I.CA SecureStore

Uživatelská příručka

Verze 4.1 a vyšší

První certifikační autorita, a.s.

Verze 4.17

Obsah

1. Úvod

Uživatelská příručka je platná pro aplikaci I.CA SecureStore verze 4.0.1.0. Uvedené verze mají stejnou funkčnost a totožné uživatelské rozhraní.

2. Přístupové údaje ke kartě

STARCOS 3.5

Přístup k čipové kartě je chráněn pomocí PINu, podobně jako je tomu např. u platebních karet.

PIN je 6-8 místné číslo. Pokud při zadávání PINu 3krát za sebou uživatel zadá chybnou hodnotu PINu, bude PIN automaticky zablokován.

PUK je 6-8 místné číslo. Pokud při zadávání PUKu 5krát za sebou uživatel zadá chybnou hodnotu PUKu,

Dojde k zablokování PUKu a tím i celé čipové karty.

Odblokování PINu pomocí PUKu je omezeno na 6 pokusů.

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 uživatel použije 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.

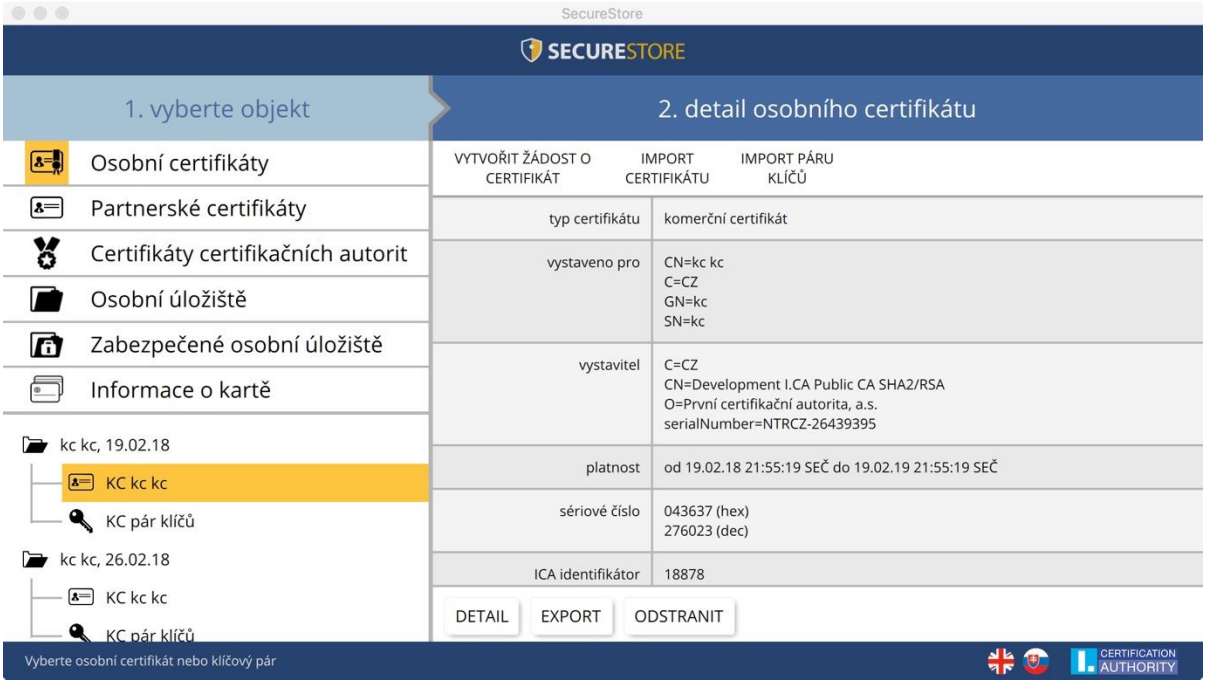
Pokud uživatel spolu s kartou obdrželi tzv. Pinovou obálku pak byla již inicializace karty provedena a hodnoty PINu a PUKu jsou uvedeny v Pinové obálce.

Pokud uživatel Pinovou obálku neobdržel, pak musí při prvním použití nové karty nastavit hodnotu PINu a PUKu.

Dialog pro inicializaci karty se zobrazí automaticky zpravidla při prvním spuštění aplikace s novou čipovou kartou. PIN a PUK si pečlivě zapamatujte.

3. Základní obrazovka

Obr. 1 - Základní obrazovka



Základní obrazovka je rozdělená do dvou částí.

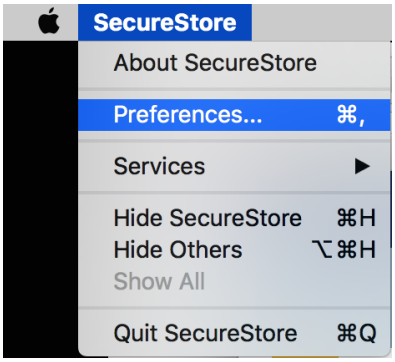
V levé části obrazovky se zobrazuje seznam objektů uložených na čipové kartě.

V pravé části obrazovky se zobrazují jednotlivé detaily objektů na čipové kartě.

3.1. Změna jazyku aplikace

Změnu uživatel může provést v pravém dolním rohu aplikace, kliknutím na příslušnou vlajku.

Obr. 2 – Menu aplikace



Verze aplikace I.CA SecureStore

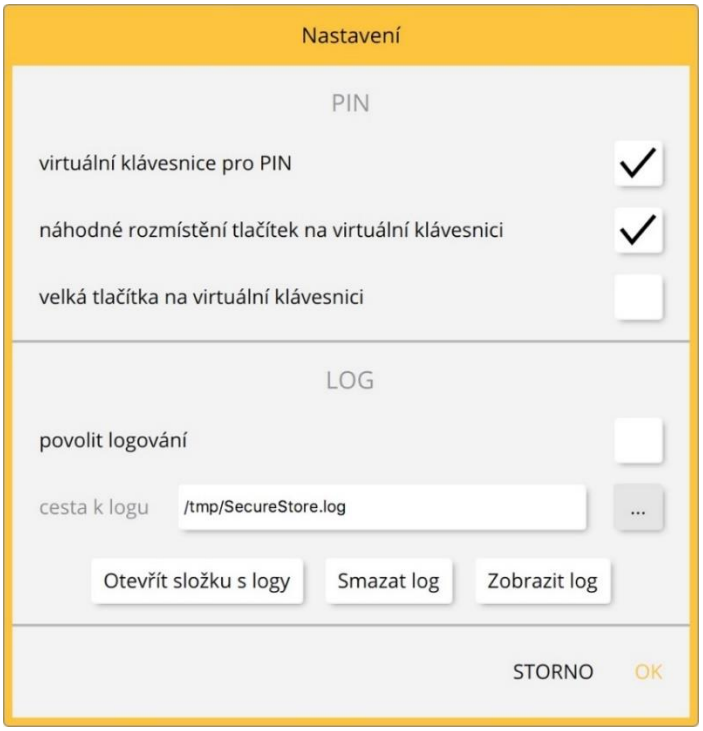
Informaci o verzi aplikace uživatel zjistí kliknutím na **About SecureStore**

Obr. 3 - Verze aplikace

Volba **Preferences** slouží pro:

1) Upravení klávesnice pro zadávání PINu

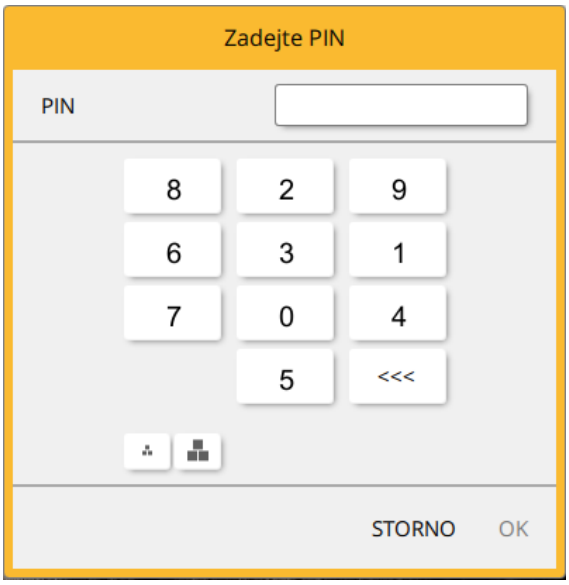
Obr. 4 - Klávesnice pro zadávání PIN



Defaultně je aplikace nastavená na hodnotu **„Náhodné rozmístění tlačítek na virtuální klávesnici“.**

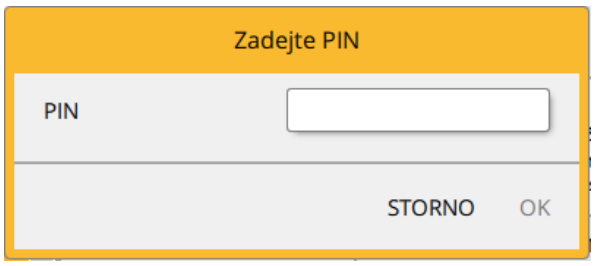
Uživatel poté zadává PIN na virtuální klávesnici kurzorem myši.

