I.CA SecureStore

User guide

Version 7.1.2 and higher

První certifikační autorita, a.s.

Version 7.18, 18.7.2024

Contents

1. Introduction

This User guide applies to the application I.CA SecureStore, Version 7.1.2 and higher. The specified versions have the same function and identical user interface.

2. Card access data

STARCOS 3.0

Smart 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 smart card.

STARCOS 3.5

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 6–8 digits. Entering a wrong PUK 5 times in a row will disable the PUK and thus also the smart card. **Re-enabling PIN using PUK is limited to 6 attempts.**

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. **Re-enabling PIN using PUK is limited to 10 attempts.**

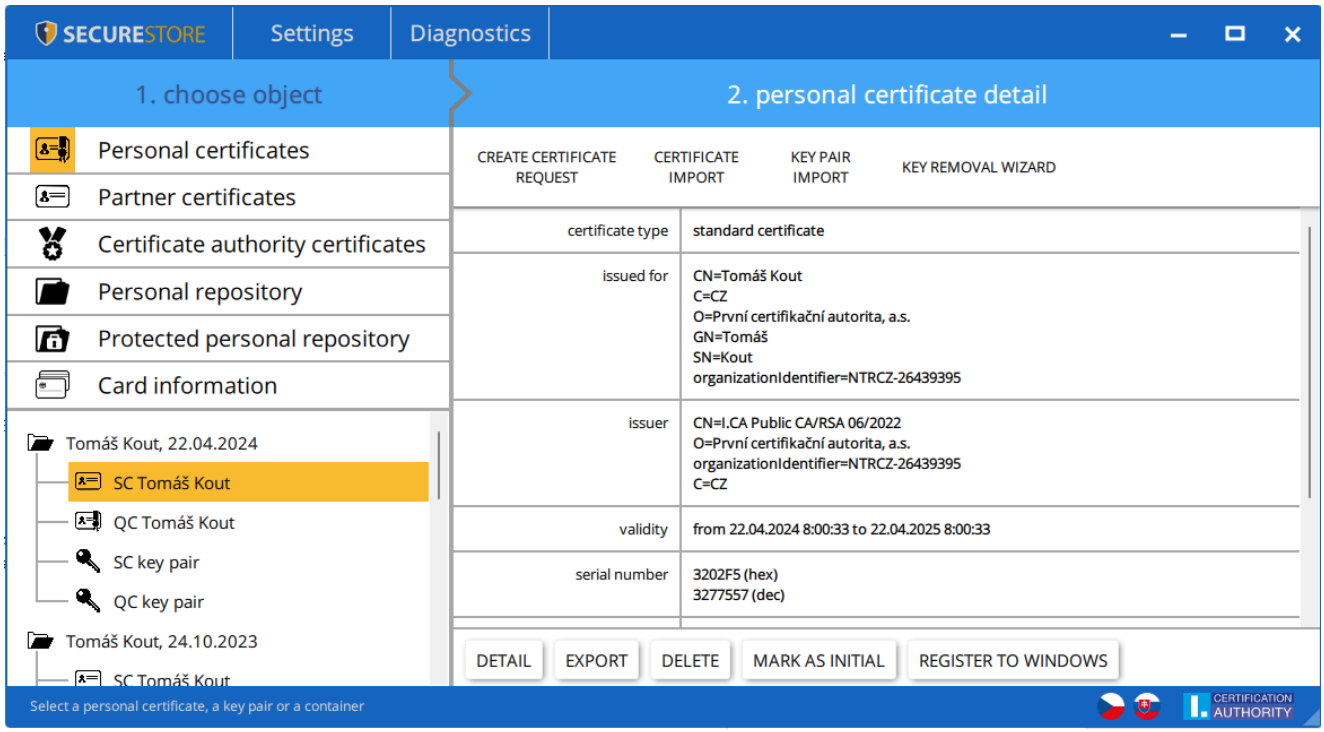
The card's segment named Secure Personal Storage is designed for storing any kind of data. This segment is protected with a special PIN, a secure storage PIN. Use the PUK referred to in the previous paragraph to re-enable the secure storage PIN. The secure storage PIN is a number of 6–8 digits.

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 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 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



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. 2.

3.1 Switching between application languages

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

Fig. 2 – switching the language

Fig. 3 – Main bar

3.2 Version of the I.CA SecureStore

Click to display the application's version.

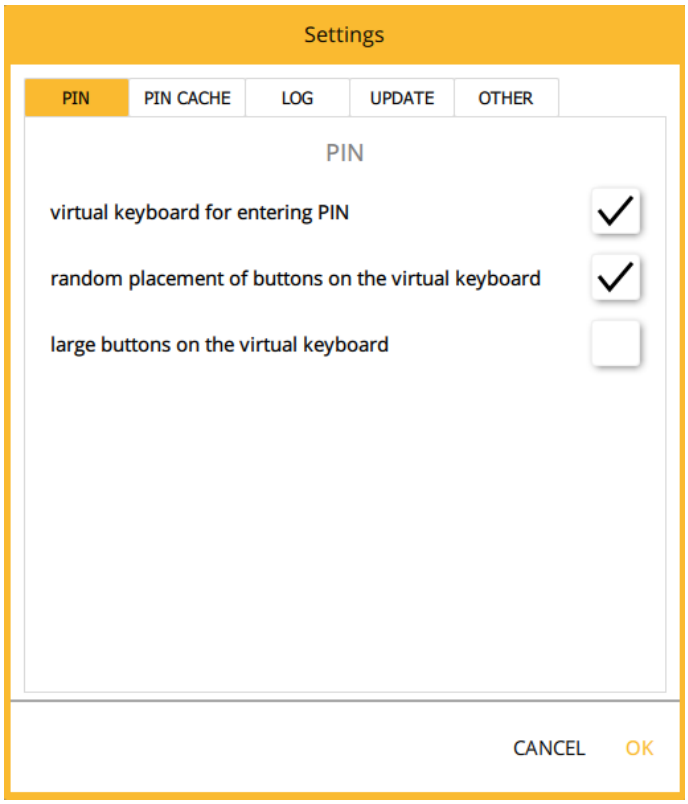
Fig. 4 – Application version

3.3 Settings

Use the Settings option to:

1) Adjust the keypad for entering PIN

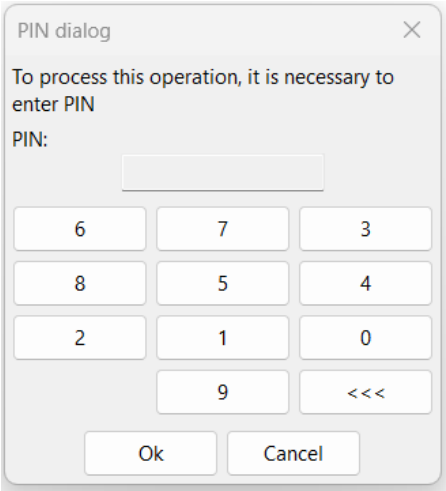
Fig. 5 – PIN Keypad



By default, the application is set to **"Random button placement on virtual keyboard for PIN".**

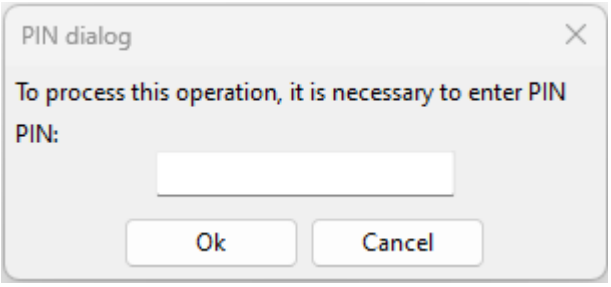
The user then enters the PIN on the virtual keyboard with the mouse cursor.

Fig. 6 - Keyboard for PIN entry.



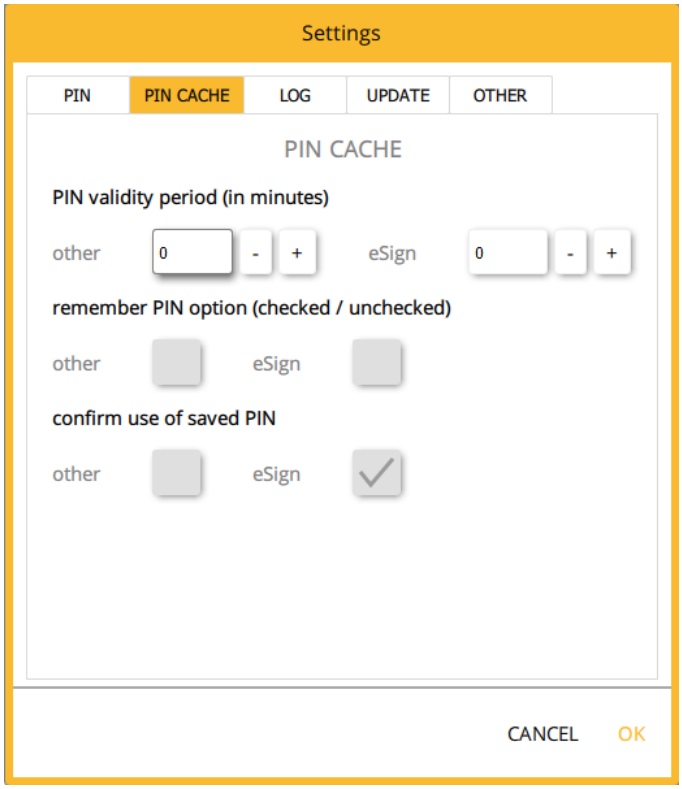
The PIN keypad can be set to "Virtual PIN keypad", where the user can then enters the PIN on the numeric keypad.

Fig. 7 - PIN entry keypad



2) PIN CACHE - the time the PIN is stored in memory, by default the value is set to 0.

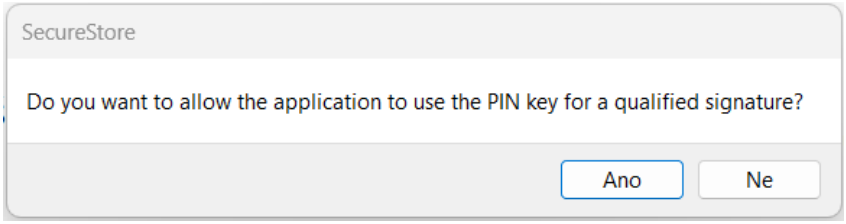
Fig. 8 - PIN memorization settings



a) **PIN storage time** (in minutes) - setting the PIN storage time
b) **The option to remember the PIN** (selected/not selected) - the user can select a time period, for which the user wants to remember the PIN, the setting is separately for:
   a. Other - encryption and authentication keys
   b. eSign - signature keys

Note: The maximum time to remember the PIN for signature keys in eSign is 30 min, for encryption keys there is no time limit. Furthermore, the application allows PIN memorization in relation to the application process.

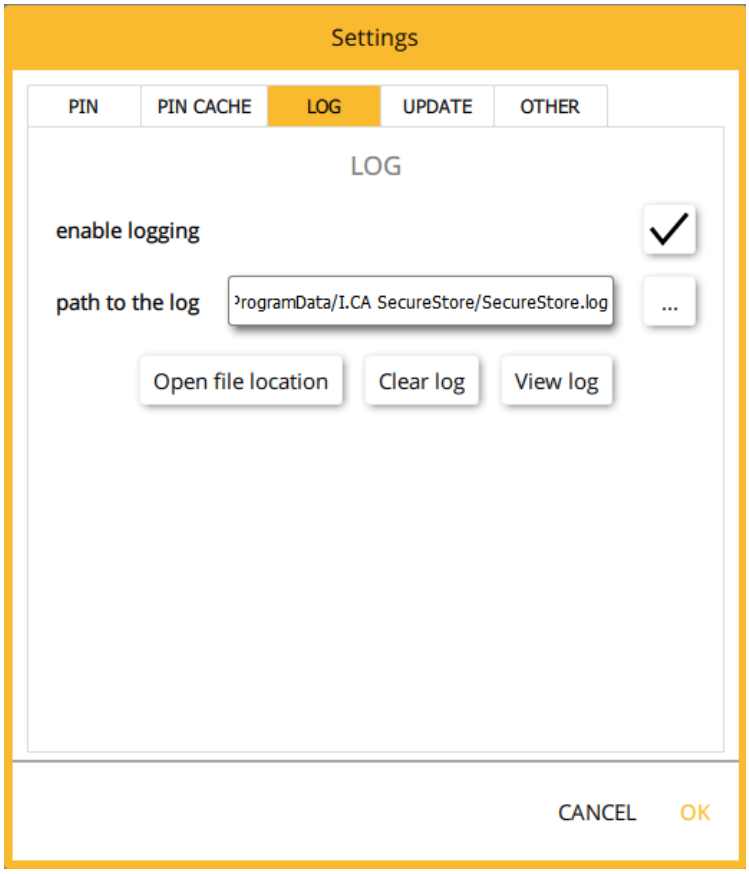
c) **Confirm the use of the stored PIN** - a function that allows you to activate the confirmation dialog that appears when the PIN is memorized and a key signature is created on the smart card. In this case, the user will be prompted whether he/she agrees to the use of the key and the creation of the signature
d) **Fig. 9 - Confirmation dialogue**



3) **Enable logging** - enable application logging, for possible analysis of technical problem when using the smart card and the application. The application records the so-called audit log, when the latest audit log will be recorded in the audit log as part of the smart card operations. Security-sensitive operations performed, such as key deletion, key generation, etc.

