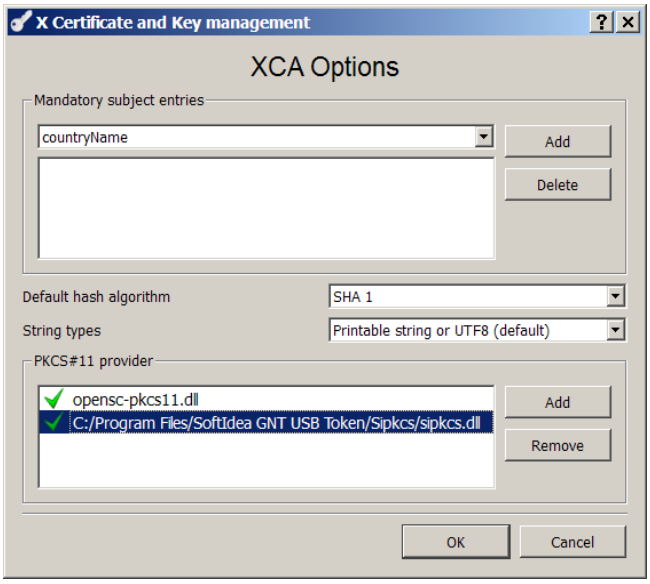


3 Nastavenie programu XCA

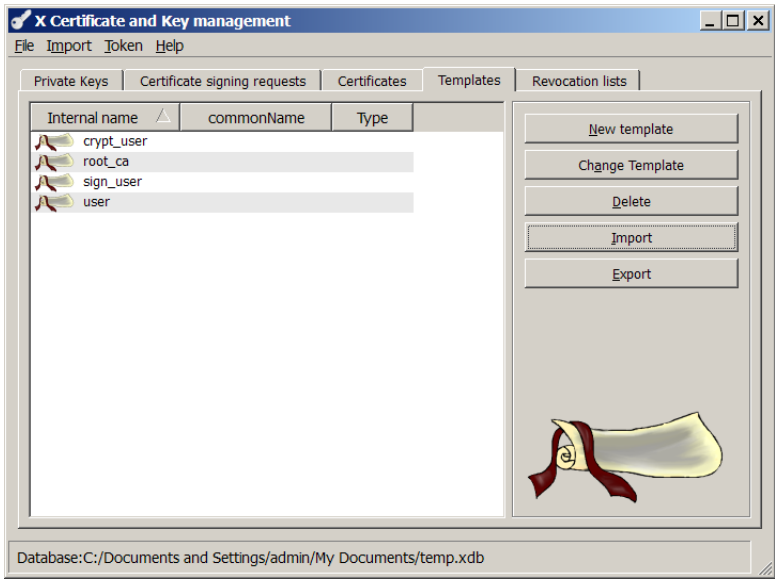
1. Otvorte program XCA a zvolte "File->New DataBase". Zvoľte meno súboru databázy a zadajte kryptograficky silné prístupové heslo k databáze.



2. Zvoľte "File->Options" a v okne "XCA Options" v časti "PKCS#11 provider" zvoľte tlačidlo "Add" a vložte cestu k modulu SIPKCS od spoločnosti *SoftIdea*.

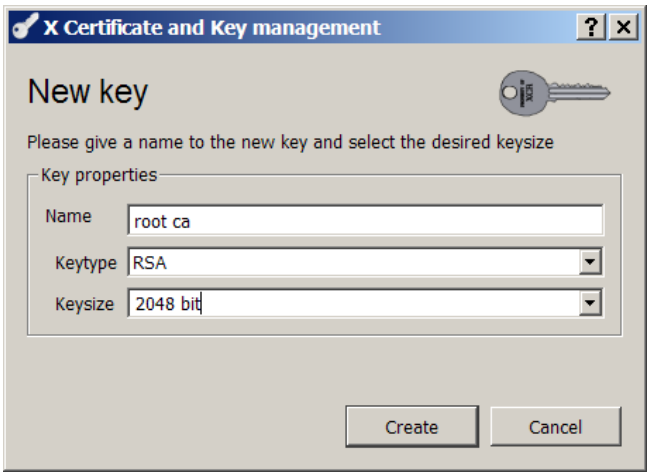


3. Zvoľte kartu "Templates" a s pomocou tlačidla "Import" importujte šablóny "user.xca", "crypt_user.xca", "root_ca.xca", "sign_user.xca". Šablóny sa nachádzajú v adresári XCA v inštalačnom adresári produktu GNT USB Token.



