



I.CA SecureStore

User Manual

Version 4.1 and higher

První certifikační autorita, a.s.

Version 4.18

Contents

1. Introduction.....	3
2. Card Access Data	3
2.1. Initialising the Card.....	3
3. Basic Screen.....	4
3.1. Switching between Application Languages.....	5
4. Displaying Key Pair Information	10
5. Certificates.....	13
5.1. Displaying a Certificate.....	13
5.2. Using Personal Certificate	13
5.3. Using CA Root Certificate	15
5.4. Registering Personal Certificate in Windows	17
6. Personal Storage.....	18
7. Navigating the Application	20
7.1. Card Information Tool Bar.....	20
7.2. Personal Certificates Tool Bar	21
7.2.1. Generating Certificate Application.....	22
7.2.2. Importing Personal Certificate	27
7.2.3. Importing Backup Key Pair (PKCS#8).....	28
7.2.4. Importing Key Pair (PKCS#12).....	29
7.2.5. Setting Certificate as Default Windows Login Certificate	29
8. Glossary	30

1. Introduction

This User Manual applies to the application I.CA SecureStore, Version 4.1. and higher. The specified versions have the same function and identical user interface.

2. Card Access Data

STARCOS 3.0

Chip card access is PIN-protected as is with payment cards, for example.

PIN is a number of 4–8 digits. PIN will be automatically disabled if a wrong PIN is entered three times in a row.

The user needs PUK to have his PIN re-enabled.

PUK is a number of 4–8 digits. Entering a wrong PUK 5 times in a row will disable the PUK and thus also the chip card.

STARCOS 3.5

Chip card access is PIN-protected as is with payment cards, for example.

PIN is a number of 6–8 digits. PIN will be automatically disabled if a wrong PIN is entered three times in a row.

PUK is a number of 6–8 digits. Entering a wrong PUK 5 times in a row will disable the PUK and thus also the chip card.

Re-enabling PIN using PUK is limited to 6 attempts.

The card's segment named ***Secure Personal Storage*** is designed for storing any kind of data. This segment is protected with a special PIN, a secure storage PIN. Use the PUK referred to in the previous paragraph to re-enable the secure storage PIN.

The secure storage PIN is a number of 4–8 digits.

2.1. Initialising the Card

Initialising the card means setting a PIN and a PUK.

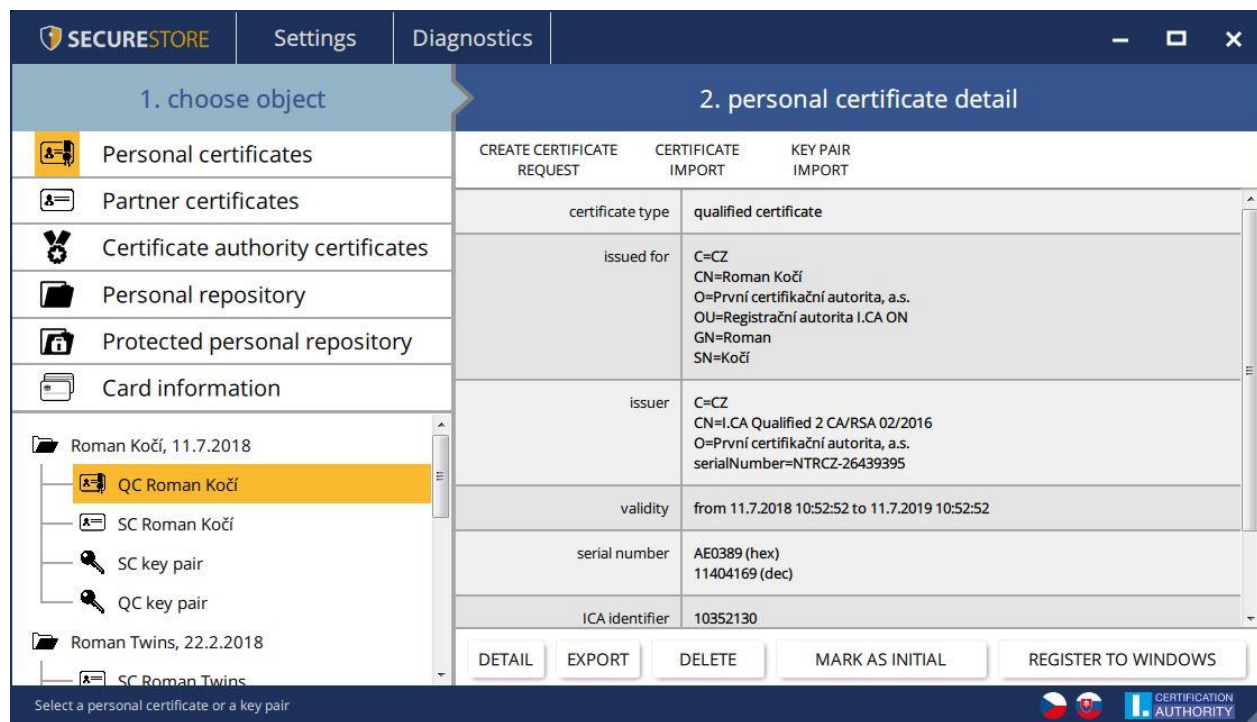
If the user has received the PIN envelope, the card has been initialised already and the PIN and the PUK are enclosed in the envelope.

If the PIN envelope has not been received, setting PIN and PUK is required in the first use of the card.

The card initialising dialogue is displayed automatically, usually in launching the application with a new chip card for the first time. Please make sure you remember your PIN and PUK.

3. Basic Screen

Fig. 1– Basic Screen



The basic screen has two segments.

The left segment shows the list of the objects saved on the chip card.

The right segment shows the details of the objects saved on the chip card.

The upper bar shows the following options, see Fig. 2.

3.1. Switching between Application Languages

Click the pertinent flag in the right bottom corner to switch to a different language.

Fig. 2 – Main Bar



Version of the I.CA SecureStore Application


Click  to display the application's version.

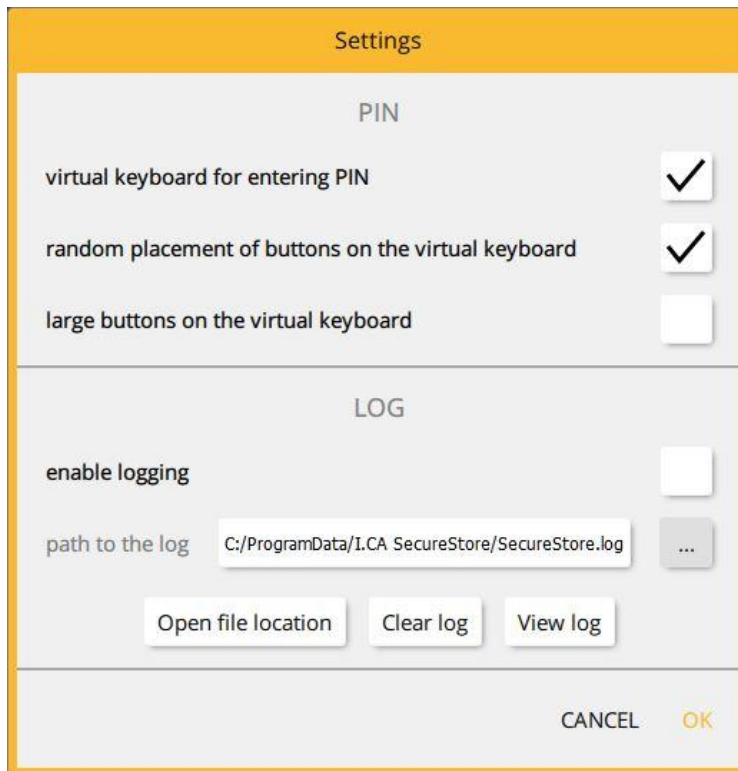
Fig. 3 – Application Version



Use the **Settings** option to:

- 1) Adjust the keypad for entering PIN

Fig. 4 – PIN Keypad



The default setting is **Random Virtual Keyboard**. This means PIN must be entered on the keyboard using the mouse cursor. If none of the PIN input options are selected, the user enters the PIN on the numeric keyboard.

Fig. 5 – Virtual PIN Keyboard

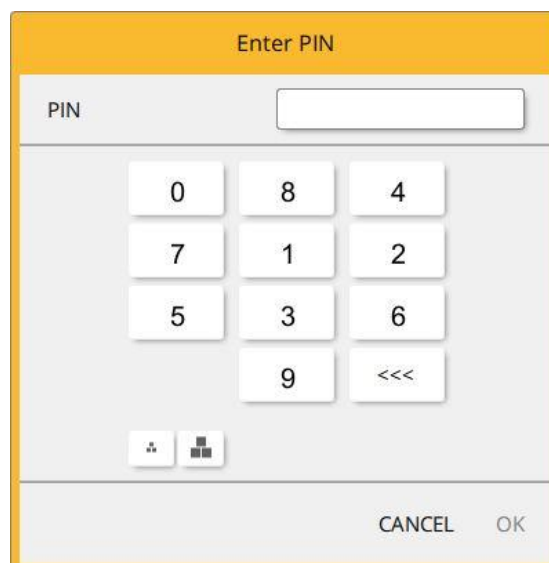
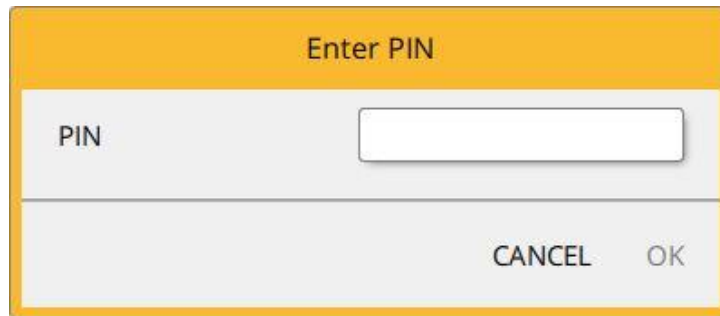


Fig. 6 - Numeric PIN Keyboard



- 2) Logging enabled – Enabling application logging in case of having to analyse a technical issue in using the chip card and the application.


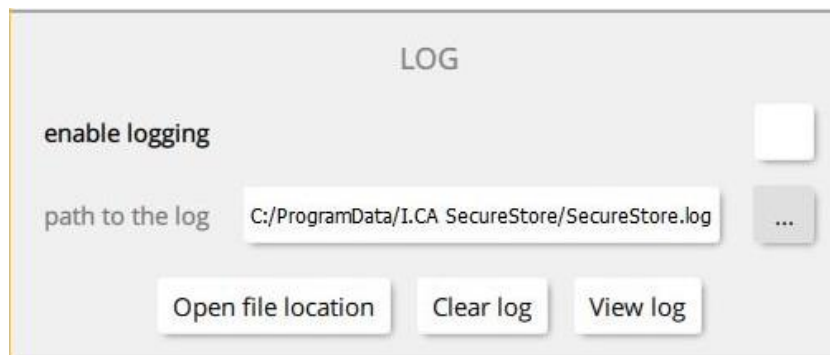
Use  to change the path where the log is saved.