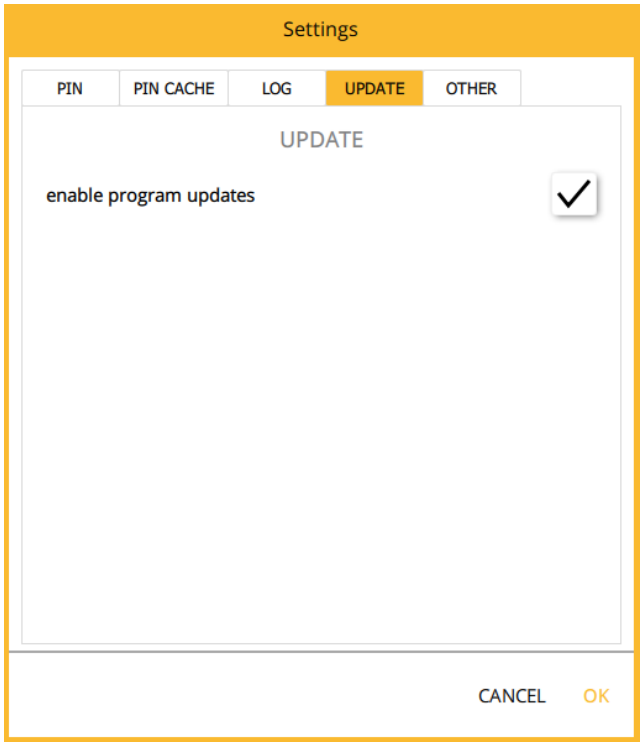
The user can change the path to the saved log file using the button ... .

Fig. 10 – Log



4) **Updates** - the settings can be used to enable/disable online updating of the application. If a new version is released, the user is informed about the new version whenever the application is launched.

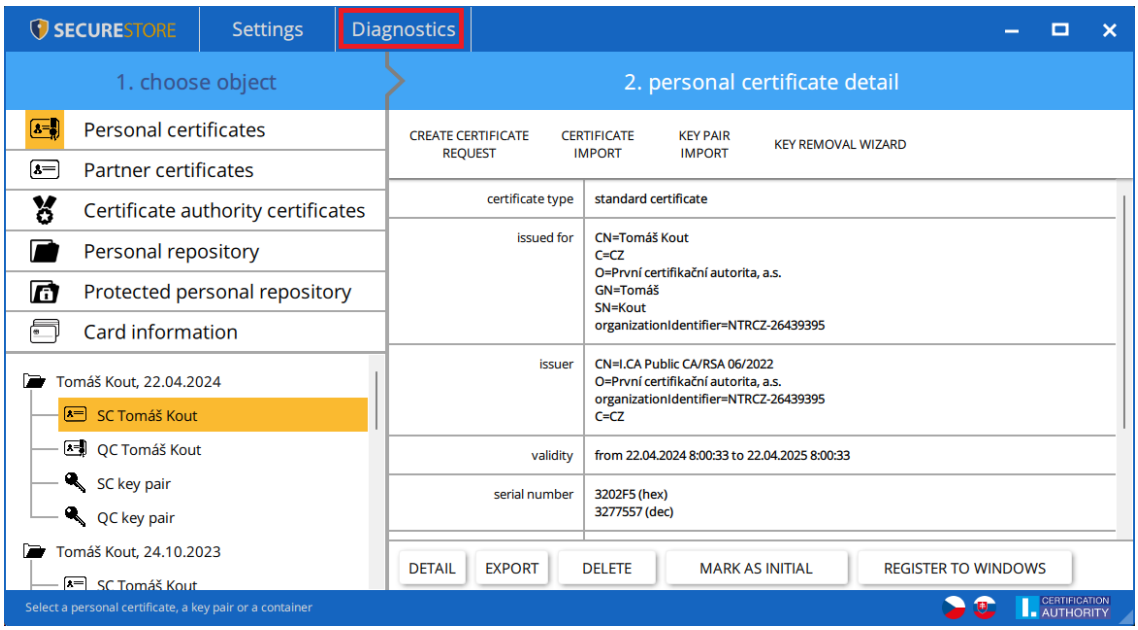
Fig. 11 - Application update settings



3.4 Diagnostic Tools

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

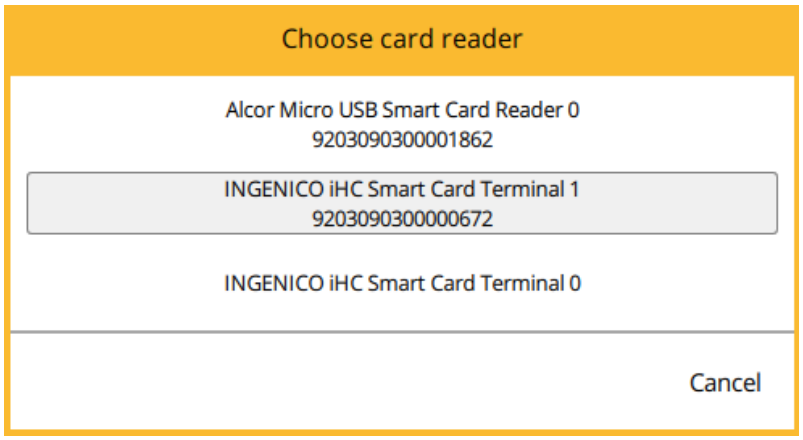
Fig. 12 – Diagnostic Tools



3.5 Selecting smart card reader

If the user has more than one smart card reader connected to the PC, the "Select smart card readers" window even after the application is started.

Fig. 13 - Selecting a smart card reader

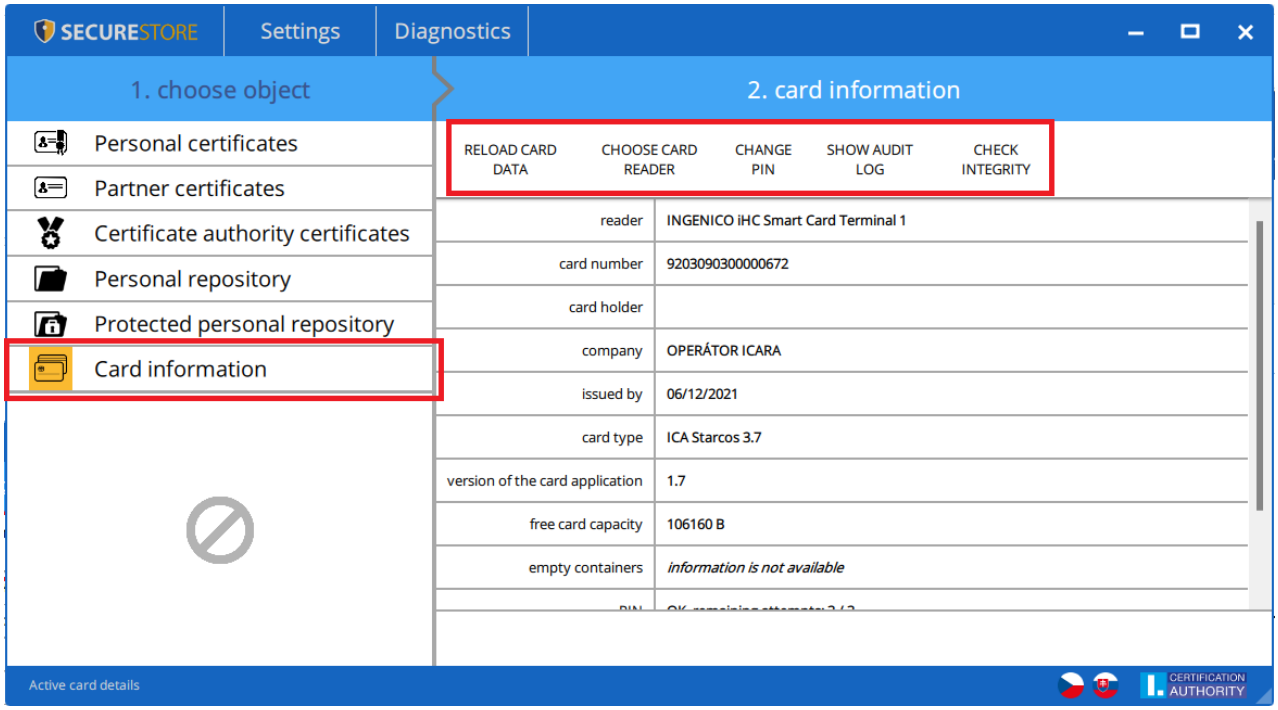


If the user has only one smart card reader connected to the PC, the window is not displayed.

3.6 Toolbar

In the toolbar, see Fig. 14, the options change according to the selected object in the left part of the screen.

Fig. 14 – Toolbar



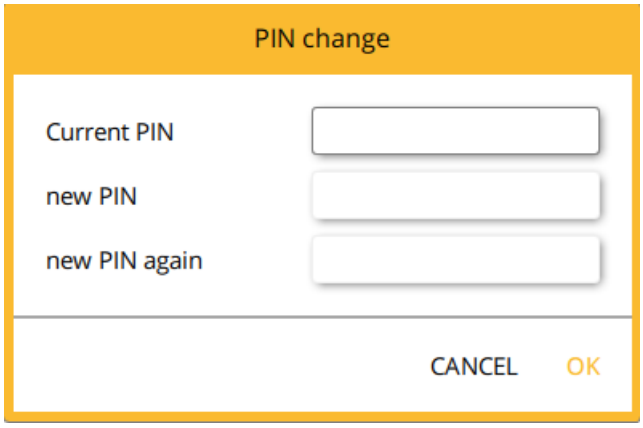
3.7 Changing PIN

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 – Changing PIN



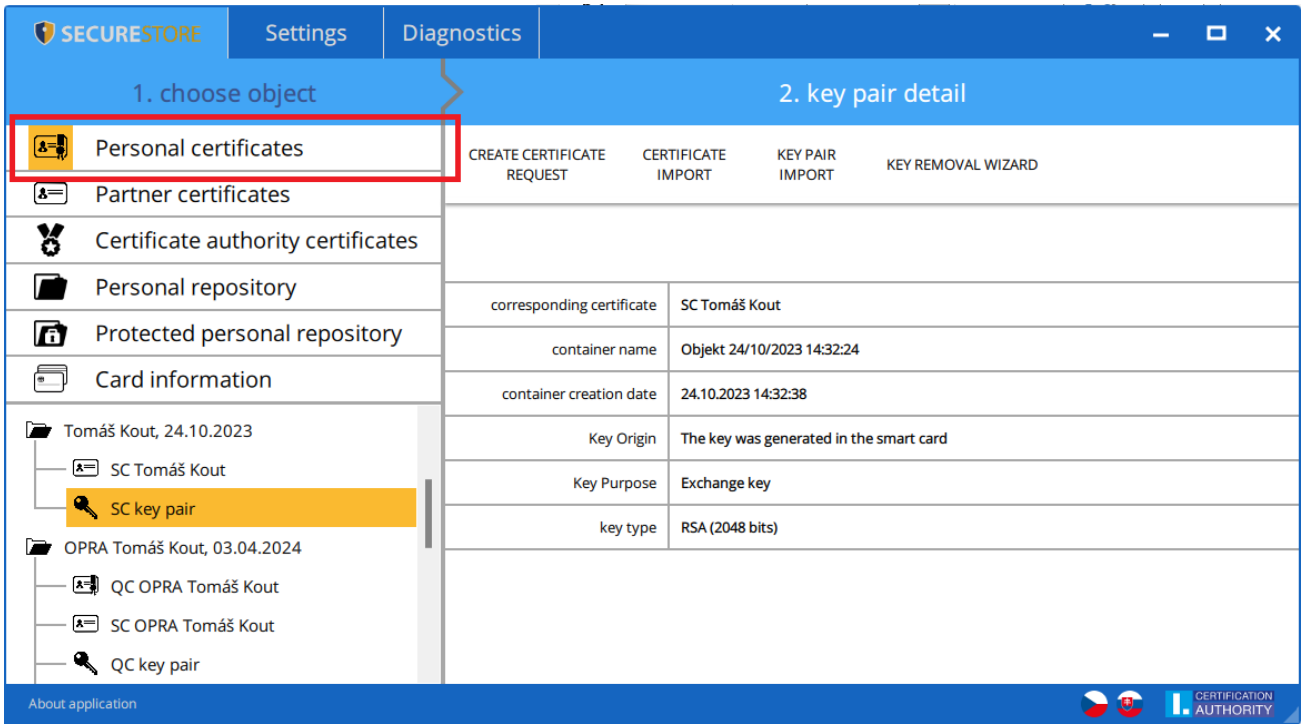
a) **<u>Starcos 3.0 and 3.5</u>** – The **Change PIN** option allows you to change the PIN provided, if the value of the original PIN is known. The **Unblock PIN** option allows a new PIN value to be set if the user blocks the PIN. A PUK is required to unblock the new PIN setting.
Unblocking a PIN using a PUK is limited to 5 attempts.

b) **<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 10 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



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.

The **"Key origin"** entry shows how the key was created on the card.

The **"Key purpose"** item indicates whether the key is an encryption or signature key.