4 Vytvorenie kľúčového páru koreňovej certifikačnej autority

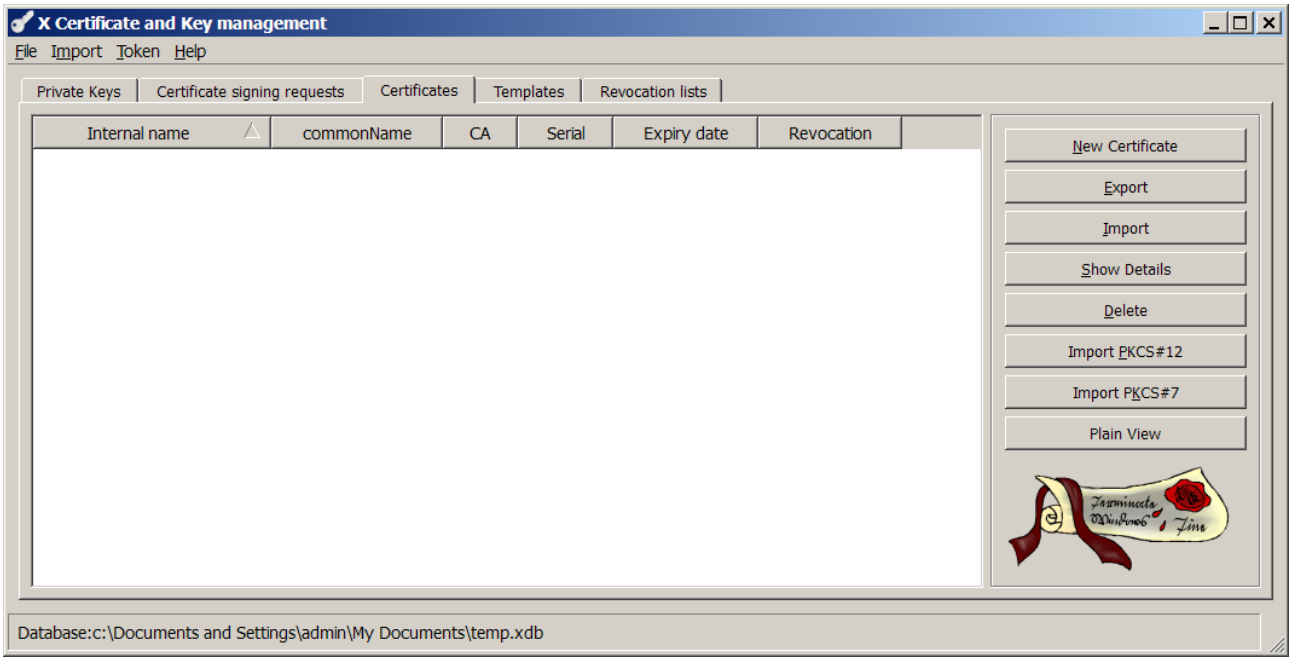
V hlavnom okne programu XCA zvoľte kartu "Private keys". Zvoľte tlačidlo "New Key". V okne "New Key" nastavte požadované údaje a stlačte tlačidlo "Create". V príklade na obrázku sme zvolili názov kľúčového páru certifikačnej autority "root ca".



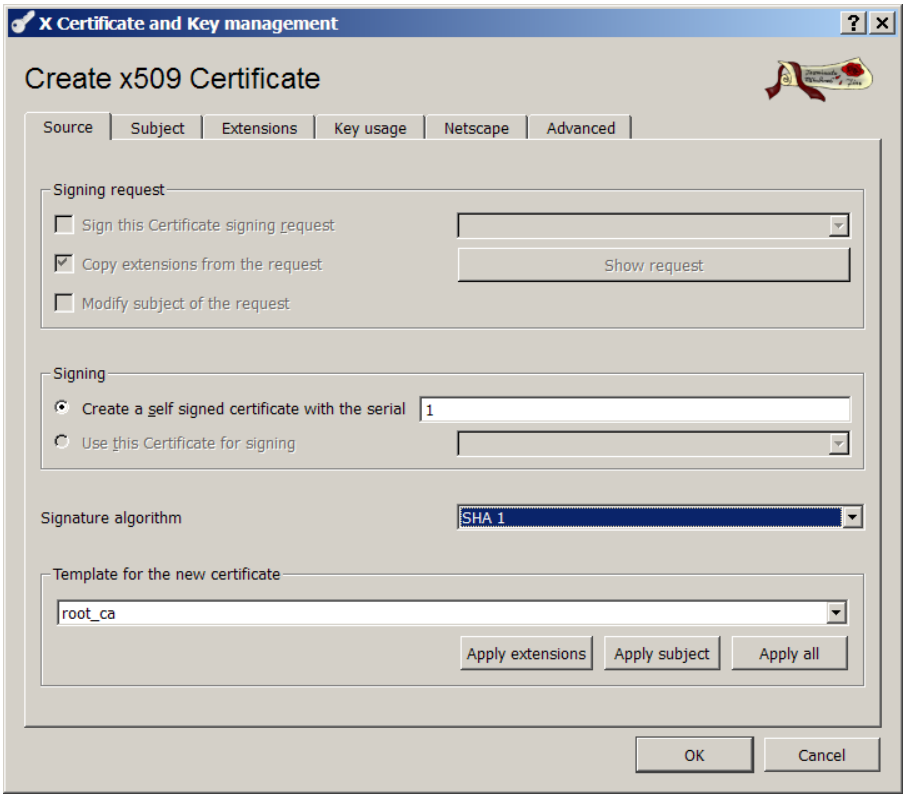
Bezpečné uloženie privátneho kľúča koreňovej certifikačnej autority je základným predpokladom bezpečnosti vytváraného systému. Postup uvedený v tomto dokumente predpokladá, že privátny kľúč koreňovej autority bude uložený v súbore databázy programu XCA vytvorenom v kapitole 3.

