SecureStore I.CA

User manual

Version 2.16 and higher

Contents

1. Introduction

This version of user manual applies to the following version of the SecureStore application: 2.16 and higher. The above-mentioned versions have the same functionality and identical user interface.

2. Access data for the card

Access to the card is protected by PIN, similarly as for e.g. payment cards.
PIN is a 4 to 8-digit number. If you enter an incorrect PIN value three times in sequence, PIN will be automatically locked.
PUK value is intended to unlock PIN.
PUK is a 4 to 8-digit number. If you enter an incorrect PUK value 5 times in sequence, PUK and the whole card will be locked.

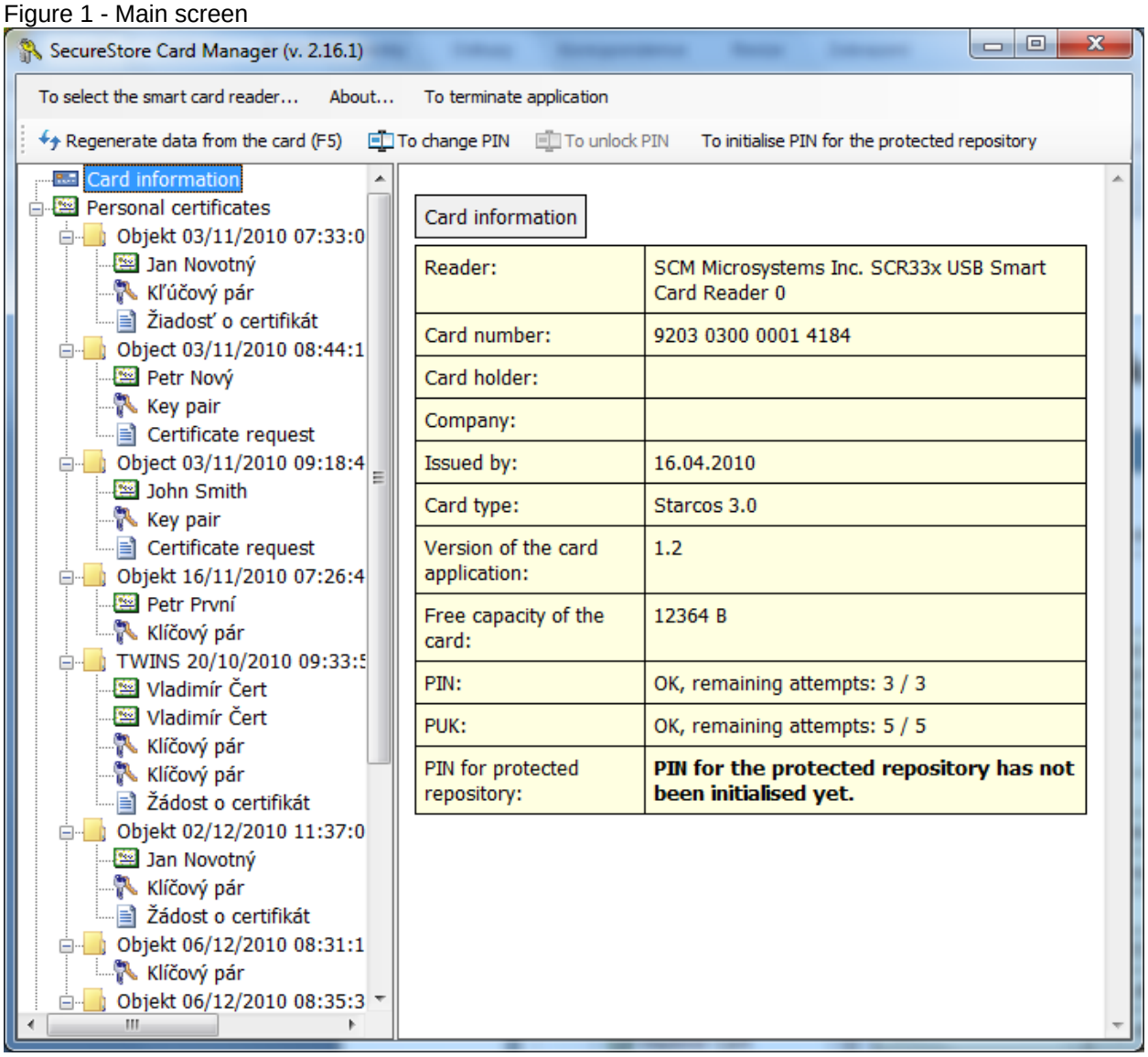
The card part called “Protected personal repositories” is intended for storage of any data. This area is protected by a special PIN, the so-called protected repository PIN. To unlock the protected repository PIN, use PUK mentioned in the previous paragraph.
The protected repository PIN is a 4 to 8-digit number.

2.1 Card initialisation

The card initialisation dialog is usually displayed at the first launch of the application if you did not receive the PIN envelope for the card. It is necessary to setup PIN and PUK to work with the newly inserted card using this dialog. It is necessary to remember this PIN and PUK very well, or to store it at a safe place so that nobody could gain access to it.