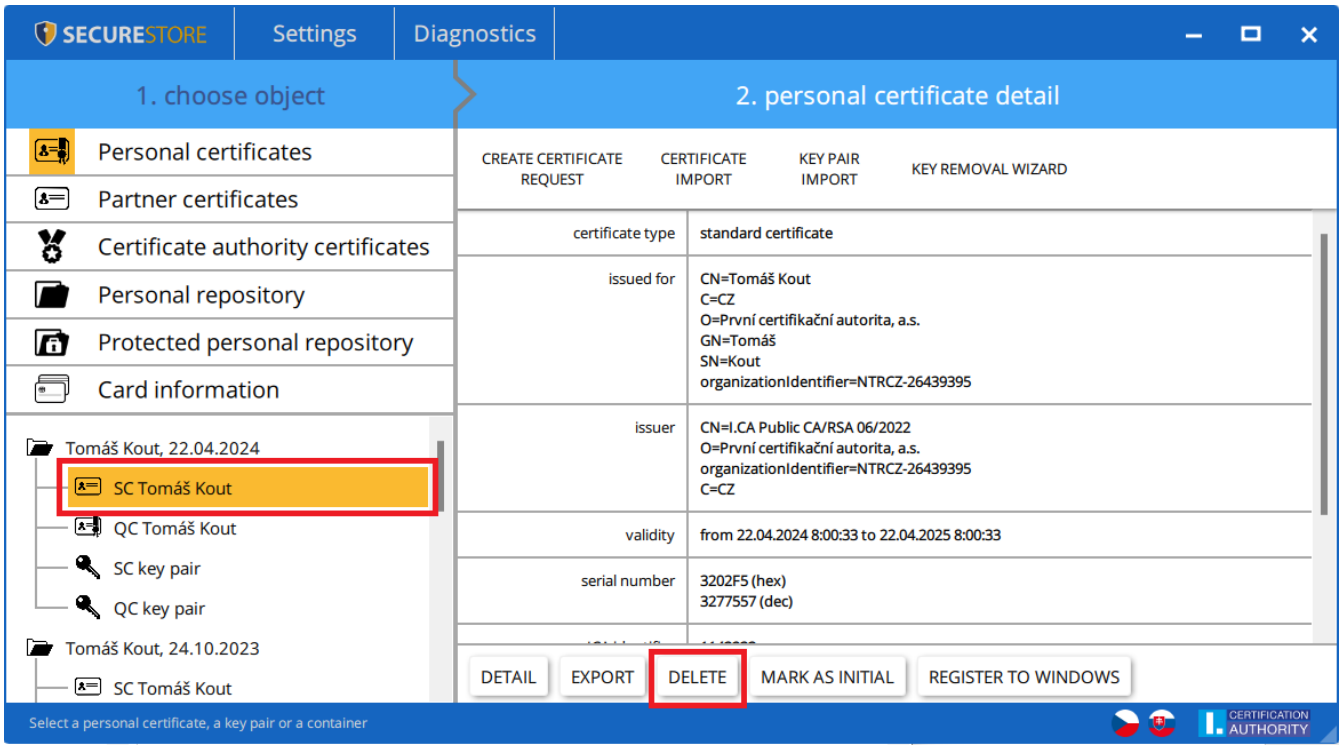
The **"Key type"** is also shown, in the example it is a key for the RSA algorithm with a length of 2048 bits.

A key pair can be removed from the card using the **"Remove"** button.

4.1 Deleting a public key

The user finds the option in the **"Personal Certificates"** object, selects the desired public key and uses the **"Delete"** button to perform the deletion.

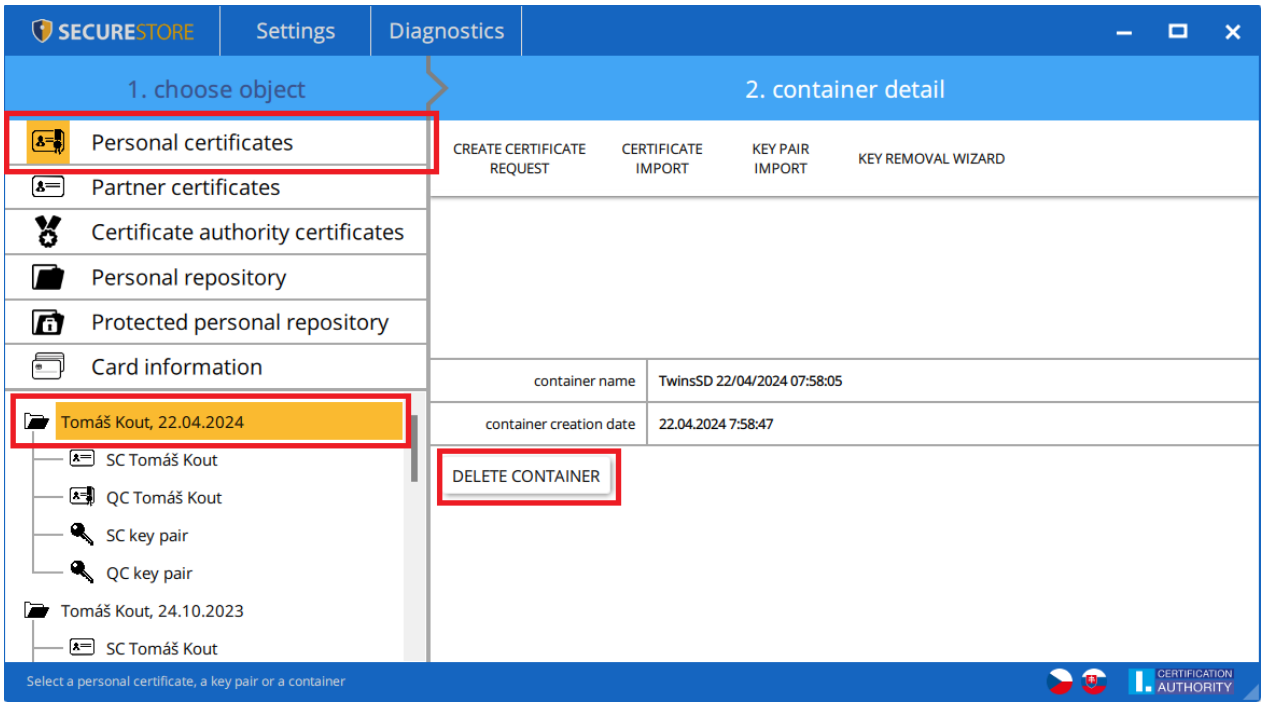
Fig. 17 - Deleting a public key



4.2 Removing the container

The user finds the option in the **"Personal Certificates"** object, selects the desired container and uses the **"delete container"** button to delete it.

Fig. 18 - Removing a container



If the user deletes the container, this session is irreversible and can no longer be signed/decrypted by the certificate!!!

4.3 Deleting a container using the key removal wizard

The user finds the option in the **"Personal Certificates"** object, selects the desired key pair and runs the **"Key Removal Wizard"** function.

Fig. 19 – Key removal wizard

The key removal wizard is divided into 3 tabs based on the type and length of the key. In this example, the key type is an RSA key with a length of 2048 bits.

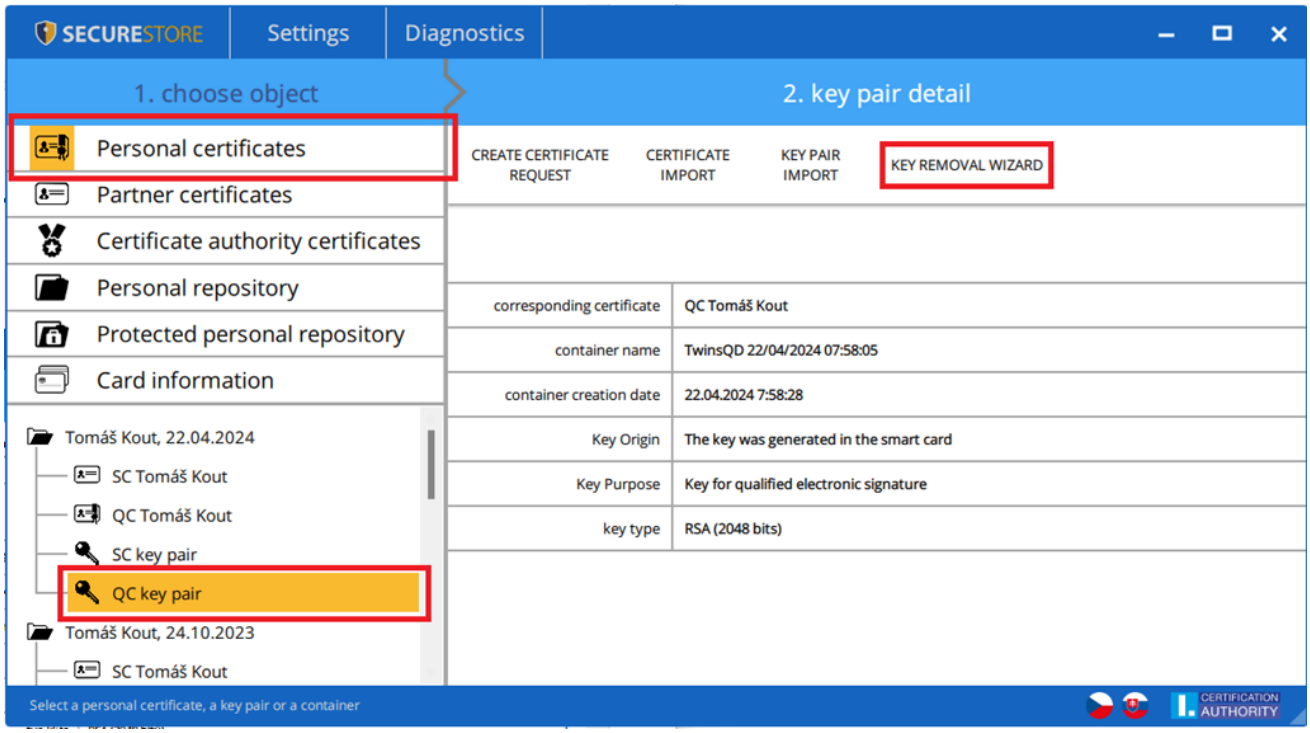
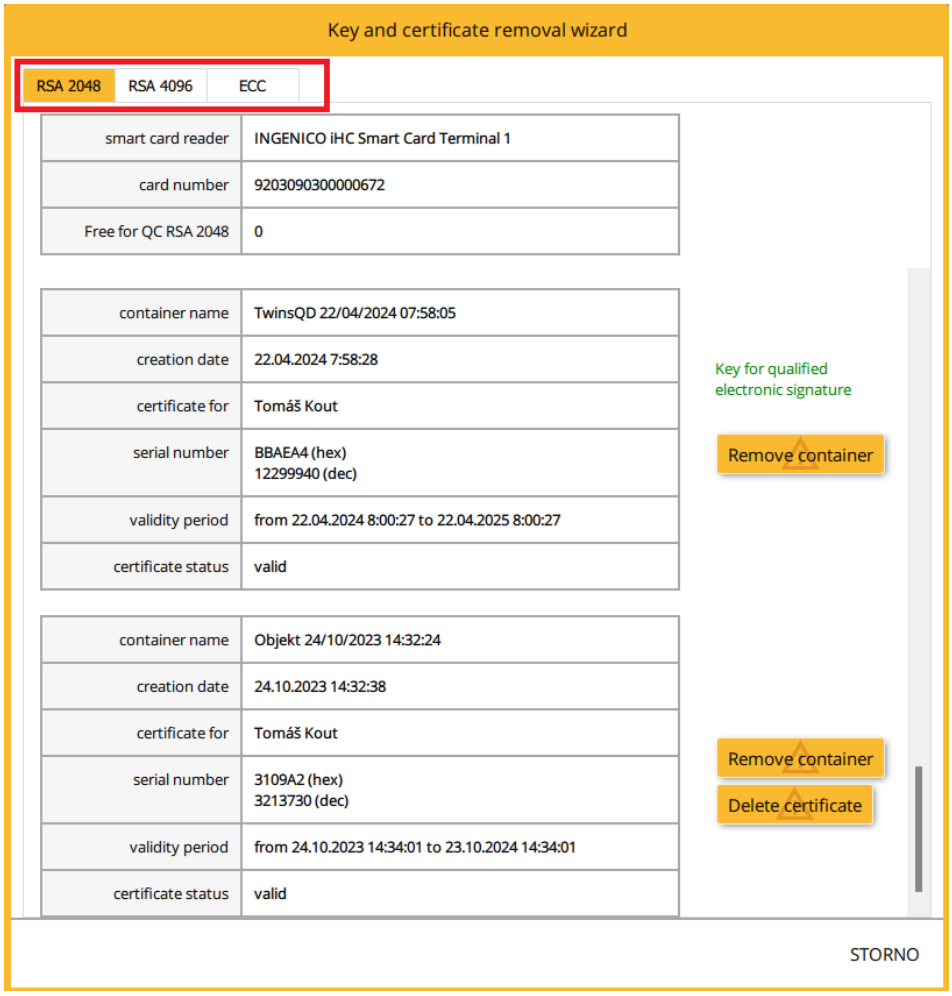


Fig. 20 - Key and certificate removal wizard



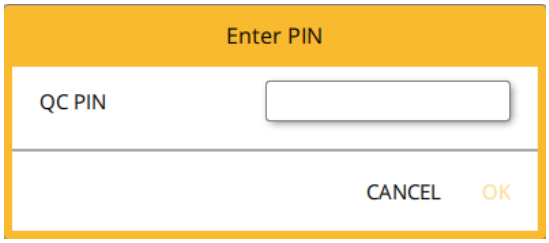
The "Remove container" option is the same as in the previous section 4.2.

If the user deletes the container, this session is irreversible and the certificate can no longer be signed/decrypted!!!

The **"Delete certificate"** option is only enabled for commercial certificates and is used to remove only the public key as in 4.1

After clicking on the **"Delete"** option, the user is prompted to enter the PIN, after entering the PIN the marked certificate/container will be deleted.