5 Vytvorenie certifikátu koreňovej certifikačnej autority

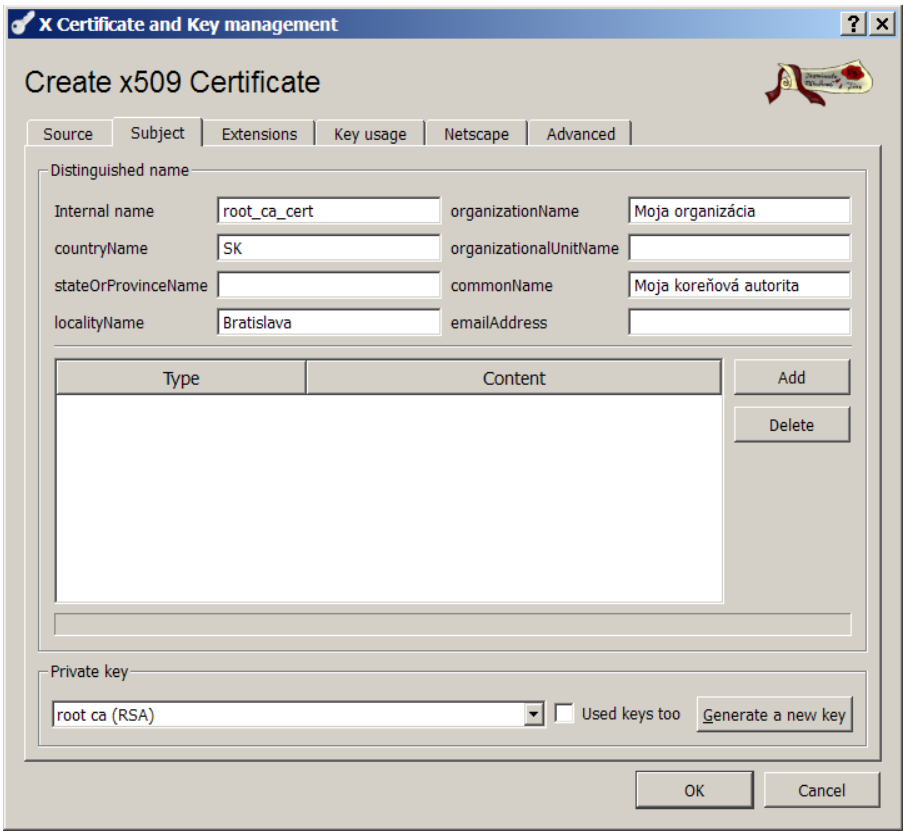
1. V karte "Certificates" zvoľte tlačidlo "New Certificate".



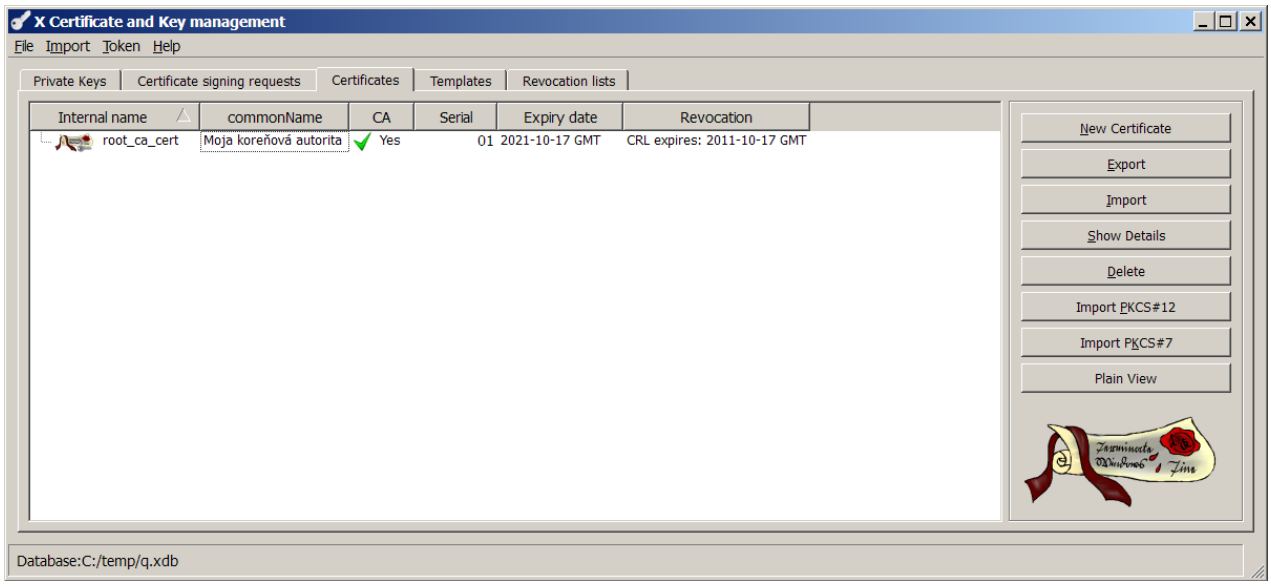
2. V karte "Source", v poli "Template for the new certificate" zvoľte šablónu "root_ca" a stlačte tlačidlo "Apply all". V poli "Signing" ponechajte zvolené "Create a self signed certificate...", môžete zvoliť sériové číslo certifikátu.



3. V karte "Subject" zvoľte privátny kľúč koreňovej certifikačnej autority a vyplňte polia podľa vzoru na nasledujúcom obrázku.