Obr. 5 - Klávesnice pro zadávání PIN



Po odškrtnutí všech možností pro zadávání PINu, uživatel zadává PIN na numerické klávesnici.

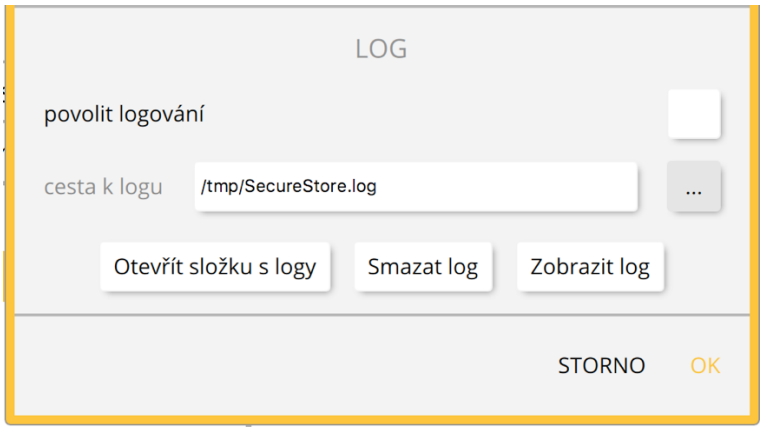
Obr. 6 - Klávesnice pro zadávání PINu



2) Povolení logování – povolení logování aplikace, pro případnou analýzu technického problému při používání čipové karty a aplikace.

Cestu k uloženému log souboru může uživatel změnit pomocí tlačítka ...

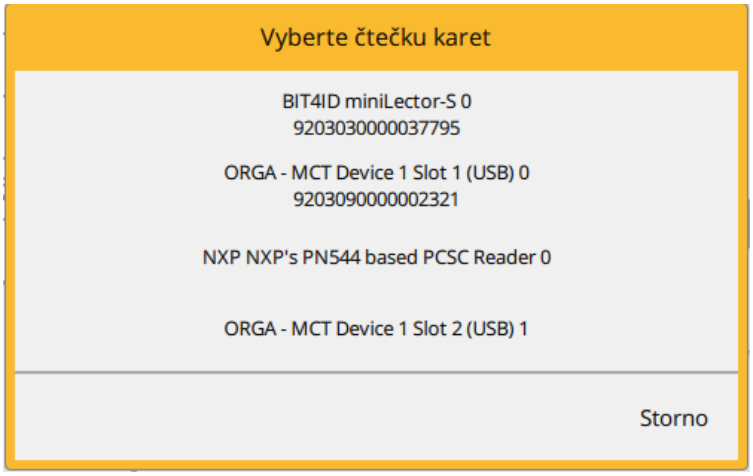
Obr. 7 - Log



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

Výběr čtečky čipových karet

Obr. 8 - Výběr čtečky čipových karet



V případě, že má uživatel k MACu připojenu pouze jednu čtečku čipových karet, není okno zobrazováno.

V nástrojové liště, viz obr. 9 se volby mění dle zvoleného objektu v levé části obrazovky.

Nástrojová lišta

Obr. 9 - Nástrojová lišta

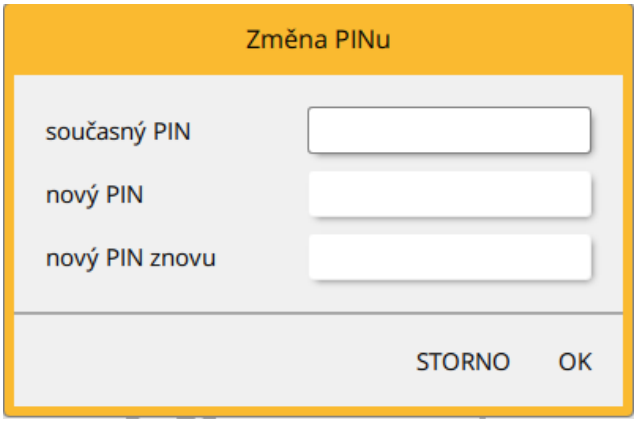
Příklad nástrojové lišty zobrazuje volby platné pro objekt **„Informace o kartě“**.

Volba **Obnovit data z karty** opakovaně načte data z čipové karty.

Volbou **Změnit PIN** uživatel provede změnu PINu ke kartě. Do dialogového okna pro změnu PINu uživatel zadá stávající PIN a 2x PIN nový.

Změna PINu

Obr. 10 - Změna PINu



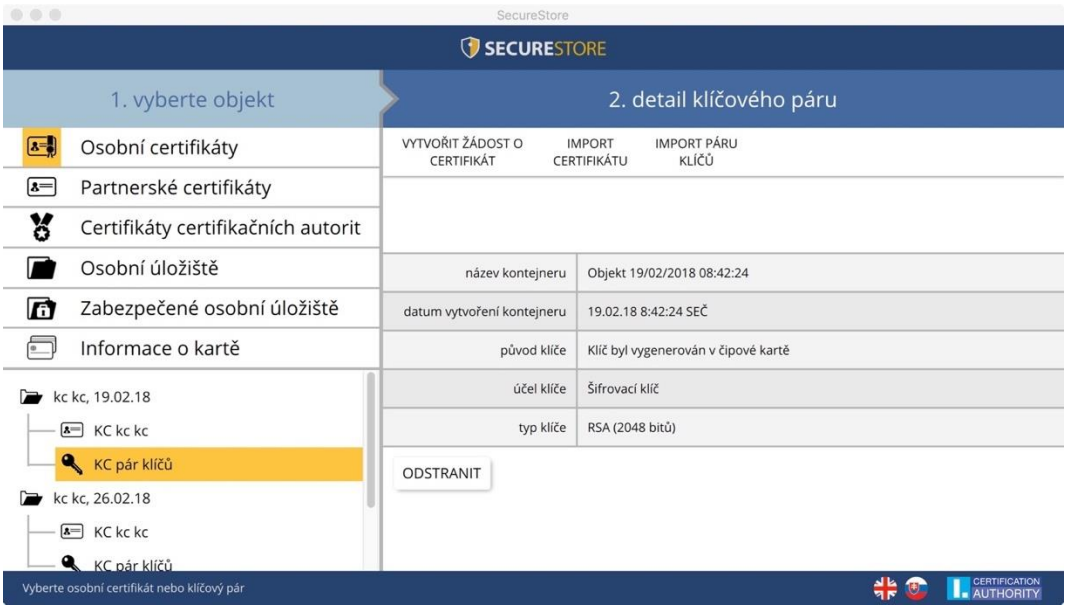
Volba **Odblokovat PIN** umožňuje nastavit novou hodnotu PINu v případě, že si uživatel PIN zablokuje. K odblokování PINu je vyžadováno zadání PUKu.

POZN.: **Odblokování PINu pomocí PUKu je omezeno na 6 pokusů.**

4. Zobrazení informací o páru klíčů

Informace o páru klíčů uživatel nalezne v objektu **„Osobní certifikáty“**.

Obr. 10 – Zobrazení informací o páru klíčů



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.