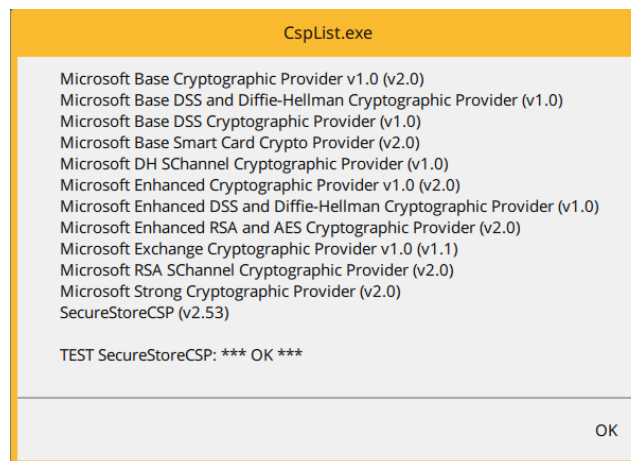
Fig. 7 – Log



Diagnostic Tools

I.CA SecureStore includes diagnostic tools to check the status of the CSP providers (cryptographic service providers) registered in MS Windows.

Fig. 8 – Diagnostic Tools



If multiple chip card readers connect to a PC, the *Select Chip Card Reader* dialogue will also display after the application has been launched.

Selecting Chip Card Reader

Fig. 9 – Selecting Chip Card Reader

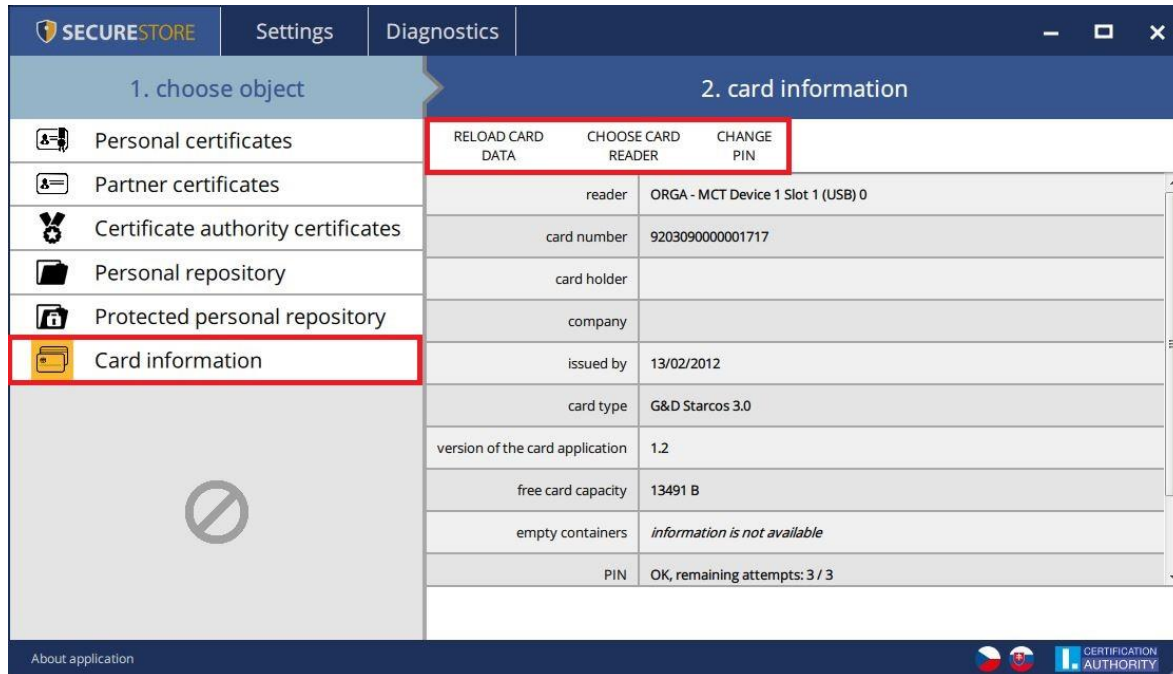


If just a single chip card reader connects to a PC, this dialogue is not displayed.

The options in the tool bar (see Fig. 10) change according to the object selected in the left screen segment.

Tool Bar

Fig. 10 – Tool Bar



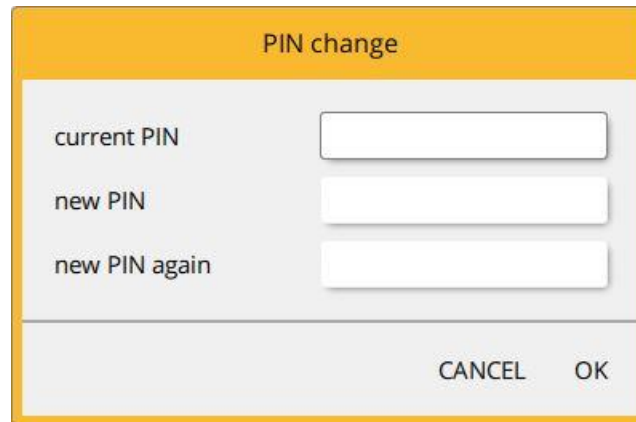
The tool bar example shows the options valid for the **Card Information** object.

Choose **Reload Card Data** to reload data from the chip card. F5 has the same function.

Choose **Change PIN** to change PIN to your card. The change PIN dialogue will ask you to enter your current PIN once and the new PIN twice.

Changing PIN

Fig. 11 – Changing PIN



PIN change

current PIN

new PIN

new PIN again

CANCEL OK

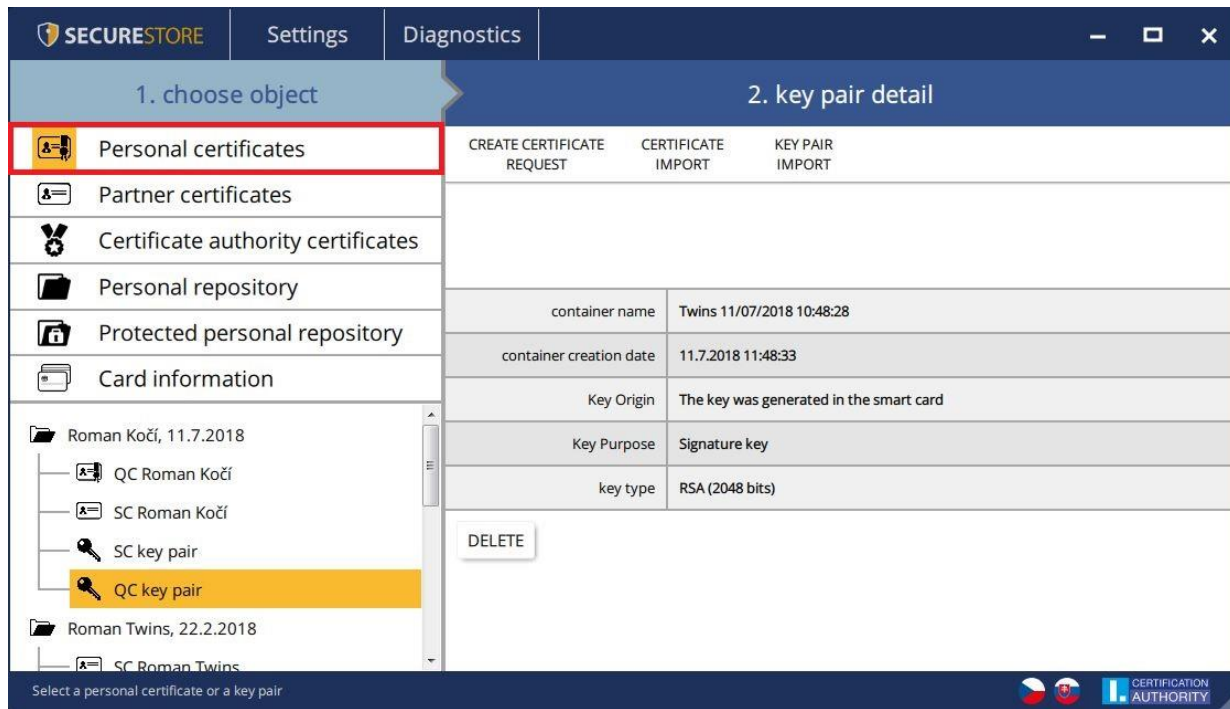
The ***Re-enable PIN*** option allows you to set a new PIN if you have caused your current PIN to be disabled. You need your PUK to re-enable your PIN.

NOTE: Re-enabling PIN using PUK is limited to 5 attempts.

4. Displaying Key Pair Information

Go to the ***Personal Certificates*** object to display the information about your key pair.

Fig. 12 – Displaying Key Pair Information



The storage stores one key pair for the certificate and two key pairs for Twins certificates.

The public/private key generation time is the exact time the key has been generated on the card or imported in the card.

Go to **Key's Origin** to display how the key was generated.

Go to **Key's Purpose** to display whether the key is an encrypting or a signature one.

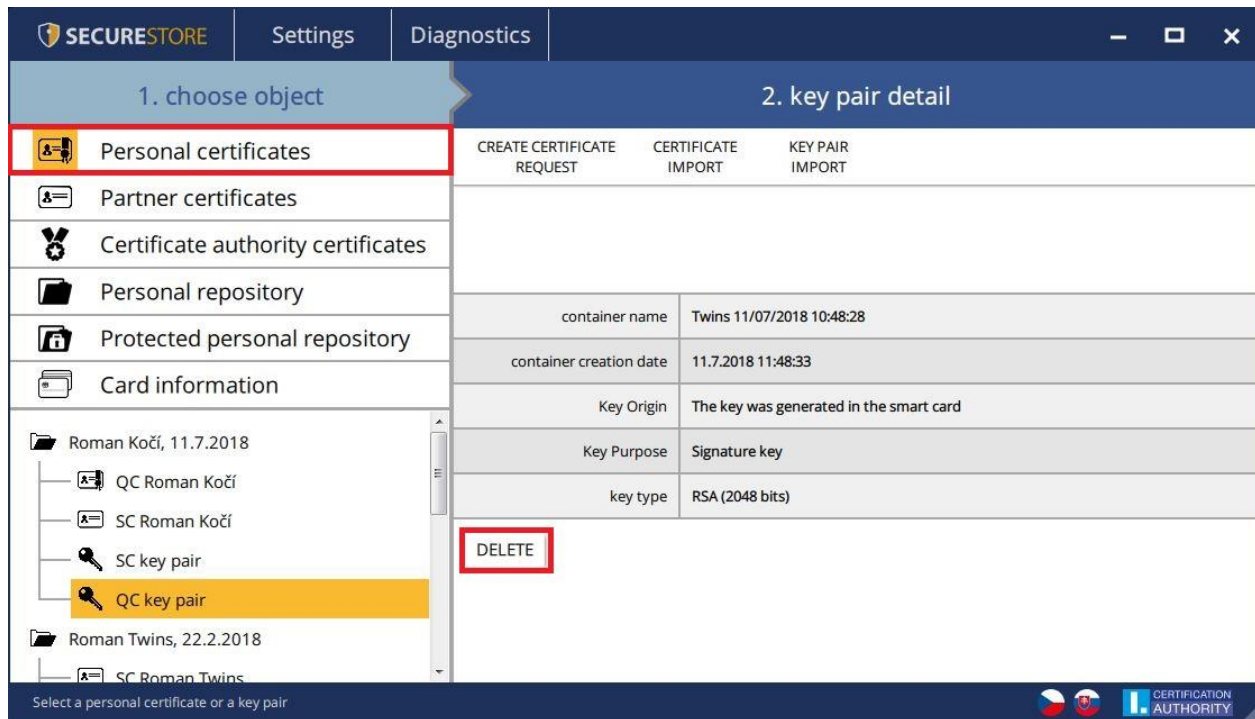
Key Type is self-explanatory; the example's key type is a 2048-bit RSA algorithm key.

