SecureStore I.CA

Užívateľská príručka

Verzia 2.16 a vyššia

Obsah

1. Úvod

Táto verzia užívateľskej príručky platí pre nasledujúce verzie Aplikácie SecureStore: 2.16 a vyššie. Uvedené verzie majú rovnakú funkčnosť a totožné užívateľské rozhranie.

2. Prístupové údaje ku karte

Prístup ku karte je chránený pomocou PINu, podobne ako napr. prístup k platobným kartám.
PIN je 4-8 miestne číslo. Ak pri zadávaní PINu 3krát za sebou zadáte nesprávnu hodnotu PINu, PIN sa automaticky zablokuje.
Na odblokovanie PINu je určená hodnota PUK.
PUK je 4-8 miestne číslo. Ak pri zadávaní PUKu 5krát za sebou zadáte nesprávnu hodnotu PUKu, dôjde k zablokovaniu PUKu a tým aj celej karty.

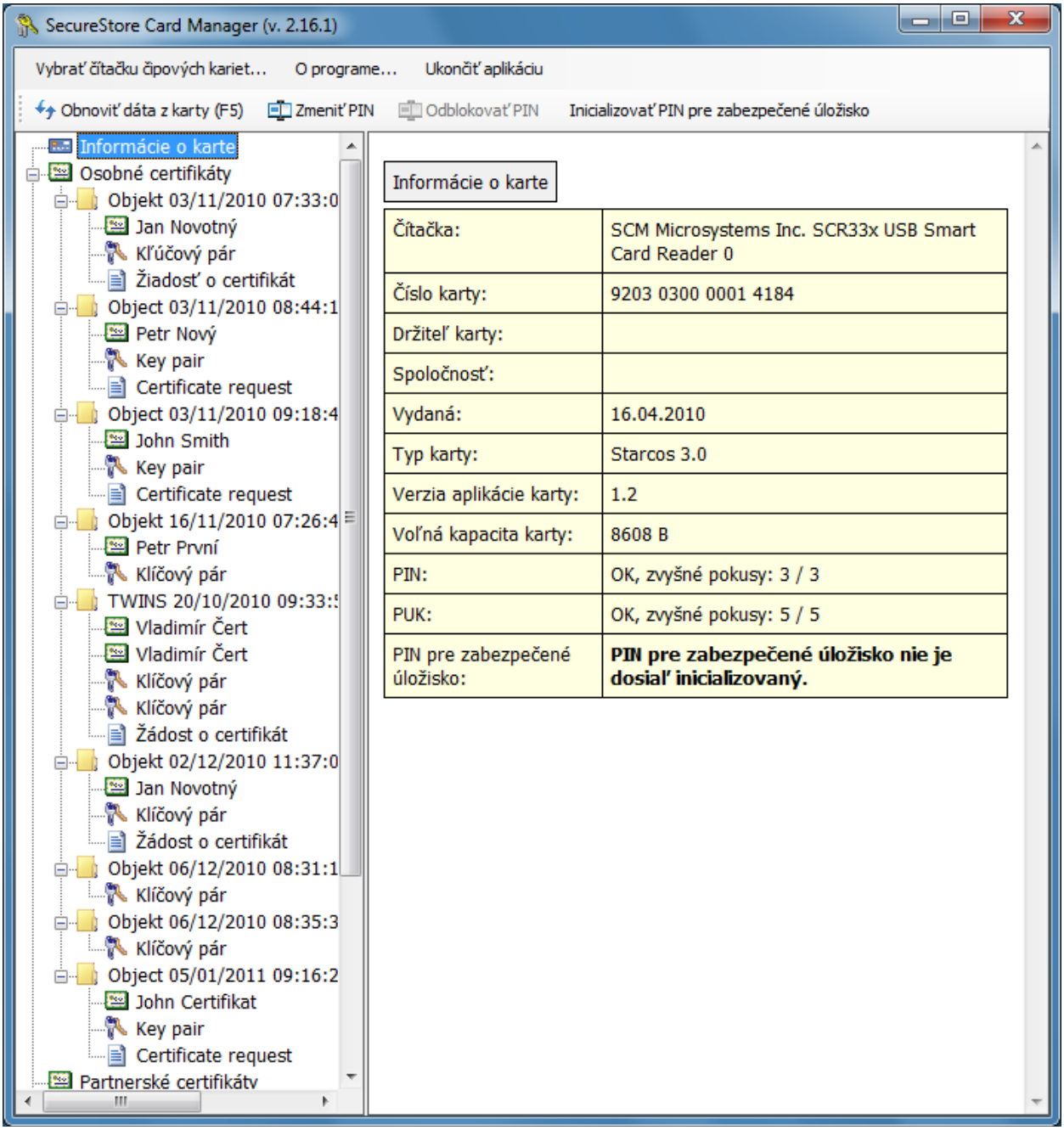
Časť karty nazvaná „Zabezpečené osobné úložiská" je určená na uloženie ľubovoľných dát. Táto oblasť je chránená zvláštnym PINom tzv. PINom pre zabezpečené úložisko. Na odblokovanie PINu pre zabezpečené úložiská použite PUK uvedený v predošlom odseku.
PIN pre zabezpečené úložiská je 4-8 miestne číslo.

2.1 Inicializácia karty

Dialóg inicializácie karty sa zobrazí spravidla pri prvom spustení aplikácie na novej karte, ak ste ku karte nedostali pinovú obálku. Pomocou tohto dialógu je potrebné nastaviť PIN a PUK pre prácu s práve vloženou kartou. Tento PIN a PUK je potrebné starostlivo si zapamätať, prípadne uložiť na bezpečné miesto, aby k nemu nemal nikto iný prístup.

3. Základná obrazovka

Obr.1 Základná obrazovka

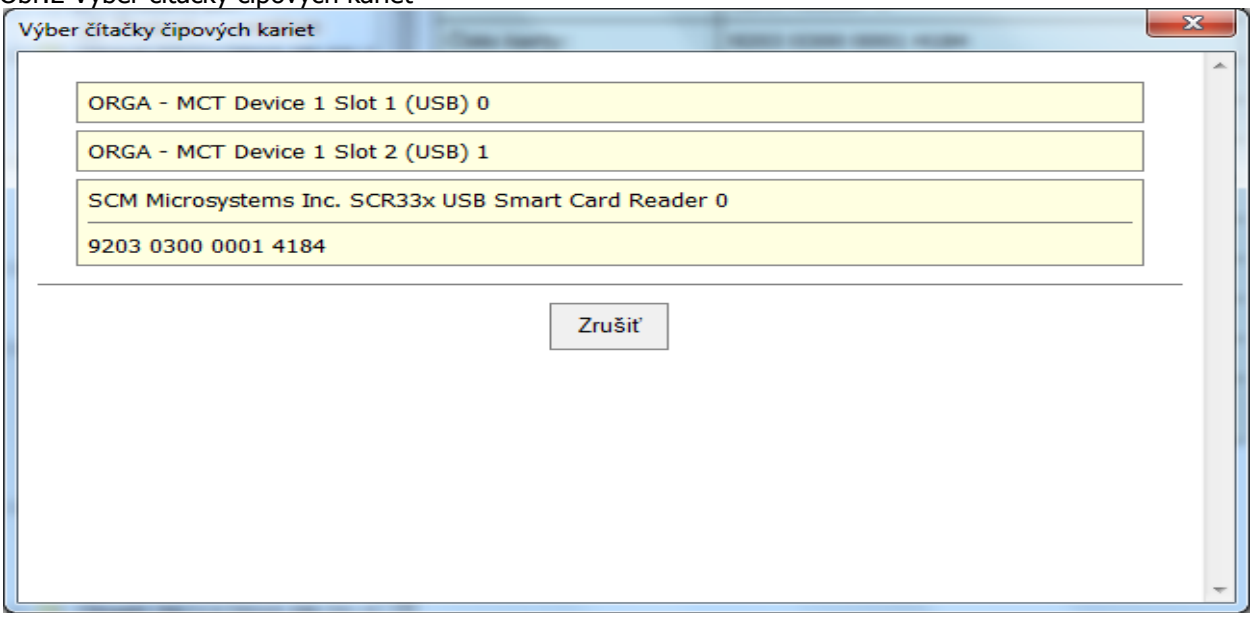


V pravej časti obrazovky sa zobrazujú základné informácie o držiteľovi karty, platnosti karty, o čítačke čipových kariet, v ktorej je karta vložená, a verzia systému súborov karty.

V hornej lište sú uvedené nasledujúce voľby:

Voľba „**Vybrať čítačku čipových kariet**" je užitočná, ak máte k PC pripojených viac čítačiek čipových kariet súčasne. Pomocou voľby môžete vybrať čítačku, s ktorou chcete pracovať. Pre čítačku čipových kariet, v ktorej je vložená karta, sa zobrazuje číslo a typ čipovej karty, viď nasledujúci obrázok.
V prípade, že máte k PC pripojených viac čítačiek čipových kariet, zobrazuje sa okno „Výber čítačiek čipových kariet " aj po spustení aplikácie.

Obr.2 Výber čítačky čipových kariet

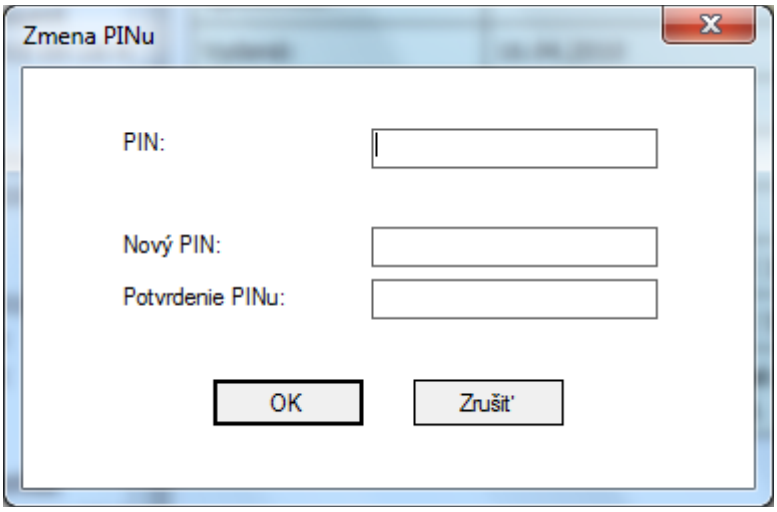


V prípade, že máte k PC pripojenú len jednu čítačku čipových kariet, okno sa nezobrazuje a informácie o nájdenej čítačke sú uvedené v prvom riadku úvodnej obrazovky.