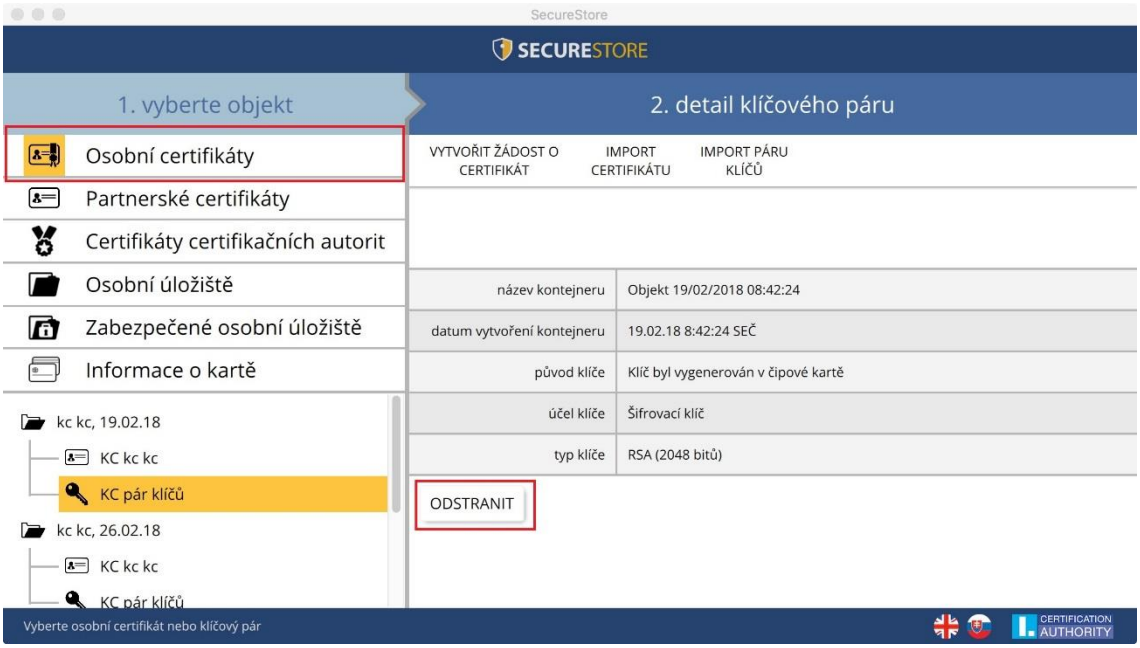
Pár klíčů je možné z karty odstranit, pomocí tlačítka „**Odstranit“**.

4.1. Odstranění klíčového páru

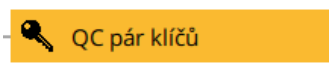
Volbu uživatel nalezne v objektu **„Osobní certifikáty“**, vybere požadovaný klíčový pár a tlačítkem **„Odstranit“** provede odstranění.

Pokud uživatel odstraní privátní klíč k osobnímu certifikátu je tato relace **nenávratná** a nepůjde již certifikátem podepisovat / dešifrovat!!!

Obr. 11 - Odstranění klíčového páru

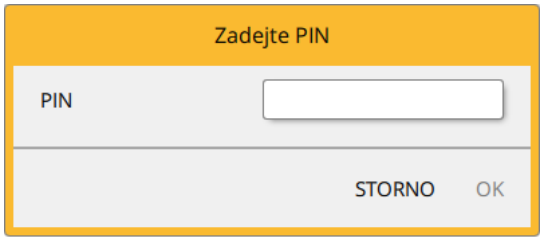


Obr. 12 – Privátní klíč



Po kliknutí na volbu „**Odstranit“** je uživatel vyzván k zadání PINu, po zadání PINu bude označený klíč odstraněn.

Obr. 13 – Zadání PINu pro odstranění klíčového páru

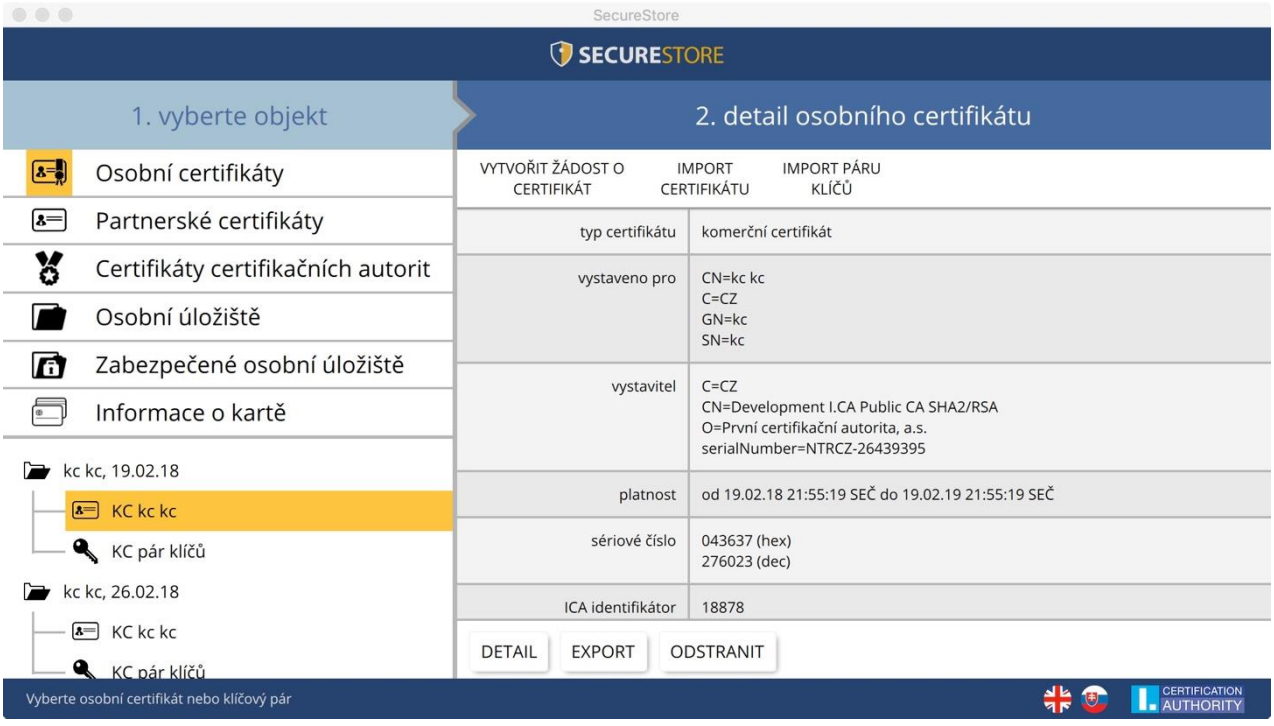


5. Certifikáty

5.1. Zobrazení certifikátu

Zobrazení certifikátu uživatel nalezne v objektu **„Osobní certifikáty“**, kde vybere požadovaný certifikát k zobrazení. Detail certifikátu se zobrazí v pravé obrazovce aplikace v **„Detailu osobního certifikátu“**.

Obr. 14 - Zobrazení certifikátu

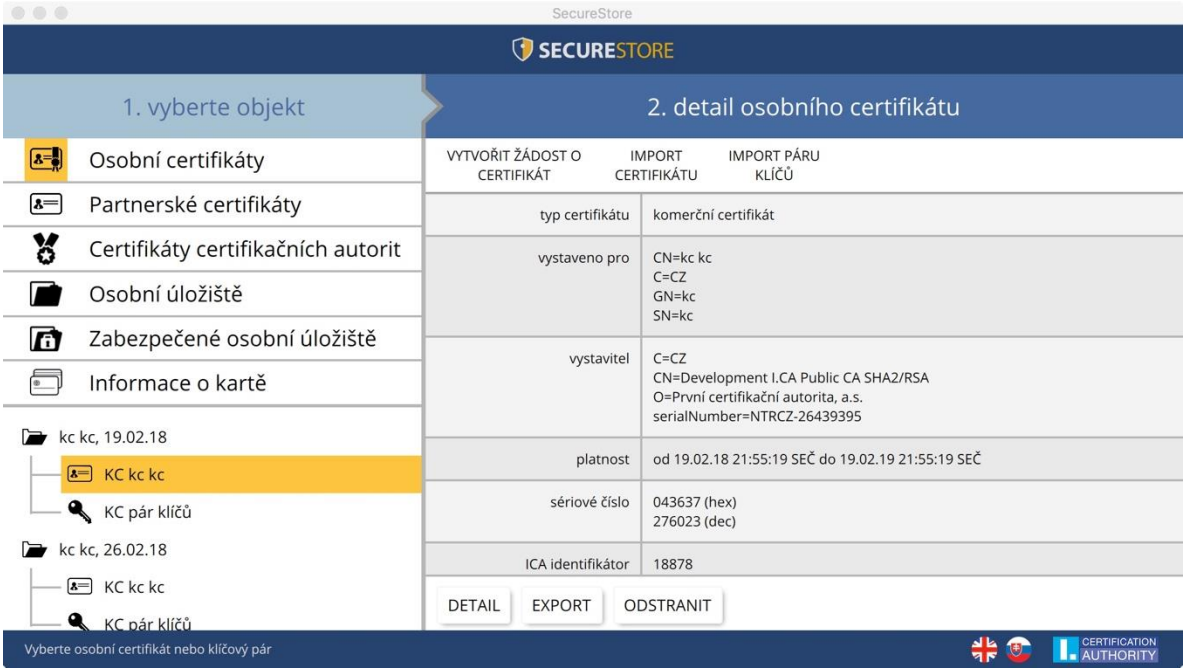


5.2. Práce s osobním certifikátem

Volby pro práci s certifikátem uloženým na kartě jsou dostupné v nástrojové liště ve spodní části aplikace.

