První certifikační autorita, a.s.

I. CERTIFICATION AUTHORITY

I.CA SecureStore macOS

User Guide

Version 8.1 and higher

Date created:	15.4.2025
version:	8.1
Number of pages:	33

CONTENT

1. Introduction

The user guide is valid for I.CA SecureStore application version 8.1 and higher. These versions have the same functionality and the same user interface.

2. Card access data

STARCOS 3.7

Smart 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 8 digits. Entering a wrong PUK 5 times in a row will disable the PUK and thus also the smart card.

Reenabling PIN using PUK is limited to 3 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 6–8 digits.

The length of the PIN for secure storage is 4-12 digits.

2.1 Card initialization

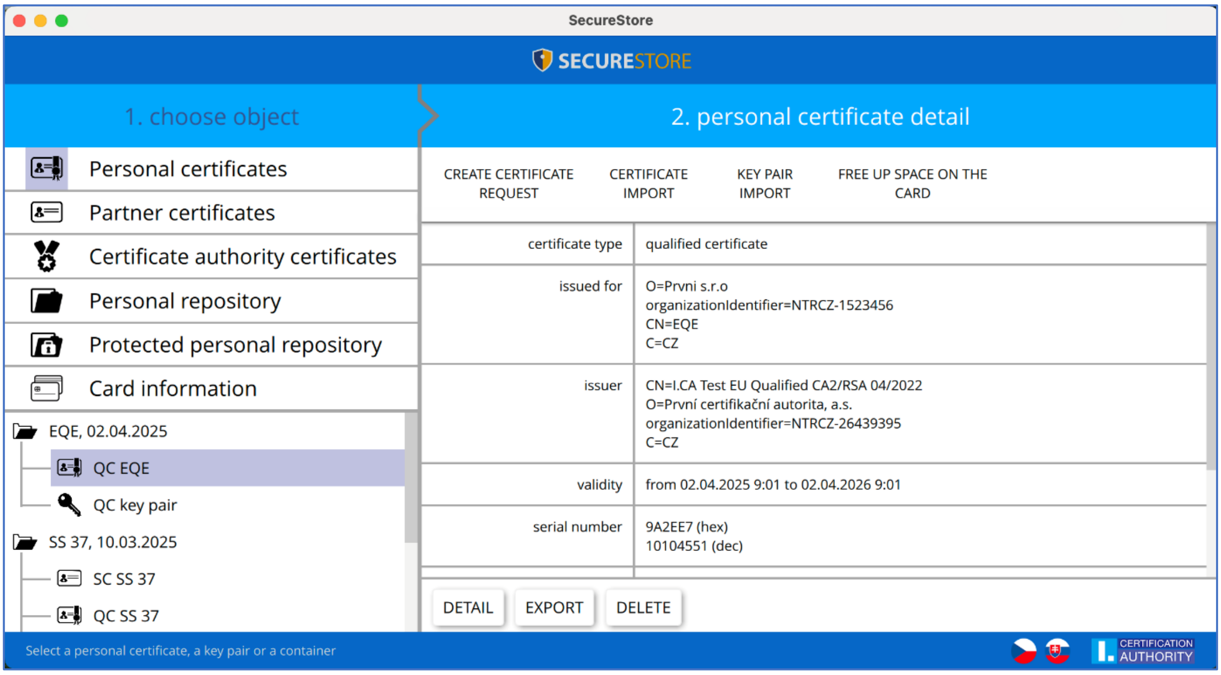
Card initialization means setting a PIN and a PUK.

If the user has received the PIN envelope, the card has been initialized already and PIN and 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 initialization dialogue is displayed automatically, usually in launching the application with a new smart card for the first time. Please make sure you remember your PIN and PUK

3. Main screen

Fig. 1 – Main screen



certificate type	qualified certificate

issued for	O=Prvni s.r.o
	organizationIdentifier=NTRCZ-1523456
	CN=EQE
	C=CZ

issuer	CN=I.CA Test EU Qualified CA2/RSA 04/2022
	O=První certifikační autorita, a.s.
	organizationIdentifier=NTRCZ-26439395
	C=CZ

validity	from 02.04.2025 9:01 to 02.04.2026 9:01
serial number	9A2EE7 (hex) 10104551 (dec)

Select a personal certificate, a key pair or a container

The main screen is divided into two parts. The left part of the screen displays a list of objects stored on the smart card. The right part of the screen displays the individual details of the object on the smart card. The top bar shows the following options – see Fig. 3.

3.1 Change the language of the application

The user can make the change in the lower right corner of the application by clicking on the appropriate flag.

Picture 2 - Switching the language

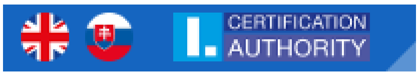
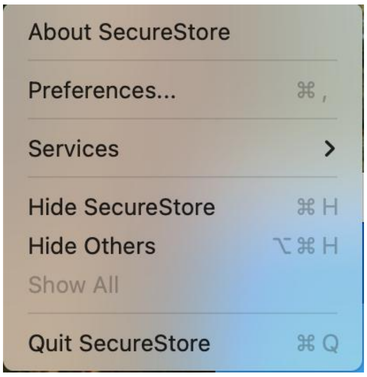
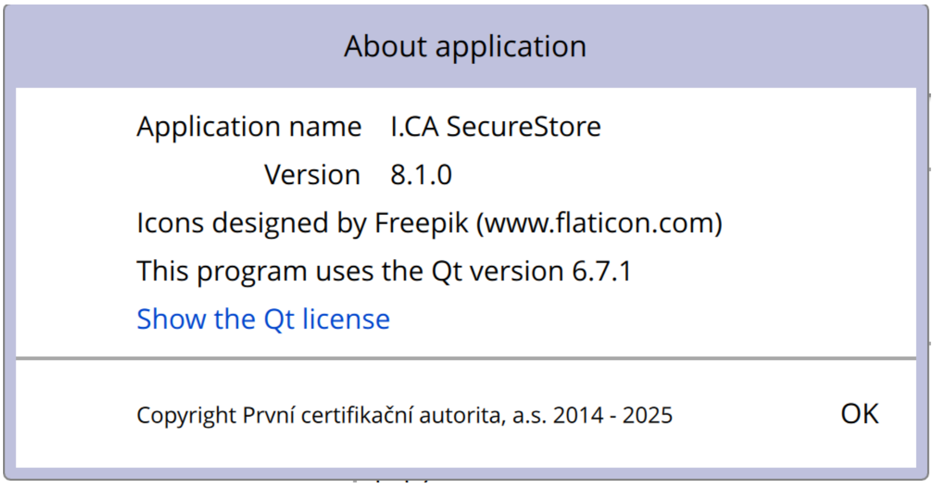


Fig. 3 - Main menu



The user can find out about the version of the application by clicking on **About SecureStore.**

Fig. 4 - Application version



About application

Application name I.CA SecureStore

Version 8.1.0

Icons designed by Freepik (www.flaticon.com)

This program uses the Qt version 6.7.1

Show the Qt license

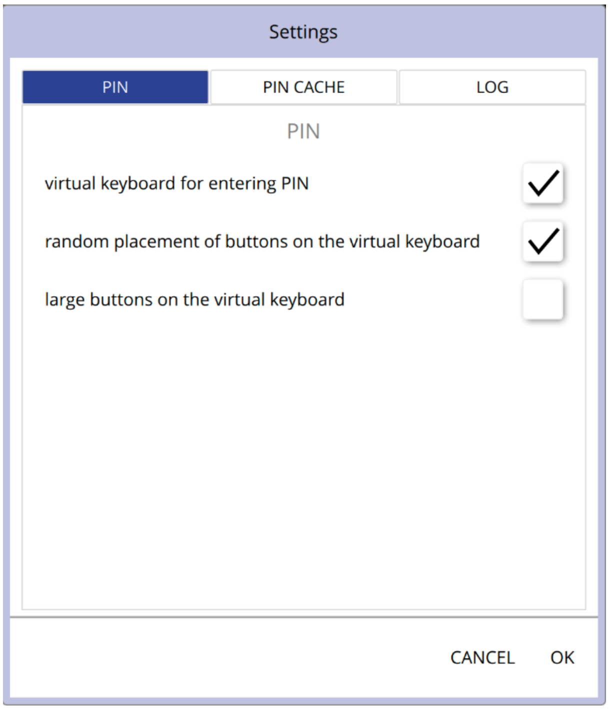
Copyright První certifikační autorita, a.s. 2014 - 2025

The **Preferences option** is used for:

1) *Adjust the keypad for entering PIN*

By default, the app is set to **"Virtual PIN Keyboard"** and **"Shuffle PIN Keyboard Buttons."**

Fig. 5 – Ping Keypad



PIN

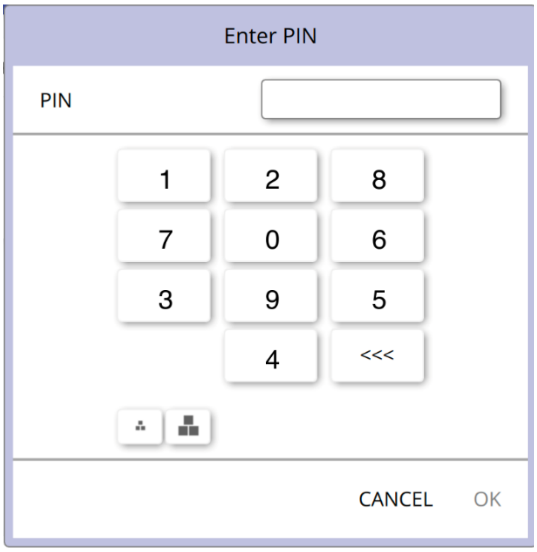
virtual keyboard for entering PIN ☑

random placement of buttons on the virtual keyboard ☑

large buttons on the virtual keyboard □

The user then enters the PIN on the virtual keyboard with the mouse cursor.

Fig. 6 – Keyboard for PIN entry

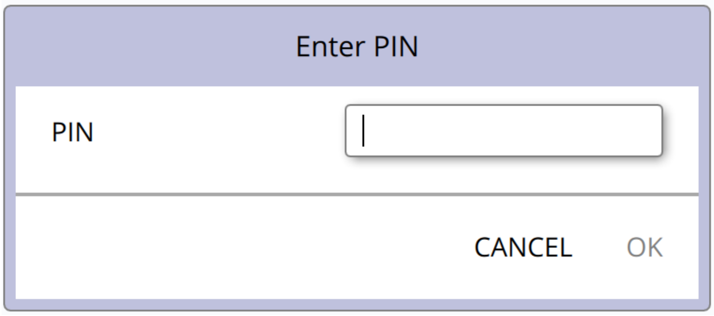


PIN

It is possible to change the PIN entry to the numeric keypad.

In "**Settings"**, you need to select the **"PIN" tab,** remove the virtual keypad option for PIN and confirm with the **"OK" button**.

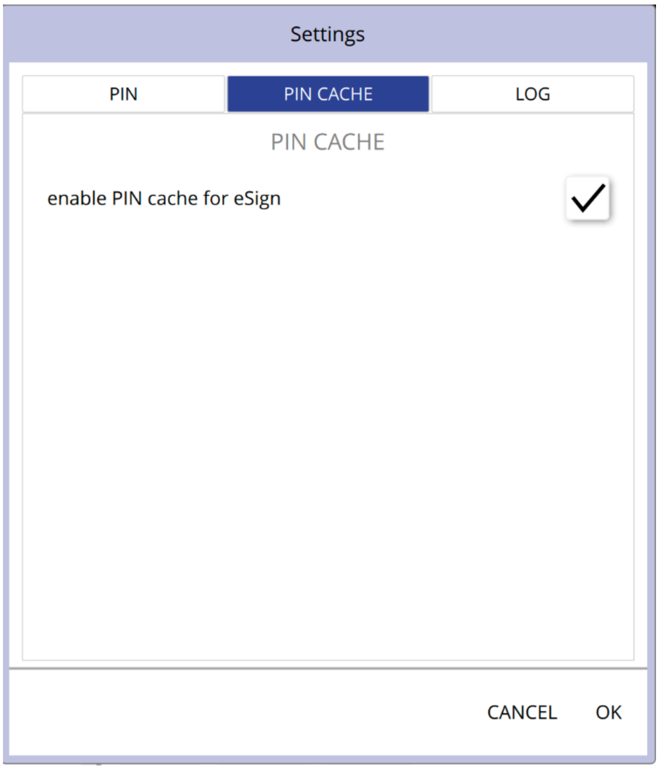
Fig. 7 – PIN keypad


Enter PIN

PIN

1) *PIN CACHE – the time the PIN is stored in memory*

Fig. 8 – PIN memorization settings


Settings

PIN CACHE

enable PIN cache for eSign ☑

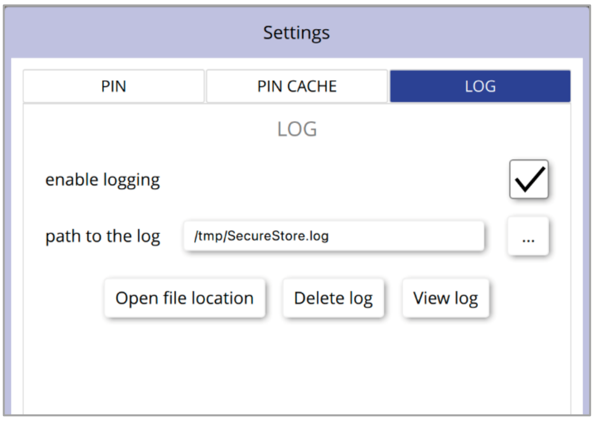
Note: Note: The time for remembering the PIN and encrypting the key is unlimited. Furthermore, the application allows you to remember the PIN in relation to the application process.

2) *LOG*

Enabling application logging for possible analysis of technical problems when using a smart card and application. The application records the so-called audit log, where the last security-sensitive operations, such as key deletion, key generation, etc., will be recorded in the audit log as part of operations with the smart card.

The user can change the path to the saved log file using the button ...

Fig. 10 – Log



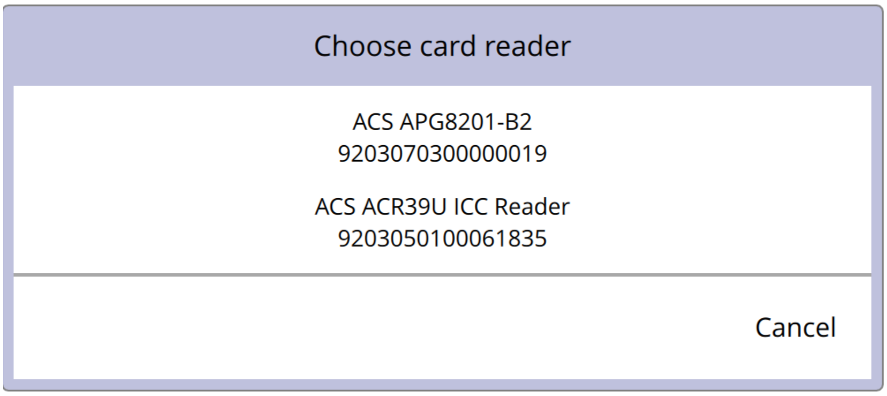
enable logging ☑

path to the log /tmp/SecureStore.log ...