3. Main screen

Figure 1 - Main screen

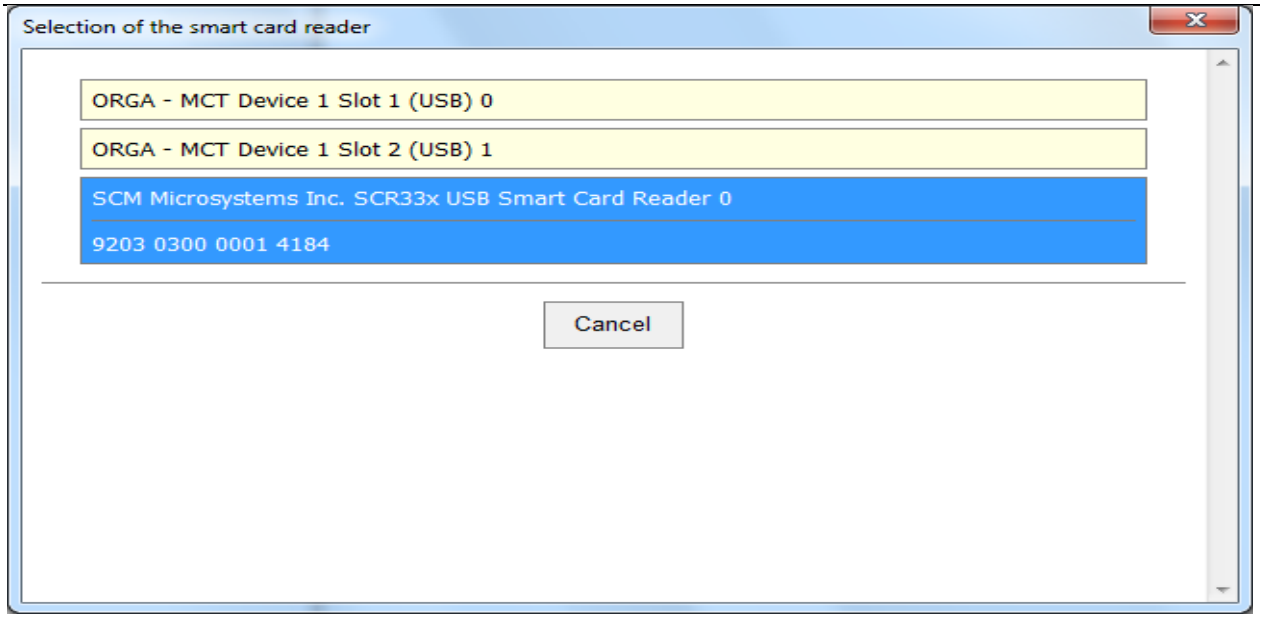


At the top right screen area, there is the basic information about the card holder, card validity, chip card reader in which the card is inserted, and the version of the card file system.

At the top bar, there are the following options:

The option "**To select chip card reader"** is useful if you have several smart card readers simultaneously connected to your PC. You can select the reader with which you want to work. The chip card number and type is displayed for the chip card reader in which the card is inserted, see the following figure.
If you have several chip card readers connected to your PC, the "Selection of the chip card reader" window is displayed even after the application is launched.

Figure 2 – Selection of the chip card reader

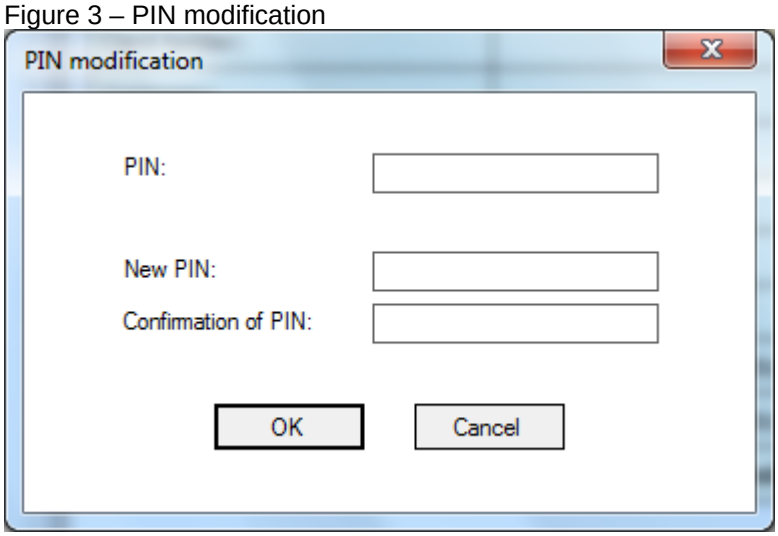


If you have only one chip card reader connected to your PC, the window is not displayed and the information about the reader detected is mentioned in the first line of the introductory screen.

The **"Restore data from the card"** option will repeatedly download the data from the chip card. F5 key has the same functionality.

The "**PIN modification"** option will change the main card PIN. It requires entering the existing PIN and the new PIN 2-times to confirm it.