Use **Delete** to remove a key pair from the card.

4.1 Removing a Key Pair

Fig. 13 – Removing a Key Pair

Go to **Personal Certificates** for user selection, select a key pair and press **Delete** to remove the key pair.



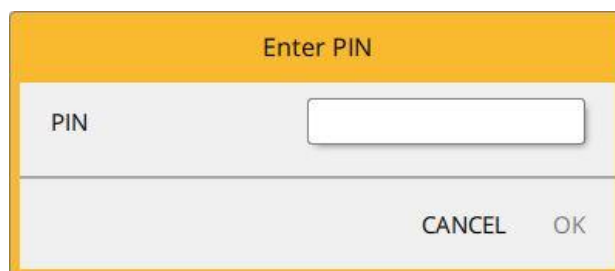
Removing a user’s private personal certificate key is an **irreversible** transaction and the certificate can no longer be used for signing/decrypting.

Fig. 14 – Private Key



Click **Delete** to be prompted to enter your PIN, and then the selected key will be removed.

Fig. 15 – Entering PIN to Remove Key Pair

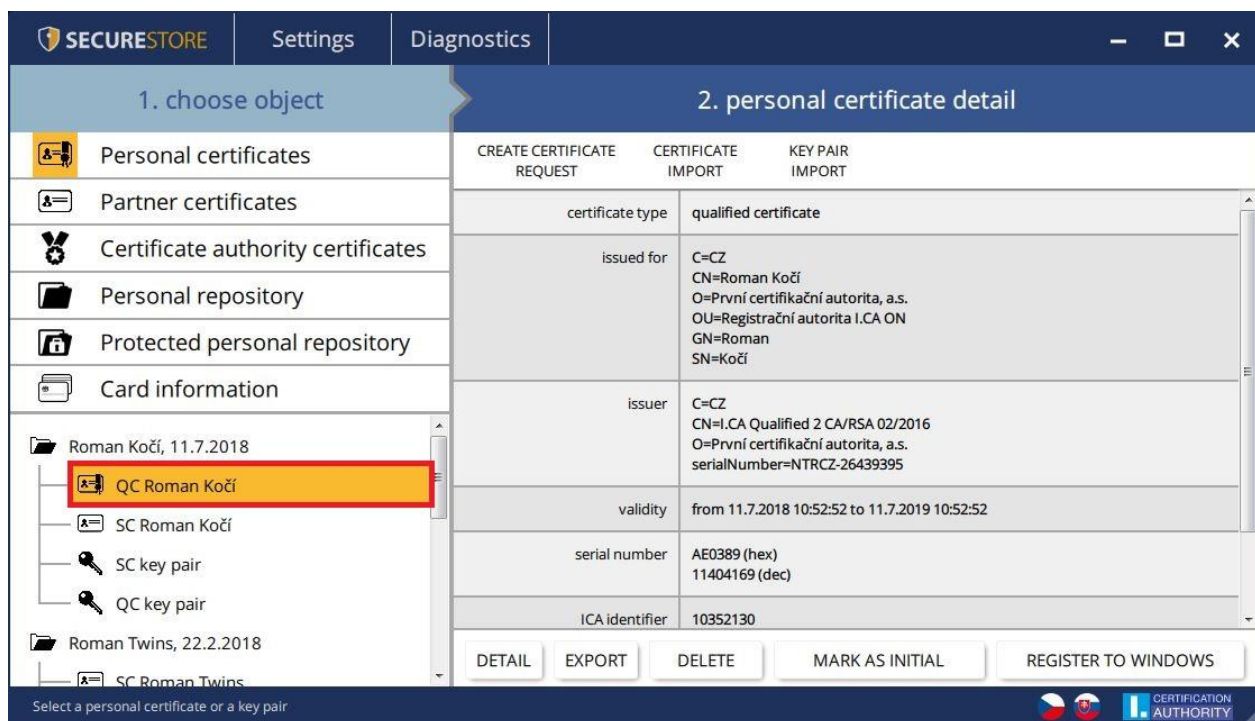


5. Certificates

5.1. Displaying a Certificate

Go to **Personal Certificates** to display the user's certificates, and select the certificate to be displayed. The certificate's details will display in **Personal Certificate Details** in the right screen.

Fig. 16 – Displaying a Certificate

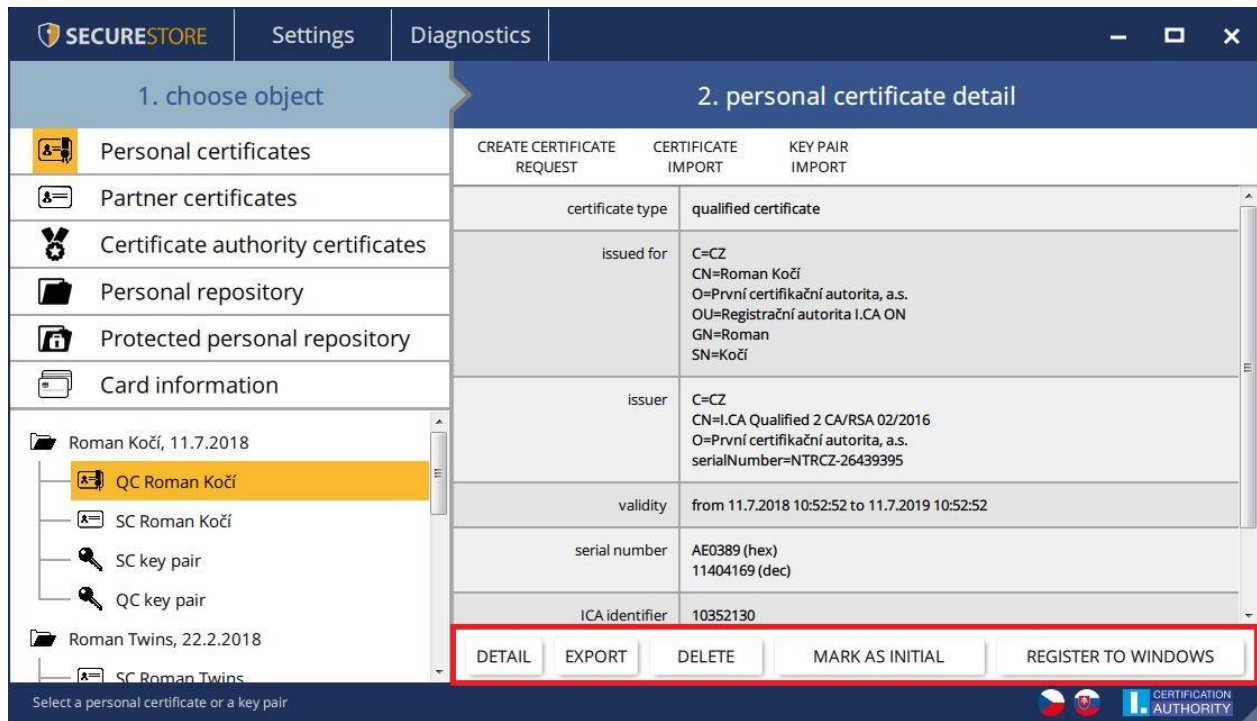


5.2. Using Personal Certificate

Go to the tools bar at the bottom of the application to access the options for the transactions available for the certificate saved on the card.

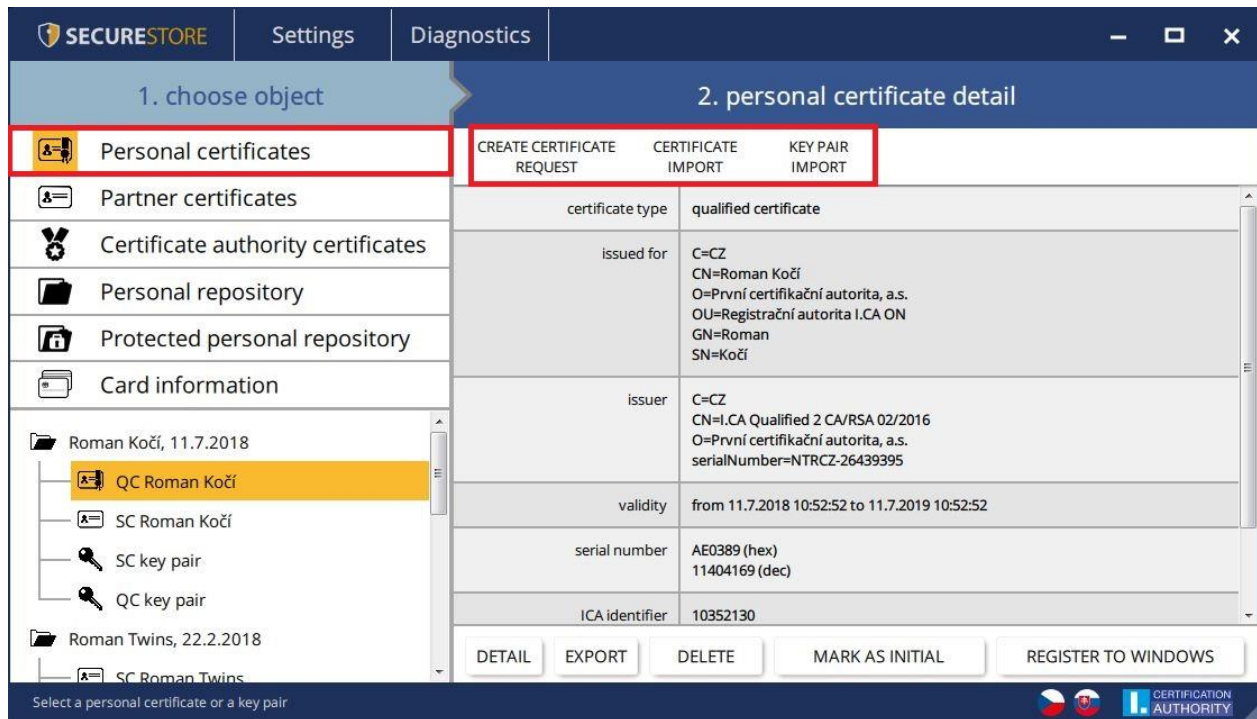
Go to **Personal Certificates** and use the tool bar to select the required certificate.

