

SecureStore I.CA

Uživatelská příručka

Verze 2.16 a vyšší

Obsah

1.	ÚVOD	3
2.	PŘÍSTUPOVÉ ÚDAJE KE KARTĚ	3
2.1	Inicializace karty	3
3.	ZÁKLADNÍ OBRAZOVKA	3
4.	ZOBRAZENÍ INFORMACÍ O PÁRU KLÍČŮ.....	6
5.	CERTIFIKÁTY	7
5.1	Zobrazení certifikátu	7
5.2	Práce s osobním certifikátem	7
5.3	Práce s kořenovým certifikátem CA.....	8
5.4	Registrace osobního certifikátu do Windows	9
6.	OSOBNÍ ÚLOŽIŠTĚ.....	10
7.	OVLÁDÁNÍ APLIKACE.....	11
7.1	Kontextové menu pro Informace o kartě	11
7.2	Kontextové menu pro složku Osobní certifikáty.....	12
7.2.1	Vytvořit žádost o certifikát.....	12
7.2.2	Import osobního certifikátu	14
7.2.3	Registrovat osobní certifikáty od Windows.....	15
7.2.4	Import páru klíčů ze zálohy (PKCS#8).....	15
7.2.5	Import páru klíčů (PKCS#12).....	15
7.3	Kontextové menu pro Objekt	16
7.3.1	Přejmenovat kontejner.....	16
7.3.2	Označit kontejner jako výchozí pro přihlášení do Windows	16
7.3.3	Odstranit kontejner.....	16
7.4	Kontextové menu pro osobní certifikát	17
7.5	Kontextové menu pro klíčový pár	18
7.6	Kontextové menu pro složku certifikáty CA	18
8.	POJMY.....	19

1. Úvod

Uživatelská příručka je platná pro aplikaci SecureStore verze 2.16. Uvedené verze mají stejnou funkčnost a totožné uživatelské rozhraní.

2. Přístupové údaje ke kartě

Přístup k čipové kartě je chráněn pomocí PINu, podobně jako je tomu např. u platebních karet. PIN je 4-8 místné číslo. Pokud při zadávání PINu 3krát za sebou zadáte chybnou hodnotu PINu, bude PIN automaticky zablokován.

K odblokování PINu je určena hodnota PUK.

PUK je 4-8 místné číslo. Pokud při zadávání PUKu 5krát za sebou zadáte chybnou hodnotu PUKu, dojde k zablokování PUKu a tím i celé karty.

Část karty nazvaná „Zabezpečená osobní úložiště“ je určena pro uložení libovolných dat. Tato oblast je chráněna zvláštním PINem tzv. PINem pro zabezpečené úložiště. K odblokování PINu pro zabezpečená úložiště použijte PUK uvedený v předchozím odstavci.

PIN pro zabezpečená úložiště je 4-8 místné číslo.

2.1 Inicializace karty

Inicializace karty spočívá v nastavení PINu a PUKu.

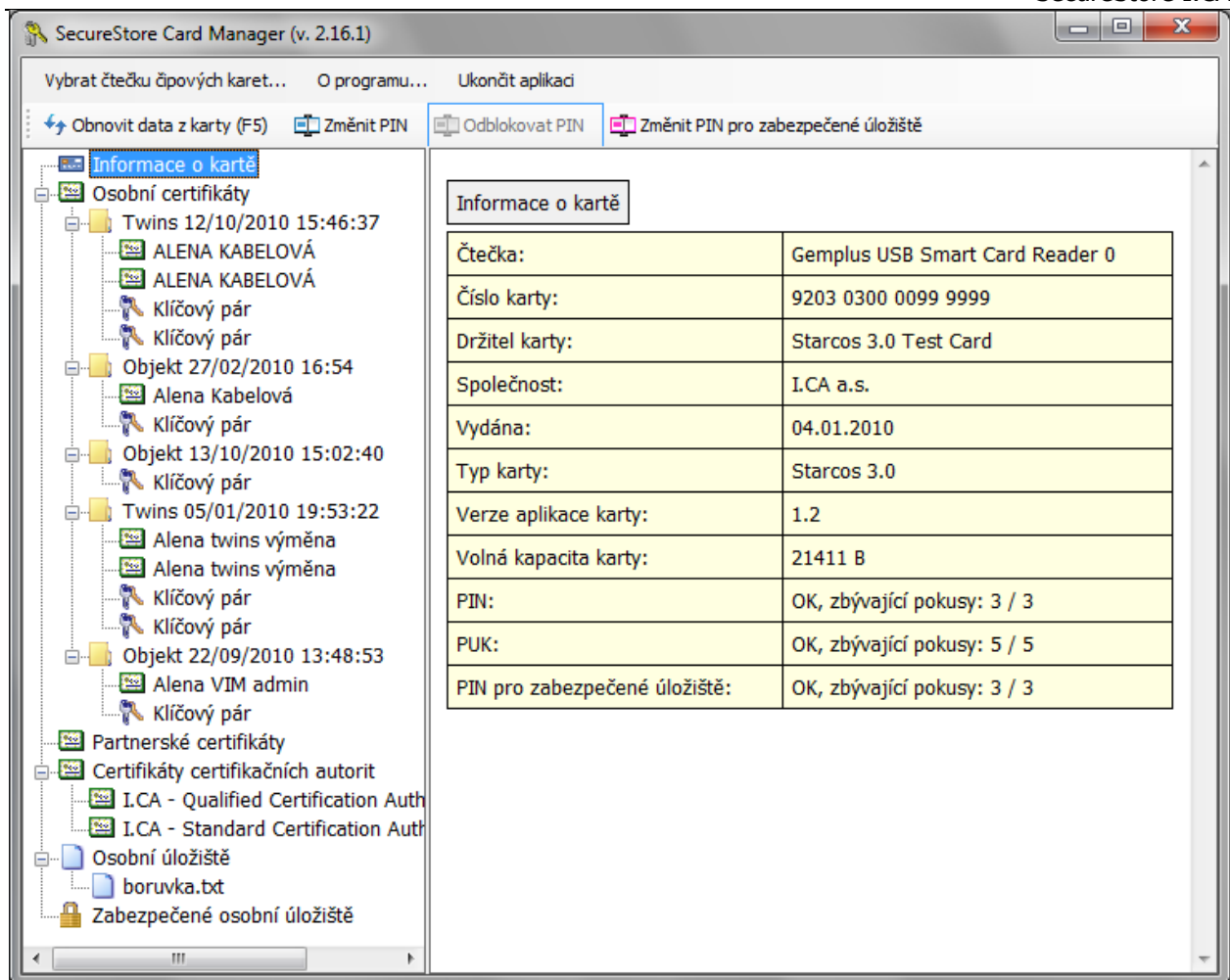
Pokud jste spolu s kartou obdrželi tzv. Pinovou obálku, pak byla již inicializace karty provedena a hodnoty PINu a PUKu jsou uvedeny v Pinové obálce.

Pokud jste Pinovou obálku neobdrželi, pak musíte při prvním použití nové karty nastavit hodnotu PINu a PUKu.

Dialog pro inicializaci karty se zobrazí automaticky zpravidla při prvním spuštění aplikace na nové kartě. PIN a PUK si pečlivě zapamatujte.

3. Základní obrazovka

Obr.1 Základní obrazovka



Základní obrazovka je rozdělená do dvou částí.

V levé části obrazovky se zobrazuje seznam objektů uložených na kartě.

V pravé části obrazovky se zobrazují základní informace o držiteli karty, o platnosti karty, o použité čtečce čipových karet a verze systému souborů karty.

V horní liště jsou uvedeny následující volby viz. obr. 3:

Obr.3 Hlavní lišta

Vybrat čtečku čipových karet... O programu... Ukončit aplikaci

Volba **„Vybrat čtečku čipových karet“** je užitečná, pokud máte k PC připojeno více čteček čipových karet současně. Pomocí volby můžete vybrat čtečku, se kterou chcete pracovat. U čtečky čipových karet, ve které je vložena karta, je zobrazeno číslo a typ čipové karty, viz následující obrázek.

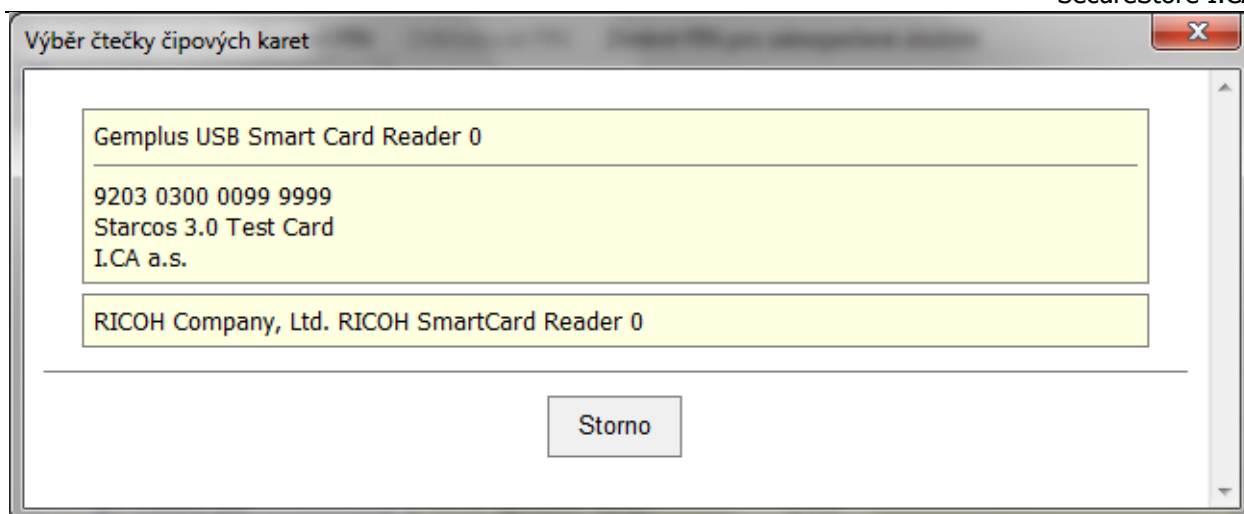
V případě, že máte k PC připojeno více čteček čipových karet, zobrazuje se okno „Výběr čteček čipových karet“ i po spuštění aplikace.