Fig. 21 - Entering the PIN to remove the certificate/container

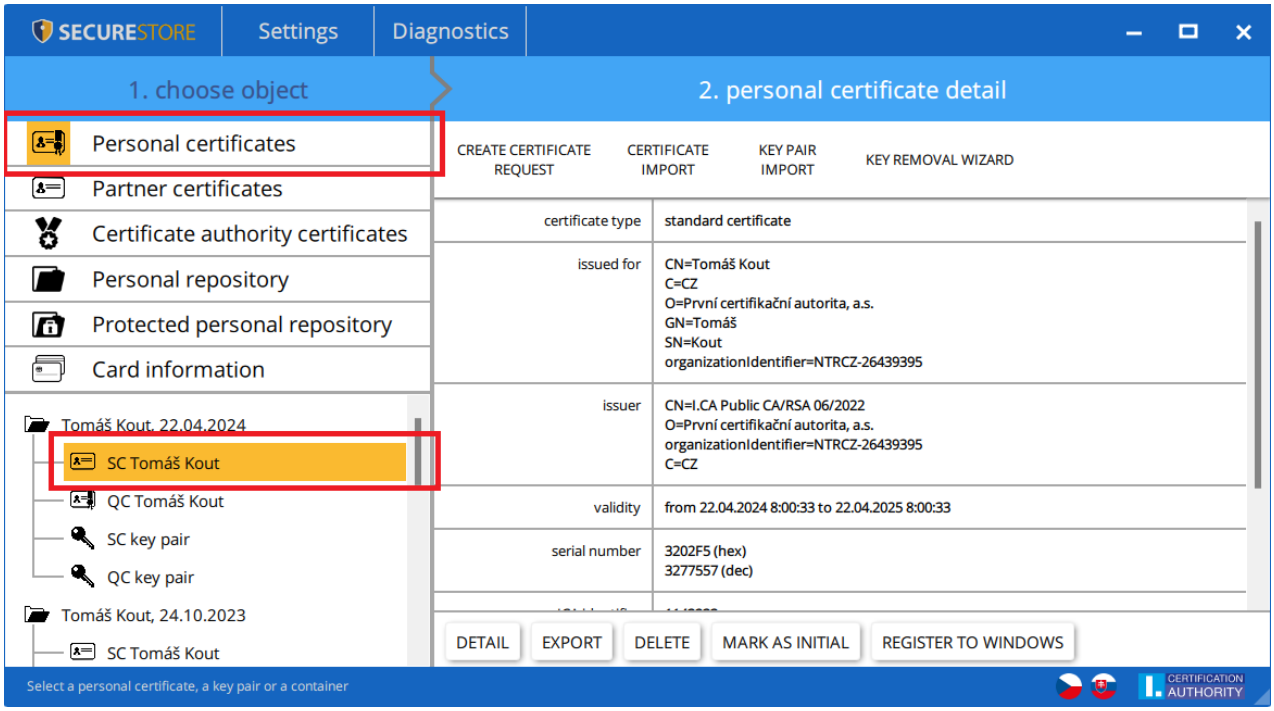


5. Certificates

5.1 Displaying the certificate

The user can find the certificate display in the **"Personal certificates"** object, where he selects the desired certificate to display. The detail of the certificate is displayed in the right screen of the application in the **"Personal certificate detail".**

Fig. 22 - Displaying the certificate

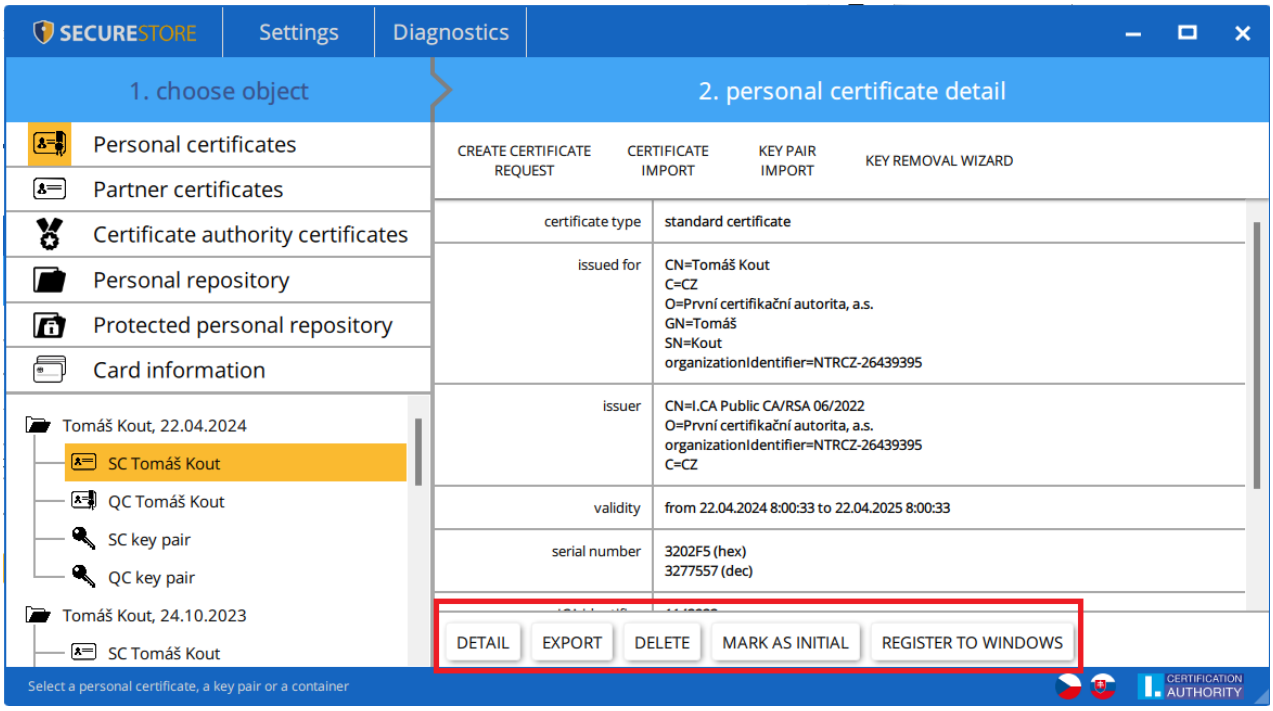


5.2 Working with a personal certificate

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

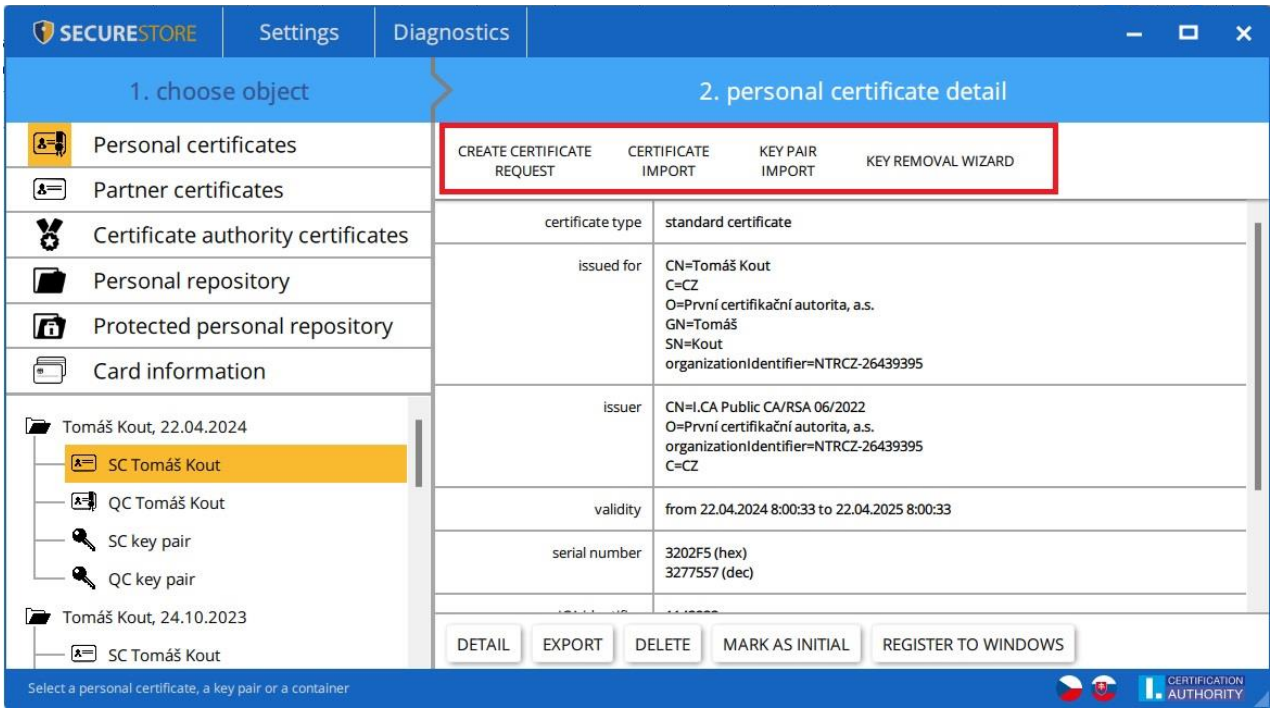
The user finds the option in the **"Personal certificates"** object and selects the required certificate for the operation using the toolbar.

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



The options for importing a certificate to a smart card are available by clicking on the **"Personal certificates"** object.

Fig. 24 - Options for importing a certificate



The personal certificate is imported in the storage where the corresponding key pair is saved. Communication partner's certificates can be imported as partner certificates.

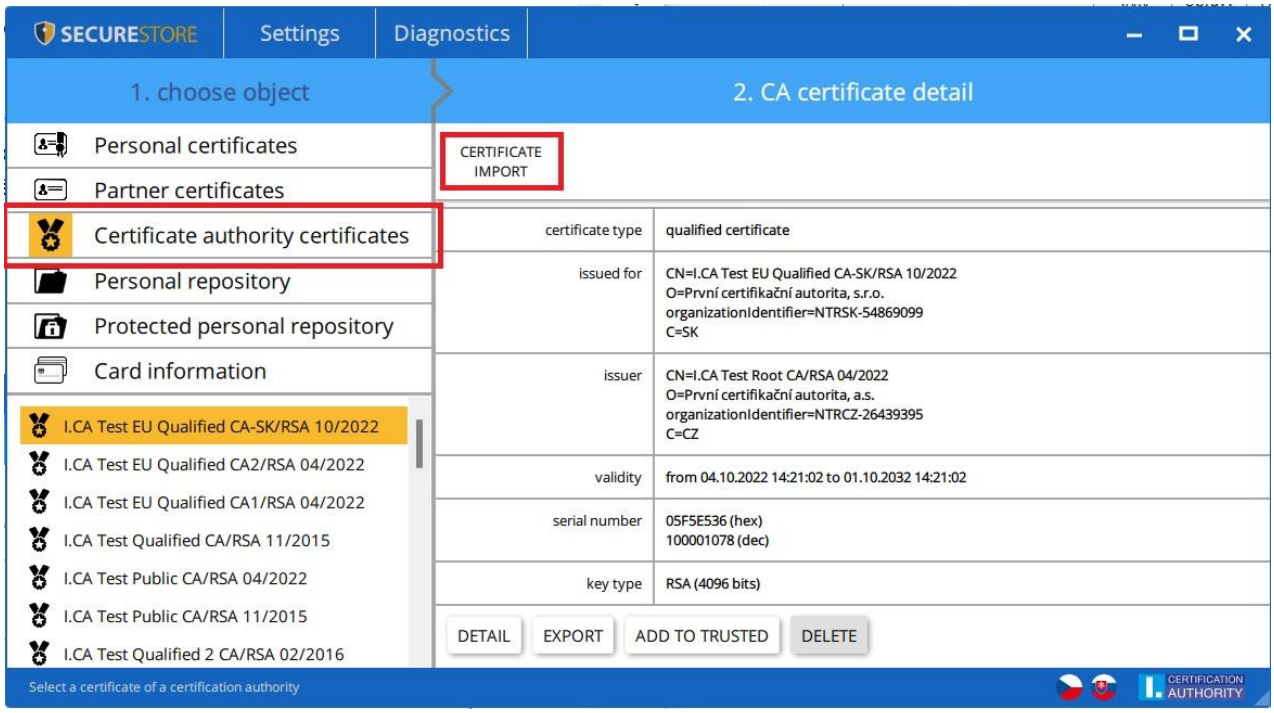
Displaying the certificate's bare data is an option for experts to make a visual check of the certificate's data.

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 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

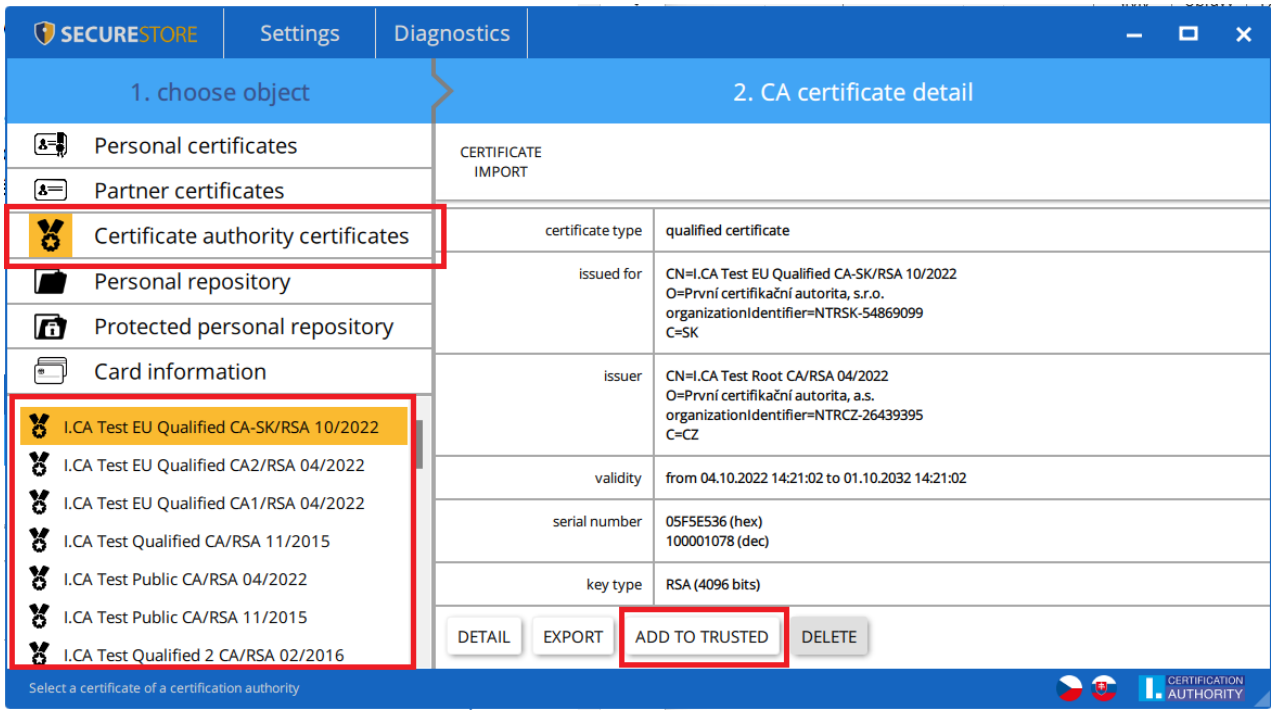
Fig. 25 – Importing a Certification Authority Certificate



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

If the user is using an older version of Windows and I.CA root certificates are not part of Windows, register the root certificate from the smart card. Use the "**Add to Trusted**" option to register, see Figure 26. Registering the root certificate to Windows requires user consent, then the root certificate is registered to MS Windows as a trusted root certificate.