Voľba „**Obnoviť dáta z karty**" opakovane načíta dáta z čipovej karty. Rovnakú funkciu má kláves F5.

Voľba „**Zmeniť PIN**" " vykoná zmenu hlavného PINu karty. Vyžaduje zadať súčasný PIN a na potvrdenie 2x nový PIN.

Obr.3 Zmena PINu

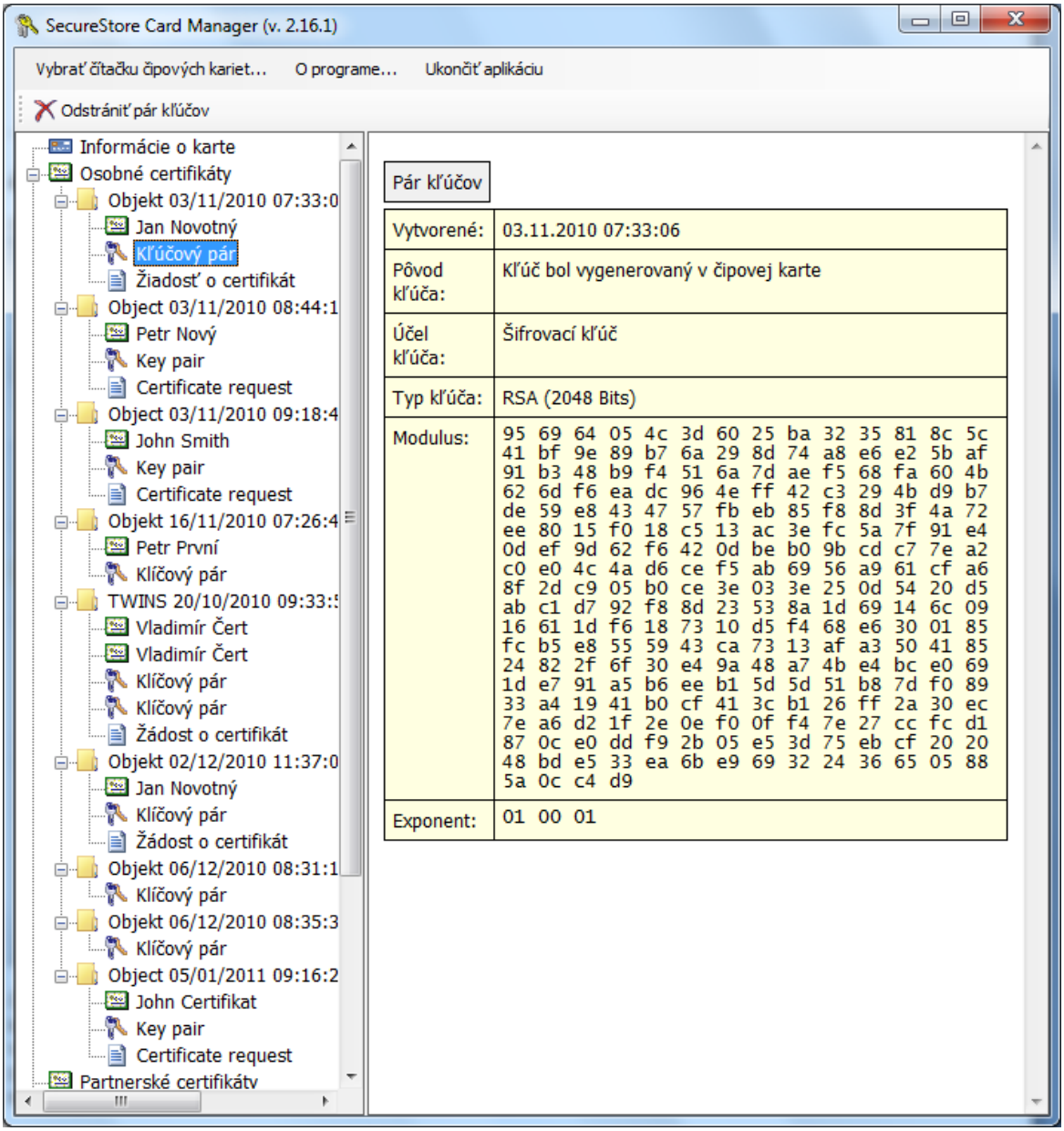


Voľba „**Odblokovať PIN**" umožňuje nastaviť novú hodnotu PINu v prípade, že si PIN zablokujete. K zablokovaniu PINu dôjde po zadaní 3 chybných hodnôt PINu. Na odblokovanie PINu sa vyžaduje zadať PUK.

Voľba „**Zmeniť PIN pre zabezpečené úložisko**" umožňuje zmeniť PIN pre špeciálnu časť karty nazývanú Zabezpečené osobné úložiská.
Voľba „**Odblokovať PIN pre zabezpečené úložisko**" umožňuje odblokovať PIN pre Zabezpečené osobné úložiská.

4. Zobrazenie informácií o páre kľúčov

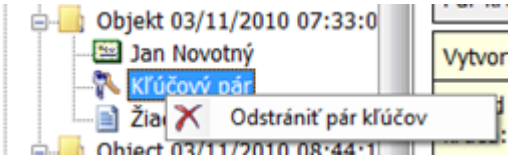
Obr.4 Pár kľúčov



Čas vytvorenia verejného/privátneho kľúča udáva presný čas, kedy sa kľúč vygeneroval na karte, alebo kedy sa na kartu importoval. Túto informáciu zobrazuje položka „Pôvod kľúča".
V položke „Účel kľúča" je uvedené, či ide o kľúč šifrovací alebo podpisový.
Ďalej je uvedený typ kľúča, v našom príklade ide o kľúč pre RSA algoritmus s dĺžkou 2048 bitov.
Nasleduje hexadecimálny výpis exponentu a modulu verejného kľúča na vizuálnu kontrolu.

Kľúče možno z karty odstrániť pomocou voľby „Odstrániť pár kľúčov". Voľba je dostupná po kliknutí pravým tlačidlom myši na danom páre kľúčov, viď nasledujúci obrázok.

Obr.5 Odstránenie páru kľúčov

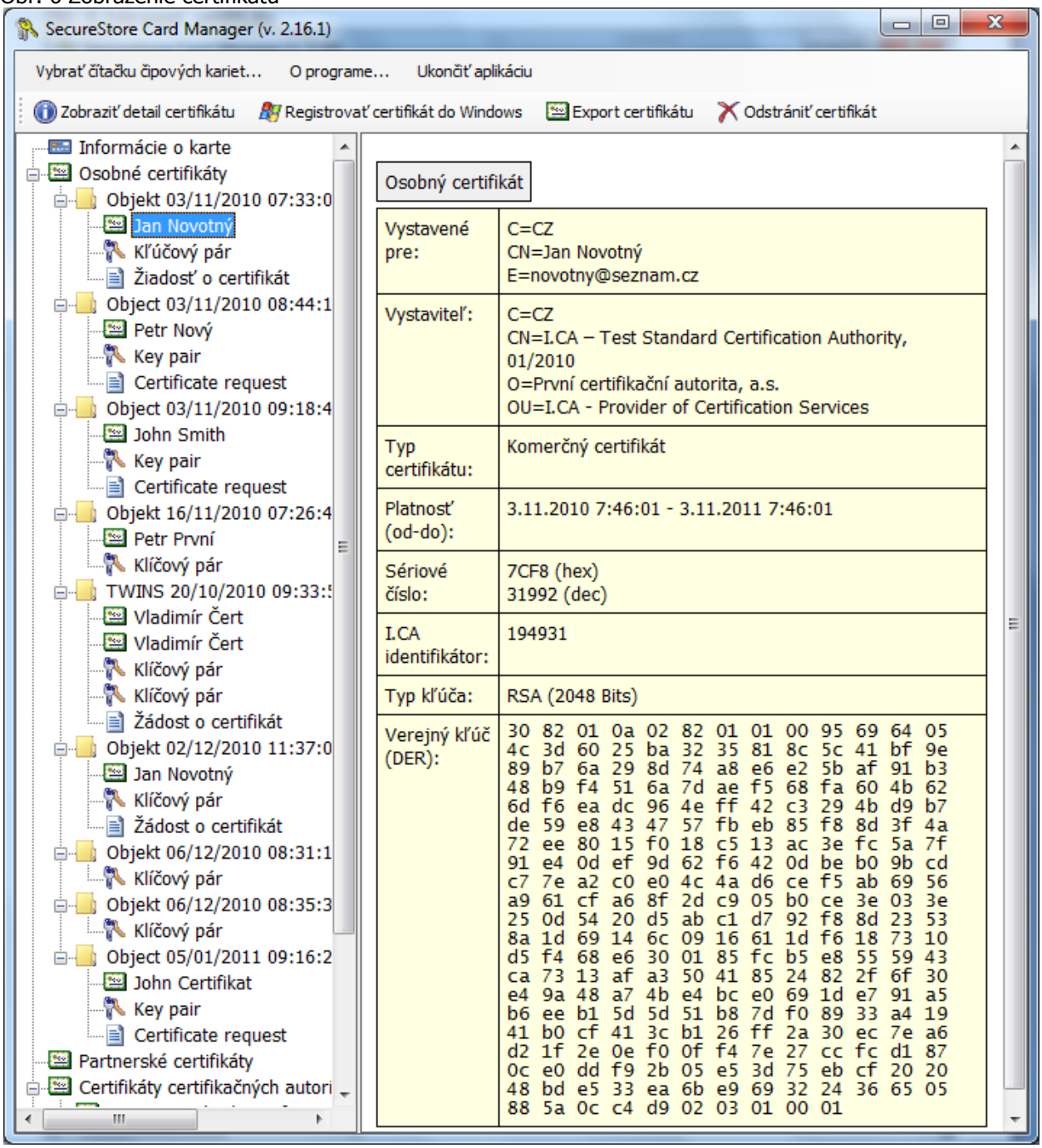


Voľba „Odstrániť pár kľúčov" nevratne odstráni pár kľúčov z karty (t.j. bude vymazaný privátny, ako aj verejný kľúč). Ak sa odstráni privátny kľúč k osobnému certifikátu, nebude viac možné certifikátom podpisovať ani dešifrovať!!!