Fig. 17 – Tool Bar Options for Working with Personal Certificate



Go to **Personal Certificates** to access the options for importing a certificate to the chip card.

Fig. 18 – Certificate Import Options



The personal certificate is imported in the storage where the corresponding key pair is saved. If no such an object exists on the card, the certificate will be imported in a separate folder without the private key.

Communication partners' certificates can be imported as partner certificates.

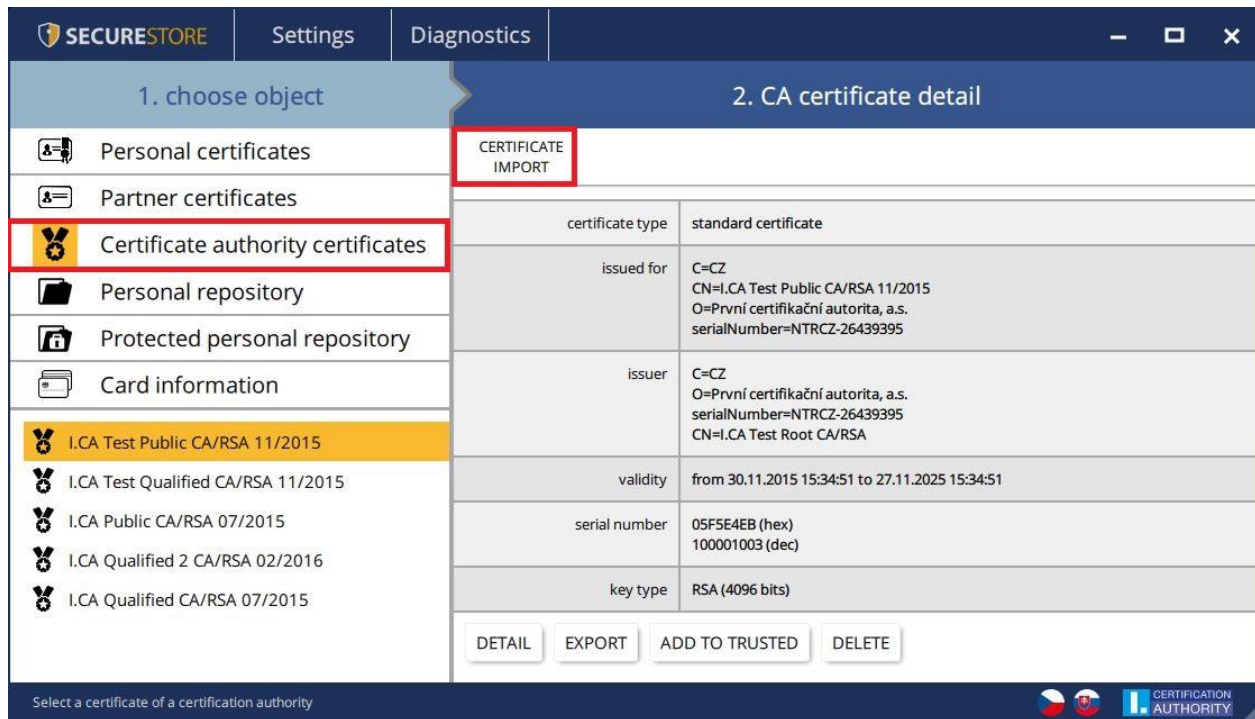
Displaying the certificate's bare data is an option for experts to make a visual check of the certificate's data.

5.3. Using CA Root Certificate

A new card contains the required certification authority root certificates, which are saved in **Certification Authority Certificates**.

A certificate can only be imported as a CA certificate if it is a certificate of a permitted CA for the given chip card. Certificates of other CAs and new CA certificates issued can be imported as .cmf files. The I.CA certificates as .cmf files can be downloaded from <https://www.ica.cz/Root-certificate>

Fig. 19 – Importing a Certification Authority Certificate

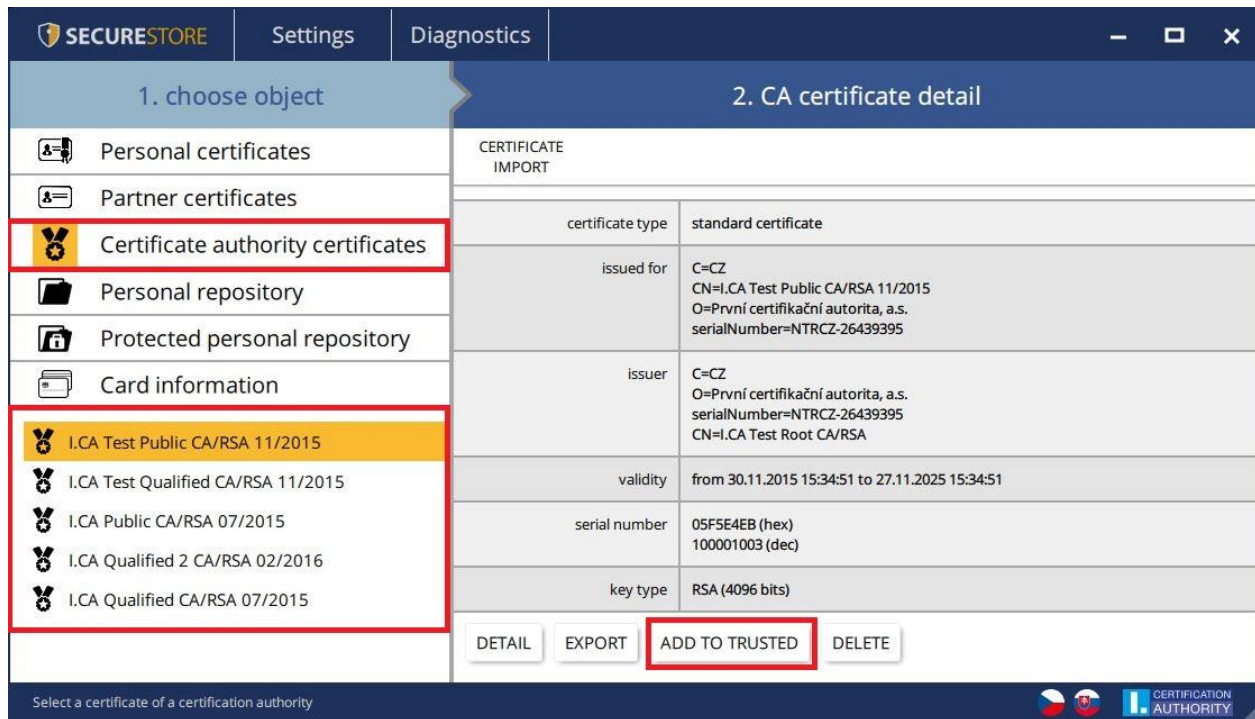


Root certificates are for verifying how trusted a personal certificate is. Working with certificates requires that root certificates are registered in Windows and Windows can thus verify whether the certificates applied in signing or encrypting are trusted ones.

If you use an older version of Windows which does not include the I.CA root certificates, please register the root certificate from your chip card by using **Add to Trusted** (see Fig. 12).

Registering a root certificate in Windows requires the user's consent, then the root certificate gets registered in MS Windows as a trusted root certificate.

Fig. 20 – Registering a Certification Authority Certificate in Windows



5.4. Registering Personal Certificate in Windows

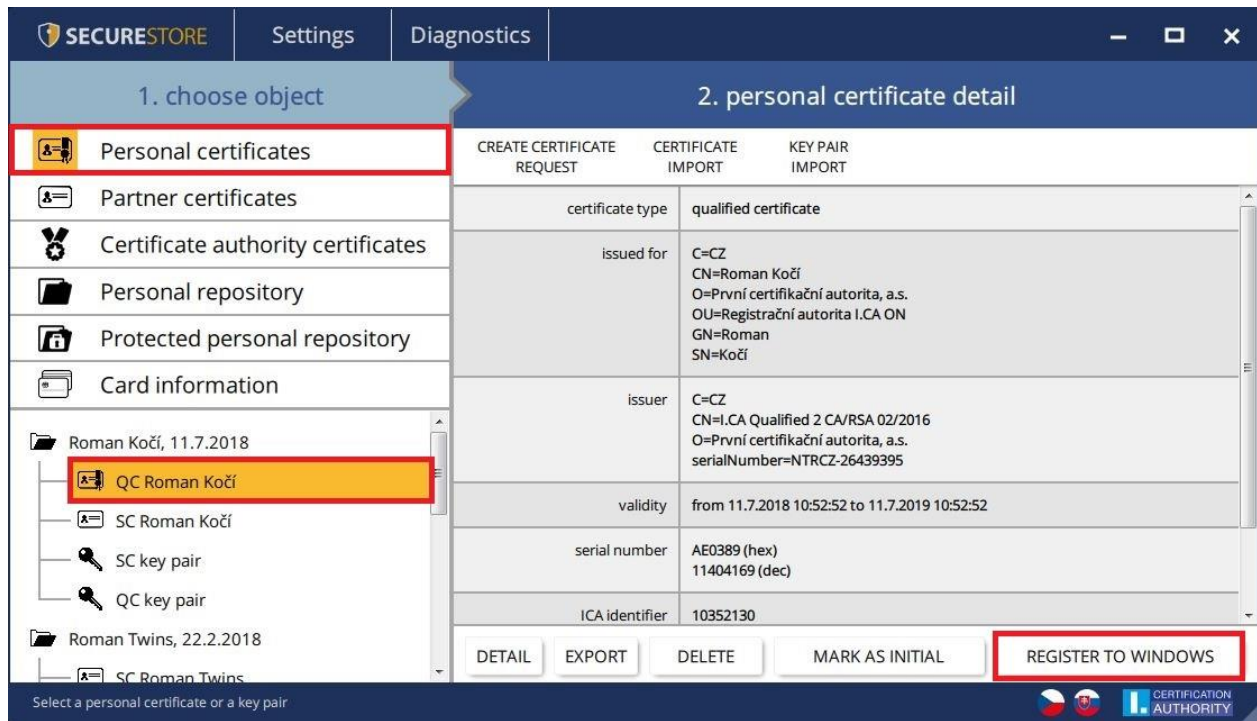
Most applications require that the personal certificate with which the user wants to work be registered in Windows.