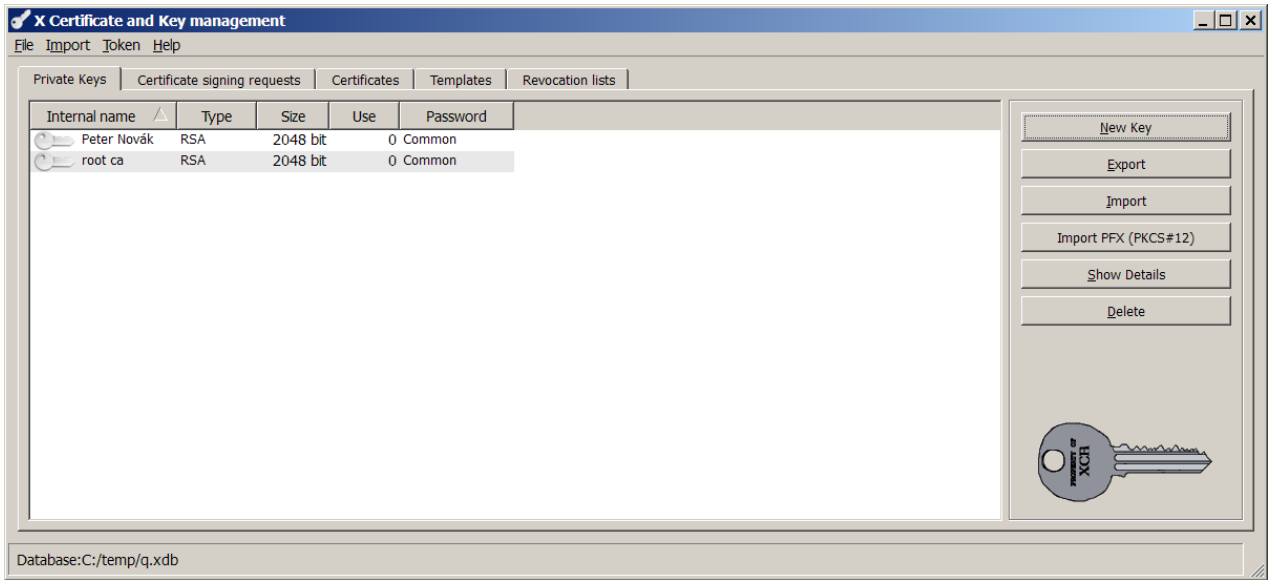


4. Stlačením tlačidla "OK" vygenerujte certifikát koreňovej certifikačnej autority. Certifikát bude zobrazený V karte "Certificates" hlavného okna aplikácie.



6 Vytvorenie kľúčového páru účastníka

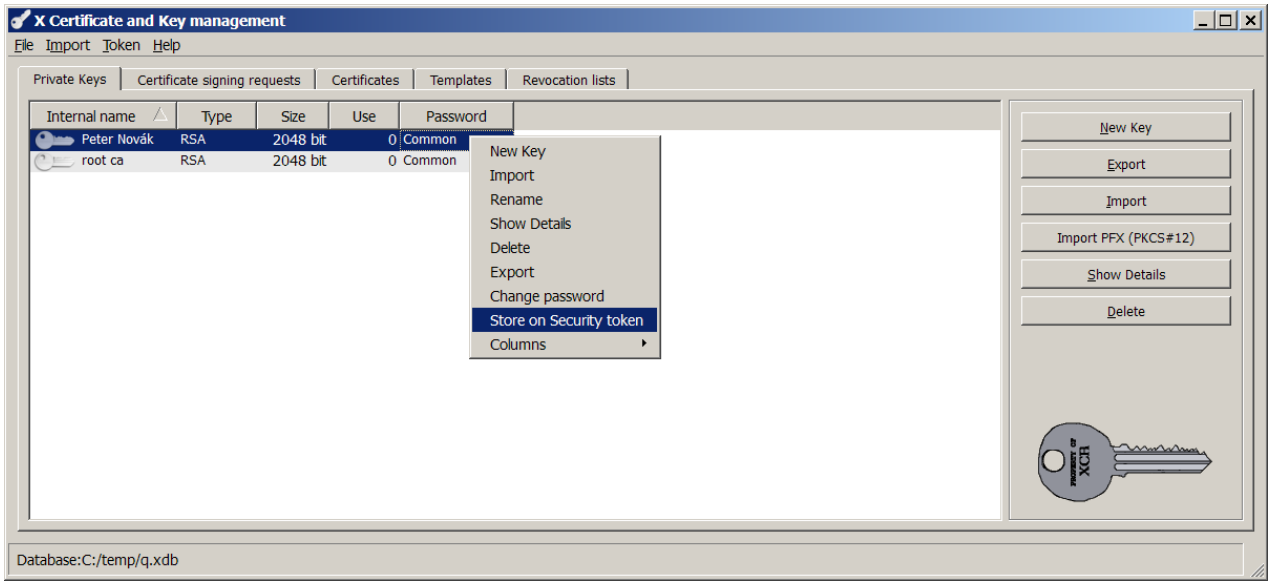
Vygenerujte kľúčový pár účastníka obdobným postupom ako v kapitole 4. V príklade na obrázku sme zvolili názov kľúčového páru "Peter Novák".



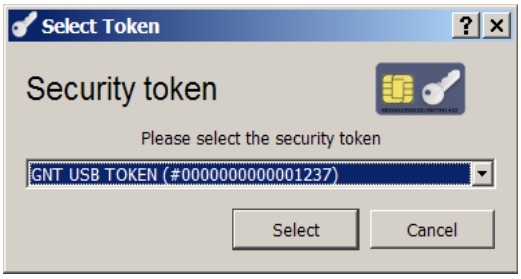
Poznámka: Ak chcete vytvoriť zálohu novo vytvoreného privátného kľúča, môžete tak urobiť exportovaním privátného kľúča pomocou tlačidla "Export". Po premiestnení privátneho kľúča na Token nebude viac možné nijakým spôsobom získať jeho hodnotu.

7 Premiestnenie kľúčového páru účastníka na GNT USB Token

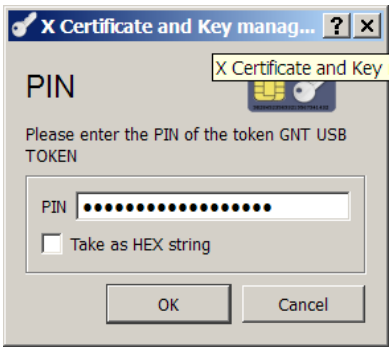
1. Vložte Token účastníka. Pravým tlačidlom myši kliknite na kľúčový pár účastníka a zvoľte "Store on security token".