Figure 26 - Registering a certification authority certificate to Windows



5.4. Registering Personal Certificate in Windows

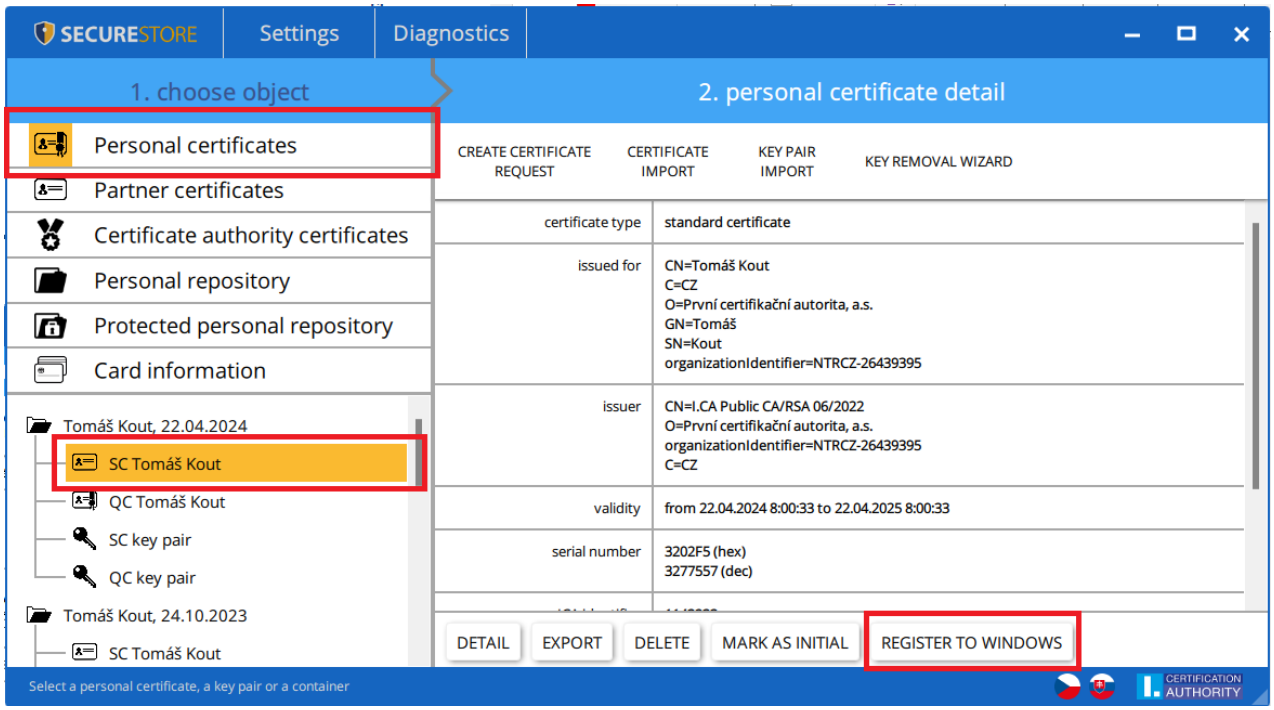
Most applications require that the personal certificate with which the user wants to work be registered in Windows.

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

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

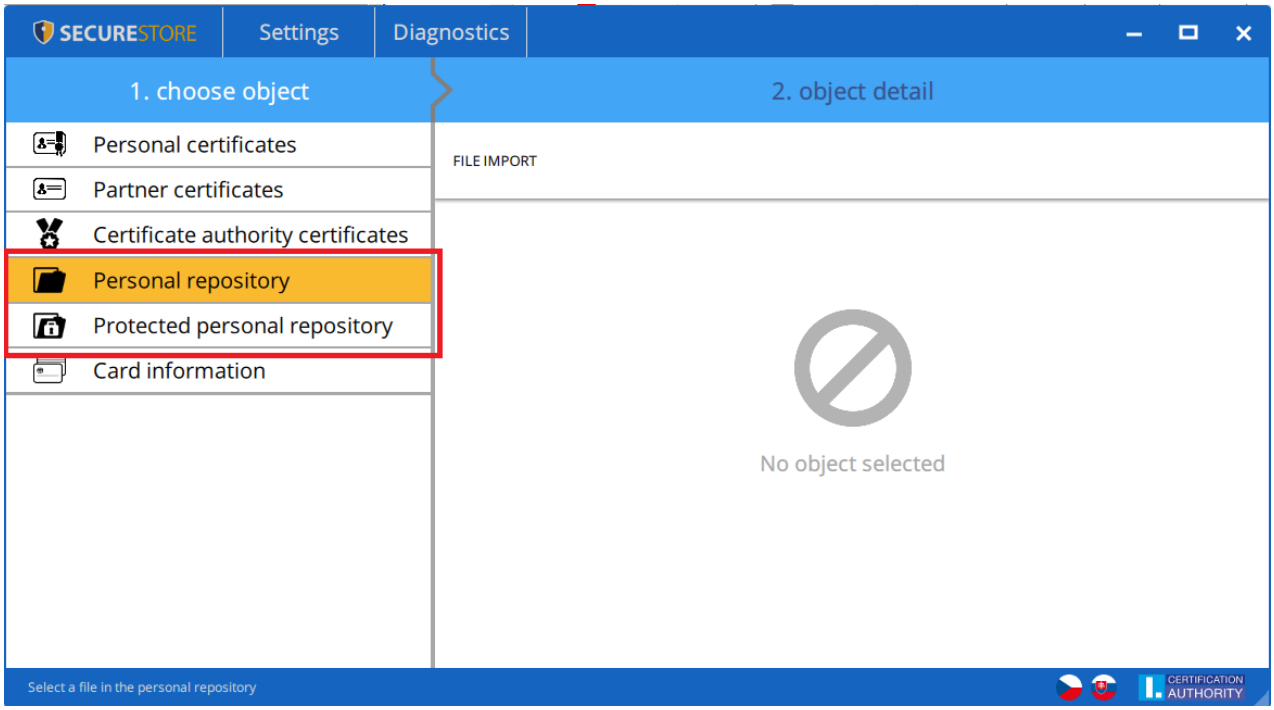
Go to **"Personal Certificates"** and select the certificate to be registered.

Fig. 27 – Registering personal certificate in Windows



6. Personal Repository

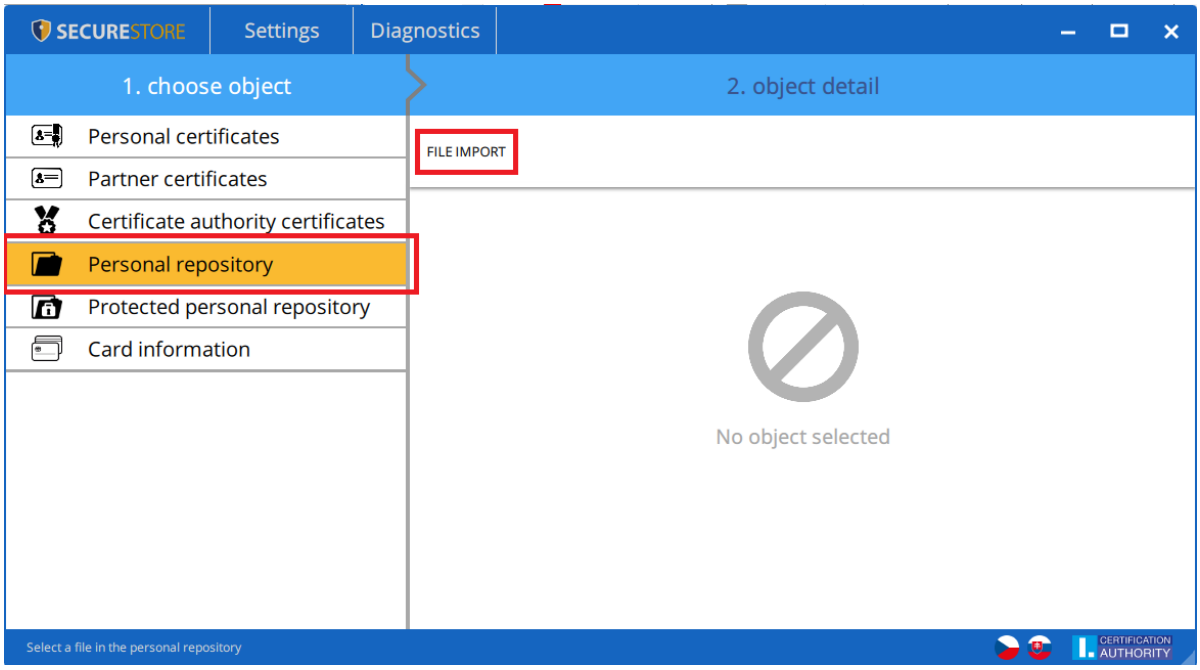
Fig. 28 – Personal Repository



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.

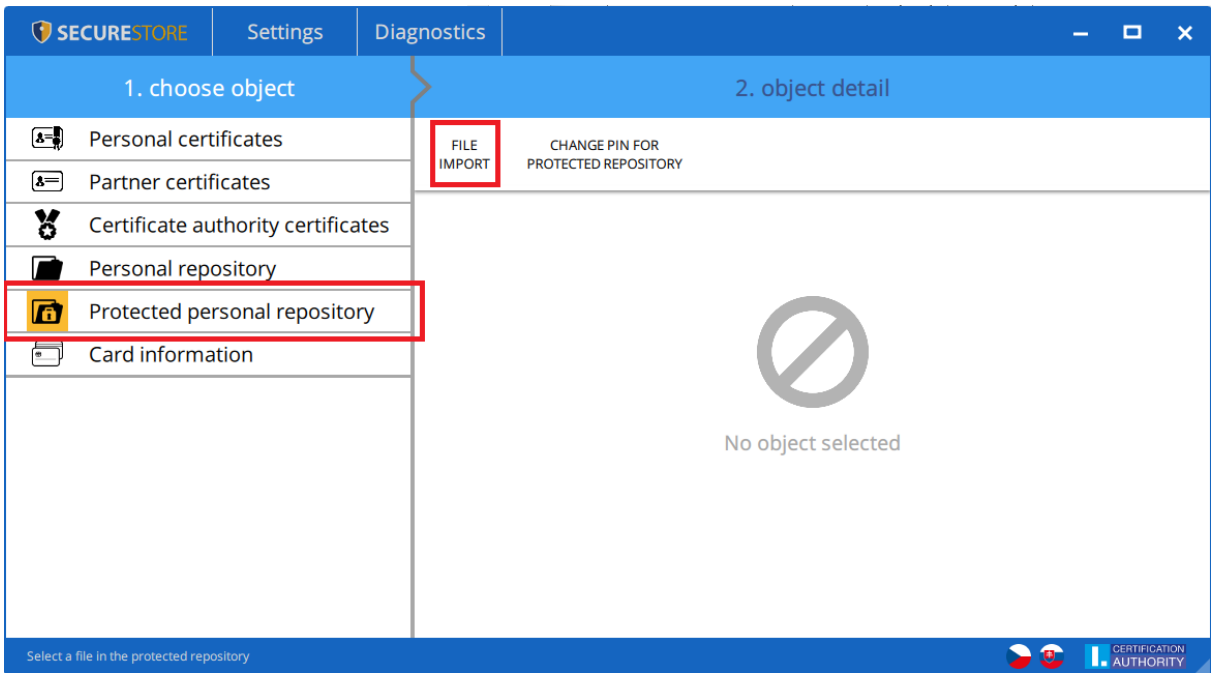
Reading and exporting secure storage files are protected with the secure storage PIN, **see Chapter 2**.