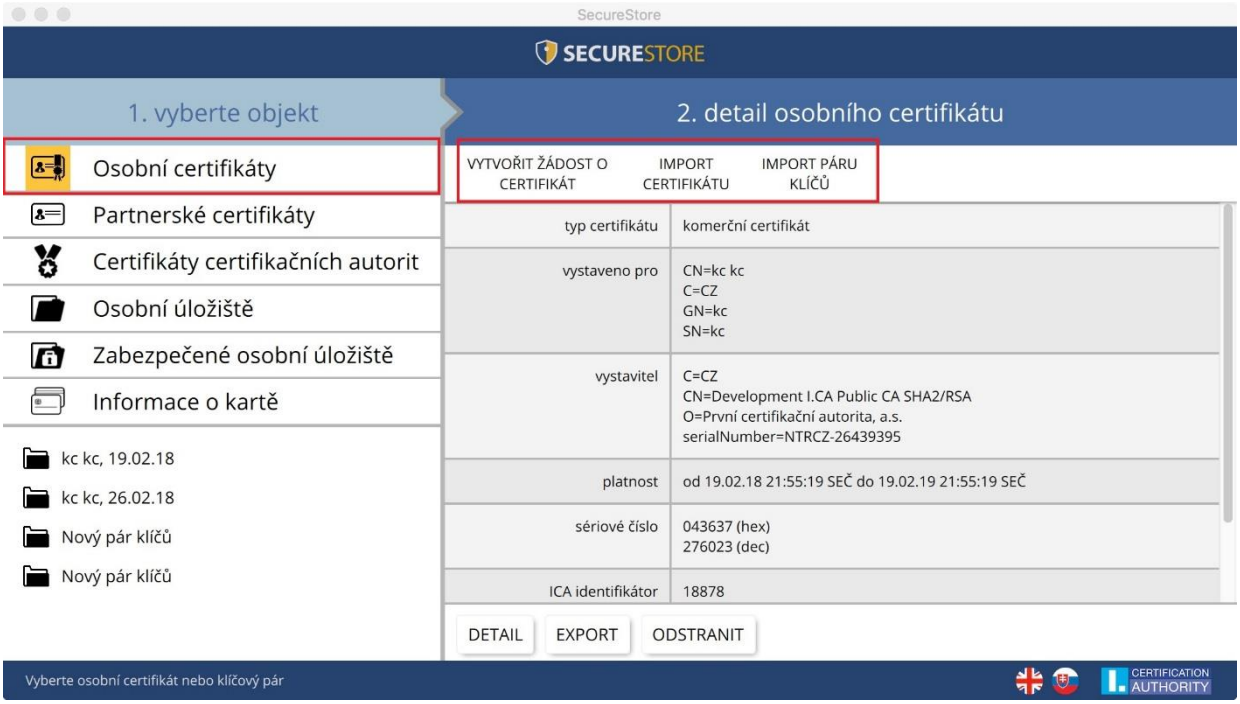
Volbu uživatel nalezne v objektu **„Osobní certifikáty“** a vybere požadovaný certifikát pro operaci pomocí nástrojové lišty.

Obr. 15 - Volby pro práci s osobním certifikátem v nástrojové liště



Volby pro import certifikátu na čipovou kartu jsou dostupné po kliknutí na objekt „**Osobní certifikáty“**.

Obr. 16 - Volby pro import certifikátu



Osobní certifikát je importován do objektu, ve kterém je uložen odpovídající pár klíčů. Pokud takový objekt na kartě neexistuje, bude certifikát importován do samostatné složky bez privátního klíče.

Jako partnerské certifikáty mohou být importovány certifikáty komunikačních partnerů.

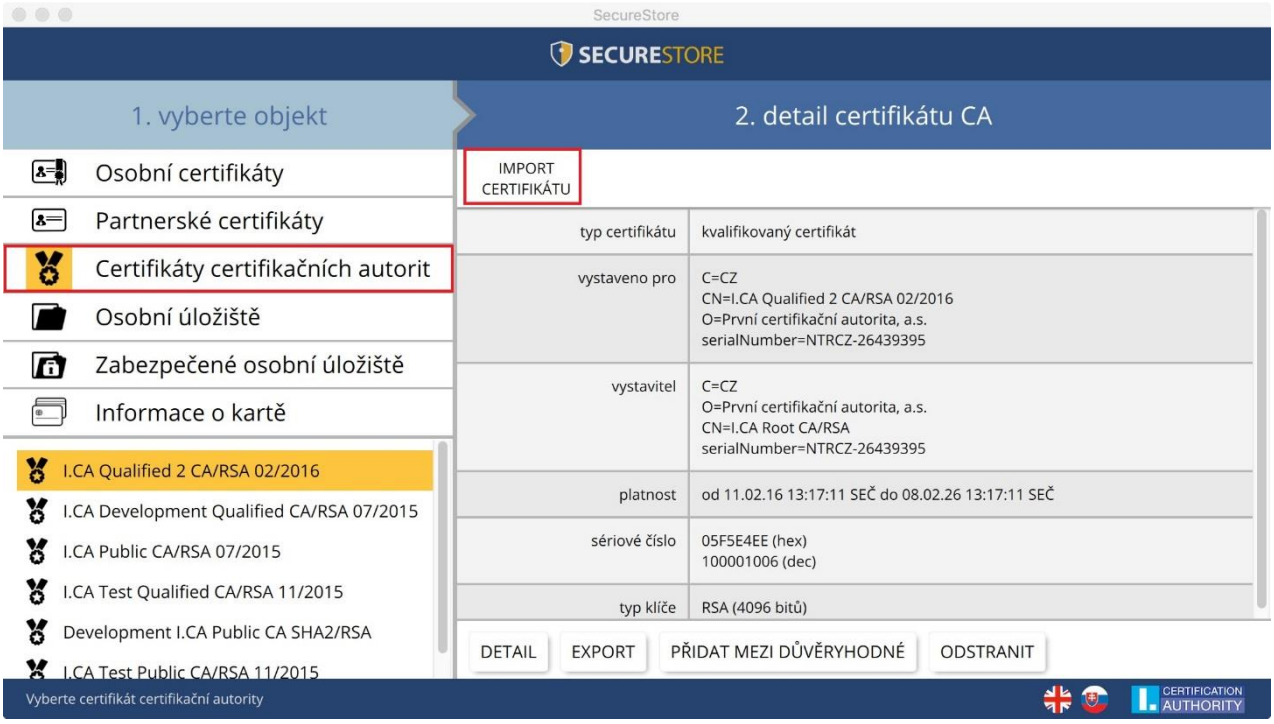
Zobrazení holých dat certifikátu slouží pouze pro odborníky pro vizuální kontrolu dat certifikátu.

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 čipovou 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 http://www.ica.cz/Korenove-certifikaty.