5. Certifikáty

5.1 Zobrazenie certifikátu

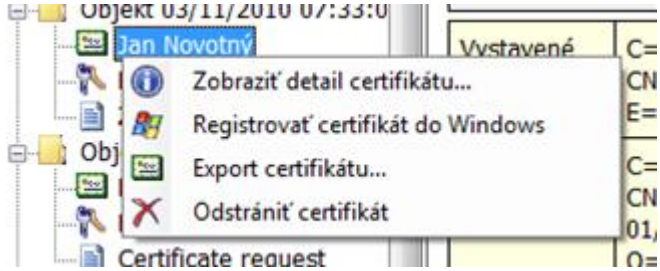
Obr. 6 Zobrazenie certifikátu



5.2 Práca s osobným certifikátom

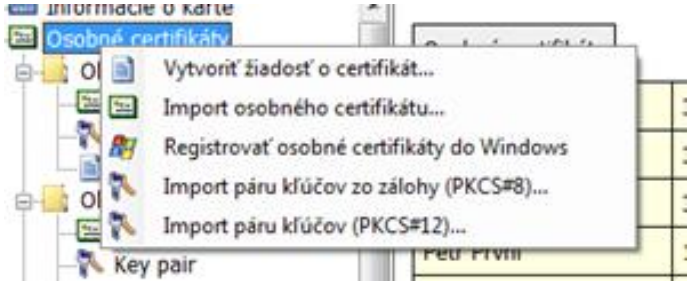
Voľby pre prácu s certifikátom uloženým na karte sú dostupné po kliknutí pravým tlačidlom myši na danom certifikáte, viď nasledujúci obrázok.

Obr. 7 Voľby pre prácu s osobným certifikátom na karte



Voľby pre import certifikátu na kartu sú dostupné po kliknutí pravým tlačidlom myši na položke osobné certifikáty, viď nasledujúci obrázok.

Obr.8 Voľby pre import a registráciu osobného certifikátu



Ak sa pri importe osobného certifikátu nenájde na karte úložisko obsahujúce príslušný pár kľúčov (súkromný a verejný), bude certifikát importovaný ako certifikát partnerov.

Ako partnerské certifikáty sa importujú tie certifikáty, ku ktorým nemáte súkromný kľúč, a ktoré sa nepovažujú za dôveryhodné certifikáty CA.

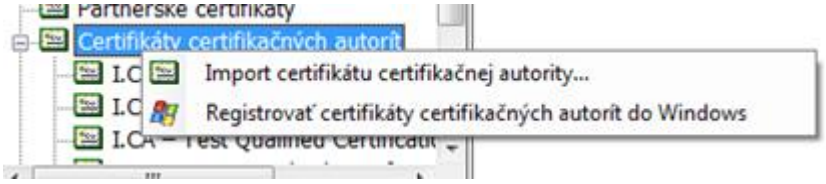
Zobrazenie holých dát certifikátu slúži len pre odborníkov na vizuálnu kontrolu dát certifikátu.

5.3 Práca s koreňovým certifikátom certifikačnej autority

Nová karta obsahuje potrebné koreňové certifikáty certifikačnej autority, ktoré sú uložené v časti „Certifikáty certifikačných autorít".

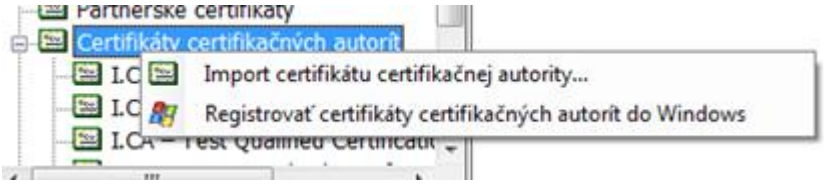
Importovať certifikát ako certifikát CA možno iba vtedy, ak ide o certifikát povolený CA pre danú kartu. Certifikáty ďalších CA alebo novo vydané certifikáty CA možno importovať vo formáte cmf.

Obr. 9 Import certifikátu certifikačnej autority



Koreňové certifikáty I.CA sú súčasťou Windows. Ak potrebujete registrovať koreňový certifikát karty, použite voľbu „Registrovať certifikát do Windows", viď obrázok obr.10. Koreňový certifikát je registrovaný do MS Windows ako dôveryhodný koreňový certifikát. Tento export vyžaduje potvrdenie registrácie pre MS Windows.

Obr.10 Registrácia certifikátu certifikačnej autority do Windows



Hromadnú registráciu koreňových certifikátov umožňuje voľba tlačidla „Registrovať certifikáty certifikačných autorít do Windows" viď obrázok obr.9.

5.4 Registrácia osobného certifikátu do Windows

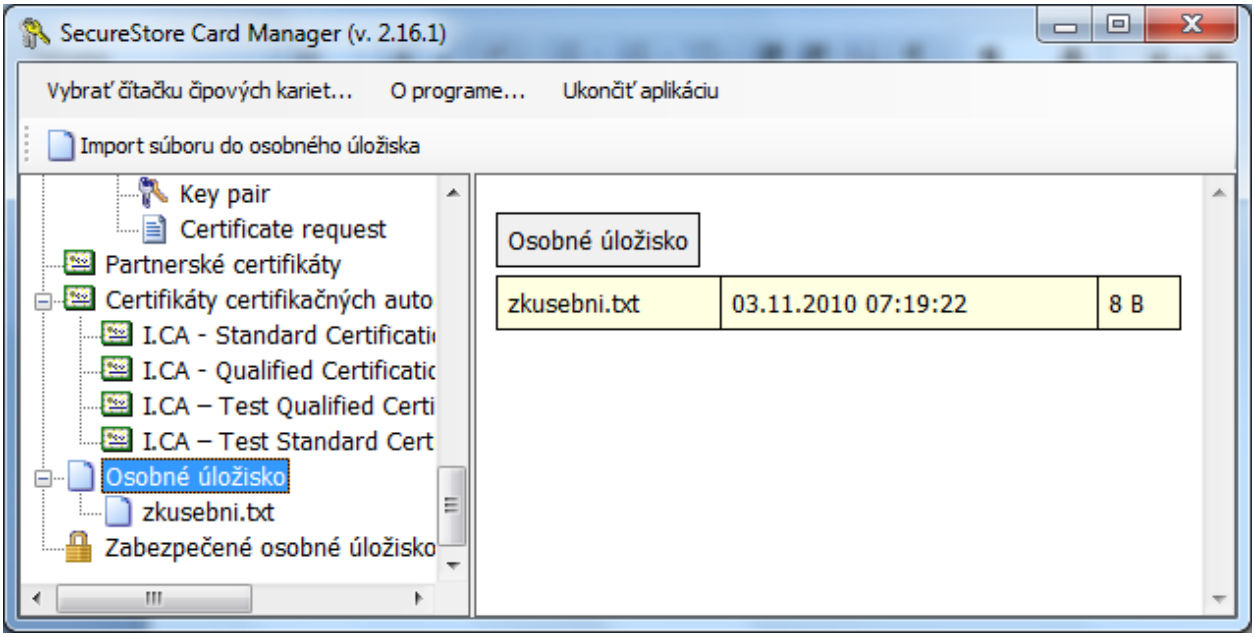
Registráciu certifikátov možno vykonať jednotlivo pre každý certifikát pomocou voľby „Registrovať certifikát do Windows", viď obrázok obr.7.

Registrácia jednotlivého certifikátu do MS Windows vyexportuje certifikát do úložiska certifikátov MS Windows. V prípade osobného certifikátu prebieha export do úložiska Osobných Certifikátov, pričom sa exportuje certifikát bez súkromného kľúča, ktorý zostáva na karte a nikdy ju neopustí. S takto zaregistrovaným certifikátom pri použití karty so súkromným kľúčom možno šifrovať alebo podpisovať.

Hromadnú registráciu osobných certifikátov umožňuje voľba „Registrovať osobné certifikáty do Windows" viď obrázok obr.8.

6. Osobné úložisko

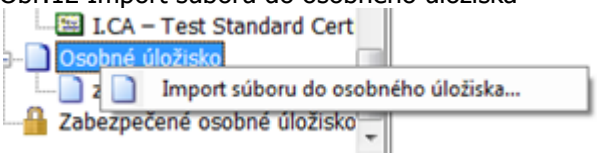
Obr.11 Osobné úložisko



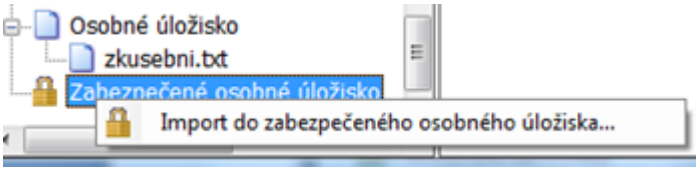
Do Osobných úložísk si môžete ukladať malé súbory (niekoľko málo kB), ktoré budú vždy poruke a zabezpečené na čipovej karte. Na kartu možno uložiť textový, ako aj binárny súbor.

Pri importe možno importovať do zabezpečených alebo verejných úložísk. Pri voľbe zabezpečených (chránených úložísk) budete vyzvaní, aby ste zadali PIN pre zabezpečené úložiská (iný PIN než hlavný). Ak použijete túto voľbu prvý raz, zobrazí sa zároveň žiadosť o nastavenie PINu pre zabezpečené úložiská.

Obr.12 Import súboru do osobného úložiska



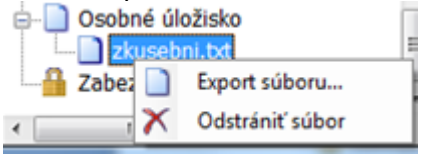
Obr.13 Import súboru do zabezpečeného úložiska



Na zobrazenie položky v zabezpečenom úložisku je potrebné zadať PIN pre zabezpečené úložiská.

Súbory uložené v osobnom úložisku možno exportovať. Pri exporte zadajte celé meno súboru včítane prípony.