Fig. 29 - Importing a file into personal repository



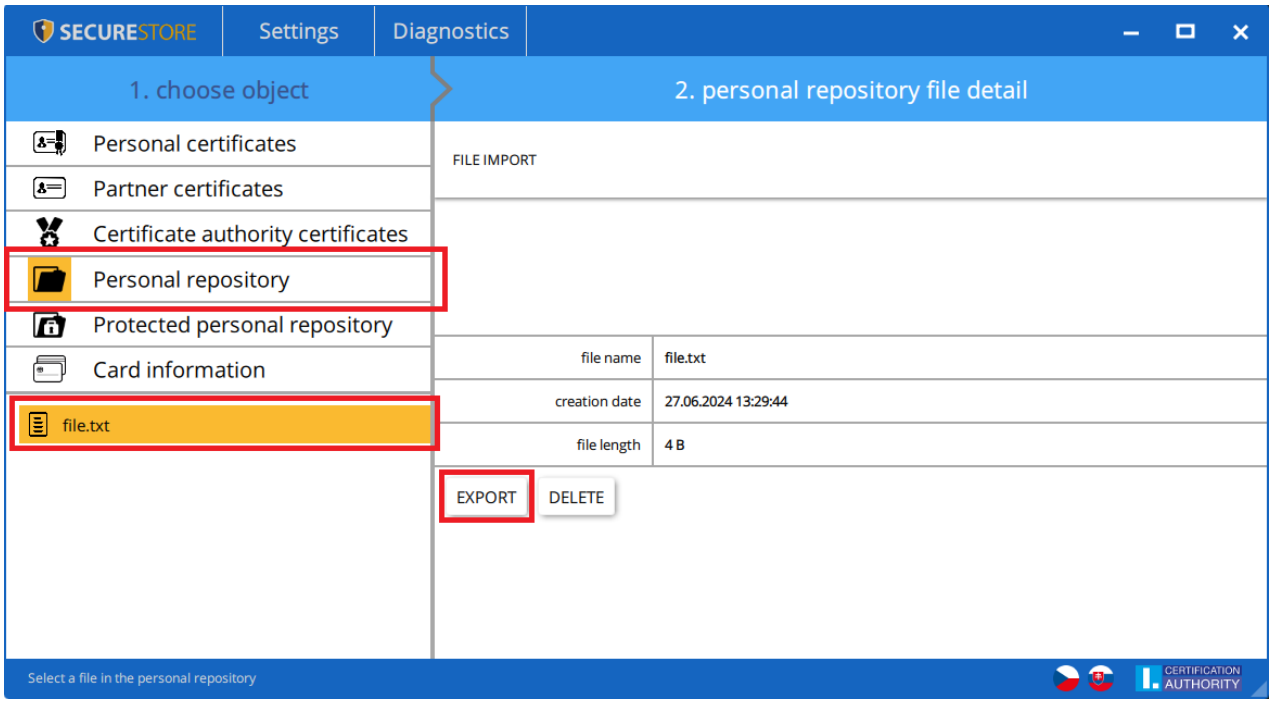
The user can find the function in the **"Personal Repository"** object and in the details of the **"File import"** object.

Figure 30 - Importing a file into a protected repository



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

Fig. 31 - Exporting a file from a personal 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.

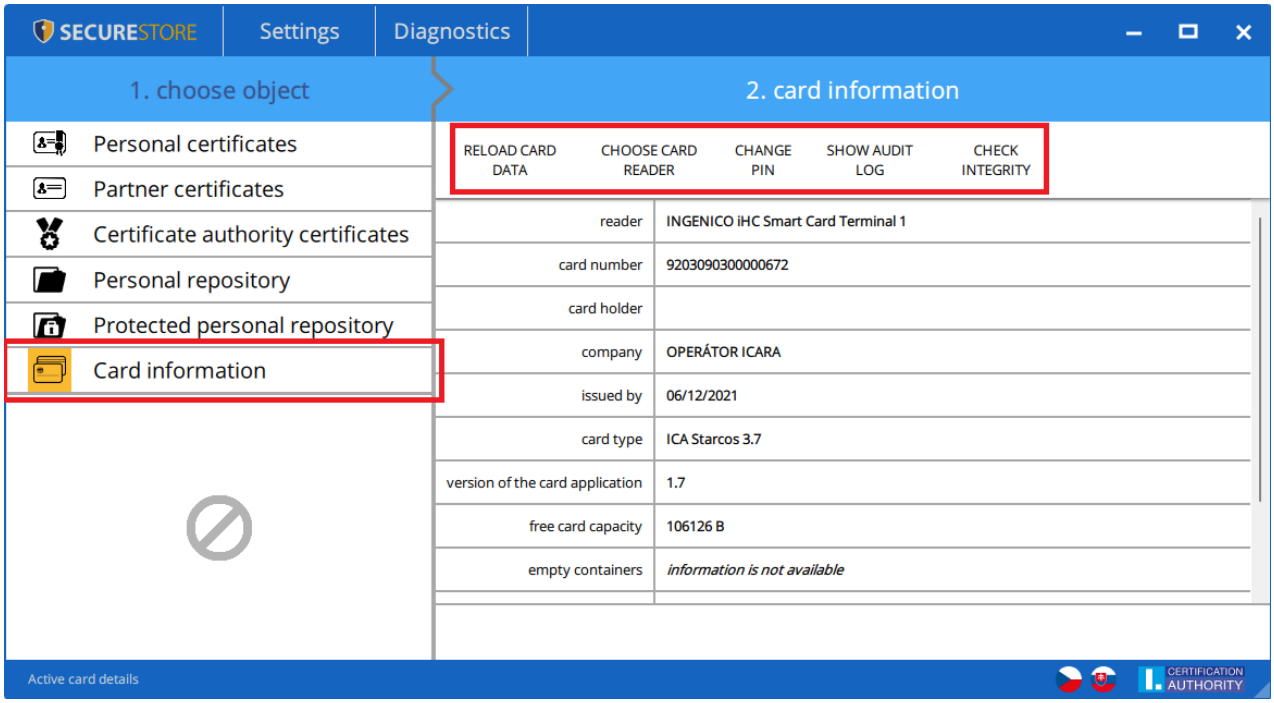
7. Application control

The 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 Toolbar for card information

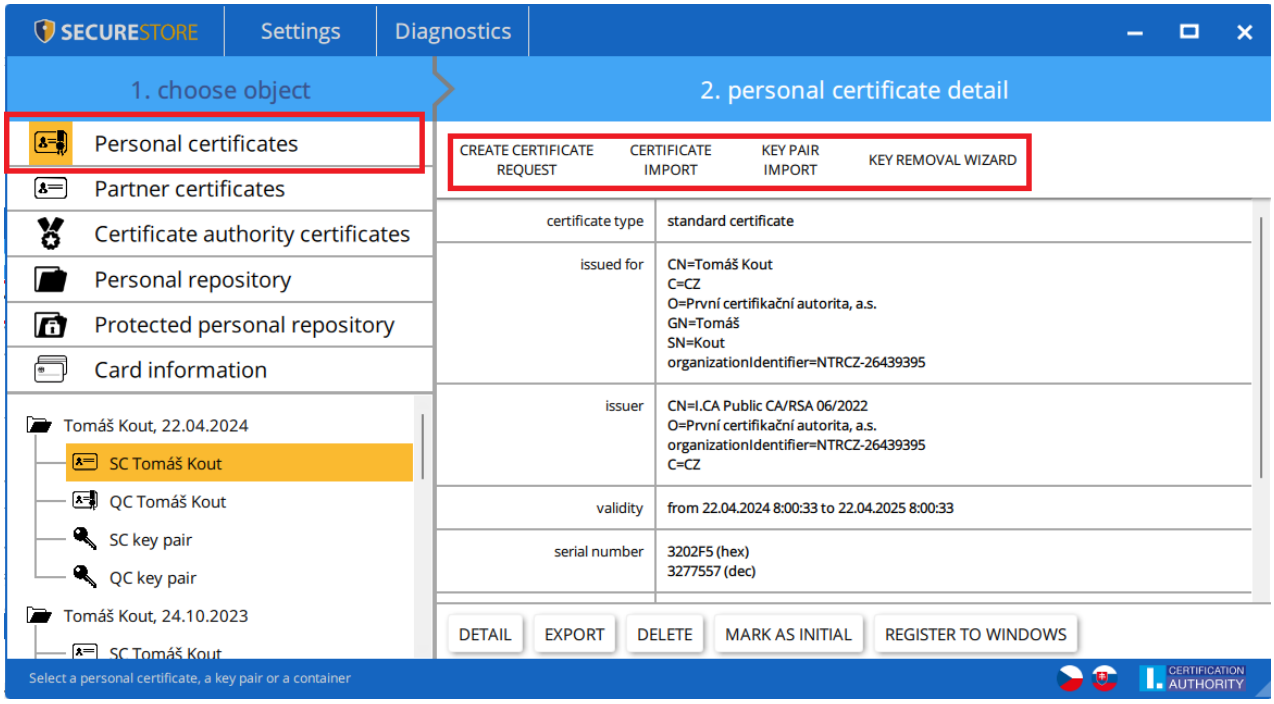
The toolbar of the “Card information” object contains basic administrative operations with the card related to PIN and PUK management and repeated loading of data from the card.

Fig. 32 – Toolbar of the "Card information" object



7.2 Toolbar for Personal certificates folder

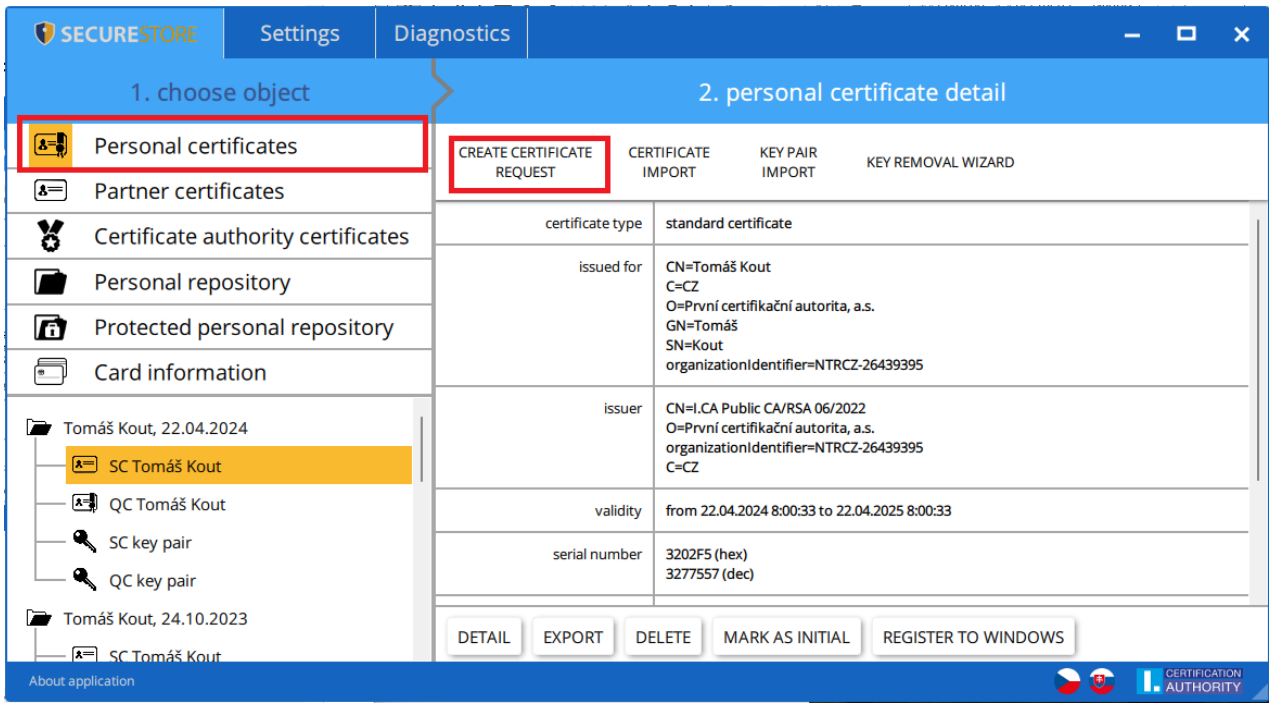
Fig. 33 – Toolbar for the "Personal Certificates" object



7.2.1 Create 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. 34 - Selecting the type of request for generating a key pair using the online generator