Obr. 17 - Import certifikátu certifikační autority

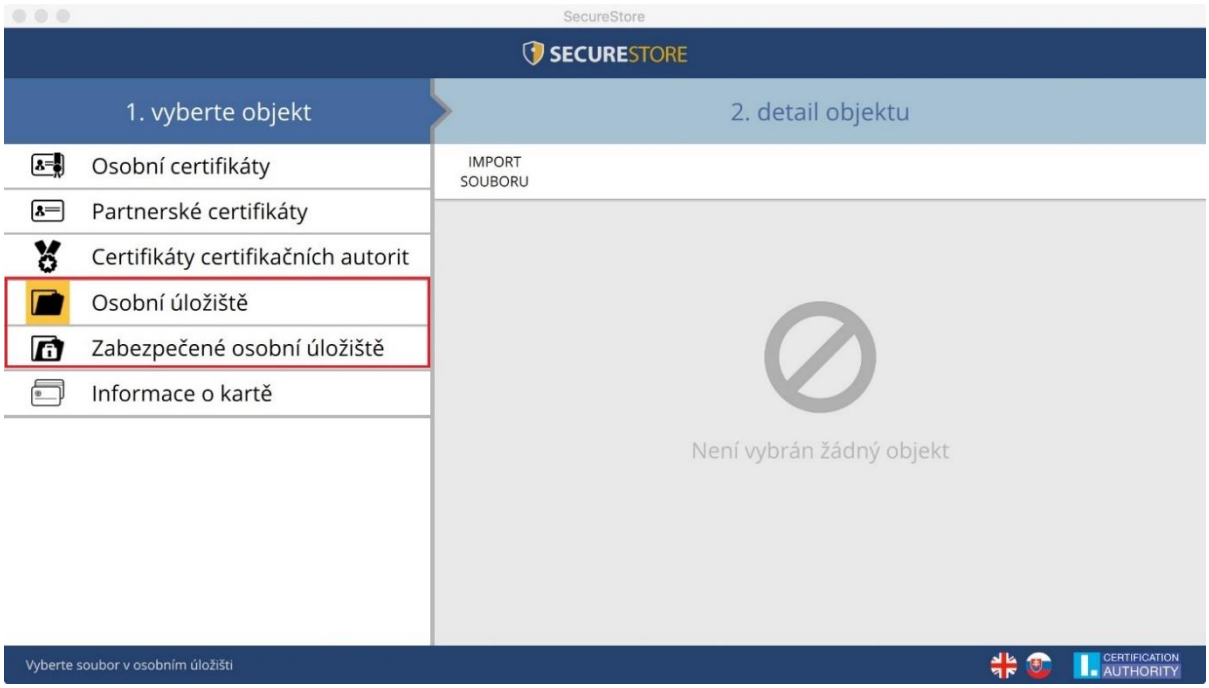


V případě, kdy nastane problém s důvěryhodností kořenových certifikátů, lze certifikáty ručně přidat mezi důvěryhodné pomocí volby „Přidat mezi důvěryhodné“. Po zadání PINu uživatele bude certifikát označen jako důvěryhodný v klíčence.

Kořenové certifikáty se používají pro ověření důvěryhodnosti osobních certifikátů.

6. Osobní úložiště

Obr. 18 - 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.

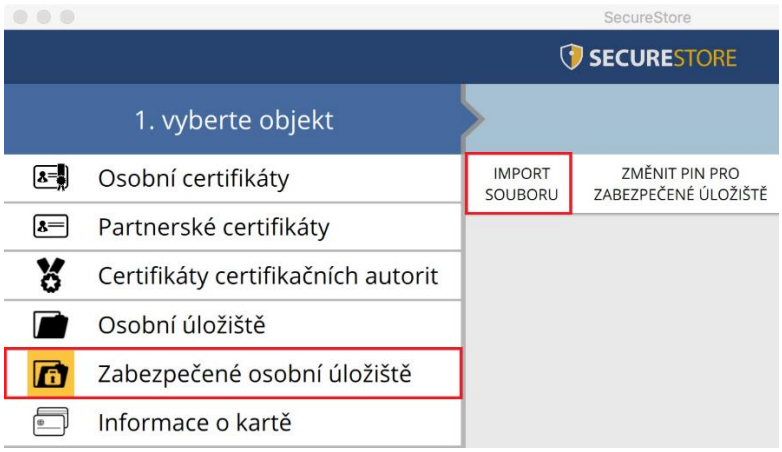
Čtení a export souboru v zabezpečeném úložišti je chráněn PINem pro zabezpečené úložiště, **viz. kapitola 2.**

Obr. 19 - Import souboru do osobního úložiště

Funkci uživatelnalezne v objektu **„Osobní úložiště“** a v detailu objektu **„Import souboru“**.

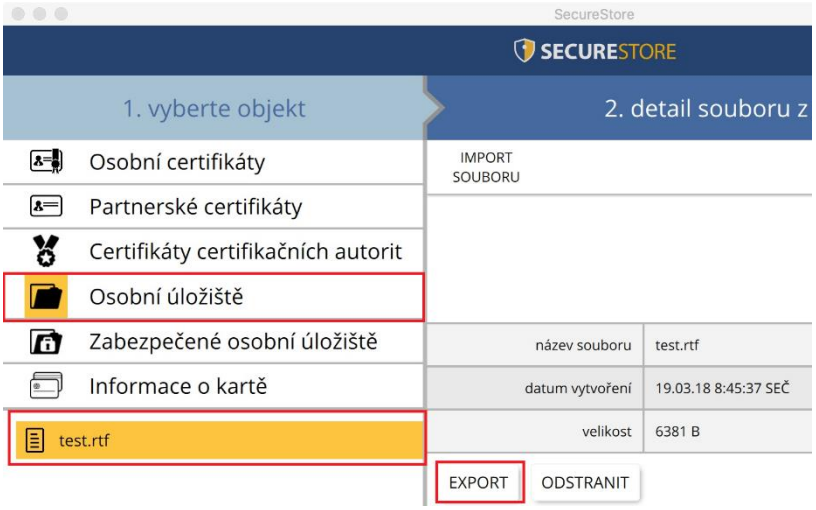
Obr. 20 - Import souboru do zabezpečeného úložiště

Funkci uživatel nalezne v objektu **„Zabezpečené osobní úložiště“** a v detailu objektu **„Import souboru“**.



Obr. 21 - Export souboru z osobního úložiště

Funkci uživatel nalezne v objektu **„Osobní úložiště“**, po výběru souboru pro export v **„Detailu souboru z osobního úložiště“** provede tlačítkem **„Export“**.



Pro odstranění souboru v zabezpečeném úložišti je zapotřebí zadat PIN k čipové kartě.

7. Ovládání aplikace

Jednotlivé funkce aplikace jsou realizovány pomocí nástrojové lišty. Nástrojová lišta se zobrazí po kliknutí na příslušný objekt v aplikaci v levé části obrazovky.

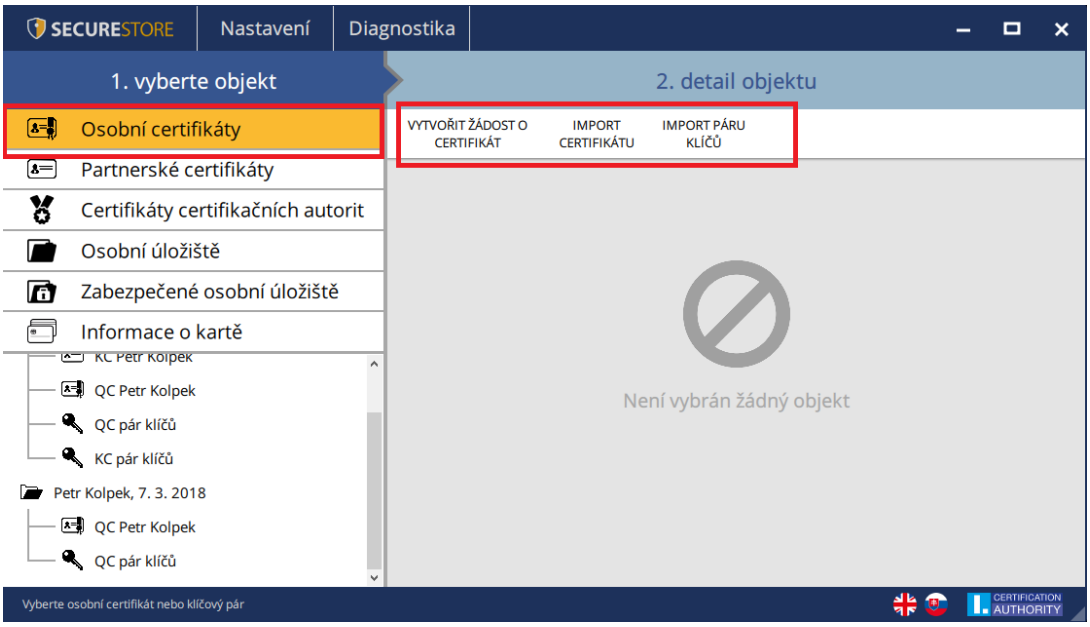
7.1. Nástrojová lišta pro Informace o kartě

Nástrojová lišta objektu **„Informace o kartě“** obsahuje základní administrativní operace s kartou související se správou PINu a PUKu a opakovaným načtením dat z karty.