Obr. 14 Export súboru z osobného úložiska



7. Ovládanie aplikácie

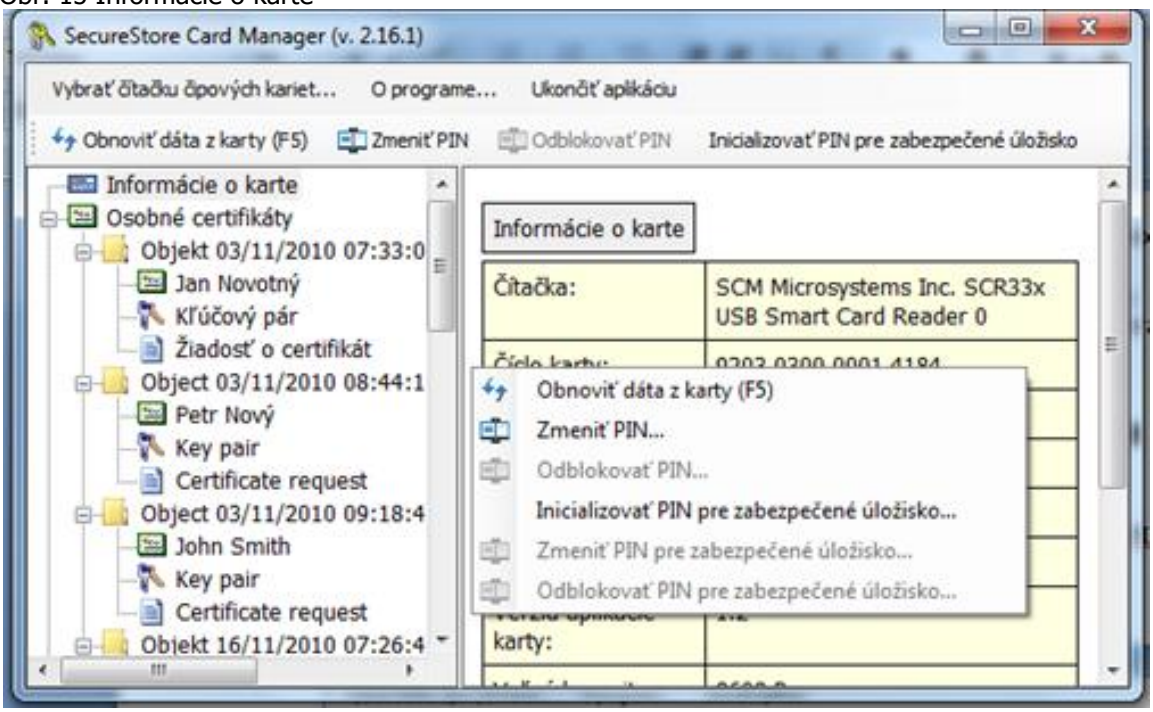
Jednotlivé funkcie aplikácie sa realizujú pomocou kontextových menu. Kontextové menu sa otvorí dvomi spôsobmi:

- kliknutím pravým tlačidlom na položke stromu v ľavej časti obrazovky
- kliknutím pravým tlačidlom nad pravou časťou obrazovky, kde sú zobrazené informácie o vybranej položke z ľavej časti obrazovky.

7.1 Kontextové menu pre Informácie o karte

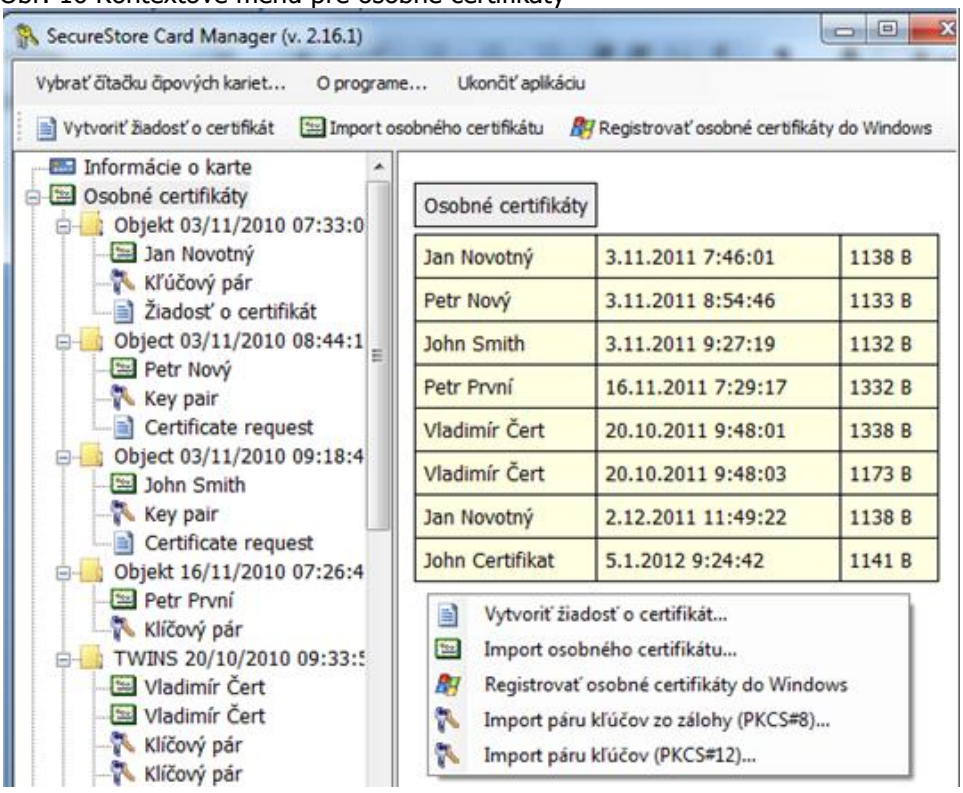
Obsahuje základné administratívne operácie nad kartou súvisiace so správou PINu a PUKu a opakovaným načítaním dát z karty.

Obr. 15 Informácie o karte



7.2 Kontextové menu pre zložku Osobné certifikáty

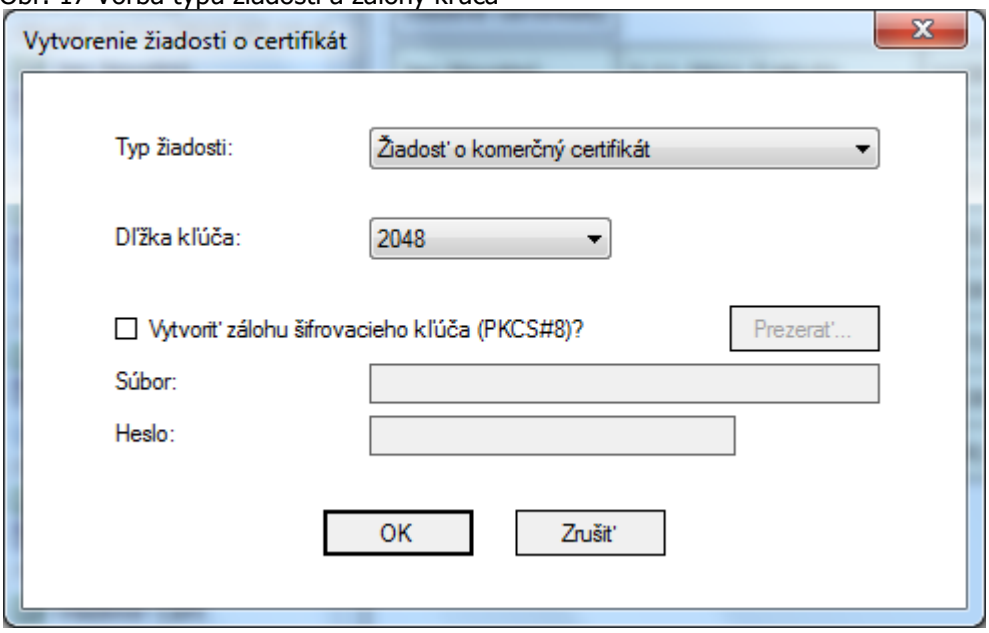
Obr. 16 Kontextové menu pre osobné certifikáty



7.2.1 Vytvoriť žiadosť o certifikát

Umožňuje vytvoriť žiadosť o certifikát. Zvoľte typ žiadosti o certifikát a pre šifrovací certifikát zadajte požiadavku na zálohovanie kľúča.

Obr. 17 Voľba typu žiadosti a zálohy kľúča



Dĺžka kľúča môže byť 1024 bitov alebo 2048 bitov. Kľúč dĺžky 2048 je dlhší a bezpečnejší. Pre certifikáty I.CA sa požaduje kľúč dĺžky 2048 bitov.

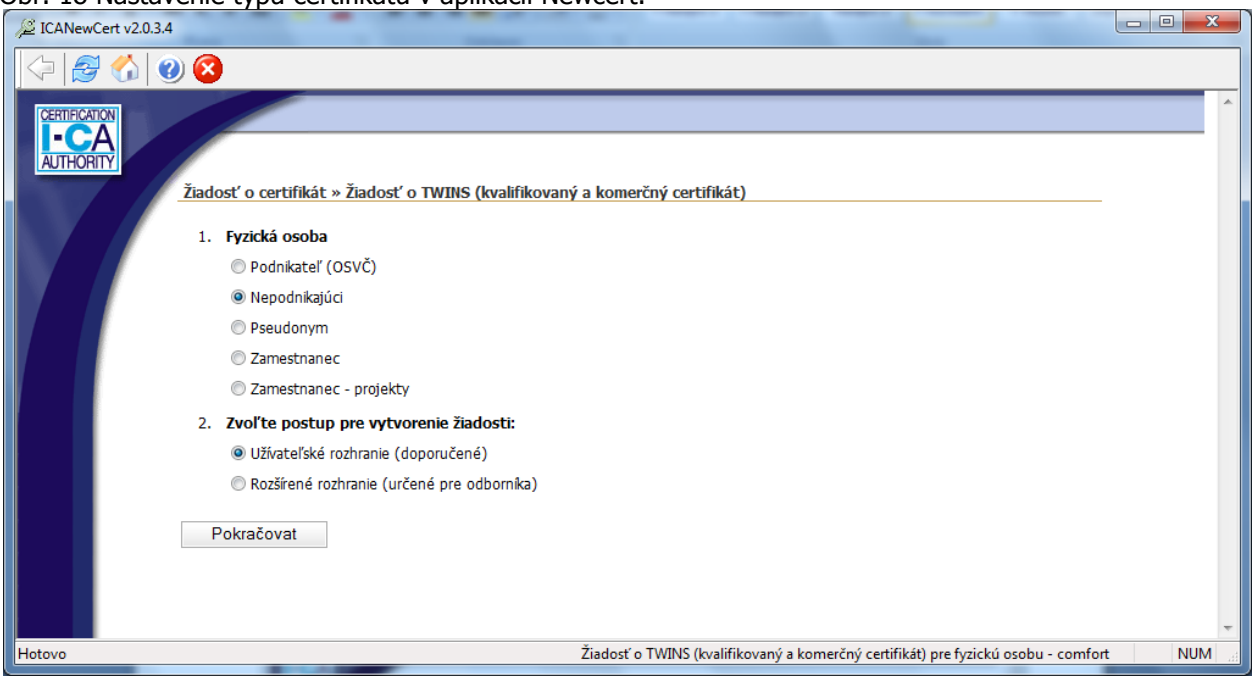
Šifrovacie kľúče možno generovať so zálohou, ktorá sa uloží mimo karty. Budú uložené do zabezpečeného PKCS#8 súboru s heslom, ktoré zadáte v okne, viď obrázok obr.17.