Volba **„O programu..“** zobrazí verzi aplikace.

Volba **„Ukončit aplikaci“**.

Volby v horní liště se nemění.

Obr. 2 Výběr čtečky čipových karet



V případě, že máte k PC připojenu pouze jednu čtečku čipových karet, není okno zobrazováno a informace o nalezené čtečce jsou uvedeny v prvním řádku úvodní obrazovky.

V nástrojové liště viz. obr. 4 se volby mění dle zvoleného objektu v levé části obrazovky.

Obr. 4 Nástrojová lišta

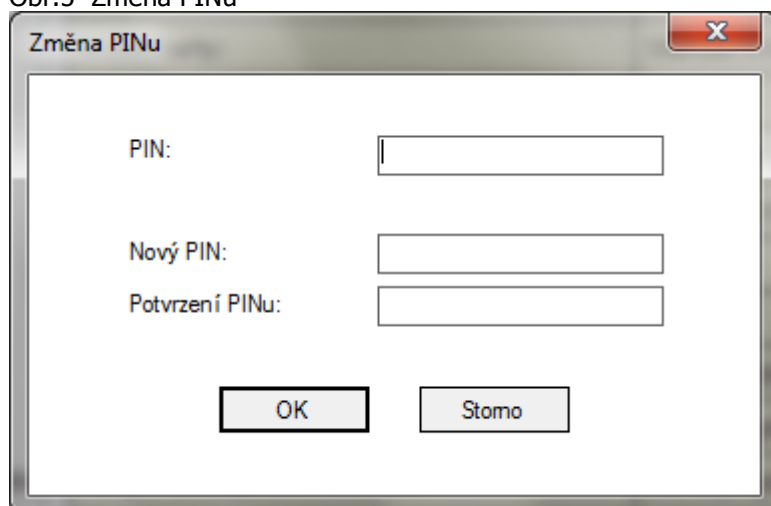


Příklad nástrojové lišty ukazuje volby platné pro celou „Informace o kartě“.

Volba „**Obnovit data z karty**“ opakovaně načte data z čipové karty. Stejnou funkci má klávesa F5.

Volba „**Změnit PIN**“ provedete změnu PINu ke kartě. Do dialogového okna pro změnu PINu zadejte stávající PIN a 2x PIN nový viz obr. 5.

Obr.5 Změna PINu



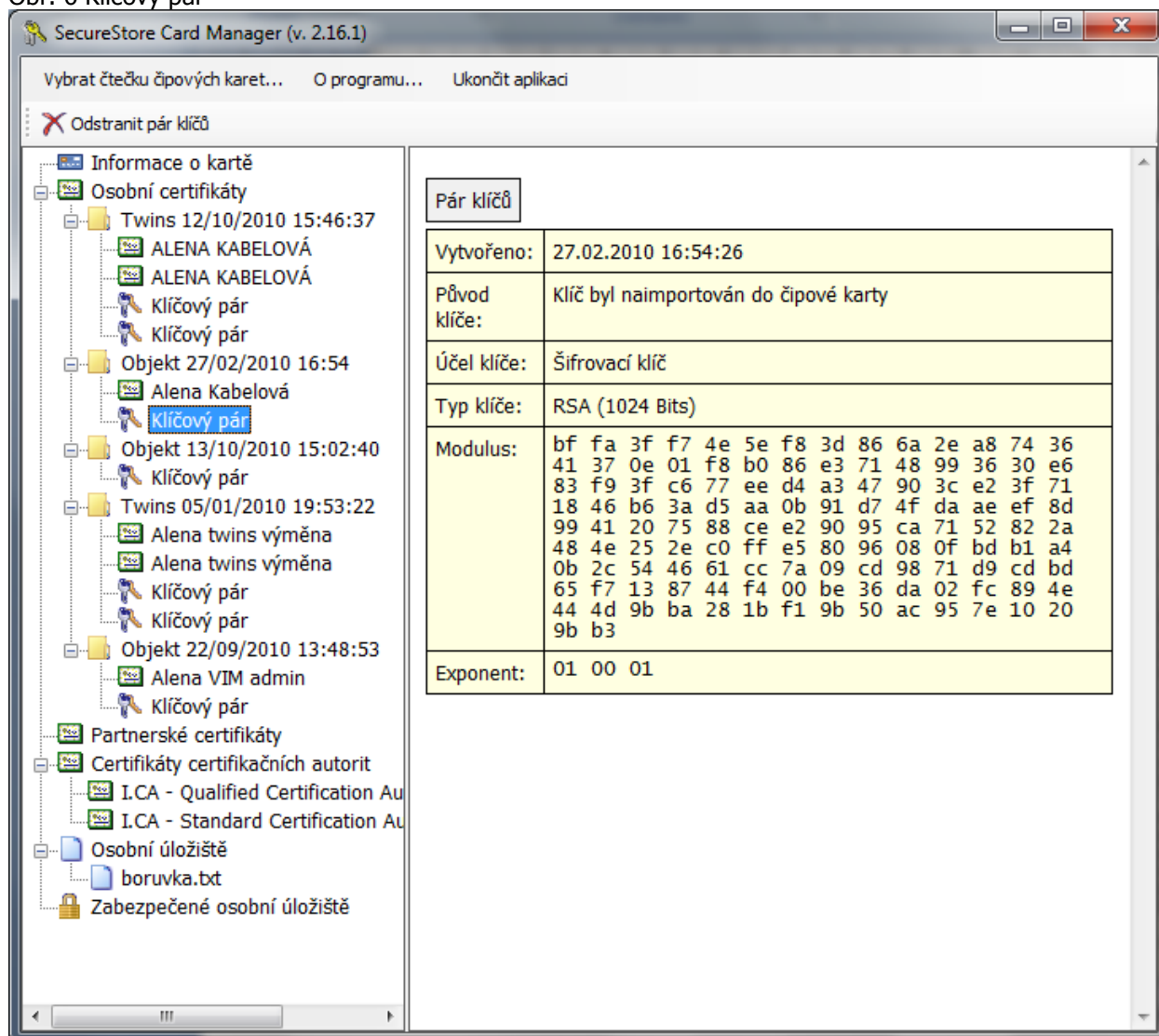
Volba „**Odblokovat PIN**“ umožňuje nastavit novou hodnotu PIN v případě, že si PIN zablokujete. K odblokování PINu je vyžadováno zadání PUKu.

Volba „**Změnit PIN pro zabezpečené úložiště**“ umožňuje změnit PIN pro speciální část karty nazvanou „Zabezpečená osobní úložiště“.

Volba „**Odblokovat PIN pro zabezpečené úložiště**“ umožňuje odblokovat PIN pro část karty nazvanou „Zabezpečená osobní úložiště“.

4. Zobrazení informací o páru klíčů

Obr. 6 Klíčový pár



V úložišti je uložen jeden pár klíčů pro certifikát, dva páry klíčů pro certifikáty typu Twins.

Čas vytvoření veřejného/privátního klíče udává přesný čas, kdy byl klíč vygenerován na kartě, nebo na kartu importován.

Způsob vzniku klíče na kartě zobrazuje položka „Původ klíče“.

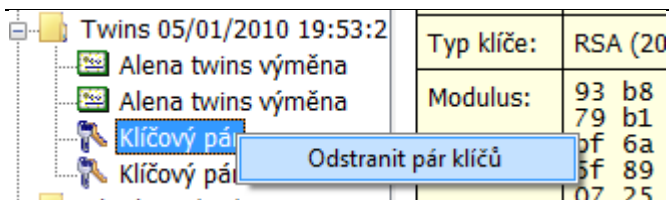
V položce „Účel klíče“ je uvedeno, zda se jedná o klíč šifrovací nebo podpisový.

Dále je uveden „Typ klíče“, v příkladu jde o klíč pro RSA algoritmus s délkou 2048 bitů.

Následuje hexadecimální výpis exponentu a modula veřejného klíče pro vizuální kontrolu.

Pár klíčů je možné z karty odstranit, pomocí volby „Odstranit pár klíčů“ v nástrojové liště. Volba je dostupná také v kontextovém menu, které se zobrazí po kliknutí pravým tlačítkem myši na daném klíčovém páru, viz následující obrázek.