Figure 3 – PIN modification

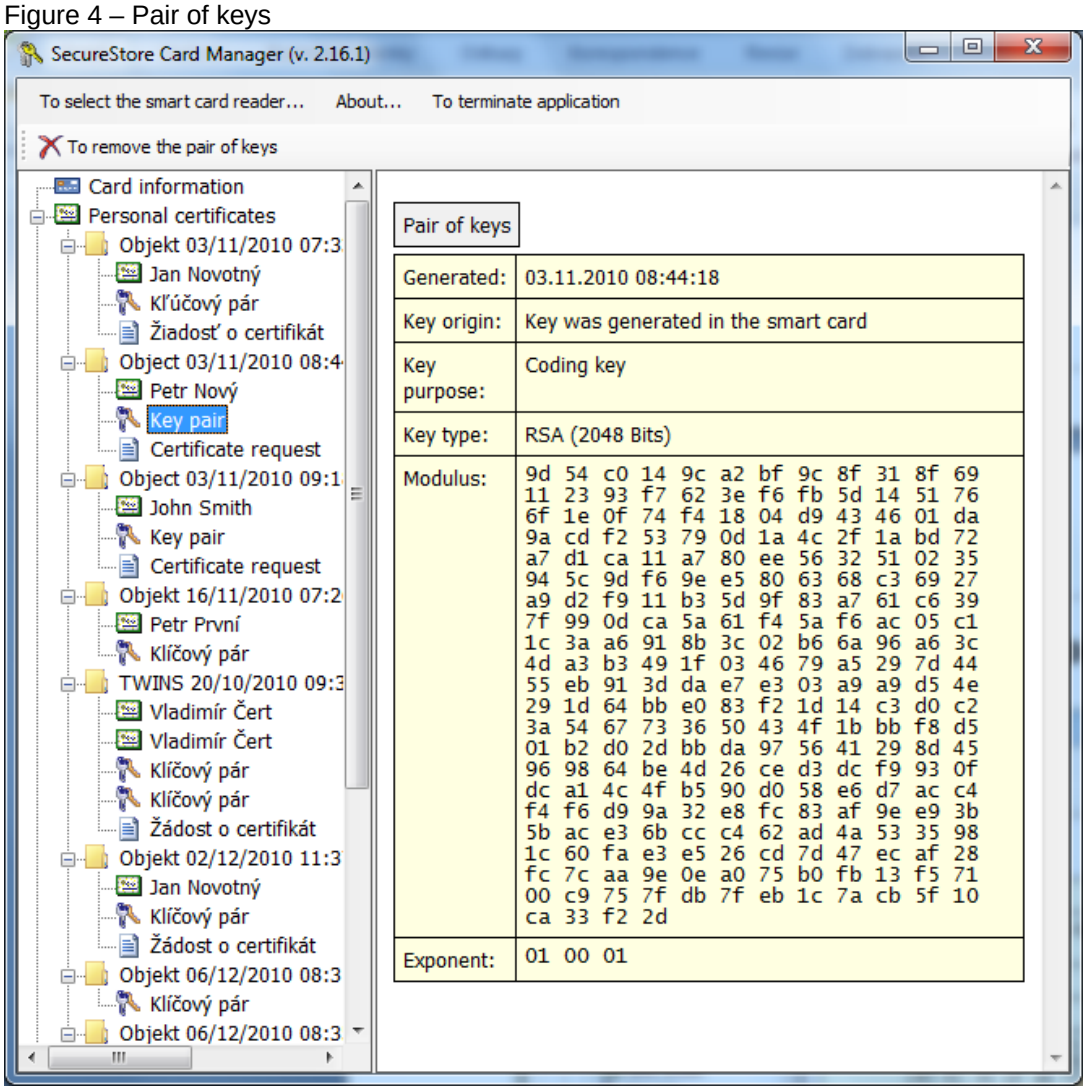


The **"Unlock PIN"** option allows setting a new PIN value in case you lock you PIN. PIN is locked after entering 3 incorrect PIN values. Entering the PUK value is needed to unlock PIN.

The option of **"PIN modification for the protected repository"** allows modifying PIN for a special cart part called the Protected personal repositories.
The option of **"PIN unlocking for the protected repository"** allows unlocking PIN for the Protected personal repositories.

4. Displaying information about the pair of keys

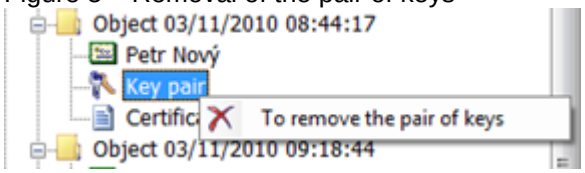
Figure 4 – Pair of keys



Time of the public/private key generation specifies exact time when they key was generated on the card or imported to the card. This information is displayed by the “Key origin” item.
In the “Key purpose” item, it is indicated whether this is the cryptographic or signature key.
Furthermore, the key type is indicated here: in our case, it is the key for the RSA algorithm with the length of 2048 bits.
It is followed by the hexadecimal list of exponent and module of the public key for visual inspection.

Keys may be removed from the card through the option of “To remove the pair of keys”. This option is available after clicking the right-hand mouse button on the particular key pair, see the figure below.

