

První certifikační autorita, a.s.



I.CA SecureStore

Uživatelská příručka

Verze 8.0 a vyšší

datum vytvoření:	17.12.2024
verze:	8.0
počet stran:	34

OBSAH

1. Úvod.....	3
2. Přístupové údaje ke kartě	3
2.1 Inicializace karty	3
3. Základní obrazovka	4
3.1 Změna jazyka aplikace	4
3.2 Diagnostika	9
4. Zobrazení informací o páru klíčů.	12
4.1 Odstranění veřejného klíče	13
4.2 Odstranění kontejneru	14
4.3 Odstranění kontejneru pomocí průvodce smazáním klíče.....	14
5. Certifikáty.....	16
5.1 Zobrazení certifikátu.....	16
5.2 Práce s osobním certifikátem	17
5.3 Práce s kořenovým certifikátem CA	18
5.4 Registrace osobního certifikátu do Windows.....	19
6. Osobní úložiště	20
7. Ovládání aplikace.....	22
7.1 Nástrojová lišta pro Informace o kartě.....	22
7.2 Nástrojová lišta pro složku Osobní certifikáty.....	23
7.2.1 Vytvořit žádost o certifikát.....	23
7.2.3 Import páru klíčů ze zálohy a import klíčů.....	29
7.2.4 Import páru klíčů ze zálohy a import klíčů.....	30
8. Pojmy	31

1. Úvod

Uživatelská příručka je platná pro aplikaci I.CA SecureStore verze 8.0 a vyšší. 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 5 pokusů.

STARCOS 3.7

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 3krát za sebou uživatel zadá chybnou hodnotu PUKu, dojde k zablokování PUKu a tím i celé čipové karty.

Odblokování PINu pomocí PUKu je omezeno na 3 pokusy.

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 zabezpečené úložiště použijte PUK uvedený v předchozím odstavci.

Délka PINu pro zabezpečené úložiště je 4-12 číslic.

2.1 Inicializace karty

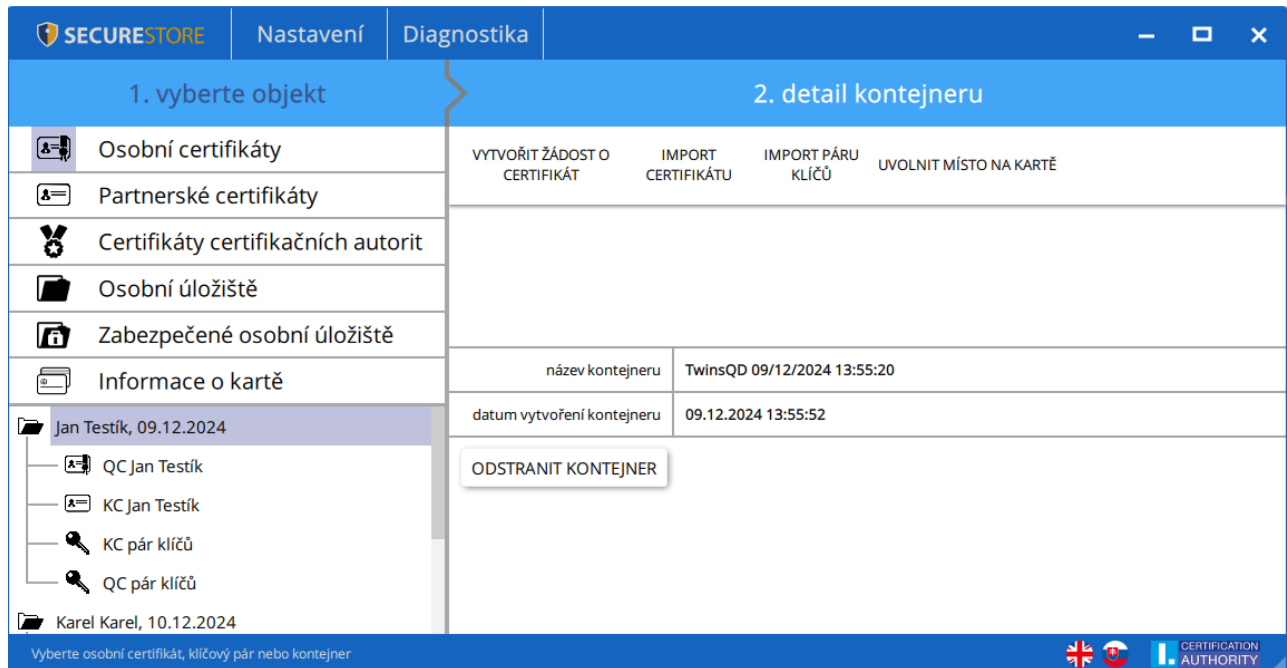
Inicializace karty spočívá v nastavení PINu a PUKu.

Pokud uživatel spolu s kartou obdržel i 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. V horní liště jsou uvedeny následující volby, viz obr. 3.

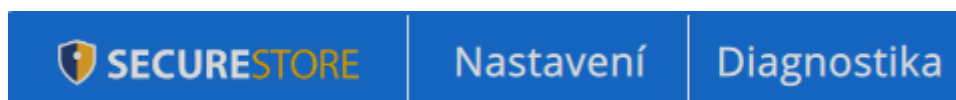
3.1 Změna jazyka aplikace

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

Obr. 2 - Změna jazyka



Obr. 3 - Hlavní lišta





Informaci o verzi aplikace uživatel zjistí kliknutím na ikonu

Obr. 4 - Verze aplikace

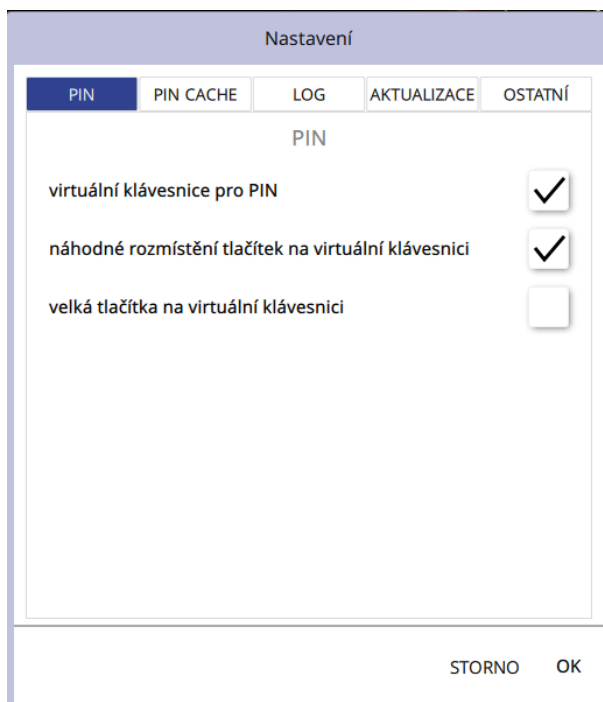


Volba **Nastavení** slouží pro:

1) *Upravení klávesnice pro zadání PIN*

Ve výchozím nastavení je aplikace nastavená na hodnotu „**Virtuální klávesnice pro PIN**“ a „**Náhodné rozmístění tlačítek na virtuální klávesnici pro PIN**“.

Obr. 5 – Nastavení klávesnice pro zadávání PIN



Uživatel poté zadává PIN na virtuální klávesnici kurzorem myši.

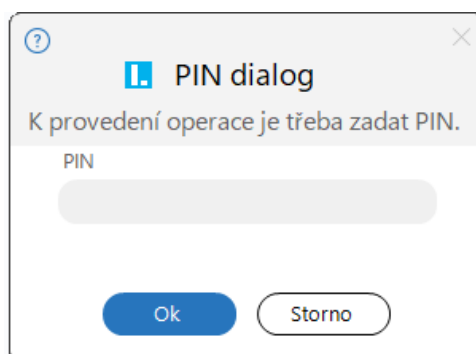
Obr. 6 – Virtuální klávesnice pro zadávání PIN



Je možné změnit zadávání PINu na numerickou klávesnici.

V „Nastavení“ je potřeba zvolit záložku „PIN“, odebrat možnost virtuální klávesnice pro PIN a potvrdit tlačítkem „OK“.

Obr. 7 – Klávesnice pro zadání PIN na numerické klávesnici



2) PIN CACHE – doba uložení PIN v paměti

Obr. 8 – Nastavení zapamatování PIN


- a) **Doba uložení PIN** (v minutách) – nastavení doby pro zapamatování PIN
- b) **Volba zapamatovat PIN** (zvoleno/nezvoleno) – uživatel si může navolit časový úsek, po jaký chce PIN zapamatovat, nastavení je zvlášť pro:
 - I. Ostatní – šifrovací a autentizační klíče
 - II. eSign – podpisové klíče

Poznámka: maximální doba pro zapamatování PIN pro podpisové klíče v eSign je 30 min, pro šifrovací klíče(ostatní) není doba omezena. Dále aplikace umožňuje zapamatování PIN ve vztahu k procesu aplikace.

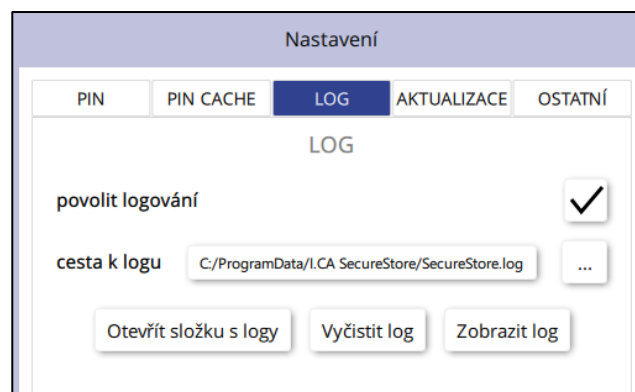
- c) **Potvrzovat použití uloženého PIN** – funkce, která umožňuje aktivovat potvrzovací dialog, který se zobrazí v době, kdy je PIN zapamatován a je vytvářen podpis klíčem na čipové kartě. V takovém případě se uživateli zobrazí hláška, zda souhlasí s použitím klíče a vytvořením podpisu

3) Povolení logování

Povolení logování aplikace, pro případnou analýzu technického problému při používání čipové karty a aplikace. Aplikace zaznamenává tzv. auditní log, kdy se v rámci operací s čipovou kartou budou do auditního logu zaznamenávat poslední provedené bezpečnostně citlivé operace, jako je mazání klíčů, generování klíčů apod.

Cestu k uloženému log souboru může uživatel změnit pomocí tlačítka 

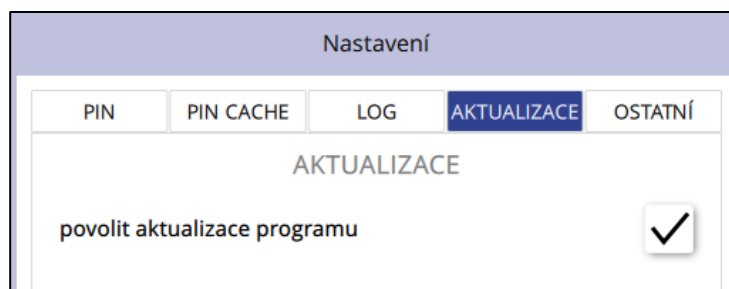
Obr. 10 – Log



4) Aktualizace

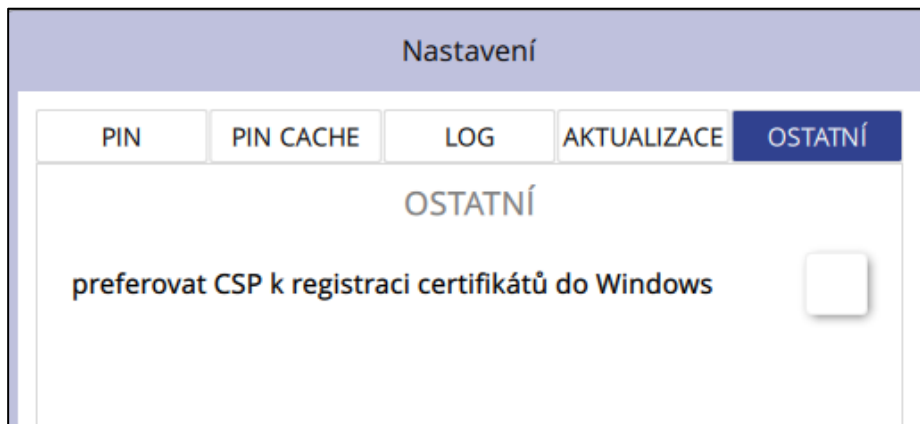
Nastavením lze povolit/zakázat online aktualizaci aplikace. Pokud dojde k vydání nové verze, je uživatel informován o nově dostupné vždy při spuštění aplikace.