Obr. 7 Odstranit pár klíčů

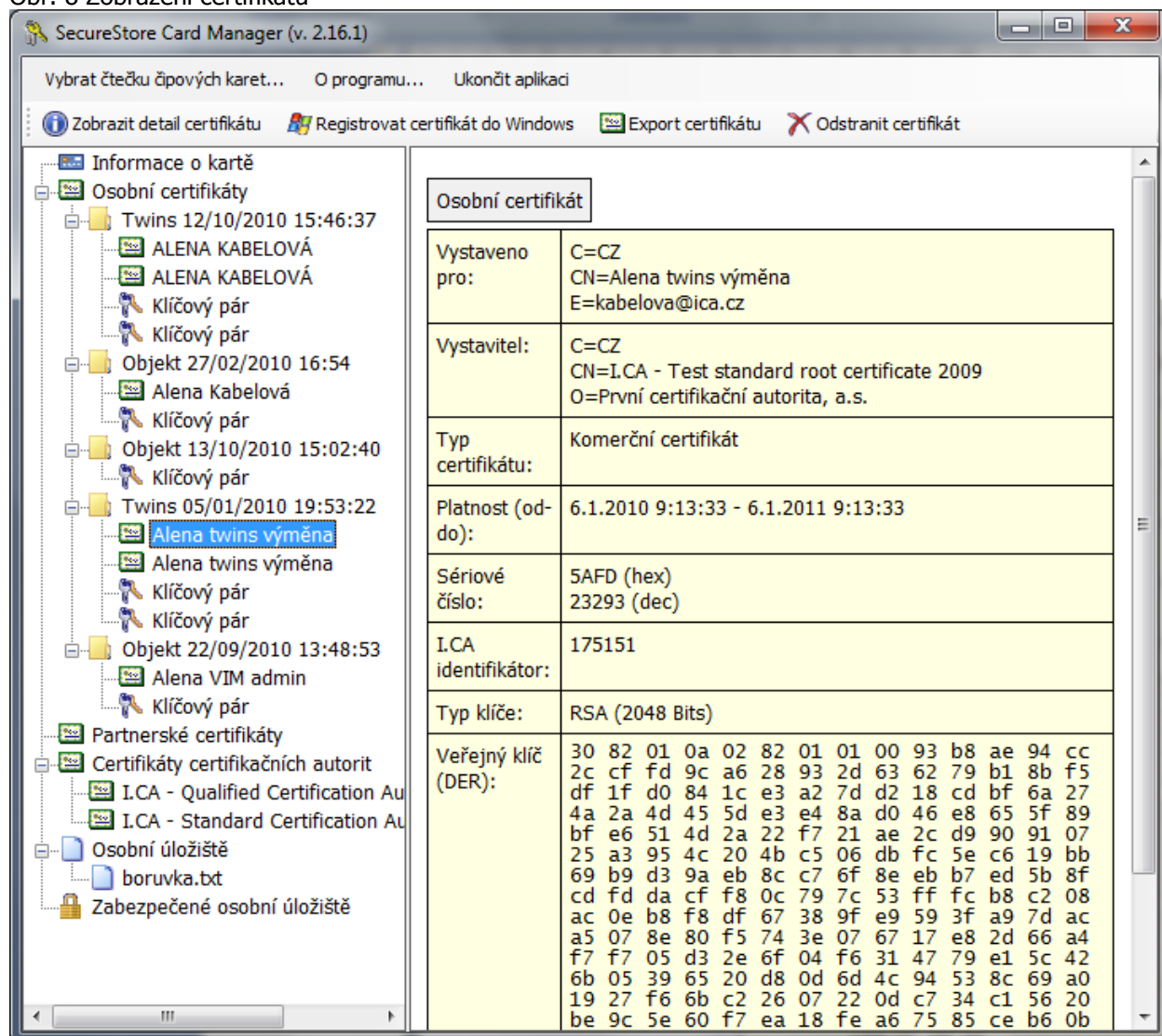


Volba „Odstranit pár klíčů“ nevratně odstraní pár klíčů z karty (tj. bude smazán jak privátní, tak veřejný klíč). Pokud je odstraněn privátní klíč k osobnímu certifikátu, nepůjde již certifikátem podepisovat a dešifrovat!!!

5. Certifikáty

5.1 Zobrazení certifikátu

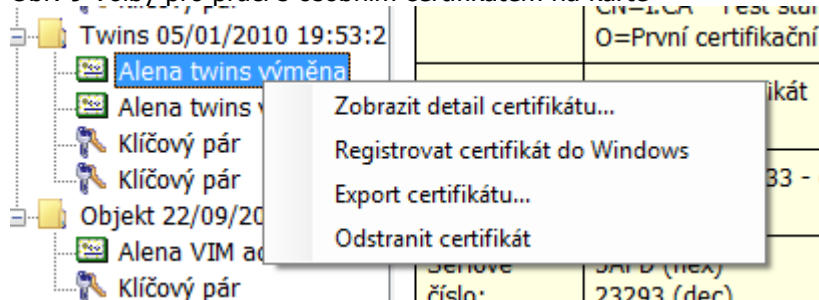
Obr. 8 Zobrazení certifikátu



5.2 Práce s osobním certifikátem

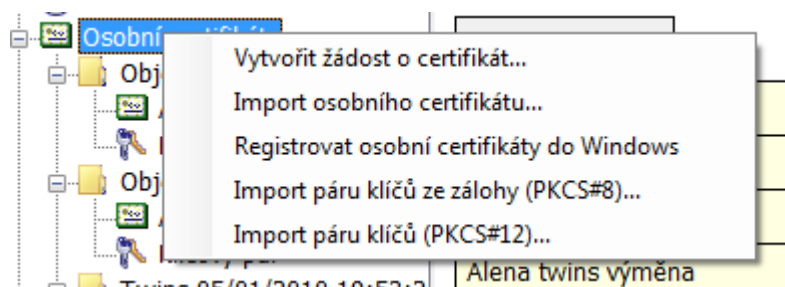
Volby pro práci s certifikátem uloženým na kartě jsou dostupné v nástrojové liště viz. obr. 8 nebo po kliknutí pravým tlačítkem myši na daném certifikátu, viz následující obrázek.

Obr. 9 Volby pro práci s osobním certifikátem na kartě



Volby pro import certifikátu na kartu jsou dostupné po kliknutí pravým tlačítkem myši na položce osobní certifikáty, viz následující obrázek.

Obr. 10 Volby pro import a registraci osobního certifikátu



Osobní certifikát je importován do úložiště, ve kterém je uložen odpovídající pár klíčů. Pokud takové úložiště na kartě neexistuje, bude certifikát importován do části karty nazvané „Partnerské certifikáty“

Jako partnerské certifikáty jsou importovány ty certifikáty, ke kterým nemáte soukromý klíč nebo které nejsou považovány za důvěryhodné certifikáty CA.

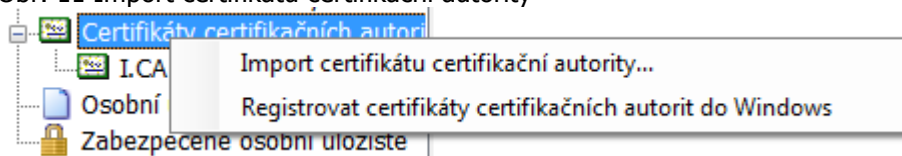
Zobrazení holých dat certifikátu slouží pouze pro odborníky pro vizuální kontrolu dat certifikátu.

5.3 Práce s kořenovým certifikátem CA

Nová karta obsahuje potřebné kořenové certifikáty certifikační autority, které jsou uloženy v části „Certifikáty certifikačních autorit“.

Importovat certifikát jako certifikát CA lze pouze tehdy, jedná-li se o certifikát povolené CA pro danou kartu. Certifikáty dalších CA nebo nově vydané certifikáty CA je možné importovat ve formátu cmf. Certifikáty I.CA ve formátu cmf jsou ke stažení na www.ica.cz.

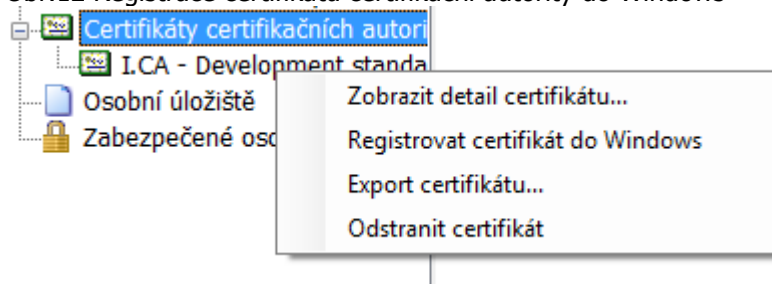
Obr. 11 Import certifikátu certifikační autority



Kořenové certifikáty se používají pro ověření důvěryhodnosti osobních certifikátů. Pro práci s certifikáty je potřeba, aby kořenové certifikáty byly registrovány ve Windows a systém Windows tak mohl ověřit důvěryhodnost certifikátů použitých pro podpis nebo šifrování.

Pokud používáte starší verzi Windows a kořenové certifikáty I.CA nejsou součástí Windows, registrujte si kořenový certifikát z karty. K registraci použijte volbu „Registrovat certifikát do Windows“, viz obrázek obr.12. Registrace kořenového certifikátu do Windows vyžaduje váš souhlas, následně je kořenový certifikát registrován do MS Windows jako důvěryhodný kořenový certifikát.

Obr.12 Registrace certifikátu certifikační autority do Windows



Hromadnou registraci kořenových certifikátů umožňuje volba tlačítka „Registrovat certifikáty certifikačních autorit do Windows“ viz obrázek obr. 11.

5.4 Registrace osobního certifikátu do Windows

Většina aplikací vyžaduje, aby byl osobní certifikát, se kterým chcete pracovat, registrovaný ve Windows.