Podpisovacie kľúče sa generujú priamo na karte a nie je žiadna možnosť, ako vyexportovať privátny kľúč von z karty.

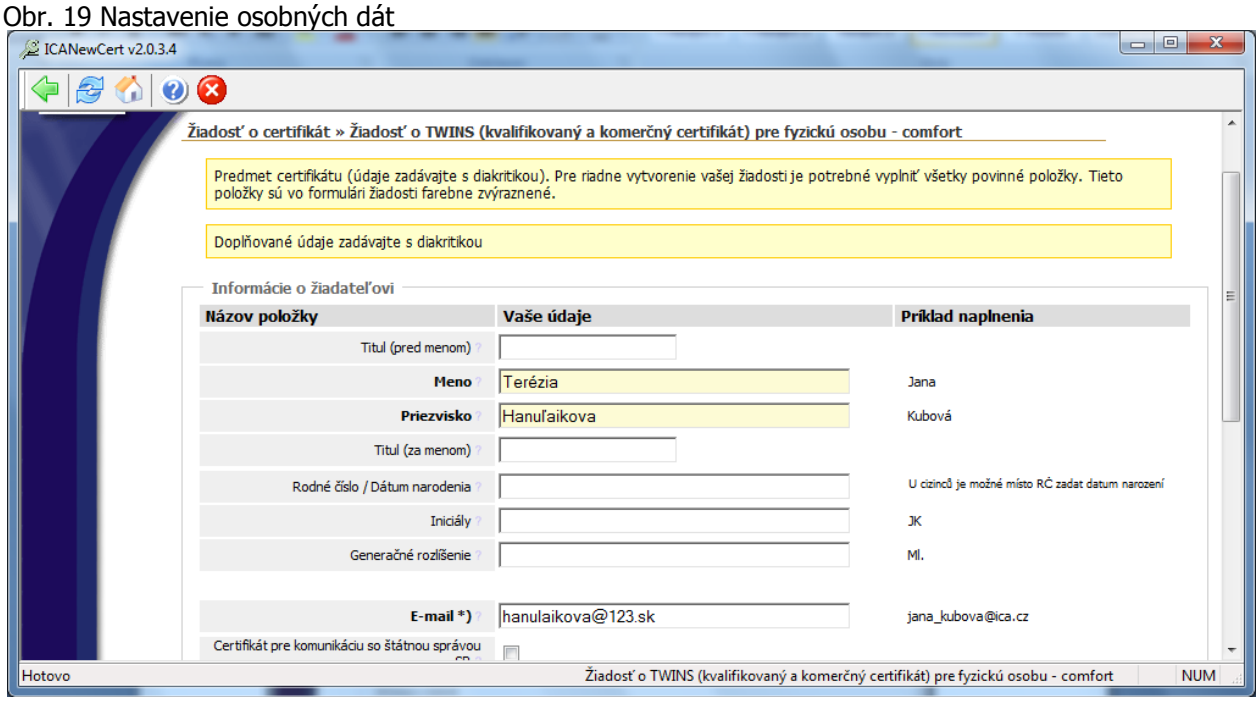
Po potvrdení tohto dialógu sa budú generovať kľúče, čo môže trvať desiatky sekúnd až minútu.

Následne sa spustí aplikácia NewCert, ktorá vygeneruje samotnú žiadosť o certifikát.

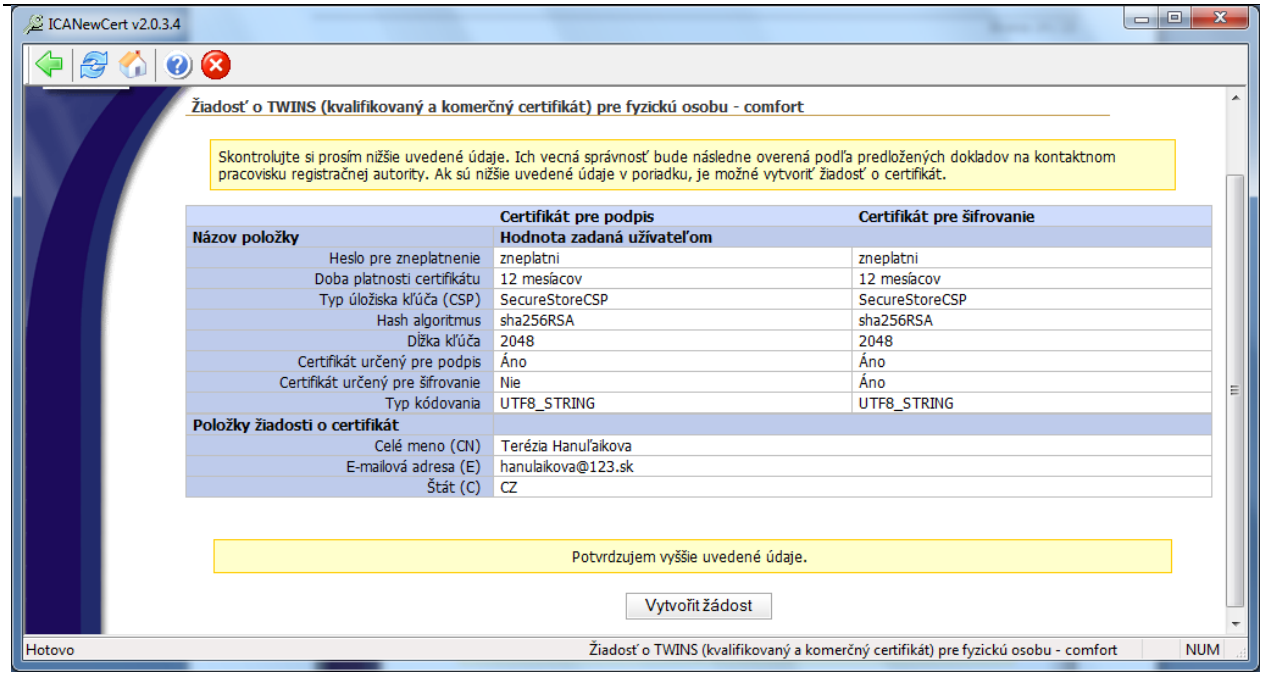
Obr. 18 Nastavenie typu certifikátu v aplikácii Newcert.