Selection of smart card reader.

If the user has more than one smart card reader connected to the PC, the "Smart Card Reader Selection" window is displayed even after the application is started.

Fig. 13 - Selecting a smart card reader



Choose card reader

ACS APG8201-B2
9203070300000019

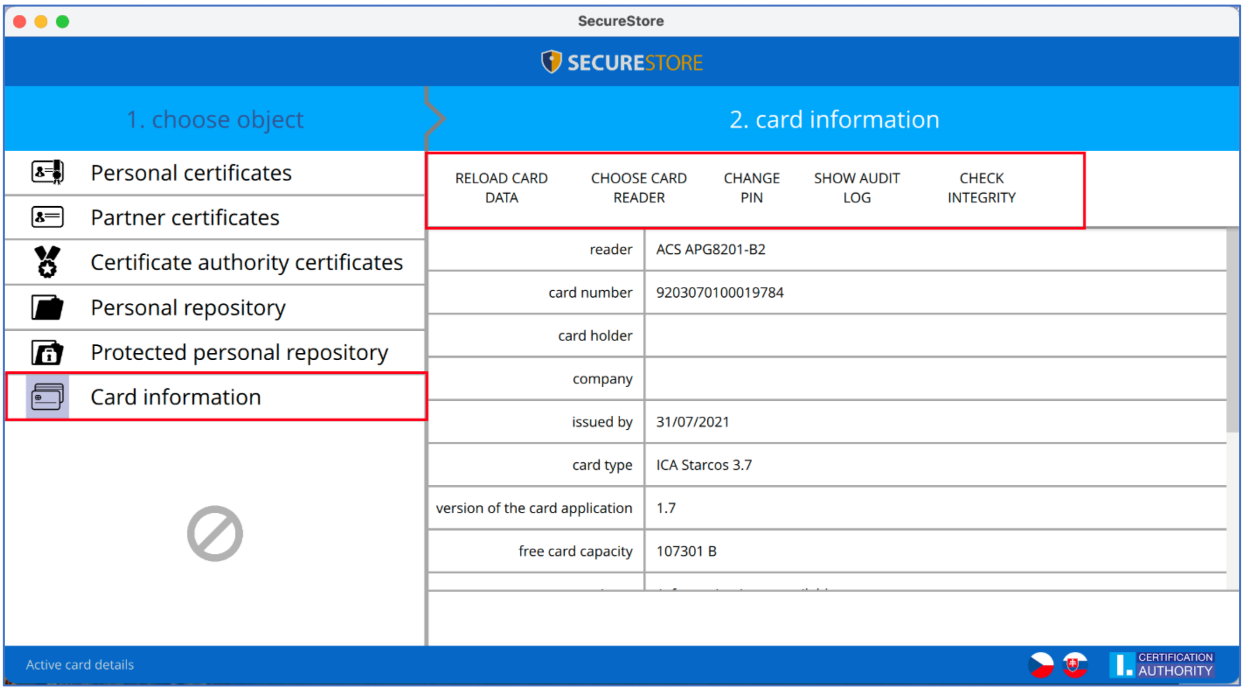
ACS ACR39U ICC Reader
9203050100061835

If the user has only one smart card reader connected to the PC, the window is not displayed.

Toolbar

In the toolbar, the options change according to the selected object on the left side of the screen.

Fig. 14 - Toolbar



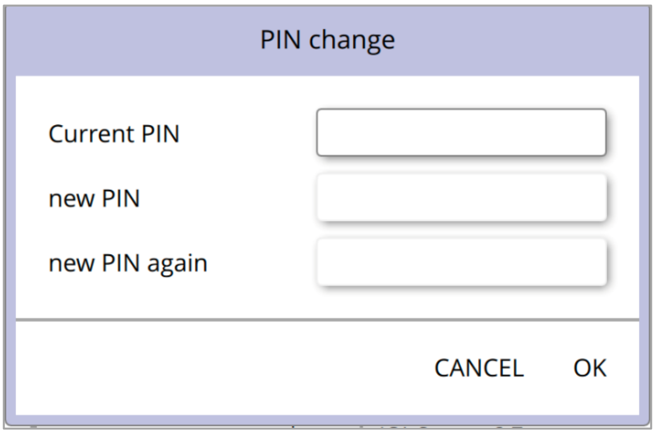
reader	ACS APG8201-B2
card number	9203070100019784
card holder	
company	
issued by	31/07/2021
card type	ICA Starcos 3.7
version of the card application	1.7
free card capacity	107301 B

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

Choose ***Reload Card Data*** to reload data from the smart 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.

Fig. 15 - Change of PIN

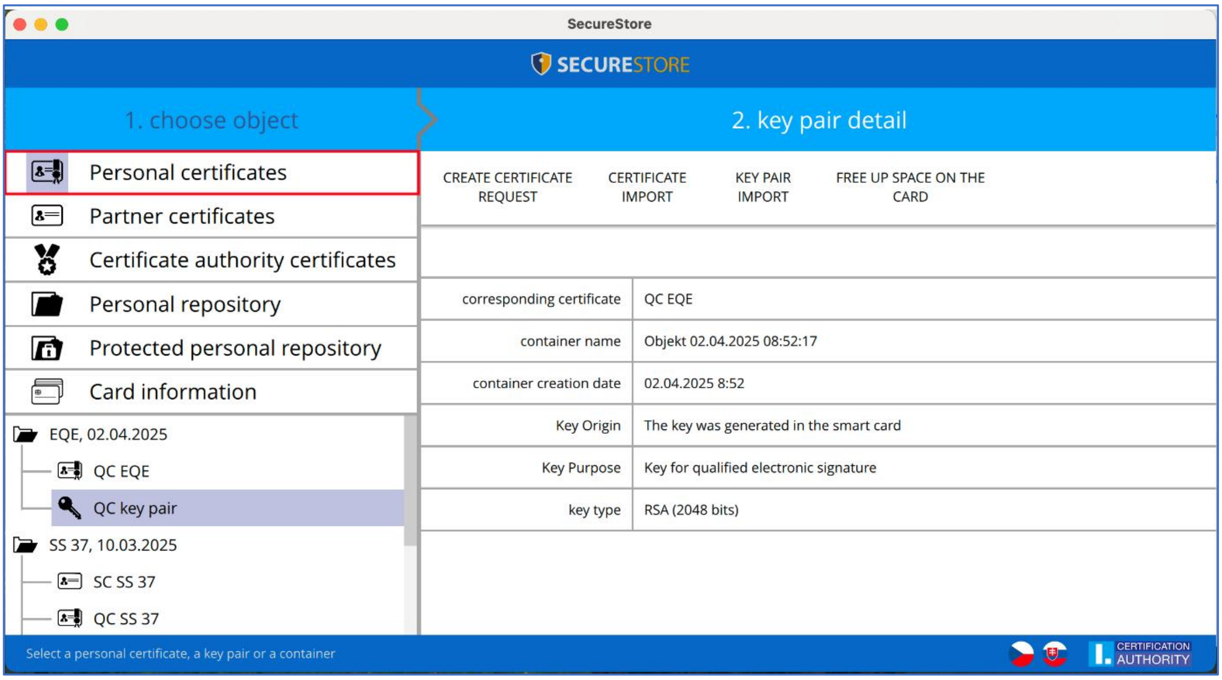


a) **<u>Starcos 3.7</u> –** The **Change PIN** option allows you to change the PIN provided, if the value of the original PIN is known. The **Unblock PIN** option allows a new PIN value to be set if the user blocks the PIN. A PUK is required to unblock the new PIN setting. By entering the PUK, the user activates 3 new attempts to enter the correct PIN. **PIN unblocking with PUK is limited to 3 attempts.**

4. Display key pair information.

The user can find information about the key pair in the **"Personal certificates"** object.

Fig. 16 – Displaying key pair information



corresponding certificate	QC EQE
container name	Objekt 02.04.2025 08:52:17
container creation date	02.04.2025 8:52
Key Origin	The key was generated in the smart card
Key Purpose	Key for qualified electronic signature
key type	RSA (2048 bits)

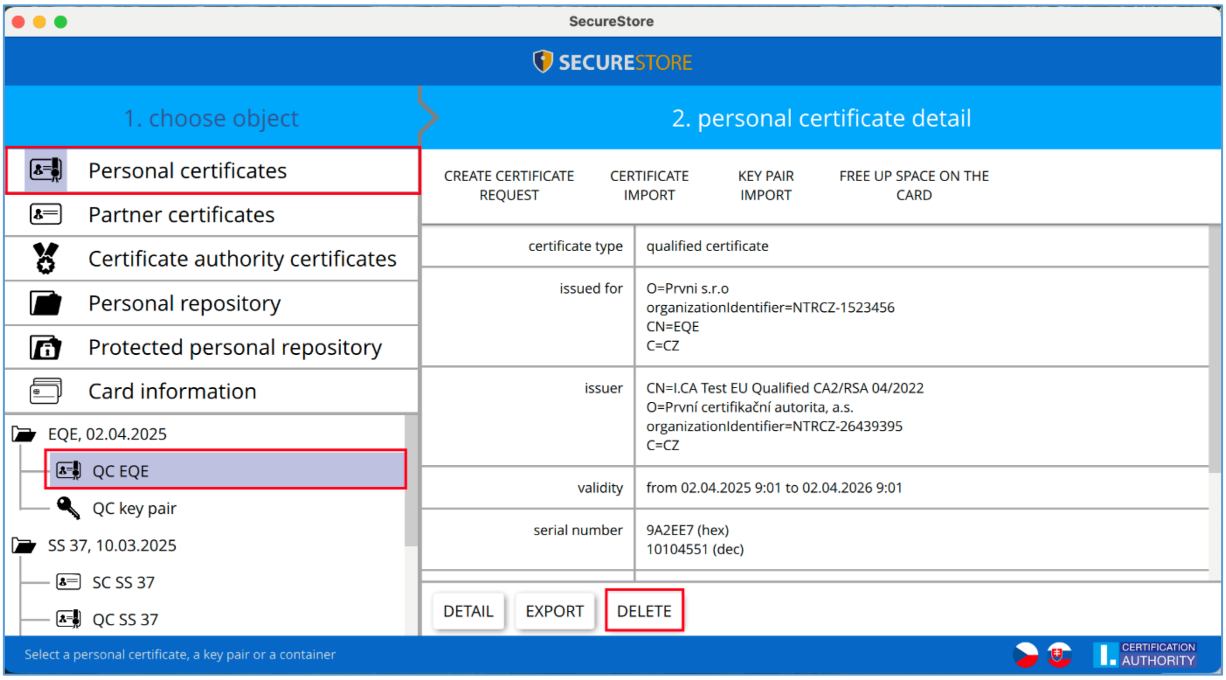
Select a personal certificate, a key pair or a container

The store stores one key pair for the certificate, two key pairs for Twins certificates. The public/private key creation time indicates the exact time when the key was generated on the card or imported to the card. The method of key creation on the card is displayed in the "**Key origin"** item. The "**Key purpose"** item specifies whether the key is an encryption key or a signature key. The "**Key type" is given next**, in the example it is a key for the RSA algorithm with a length of 2048 bits. A pair of keys can be removed from the card using the "**Delete" button**.

4.1 Deleting a public key

The user can find the option in the **"Personal certificates"** object, select the required public key and use the **"Delete"** button to delete it.

Fig. 17 - Deleting the public key



certificate type	qualified certificate

issued for	O=Prvni s.r.o
	organizationIdentifier=NTRCZ-1523456
	CN=EQE
	C=CZ

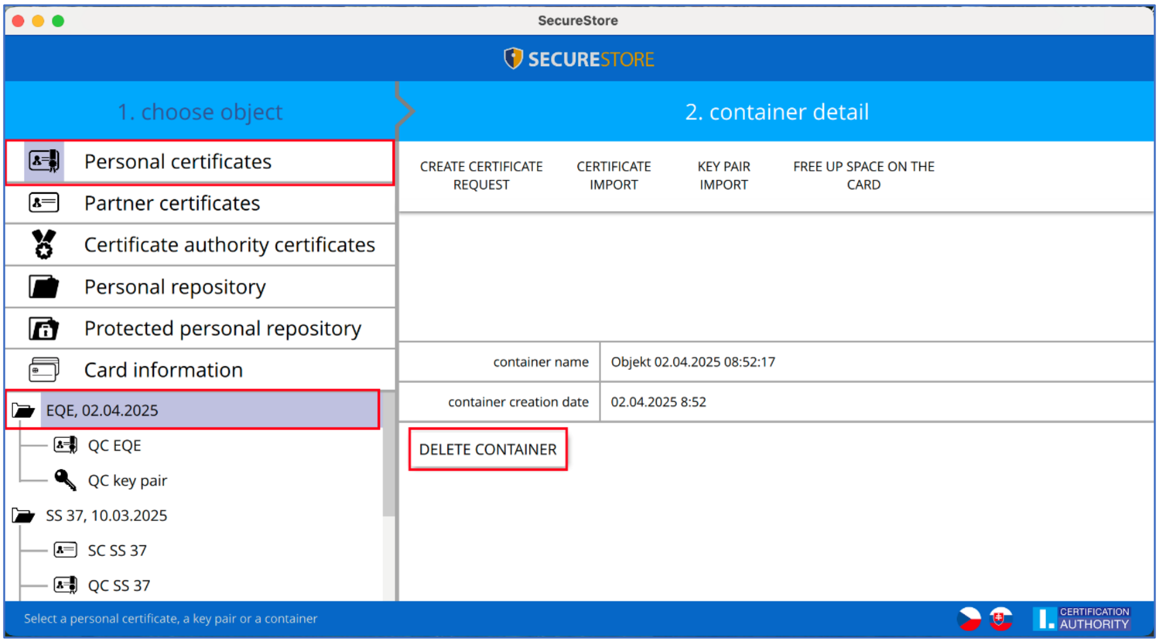
issuer	CN=I.CA Test EU Qualified CA2/RSA 04/2022
	O=První certifikační autorita, a.s.
	organizationIdentifier=NTRCZ-26439395
	C=CZ

validity	from 02.04.2025 9:01 to 02.04.2026 9:01
serial number	9A2EE7 (hex) 10104551 (dec)

Select a personal certificate, a key pair or a container

4.2 Delete a container

The user can find the option in the **"Personal certificates"** object, select the desired container and use the **"delete container"** button to delete it after entering the PIN.