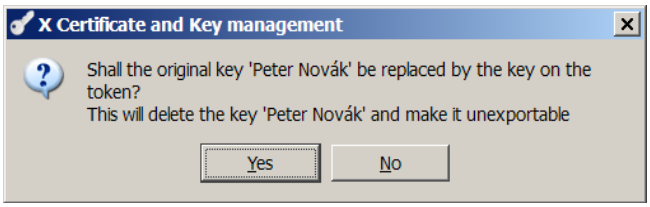
2. V okne "Security Token" zvoľte Token prislúchajúci danému účastníkovi. Token je jednoznačne identifikovaný sériovým číslom zobrazeným v zátvorke. Aby ste vylúčili možnosť omylu, vložte do systému vždy len jediný token, prislúchajúci aktuálne obsluhovanému účastníkovy.



3. V okne PIN vložte užívateľské heslo tak, ako ste ho pre daný Token inicializovali programom Ginit (textové pole PIN1 na obrázku v kapitole 2).



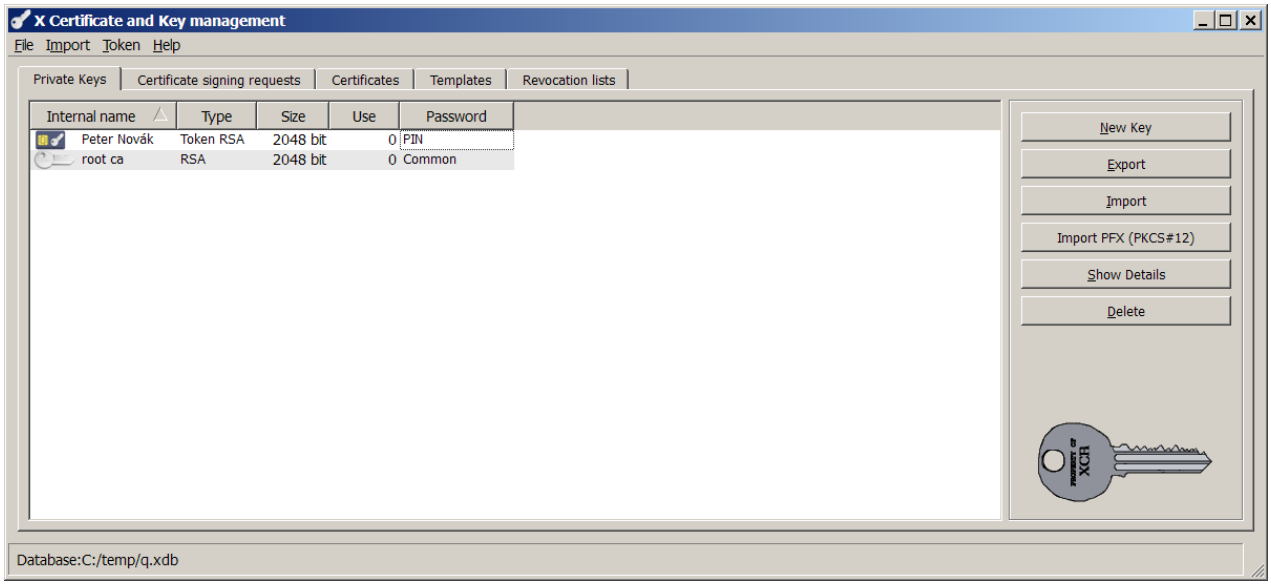
4. V nasledujúcom okne potvrďte tlačidlom "Yes", že pôvodný kľúč má byť nahradený kľúčom na GNT USB Tokene.



Poznámka: Po vykonaní tohoto kroku nebude možné nijakým spôsobom získať hodnotu privátneho kľúča účastníka. Kľúč bude fyzicky uložený v bezpečnom úložisku Tokenu a akékoľvek kryptografické operácie s ním budú vykonané v zabezpečenom prostredí Tokenu.

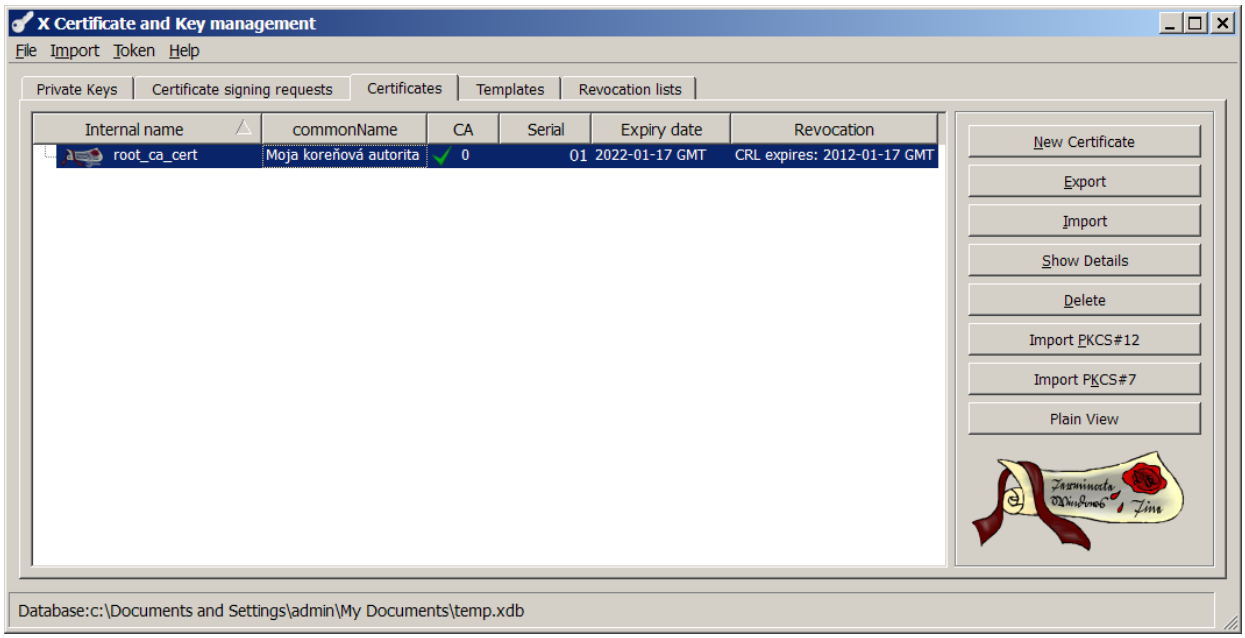
---

5. Úspešné premiestnenie kľúčového páru indikuje ikona "elektronickej karty" v hlavnom okne aplikácie.