Obr. 11 – Nastavení aktualizace aplikace



5) Ostatní

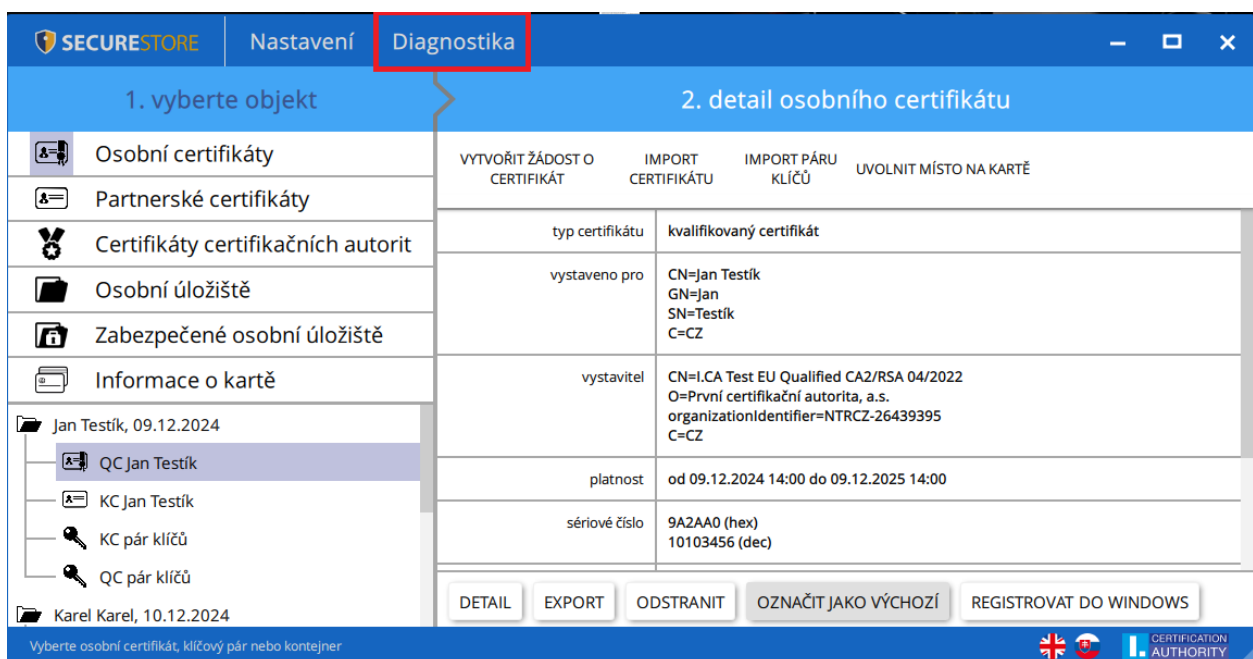
Nastavení certifikátu pod starším providerem.



3.2 Diagnostika

Součástí aplikace I.CA SecureStore je diagnostika, která zjistí stav CSP providerů (poskytovatelů kryptografických služeb) zaregistrovaných v MS Windows.

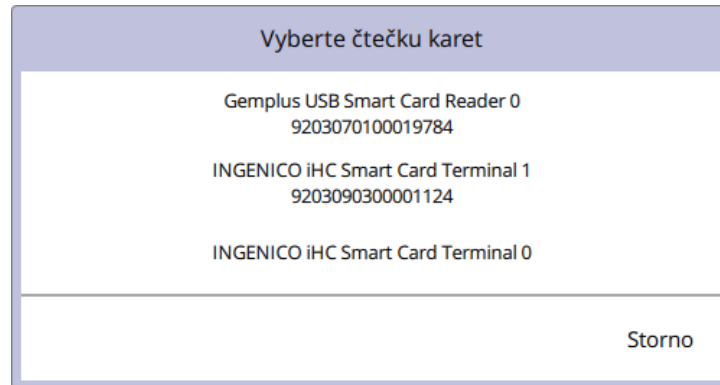
Obr. 12 – Diagnostika



Výběr čtečky čipových karet.

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

Obr. 13 - Výběr čtečky čipových karet

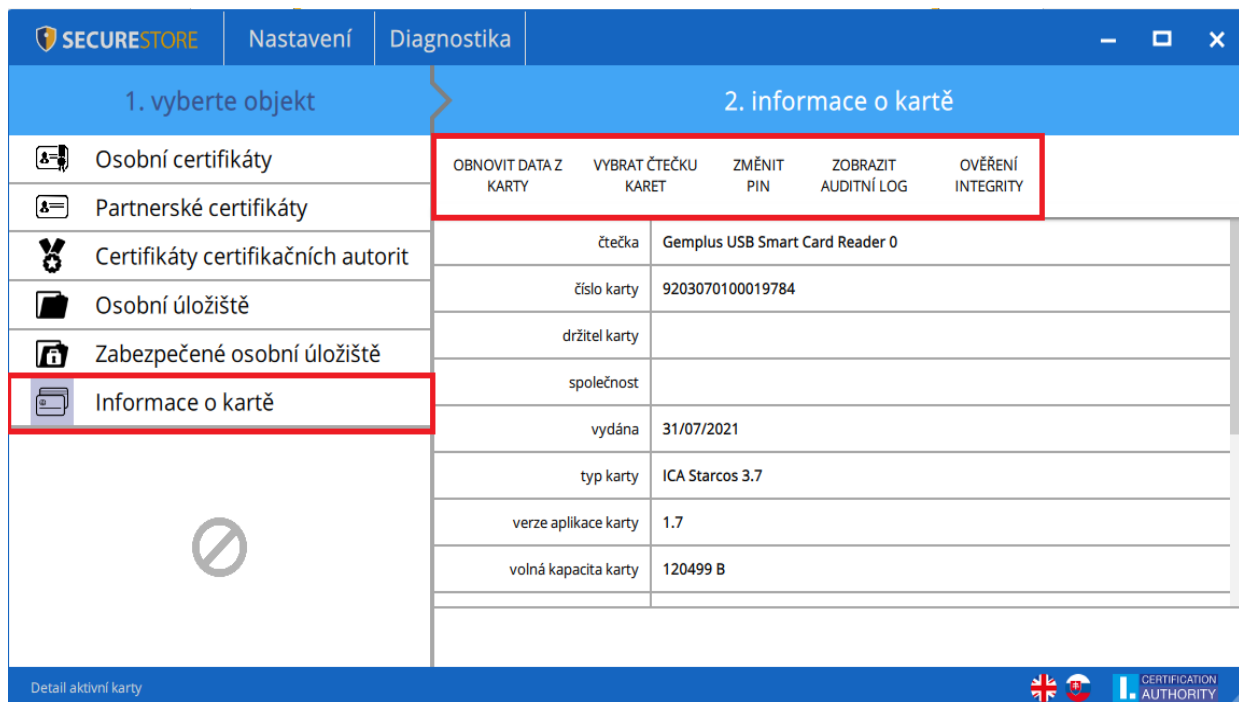


V případě, že má uživatel k PC připojenu pouze jednu čtečku čipových karet, není okno zobrazováno.

Nástrojová lišta

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

Obr. 14 - Nástrojová lišta



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

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

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

Obr. 15 - Změna PINu

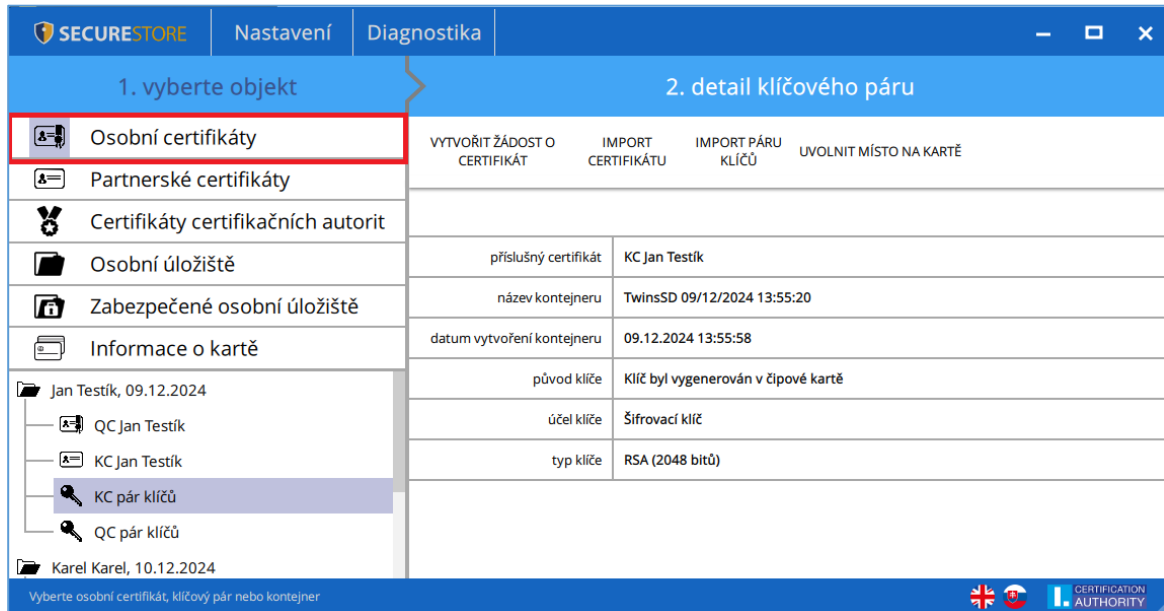
The image shows a dialog box titled "Změna PINu". It contains three text input fields stacked vertically. The first field is labeled "Současný PIN", the second "nový PIN", and the third "nový PIN znovu". Below the input fields, there is a horizontal line, and at the bottom right of the dialog, there are two buttons: "STORNO" and "OK".











- a) **Starcos 3.5** – Volba **změna PIN** umožňuje změnit PIN za předpokladu, že je známá hodnota původního PINu. Volba **Odblokovat PIN** umožňuje nastavit novou hodnotu PIN v případě, že si uživatel PIN zablokuje. K odblokování nastavení nového PINu je vyžadováno zadání PUKu. **Odblokování PINu pomocí PUKu je omezeno na 5 pokusů.**
- b) **Starcos 3.7** – Volba **změna PIN** umožňuje změnit PIN za předpokladu, že je známá hodnota původního PINu. Volba **Odblokovat PIN** slouží pro případ, že si uživatel PIN zablokuje. K odblokování PINu je vyžadováno zadání PUKu. Zadáním PUKu uživatel aktivuje nové 3 pokusy na zadání správného PINu. **Odblokování PINu pomocí PUKu je omezeno na 3 pokusy.**

4. Zobrazení informací o páru klíčů.

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

Obr. 16 – Zobrazení informací o páru klíčů



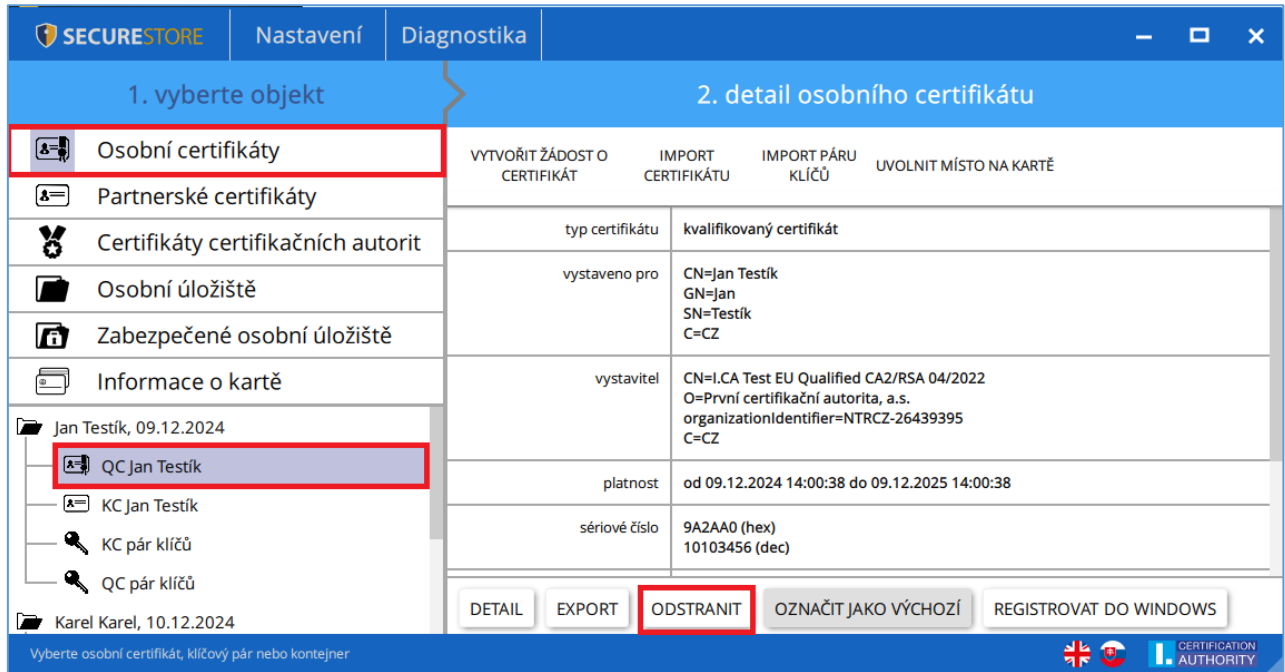
1. vyberte objekt		2. detail klíčového páru	
 Osobní certifikáty		VYTVORIT ŽÁDOST O CERTIFIKÁT	IMPORT CERTIFIKÁTU
 Partnerské certifikáty		IMPORT PÁRU KLÍČŮ	UVOLNIT MÍSTO NA KARTĚ
 Certifikáty certifikačních autorit			
 Osobní úložiště		příslušný certifikát	KC Jan Testík
 Zabezpečené osobní úložiště		název kontejneru	TwinsSD 09/12/2024 13:55:20
 Informace o kartě		datum vytvoření kontejneru	09.12.2024 13:55:58
Jan Testík, 09.12.2024		původ klíče	Klíč byl vygenerován v čipové kartě
 QC Jan Testík		účel klíče	Šifrovací klíč
 KC Jan Testík		typ klíče	RSA (2048 bitů)
 KC pár klíčů			
 QC pár klíčů			
Karel Karel, 10.12.2024			

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 veřejného klíče

Volbu uživatel nalezne v objektu „Osobní certifikáty“, vybere požadovaný veřejný klíč a tlačítkem „Odstranit“ provede odstranění.