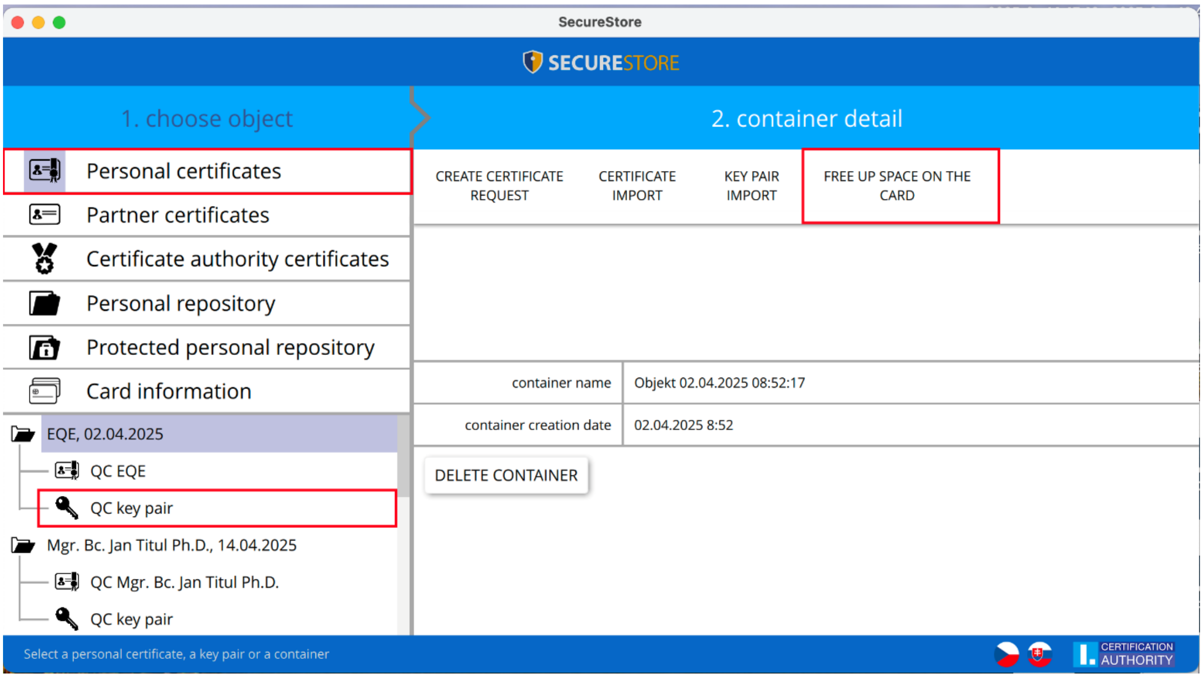
container name	Objekt 02.04.2025 08:52:17
container creation date	02.04.2025 8:52

Warning: If the user deletes the container, this session is irreversible and it will no longer be possible to sign/decrypt with the certificate!!

4.3 Deleting a container using the key removal wizard

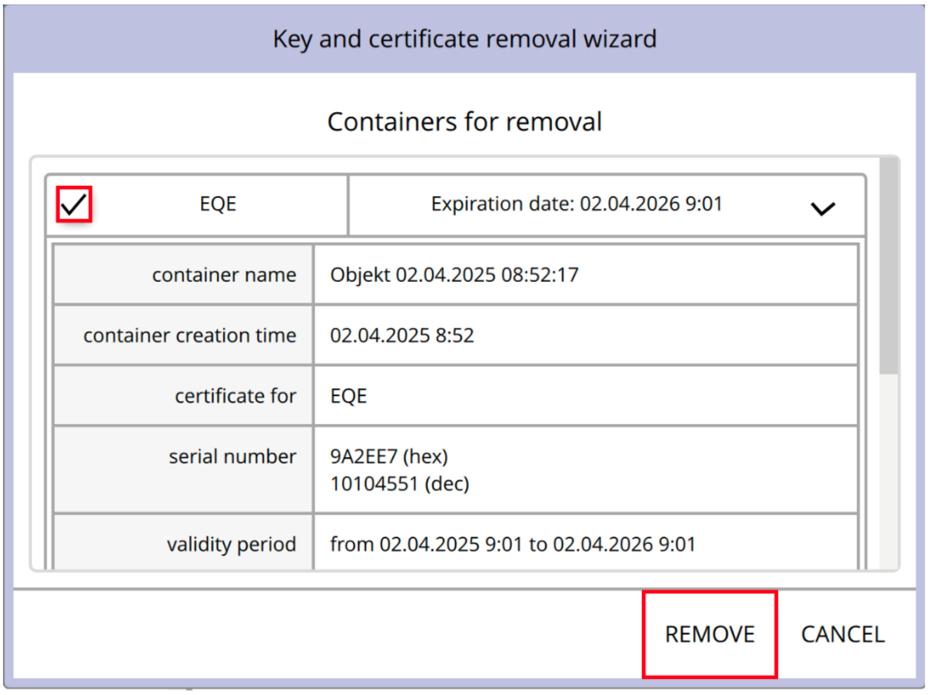
The user can find the option in the **"Personal certificates"** object, select the required key pair and start the **"Free up space on the card" function.**

Fig. 19 - Free up space on the card



container name	Objekt 02.04.2025 08:52:17
container creation date	02.04.2025 8:52

Fig. 20 Key and certificate removal wizard



Key and certificate removal wizard

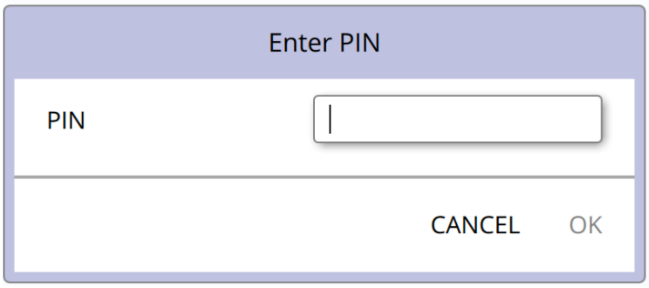
Containers for removal

☑ EQE	Expiration date: 02.04.2026 9:01
container name	Objekt 02.04.2025 08:52:17
container creation time	02.04.2025 8:52
certificate for	EQE
serial number	9A2EE7 (hex) 10104551 (dec)
validity period	from 02.04.2025 9:01 to 02.04.2026 9:01

Select the certificate, the **"Remove" option will appear**. This will delete the entire container.
If the user deletes the container, this session is irreversible and it will no longer be possible to sign/decrypt with the certificate!!

The **"Remove certificate"** option is only available for commercial certificates and is used to remove only the public key as in point 4.1
After clicking on the "**Delete" option,** the user is asked to enter the PIN, after entering the PIN, the marked certificate/container will be deleted

Figure 21 – Entering the PIN to delete the certificate/container

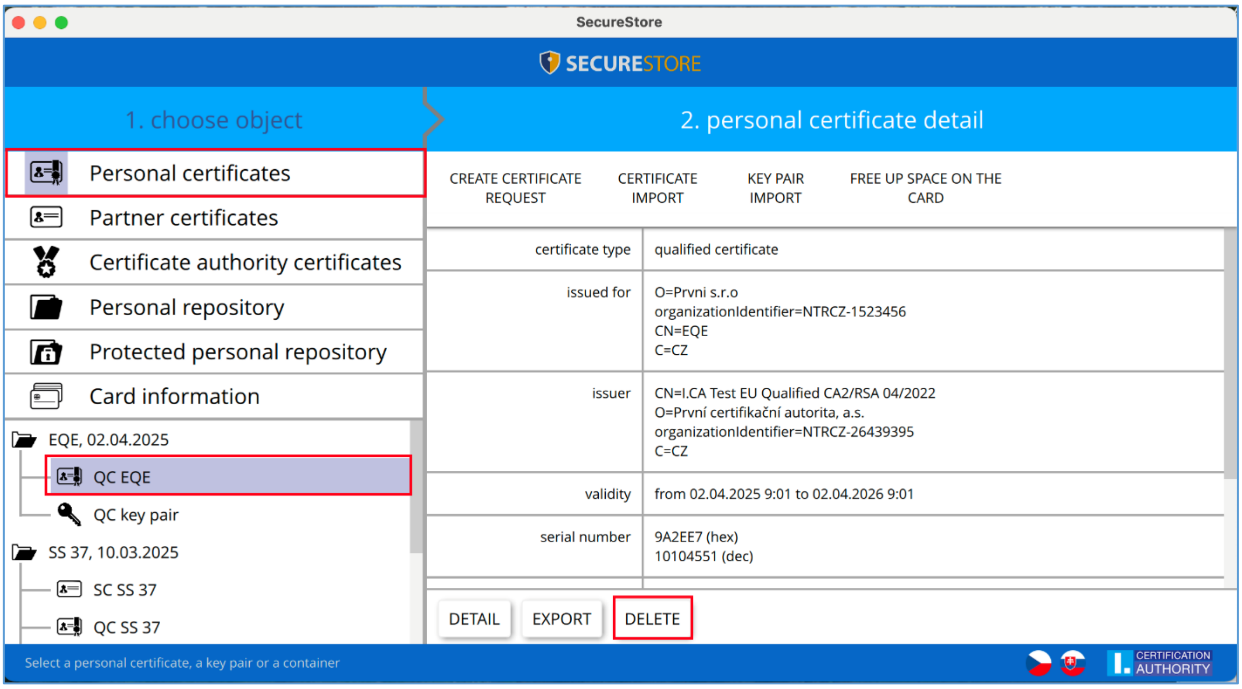


5.Certificates

5.1 Displaying the certificate

The user selects the certificate for which they want to view the details in the **"Personal certificates" object**. The certificate detail is displayed in the right screen of the application in **the "Personal certificate detail".**

Fig. 22 – Certificate display



certificate type	qualified certificate

issued for	O=Prvni s.r.o
	organizationIdentifier=NTRCZ-1523456
	CN=EQE
	C=CZ

issuer	CN=I.CA Test EU Qualified CA2/RSA 04/2022
	O=První certifikační autorita, a.s.
	organizationIdentifier=NTRCZ-26439395
	C=CZ

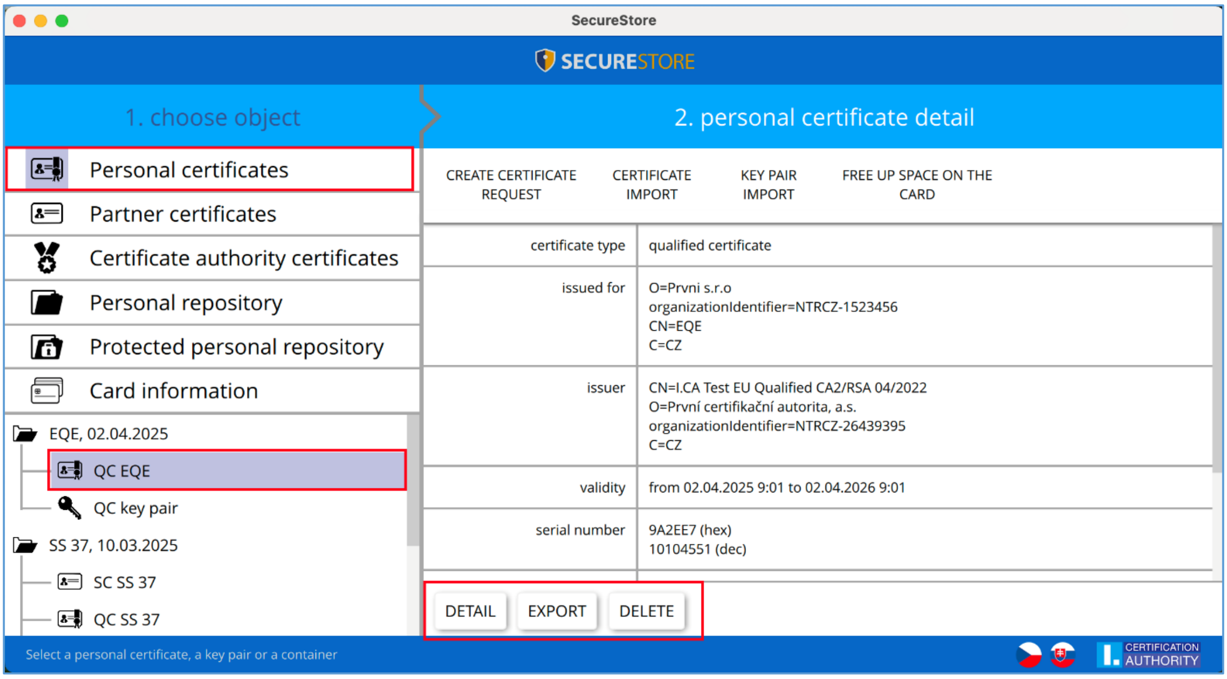
validity	from 02.04.2025 9:01 to 02.04.2026 9:01
serial number	9A2EE7 (hex) 10104551 (dec)

5.2 Working with a personal certificate

Options for working with the certificate stored on the smart card are available in the toolbar at the bottom of the application.

In the **"Personal certificates" object** , the user selects the desired certificate and then selects the desired operation in the toolbar.