Use **Register in Windows** to register each certificate separately.

This option will register the personal certificate from the chip card in the personal Windows storage.

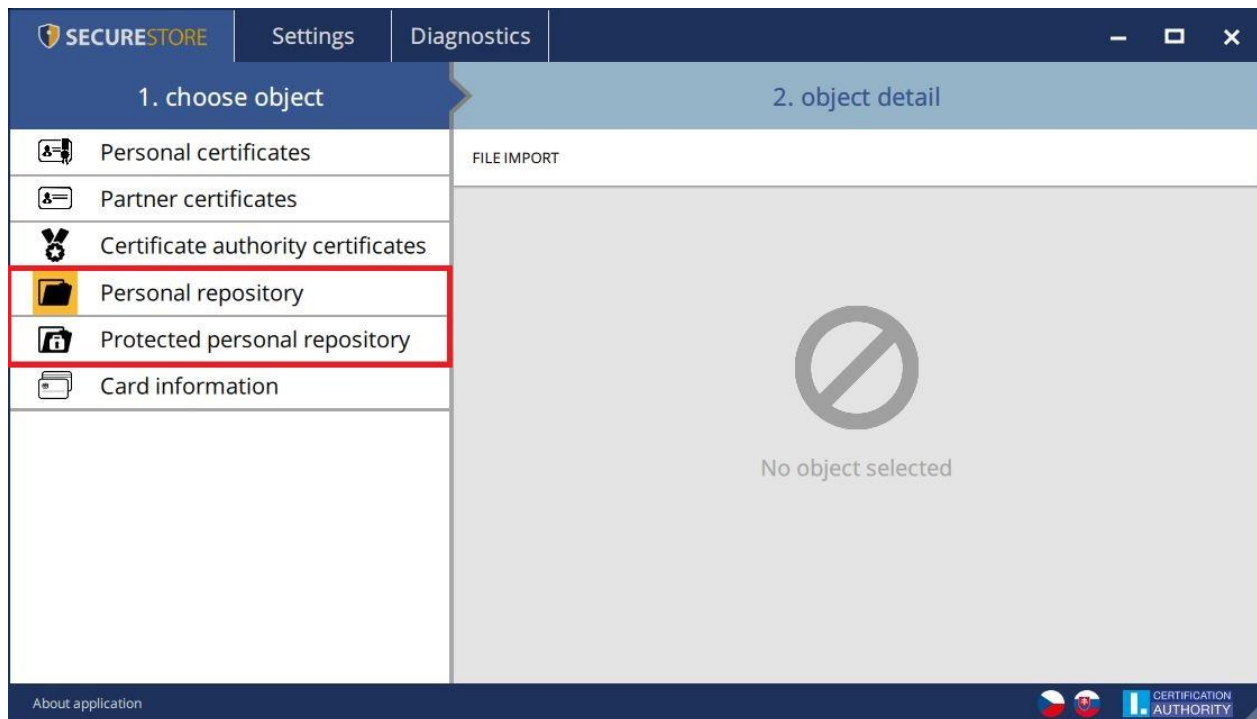
Go to **Personal Certificates** and select the certificate to be registered.

Fig. 21 – Registering Personal Certificate in Windows



6. Personal Storage

Fig. 22 – Personal Storage



Small files (of just several kB) can be saved in **Personal Storage** or **Secure Personal Storage** on the card. Text as well as binary files can be saved.

Reading and exporting secure storage files are protected with the secure storage PIN (see **Chapter 2**).

Fig. 23 – Importing Files in Personal Repository

Go to **Personal repository** and the detail of **Import Files**.



Fig. 24 – Importing Files in Secure Storage

Go to **Protected personal repository** and the detail of **File Import**.

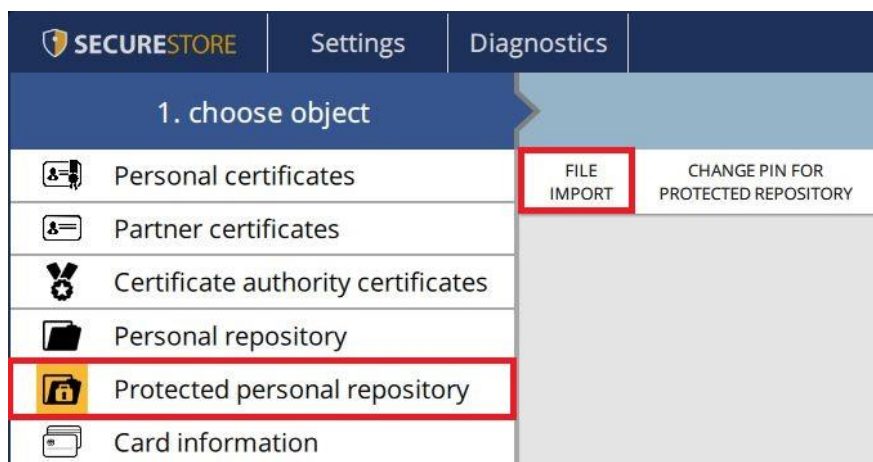
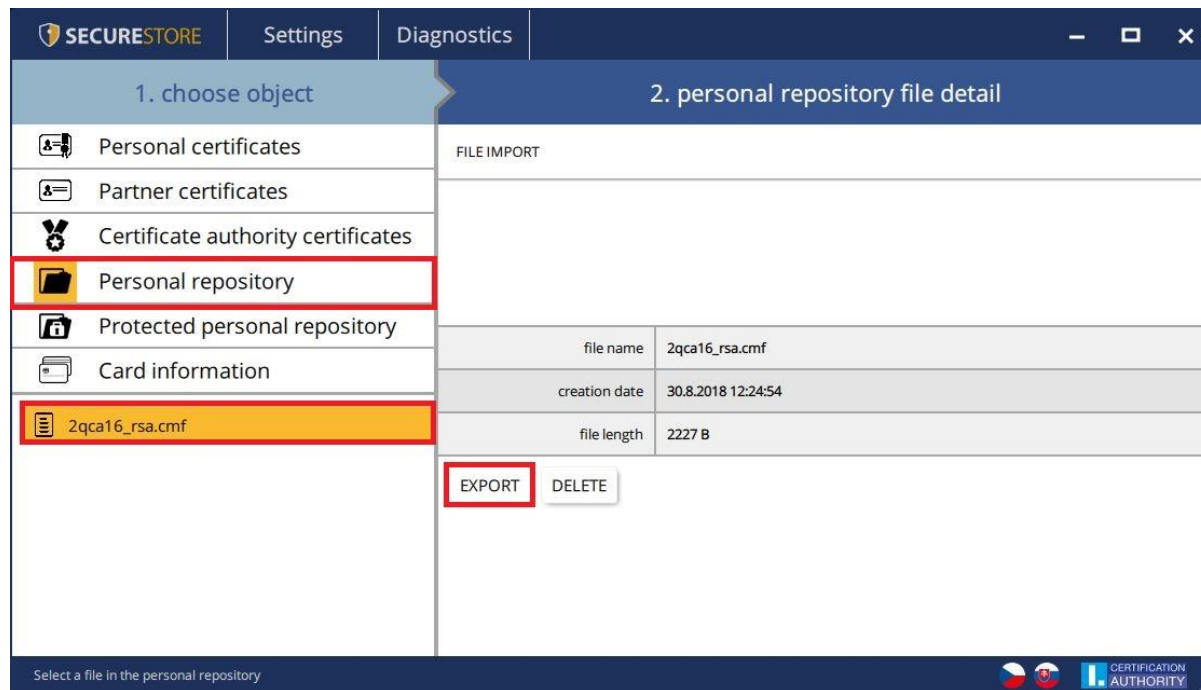


Fig. 25 – Exporting Files from Personal Repository

Go to **Personal Repository** > **Personal Repository File Details**, select the file(s) to be exported and click/press **Export**.



You need to enter the card's PIN to remove a file from the secure storage.

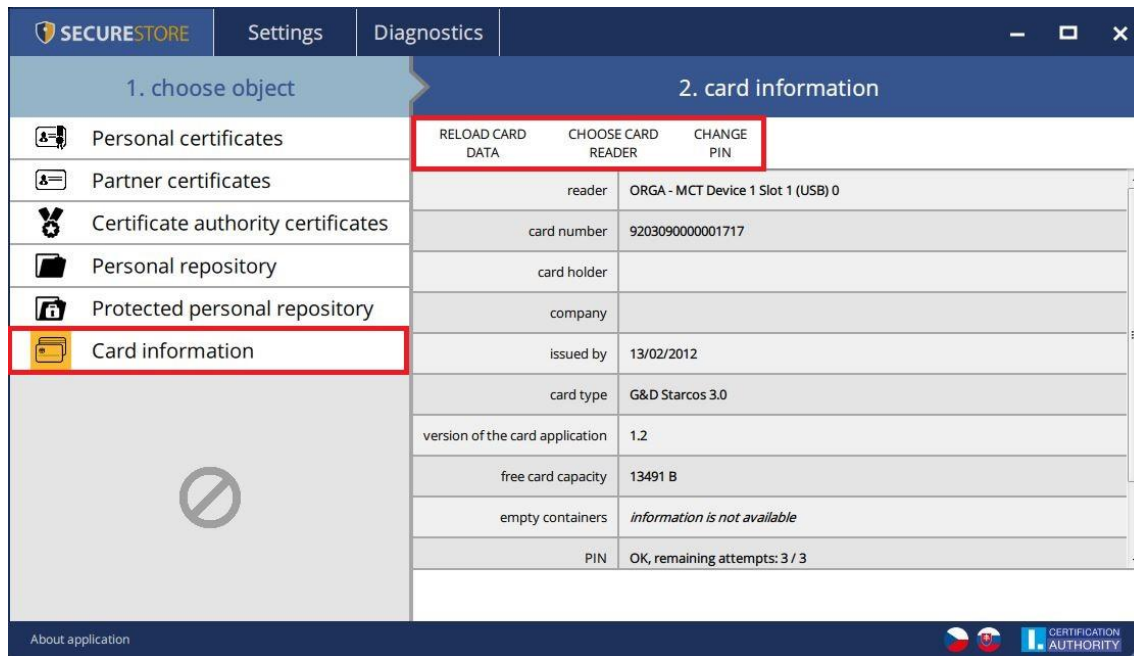
7. Navigating the Application

You access the application's functions using a tool bar. To access the tool bar, click the desired object in the left screen segment.