Obr. 17 - Odstranění veřejného klíče



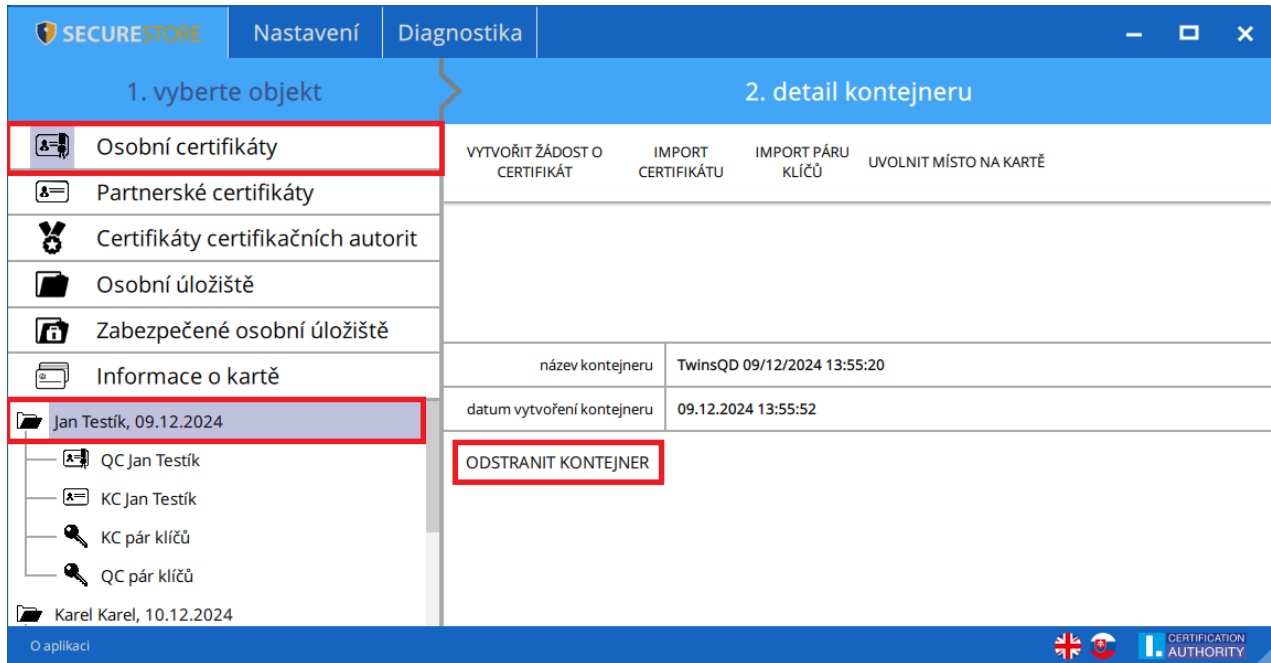
The screenshot shows the SECURESTORE application interface. The left sidebar is titled "1. vyberte objekt" and contains a tree view of objects. The "Osobní certifikáty" (Personal Certificates) folder is selected, and its contents are expanded to show "QC Jan Testík", "KC Jan Testík", "KC pár klíčů", and "QC pár klíčů". The "QC Jan Testík" item is highlighted with a red box. The main area is titled "2. detail osobního certifikátu" and displays details for the selected certificate. At the bottom of the main area, the "ODSTRANIT" button is highlighted with a red box.

1. vyberte objekt		2. detail osobního certifikátu			
Osobní certifikáty		VYTVORIT ŽÁDOST O CERTIFIKÁT	IMPORT CERTIFIKÁTU	IMPORT PÁRU KLÍČŮ	UVOLNIT MÍSTO NA KARTĚ
Partnerské certifikáty		typ certifikátu	kvalifikovaný certifikát		
Certifikáty certifikačních autorit		vystaveno pro	CN=Jan Testík GN=Jan SN=Testík C=CZ		
Osobní úložiště		vystavitel	CN=I,CA Test EU Qualified CA2/RSA 04/2022 O=První certifikační autorita, a.s. organizationIdentifier=NTRCZ-26439395 C=CZ		
Zabezpečené osobní úložiště		platnost	od 09.12.2024 14:00:38 do 09.12.2025 14:00:38		
Informace o kartě		sériové číslo	9A2AA0 (hex) 10103456 (dec)		
Jan Testík, 09.12.2024		DETAIL EXPORT ODSTRANIT OZNAČIT JAKO VÝCHOZÍ REGISTROVAT DO WINDOWS			
QC Jan Testík					
KC Jan Testík					
KC pár klíčů					
QC pár klíčů					
Karel Karel, 10.12.2024					

Vyberte osobní certifikát, klíčový pár nebo kontejner

4.2 Odstranění kontejneru

Volbu uživatel nalezne v objektu „Osobní certifikáty“, vybere požadovaný kontejner a tlačítkem „odstranit kontejner“, po zadání PINu provede jeho odstranění.

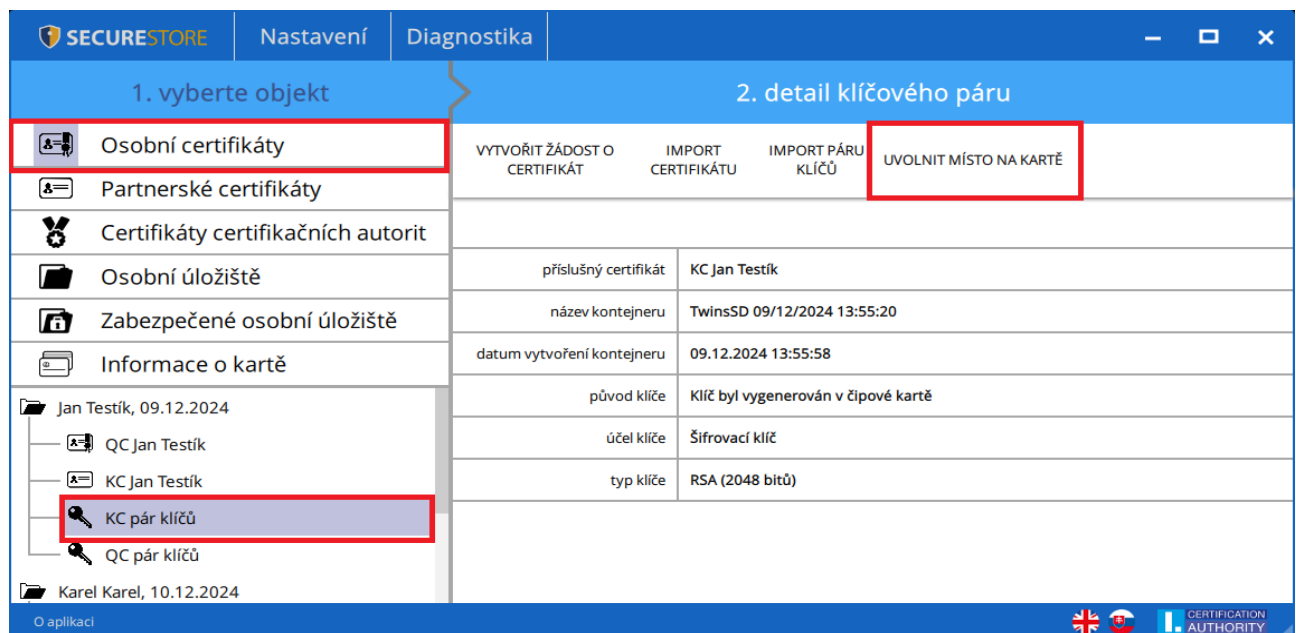


Upozornění: Pokud uživatel odstraní kontejner je tato relace nenávratná a nepůjde již certifikátem podepisovat / dešifrovat!!!

4.3 Odstranění kontejneru pomocí průvodce smazáním klíče

Volbu uživatel nalezne v objektu „Osobní certifikáty“, vybere požadovaný klíčový pár a spustí funkci „Uvolnit místo na kartě“.

Obr. 19 - Průvodce smazáním klíče



Obr. 20 Průvodce smazáním klíčů a certifikátů

Průvodce smazáním klíčů a certifikátů

Kontejnery k odstranění

<input checked="" type="checkbox"/>	Jan Testík	Datum vypršení platnosti: 09.12.2025 14:00:48
název kontejneru	TwinsSD 09/12/2024 13:55:20	
čas vytvoření kontejneru	09.12.2024 13:55:58	
certifikát pro	Jan Testík	
sériové číslo	01B285 (hex) 111237 (dec)	
platnost (od-do)	od 09.12.2024 14:00:48 do 09.12.2025 14:00:48	

Označením certifikátu se zobrazí volba „Smazat“. Tím se smaže celý kontejner.

Pokud uživatel odstraní kontejner je tato relace nenávratná a nepůjde již certifikátem podepisovat/dešifrovat!!!

Volba „Odstranit certifikát“ je umožněna pouze pro komerční certifikáty a slouží pro odstranění pouze veřejného klíče stejně jako v bodu [4.1](#)

Po kliknutí na volbu „Odstranit“ je uživatel vyzván k zadání PIN, po zadání PIN bude označený certifikát/kontejner odstraněn

Obr. 21 – Zadání PINu pro odstranění certifikátu/kontejneru

Zadejte PIN

PIN

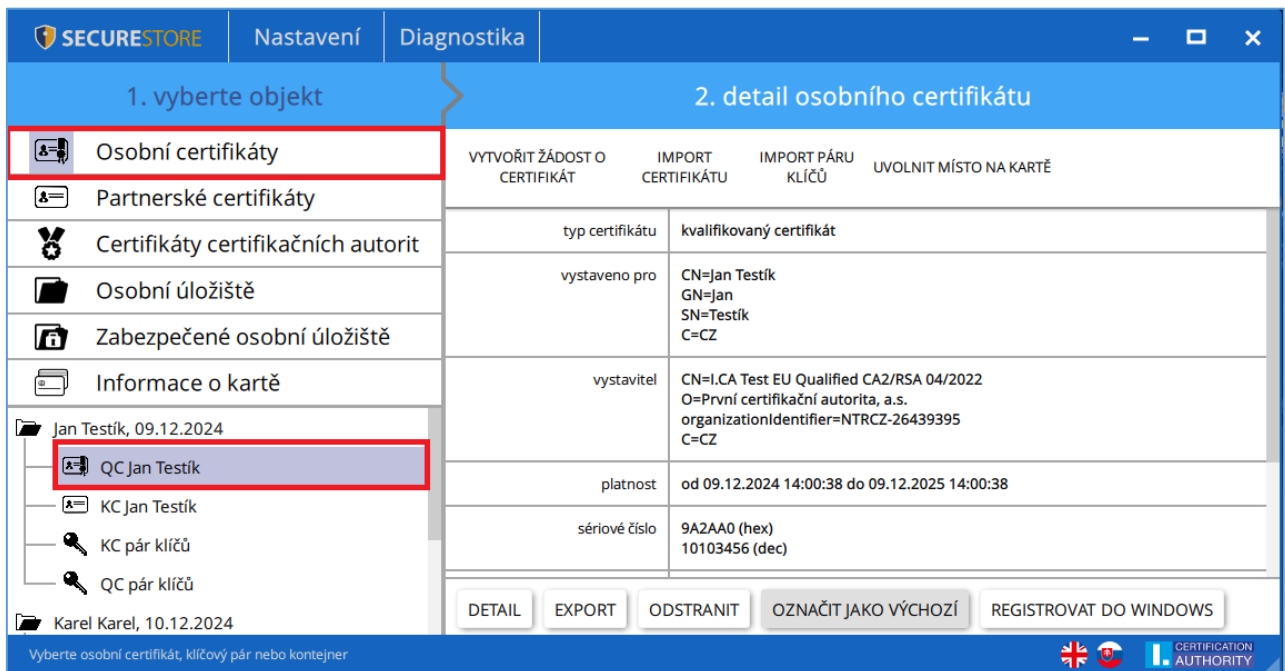
STORNO OK

5. Certifikáty

5.1 Zobrazení certifikátu

Uživatel vybere certifikát ke kterému chce zobrazit podrobnosti v objektu „Osobní certifikáty“. Detail certifikátu se zobrazí v pravé obrazovce aplikace v „Detailu osobního certifikátu“.

Obr. 22 – Zobrazení certifikátu



The screenshot shows the SECURESTORE application interface. The top navigation bar includes 'SECURESTORE', 'Nastavení', and 'Diagnostika'. The main content is split into two panes: '1. vyberte objekt' and '2. detail osobního certifikátu'.