Fig. 23 - Options for working with a personal certificate in the toolbar



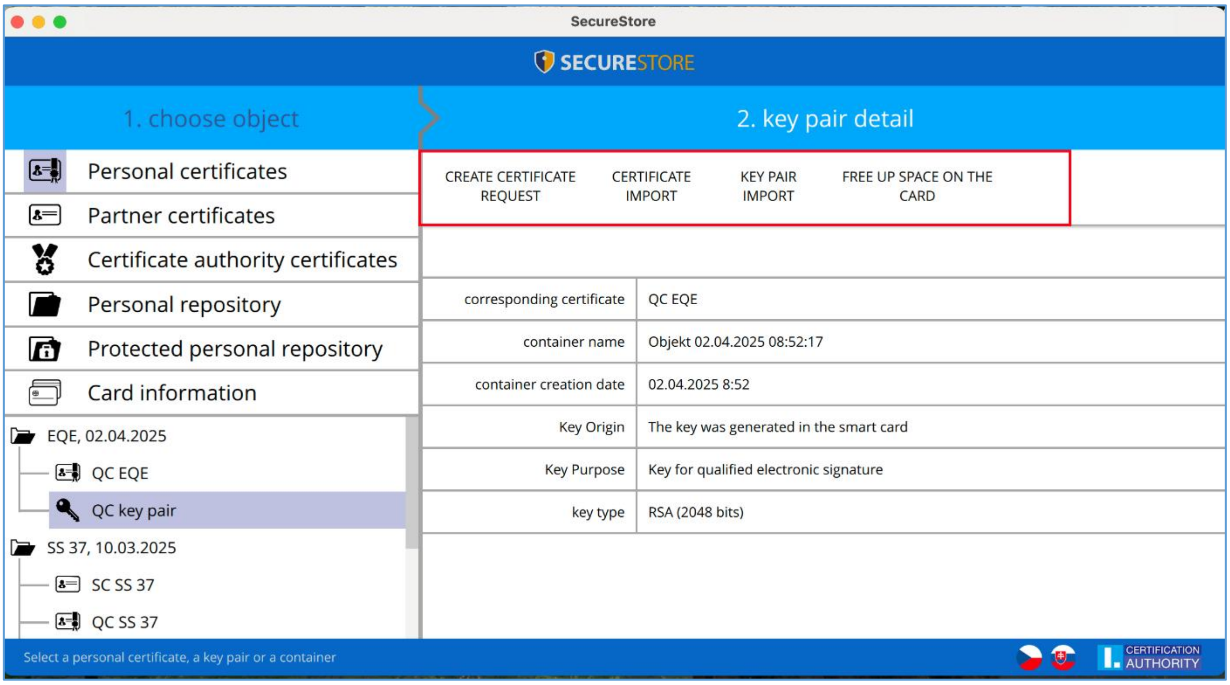
certificate type	qualified certificate

issued for	O=Prvni s.r.o
	organizationIdentifier=NTRCZ-1523456
	CN=EQE
	C=CZ

issuer	CN=I.CA Test EU Qualified CA2/RSA 04/2022
	O=První certifikační autorita, a.s.
	organizationIdentifier=NTRCZ-26439395
	C=CZ

validity	from 02.04.2025 9:01 to 02.04.2026 9:01
serial number	9A2EE7 (hex) 10104551 (dec)

Fig. 24 - Options for importing certificates



corresponding certificate	QC EQE
container name	Objekt 02.04.2025 08:52:17
container creation date	02.04.2025 8:52
Key Origin	The key was generated in the smart card
Key Purpose	Key for qualified electronic signature
key type	RSA (2048 bits)

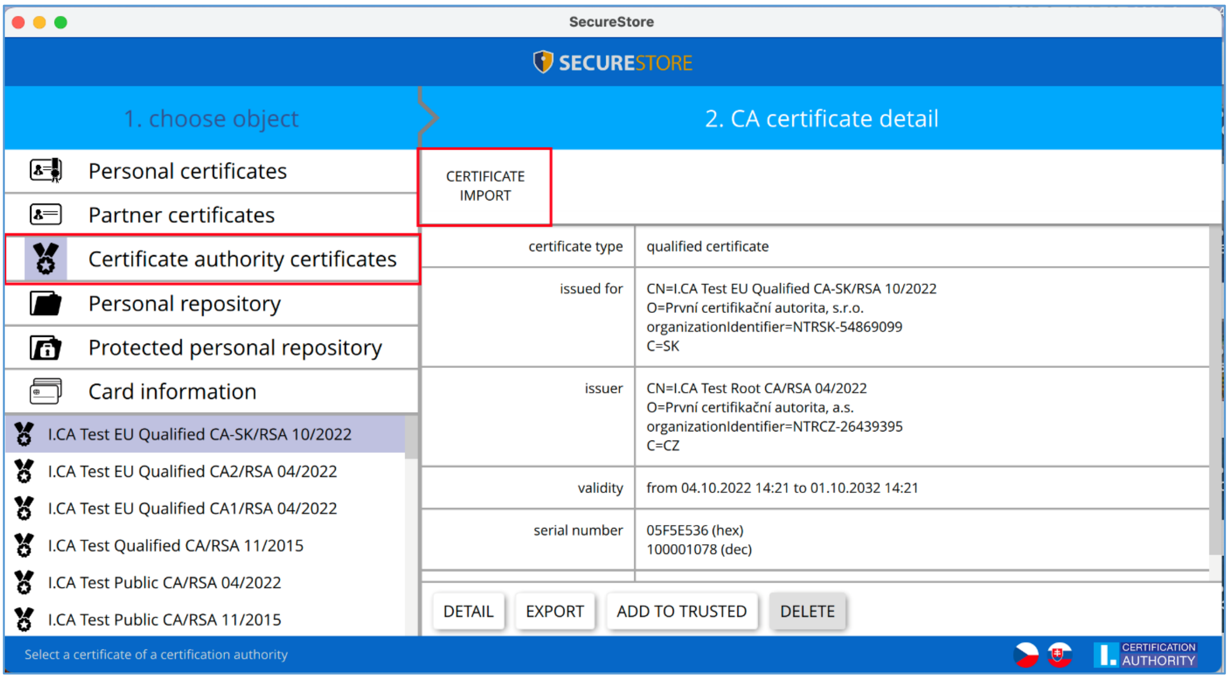
The personal certificate is imported into the store, where the corresponding key pair is stored. Communication partner certificates can be imported as partner certificates. The plain certificate data view is only for professionals to visually inspect the certificate data.

5.3 Working with the 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 smart 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/Rootcertificate

Fig.25 – Importing the certificate of the certification authority


SecureStore
SECURESTORE
1. choose object
2. CA certificate detail
Personal certificates
Partner certificates
Certificate authority certificates
Personal repository
Protected personal repository
Card information
I.CA Test EU Qualified CA-SK/RSA 10/2022
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
CERTIFICATE IMPORT
DETAIL
EXPORT
ADD TO TRUSTED
DELETE
Select a certificate of a certification authority
CERTIFICATION AUTHORITY

certificate type	qualified certificate

issued for	CN=I.CA Test EU Qualified CA-SK/RSA 10/2022
	O=První certifikační autorita, s.r.o.
	organizationIdentifier=NTRSK-54869099
	C=SK

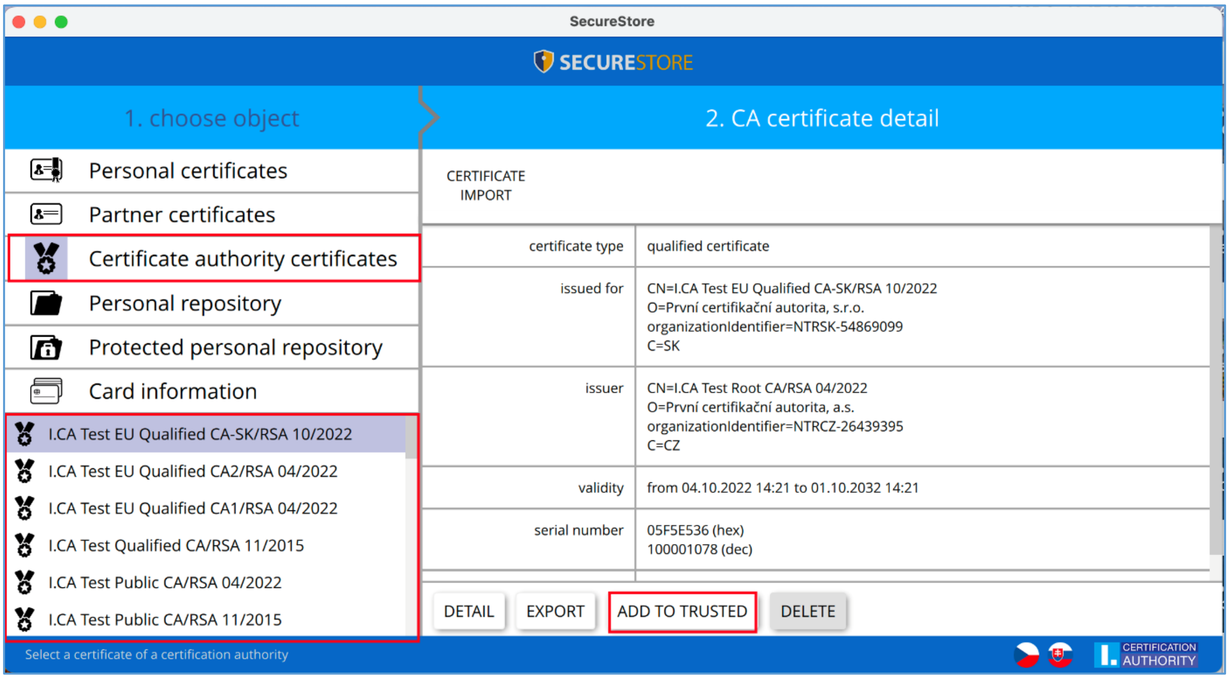
issuer	CN=I.CA Test Root CA/RSA 04/2022
	O=První certifikační autorita, a.s.
	organizationIdentifier=NTRCZ-26439395
	C=CZ

validity	from 04.10.2022 14:21 to 01.10.2032 14:21
serial number	05F5E536 (hex) 100001078 (dec)

Root certificates are used to verify the trust of personal certificates. To work with certificates, root certificates must be registered with Windows so that Windows can verify the trust of the certificates used for signing or encryption.

If the user is using an earlier version of Windows and the root certificates I.CA are not included with Windows, register the root certificate from a smart card. To register, use the **"Add to trusted"** option, see Fig. 26. Registration of the root certificate into Windows requires the user's consent, then the root certificate is registered in MS Windows as a trusted root certificate.

Fig. 26 – Registering a certification authority certificate



I.CA Test EU Qualified CA-SK/RSA 10/2022
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

certificate type	qualified certificate

issued for	CN=I.CA Test EU Qualified CA-SK/RSA 10/2022
	O=První certifikační autorita, s.r.o.
	organizationIdentifier=NTRSK-54869099
	C=SK

issuer	CN=I.CA Test Root CA/RSA 04/2022
	O=První certifikační autorita, a.s.
	organizationIdentifier=NTRCZ-26439395
	C=CZ

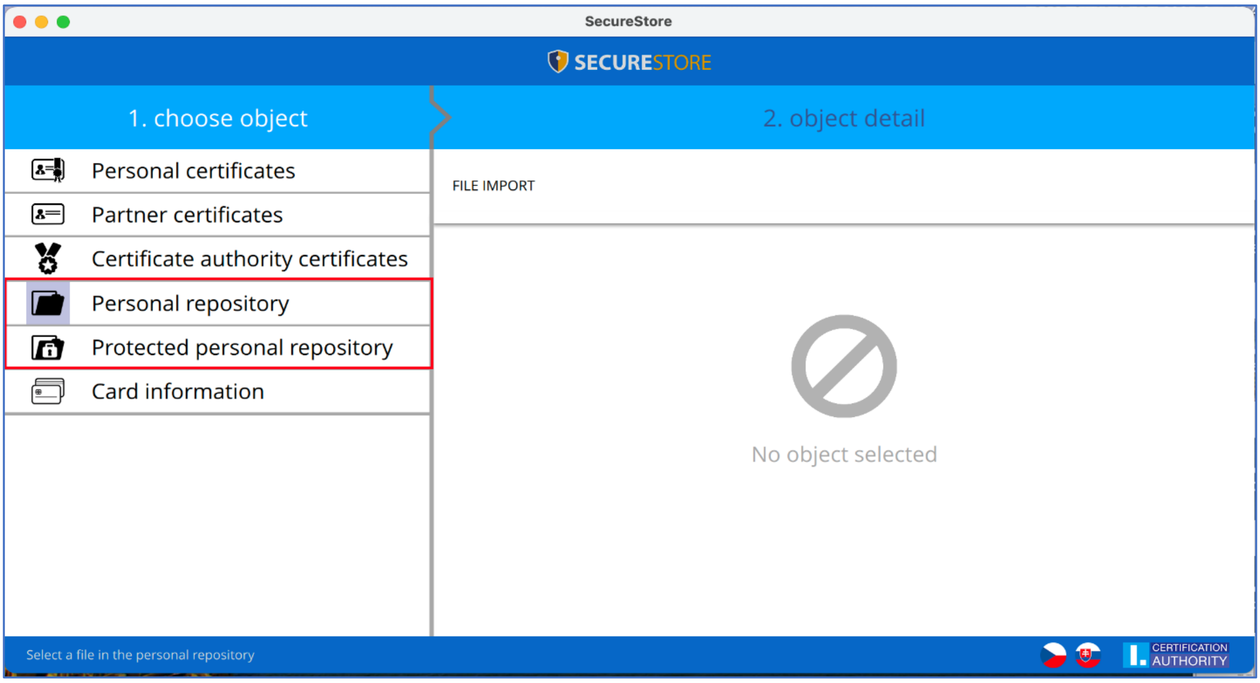
validity	from 04.10.2022 14:21 to 01.10.2032 14:21
serial number	05F5E536 (hex) 100001078 (dec)

Select a certificate of a certification authority

6. Personal repository

The user can store small files (a few kB) in the **"Personal repository"** or **"Protected personal repository"** section of the tab. Text as well as binary files can be saved to the tab. Reading and exporting secure storage files are protected with the secure storage PIN, **see Chapter 2**. **Fig.**