7.1. Card Information Tool Bar

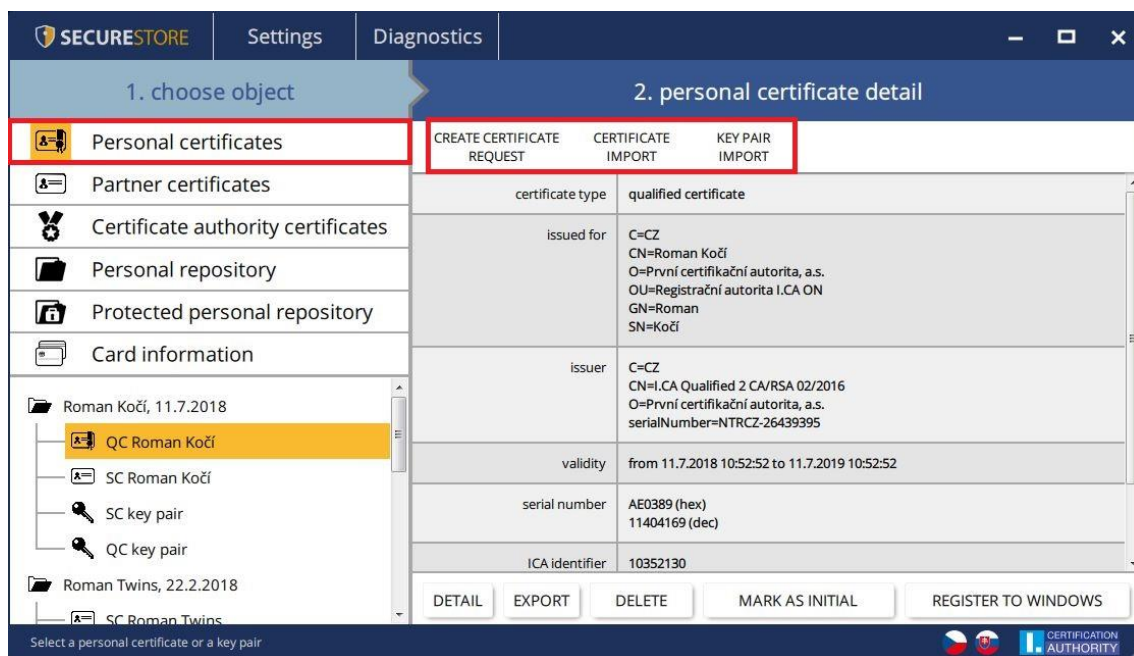
The **Card Information** tool bar provides the basic administration transactions pertinent to PIN and PUK administration and the reloading of the data from the card.

Fig. 26 – Card Information Tool Bar



7.2. Personal Certificates Tool Bar

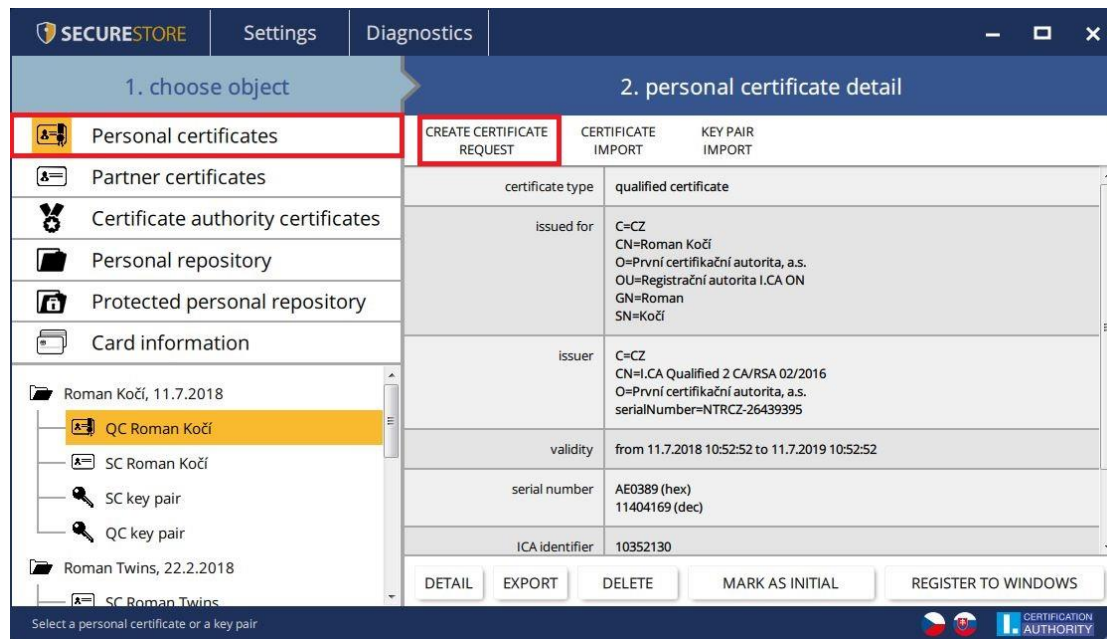
Fig. 27 – Personal Certificates Tool Bar



7.2.1. Generating Certificate Application

The **Generate Certificate Application** option opens the I.CA website and chooses the required certificate application type for generating a key pair using the online generator.

Fig. 28 – Choosing Application Type to Generate Key Pair with Online Generator



Once the certificate application type is selected, the user is directed to the I.CA online generator, where a system test needs to be run (to check you have the components required for launching the online generator).

Fig. 29 – Choosing Certificate Application Type

První certifikační autorita, A.S. | SPOJENÍ S DŮVĚROU

O NÁS | REGISTRAČNÍ AUTORITY | PRODUKTY A SLUŽBY | CENÍK | PODPORA | KONTAKTY

> Produkty a služby > HW řešení a čipové karty > SecureStore I.CA > SecureStore I.CA – request

Čipová karta
výběr typu žádosti

Žádost o kvalifikovaný certifikát
Žádost o komerční certifikát
Žádost o Twins

Vyberte si typ certifikátu, který požadujete na Vaši čipovou kartu vydat a postupujte dle pokynů průvodce.

Čipová karta
výběr typu žádosti

Žiadosť o kvalifikovaný certifikát
Žiadosť o komerčný certifikát
Žiadosť o Twins

Vyberte si typ certifikátu, ktorý požadujete na Vašu čipovú kartu vydat a postupujte podľa pokynov sprievodcu.

Smart card

Request Qualified certificate
Request Commercial certificate
Request Twins

For the issuance of a certificate on a smart card, you can choose the type and further follow the wizard.

Fig. 30 – 1. System Test – Online Generator

1. Test system | 2. Entering data | 3. Verification | 4. Saving request | 5. Completion

Is your computer ready?

First it is necessary to test whether your computer meets the minimum requirements for trouble-free generation of request. Through the tests, you may be asked to perform some updates software components, in this case it is necessary to confirm acceptance of these updates.
In case of complications contact [technical support I.CA](#).

Begin analysis

Waiting for test launch

RESULT	DESCRIPTION	DETAILS
	Operation system version	
	Browser type and version	
	Support of JavaScript	
	Support of extensions or Java language	
	Support of I.CA Java Applet	
	Support of Starcos smart card / I.CA SecureStore application	
	Support of cookies storage	

Continue

Fig. 31 – 2. Entering Data – Online Generator

1. Test system
2. Entering data
3. Verification
4. Saving request
5. Completion

INFORMATION ABOUT THE APPLICANT
SHOW OTHER OPTIONS >>

<input type="radio"/> Current user (individual - non-entrepreneurial)	<input type="text" value="Degree (before name)"/>	<input type="text" value="Degree (after name)"/>
<input checked="" type="radio"/> Employee (incl. statutory body members)	<input type="text" value="Roman"/>	<input type="text" value="koči"/>
<input type="radio"/> A legal entity (company - self-employed)	<input type="text" value="test@ica.cz"/>	<input type="text" value="test@ica.cz"/>
<input type="radio"/> Pseudonym	<input type="text" value="První certifikační autorita, a.s."/>	<input type="text" value="test@ica.cz"/>

OPTIONAL IDENTIFIER OF NATURAL ENTITY

Insert optional identifier for individuals

OPTIONAL IDENTIFIER OF ORGANIZATION

Insert optional identifier for organization

Revocation password	<input type="text" value="exit"/>
Key Repository Type (CSP)	<input type="text" value="SecureStore CSP / Smart card I.CA"/>

Certificate containing IK MPSV for communication with the public authorities

Certificate sent in the ZIP format

Save the application in the card

ADVANCED CERTIFICATE OPTIONS >>

Continue

Fig. 32 – 3. Checking Data– Online Generator

1. Test system 2. Entering data 3. Verification 4. Saving request 5. Completion

INFORMATION ABOUT THE APPLICANT	
Full name	Roman kočí
Name	Roman
Surname	kočí
Organization	První certifikační autorita, a.s.
E-mail in the certificate	test@ica.cz
Country	Czech Republic
CERTIFICATE SETTING	
Type of the certificate	Qualified certificate
Type of applicant	Employee (incl. statutory body members)
Certificate containing IK MPSV for communication with the public authorities	Yes
Revocation password	exit
E-mail for contact with I.CA	test@ica.cz
Certificate sent in the ZIP format	Yes
Period of validity	365 days
Key Repository Type (CSP)	SecureStore CSP / Smart card I.CA
Algorithm thumbnails / Key length	sha256WithRSAEncryption / 2048
Usage setting key	Non Repudiation / Digital Signature
Extended usage setting key	id-kp-emailProtection
Encoding type	UTF8_STRING

Continue

Fig. 33 – Generating Key Pair and Signing Application – Online Generator

If multiple chip cards connect to your PC, you need to select in the dialogue the card to which the key pair will be generated. You will be prompted to enter PIN after selecting the chip card.