1. vyberte objekt:

- Osobní certifikáty (highlighted with a red box)
- Partnerské certifikáty
- Certifikáty certifikačních autorit
- Osobní úložiště
- Zabezpečené osobní úložiště
- Informace o kartě
- Jan Testík, 09.12.2024
 - QC Jan Testík (highlighted with a red box)
 - KC Jan Testík
 - KC pár klíčů
 - QC pár klíčů
- Karel Karel, 10.12.2024

2. detail osobního certifikátu:

Buttons: VYTVOŘIT ŽÁDOST O CERTIFIKÁT, IMPORT CERTIFIKÁTU, IMPORT PÁRU KLÍČŮ, UVOLNIT MÍSTO NA KARTĚ

typ certifikátu	kvalifikovaný certifikát
vystaveno pro	CN=Jan Testík GN=Jan SN=Testík C=CZ
vystavitel	CN=I.CA Test EU Qualified CA2/RSA 04/2022 O=První certifikační autorita, a.s. organizationIdentifier=NTRCZ-26439395 C=CZ
platnost	od 09.12.2024 14:00:38 do 09.12.2025 14:00:38
sériové číslo	9A2AA0 (hex) 10103456 (dec)

Buttons: DETAIL, EXPORT, ODSTRANIT, OZNAČIT JAKO VÝCHOZÍ, REGISTROVAT DO WINDOWS

Footer: Vyberte osobní certifikát, klíčový pár nebo kontejner. CERTIFICATION AUTHORITY logo.

5.2 Práce s osobním certifikátem

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

V objektu „Osobní certifikáty“ vybere uživatel požadovaný certifikát a následně zvolí požadovanou operaci v nástrojové liště.

Obr. 23 - Volby pro práci s osobním certifikátem v nástrojové liště

1. vyberte objekt		2. detail osobního certifikátu			
Osobní certifikáty		VYTVOŘIT ŽÁDOST O CERTIFIKÁT	IMPORT CERTIFIKÁTU	IMPORT PÁRU KLÍČŮ	UVOLNIT MÍSTO NA KARTĚ
Partnerské certifikáty		typ certifikátu	kvalifikovaný certifikát		
Certifikáty certifikačních autorit		vystaveno pro	CN=Jan Testík GN=Jan SN=Testík C=CZ		
Osobní úložiště		vystavitel	CN=I.CA Test EU Qualified CA2/RSA 04/2022 O=První certifikační autorita, a.s. organizationIdentifier=NTRCZ-26439395 C=CZ		
Zabezpečené osobní úložiště		platnost	od 09.12.2024 14:00:38 do 09.12.2025 14:00:38		
Informace o kartě		sériové číslo	9A2AA0 (hex) 10103456 (dec)		
Jan Testík, 09.12.2024		<input type="button" value="DETAIL"/> <input type="button" value="EXPORT"/> <input type="button" value="ODSTRANIT"/> <input type="button" value="OZNAČIT JAKO VÝCHOZÍ"/> <input type="button" value="REGISTROVAT DO WINDOWS"/>			
QC Jan Testík					
KC Jan Testík					
KC pár klíčů					
QC pár klíčů					
Karel Karel, 10.12.2024					

Obr. 24 - Volby pro import certifikátu

1. vyberte objekt		2. detail osobního certifikátu			
Osobní certifikáty		VYTVOŘIT ŽÁDOST O CERTIFIKÁT	IMPORT CERTIFIKÁTU	IMPORT PÁRU KLÍČŮ	UVOLNIT MÍSTO NA KARTĚ
Partnerské certifikáty		typ certifikátu	kvalifikovaný certifikát		
Certifikáty certifikačních autorit		vystaveno pro	CN=Jan Testík GN=Jan SN=Testík C=CZ		
Osobní úložiště		vystavitel	CN=I.CA Test EU Qualified CA2/RSA 04/2022 O=První certifikační autorita, a.s. organizationIdentifier=NTRCZ-26439395 C=CZ		
Zabezpečené osobní úložiště		platnost	od 09.12.2024 14:00:38 do 09.12.2025 14:00:38		
Informace o kartě		sériové číslo	9A2AA0 (hex) 10103456 (dec)		
Jan Testík, 09.12.2024		<input type="button" value="DETAIL"/> <input type="button" value="EXPORT"/> <input type="button" value="ODSTRANIT"/> <input type="button" value="OZNAČIT JAKO VÝCHOZÍ"/> <input type="button" value="REGISTROVAT DO WINDOWS"/>			
QC Jan Testík					
KC Jan Testík					
KC pár klíčů					
QC pár klíčů					
Karel Karel, 10.12.2024					

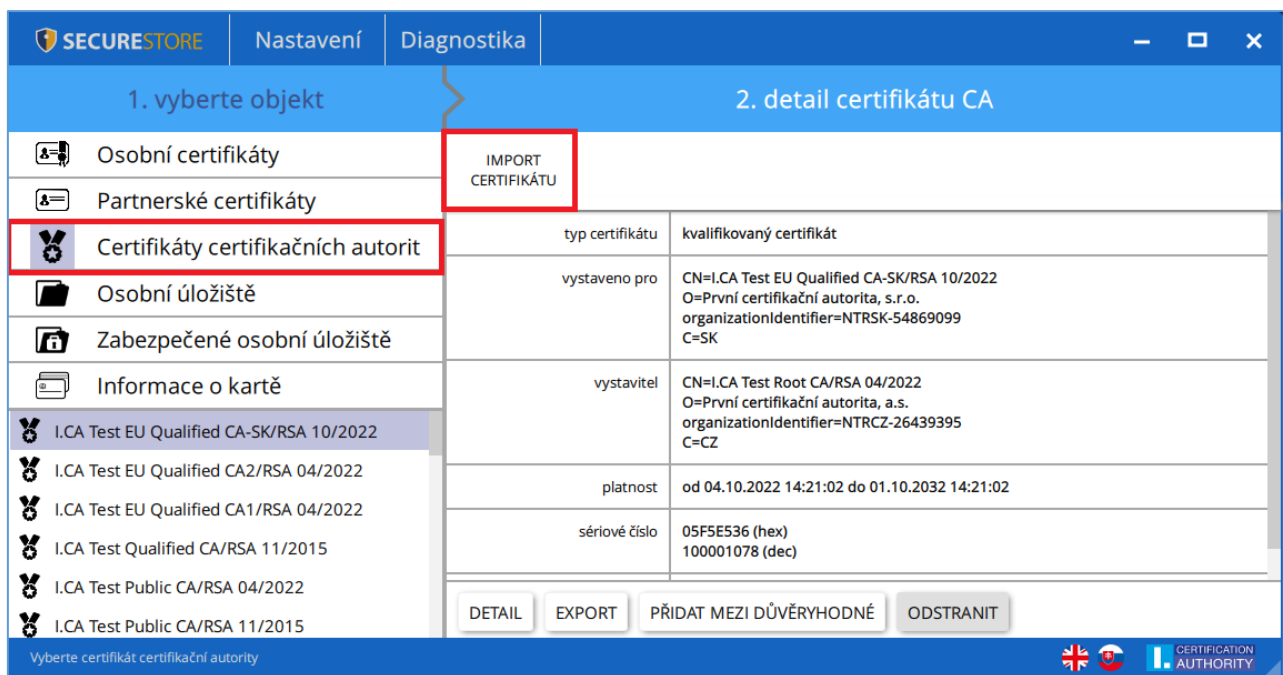
Osobní certifikát je importován do úložiště, ve kterém je uložen odpovídající pár klíčů. Jako partnerské certifikáty mohou být importovány certifikáty komunikačních partnerů. Zobrazení holých dat certifikátu slouží pouze pro odborníky pro vizuální kontrolu dat certifikátu.

5.3 Práce s kořenovým certifikátem CA

Nová čipová 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. nebo .icf, Certifikáty I.CA ve formátu .cmf jsou ke stažení na <http://www.ica.cz/Korenove-certifikaty>.

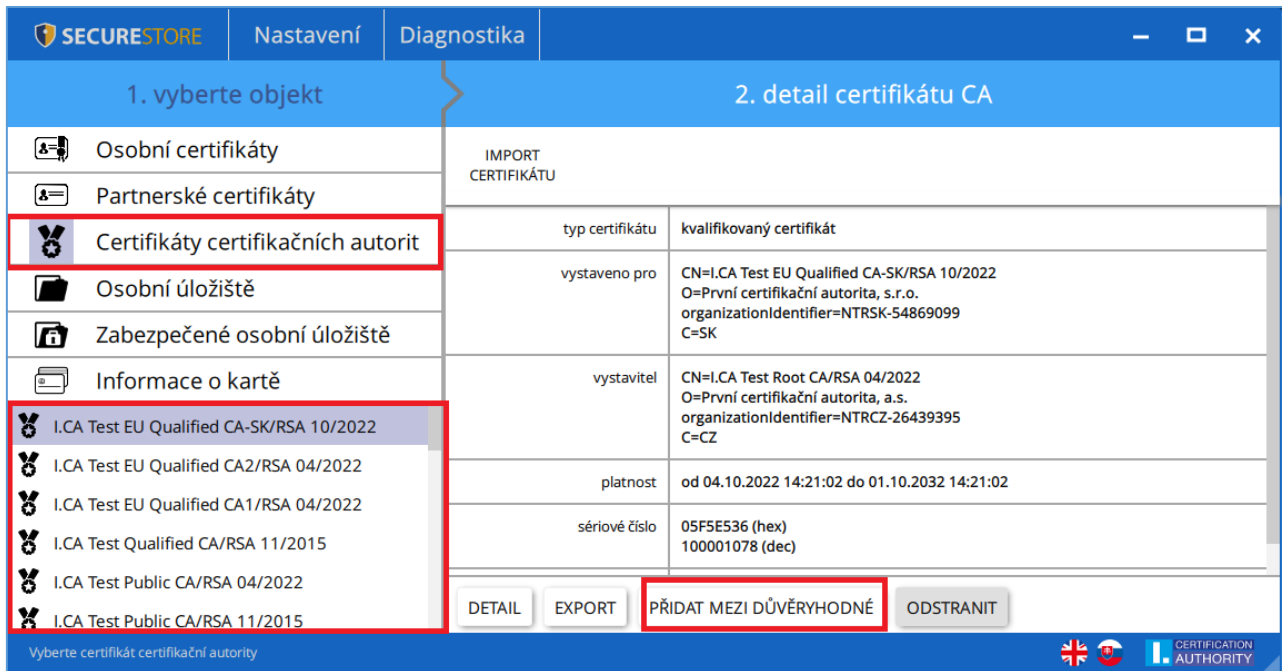
Obr.25 – Import certifikátu certifikační autority



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 uživatel používá starší verzi Windows a kořenové certifikáty I.CA nejsou součástí Windows, registrujte si kořenový certifikát z čipové karty. K registraci použijte volbu „**Přidat mezi důvěryhodné**“, viz obrázek obr. 26. Registrace kořenového certifikátu do Windows vyžaduje souhlas uživatele, následně je kořenový certifikát registrován do MS Windows jako důvěryhodný kořenový certifikát.