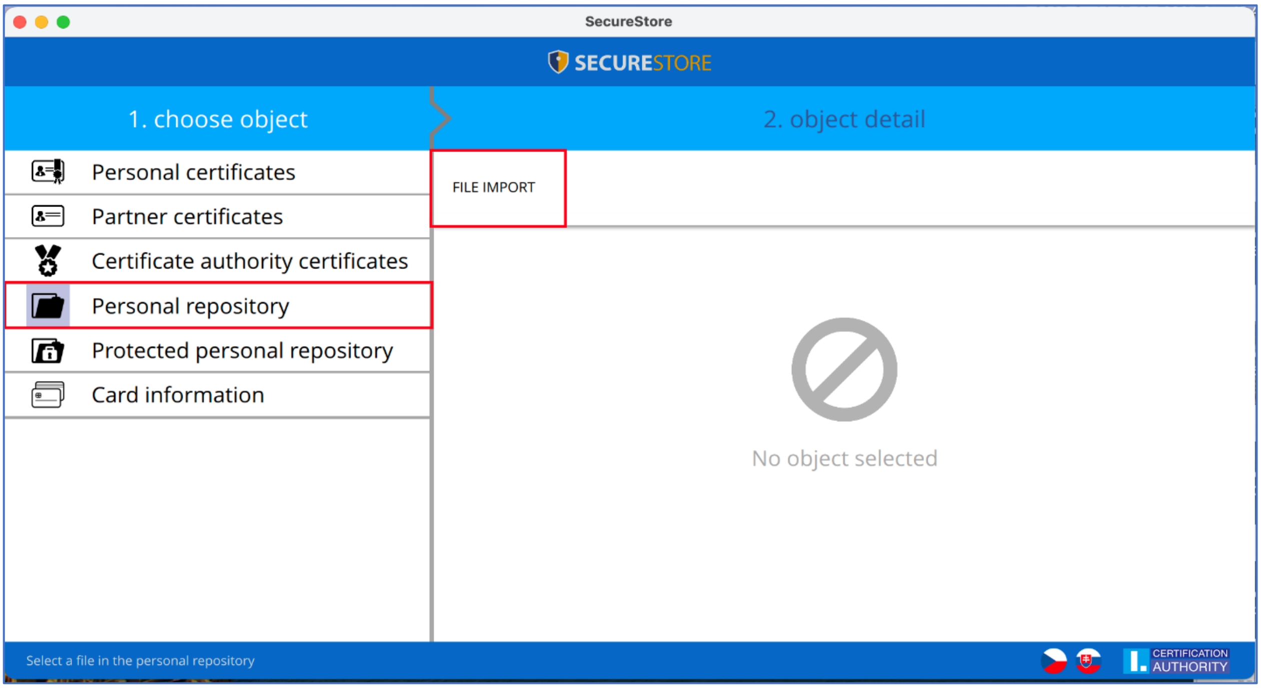
Fig. 27 – Personal repository



Select a file in the personal repository

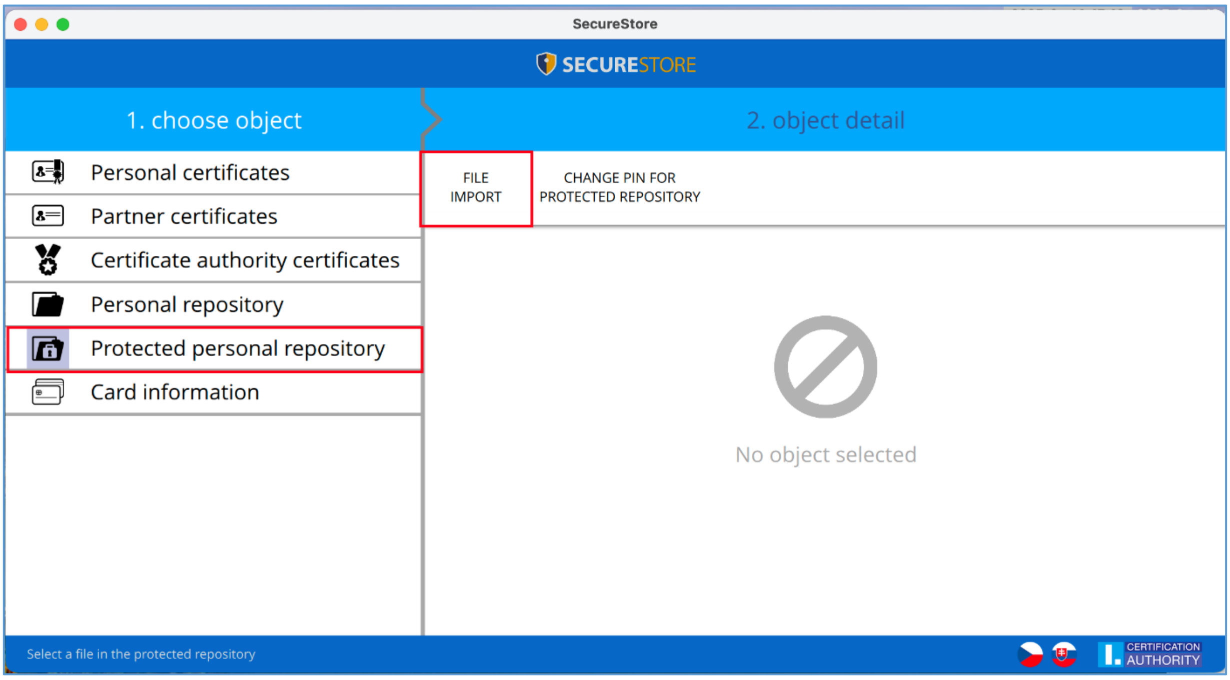
The function can be found in the **"Personal repository** object and in the "**File import" object detail**.

Fig. 28 - Importing a file into personal repository



The user can find the function in the **"Protected Personal Repository"** object and in the detail of the **"File import"**

Fig. 29 - Importing a file into a secure repository

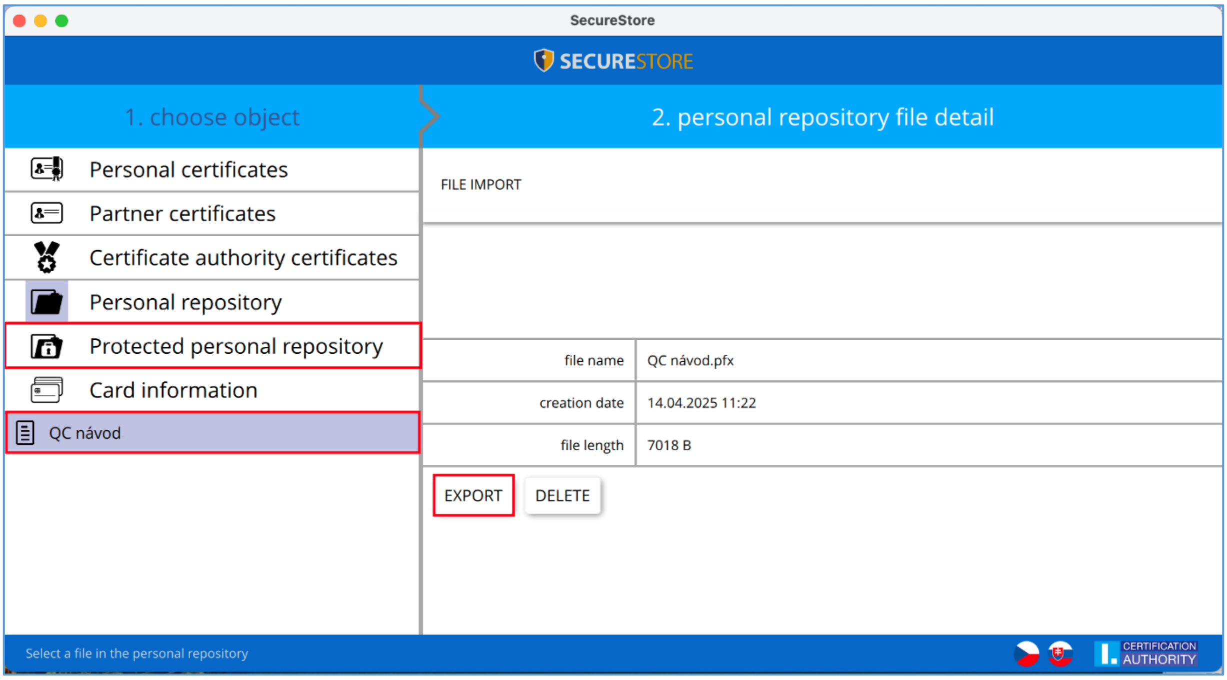


Select a file in the protected repository

The user can find the function in the **"Personal Repository"** object, after selecting the file to export in the **"Personal Repository File Detail"**, he will click the **"Export"** button.

In order to delete a file in the protected repository, a PIN is required.

Fig. 30 - Exporting a file from a personal repository



file name	QC návod.pfx
creation date	14.04.2025 11:22
file length	7018 B

Select a file in the personal repository

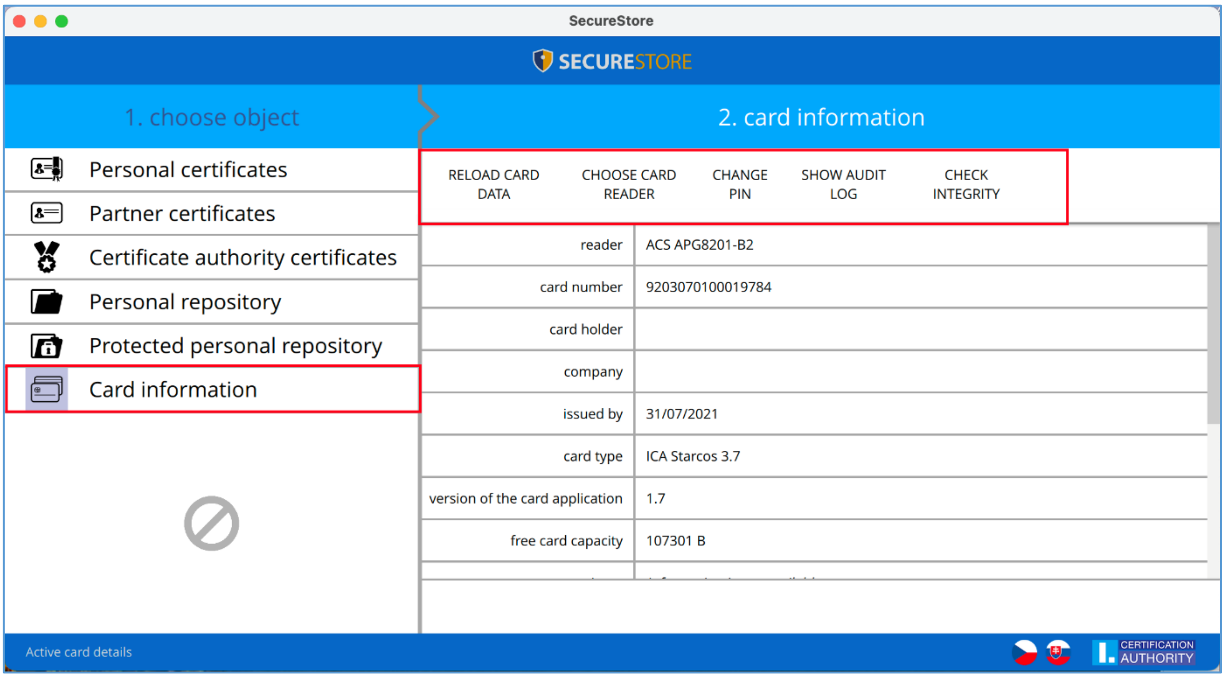
7. Application control

Individual functions of the application are implemented using the toolbar. The toolbar is displayed by clicking on the appropriate object on the left side of the application screen.

7.1 Card Information toolbar

The toolbar of the **"Card Information" object** contains basic administration operations with the card related to PIN and PUK management and repeated loading of data from the card.

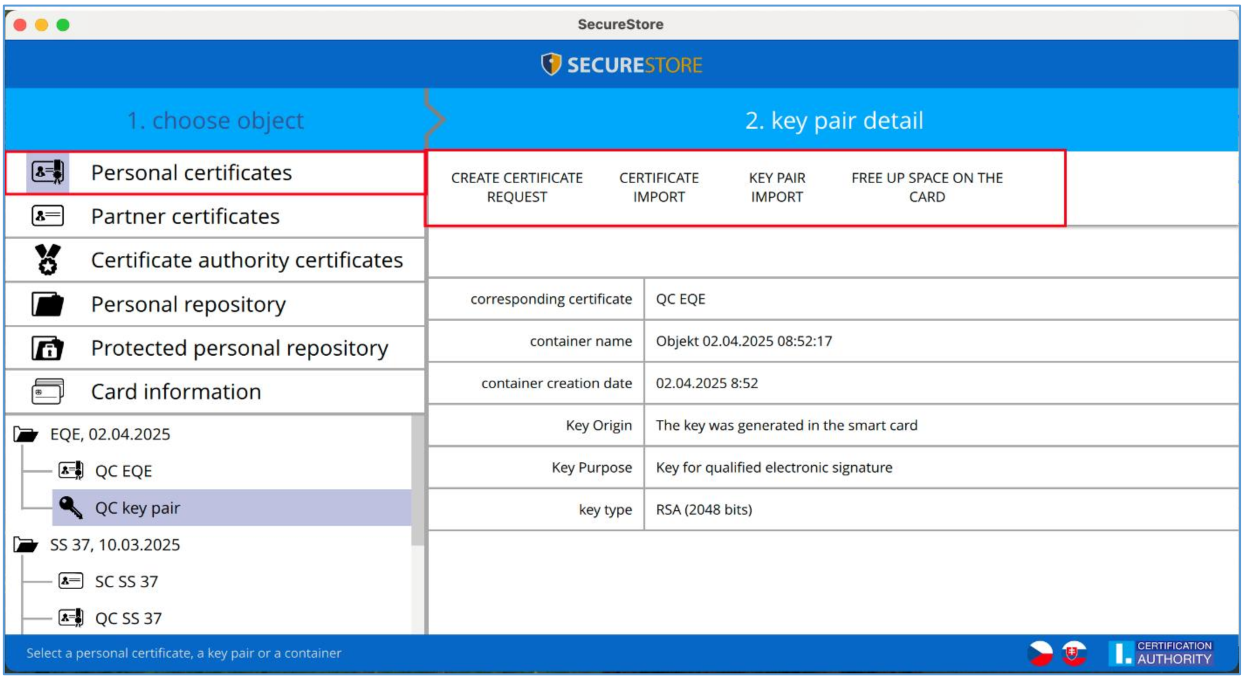
Fig. 31 – Toolbar for the "Card Information" object



reader	ACS APG8201-B2
card number	9203070100019784
card holder	
company	
issued by	31/07/2021
card type	ICA Starcos 3.7
version of the card application	1.7
free card capacity	107301 B

7.2 Toolbar for Personal certificates folder

Fig. 32 - Toolbar for the "Personal certificates" object



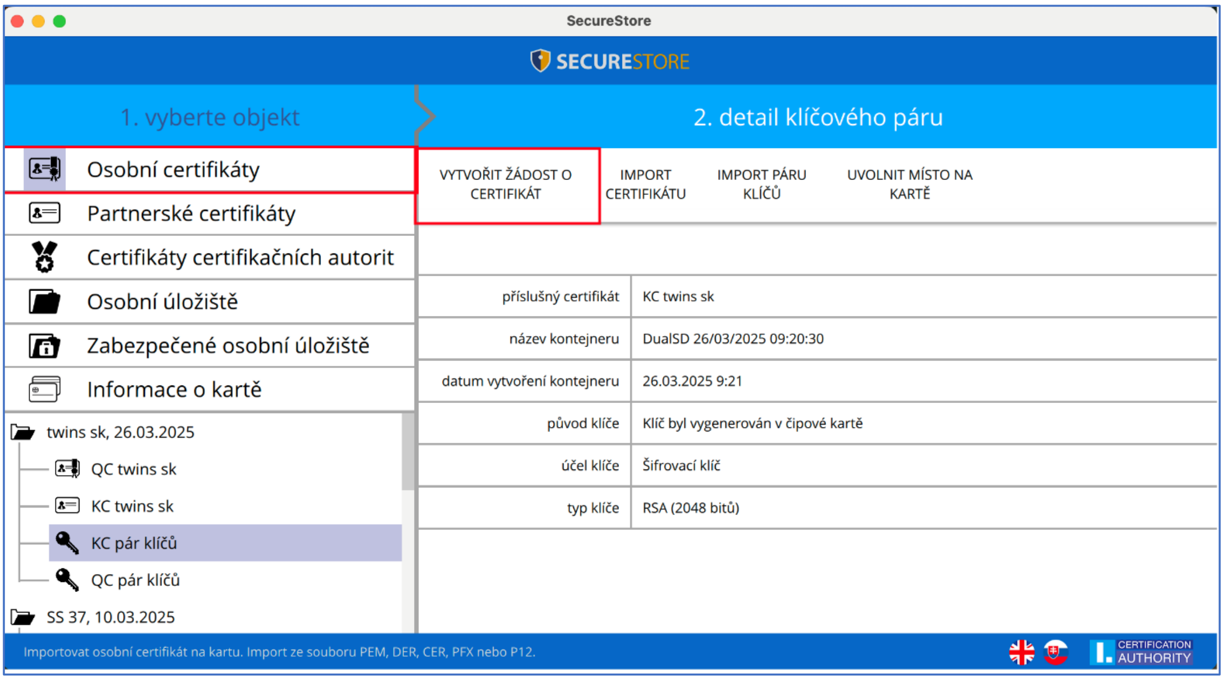
corresponding certificate	QC EQE
container name	Objekt 02.04.2025 08:52:17
container creation date	02.04.2025 8:52
Key Origin	The key was generated in the smart card
Key Purpose	Key for qualified electronic signature
key type	RSA (2048 bits)

Select a personal certificate, a key pair or a container

7.2.1 Create a Certificate Request

The “**Create certificate request**” option will redirect the user to the I.CA website, where they select the desired type of the certificate request to generate a key pair using the on-line generator.