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

Fig. 35 - Selecting the type of certificate applicant

Fig. 36 - Data entry – on-line generator

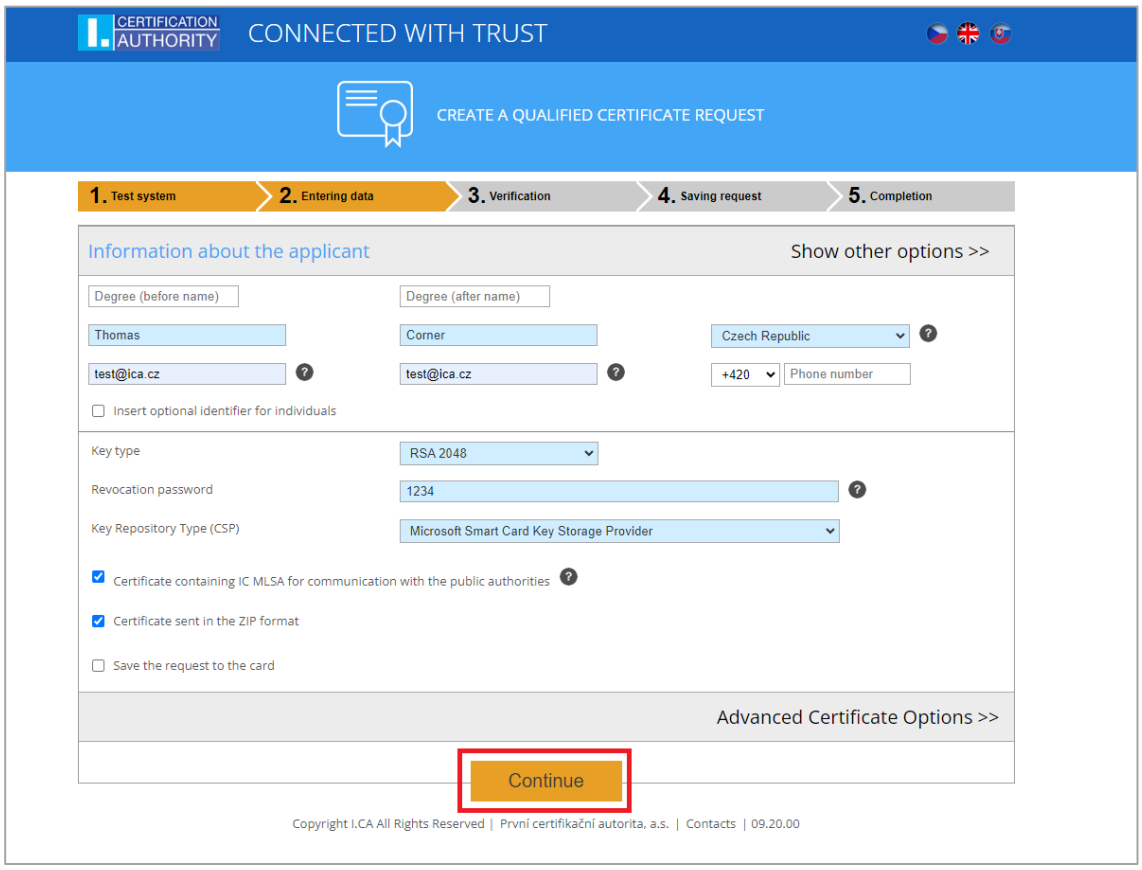
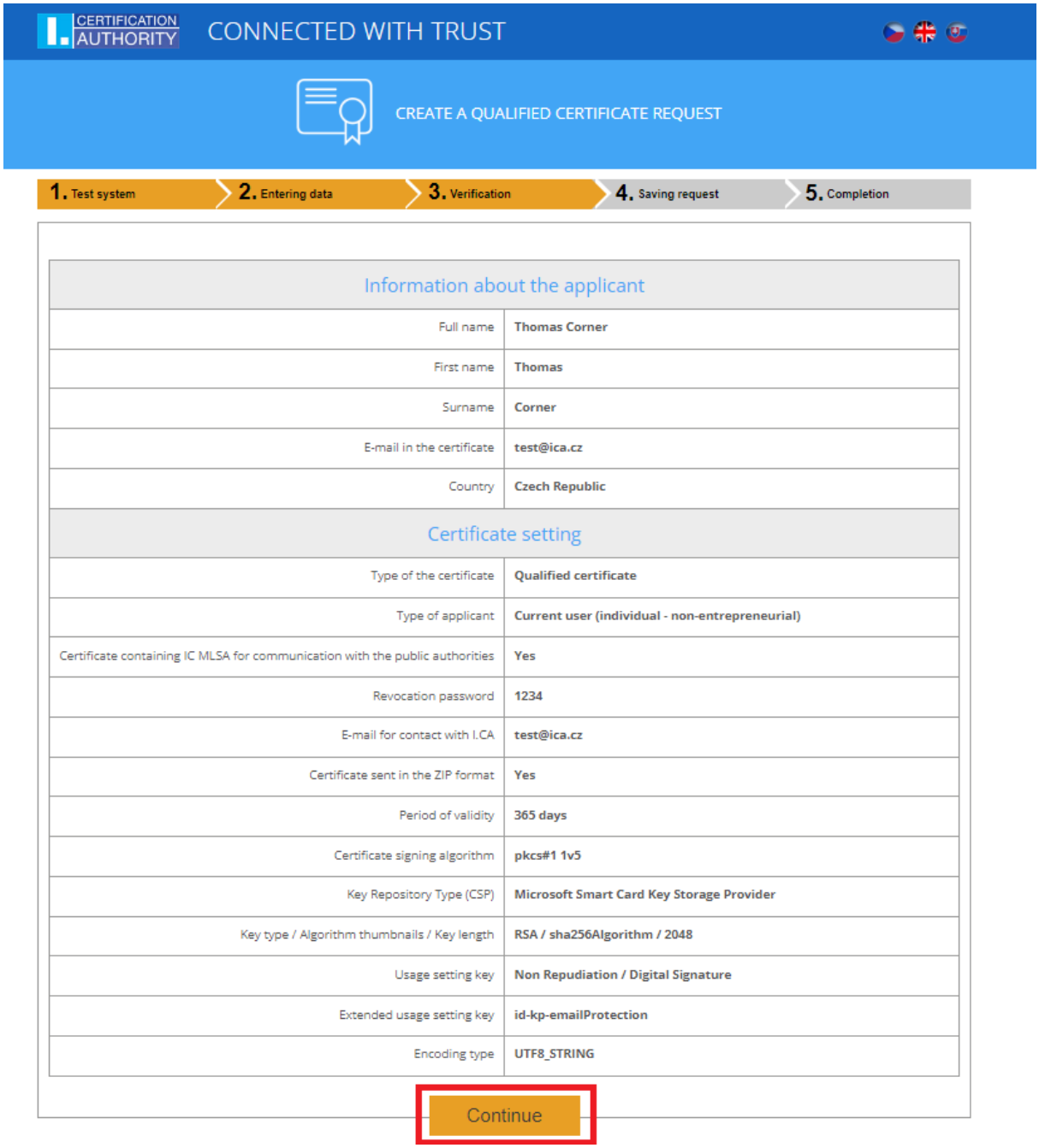


Fig. 37 - Data check – on-line generator



Generating key pairs and signing the request - on-line generator

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. 38 - Generating a private key

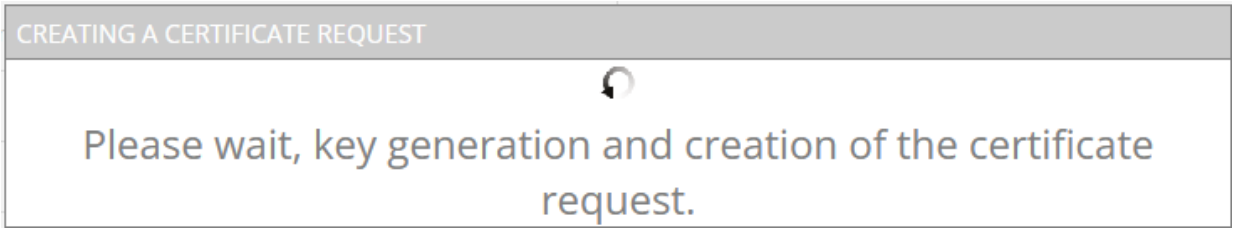


Fig. 39 - Selecting a smart card reader

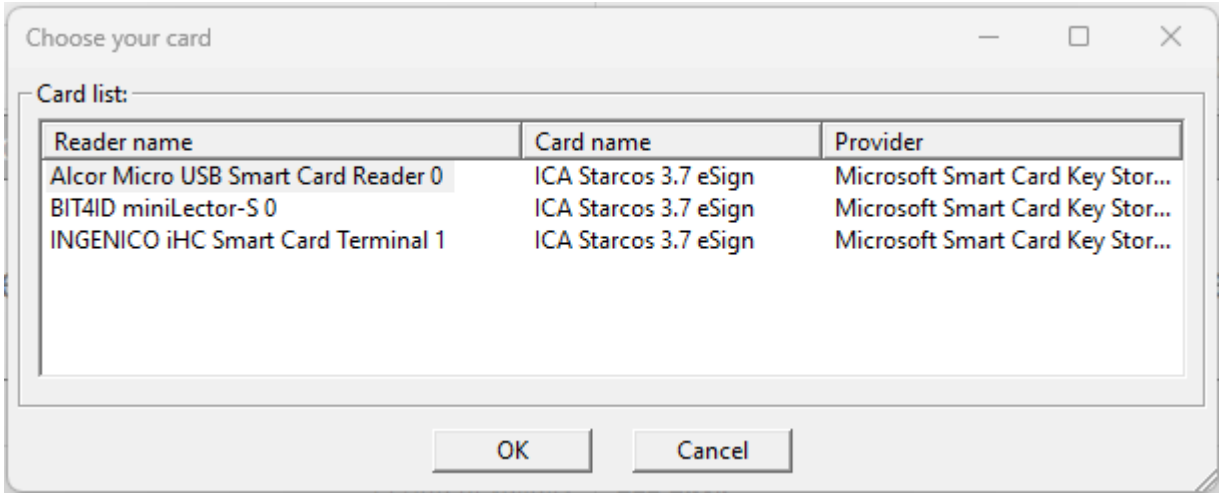


Fig. 40 - Entering the PIN to generate the key pair and signing the request

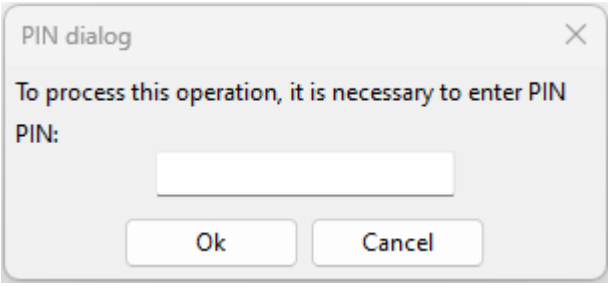
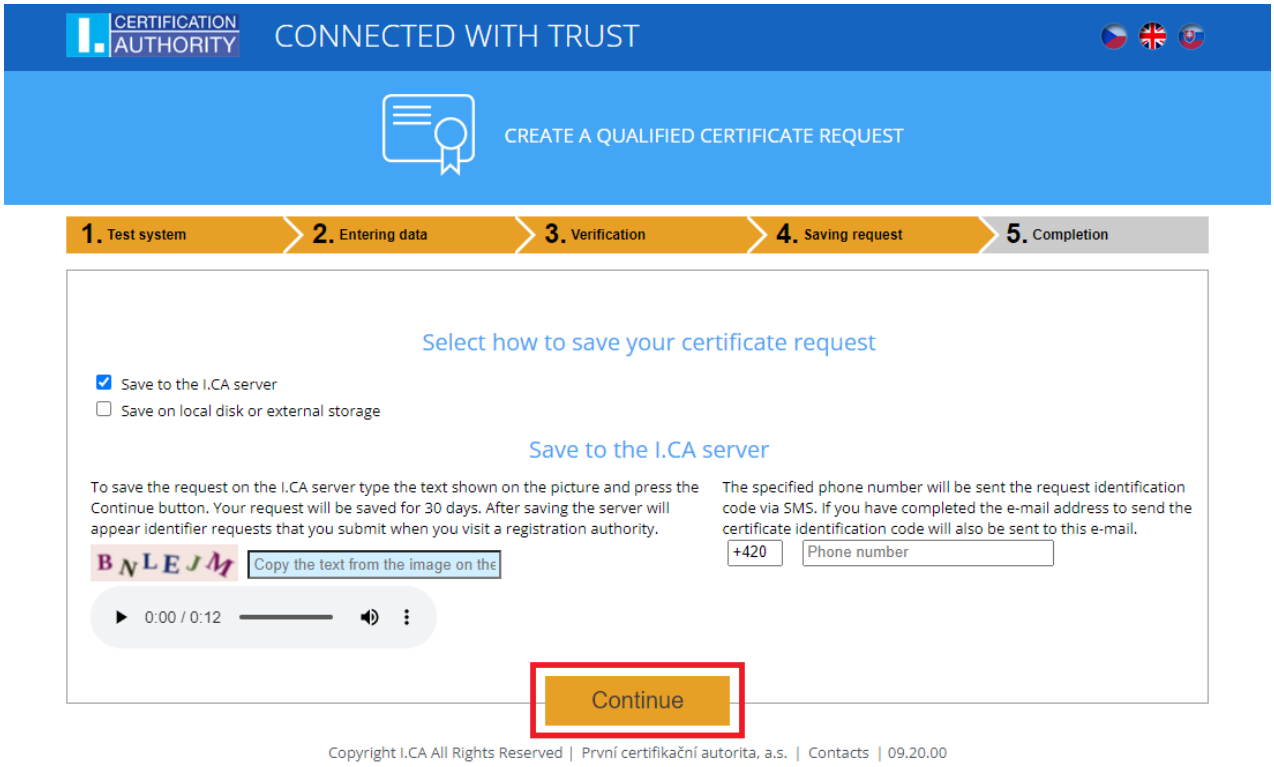


Fig. 41 – Saving the request – on-line generator

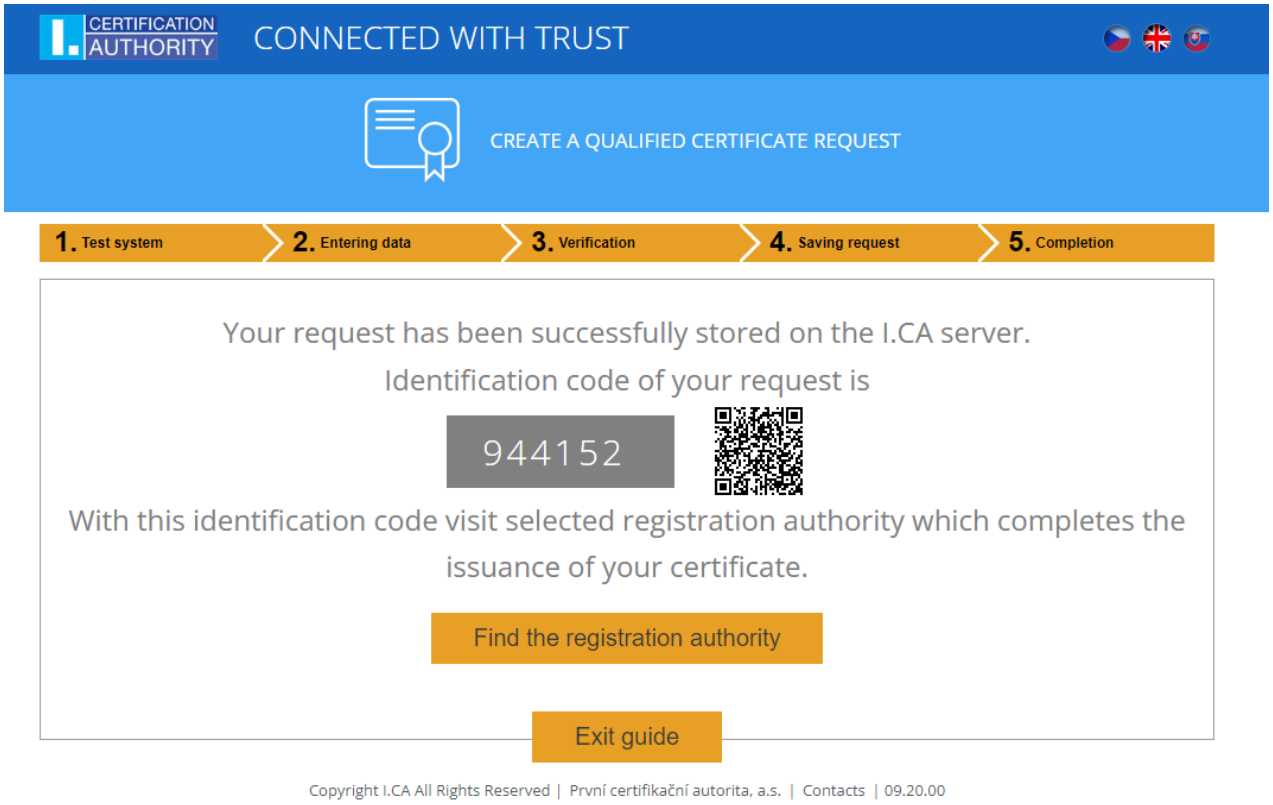


Choosing a way to save a certificate request.