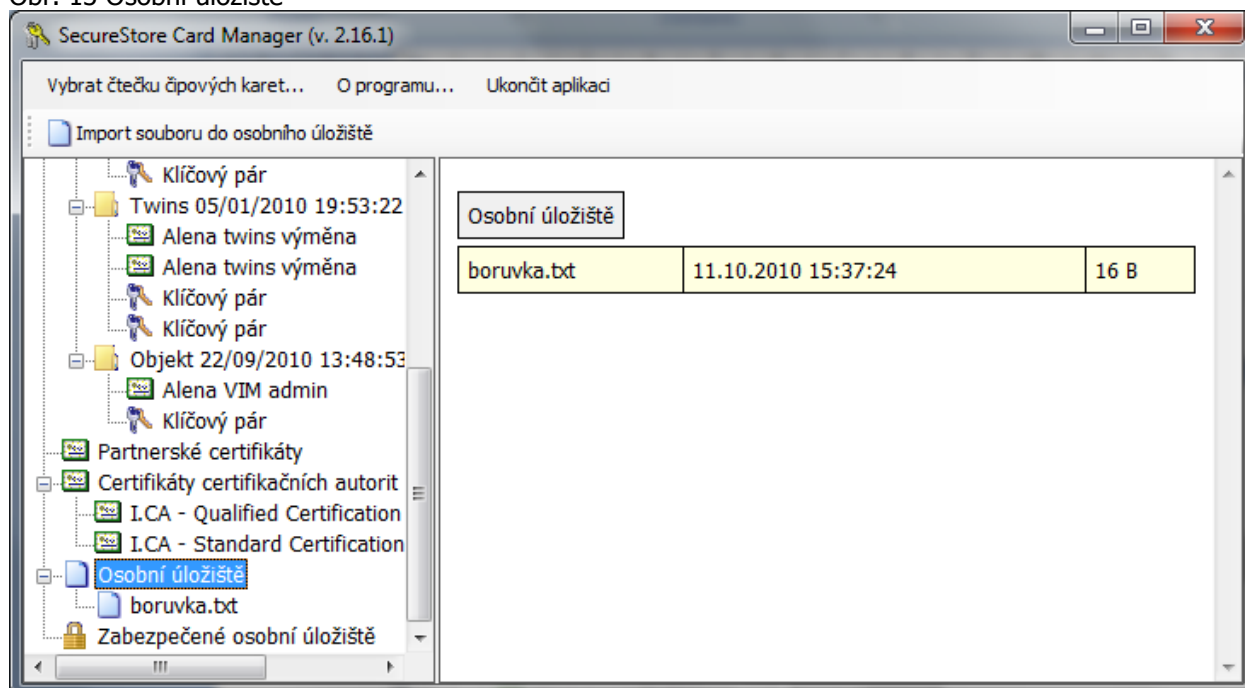
Registraci certifikátů je možno provést jednotlivě pro každý certifikát pomocí volby „Registrovat certifikát do Windows“, viz obrázek obr. 9.

Registrace jednotlivého certifikátu do MS Windows uloží certifikát do úložiště certifikátů MS Windows. V případě osobního certifikátu probíhá export do úložiště osobních certifikátů. Při exportu je exportován certifikát bez soukromého klíče. Soukromý klíč zůstává na kartě a nikdy ji neopustí.

Hromadnou registraci osobních certifikátů umožňuje volba „Registrovat osobní certifikáty do Windows“ viz obrázek obr.10.

6. Osobní úložiště

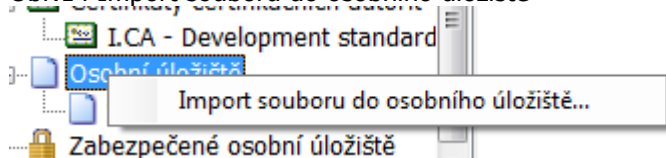
Obr. 13 Osobní úložiště



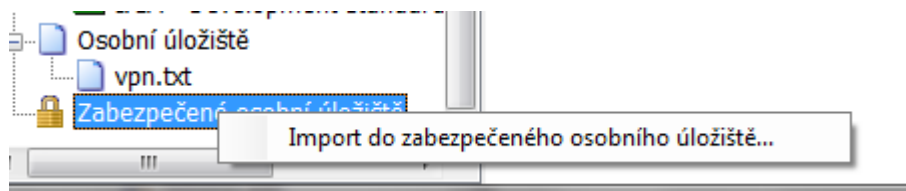
Do části karty nazvané „Osobních úložiště“ resp. „Zabezpečená osobní úložiště“ si můžete ukládat malé soubory (několik málo kB). Na kartu lze uložit jak textový, tak binární soubor.

Čtení a export souboru v zabezpečeném úložišti je chráněn PINem pro zabezpečené úložiště.

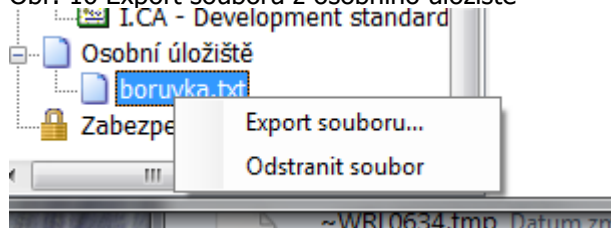
Obr.14 Import souboru do osobního úložiště



Obr.15 Import souboru do zabezpečeného úložiště



Obr. 16 Export souboru z osobního úložiště



Pro odstranění souboru v zabezpečeném úložišti je zapotřebí zadat PIN karty.

7. Ovládání aplikace

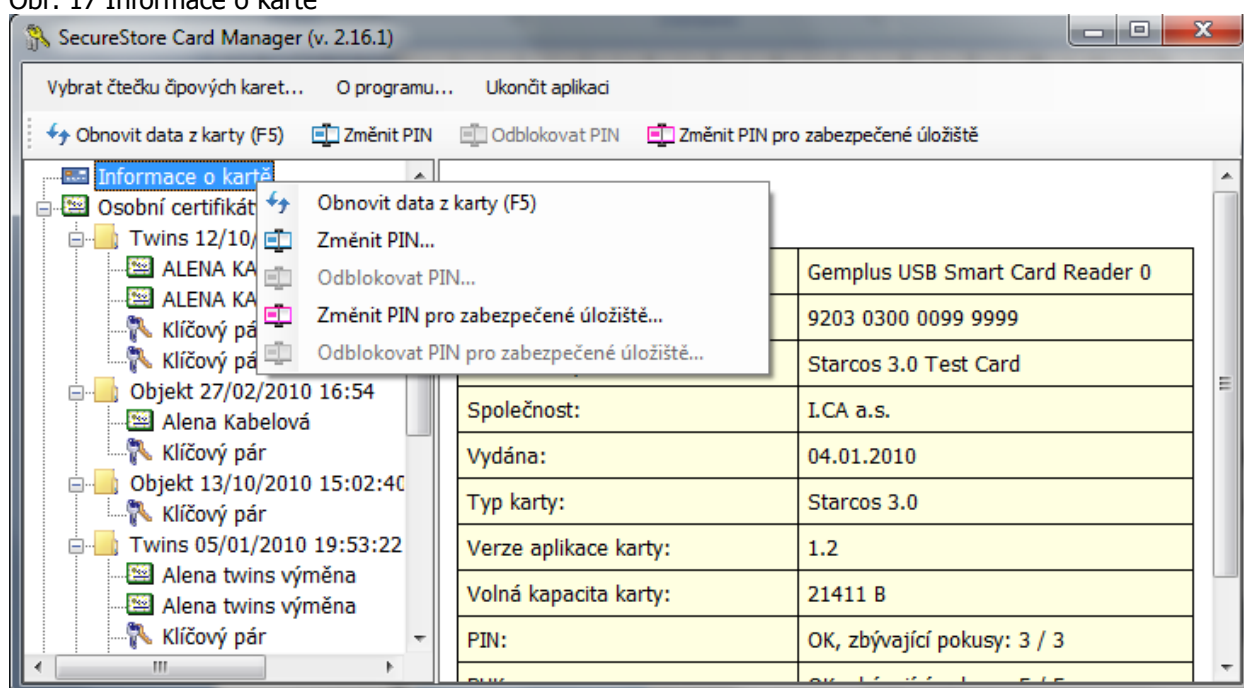
Jednotlivé funkce aplikace jsou realizovány pomocí kontextových menu. Kontextové menu se otevře

- po kliknutí pravým tlačítkem na položce stromu v levé části obrazovky nebo
- po kliknutí pravým tlačítkem nad pravou částí obrazovky