Figure 5 – Removal of the pair of keys

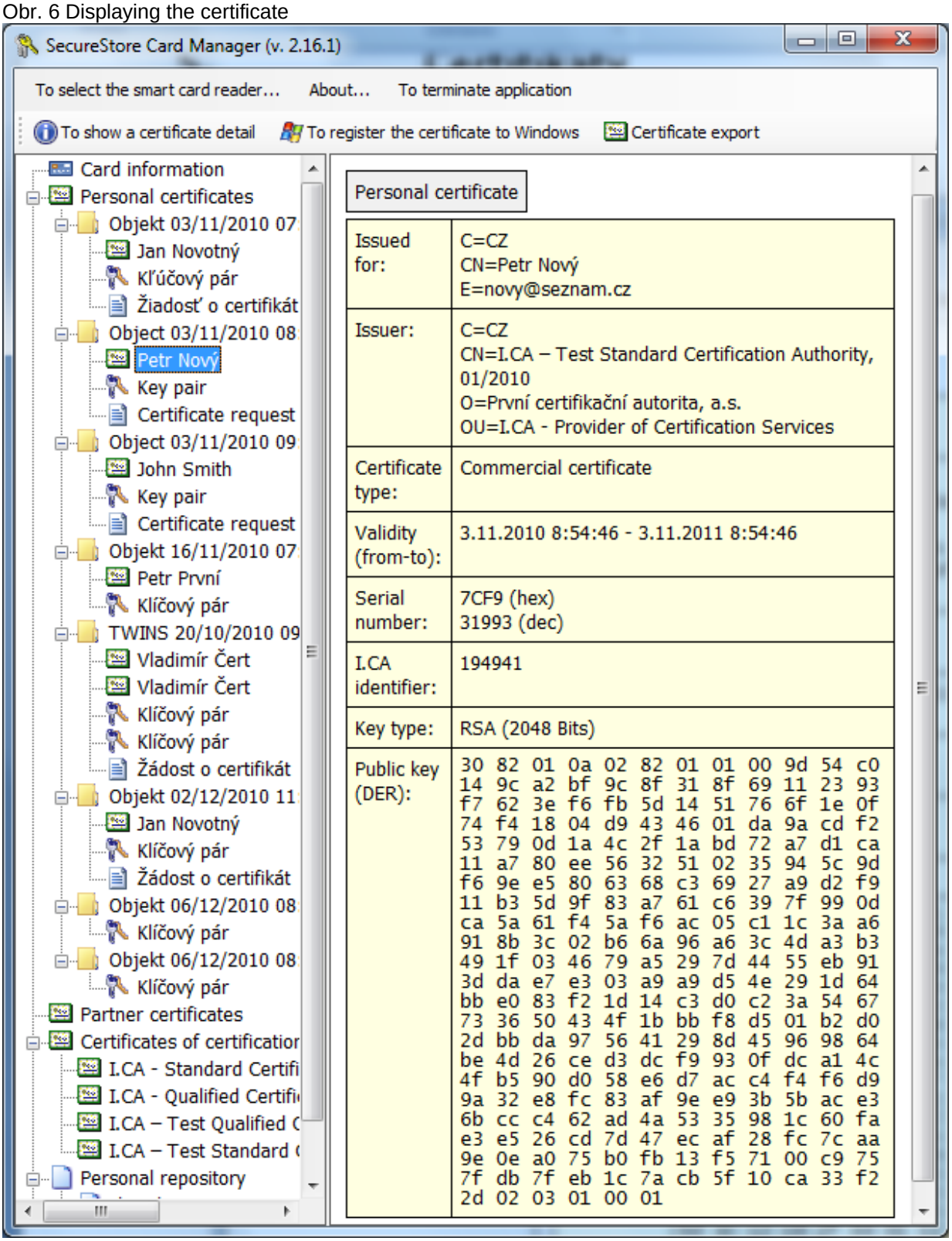


The option of “To remove the pair of keys” will irreversibly remove the pair of keys from the card (i.e. both the private and public keys will be deleted). If the private key for a private certificate is removed, it is not possible to sign and decipher with the certificate anymore!

5. Certificates

5.1 Displaying the certificate

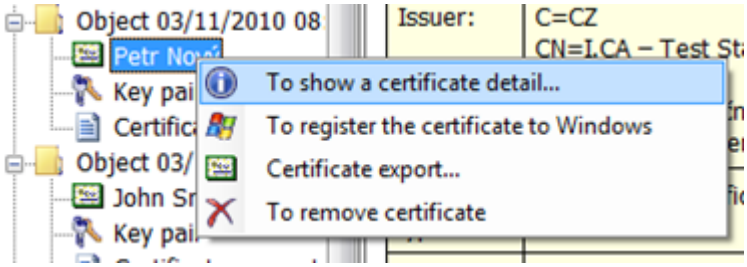
Obr. 6 Displaying the certificate



5.2 Work with the personal certificate

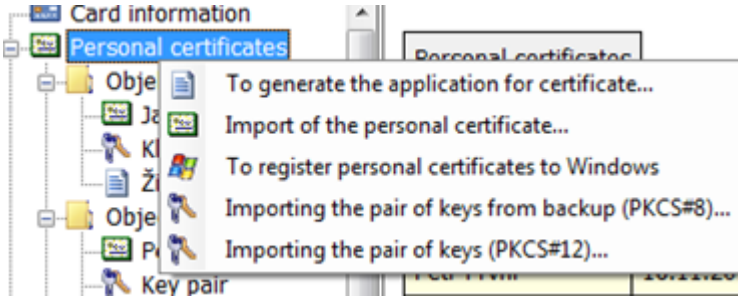
Options for working with the certificate stored on the card are accessible after clicking the right-hand mouse button on the particular certificate, see the figure below.