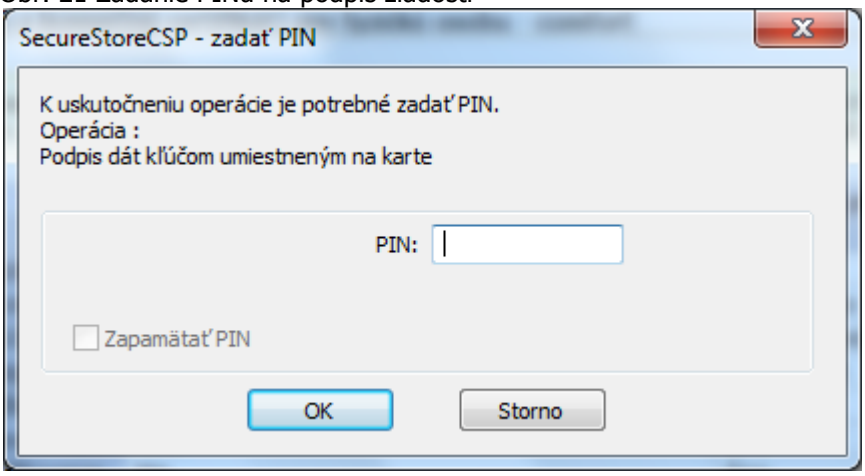
Obr. 19 Nastavenie osobných dát



Obr. 20 Potvrdenie poskytnutých dát pre žiadosť



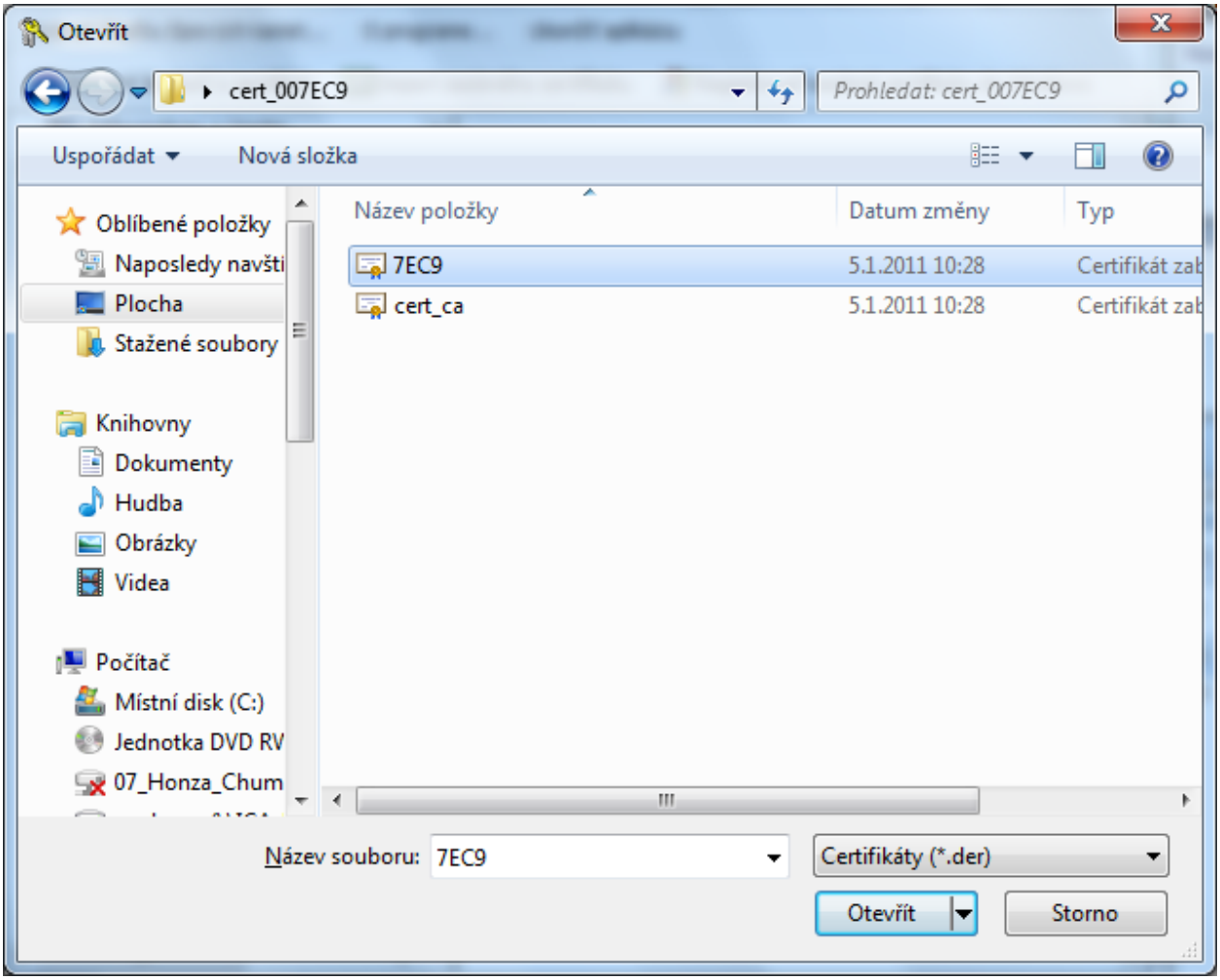
Obr. 21 Zadanie PINu na podpis žiadosti



7.2.2 Import osobného certifikátu

Funkcia umožňuje import osobného certifikátu z disku na kartu. Certifikát sa importuje vo formáte der. Importovaný certifikát sa uloží do toho úložiska na karte, ktoré obsahuje kľúče k certifikátu.
Ak na karte neexistuje úložisko so zodpovedajúcimi kľúčmi, certifikát sa uloží do časti karty označenej ako „Partnerské certifikáty".

Obr.22 Výber súboru s certifikátom pre import na kartu



7.2.3 Registrovať osobné certifikáty do Windows

Voľba zaregistruje všetky osobné certifikáty z karty do osobného úložiska vo Windows.

7.2.4 Import páru kľúčov zo zálohy (PKCS#8)...

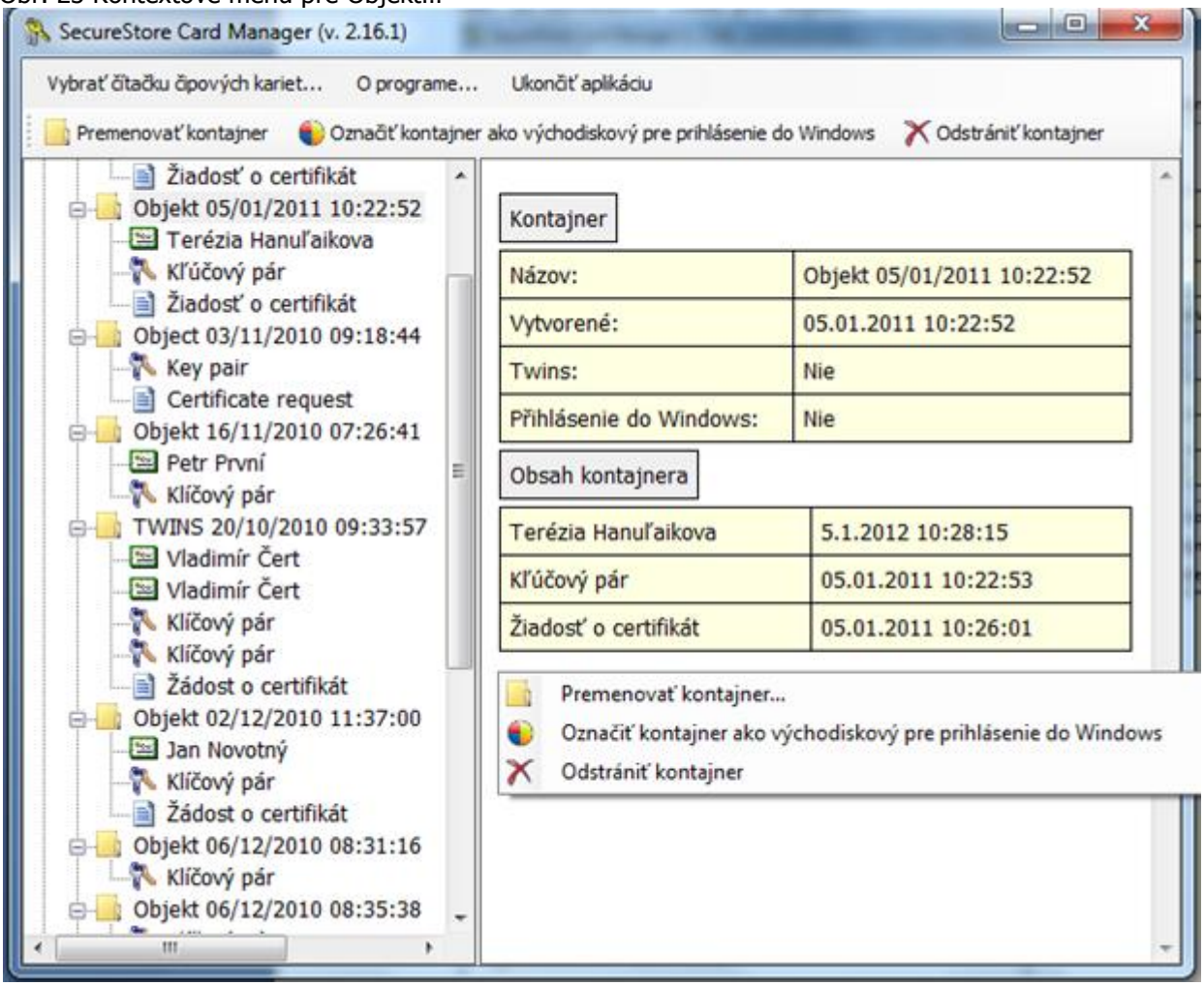
Voľba importuje na kartu kľúče, ktoré boli počas procesu generovania žiadosti o šifrovací certifikát uložené na disk.

7.2.5 Import páru kľúčov (PKCS#12)...

Voľba importuje na kartu kľúče, ktoré sú uložené vo formáte PKCS#12 na disku.

7.3 Kontextové menu pre Objekt

Obr. 23 Kontextové menu pre Objekt…



7.3.1 Premenovať kontajner

Voľba umožňuje premenovanie vybraného kontajneru.

7.3.2 Označiť kontajner ako východiskový na prihlásenie do Windows

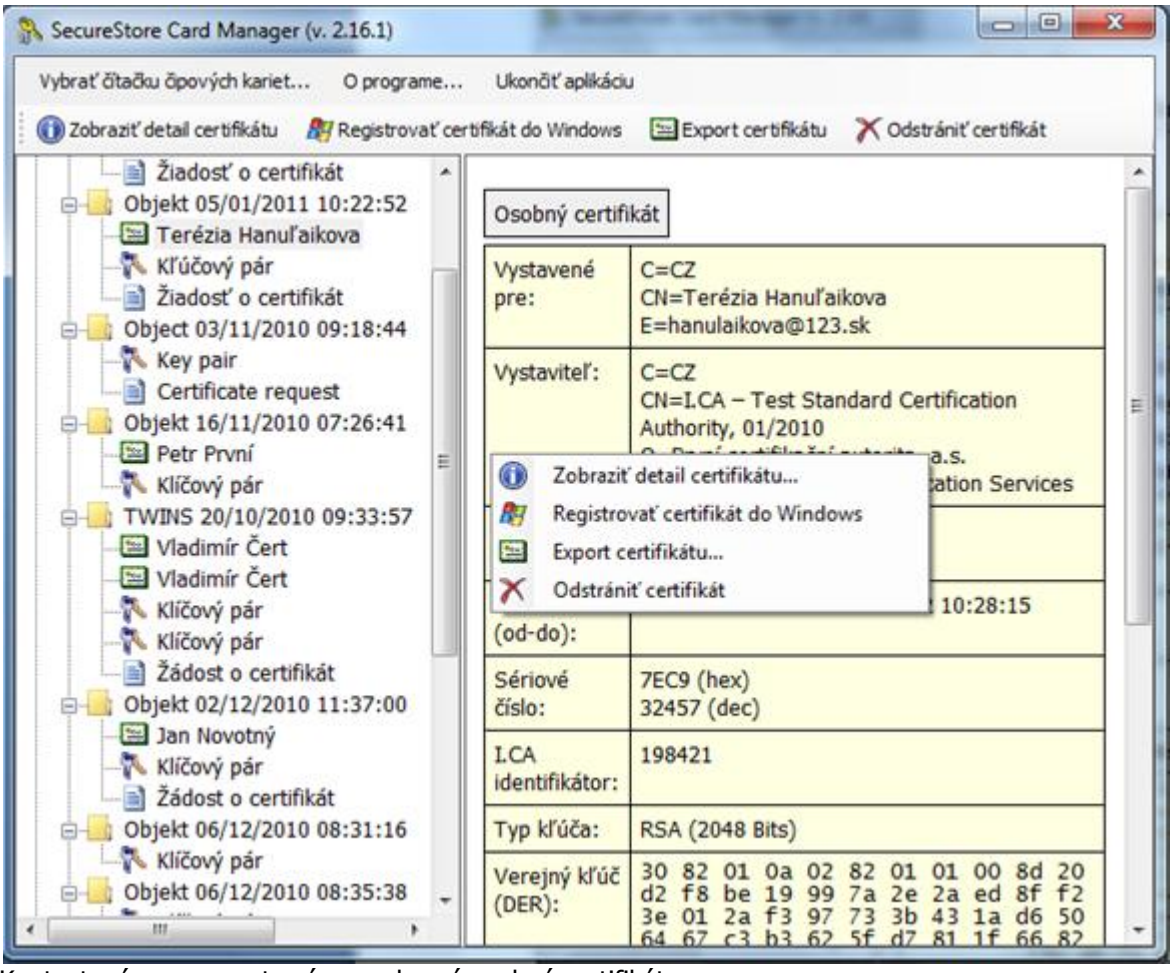
Voľba umožňuje označiť vybraný kontajner ako východiskový na prihlásenie do Windows. Certifikát a kľúč v tomto kontajneri sa použijú pri prihlasovaní do Windows.