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 **"Save to local disk or external storage"** is selected, a file with the generated request called cert****.req is saved.

Fig. 42 - Completion – on-line generator

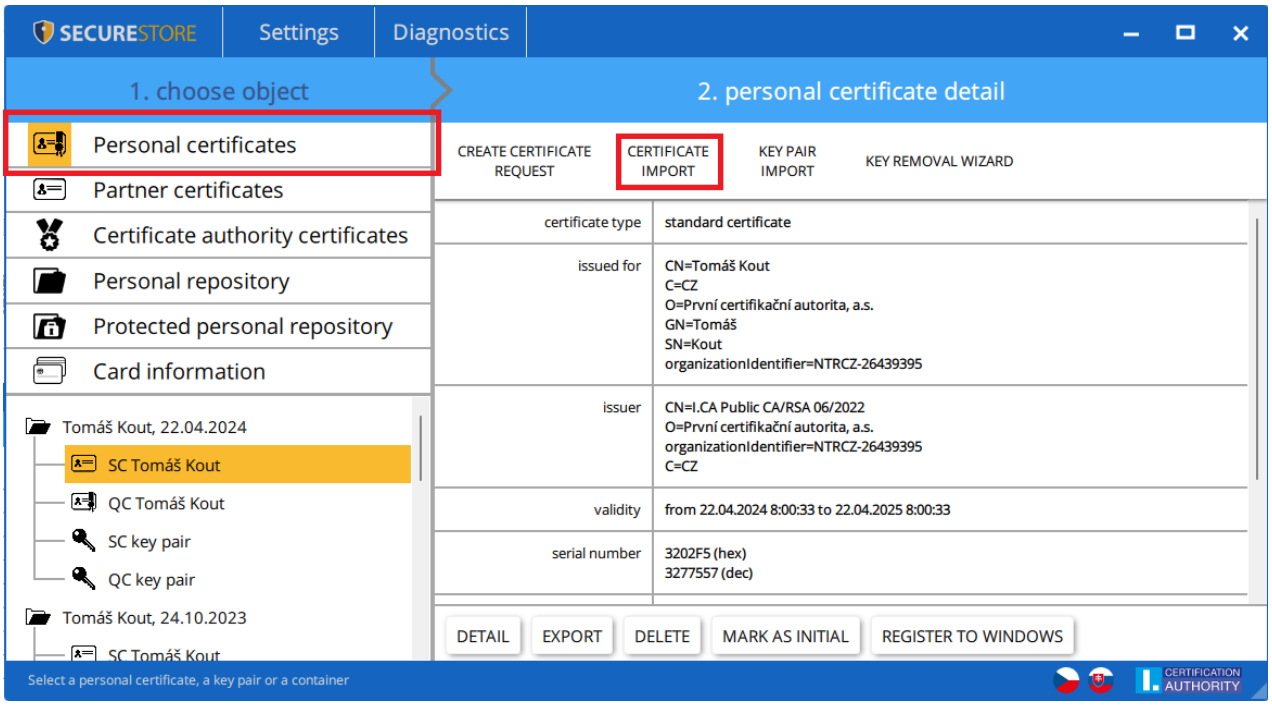


With the six-digit numerical code for the request stored on the I.CA server or with the req. file on a portable USB medium, the user then visits the registration authority, which can be searched for using the **"Find registration authority"** button.

7.2.2. Importing a personal certificate

This function allows you to import a personal certificate from disk to smart card. The certificate is imported in cer./der. format. The user can find the function in the **"Personal certificates"** object.

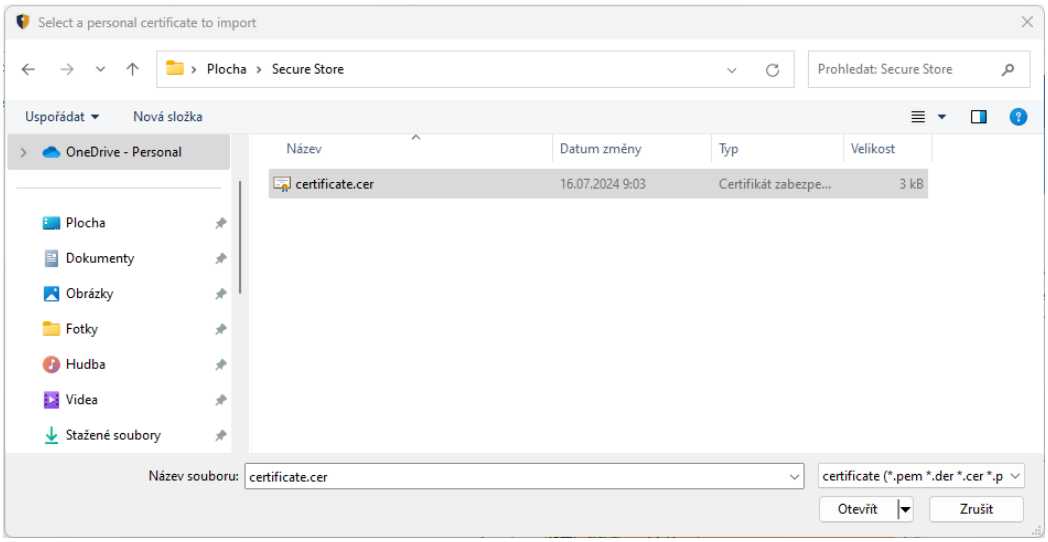
Fig. 43 - Importing a personal certificate



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

If there is no storage on the smart card containing the appropriate keys, the certificate will be stored in the part of the card marked **"Partner Certificates"**.

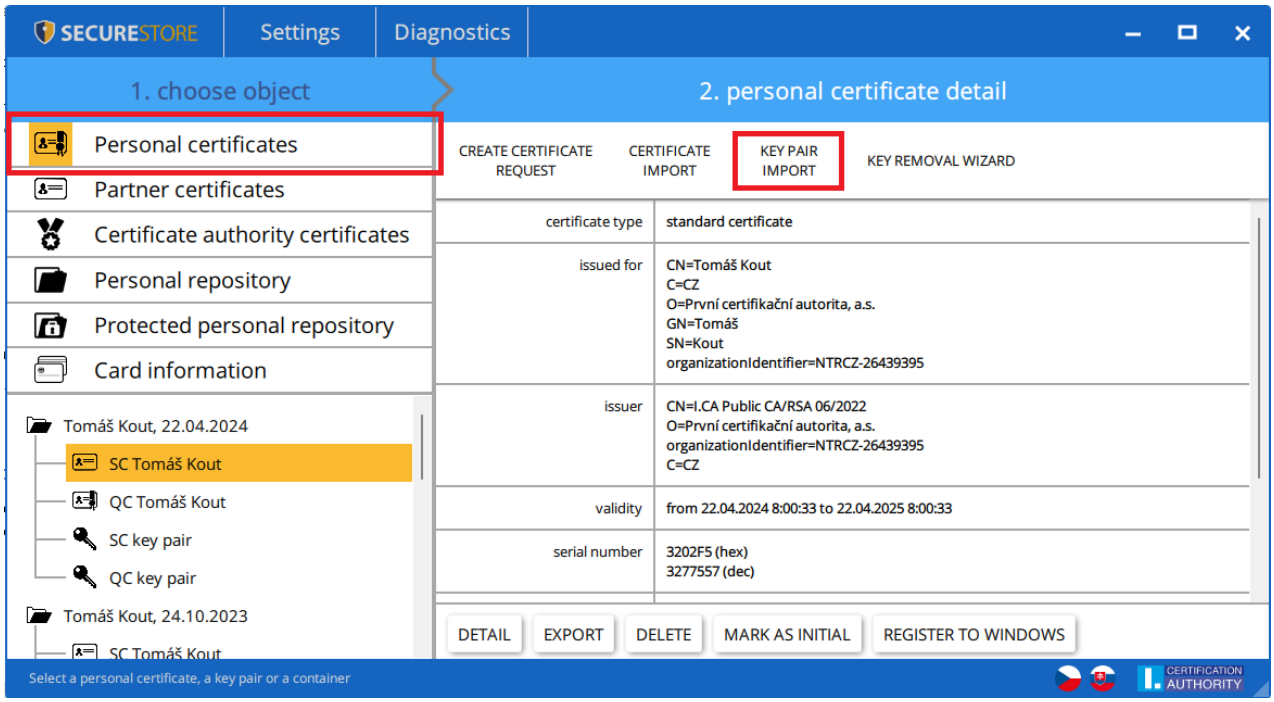
Fig. 44 - Selecting a certificate file to be imported to the card



7.2.3 Importing a key pair from a backup (PKCS#8) and importing keys (PKCS#12)

This option imports the keys that were saved to disk during the process of generating the encryption certificate request (PKCS#8) onto the smart card. The user can find the function in the **"Personal Certificates"** object. In the same way, keys with a certificate that are stored in PKCS#12 format on disk can be imported to the smart card.

Fig. 45 - Importing a key pair from a backup (PKCS#8) and a key pair (PKCS#12)

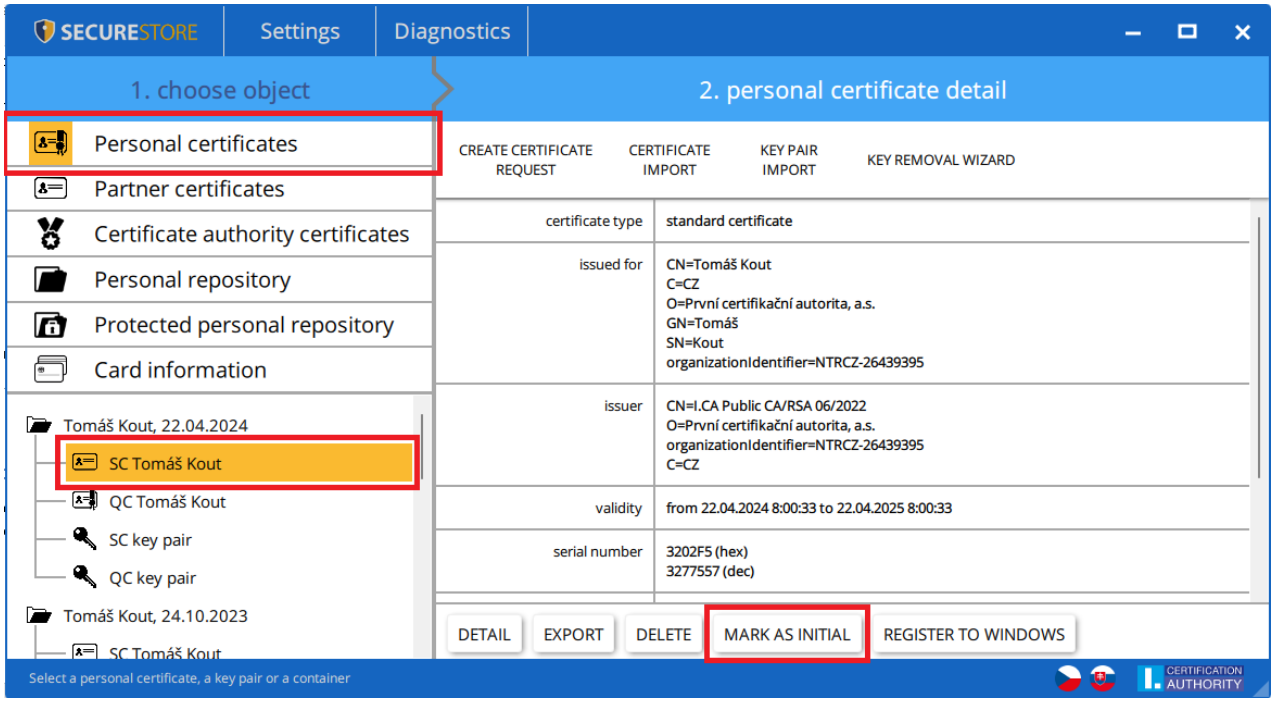


7.2.4 Set the certificate as the default for logging into Windows

This option allows you to mark the selected certificate as the default for Windows login. The selected certificate will be used when logging into Windows.

The user can find the function in the **"Personal certificates"** object, where he selects the certificate intended for this function and confirms it with the "Mark as default" button.

Fig. 46 - Mark certificate as default for Windows login



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.

Windows login certificate - must contain specific information. Therefore, you cannot use any certificate to log in to Windows. The I.CA registration authority will provide the correct certificate for logging in upon request. The storage on the card containing the login certificate must be marked for authentication. Only one storage on the card can be marked for authentication.

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.