Figure 7 – Options for working with the personal certificate on the card



Options for the certificate import to the card are available after clicking the right-hand mouse button on the personal certificates item, see the figure below.

Figure 8 – Options for import and registration of a personal certificate



If the repository containing the appropriate key pair (private and public) is not found on the card during the personal certificate import, the certificate will be imported as the certificate of partners.

The certificates for which you do not have a private key and that are not considered trustworthy CA certificates are imported as partner certificates.

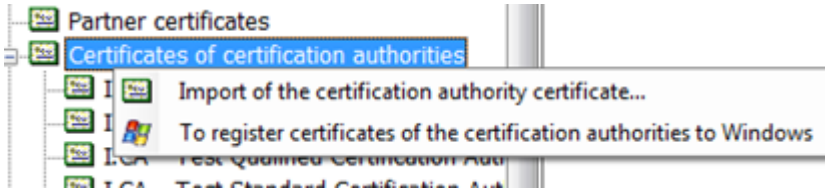
Displaying the raw certificate data is intended only for experts to check the certificate data visually.

5.3 Work with the root certificate of the certification authority

The new card contains the necessary root certificates of the certification authority that are stored in the part of “Certificates of certification authorities”.

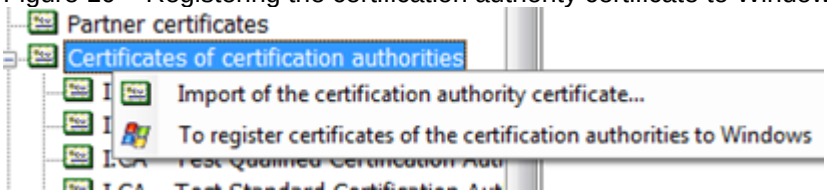
The certificate can be imported as the CA certificate only in case it is the certificate of a permitted CA for the particular card. Certificates of other CAs or the newly issued CA certificates can be imported in the cmf format.

Figure 9 – Import of the certification authority certificate



The root I.CA certificates constitute a part of Windows. If you need to register root certificate for a card, use the option “To register the certificate to Windows”, see Figure 10. The root certificate is registered to MS Windows as a trustworthy root certificate. This export requires confirmation of registration for MS Windows.

Figure 10 – Registering the certification authority certificate to Windows



A mass registration of root certificates is allowed by the option “To register certificates of the certification authorities to Windows" button, see Figure 9.

5.4 Registration of personal certificate to Windows

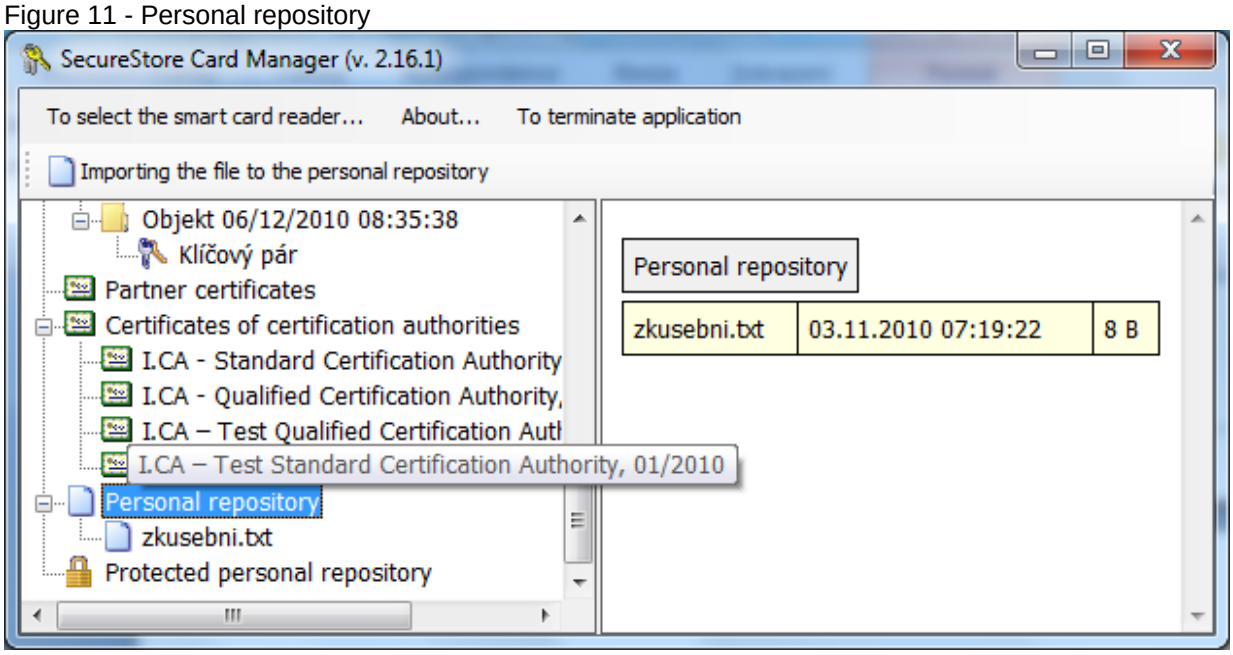
Registration of certificates can be accomplished individually for each certificate by the option “To register the certificate to Windows”, see Figure 7.