Obr. 22 - Nástrojová lišta pro objekt „Informace o kartě“

7.2. Nástrojová pro složku Osobní certifikáty

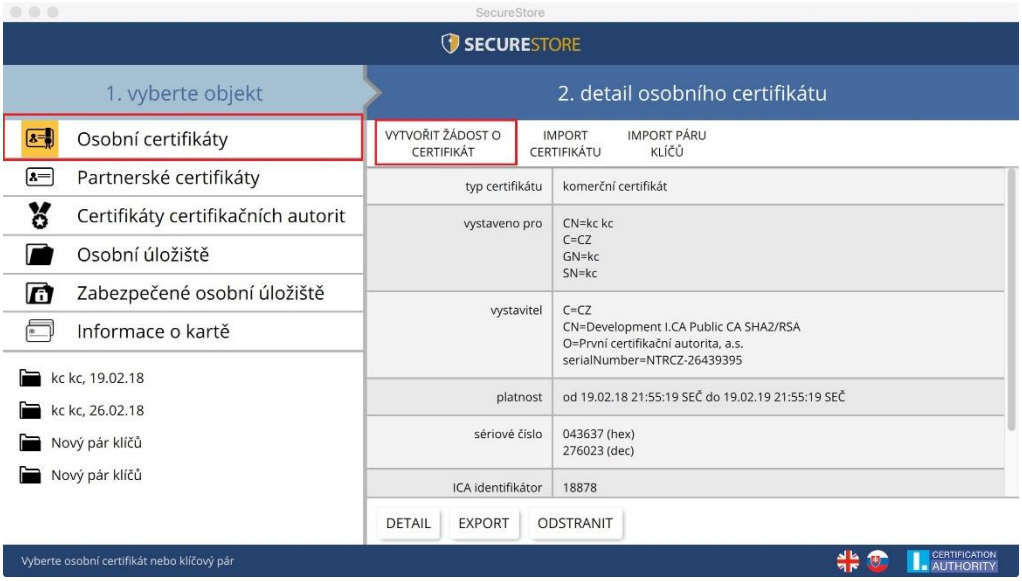
Obr. 23 - Nástrojová lišta pro objekt „Osobní certifikáty“



7.2.1. Vytvořit žádost o certifikát

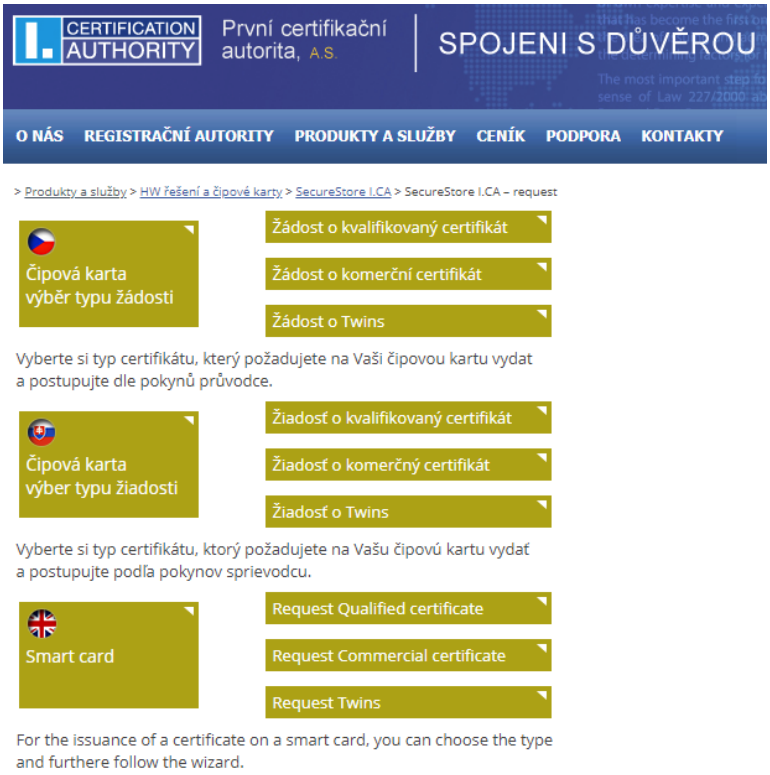
Volba **„Vytvořit žádost o certifikát“** přesměruje uživatele na webové stránky I.CA a zvolí požadovaný typ žádosti o certifikát pro generování páru klíčů pomocí online generátoru.

Obr. 24 - Volba typu žádosti pro generování páru klíčů pomocí online generátoru

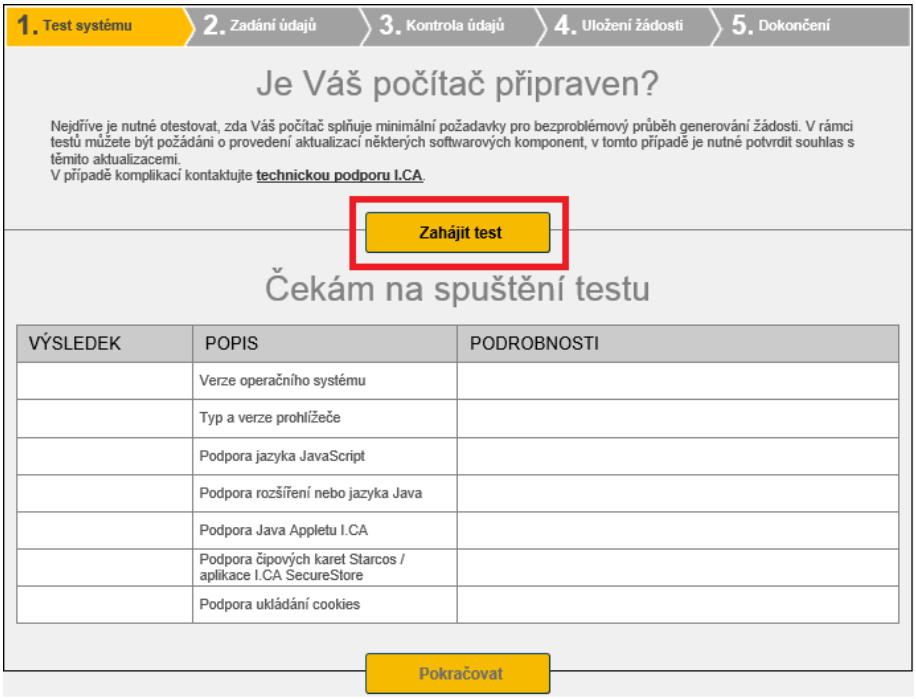


Po zvolení typu žádosti o certifikát bude uživatel přesměrován na I.CA online generátor, kde je potřebné projít testem systému (mít nainstalované potřebné komponenty pro spuštění online generátoru).

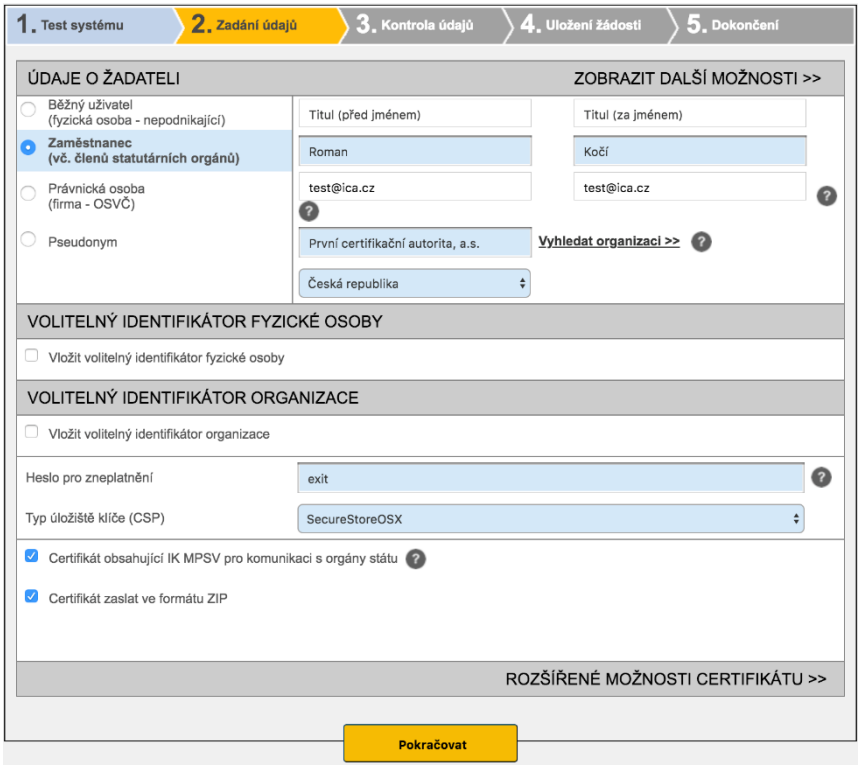
Obr. 25 - Volba typu žádosti o certifikát