Fig. 33 - Selecting the type of request for generating a key pair using the online generator

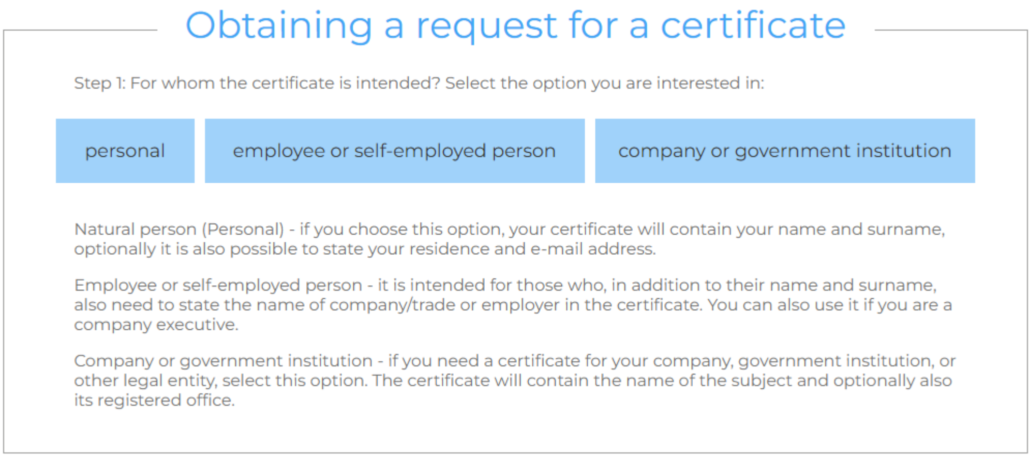


příslušný certifikát	KC twins sk
název kontejneru	DualSD 26/03/2025 09:20:30
datum vytvoření kontejneru	26.03.2025 9:21
původ klíče	Klíč byl vygenerován v čipové kartě
účel klíče	Šifrovací klíč
typ klíče	RSA (2048 bitů)

Importovat osobní certifikát na kartu. Import ze souboru PEM, DER, CER, PFX nebo P12.

After selecting the type of applicant and requesting a certificate, the user will be redirected to the I.CA on-line generator, where it is necessary to pass a system test (have the necessary components installed to run the online generator).

Fig. 34 - Selection of the type of certificate applicant


personal
employee or self-employed person
company or government institution

Obtaining a request for a certificate

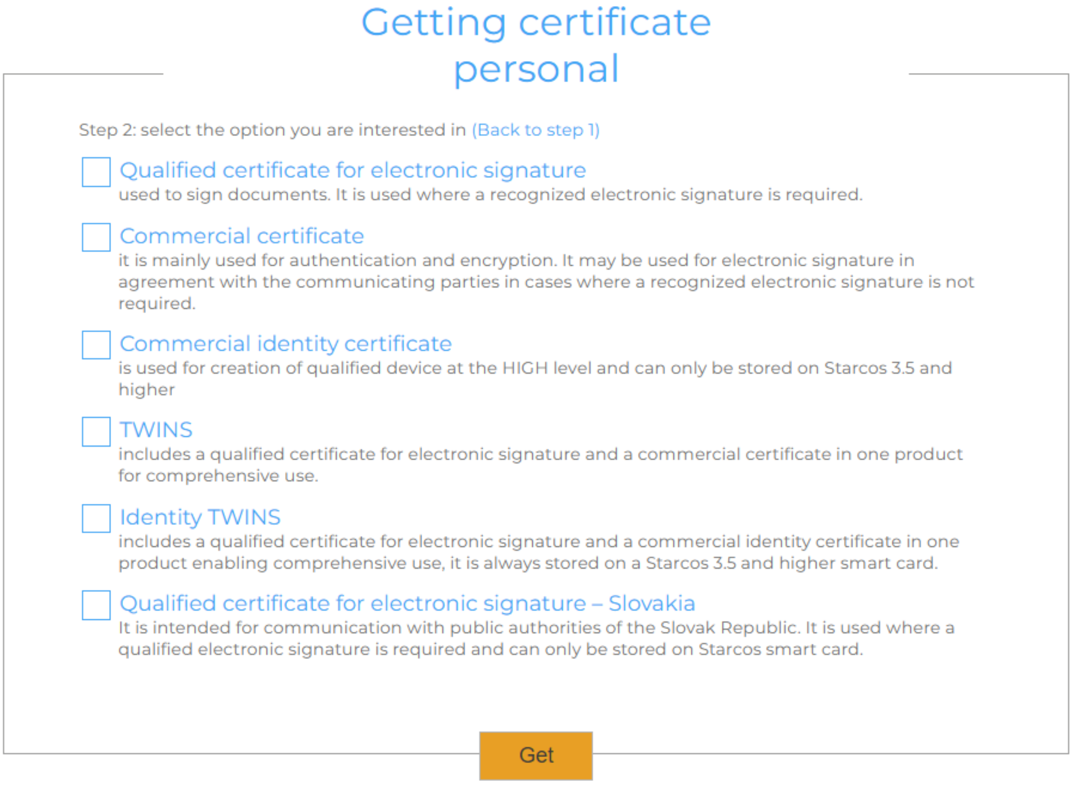
Step 1: For whom the certificate is intended? Select the option you are interested in:

Natural person (Personal) - if you choose this option, your certificate will contain your name and surname, optionally it is also possible to state your residence and e-mail address.

Employee or self-employed person - it is intended for those who, in addition to their name and surname, also need to state the name of company/trade or employer in the certificate. You can also use it if you are a company executive.

Company or government institution - if you need a certificate for your company, government institution, or other legal entity, select this option. The certificate will contain the name of the subject and optionally also its registered office.

Fig. 35 - Selection of the type of certificate request



Getting certificate personal

Step 2: select the option you are interested in (Back to step 1)

□ Qualified certificate for electronic signature
used to sign documents. It is used where a recognized electronic signature is required.

□ Commercial certificate
it is mainly used for authentication and encryption. It may be used for electronic signature in agreement with the communicating parties in cases where a recognized electronic signature is not required.

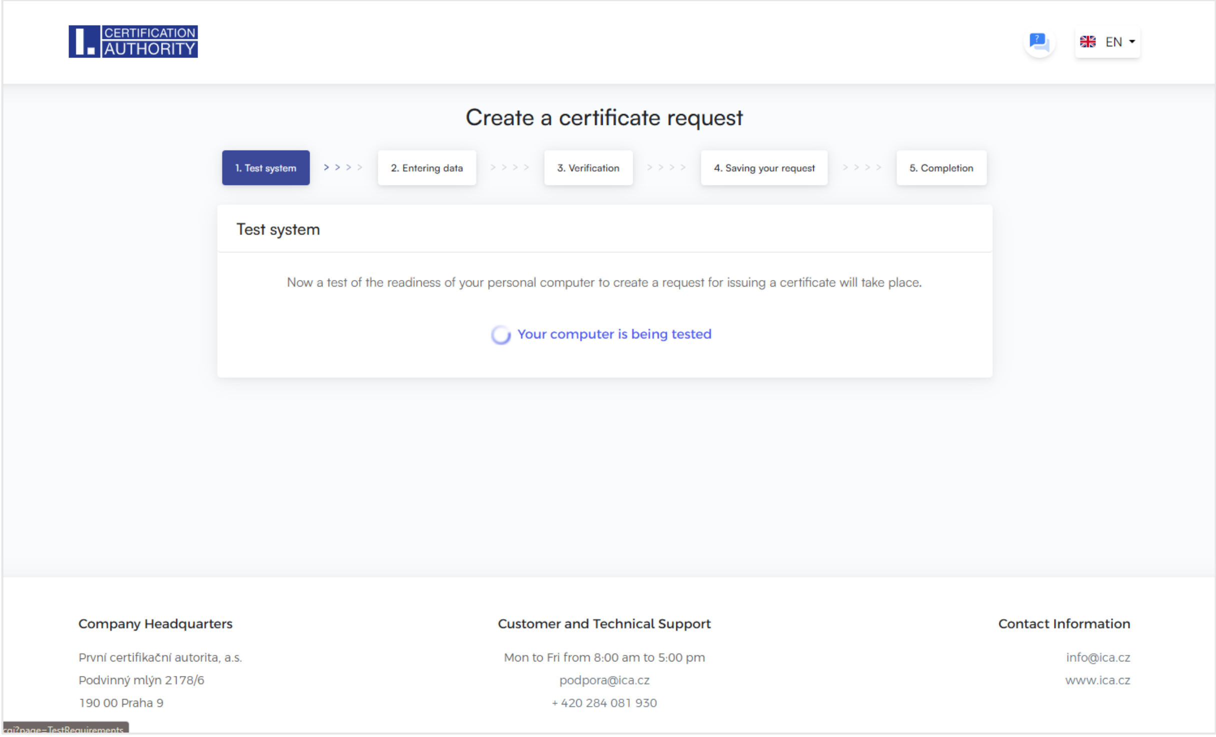
□ Commercial identity certificate
is used for creation of qualified device at the HIGH level and can only be stored on Starcos 3.5 and higher

□ TWINS
includes a qualified certificate for electronic signature and a commercial certificate in one product for comprehensive use.

□ Identity TWINS
includes a qualified certificate for electronic signature and a commercial identity certificate in one product enabling comprehensive use, it is always stored on a Starcos 3.5 and higher smart card.

□ Qualified certificate for electronic signature – Slovakia
It is intended for communication with public authorities of the Slovak Republic. It is used where a qualified electronic signature is required and can only be stored on Starcos smart card.

Fig. 36 - 1. Test system



Create a certificate request

Test system

Now a test of the readiness of your personal computer to create a request for issuing a certificate will take place.

Your computer is being tested

Company Headquarters

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

Customer and Technical Support

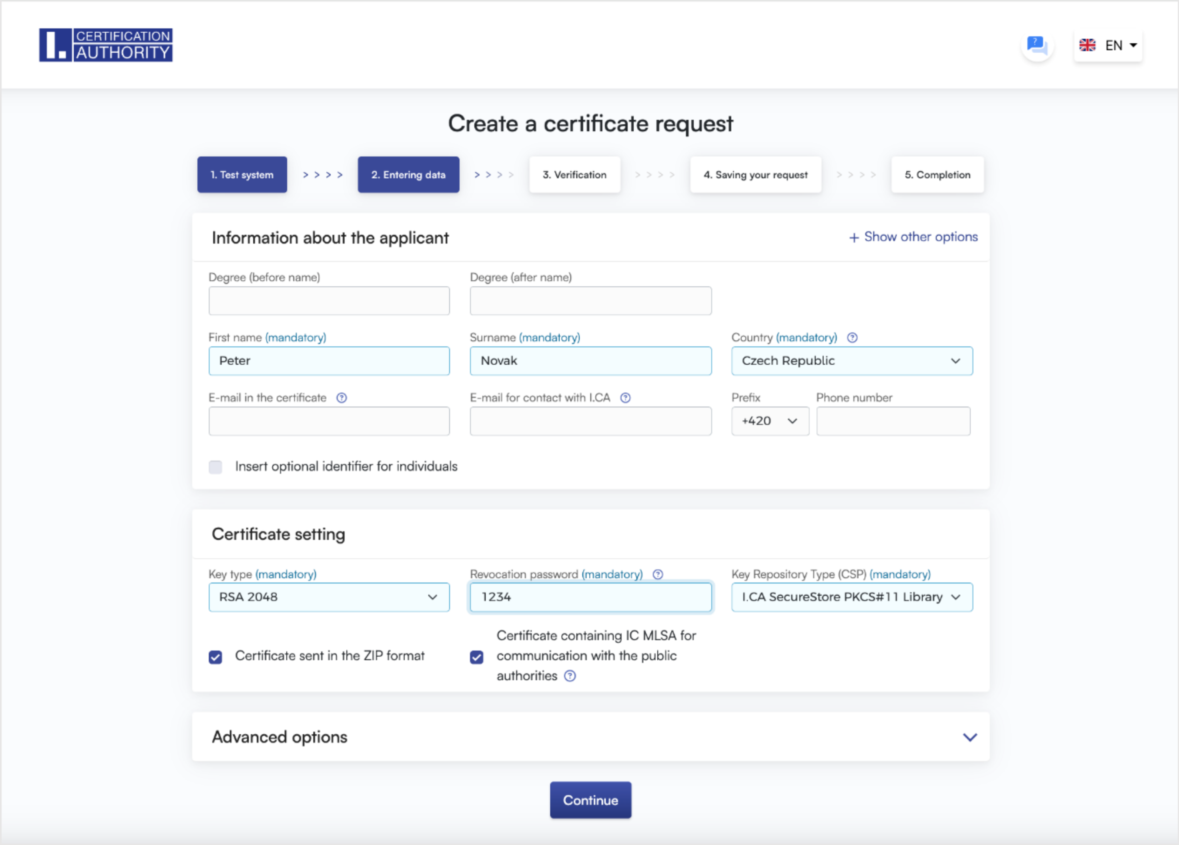
Mon to Fri from 8:00 am to 5:00 pm
podpora@ica.cz
+ 420 284 081 930

Contact Information

info@ica.cz
www.ica.cz

cgi?page=TestRequirements

Fig. 37–2. Entering data



Create a certificate request

Information about the applicant

Degree (before name):
Degree (after name):
First name (mandatory): Peter
Surname (mandatory): Novak
Country (mandatory): Czech Republic
E-mail in the certificate:
E-mail for contact with I.CA:
Prefix: +420
Phone number:

□ Insert optional identifier for individuals

Certificate setting

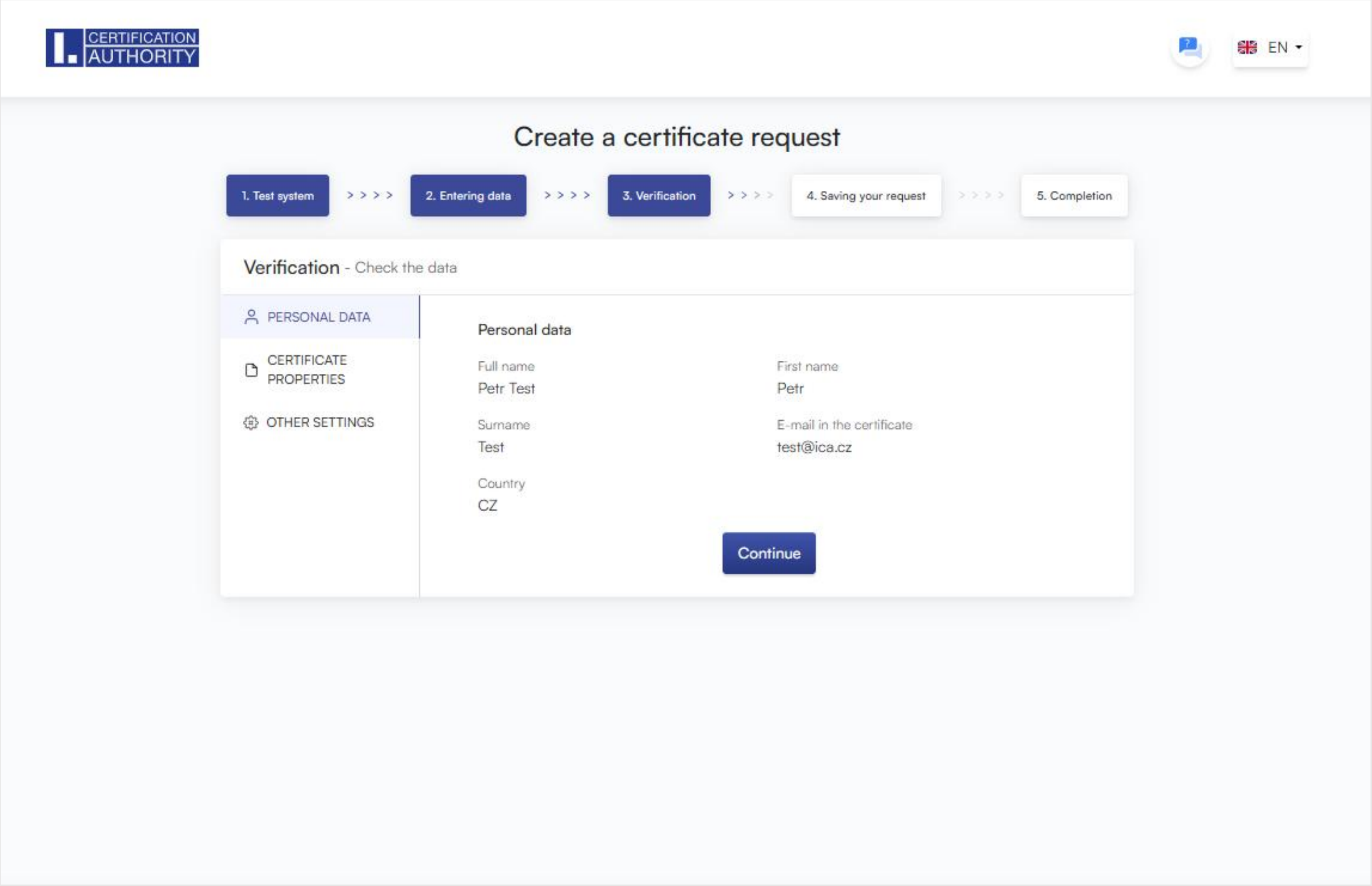
Key type (mandatory): RSA 2048
Revocation password (mandatory): 1234
Key Repository Type (CSP) (mandatory): I.CA SecureStore PKCS#11 Library

☑ Certificate sent in the ZIP format

☑ Certificate containing IC MLSA for communication with the public authorities

Advanced options

Fig. 38–3. Verification



Create a certificate request

Verification - Check the data

Personal data

Full name
Petr Test

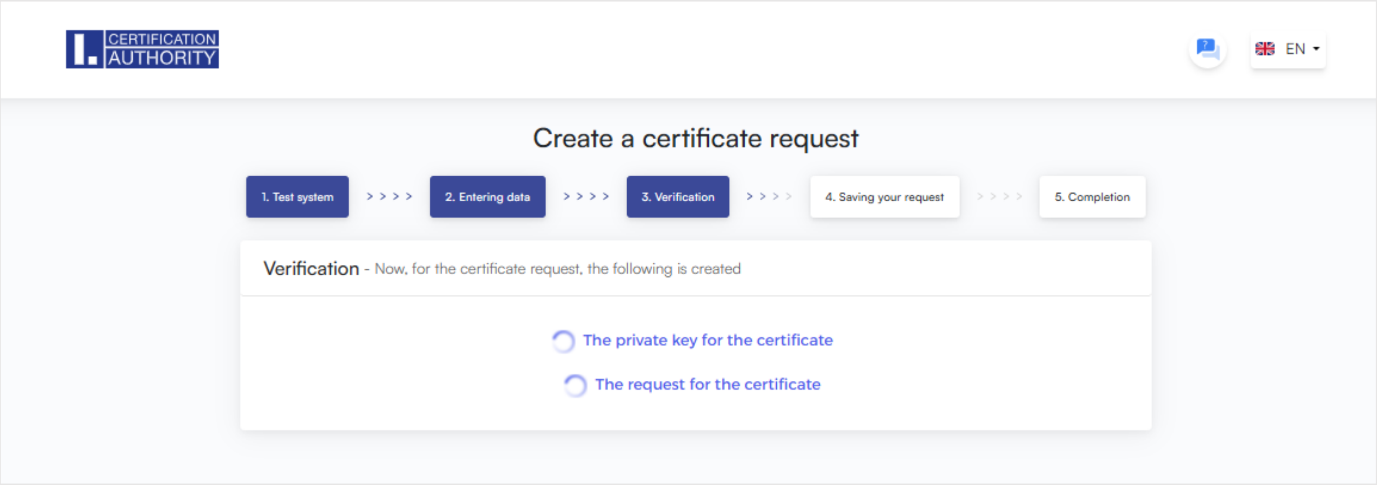
First name
Petr

Surname
Test

E-mail in the certificate
test@ica.cz

Country
CZ

Fig. 39 – Generating a private key



Create a certificate request

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

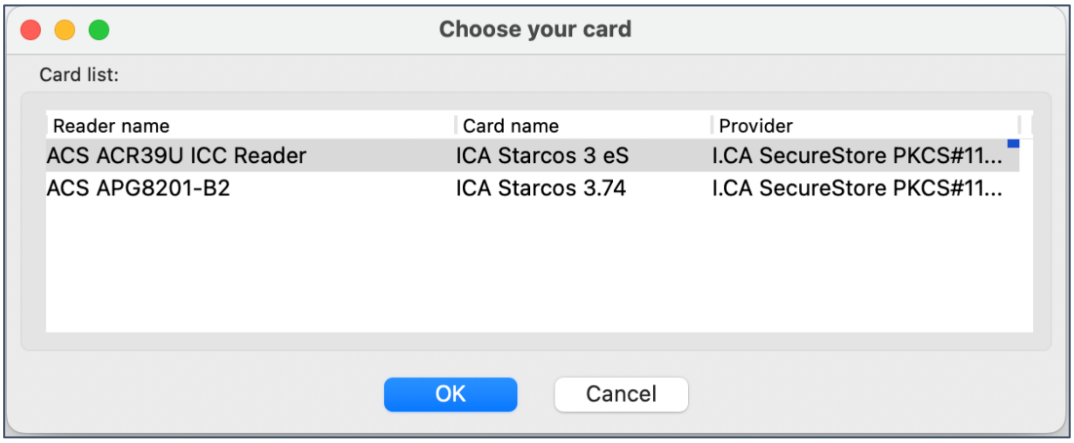
Verification - Now, for the certificate request, the following is created

The private key for the certificate

The request for the certificate

If the user has more than one smart card connected to the PC, the user selects in the dialog box which key pair should be generated. After selecting the smart card, the system prompts the user to enter the PIN.

Fig. 40 – Selecting a smart card reader

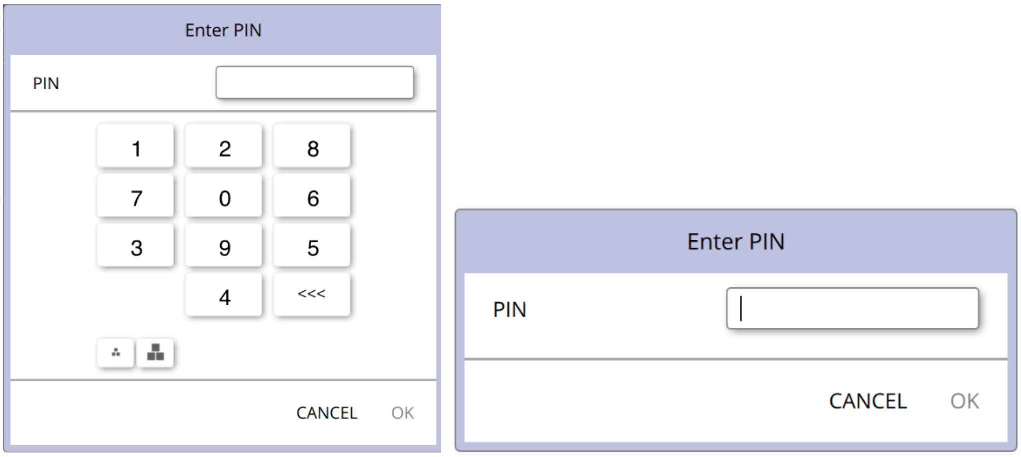


Choose your card

Card list:

Reader name	Card name	Provider
ACS ACR39U ICC Reader	ICA Starcos 3 eS	I.CA SecureStore PKCS#11...
ACS APG8201-B2	ICA Starcos 3.74	I.CA SecureStore PKCS#11...

Fig. 41 - Entering the PIN to generate the key pair and signing the request



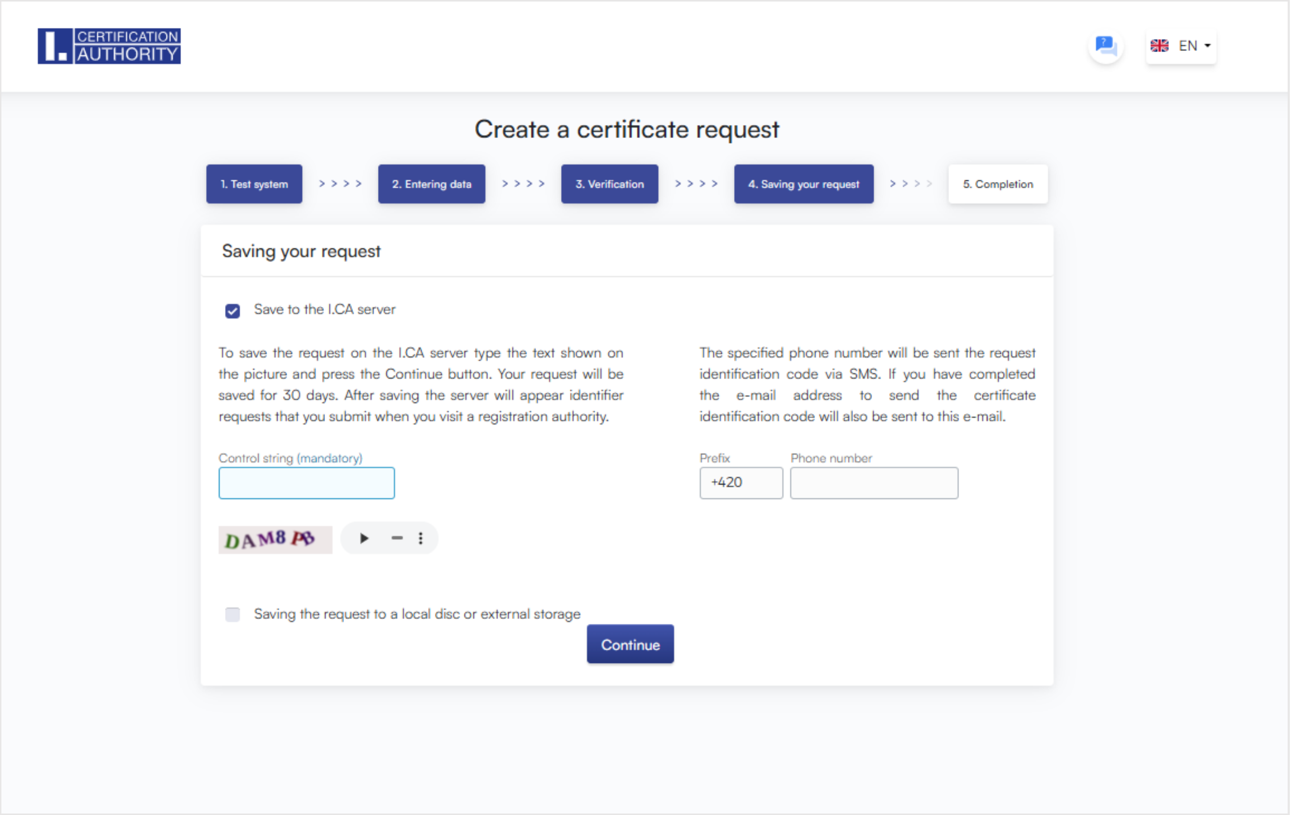
Enter PIN

PIN

Enter PIN

PIN

Fig. 42–4. Saving your request



Create a certificate request

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

Saving your request

☑ Save to the I.CA server

To save the request on the I.CA server type the text shown on the picture and press the Continue button. Your request will be saved for 30 days. After saving the server will appear identifier requests that you submit when you visit a registration authority.

The specified phone number will be sent the request identification code via SMS. If you have completed the e-mail address to send the certificate identification code will also be sent to this e-mail.

Control string (mandatory)

Prefix: +420

Phone number

□ Saving the request to a local disc or external storage

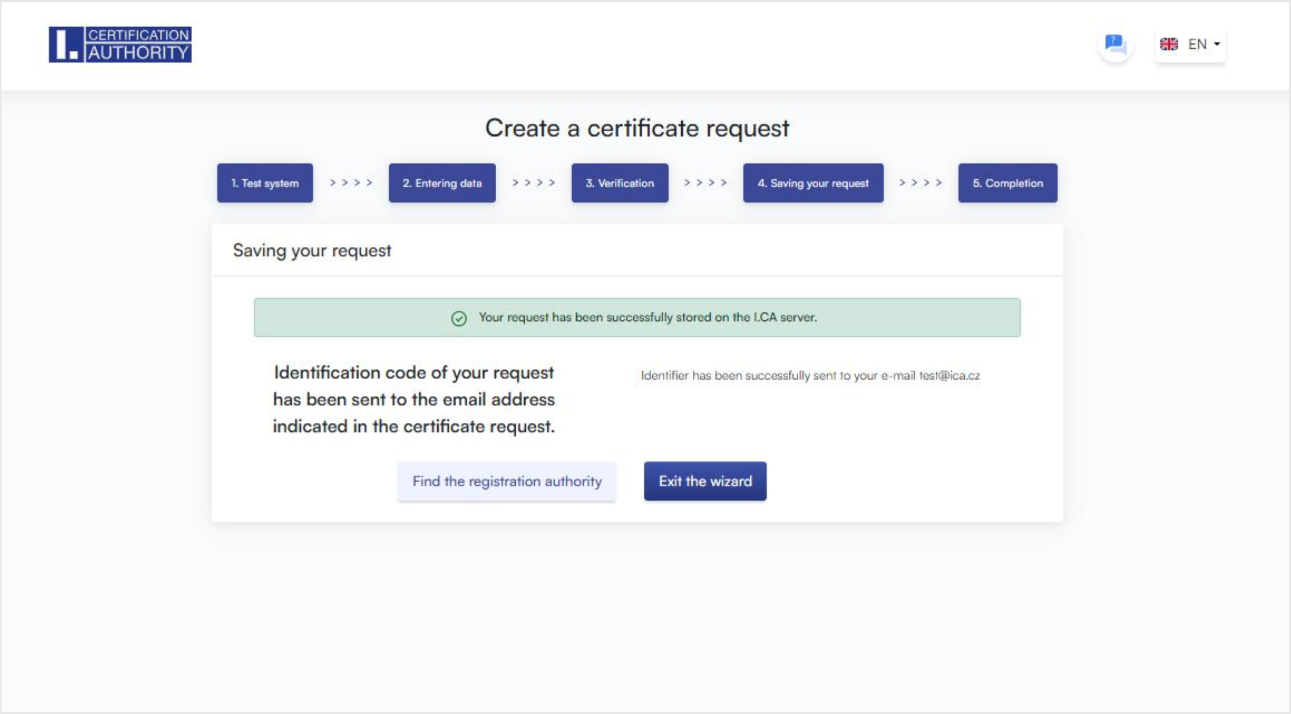
Continue

Choosing a way to save a certificate request.