7.1 Kontextové menu pro Informace o kartě

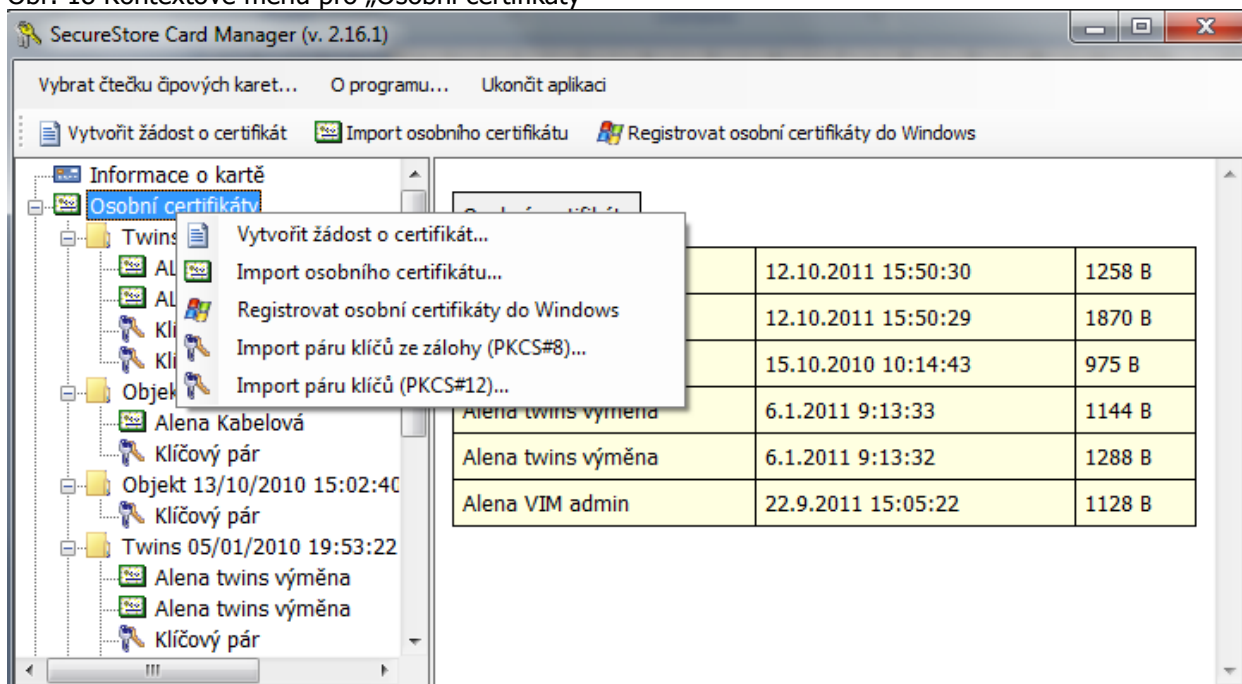
Kontextové menu položky „Informace o kartě“ obsahuje základní administrativní operace nad kartou související se správou PINu a PUKu a opakovaným načtením dat z karty.

Obr. 17 Informace o kartě



7.2 Kontextové menu pro složku Osobní certifikáty

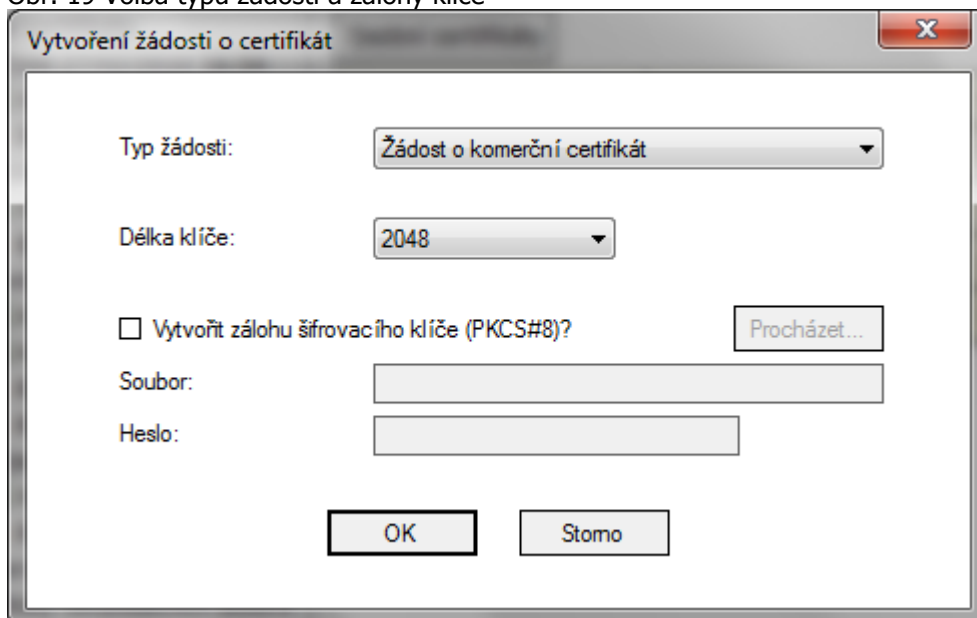
Obr. 18 Kontextové menu pro „Osobní certifikáty“



7.2.1 Vytvořit žádost o certifikát

Volba vytvořit žádost o certifikát umožňuje definovat naplnění žádosti o certifikát a generování páru klíčů.

Obr. 19 Volba typu žádosti a zálohy klíče



Pro certifikáty I.CA je požadován klíč o délce 2048 bitů.

Klíče šifrovací je možné generovat se zálohou, která se uloží mimo kartu. Záloha klíčů bude uložena do zabezpečeného PKCS#8 souboru s heslem, které zadáte v okně viz. obrázek obr. 17. Pro šifrovací certifikát doporučujeme zatrhnout volbu „Vytvořit zálohu šifrovacího klíče (PKCS#8)“.

Podepisovací klíče jsou generovány přímo na kartě. Vlastnosti karty zajišťují, že privátní klíč není možno z karty exportovat.

Po potvrzení tohoto dialogu z obr. 19 budou generovány klíče. Generování klíčů může trvat desítky sekund až minutu.

Po vygenerování klíčů bude spuštěna aplikace NewCert, která vytvoří žádost o certifikát.

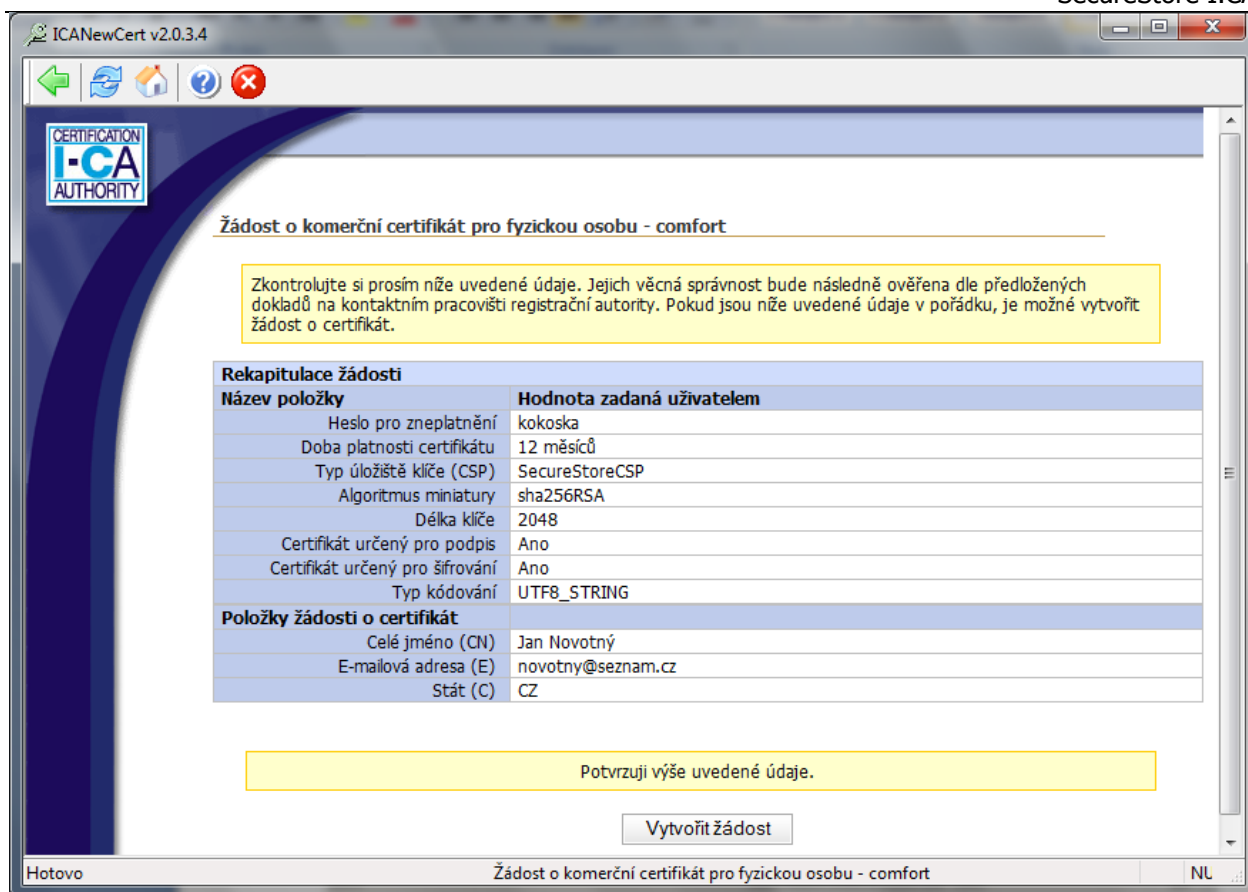
Obr. 20 Nastavení typu certifikátu v aplikaci Newcert.