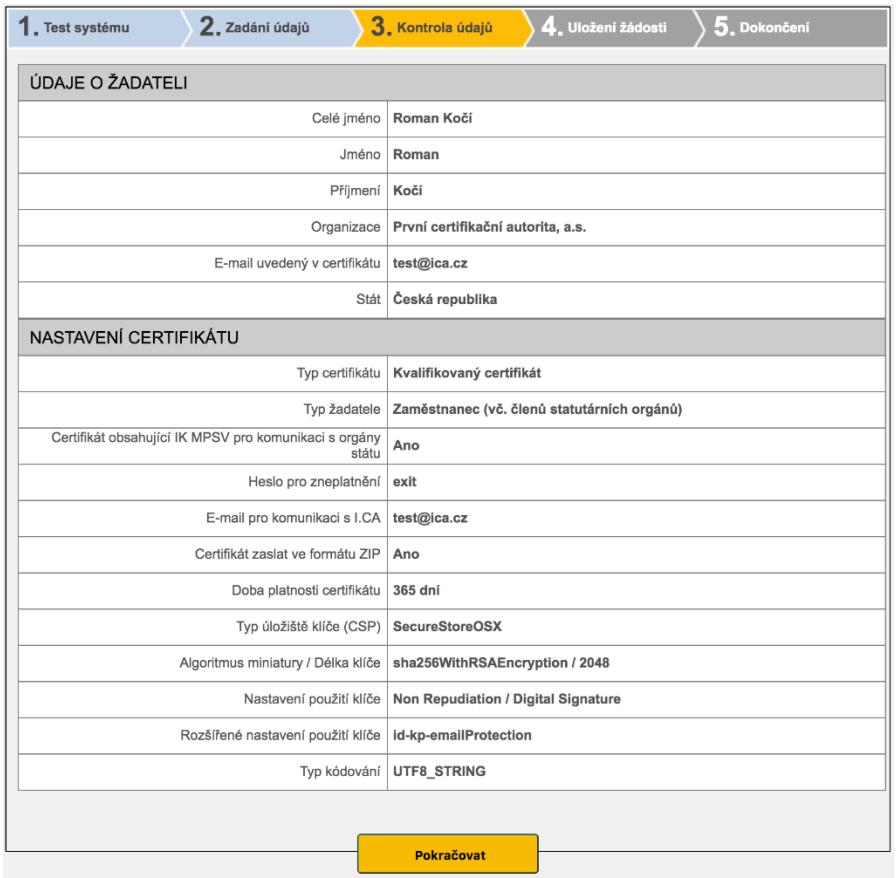
Obr. 26 – 1. Test systému – online generátor



Obr. 27 – 2. Zadání údajů - online generátor



Obr. 28 – 3. Kontrola údajů – online generátor



Obr. 29 Generování párů klíčů a podpis žádosti – online generátor

Obr. 30 - Zadání PINu pro vytvoření klíčového páru a podpis žádosti

Obr. 31 – 4. Uložení žádosti – online generátor

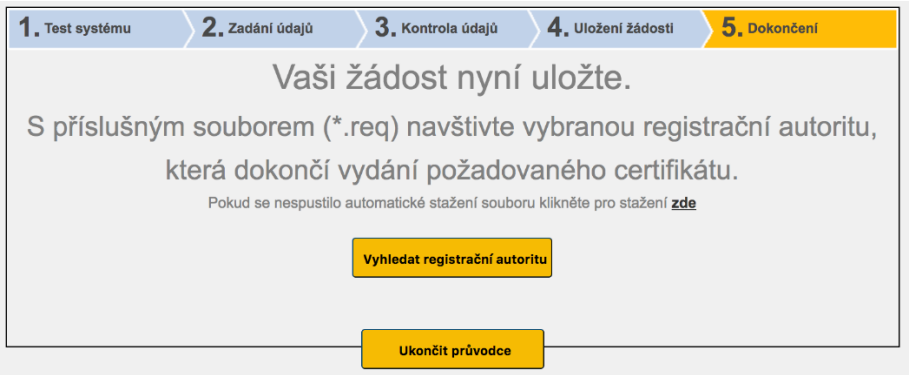
Výběr způsobu uložení žádosti o certifikát

Při volbě **„Uložení na server I.CA“** bude uživateli zaslán na kontaktní e-mail uvedený v žádosti o certifikát šestimístný číselný kód uložené žádosti na serveru I.CA.

Při volbě **„Uložení na lokální disk nebo externí úložiště“** se uloží soubor s vygenerovanou žádosti s názvem cert****.req.

Obr. 32 – 5. Dokončení – online generátor

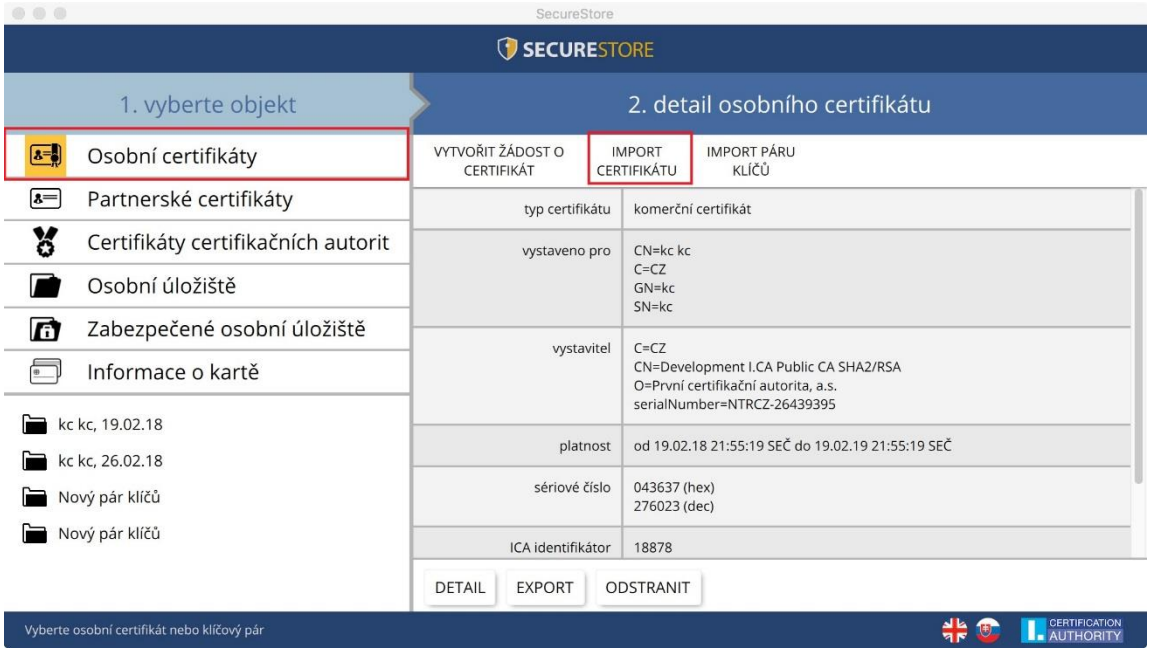
S šestimístným číselným kódem k uložené žádosti na serveru I.CA nebo se souborem req. na přenosném USB médiu následně uživatel navštíví registrační autoritu, kterou případně lze vyhledat tlačítkem **„Vyhledat registrační autoritu“.**



7.2.2. Import osobního certifikátu

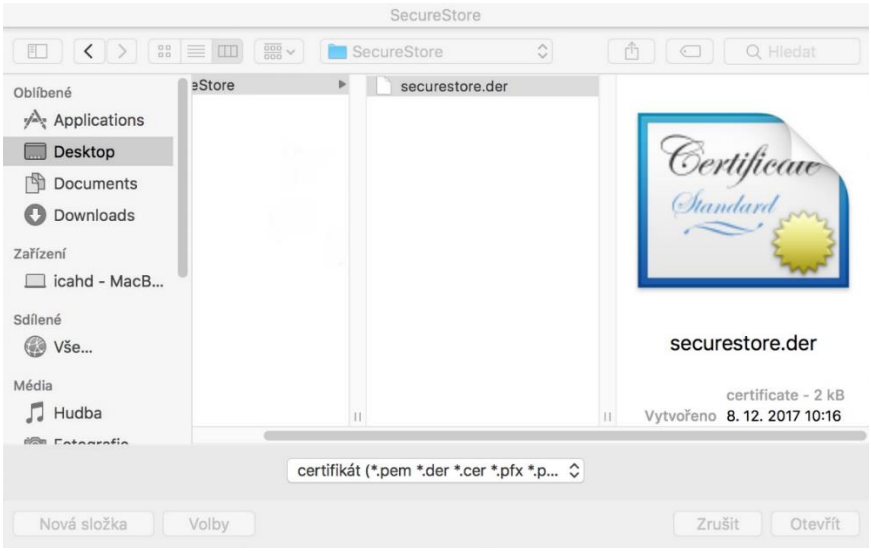
Funkce umožňuje import osobního certifikátu z disku na čipovou kartu. Certifikát se importuje ve formátu .cer / .der. Funkci uživatel nalezne v objektu **„Osobní certifikáty“.**

Obr. 33 – Import osobního certifikátu



Importovaný certifikát se uloží do toho úložiště na čipové kartě, které obsahuje klíče k certifikátu.