Obr. 26 - Registrace certifikátu certifikační autority do Windows

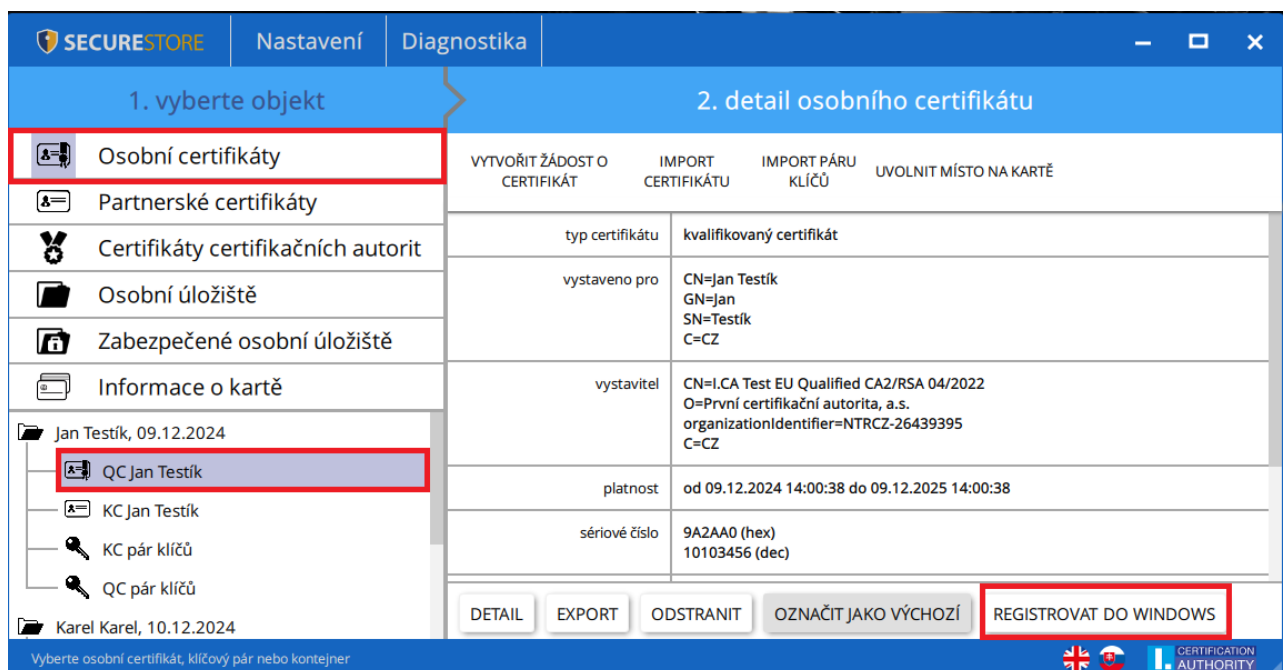


1. vyberte objekt		2. detail certifikátu CA	
Osobní certifikáty		IMPORT CERTIFIKÁTU	
Partnerské certifikáty		typ certifikátu	kvalifikovaný certifikát
Certifikáty certifikačních autorit		vystaveno pro	CN=I.CA Test EU Qualified CA-SK/RSA 10/2022 O=První certifikační autorita, s.r.o. organizationIdentifier=NTRSK-54869099 C=SK
Osobní úložiště		vystavitel	CN=I.CA Test Root CA/RSA 04/2022 O=První certifikační autorita, a.s. organizationIdentifier=NTRCZ-26439395 C=CZ
Zabezpečené osobní úložiště		platnost	od 04.10.2022 14:21:02 do 01.10.2032 14:21:02
Informace o kartě		sériové číslo	05F5E536 (hex) 100001078 (dec)
I.CA Test EU Qualified CA-SK/RSA 10/2022		<input type="button" value="DETAIL"/> <input type="button" value="EXPORT"/> <input type="button" value="PŘIDAT MEZI DŮVĚRYHODNÉ"/> <input type="button" value="ODSTRANIT"/>	
I.CA Test EU Qualified CA2/RSA 04/2022			
I.CA Test EU Qualified CA1/RSA 04/2022			
I.CA Test Qualified CA/RSA 11/2015			
I.CA Test Public CA/RSA 04/2022			
I.CA Test Public CA/RSA 11/2015			

5.4 Registrace osobního certifikátu do Windows

Většina aplikací vyžaduje, aby byl osobní certifikát, se kterým požaduje uživatel pracovat, registrovaný ve Windows. Registraci certifikátů je možno provést jednotlivě pro každý certifikát pomocí volby „**Registrovat do Windows**“. Volba zaregistruje osobní certifikát z čipové karty do osobního úložiště ve Windows. Funkci uživatel naleznete v objektu „**Osobní certifikáty**“, v objektu vybere požadovaný certifikát k zaregistrování.

Obr. 27 Registrace Osobního certifikátu do Windows

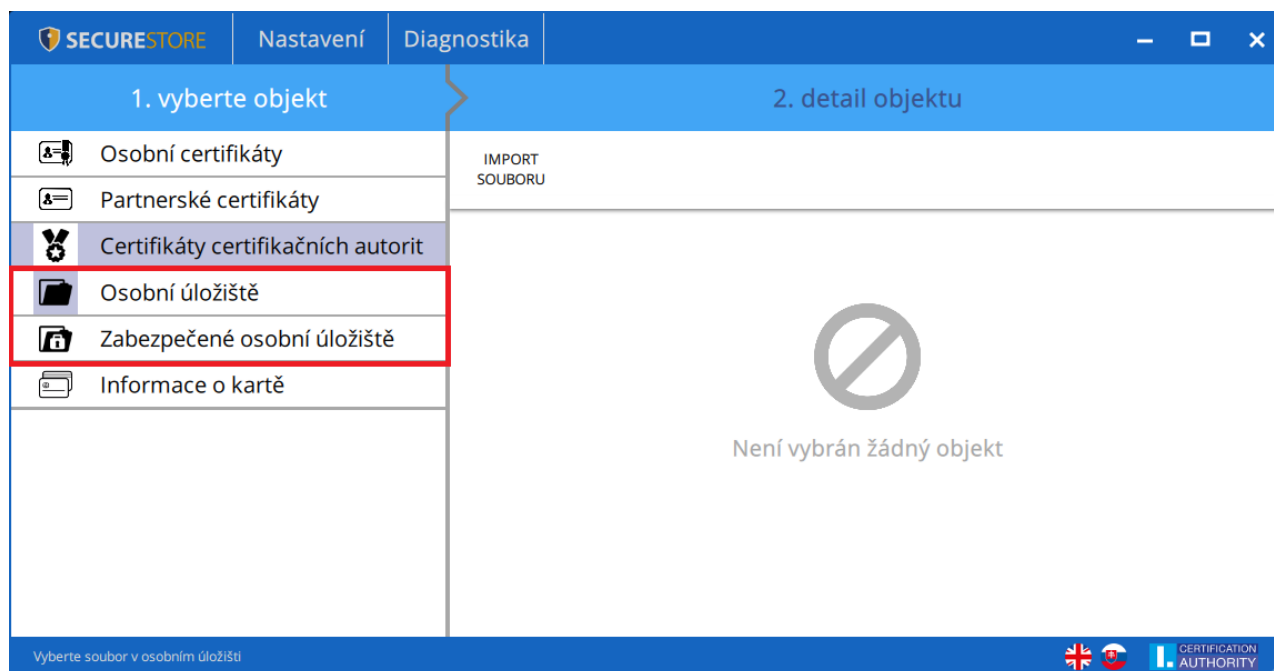


1. vyberte objekt		2. detail osobního certifikátu	
Osobní certifikáty		VYTVOŘIT ŽÁDOST O CERTIFIKÁT IMPORT CERTIFIKÁTU IMPORT PÁRU KLÍČŮ UVOLNIT MÍSTO NA KARTĚ	
Partnerské certifikáty		typ certifikátu	kvalifikovaný certifikát
Certifikáty certifikačních autorit		vystaveno pro	CN=Jan Testík GN=Jan SN=Testík C=CZ
Osobní úložiště		vystavitel	CN=I.CA Test EU Qualified CA2/RSA 04/2022 O=První certifikační autorita, a.s. organizationIdentifier=NTRCZ-26439395 C=CZ
Zabezpečené osobní úložiště		platnost	od 09.12.2024 14:00:38 do 09.12.2025 14:00:38
Informace o kartě		sériové číslo	9A2AA0 (hex) 10103456 (dec)
Jan Testík, 09.12.2024		<input type="button" value="DETAIL"/> <input type="button" value="EXPORT"/> <input type="button" value="ODSTRANIT"/> <input type="button" value="OZNAČIT JAKO VÝCHOZÍ"/> <input type="button" value="REGISTROVAT DO WINDOWS"/>	
QC Jan Testík			
KC Jan Testík			
KC pár klíčů			
QC pár klíčů			
Karel Karel, 10.12.2024			

6. Osobní úložiště

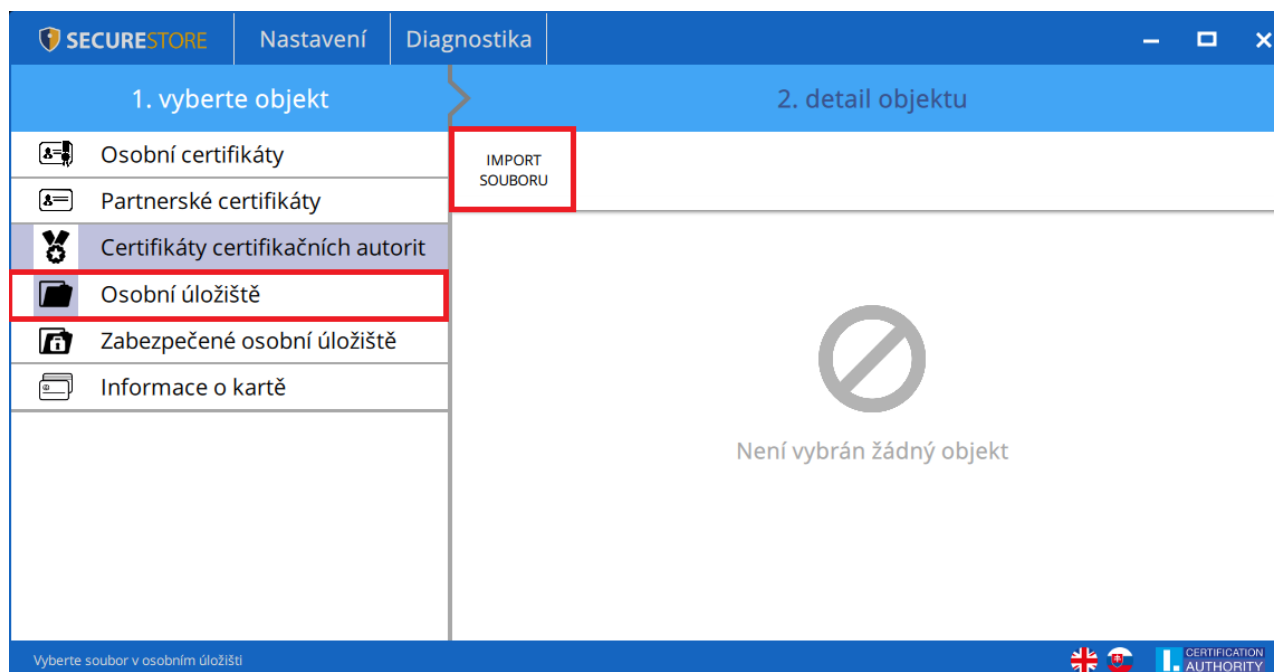
Do části karty nazvané „**Osobních úložiště**“ resp. „**Zabezpečená osobní úložiště**“ si může uživatel ukládat malé soubory (několik málo kB). Na kartu lze uložit jak textový, tak binární soubor. Čtení a export souboru v zabezpečeném úložišti je chráněn PINem pro zabezpečené úložiště, viz. kapitola 2.

Obr. 28 – Osobní úložiště



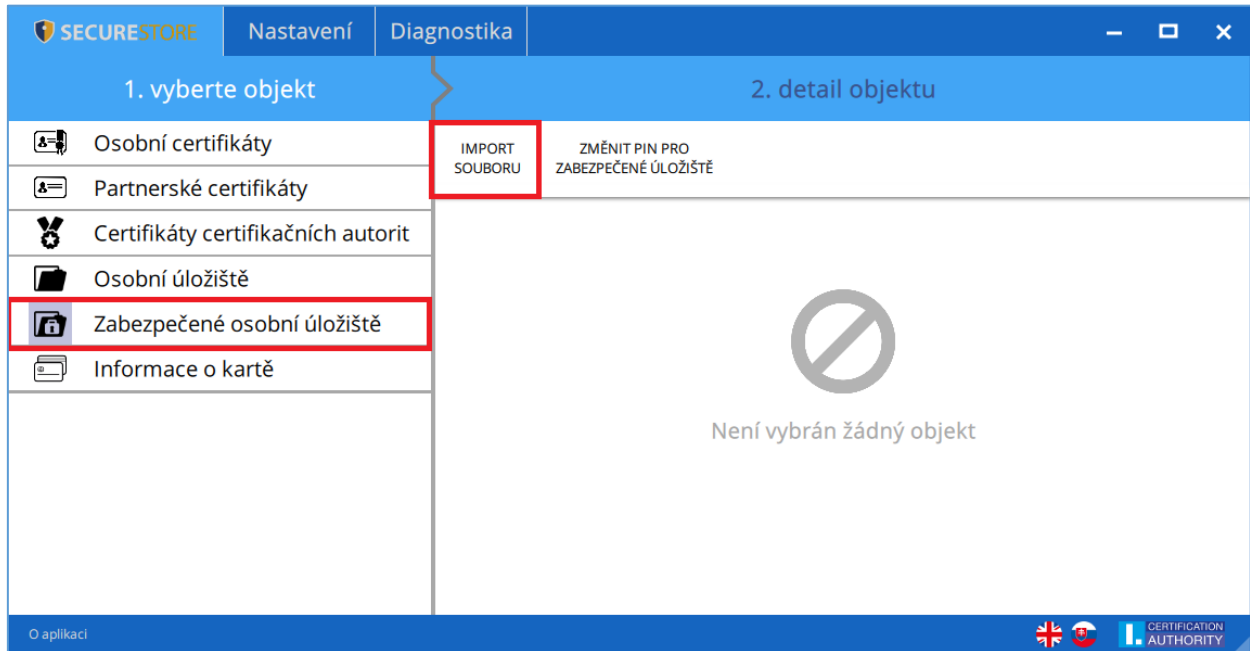
Funkci uživatel nalezne v objektu „**Osobní úložiště**“ a v detailu objektu „**Import souboru**“.