7.3.3 Odstrániť kontajner

Voľba umožňuje zmazať z karty kontajner včítane certifikátu a kľúčov, ktoré obsahuje.

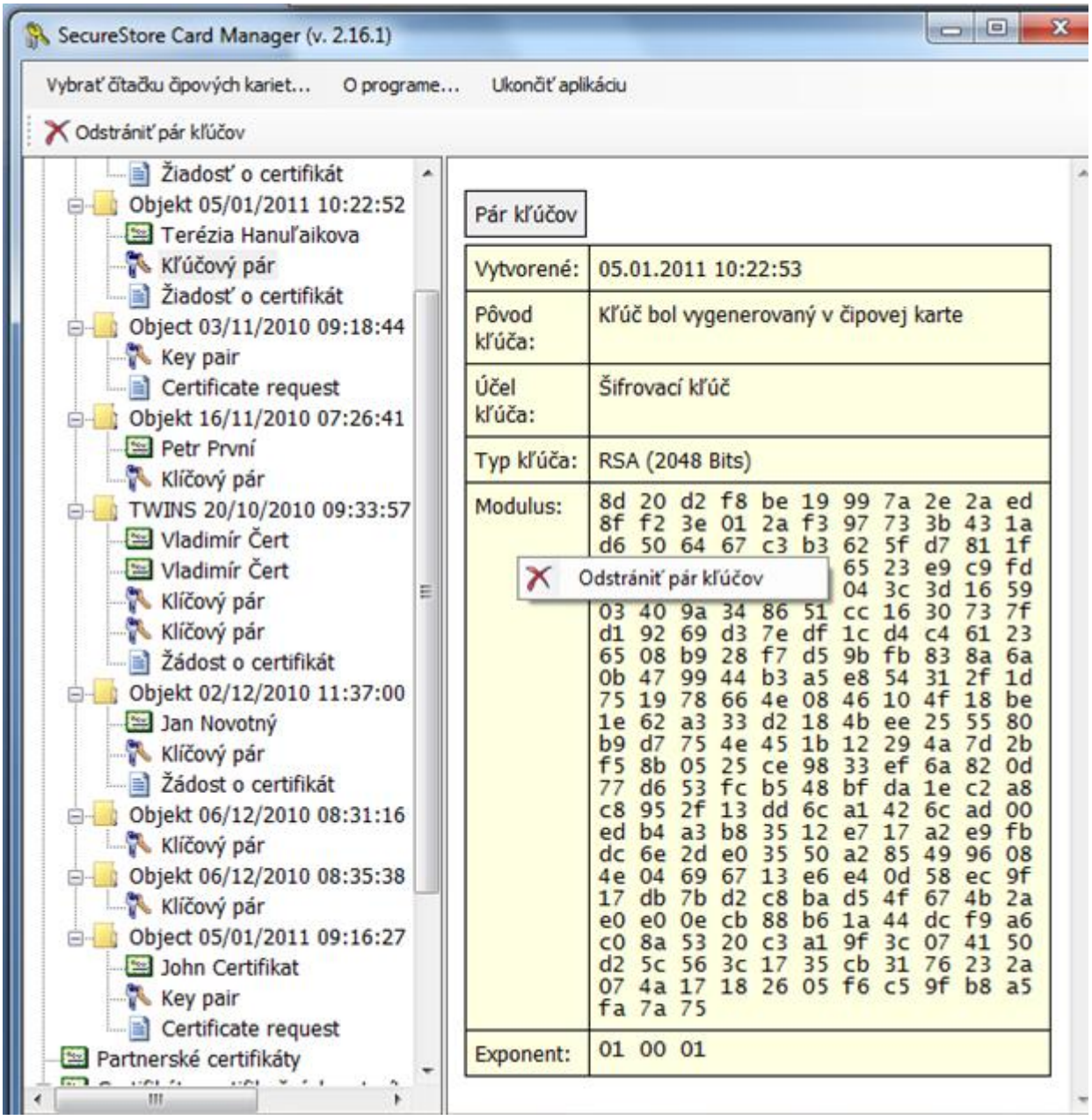
7.4 Kontextové menu pre osobný certifikát

Obr. 24 Kontextové menu pre osobný certifikát.

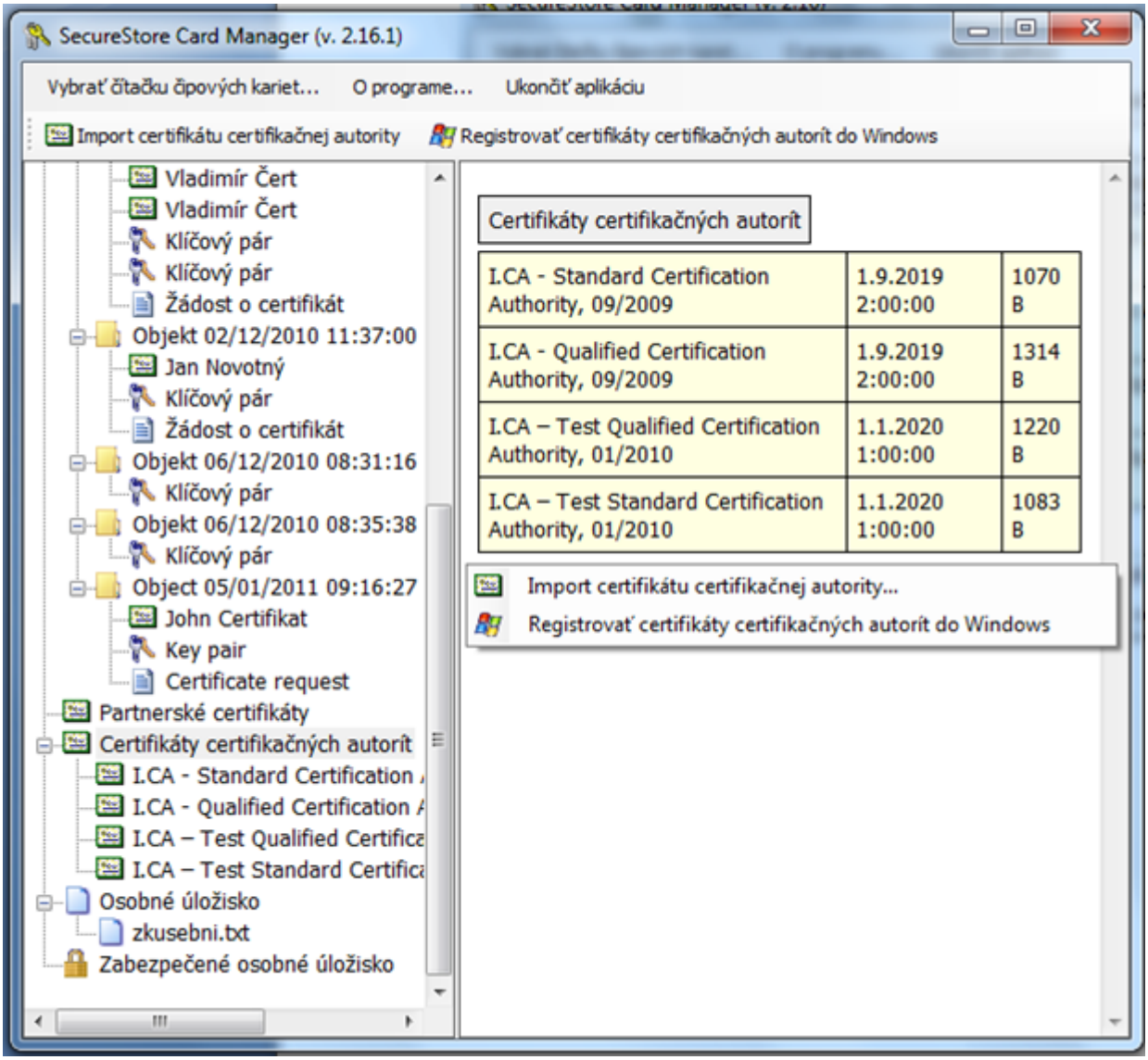


Kontextové menu sa otvorí pre vybraný osobný certifikát.

7.5 Kontextové menu pre kľúčový pár



7.6 Kontextové menu pre zložku certifikáty CA



8. Pojmy

- Certifikačná autorita
  ... je nezávislý dôveryhodný subjekt, ktorý klientovi vydáva certifikát. Certifikačná autorita garantuje jednoznačnú väzbu medzi klientom a jeho certifikátom.

- Registračná autorita
  ... je kontaktné pracovisko, ktoré slúži na komunikáciu s klientmi. Zabezpečuje najmä prijímanie žiadostí o certifikáty a ich následné odovzdávanie klientom. Toto pracovisko vykonáva overovanie totožnosti žiadateľa o certifikát a zhodu žiadosti s predloženými dokladmi. Registračné autority nevydávajú certifikáty, iba o ne žiadajú na centrálnom pracovisku I.CA.

- Kryptografické operácie
  ... sú operácie využívajúce kľúče na šifrovanie a dešifrovanie. V prípade čipovej karty sa využíva tzv. asymetrická kryptografia, t.j. pomocou dvojice kľúčov sa vykonáva šifrovanie, dešifrovanie a vytvára sa a overuje elektronický podpis.

- Elektronický podpis
  ... predstavuje údaje v elektronické podobe, ktoré sú pripojené k dátovej správe, alebo sú s ňou logicky spojené a umožňujú overenie totožnosti podpísanej osoby vo vzťahu k podpísanej správe.

- Dáta na tvorbu elektronického podpisu
  ... sú jedinečné dáta, ktoré podpisujúca osoba používa na vytváranie elektronického podpisu (v zmysle zákona o elektronickom podpise); ide o súkromný kľúč príslušného asymetrického kryptografického algoritmu (tu RSA).

- Čipová karta
  ... je prostriedok na bezpečné uloženie súkromného kľúča používateľa a prostriedok na vytváranie elektronického podpisu. Na čipovej karte sú okrem súkromných kľúčov uložené aj certifikáty klienta, certifikáty certifikačných autorít a môžu tu byť aj ďalšie dáta.