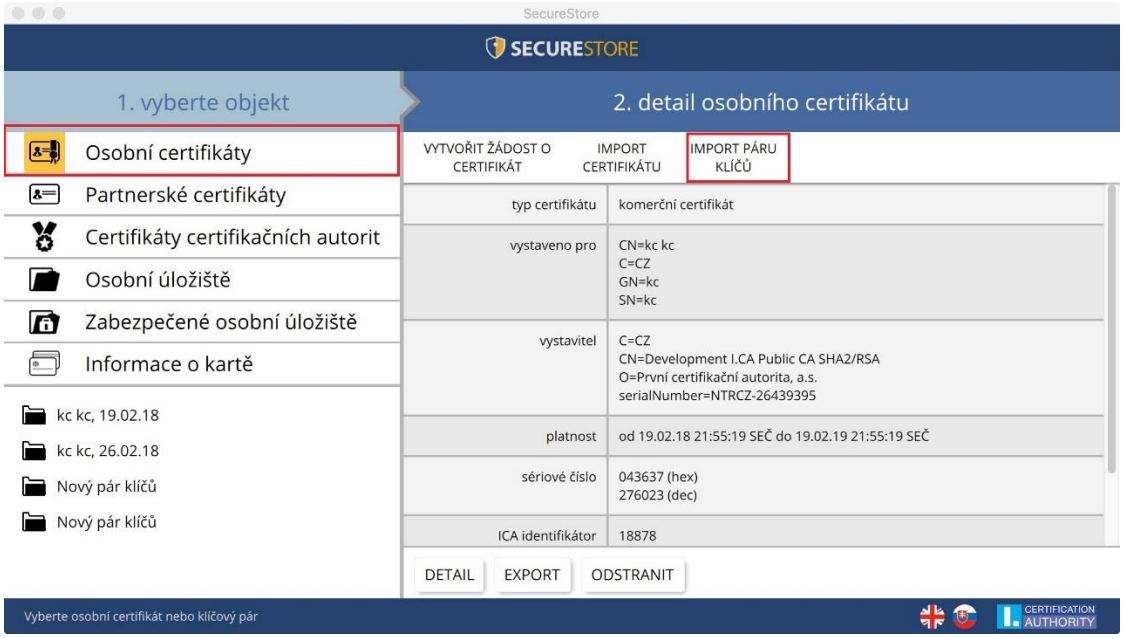
Obr. 34 Výběr souboru s certifikátem pro import na kartu



7.2.3. Import páru klíčů ze zálohy (PKCS#8)…

Volba importuje na kartu klíče, které byly během procesu generování žádosti o šifrovací certifikát uloženy na disk. Funkci uživatel nalezne v objektu **„Osobní certifikáty“**.

Obr. 35 – Import páru klíčů ze zálohy (PKCS#8)

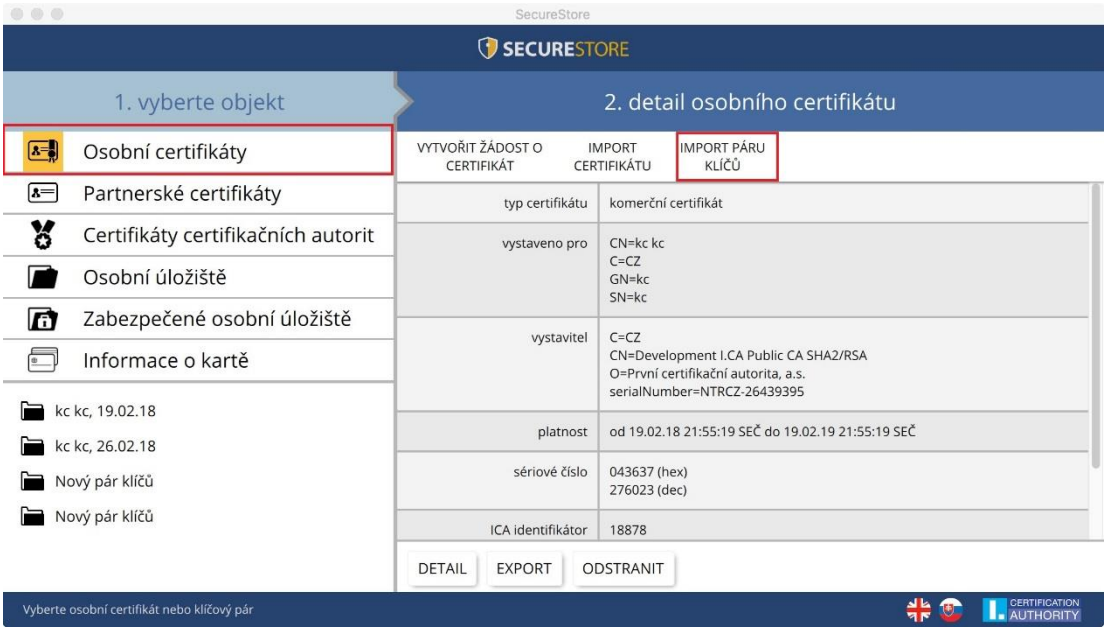


7.2.4. Import páru klíčů (PKCS#12)…

Volba importuje na kartu klíče s certifikátem, které jsou uloženy ve formátu PKCS#12 na disku.

Funkci uživatel nalezne v objektu **„Osobní certifikáty“**.

Obr. 36 – Import páru klíčů (PKCS#12)



8. Pojmy

- **Certifikační autorita** - nezávislý důvěryhodný subjekt, který klientovi vydává certifikát. Certifikační autorita garantuje jednoznačnou vazbu mezi klientem a jeho certifikátem.

- **Registrační autorita** - 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** - operace využívající klíče k šifrování a dešifrování. V případě čipové karty je využívaná tzv. asymetrická kryptografie, tj. pomocí dvojice klíčů je prováděno šifrování, dešifrování a je vytvářen a ověřován elektronický podpis.

- **Elektronický podpis** - údaje v elektronické podobě, které 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** - 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** - 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** - slouží jako 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** - 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 dodávaná ke každé kartě.

- **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.

- **Certifikát** - obdoba 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** - veřejná část páru klíčů uživatele, je určena pro ověřování elektronického podpisu a případně pro šifrování.

- **Soukromý klíč** - 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 (1 rok). 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.

- **Kvalifikovaný certifikát -** striktně řízen nařízením EU č. 910/2014 a slouží výhradně pro oblast elektronického podpisu. Vytváření, správa a použití kvalifikovaného certifikátu se řídí zvláštními příslušnými certifikačními politikami. I.CA poskytuje ve dvou variantách **Standard (privátní klíč uložen v MS Windows)** a **Comfort (privátní klíč uložen v čipové kartě).**

- **Komerční certifikát** - vydáván fyzickým nebo právnickým osobám, vhodný pro běžné využití. I.CA poskytuje ve dvou variantách **Standard (privátní klíč uložen v MS Windows)** a **Comfort (privátní klíč uložen v čipové kartě).**

- **Certifikát certifikační autority** - používán k ověřování správnosti a důvěryhodnosti klientských certifikátů. Jeho instalací na svém MACu 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.

- **Seznam veřejných certifikátů I.CA** - 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 komerčních a kvalifikovaných certifikátů I.CA naleznete zde:

  http://www.ica.cz/Verejne-certifikaty

- **Certifikační autority podporované kartou** - každá čipová karta vydaná I.CA má definovaný seznam tzv. podporovaných certifikačních autorit, jejichž certifikáty je možné na kartu uložit.

- **Následný certifikát** – je vydán klientovi na základě zaslané elektronické žádosti v době 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 nepopiratelnosti, 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 (nepopiratelnost)** - 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.