Obr. 21 Nastavení osobních dat

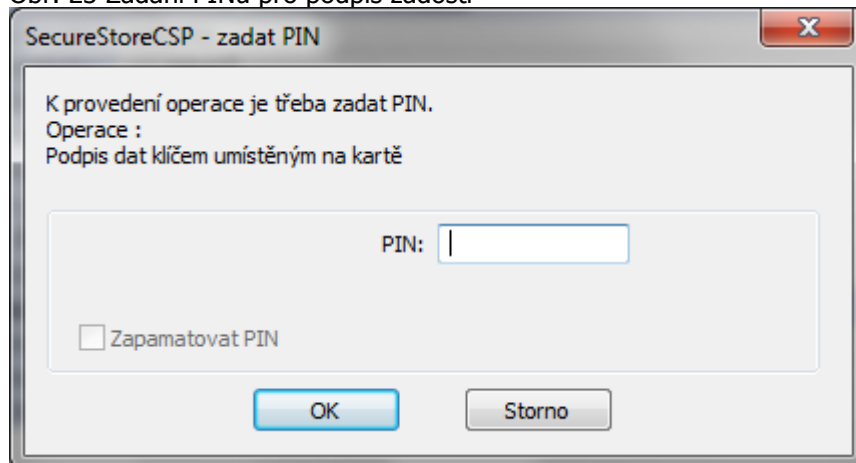
Název položky	Vaše údaje	Příklad naplnění
Titul (před jménem)		
Jméno	Jan	Jirina
Příjmení	Novotný	Nováková
Titul (za jménem)		
Rodné číslo / Datum narození		U cizinců je možné místo RČ zadat datum narození

Adresa trvalého bydliště		
Ulice (ST)		Česká
Číslo popisné/orientační (ST)		11/22
Město (L)		Mělník
Stát	Česká republika	
E-mail *	novotny@seznam.cz	jirina_novakova@ica.cz

Obr. 22 Potvrzení poskytnutých dat pro žádost



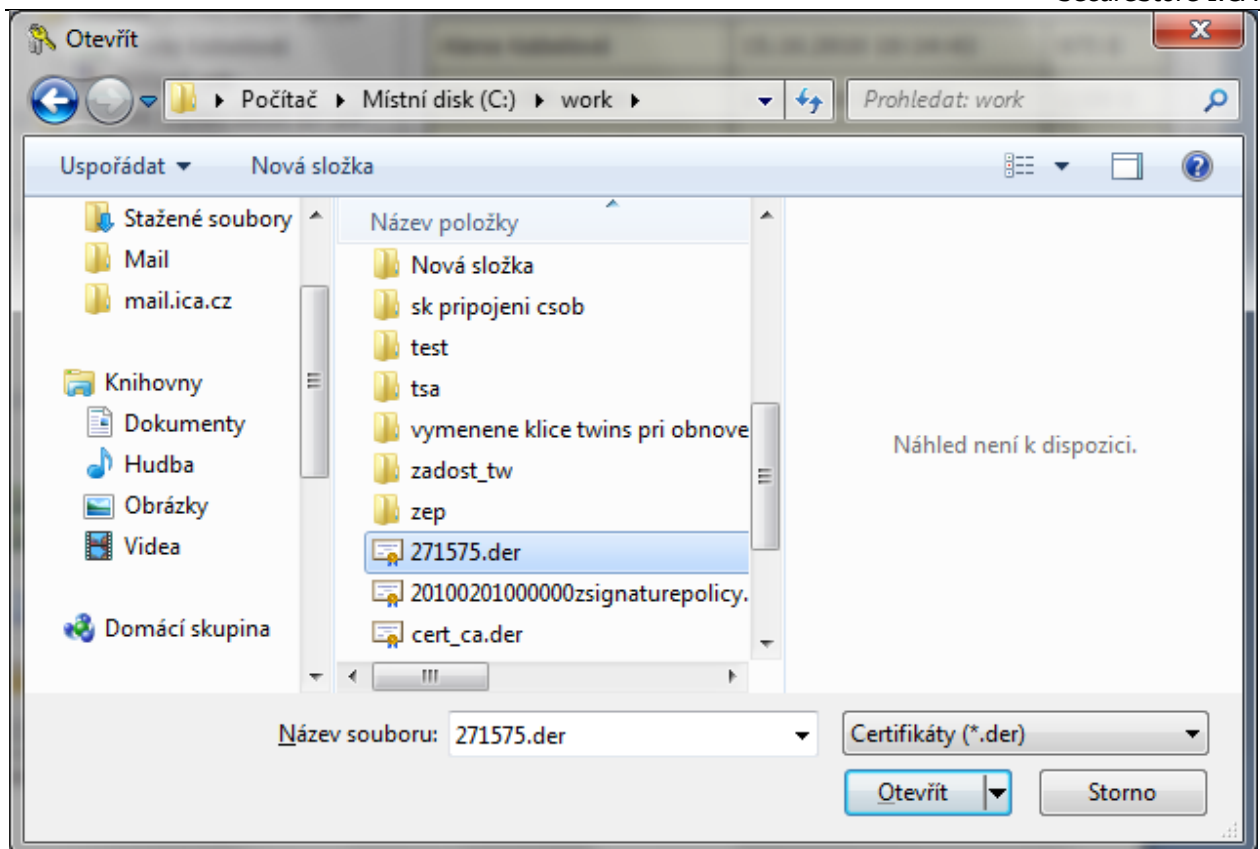
Obr. 23 Zadání PINu pro podpis žádosti



7.2.2 Import osobního certifikátu

Funkce umožňuje import osobního certifikátu z disku na kartu. Certifikát se importuje ve formátu der. Importovaný certifikát se uloží do toho úložiště na kartě, které obsahuje klíče k certifikátu. Pokud na kartě neexistuje úložiště obsahující odpovídající klíče, bude certifikát uložen do části karty označené jako „Partnerské certifikáty“.

Obr.24 Výběr souboru s certifikátem pro import na kartu



7.2.3 Registrovat osobní certifikáty od Windows

Volba zaregistruje všechny osobní certifikáty z karty do osobního úložiště ve Windows.

7.2.4 Import páru klíčů ze zálohy (PKCS#8)...

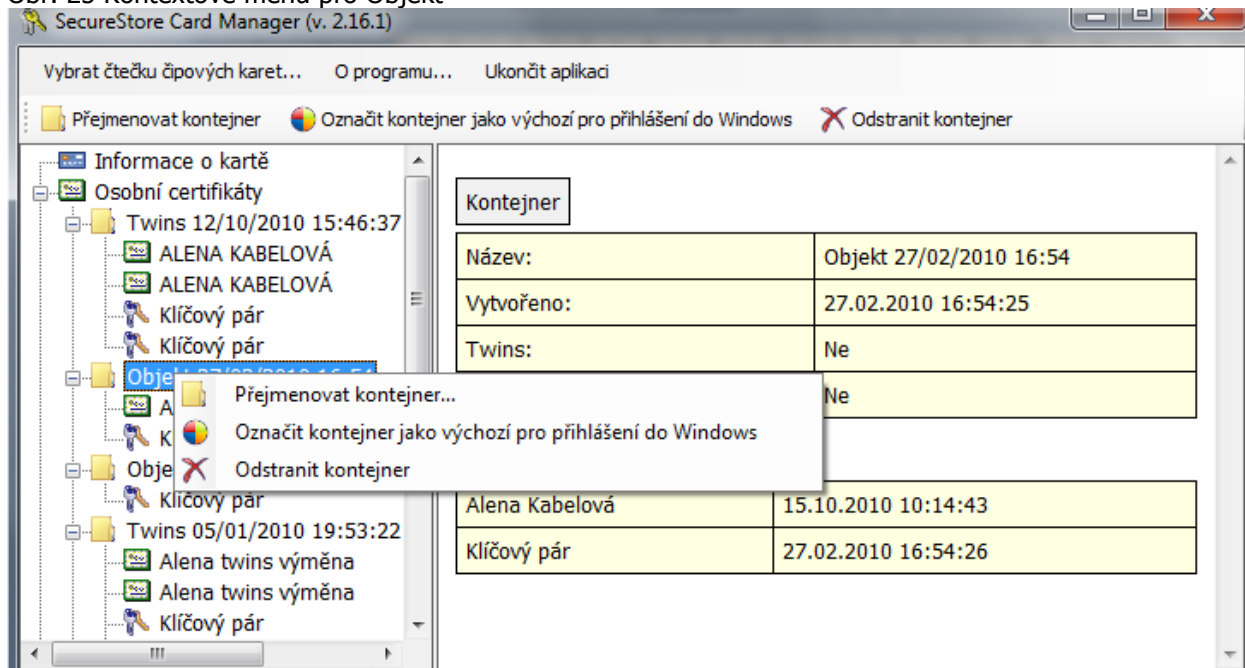
Volba importuje na kartu klíče, které byly během procesu generování žádosti o šifrovací certifikát uloženy na disk.

7.2.5 Import páru klíčů (PKCS#12)...

Volba importuje na kartu klíče, které jsou uložena ve formátu PKCS#12 na disku.

7.3 Kontextové menu pro Objekt

Obr. 25 Kontextové menu pro Objekt



7.3.1 Přejmenovat kontejner

Volba umožňuje přejmenování vybraného kontejneru.