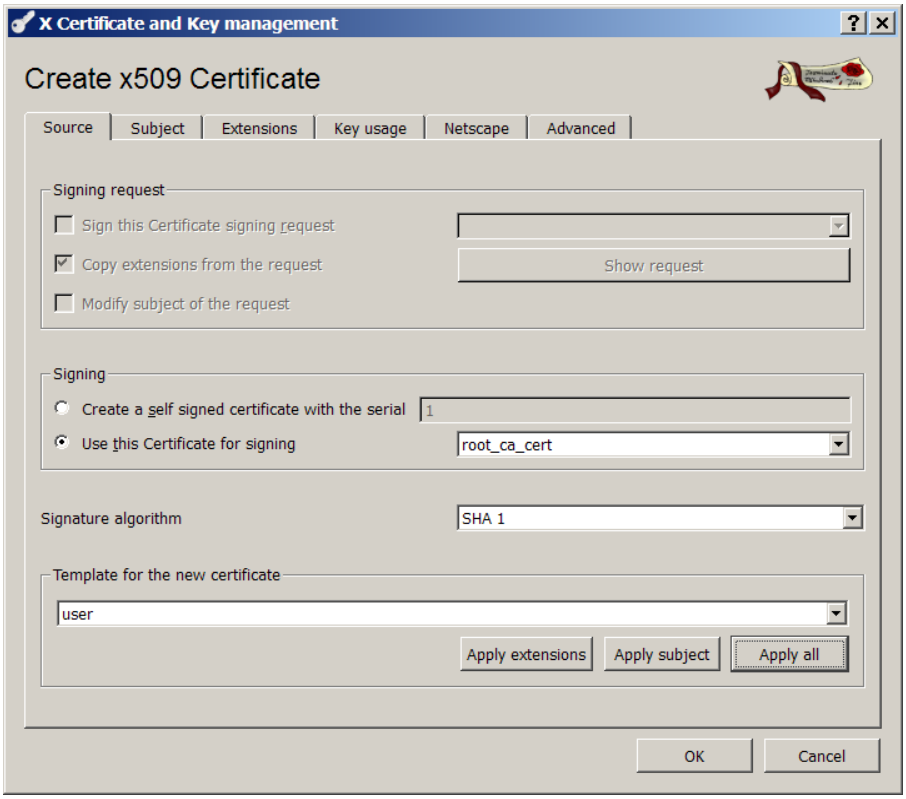


8 Vytvorenie certifikátu účastníka

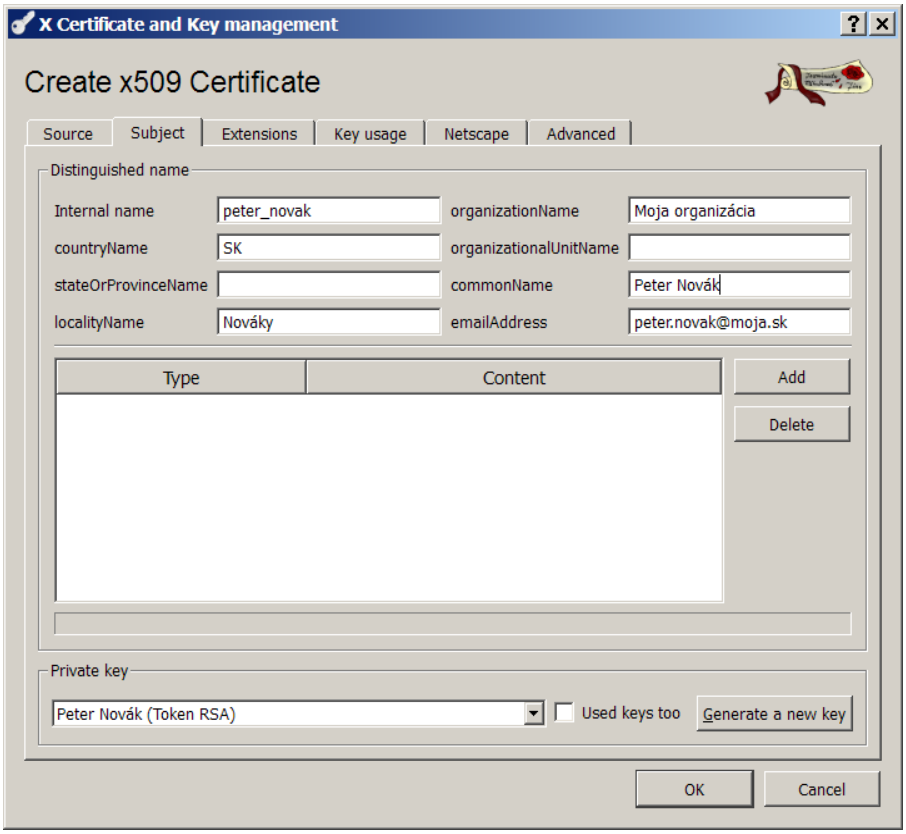
1. V karte "Certificates" označte certifikát koreňovej autority a zvoľte tlačidlo "New Certificate".