Obr. 29 - Import souboru do osobního úložiště



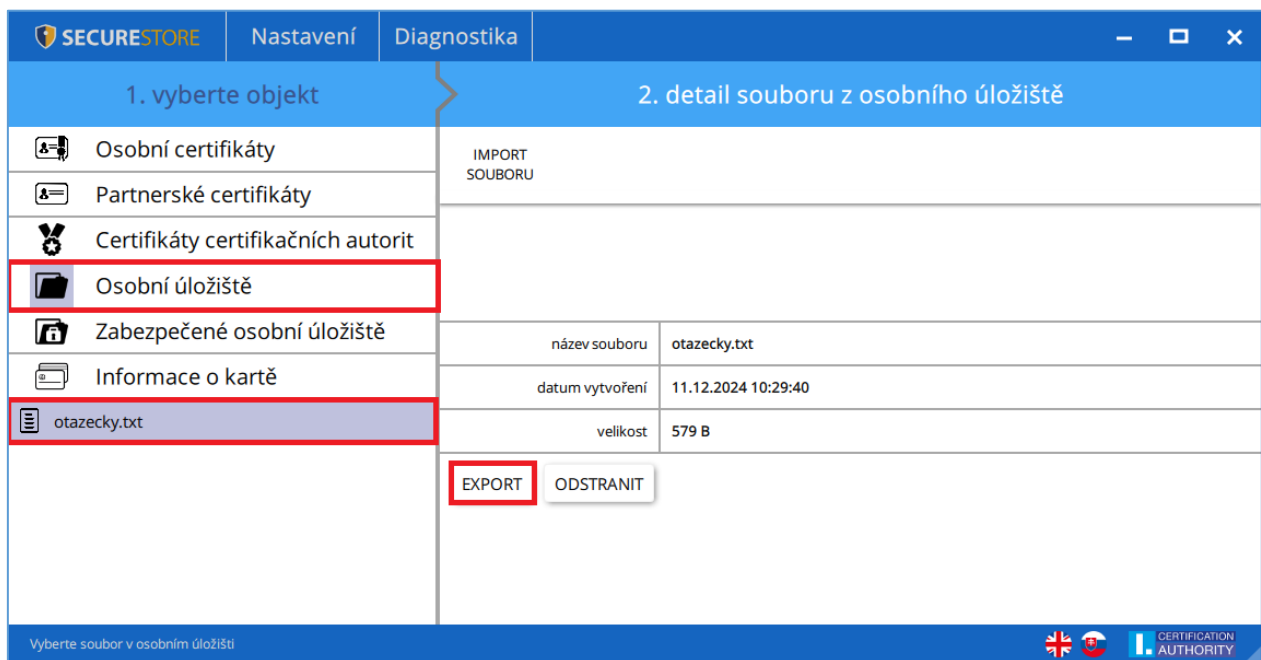
Funkci uživatel nalezne v objektu „Zabezpečené Osobní úložiště“ a v detailu objektu „Import souboru“.

Obr. 30 - Import souboru do zabezpečeného úložiště



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

Obr. 31 - Export souboru z osobního úložiště



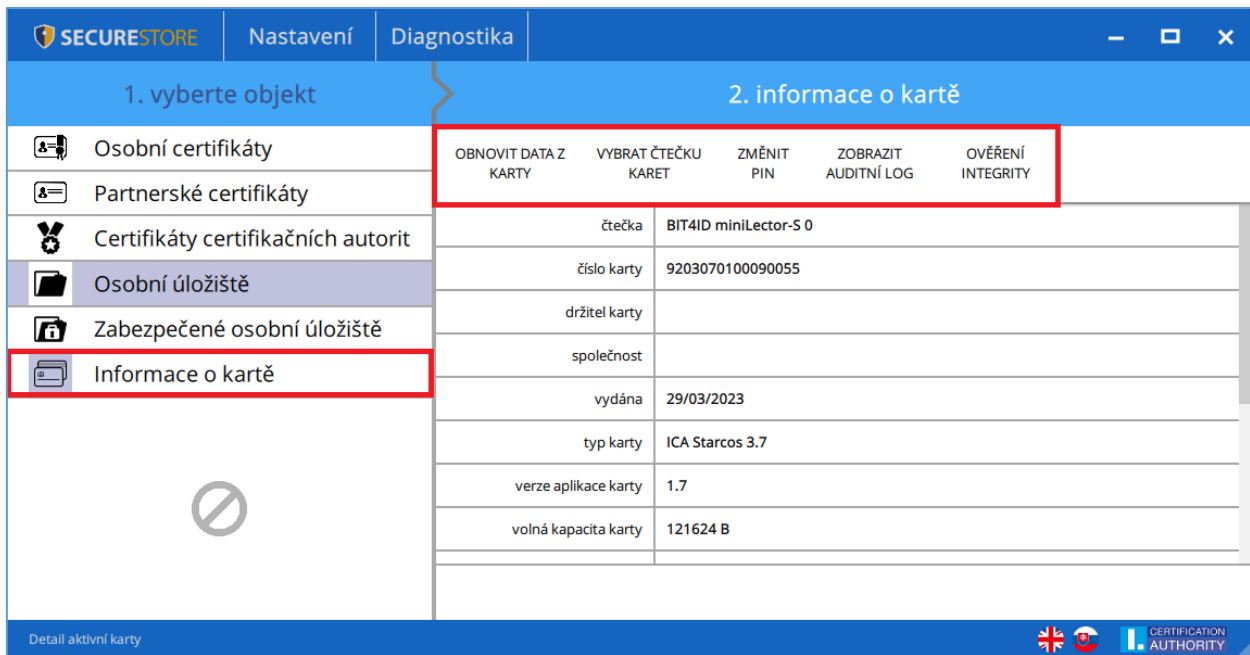
7. Ovládání aplikace

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. 32 – Nástrojová lišta pro objekt „Informace o kartě“



The screenshot shows the application interface with the 'Informace o kartě' tool selected. The tool list on the left includes: Osobní certifikáty, Partnerské certifikáty, Certifikáty certifikačních autorit, Osobní úložiště, Zabezpečené osobní úložiště, and Informace o kartě (highlighted). The right pane shows the tool list for 'Informace o kartě' with buttons: OBNOVIT DATA Z KARTY, VYBRAT ČTEČKU KARET, ZMĚNIT PIN, ZOBRAZIT AUDITNÍ LOG, and OVĚŘENÍ INTEGRITY. Below the buttons is a table of card details.

čtečka	BIT4ID miniLector-S 0
číslo karty	9203070100090055
držitel karty	
společnost	
vydána	29/03/2023
typ karty	ICA Starcos 3.7
verze aplikace karty	1.7
volná kapacita karty	121624 B

Detail aktivní karty

7.2 Nástrojová lišta pro složku Osobní certifikáty

Obr. 33 - Nástrojová lišta pro objekt „Osobní certifikáty“

The screenshot shows the SECURESTORE interface with the 'Nastavení' and 'Diagnostika' tabs. The main area is divided into two sections: '1. vyberte objekt' and '2. detail osobního certifikátu'. In the '1. vyberte objekt' section, 'Osobní certifikáty' is selected. Below it, a list of tools is shown, with 'VYTVORIT ŽÁDOST O CERTIFIKÁT' highlighted by a red box. Other tools include 'IMPORT CERTIFIKÁTU', 'IMPORT PÁRU KLÍČŮ', and 'UVOLNIT MÍSTO NA KARTĚ'. The '2. detail osobního certifikátu' section displays details for a certificate issued to 'Jan Testík' on 09.12.2024, including its type, issuer, validity period, and serial number. At the bottom, there are buttons for 'DETAIL', 'EXPORT', 'ODSTRANIT', 'OZNAČIT JAKO VÝCHOZÍ', and 'REGISTROVAT DO WINDOWS'.

7.2.1 Vytvořit žádost o certifikát

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

Obr. 34 - Volba typu žádosti pro generování páru klíčů pomocí online generátor

This screenshot is identical to the one above, showing the SECURESTORE interface. The 'VYTVORIT ŽÁDOST O CERTIFIKÁT' button in the tool list is highlighted with a red box, indicating the selection of the 'Create certificate request' tool.

Po zvolení typu žadatele a 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. 35 - Volba typu žadatele o certifikát

Získání žádosti o certifikát

Krok 1: Pro koho je certifikát určen? Vyberte jednu z možností:

fyzická osoba

zaměstnanec nebo OSVČ

právnícká osoba nebo úřad

Fyzická osoba – pokud zvolíte tuto možnost, bude váš certifikát obsahovat Vaše jméno a příjmení, volitelně je možné uvést také bydliště a e-mailovou adresu.

Zaměstnanec nebo OSVČ – tato volba je určena pro ty, kdo v certifikátu potřebují uvést mimo jména a příjmení také název svého zaměstnavatele (organizace) nebo živnosti. Můžete ji také využít, pokud jste jednatelem společnosti.

Firma nebo státní instituce – pokud potřebujete certifikát pro vaši firmu, státní instituci nebo jiný právní subjekt, zvolte tuto možnost. Certifikát bude obsahovat název subjektu a volitelně také jeho sídlo.

Obr. 36 - Volba typu žádosti o certifikát

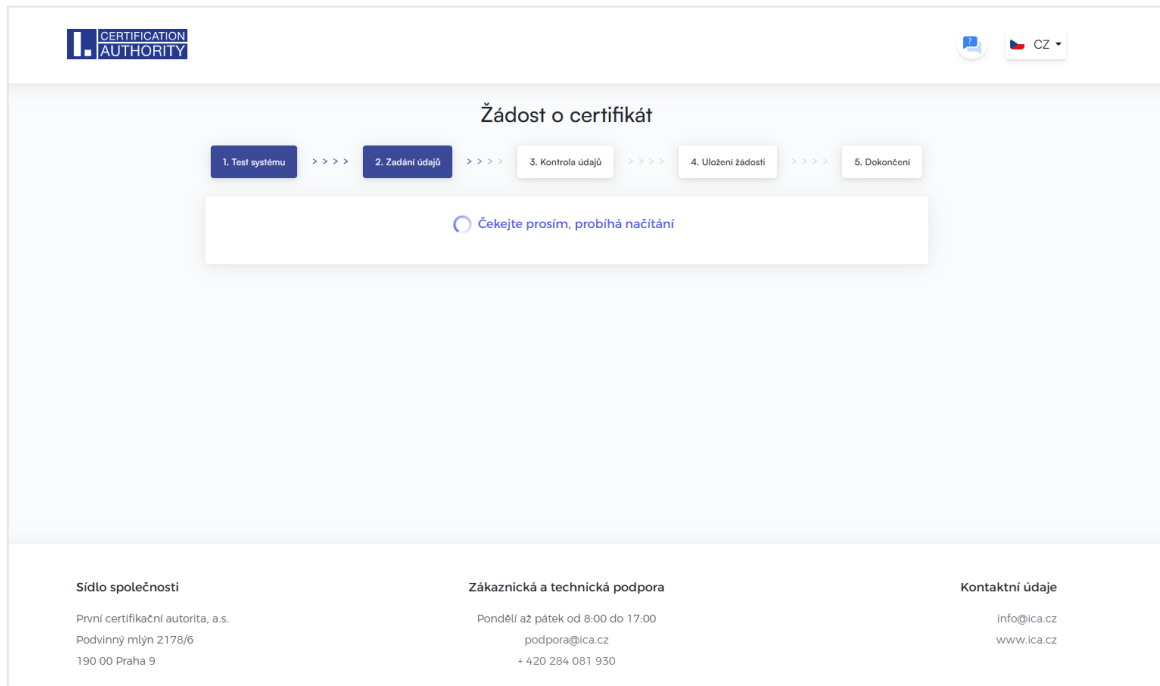
Získání certifikátu fyzická osoba

Krok 2: vyberte možnost, o kterou máte zájem ([zpátky ke kroku 1](#))

- Kvalifikovaný certifikát pro elektronický podpis**
používá se pro podepisování dokumentů. Využívá se tam, kde je vyžadován uznávaný elektronický podpis.
- Komerční certifikát**
slouží zejména pro autentizaci a šifrování. Pro elektronický podpis může být používán po dohodě komunikujících stran v případech, kdy není vyžadován uznávaný elektronický podpis.
- Komerční identitní certifikát**
slouží pro vytvoření kvalifikovaného prostředku na úrovni VYSOKÁ, je vždy uložen na čipové kartě Starcos 3.5 a vyšší
- TWINS**
zahrnuje kvalifikovaný certifikát pro elektronický podpis a komerční certifikát v jednom produktu umožňujícím komplexní využití.
- Identitní TWINS**
zahrnuje kvalifikovaný certifikát pro elektronický podpis a komerční certifikát pro elektronickou identifikaci v jednom produktu umožňující komplexní využití, je vždy uložen na čipové kartě Starcos 3.5 a vyšší.
- Kvalifikovaný certifikát pro elektronický podpis – Slovensko**
je určen pro komunikaci s orgány veřejné moci Slovenské republiky. Využívá se tam, kde je vyžadován kvalifikovaný elektronický podpis a musí být uložen na čipové kartě Starcos