Registration of an individual certificate to MS Windows will export the certificate to the certificate repository of MS Windows. In case of personal certificate, export to the personal certificates repository takes place and the certificate is exported without the private key: it will stay on the card and will never leave it. It is possible to encrypt and sign with such registered certificate by using a card with a private key.

A mass registration of personal certificates is allowed by the option of the “To register personal certificates to Windows", see Figure 8.

6. Personal repository

Figure 11 - Personal repository



You can save small files (a few kB) to Personal Repositories; they will be ready at hand and protected on the chip card. On the card, you can save both the text file and the binary file.

It is possible to import both to the protected and to the public repositories. For the option of protected (secured) repositories, you will be asked to enter PIN for protected repositories (different from the main PIN). If this option is used for the first time, the request to setup the PIN for protected repositories will be simultaneously displayed.

Figure 12 – Importing the file to the personal repository

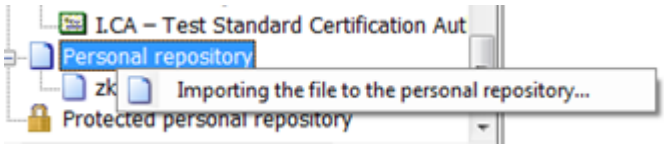
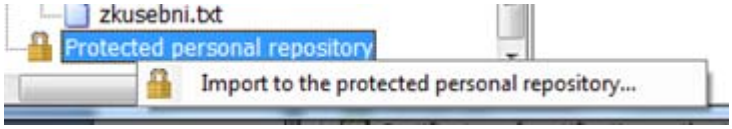


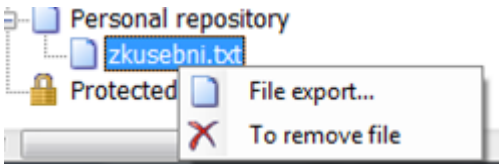
Figure 13 – Importing the file to the protected personal repository



To display the items in the protected repository, you must enter PIN for the protected repositories.

The files stored in the personal repository can be exported; for their export, enter the whole file name including its suffix.

Figure 14 – Exporting the file from the personal repository



7. Application control

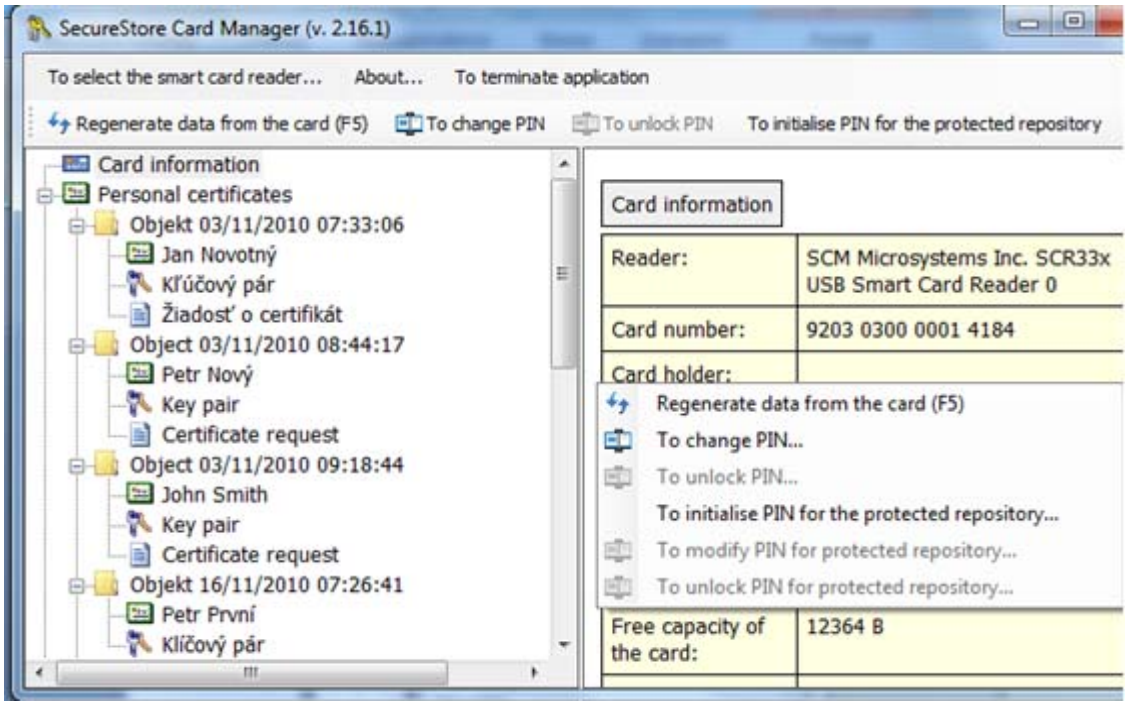
The individual application functions are realised by means of context menu. Context menu can be opened in two ways:

- Clicking the tree item in the left part of the screen with the right-hand button
- Clicking over the right screen area with the right-hand button; there is information about the selected item from the left part of the screen.