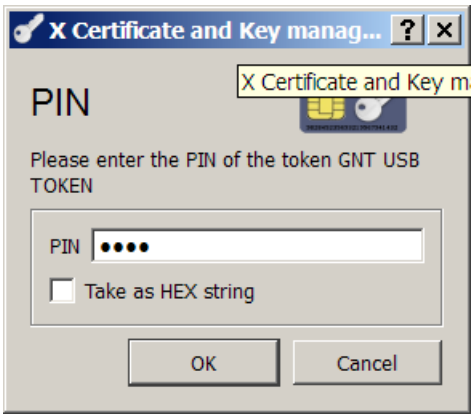
2. V karte "Source", v poli "Template for the new certificate" zvoľte šablónu "user" a stlačte tlačidlo "Apply all". Overte, že v poli "Signing" je zvolené podpísanie certifikátom koreňovej certifikačnej autority.



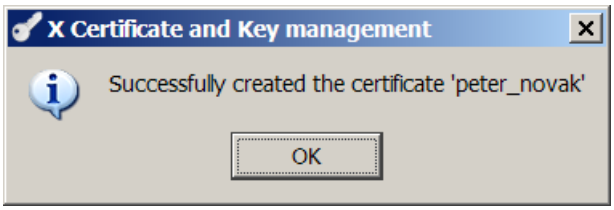
3. V karte "Subject" zvoľte privátny kľúč učastníka a vyplňte polia podľa vzoru na nasledujúcom obrázku. Stlačením tlačidla "OK" vygenerujte certifikát.



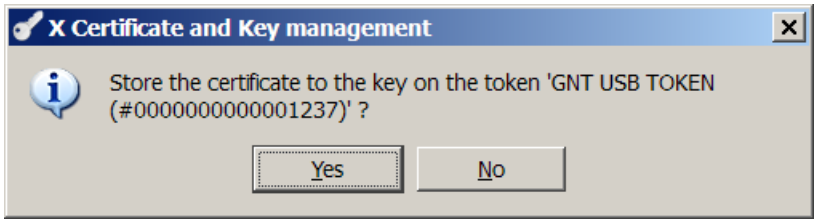
4. V okne PIN vložte užívateľské heslo tak, ako ste ho pre daný Token inicializovali programom Ginit (textové pole PIN1 na obrázku v kapitole 2).



5. Aplikácia potvrdí úspešné vygenerovanie certifikátu. Stlačte "OK".

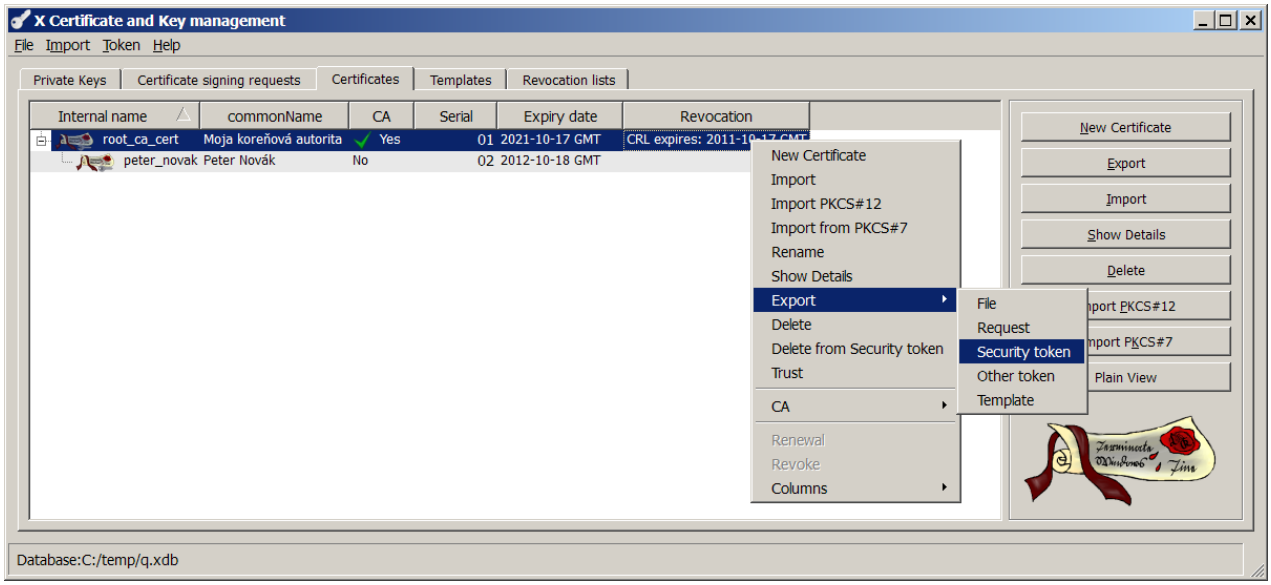


6. V nasledujúcom okne potvrďte, že certifikát má byť uložený na Tokene účastníka. Po výzve znova vložte užívateľské heslo.