7.3.2 Označit kontejner jako výchozí pro přihlášení do Windows

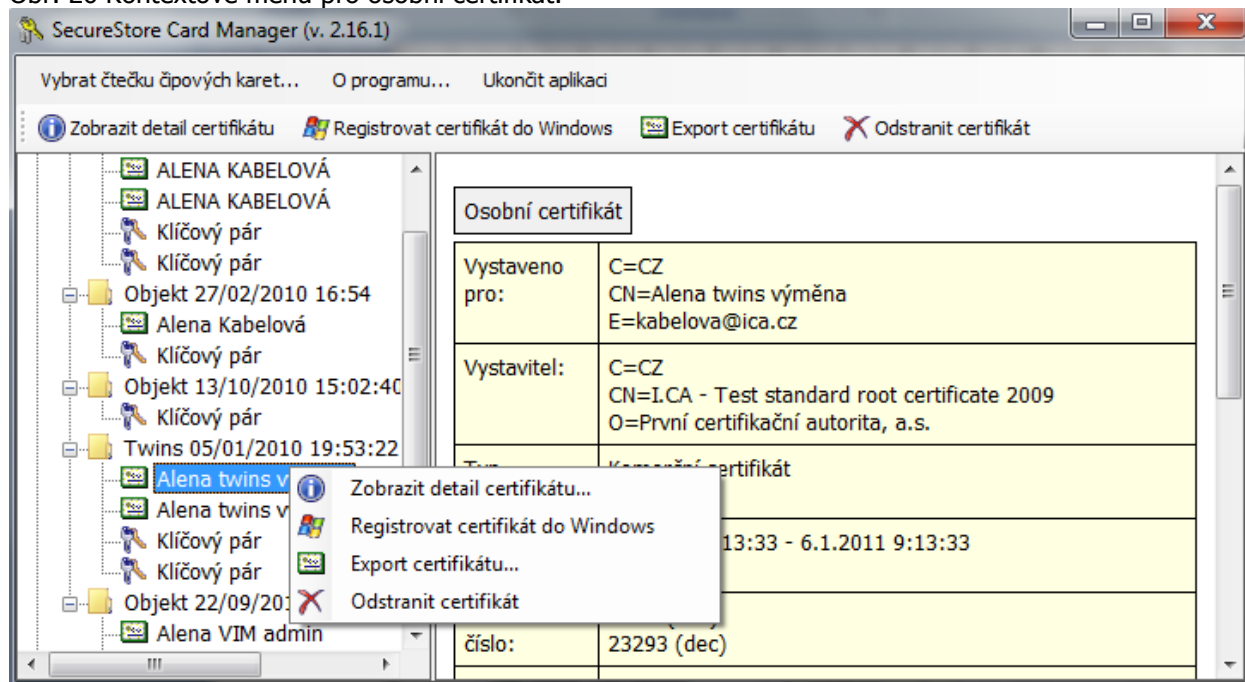
Volba umožňuje označit vybraný kontejner jako výchozí pro přihlášení do Windows. Certifikát a klíč v tomto kontejneru bude použit při přihlašování do Windows.

7.3.3 Odstranit kontejner

Volba umožňuje smazat kontejner z karty včetně certifikátu a klíčů, které obsahuje.

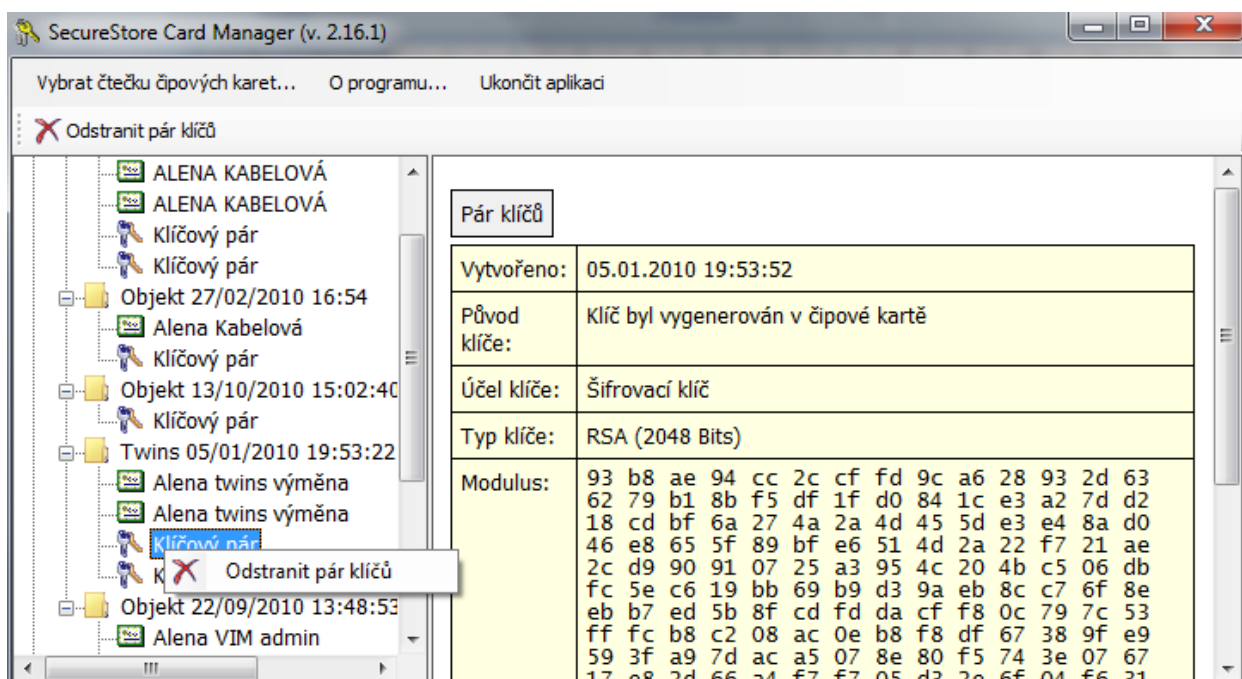
7.4 Kontextové menu pro osobní certifikát

Obr. 26 Kontextové menu pro osobní certifikát.