When choosing **"Save to I.CA server"**, a six-digit numeric code of the saved request on the I.CA server will be sent to the user's contact e-mail specified in the certificate request.

When **"Saving the request to loca disc or external storage"** is selected, a file with the generated request called cert****.req is saved.

With a six-digit numeric code to the stored request on the I.CA server or with a req file. on the portable USB media, the user then visits the registration authority, which can be searched for by the " **Search registration authority" button.**



Create a certificate request

Saving your request

Your request has been successfully stored on the I.CA server.

Identification code of your request has been sent to the email address indicated in the certificate request.

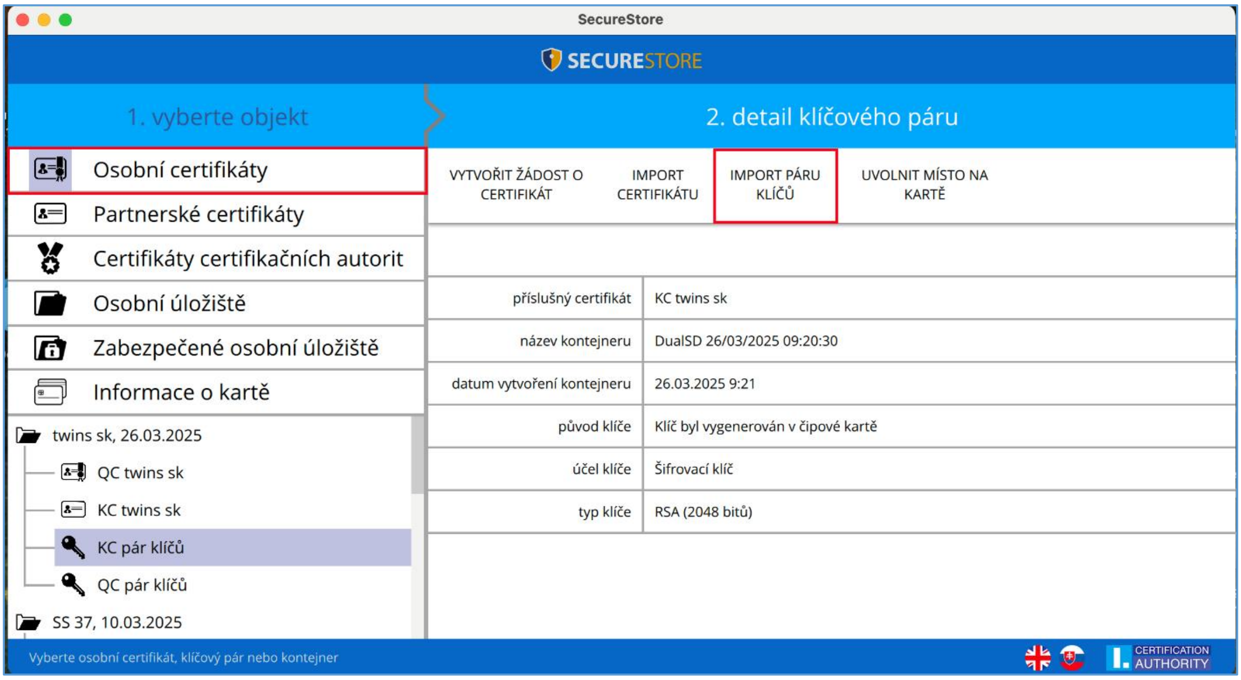
Identifier has been successfully sent to your e-mail test@ica.cz

Fig. 43–5. Completion

7.2.2 Importing a key pair from a backup and importing keys

This option imports keys to the smart card that were stored on disk during the encryption certificate request generation process. The function can be found in the **"Personal certificates"** object. In the same way, you can import keys with a certificate to a smart card that are stored in PKCS#12 format on disk.

Fig. 44 – Importing a key pair from a backup and a key pair



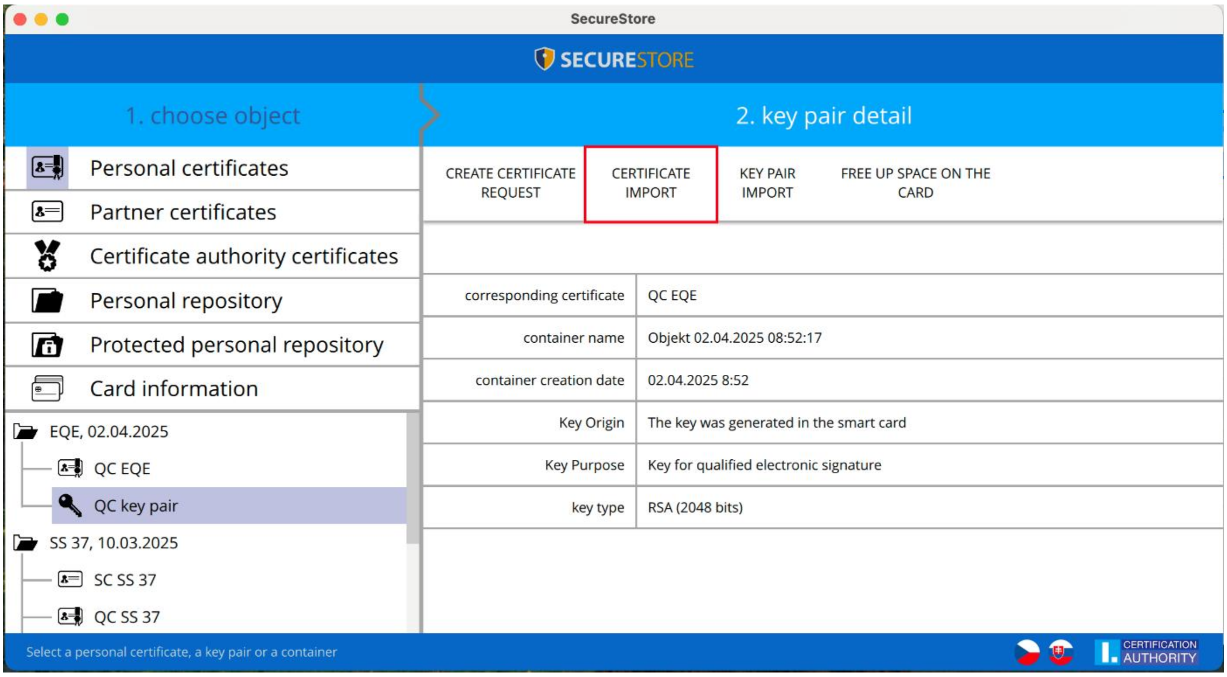
příslušný certifikát	KC twins sk
název kontejneru	DualSD 26/03/2025 09:20:30
datum vytvoření kontejneru	26.03.2025 9:21
původ klíče	Klíč byl vygenerován v čipové kartě
účel klíče	Šifrovací klíč
typ klíče	RSA (2048 bitů)

Vyberte osobní certifikát, klíčový pár nebo kontejner

The imported certificate is stored in a store on the smart card that contains the keys to the certificate.

If there is no storage on the smart card that contains the appropriate keys, the certificate is stored in the "Partner Certificates" section of the card.

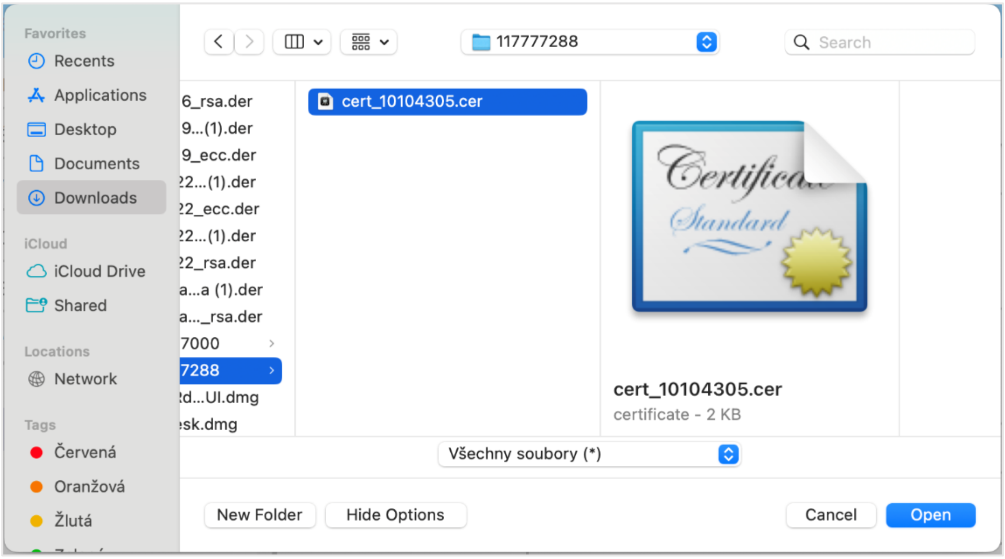
Fig. 45 - Importing a certificate



corresponding certificate	QC EQE
container name	Objekt 02.04.2025 08:52:17
container creation date	02.04.2025 8:52
Key Origin	The key was generated in the smart card
Key Purpose	Key for qualified electronic signature
key type	RSA (2048 bits)

Select a personal certificate, a key pair or a container

Selecting the certificate file to import into the card



cert_10104305.cer
certificate - 2 KB

Všechny soubory (*)

8. Definitions

- **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 contact workplace 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 applicant's 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 operations** – operations using a key to encrypt and decrypt. Asymmetric cryptography is used for the smart 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.

- **Data for creating an electronic signature**- 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 relevant asymmetric cryptographic algorithm (RSA in this instance).

- **Smart card** - a device providing secure storage of the user's private key and allowing the user to create electronic signature. The smart 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 belongs to a specific card and contains the card's unique identification and PIN and PUK values. Some cards may be supplied without a PIN envelope.

- **Repository** – memory space on a medium, such as disk or smart card, where the key pair and the certificate are saved. A single smart card may have as many as 8 different storage compartments at a time. The smart card repository has its unique name. SIGNATURE type storage does not permit creating key backups when generating a certification request. Any certificate for which keys are backed up thus must be saved in OTHER storage.

- **Certification request** – is completed by filling a form with applicant data. The applicant's public key is attached to the information filled in the request form and all this structure is signed with the applicant's private key. Certification request is digital data that include all the data required for the certificate to be issued

- **Certificate** – proof of identity analogous to personal identity card, client uses his certificates to prove his 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 implement client's requests. A certificate is uniquely tied to a pair of keys, which the user uses in electronic communication. The key pair consists of the public key and the private key.

- **Public key** - the public part of the user's key pair, it is intended for electronic signature authentication and possibly for encryption.

- **Private key** - the secret part of the user's key pair, it is used for creating an electronic signature and possibly for decryption. Due to the use of a private key, the highest possible security must be provided for it. For this reason, a smart card is used to store the key. The private key used for decryption needs to be kept for the lifetime of the encrypted documents and messages. The user can store this key on the card and it is recommended to keep it on a backup medium at the same time.

- **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 stored in Windows) or the **Comfort** version (the private key is stored in the smart card).

- **Qualified certificate** – is strictly subject to EU Regulation 910/2014 and designed solely for electronic signatures. Creating, managing and using qualified certificates are governed by relevant certification policies. Qualified certificates are issued in the **Standard** version (the private key is stored in Windows) or the **Comfort** version (the private key is stored in the smart card).

- **Certification authority certificate** – is used to verify the correctness and trustworthiness of client certificates. By installing it on your PC, the user declares to the operating system his trust in such a certificate authority. In practice, this means that if the user receives a message that is electronically signed with a certificate issued by that particular certification authority, it is seen as trustworthy by the system. In other cases, the message appears to be untrusted.

- **List of public I.CA (commercial) certificates** - a list of certificates issued by I. CA, for which their owners have agreed to make them public. This does not include "test" certificates and certificates for which the owner has not agreed to disclose.
  The list of public commercial and qualified I.CA certificates can be found here:

  https://www.ica.cz/List-public-certificates

- **Certification authorities supported by the card** - each smart card issued by I.CA has a defined list of supported certification authorities whose certificates can be stored on the card.

- **Subsequent certificate** - is issued to the client on the basis of an electronic request sent during the validity of the initial certificate. A subsequent certificate is issued only if the client does not request to change the items of the previous certificate. If it is requested, it is not a subsequent certificate, but another initial one. When issuing a subsequent certificate before the expiry of the initial certificate, the presence of the client at the I.CA registration authority is no longer necessary. The client simply sends an electronically signed request for the issuance of a subsequent certificate in a standardized electronic form using a valid certificate.

- **Key usage**

  - **DigitalSignature (digital signature)** - This flag (bit) is primarily set if the certificate is to be used in connection with a digital signature, except for nonrepudiation, certificate signatures, and CA invalidated certificate lists. Usage: this bit is currently to be set in cases where the user intends to use his private key associated with the issued certificate for the creation of a digital signature in general (e.g. when using the certificate in secure e-mail).

  - **NonRepudiation** - this flag is set if the public key (through digital signature verification) is to be used to prove accountability for a particular action by the signer. Usage: this bit is currently to be set especially in cases of qualified certificates where the user intends to use his private key associated with the issued certificate to create an electronic signature.

  - **KeyEncipherment** - this flag shall be set if the public key is to be used to transmit cryptographic keys. Usage: this bit shall be set if the user intends to use the certificate for encryption purposes within secure electronic mail. In MS Outlook, this bit must also be set if the user does not have another certificate that can be used for encryption.

- The PKCS#12 format of the RSA keys and the certificate can be stored in a single file in the so-called PKCS#12 format, which is defined by the PKCS#12 standard. In this format, it is possible, for example, to export the RSA key certificate from Windows storage if private key export is enabled. The content of the file is password protected. The file has the extension pfx or p12.