7.1 Context menu for Card Information

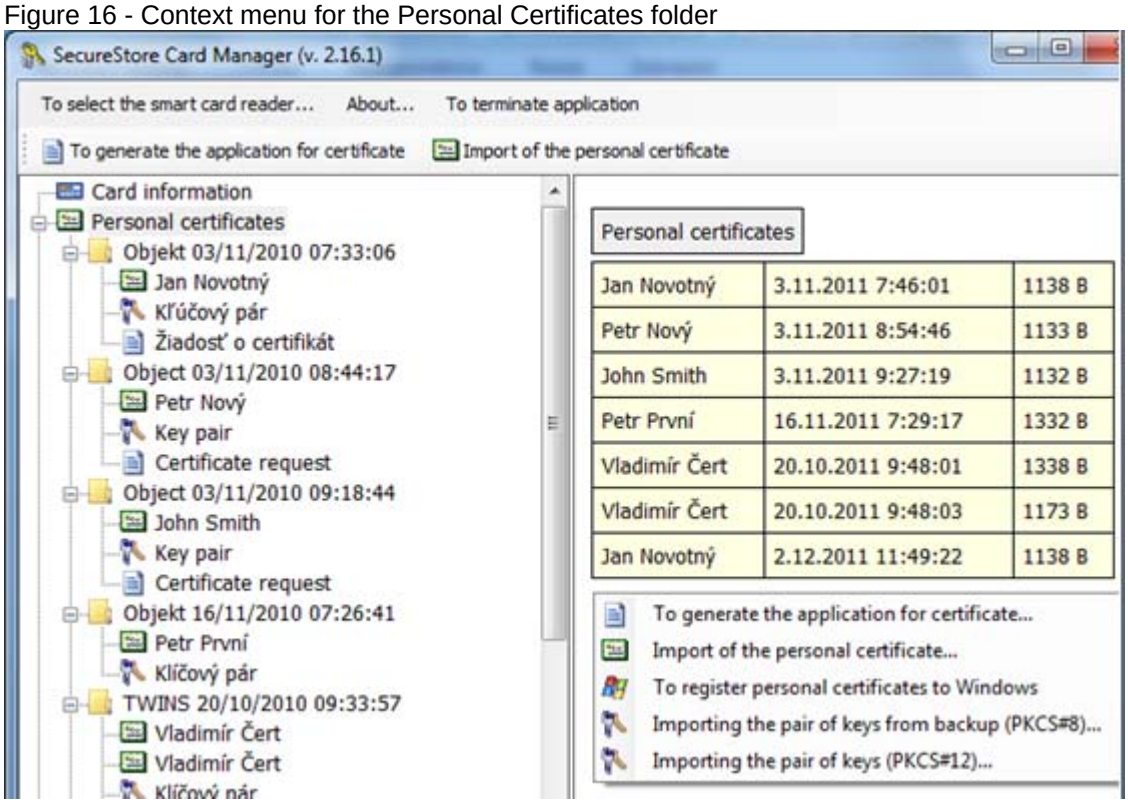
It includes basic administrative operations concerning the card that are associated with PIN and PUK administration and with repeated data download from the card.

Figure 15 – Card Information



7.2 Context menu for the Personal Certificates folder

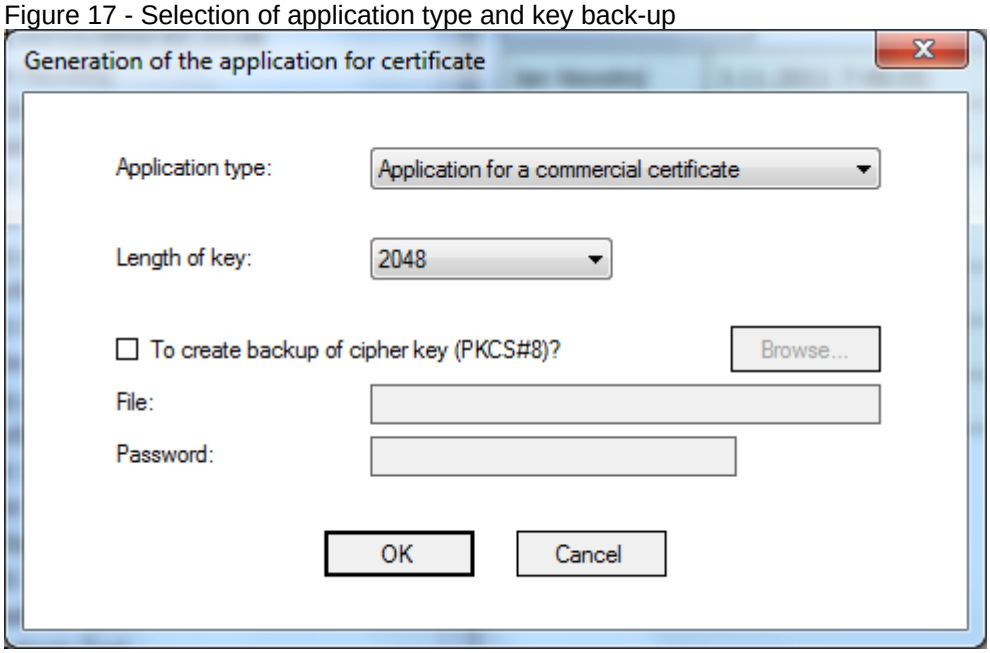
Figure 16 - Context menu for the Personal Certificates folder



7.2.1 Generate application for certificate

It allows generation of an application for certificate. Select the type of application for certificate and enter the request to back-up the key for the cryptographic certificate.