Získat

Obr. 37 - 1. Test systému



Žádost o certifikát

1. Test systému >>>> 2. Zadání údajů >>>> 3. Kontrola údajů >>>> 4. Uložení žádosti >>>> 5. Dokončení

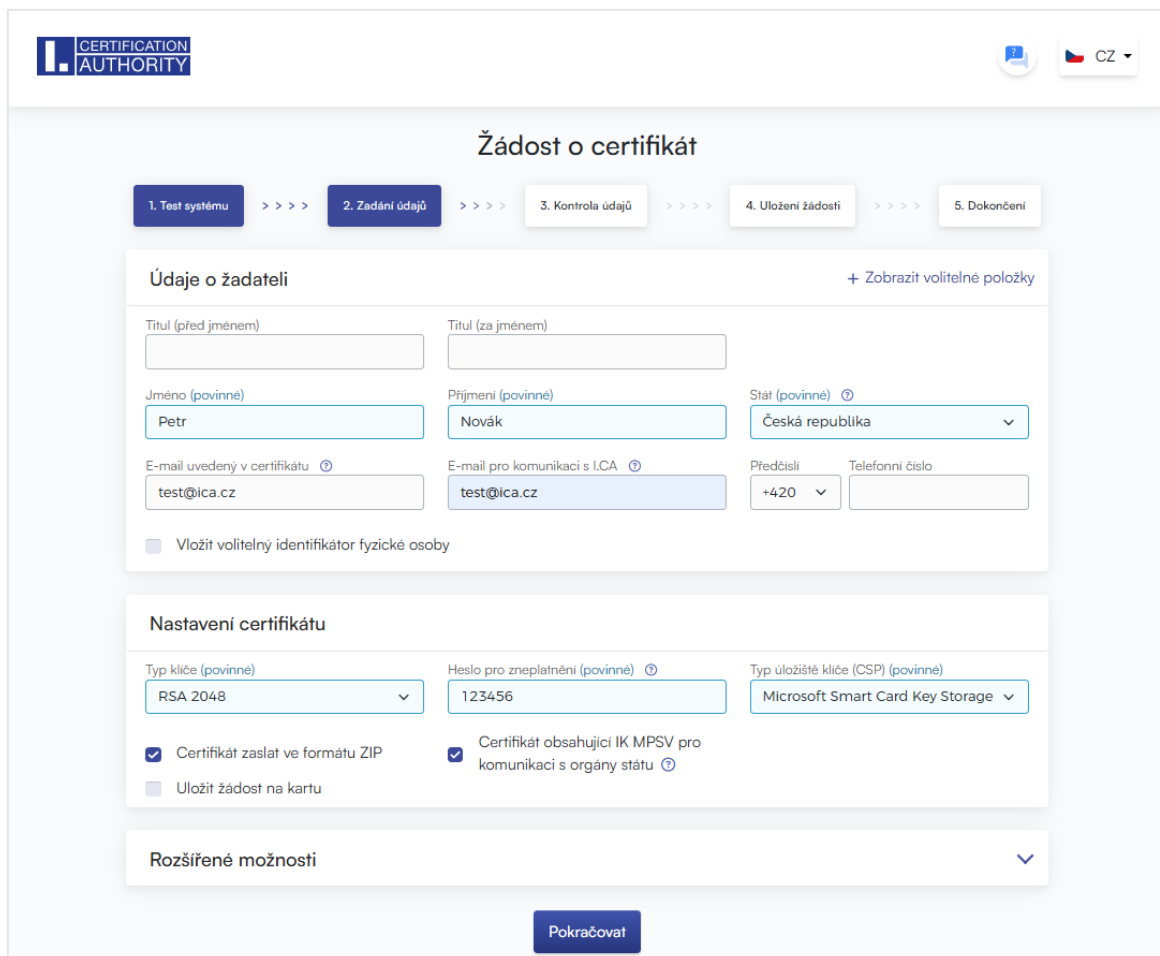
Čekejte prosím, probíhá načítání

Sídlo společnosti
První certifikační autorita, a.s.
Podvinný mlýn 2178/6
190 00 Praha 9

Zákaznická a technická podpora
Pondělí až pátek od 8:00 do 17:00
podpora@ica.cz
+ 420 284 081 930

Kontaktní údaje
info@ica.cz
www.ica.cz

Obr. 38 - 2. Zadání údajů



Žádost o certifikát

1. Test systému >>>> 2. Zadání údajů >>>> 3. Kontrola údajů >>>> 4. Uložení žádosti >>>> 5. Dokončení

Údaje o žadateli + Zobrazit volitelné položky

Titul (před jménem) Titul (za jménem)

Jméno (povinné) Příjmení (povinné) Stát (povinné)

E-mail uvedený v certifikátu E-mail pro komunikaci s I.CA Předčísli Telefonní číslo

Vložit volitelný identifikátor fyzické osoby

Nastavení certifikátu

Typ klíče (povinné) Heslo pro zneplatnění (povinné) Typ úložiště klíče (CSP) (povinné)

Certifikát zaslat ve formátu ZIP Certifikát obsahující IK MPSV pro komunikaci s orgány státu

Uložit žádost na kartu

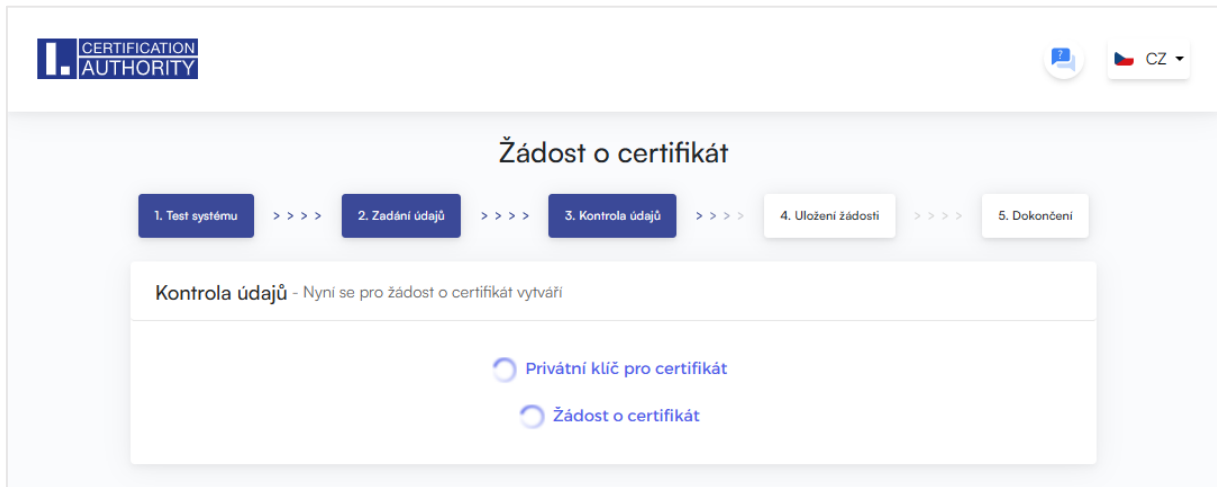
Rozšířené možnosti ▾

Pokračovat

Obr. 39 - 3. Kontrola údajů

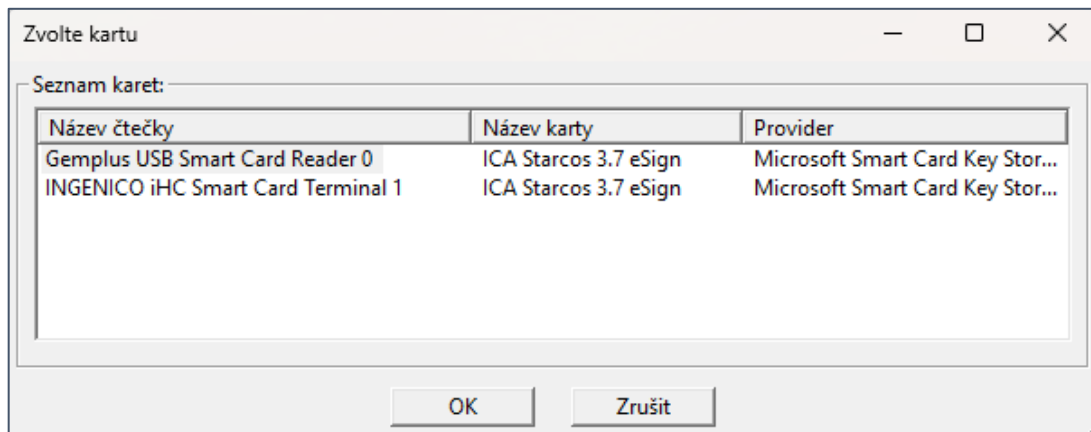
The screenshot shows a web interface for a certificate request. At the top, there is a navigation bar with the 'CERTIFICATION AUTHORITY' logo on the left and a language selector set to 'CZ' on the right. Below the navigation bar, the main heading is 'Žádost o certifikát'. A progress indicator shows five steps: 1. Test systému, 2. Zadání údajů, 3. Kontrola údajů (highlighted), 4. Uložení žádosti, and 5. Dokončení. The main content area is titled 'Kontrola údajů - Zkontrolujte údaje'. On the left, there is a sidebar with three menu items: 'OSOBNÍ ÚDAJE' (selected), 'VLASTNOSTI CERTIFIKÁTU', and 'OSTATNÍ NASTAVENÍ'. The main content area displays the following information under the heading 'Osobní údaje':
Celé jméno: Petr Novák
Jméno: Petr
Příjmení: Novák
E-mail uvedený v certifikátu: test@ica.cz
Stát: CZ
At the bottom right of the form, there is a blue button labeled 'Pokračovat'.

Obr. 40 – Generování soukromého klíče

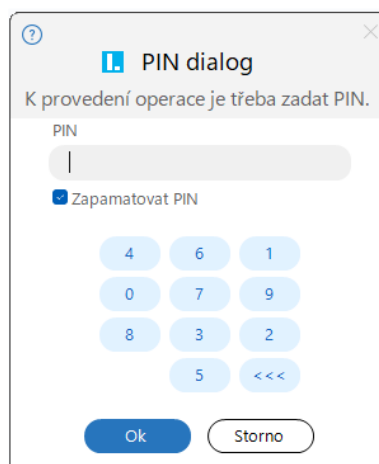


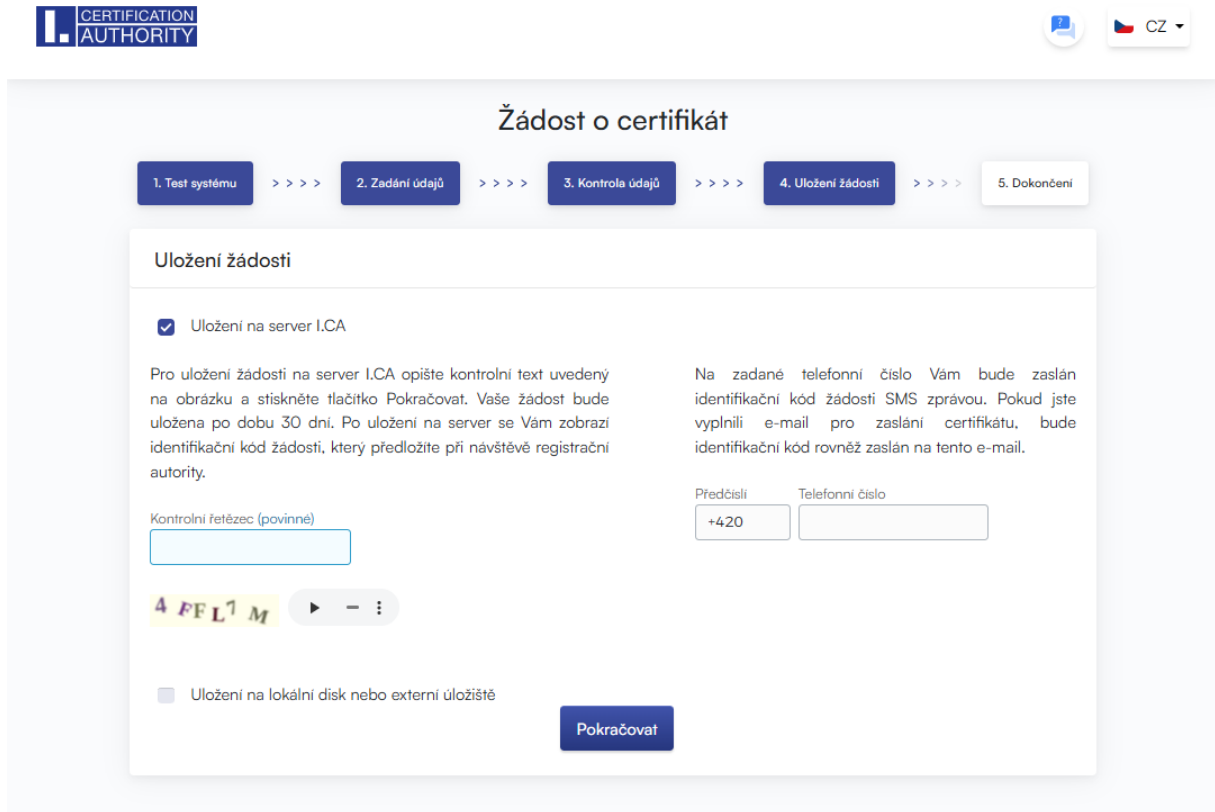
Pokud má uživatel k PC připojeno více čipových karet v dialogovém okně zvolí, na kterou má být klíčový pár generován. Po výběru čipové karty systém vyzve uživatele k zadání PIN.