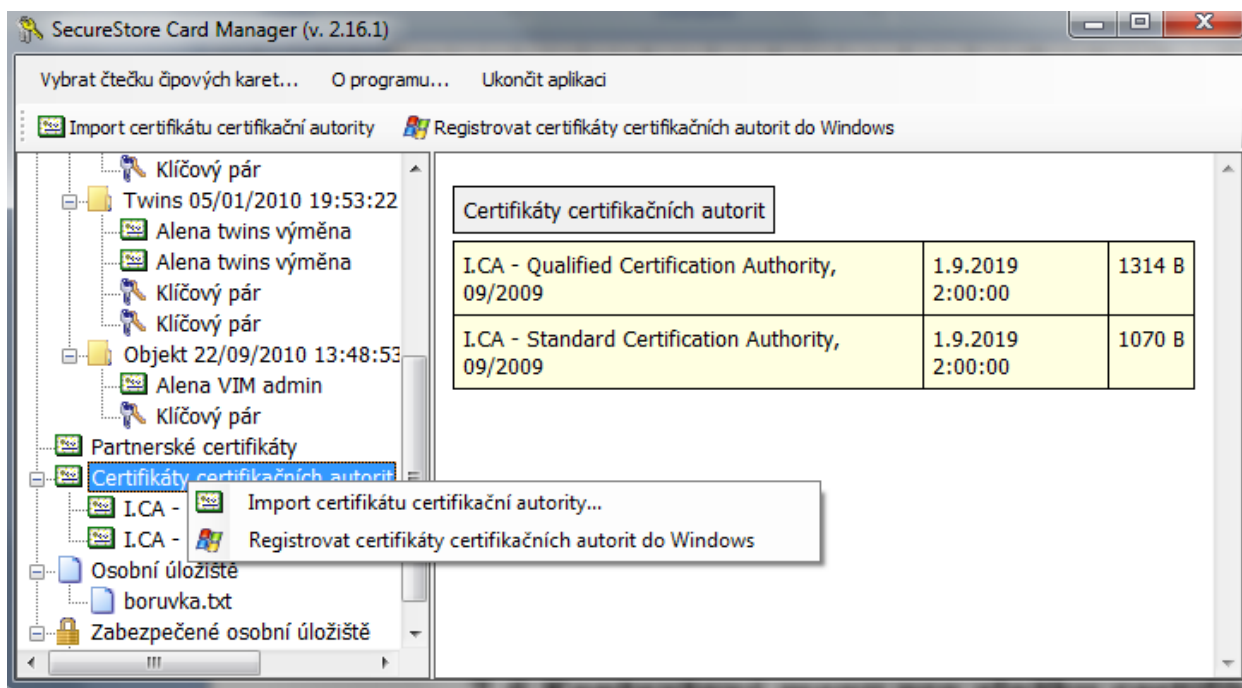
7.5 Kontextové menu pro klíčový pár

Obr. 26 Kontextové menu pro klíčový pár



7.6 Kontextové menu pro složku certifikáty CA

Obr. 27 Kontextové menu pro Certifikáty certifikačních autorit



8. Pojmy

- **Certifikační autorita**
... je nezávislý důvěryhodný subjekt, který klientovi vydává certifikát. Certifikační autorita garantuje jednoznačnou vazbu mezi klientem a jeho certifikátem.
- **Registrační autorita**
... je kontaktní pracoviště sloužící ke komunikaci s klienty. Zajišťuje zejména přijímání žádostí o certifikáty a jejich následné předávání klientům. Tato pracoviště provádějí ověřování totožnosti žadatele o certifikát a shodu žádosti s předloženými doklady. Registrační autority nevydávají certifikáty, pouze o ně žádají na centrálním pracovišti I.CA.
- **Kryptografické operace**
... jsou operace využívající klíče k šifrování a dešifrování. V případě čipové karty je využívána tzv. asymetrická kryptografie, tj. pomocí dvojice klíčů je prováděno šifrování, dešifrování a je vytvářen a ověřován elektronický podpis.
- **Elektronický podpis**
... jsou údaje v elektronické podobě, jsou připojené k datové zprávě nebo jsou s ní logicky spojené a umožňují ověření totožnosti podepsané osoby ve vztahu k podepsané zprávě.
- **Data pro tvorbu elektronického podpisu**
... jsou jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu (ve smyslu zákona o elektronickém podpisu); jedná se o soukromý klíč příslušného asymetrického kryptografického algoritmu (zde RSA).
- **Čipová karta**
... je prostředek pro bezpečné uložení soukromého klíče uživatele a prostředek na vytváření elektronického podpisu. Na čipové kartě jsou uloženy vedle soukromých klíčů i certifikáty klienta, certifikáty certifikačních autorit a mohou zde být další data.
- **PIN a PUK**
... je ochrana přístupu ke kartě, tj. při zápisu na kartu nebo při používání soukromých klíčů z karty. Ochranné kódy mohou být na kartě předem nastaveny a uživatel dostane tyto hodnoty v tzv. pinové obálce nebo si klient sám hodnoty PIN a PUK na kartě nastavuje.
- **Pinová obálka**
... je dopis, který klient může obdržet spolu s kartou. Pinová obálka přísluší ke konkrétní kartě, obsahuje jednoznačnou identifikaci karty a hodnoty PIN a PUK. Pinová obálka není dodávána ke každé kartě.
- **Úložiště**
... je paměťový prostor na médiu (disku, čipové kartě), kde je uložen pár klíčů spolu s certifikátem. Na čipové kartě může existovat najednou až 8 různých úložišť. Úložiště na čipové kartě má své jednoznačné jméno. Úložiště typu PODPIS nepovolují vytváření zálohy klíčů při generování žádosti o certifikát. Všechny certifikáty, u kterých je vytvářena záloha klíčů, jsou proto ukládány do úložišť typu OSTATNÍ.
- **Žádost o certifikát**
... vzniká na základě vyplnění formuláře, který obsahuje údaje o žadateli. K informacím, které žadatel vyplní do formuláře žádosti je připojen vygenerovaný veřejný klíč žadatele a celá tato struktura je podepsána soukromým klíčem žadatele. Žádost o certifikát jsou digitální data, která obsahují veškeré informace, potřebné pro vydání certifikátu. Žádost o certifikát si uživatel může vytvořit pomocí programu ComfortChip nebo na www stránkách I.CA www.ica.cz.

- **Certifikát**
... je obdobou průkazu totožnosti, klient se jím prokazuje při elektronické komunikaci. Získání certifikátu se velice blíží standardním postupům získání občanského průkazu. I.CA tyto služby zajišťuje prostřednictvím sítě kontaktních pracovišť - registračních autorit, které realizují požadavky svých klientů. Certifikát je jednoznačně svázán s párem klíčů, který uživatel používá v elektronické komunikaci. Pár klíčů je tvořen tzv. veřejným klíčem a soukromým klíčem.
- **Veřejný klíč**
... je veřejná část páru klíčů uživatele, je určena pro ověřování elektronického podpisu a případně pro šifrování.
- **Soukromý klíč**
... je tajná část páru klíčů uživatele, je určena pro vytváření elektronického podpisu a případně pro dešifrování. Vzhledem k použití soukromého klíče je pro něj třeba zajistit co nejvyšší bezpečnost. Z tohoto důvodu je pro uchování klíče využita čipová karta. Soukromý klíč, používaný pro dešifrování, je potřeba uchovávat po celou dobu existence šifrovaných dokumentů a zpráv. Tento klíč si může uživatel uchovat na kartě a doporučujeme současně i na záložním médiu.
- **Doba platnosti certifikátu**
Každý certifikát je vydáván na dobu určitou. Doba platnosti je uvedena v každém certifikátu. Certifikát, používaný pro elektronický podpis, je po skončení doby platnosti nepotřebný. Certifikát, používaný pro šifrování, je nutno uchovat i po skončení doby platnosti pro dešifrování starších zpráv.
- **Komerční certifikát standard**
Certifikáty standard představují osobní certifikáty vhodné pro běžné využití. Jsou vydávány fyzickým nebo právnickým osobám na základě řádně vyplněné žádosti o certifikát, předané kontaktnímu pracovišti I.CA současně s předložením požadovaných dokladů pro nezbytné ověření totožnosti žadatele.
- **Komerční certifikát comfort**
Certifikáty comfort představují osobní certifikáty, jejichž hlavní odlišností od certifikátů standard je čipová karta, která je součástí této služby. Slouží jako médium k bezpečnému uložení dat pro tvorbu elektronického podpisu a bezpečnému vytváření elektronického podpisu. Tato služba je určena především pro firemní účely, je však poskytována fyzickým i právnickým osobám.
- **Kvalifikovaný certifikát**
... je striktně řízen zákonem č. 227/2000 Sb. a slouží výhradně pro oblast elektronického podpisu. Vytváření, správa a použití kvalifikovaného certifikátu se řídí zvláštními příslušnými certifikačními politikami.
- **Klientský Komerční certifikát**
... je vydáván fyzickým nebo právnickým osobám na základě řádně vyplněné žádosti o certifikát předané kontaktnímu pracovišti I.CA, současně s předložením požadovaných dokladů pro nezbytné ověření totožnosti žadatele. Délka platnosti těchto certifikátů je vždy závislá na délce použitého kryptografického klíče.
- **Klientský certifikát**
... certifikát vydaný klientovi I.CA na základě řádně vyplněné žádosti o certifikát předané kontaktnímu pracovišti I.CA, současně s předložením požadovaných dokladů pro nezbytné ověření totožnosti žadatele. V případě I.CA se může jednat buď o komerční, nebo o kvalifikovaný certifikát.
- **Certifikát certifikační autority**
... je používán k ověřování správnosti a důvěryhodnosti klientských certifikátů. Jeho instalací na své PC uživatel deklaruje operačnímu systému svou důvěru v takovou certifikační autoritu. V praxi to znamená, že pokud uživateli přijde zpráva, která je elektronicky podepsána certifikátem vydaným právě touto certifikační autoritou, je systémem chápán jako důvěryhodný. V ostatních případech se zpráva jeví jako nedůvěryhodná.

- **Certifikát pro přihlášení do Windows**
Certifikát pro přihlášení do Windows musí obsahovat specifické údaje. Pro přihlášení do Windows není možné proto použít jakýkoli certifikát. Registrační autorita I.CA na požádání zajistí vydání správného certifikátu pro přihlašování. Úložiště na kartě obsahující certifikát pro přihlášení musí být označeno pro autentizaci. Označeno pro autentizaci může být na kartě právě jedno úložiště.
- **Seznam veřejných certifikátů (komerčních)**
... je seznam certifikátů vydaných I.CA, u kterých jejich majitelé souhlasili se zveřejněním. Nejsou zde certifikáty typu "testovací" a certifikáty, u kterých jejich majitel se zveřejněním nesouhlasil.
- **Seznam veřejných certifikátů (kvalifikovaných)**
... je seznam kvalifikovaných certifikátů vydaných I.CA. V případě těchto certifikátů je jejich zveřejnění dáno zákonem 227/2000 Sb., o elektronickém podpisu.
- **Certifikační autority podporované kartou**
Každá čipová karta vydaná I.CA má definovaný seznam tzv. podporovaných certifikačních autorit, jejichž certifikáty je možné na kartu uložit.
- **Obnova certifikátu - „následný“ certifikát**
... je vydán klientovi po uplynutí doby platnosti certifikátu prvotního. Následný certifikát je vydán pouze v případě, že klient nepožaduje změnu položek předchozího certifikátu. Pokud ji požaduje, nejedná se o certifikát následný, ale další prvotní. Při vydávání následného certifikátu před vypršením platnosti prvotního certifikátu není již nutná přítomnost zákazníka na registrační autoritě I.CA. Klient pouze zašle s využitím platného certifikátu elektronicky podepsanou žádost o vydání následného certifikátu ve standardizované elektronické podobě.
- **Použití klíče**
 - **DigitalSignature (digitální podpis)** - primárně se tento příznak (bit) nastavuje, pokud certifikát má být použit v souvislosti s digitálním podpisem s výjimkou zajištění nepopíratelnosti, podpisů certifikátů a seznamů zneplatněných certifikátů certifikační autoritou.
Použití: tento bit je nutno v současné době nastavit v případech, kdy uživatel zamýšlí používat svůj soukromý klíč spojený s vydaným certifikátem obecně pro vytváření digitálního podpisu (např. při použití certifikátu v rámci bezpečné elektronické pošty).
 - **NonRepudiation (nepopíratelnost)** - tento příznak se nastavuje, pokud má být veřejný klíč (prostřednictvím ověření digitálního podpisu) použit k prokázání odpovědnosti za určitou akci podepisující osoby.
Použití: tento bit je nutno v současné době nastavit zejména v případech kvalifikovaných certifikátů, kdy uživatel zamýšlí používat svůj soukromý klíč spojený s vydaným certifikátem pro vytváření elektronického podpisu.
 - **KeyEncipherment (šifrování klíče)** - tento příznak se nastavuje, pokud má být veřejný klíč použit k přenosu kryptografických klíčů.
Použití: tento bit je nutno nastavit, pokud uživatel zamýšlí použít certifikát pro účely šifrování v rámci bezpečné elektronické pošty. V prostředí MS Outlook je rovněž nutno tento bit nastavit v případě, že uživatel nemá jiný certifikát, který lze použít k šifrování.
 - **DataEncipherment (šifrování dat)** - tento příznak se nastavuje, pokud má být veřejný klíč použit k šifrování dat (s výjimkou kryptografických klíčů).
Použití: obecně je nutno nastavit tento bit, pokud veřejný klíč obsažený v certifikátu bude používán pro šifrování obecných dat, např. dokumentů. Pro účely bezpečné elektronické pošty jej není nutno nastavovat.
- **Formát PKCS#12**
RSA klíče a certifikát lze uložit do jednoho souboru v tzv. formátu PKCS#12, který je definovaný normou PKCS#12. V tomto formátu je možno např. exportovat RSA klíče certifikát z úložiště Windows, pokud je povolen export soukromého klíče. Obsah souboru je chráněn heslem. Soubor má příponu pfx nebo p12.