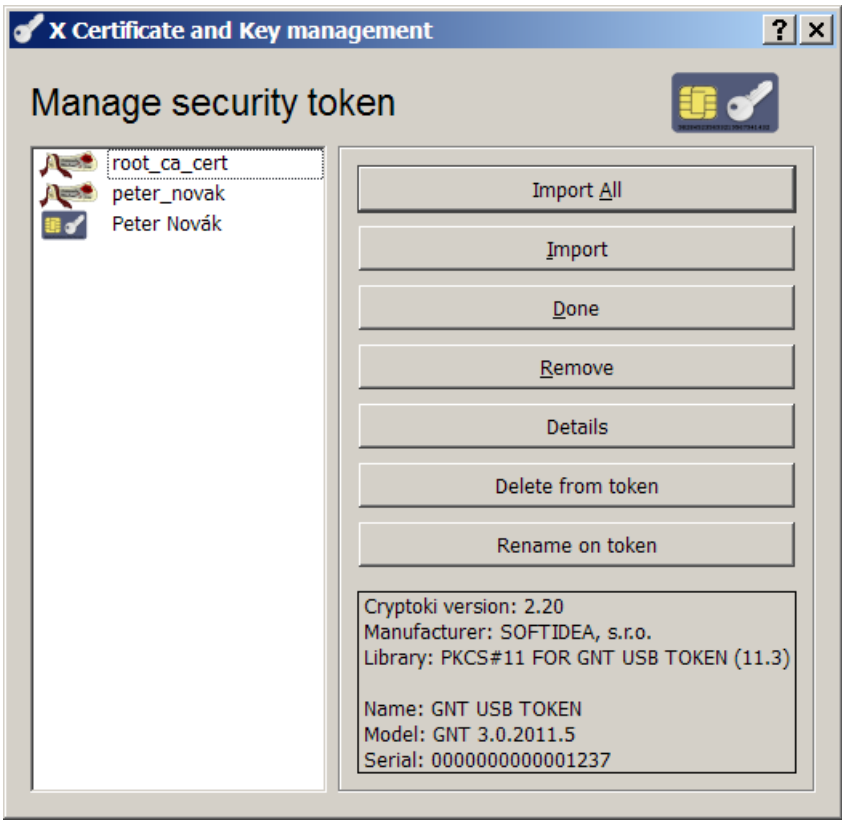
9 Uloženie certifikátu koreňovej certifikačnej autority na Token účastníka

V karte "Certificates" kliknite pravým tlačidlom myši na certifikát koreňovej autority, zvoľte "Export->Security token". V nasledujúcich oknách zvoľte Token účastníka a vložte užívateľské heslo ako v kapitole 7 kroky 2 a 3.



10 Overenie obsahu Tokenu účastníka

1. V hlavnom menu programu XCA zvoľte "Token->Manage security token" a zvoľte token účastníka. V okne "Manage security token" overte, že Token obsahuje certifikát koreňovej autority a certifikát a privátny kľúč účastníka.



V kapitolách 6 až 9 je popísaný systém kde ten istý certifikát a kľúčový pár sa používa na podpisovanie i šifrovanie správ. Je ale tiež možné pre účastníka vytvoriť dva certifikáty a kľúčové páry - jeden určený na podpisovanie a druhý na šifrovanie správ. Ak sa rozhodnete implementovať systém týmto spôsobom, vytvorte pre každého účastníka dva kľúčové páry a pre vytvorenie príslušných certifikátov použite šablóny "sign_user.xca" a "crypt_user.xca". Podobne je možné tiež zabezpečiť použitie rovnakého kryptografického kľúča viacerými aplikáciami. Ak napríklad vygenerujete kryptografické kľúče účastníka programom PGP, následne pre tieto kľúče v programe XCA vytvoríte príslušné certifikáty a zahrniete ich do systému zabezpečenia poštovej komunikácie, môžete využívať ten istý kľúčový pár v oboch aplikáciách.

11 Odovzdanie užívateľovi

Overte, že počítač užívateľa obsahuje inštaláciu produktu GNT USB Token od spoločnosti *SoftIdea*. Postačujúca je "štandardná inštalácia bez podpory administrácie". Overte, že poštový klient užívateľa je nastavený podľa dokumentu ***Šifrovanie elektronickej pošty - príručka používateľa (AN101011).*** Odovzdajte užívateľovi Token a dočasné heslo užívateľa.

12 Záver

Implementáciou systému zabezpečenia poštovej komunikácie podľa tejto príručky ste vytvorili systém siete dôvery s koreňovou certifikačnou autoritou založený na kryptografickom systéme s verejným kľúčom so šifrou RSA. Privátny kľúč každého z účastníkov je uložený v bezpečnom úložišti účastníkovho osobného hardvérového kryptografického zariadenia *GNT USB Token*. Privátny kľúč koreňovej certifikačnej autority je uložený v súbore databázy *XCA* chránenom heslom. Pre dosiahnutie veľmi vysokej úrovne bezpečnosti systému odporúčame navyše zašifrovať súbor databázy *XCA*. Každý z účastníkov obdržal pre prvý prístup k svojmu Tokenu dočasné heslo užívateľa, ktoré by mal následne zmeniť v prostredí poštového klienta *Thunderbird*. Pre každý Token účastníka je definované i heslo administrátora, ktoré môže byť v prípade straty hesla užívateľom použité na zmenu užívateľského hesla administrátorom v prostredí aplikácie *Ginit*.

13 Dokumentácia

1 GNT USB Token - dátový list, SoftIdea, s.r.o. , Máj 2011, http://www.softidea.sk/gnt_datasheet_sk.pdf

2 Šifrovanie elektronickej pošty - Príručka používateľa (AN101011), SoftIdea, s.r.o. , December 2011, http://www.softidea.sk/an101011_sk.pdf

3 GINIT - užívateľský manuál, SoftIdea, s.r.o. , Máj 2011, http://www.softidea.sk/ginit_manual_sk.pdf

4 SIPKCS - Aplikačné programové rozhranie PKCS#11 pre GNT USB Token, SoftIdea, s.r.o. , Máj 2011, http://www.softidea.sk/sipkcs_specification_sk.pdf

SoftIdea s.r.o.
Sliačska 10, 831 02 Bratislava
tel.: +421 2 444 60 444
fax.: +421 2 446 40 441
http://www.softidea.sk
info@softidea.sk