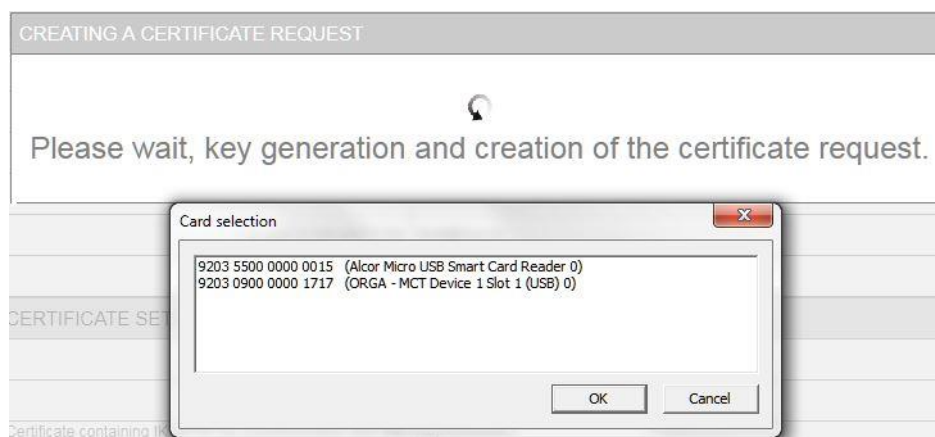


Fig. 34 – Entering PIN to Generate Key Pair and Sign Application

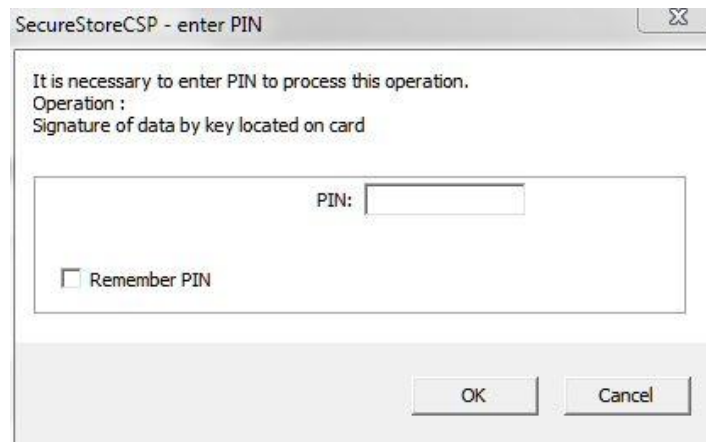


Fig. 35 – 4. Saving Application – Online Generator

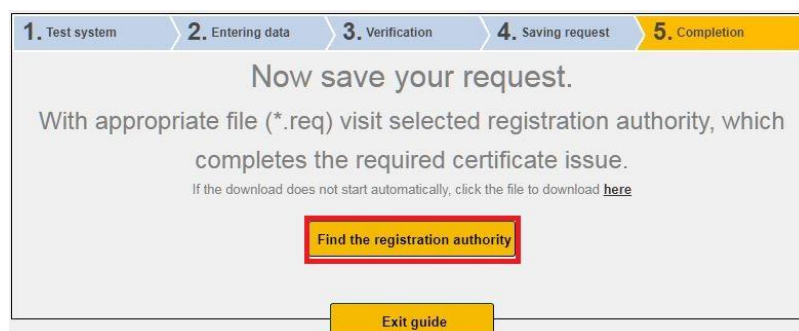
Selecting where certificate application is saved

If you choose **Save on I.CA Server**, a six-digit code of the application saved on the I.CA server is sent to the contact email specified in the certificate application.

If you choose **Save on Local Drive or External Storage**, a cert****.req file containing the generated application is saved.

Fig. 36 – 5. Completion – Online Generator

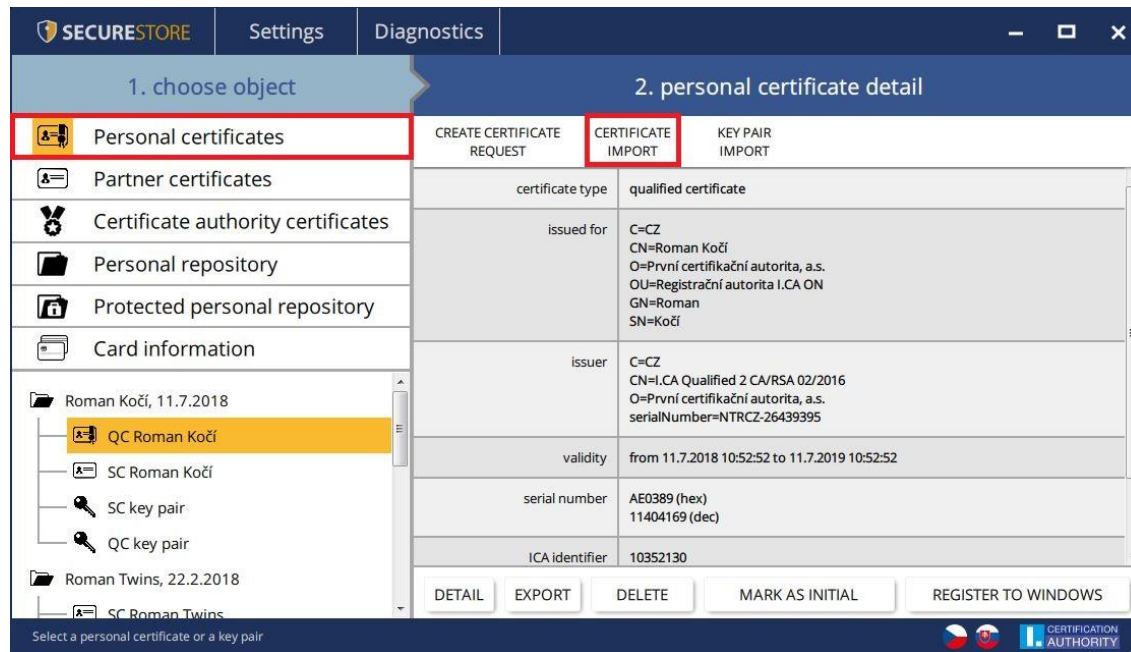
The six-digit code for the application saved on the I.CA server or the .req file saved on a portable USB must then be delivered by hand to the registration authority; press **Search for Registration Authority** to look up a registration authority.



7.2.2. Importing Personal Certificate

This feature imports a personal certificate from a drive onto the chip card. The cer. / .der format is required for import. Go to **Personal Certificates** to access this feature.

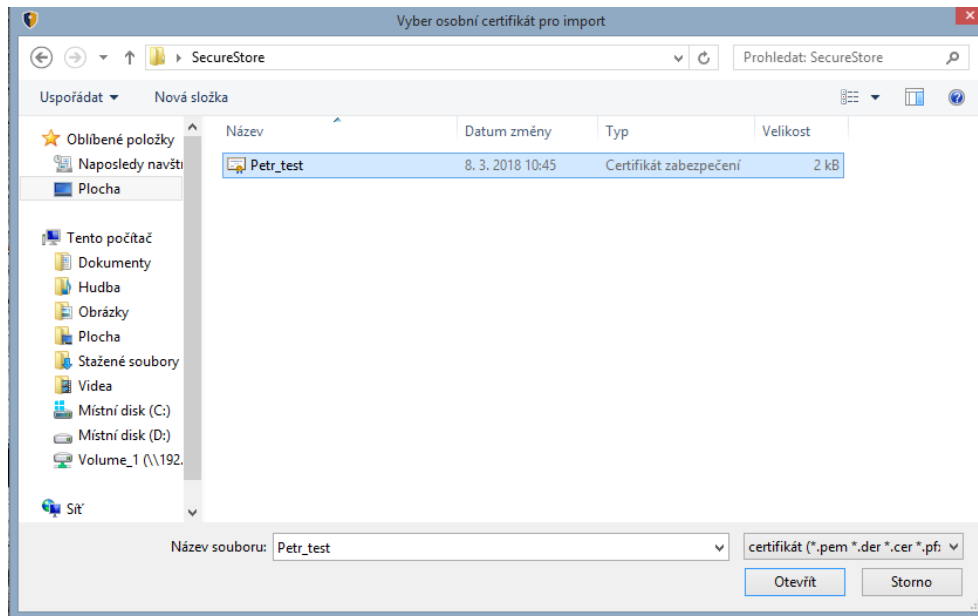
Fig. 37 – Importing Personal Certificate



After import the certificate is saved in that chip card storage where the certificate's keys are stored.

If no such storage with the corresponding keys exists on the chip card, the certificate is saved in the **Partner Certificates** chip card segment.

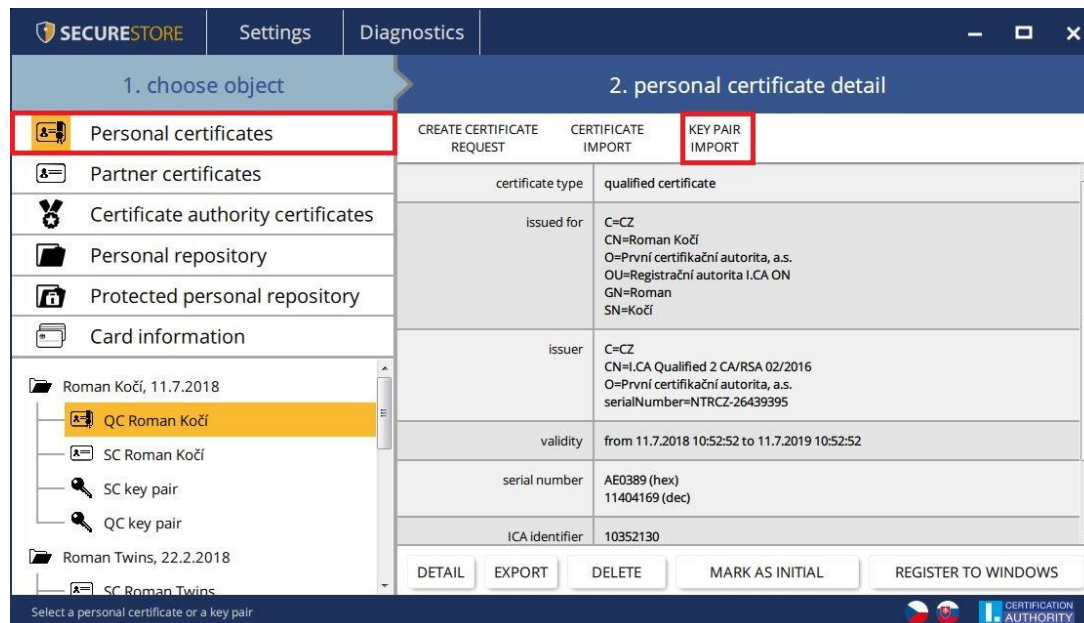
Fig. 38 – Selecting Certificate File for Card Import



7.2.3. Importing Backup Key Pair (PKCS#8)...

This option imports those keys into the card which were saved on the drive in generating a encrypting certificate application. Go to **Personal Certificates** to access this feature.