Obr. 41 – Výběr čtečky čipových karet



Obr. 42 - Zadání PIN pro vytvoření klíčového páru a podpis žádosti



Obr. 43 - 4. Uložení žádosti


The screenshot shows a web interface for 'Žádost o certifikát' (Certificate Request). At the top, there is a progress bar with five steps: 1. Test systému, 2. Zadání údajů, 3. Kontrola údajů, 4. Uložení žádosti (current step), and 5. Dokončení. The main content area is titled 'Uložení žádosti' and contains the following elements:

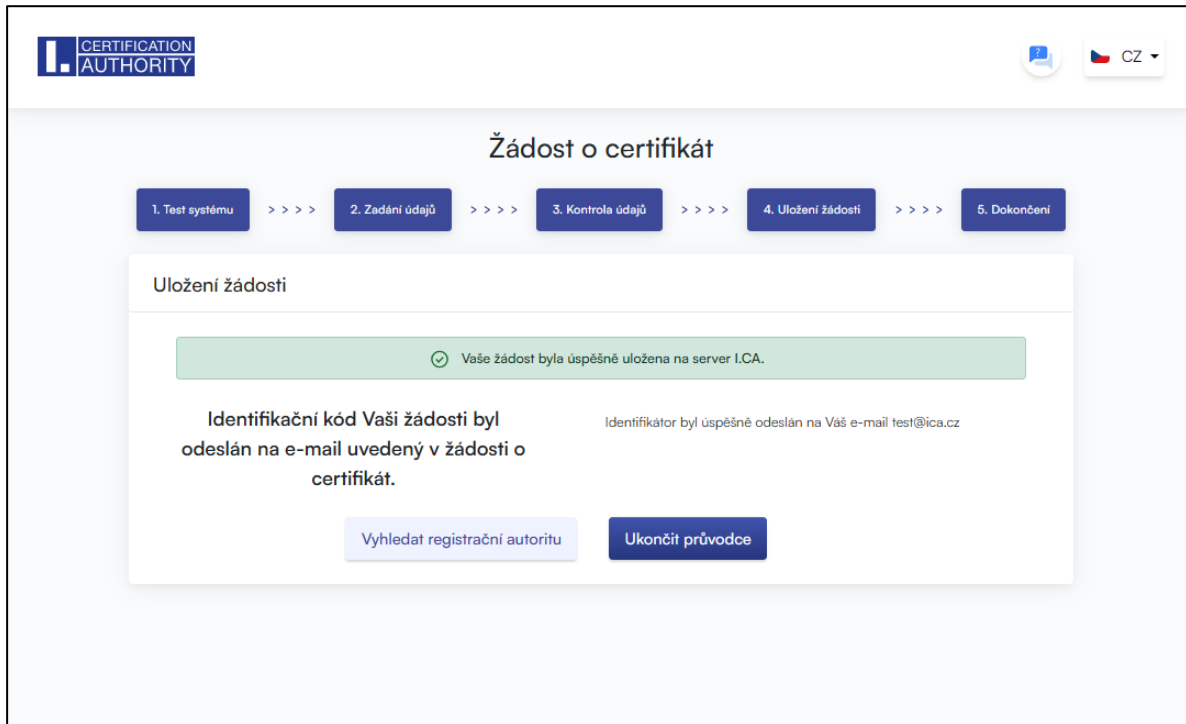
- A checked checkbox labeled 'Uložení na server I.CA'.
- Text explaining that upon submission to the I.CA server, a control text will be shown on the screen, and the user should click 'Pokračovat'. The request will be stored for 30 days, and a six-digit identification code will be displayed. This code is used to present the registration authority upon visit.
- Text explaining that upon submission to the I.CA server, a six-digit identification code will be sent via SMS to the provided phone number. If an email was provided, the code will also be sent via email.
- Form fields for 'Předčísli' (Country code) with '+420' and 'Telefonní číslo' (Phone number).
- A 'Kontrolní řetězec (povinné)' (Control string) field with a text input box.
- A visual representation of the control string: '4 PFL1 M' with a play button and a menu icon.
- An unchecked checkbox labeled 'Uložení na lokální disk nebo externí úložiště'.
- A blue 'Pokračovat' (Continue) button.

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 žádostí s názvem cert****.req. 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**“.

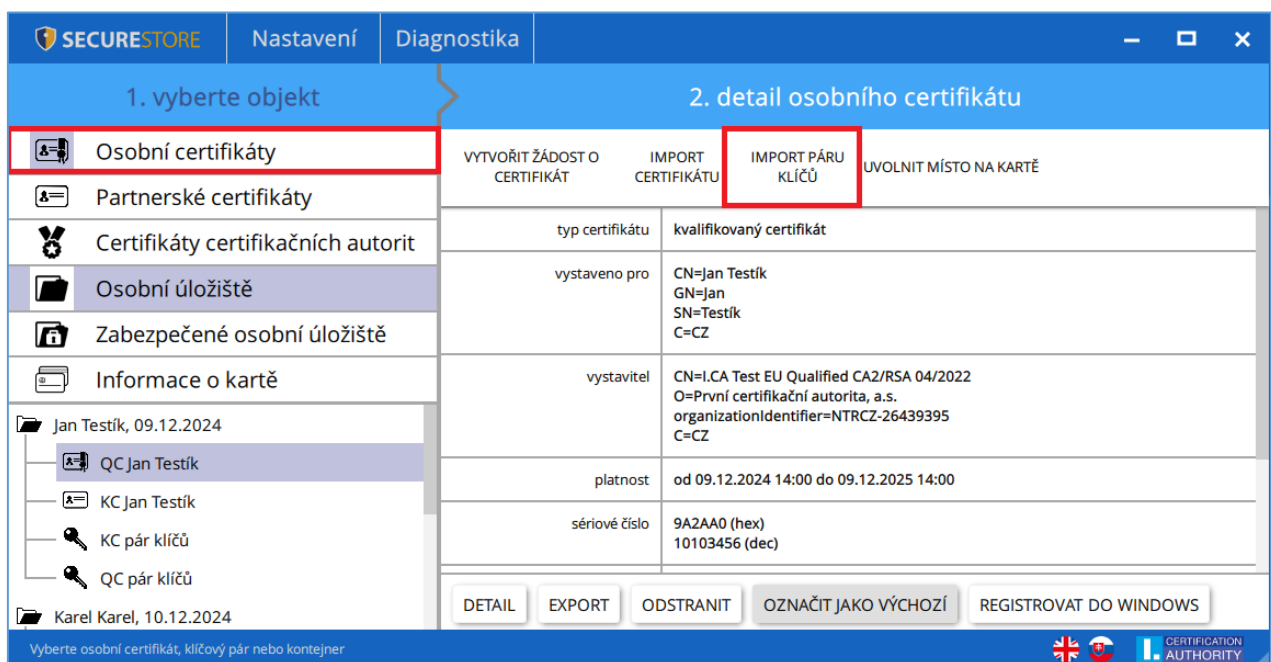
Obr. 44 - 5. Dokončení



7.2.3 Import páru klíčů ze zálohy a import klíčů

Volba importuje na čipovou kartu klíče, které byly během procesu generování žádosti o šifrovací certifikát uloženy na disk. Funkci uživatel nalezne v objektu „Osobní certifikáty“. Stejným způsobem lze importovat na čipovou kartu klíče s certifikátem, které jsou uloženy ve formátu PKCS#12 na disku.

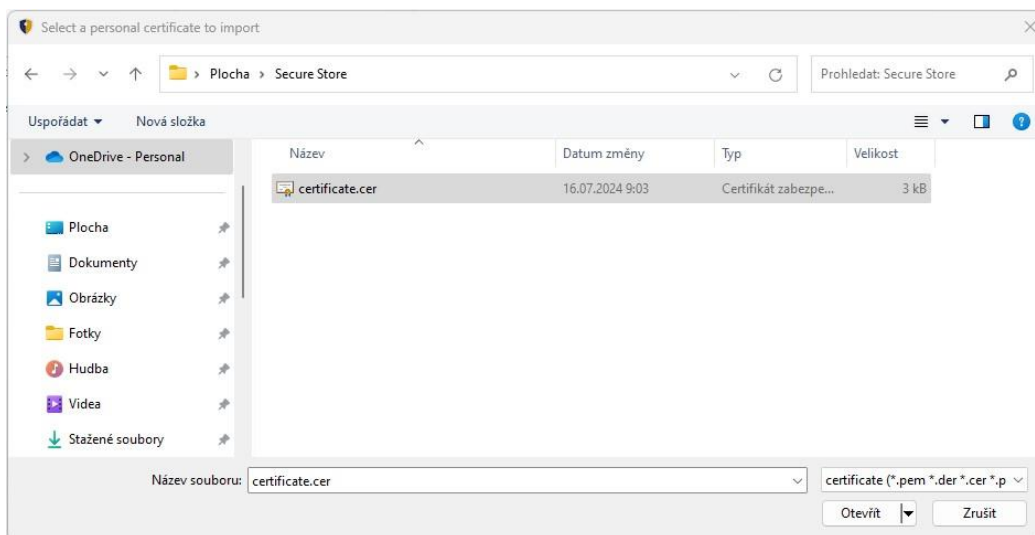
Obr. 47 – Import páru klíčů ze zálohy a páru klíčů



Importovaný certifikát je uložen v úložišti na čipové kartě, které obsahuje klíče k certifikátu.

Pokud na čipové kartě není úložiště obsahující příslušné klíče, certifikát se uloží do části karty označené „Partnerské certifikáty“.

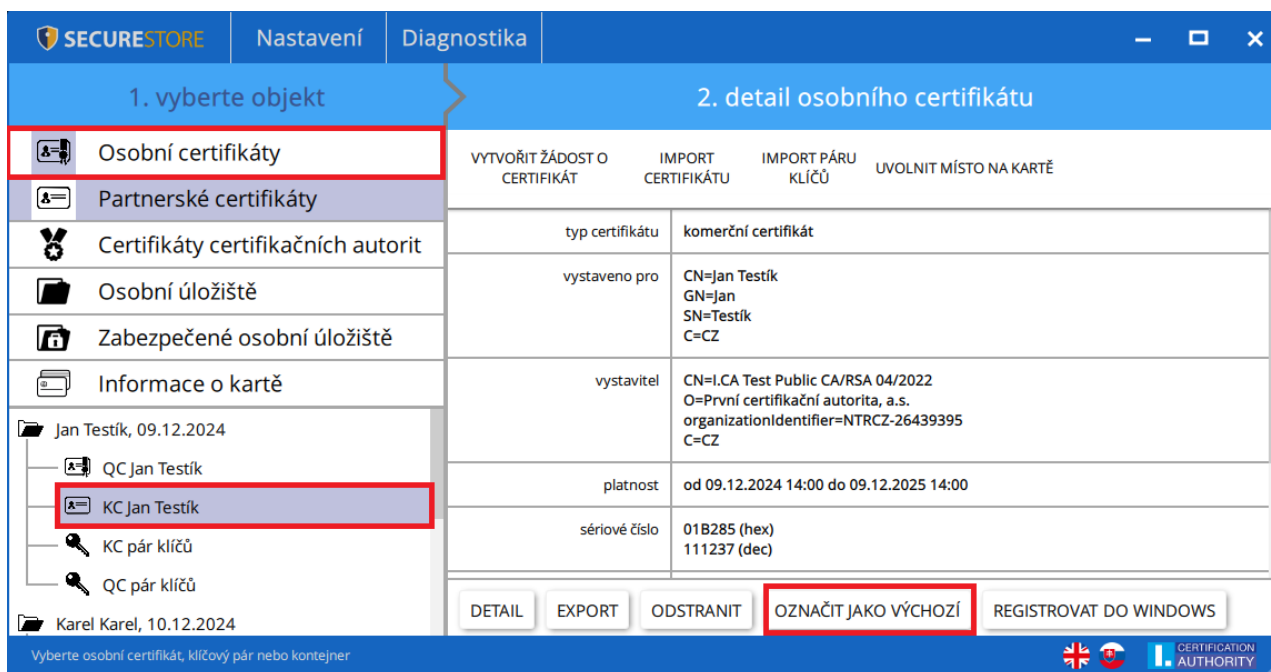
Výběr souboru certifikátu, který má být importován na kartu



7.2.4 Import páru klíčů ze zálohy a import klíčů

Volba umožňuje označit vybraný certifikát jako výchozí pro přihlášení do Windows. Vybraný certifikát a bude použit při přihlašování do Windows.

Funkci uživatel nalezne v objektu „Osobní certifikáty“, kde zvolí certifikát určený k této funkci a tlačítkem „Označit jako výchozí“ potvrdí. Obr. 48 - Označit certifikát jako výchozí pro přihlášení do Windows



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 využívána 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 dodávána ke každé kartě.
- **Úložiště** - 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.
- **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.
- **Komerční certifikát** - vydáván fyzickým nebo právnickým osobám, vhodný pro běžné využití. Je poskytován ve dvou variantách **Standard** (privátní klíč uložen v MS Windows) a **Comfort** (privátní klíč uložen v čipové kartě).
- **Kvalifikovaný certifikát** - striktně řízen nařízením EU č. 910/2014 a slouží výhradně pro oblast elektronického podpisu. Vytváření, správa a použití kvalifikovaného certifikátu se řídí příslušnými certifikačními politikami. Je poskytován 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 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** - musí obsahovat specifické údaje. Pro přihlášení do Windows není proto možné 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 I.CA (komerčních)** - 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.

- 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.