- PIN a PUK
  ... je ochrana prístupu ku karte, t.j. pri zápise na kartu alebo pri používaní súkromných kľúčov z karty. Ochranné kódy môžu byť na karte vopred nastavené a používateľ dostane tieto hodnoty v tzv. pinovej obálke, alebo si klient sám nastavuje hodnoty PINu a PUKu na karte.

- Pinová obálka
  ... je list, ktorý klient môže prijať spolu s kartou. Pinová obálka náleží ku konkrétnej karte, obsahuje jednoznačnú identifikáciu karty a hodnoty PINu a PUKu. Pinová obálka sa nedodáva ku každej karte.

- Úložisko
  ... je pamäťový priestor na médiu (disku, čipovej karte), kde je uložený pár kľúčov spolu s certifikátom. Na čipovej karte môže existovať naraz až 8 rôznych úložísk. Úložisko na čipovej karte má svoje jednoznačné meno. Úložisko typu PODPIS nepovoľuje vytvárať zálohy kľúčov pri generovaní žiadosti o certifikát. Všetky certifikáty, u ktorých sa vytvára záloha kľúčov, sa preto ukladajú do úložísk typu OSTATNÉ.

- Žiadosť o certifikát
  ... vzniká na základe vyplnenia formulára, ktorý obsahuje údaje o žiadateľovi. K informáciám, ktoré žiadateľ vyplní do formulára žiadosti, je pripojený vygenerovaný verejný kľúč žiadateľa a celá táto štruktúra je podpísaná súkromným kľúčom žiadateľa. Žiadosť o certifikát predstavuje digitálne dáta, ktoré obsahujú všetky informácie potrebné na vydanie certifikátu. Žiadosť o certifikát si používateľ môže vytvoriť pomocou programu ComfortChip alebo na www stranách I.CA www.ica.cz.

- Certifikát
  ... je obdobou preukazu totožnosti, klient sa ním preukazuje pri elektronickej komunikácii. Získanie certifikátu sa veľmi približuje štandardným postupom získania občianskeho preukazu. I.CA tieto služby zabezpečuje prostredníctvom siete kontaktných pracovísk - registračných autorít, ktoré realizujú požiadavky svojich klientov. Certifikát je jednoznačne zviazaný s párom kľúčov, ktorý používateľ používa v elektronickej komunikácii. Pár kľúčov sa vytvára tzv. verejným kľúčom a súkromným kľúčom.

- Verejný kľúč
  ... je verejná časť páru kľúčov používateľa, je určená na overovanie elektronického podpisu a prípadne na šifrovanie.

- Súkromný kľúč
  ... je tajná časť páru kľúčov používateľa, je určená na vytváranie elektronického podpisu a prípadne na dešifrovanie. Vzhľadom na použitie súkromného kľúča je treba zaistiť čo najvyššiu bezpečnosť. Z tohto dôvodu sa na uchovanie kľúča využíva čipová karta. Súkromný kľúč, používaný na dešifrovanie, je potrebné uchovávať po celý čas existencie šifrovaných dokumentov a správ. Tento kľúč si môže používateľ uchovať na karte, ale zároveň odporúčame, aby sa uchovával aj na záložnom médiu.

- Obdobie platnosti certifikátu
  Každý certifikát sa vydáva na určité obdobie. Obdobie platnosti je uvedené v každom certifikáte. Certifikát, ktorý sa používa na elektronický podpis, je po skončení obdobia platnosti nepotrebný. Certifikát, ktorý sa používa na šifrovanie, je nutné uchovať aj po skončení obdobia platnosti na dešifrovanie starších správ.

- Komerčný certifikát standard
  Certifikáty standard predstavujú osobné certifikáty vhodné na bežné využitie. Vydávajú sa fyzickým alebo právnickým osobám na základe riadne vyplnenej žiadosti o certifikát odovzdanej kontaktnému pracovisku I.CA spolu s predložením požadovaných dokladov na nevyhnutné overenie totožnosti žiadateľa.

- Komerčný certifikát comfort
  Certifikáty comfort predstavujú osobné certifikáty, ktorých hlavnou odlišnosťou od certifikátov standard je čipová karta, ktorá je súčasťou tejto služby. Slúži ako médium na bezpečné uloženie dát na tvorbu elektronického podpisu a bezpečné vytváranie elektronického podpisu. Táto služba je určená predovšetkým pre firemné účely, poskytuje sa však fyzickým aj právnickým osobám.

- Kvalifikovaný certifikát
  ... sa striktne riadi zákonom č. 227/2000 Zb. a slúži výhradne pre oblasť elektronického podpisu. Vytváranie, správa a použitie kvalifikovaného certifikátu sa riadi osobitnými príslušnými certifikačnými politikami.

- Klientsky Komerčný certifikát
  ... sa vydáva fyzickým alebo právnickým osobám na základe riadne vyplnenej žiadosti o certifikát odovzdanej kontaktnému pracovisku I.CA spolu s predložením požadovaných dokladov na nevyhnutné overenie totožnosti žiadateľa. Dĺžka platnosti tohto certifikátu vždy závisí od dĺžky použitého kryptografického kľúča.

- Klientsky certifikát
  ... certifikát vydaný klientovi I.CA na základe riadne vyplnenej žiadosti o certifikát odovzdanej kontaktnému pracovisku I.CA, spolu s predložením požadovaných dokladov na nevyhnutné overenie totožnosti žiadateľa. V prípade I.CA sa môže jednať buď o komerčný alebo kvalifikovaný certifikát.

- Certifikát certifikačnej autority
  ... sa používa na overovanie správnosti a dôveryhodnosti klientskych certifikátov. Jeho inštaláciou na svoj PC používateľ deklaruje operačnému systému svoju dôveru v takúto certifikačnú autoritu. V praxi to znamená, že ak príde používateľovi správa, ktorá je elektronicky podpísaná

certifikátom vydaným práve touto certifikačnou autoritou, systém ho chápe ako dôveryhodný. V ostatných prípadoch sa správa javí ako nedôveryhodná.

- Certifikát na prihlásenie do Windows
  Certifikát na prihlásenie do Windows musí obsahovať špecifické údaje. Na prihlásenie do Windows nemožno preto použiť akýkoľvek certifikát. Registračná autorita I.CA na požiadanie zabezpečí vydanie správneho certifikátu na prihlasovanie. Úložisko na karte obsahujúce certifikát na prihlásenie musí byť označené pre autentizáciu. Pre autentizáciu môže byť na karte označené práve jedno úložisko.

- Zoznam verejných certifikátov (komerčných)
  ... je zoznam certifikátov vydaných I.CA, v prípade ktorých ich majitelia súhlasili so zverejnením. Nie sú tu certifikáty typu "testovacie" a certifikáty, so zverejnením ktorých ich majiteľ nesúhlasil.

- Zoznam verejných certifikátov (kvalifikovaných)
  ... je zoznam kvalifikovaných certifikátov vydaných I.CA. V prípade týchto certifikátov je ich zverejnenie dané zákonom 227/2000 Zb., o elektronickom podpise.

- Certifikačné autority podporované kartou
  Každá čipová karta vydaná I.CA má definovaný zoznam tzv. podporovaných certifikačných autorít, ktorých certifikáty možno na kartu uložiť.

- Obnova certifikátu - „následný" certifikát
  ... je vydaný klientovi po uplynutí doby platnosti prvotného certifikátu. Následný certifikát je vydaný iba v prípade, že klient nepožaduje zmenu položiek predošlého certifikátu. Ak ju požaduje, nejedná sa o certifikát následný, ale o ďalší prvotný certifikát. Pri vydávaní následného certifikátu pred vypršaním platnosti prvotného certifikátu už nie je nutná prítomnosť zákazníka na registračnej autorite I.CA. Klient iba zašle s využitím platného certifikátu elektronicky podpísanú žiadosť o vydanie následného certifikátu v štandardizovanej elektronické podobe.

- Použitie kľúča
  - **DigitalSignature (digitálny podpis)** - primárne sa tento príznak (bit) nastavuje, ak sa má certifikát použiť v súvislosti s digitálnym podpisom s výnimkou zabezpečenia nepopierateľnosti, podpisov certifikátov a zoznamov zneplatnených certifikátov certifikačnou autoritou.
    Použitie: tento bit je nutné v súčasnej dobe nastaviť v prípadoch, kedy používateľ zamýšľa používať svoj súkromný kľúč spojený s vydaným certifikátom všeobecne na vytváranie digitálneho podpisu (napr. pri použití certifikátu v rámci bezpečnej elektronickej pošty).
  - **NonRepudiation (nepopierateľnosť)** - tento príznak sa nastavuje, ak sa má verejný kľúč (prostredníctvom overenia digitálneho podpisu) použiť na preukázanie zodpovednosti za určitú akciu podpisujúcej osoby.
    Použitie: tento bit je nutné v súčasnej dobe nastaviť najmä v prípadoch kvalifikovaných certifikátov, kedy používateľ zamýšľa používať svoj súkromný kľúč spojený s vydaným certifikátom na vytváranie elektronického podpisu.
  - **KeyEncipherment (šifrovanie kľúča)** - tento príznak sa nastavuje, ak sa má verejný kľúč použiť na prenos kryptografických kľúčov.
    Použitie: tento bit je nutné nastaviť, ak používateľ zamýšľa použiť certifikát na účely šifrovania v rámci bezpečnej elektronické pošty. V prostredí MS Outlook je takisto nutné tento bit nastaviť v prípade, ak používateľ nemá iný certifikát, ktorý možno použiť na šifrovanie.
  - **DataEncipherment (šifrovanie dát)** - tento príznak sa nastavuje, ak sa má verejný kľúč použiť na šifrovanie dát (s výnimkou kryptografických kľúčov).
    Použitie: všeobecne je nutné nastaviť tento bit, ak sa bude verejný kľúč obsiahnutý v certifikáte používať na šifrovanie všeobecných dát, napr. dokumentov. Na účely bezpečnej elektronickej pošty ho nie je nutné nastavovať.

- Formát PKCS#12
  RSA kľúče a certifikát možno uložiť do jedného súboru v tzv. formáte PKCS#12, ktorý je definovaný normou PKCS#12. V tomto formáte možno napr. exportovať RSA kľúče a certifikát z úložiska Windows, ak je povolený export súkromného kľúča. Obsah súboru je chránený heslom. Súbor má príponu pfx alebo p12.