Fig. 39 – Importing Backup Key Pair (PKCS#8)

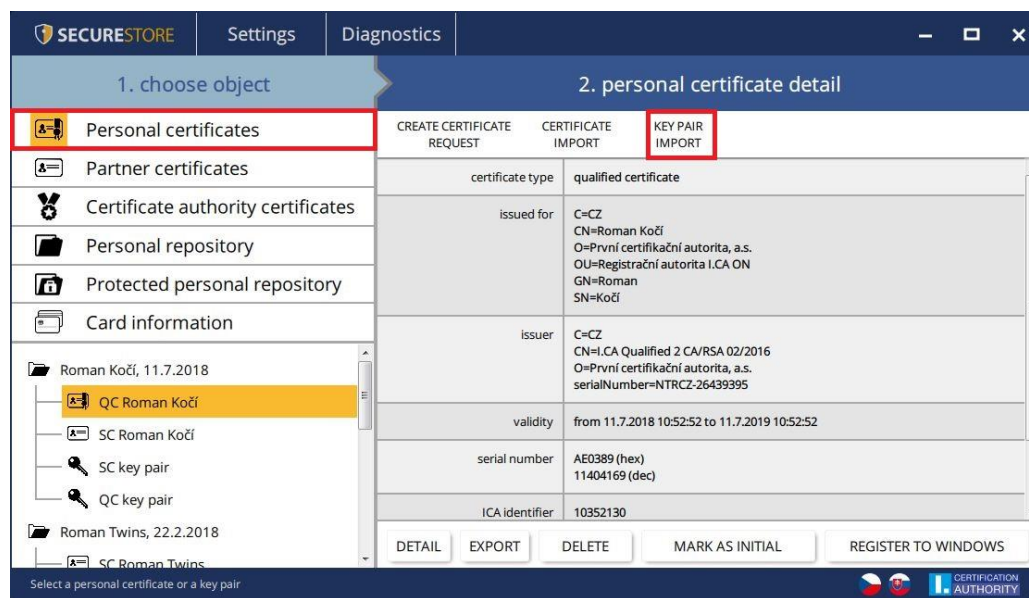


7.2.4. Importing Key Pair (PKCS#12)...

This option imports into the card those keys with certificate which are saved in the PKCS#12 format on the drive.

Go to **Personal Certificates** to access this feature.

Fig. 40 – Importing Key Pair (PKCS#12)

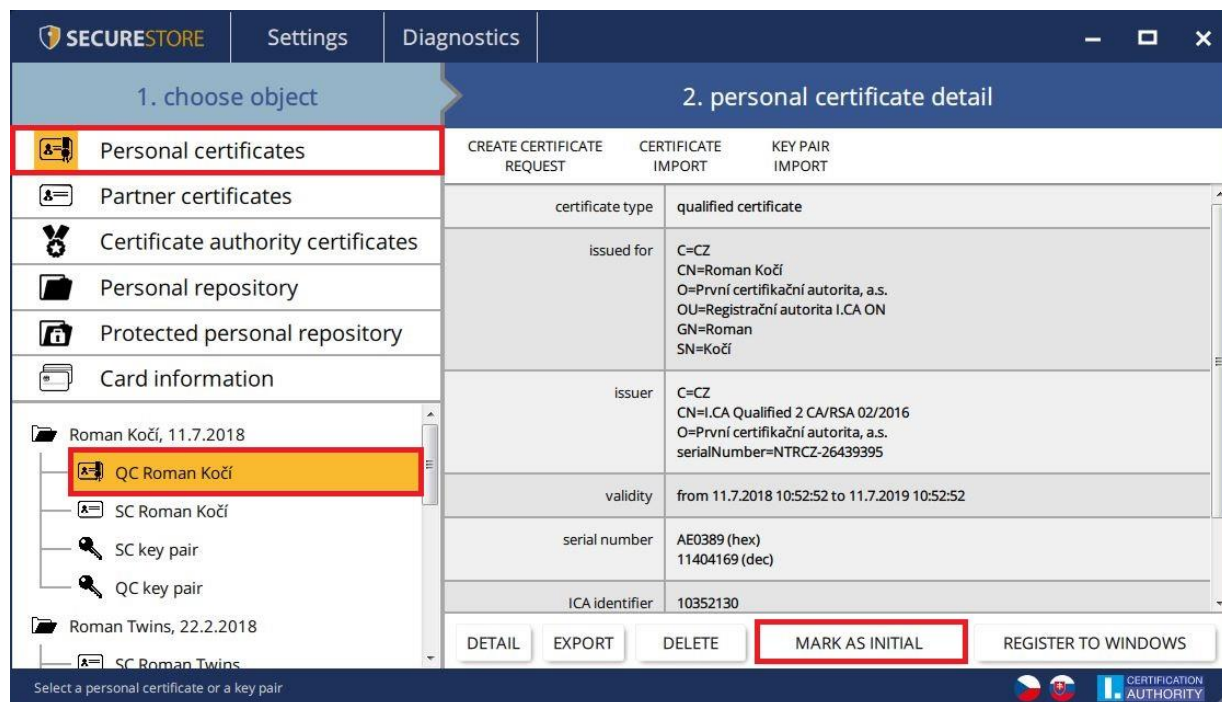


7.2.5. Setting Certificate as Default Windows Login Certificate

This option set the selected certificate as the default Windows login certificate. The selected certificate will be used for logging to Windows.

Go to **Personal Certificates** to access this feature, select the pertinent certificate and press **Set as Default** to confirm.

Fig. 41 – Setting Certificate as Default Windows Login Certificate



8. Glossary

- **Certification authority** – an independent trusted entity that issues certificates to clients. The certification authority guarantees that the link between a client and his certificate is unique.
- **Registration authority** – a point of contact for communication with clients. The primary job of a registration authority is to receive certificate applications and deliver certificates to clients. Registration authorities verify certificate applicants' identity and whether applications match the documents submitted. Registration authorities issue no certificates; they only submit certification applications to the I.CA central office.
- **Cryptographic transactions** – transactions using a key to encrypt and decrypt. Asymmetric cryptography is used for the chip cards – encryption and decryption are done with a pair of keys and an electronic signature is created and verified.

- **Electronic signature** – electronic data attached to, or logically linked with, a data message that permits verifying the signed person’s signature in relation to the signed message.
- **Electronic signature data** – unique data used by the signing person to create their electronic signature (in the meaning of the Electronic Signature Act); it is the private key of the pertinent asymmetric cryptographic algorithm (RSA in this instance).
- **Chip card** – a device providing secure storage of the user’s private key and allowing the user to create electronic signature. The chip card contains private keys, client’s certificates and certification authority certificates, and can also hold other data.
- **PIN and PUK** – a means to protect access to the card, that is, writing on the card and using the private keys saved on the card. These protective codes can be set in the card beforehand, with the user receiving the codes in the PIN envelope, or it is the client who sets his PIN and PUK for his card.
- **PIN envelope** – the letter a client may receive along with his card. A PIN envelope pertains to a specific card and contains the card’s unique identification, PIN and PUK. Some cards may be supplied without a PIN envelope.
- **Storage** – memory space on a medium, such as disk or chip card, where the key pair and the certificate are saved. A single chip card may have as many as 8 different storage compartments at a time. The chip card storage has its unique name. SIGNATURE-type storage does not permit creating key backups when generating a certification application. Any certificate for which keys are backed up thus must be saved in OTHER storage.
- **Certification application** – is completed by filling a form with applicant data. The applicant’s public key is attached to the information filled in the application form and all this structure is signed with the applicant’s private key. Certification application is digital data that include all the data required for the certificate to be issued.
- **Certificate** – proof of identity analogous to personal identity card; clients use their certificates to prove their identity in electronic communication. The procedure for getting the certificate is very similar to that for getting a personal identity card. I.CA provides these services through a network of points of contact – registration authorities, which deal with clients’ requests. A certificate is uniquely tied to a pair of keys the user

uses in electronic communication. The key pair is comprised of the public key and the private key.

- **Public key** – the public segment of the user’s key pair; the public key is used for verifying the electronic signature and encrypting (if any).
- **Private key** – the secret segment of the user’s key pair; the private key is used for creating the electronic signature and decrypting (if any). Therefore, the private key should enjoy the best protection possible and that is why it is stored on a chip card. A encrypting private key has to be kept throughout the existence of encrypted documents and messages. You may store this key on your card; it is recommended you also make and keep a backup copy elsewhere.
- **Certificate validity** – every certificate is issued for a definite period of time (1 year). The term of validity is specified in each certificate. The certificate used for electronic signature becomes useless after expiration. The encrypting certificate has to be kept beyond the term of validity to decrypt earlier messages.
- **Commercial certificate** – is issued to natural persons or legal entities and is suitable for regular use. Commercial certificates are issued in the **Standard** version (the private key is kept in Windows) or the **Comfort** version (the private key is kept on chip card).
- **Qualified certificate** – is strictly subject to EU Regulation 910/2014 and designed solely for electronic signatures. Creating, administering and using qualified certificates are governed by relevant certification policies. Qualified certificates are issued in the **Standard** version (the private key is kept in Windows) or the **Comfort** version (the private key is kept on chip card).
- **Certification authority certificate** – is used for verifying whether client certificates are correct and trusted. If you install a certification authority certificate on your PC, you declare to your operating system you trust that certification authority. In practice this means that if you receive a message electronically signed with a certificate issued by that certification authority, your system treats that certificate as a trusted one. In any other instance the message appears non-trusted.
- **Windows login certificate** – must contain specific data, so logging in to Windows with just any certificate is not possible. The I.CA registration authority arranges upon request that you are issued the right login certificate. The card storage containing the login

certificate must be designated as the authentication storage. A single card can only have just one storage compartment designated as the authentication storage.

- **List of public (commercial) I.CA certificates** – lists those I.CA-issued certificates whose holders have permitted publication. The list includes no ‘testing’ certificates and no certificates whose holders have not permitted publication.
 You can access the list of public commercial and qualified I.CA certificates here:
<https://www.ica.cz/List-public-certificates>

- **Card-supported certification authorities** – every card issued by I.CA has a defined list of supported certification authorities, and their certificates can be saved on the card.

- **Subsequent certificate** – is issued to the client upon a submitted electronic application, before the original certificate expires. The subsequent certificate is only issued if the client requests no change in the items of the previous certificate. If the client requests changes, he is issued a new original certificate rather than a subsequent one. Clients are not required to visit a I.CA registration authority to be issued a subsequent certificate before their original certificates expire. They only fill in and submit the standardised electronic subsequent certificate application electronically signed with their valid certificate.

- **Key usage**
 - **DigitalSignature** – Primarily, this attribute (bit) is set if the certificate is to be used in connection with a digital signature except ensuring non-repudiation, certificate signatures and certificate revocation lists by the certification authority. Usage: This bit must currently be set if the user’s private key linked to the issued certificate is intended to be used for creating digital signatures, such as using the certificate in secure electronic mail.
 - **NonRepudiation** – This attribute is set if the public key is to be used (by means of digital signature verification) for proving liability for a transaction made by the signing person. Usage: This bit must currently be set particularly with qualified certificates where the user’s private key linked to the issued certificate is intended to be used for creating electronic signatures.
 - **KeyEncipherment** – This attribute is set if the public key is to be used for transferring cryptographic keys. Usage: This bit must currently be set if the user’s certificate is intended to be used for encryption in secure electronic mail. In MS Outlook this bit must also be set if the use has no other certificate to use for encryption.

- The PKCS#12 format - a RSA key and the certificate can be saved in a single file, which is defined by the PKCS#12 standard. This format allows various operations, such as exporting the RSA keys of the certificate from the Windows storage if export of private key is permitted. The file content is password-protected. The file extension is pfx or p12.