Figure 17 - Selection of application type and key back-up



The key length may be 1024 bits or 2048 bits. A key of a 2048-bit length is longer and safer. A key of 2048-bit length is required for the I.CA certificates.

Cryptographic keys can be generated with back-up that is stored outside the card. They will be stored to the secured PKCS#8 file with a password that you will enter in the window, see Figure 17.

The signing keys are generated directly on the card, and it is not possible to export the private key outside the card.

The keys will be generated after confirmation of this dialog: it can take tens of seconds up to 1 minute.

Subsequently, the NewCert application will be launched and it will generate the application for certificate.

Figure 18 - Selection of the certificate type in the NewCert application.

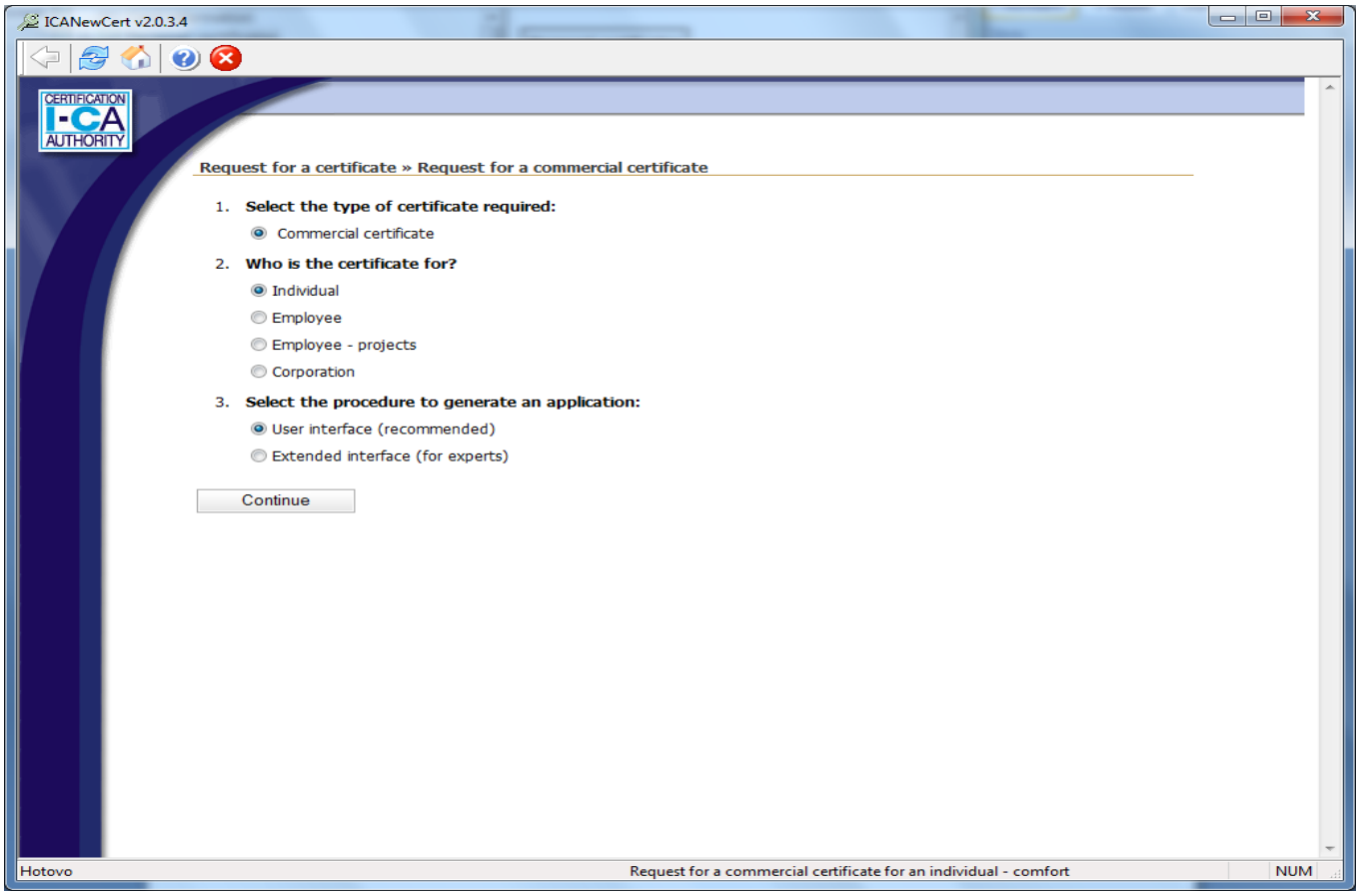


Figure 19 – Personal data setting

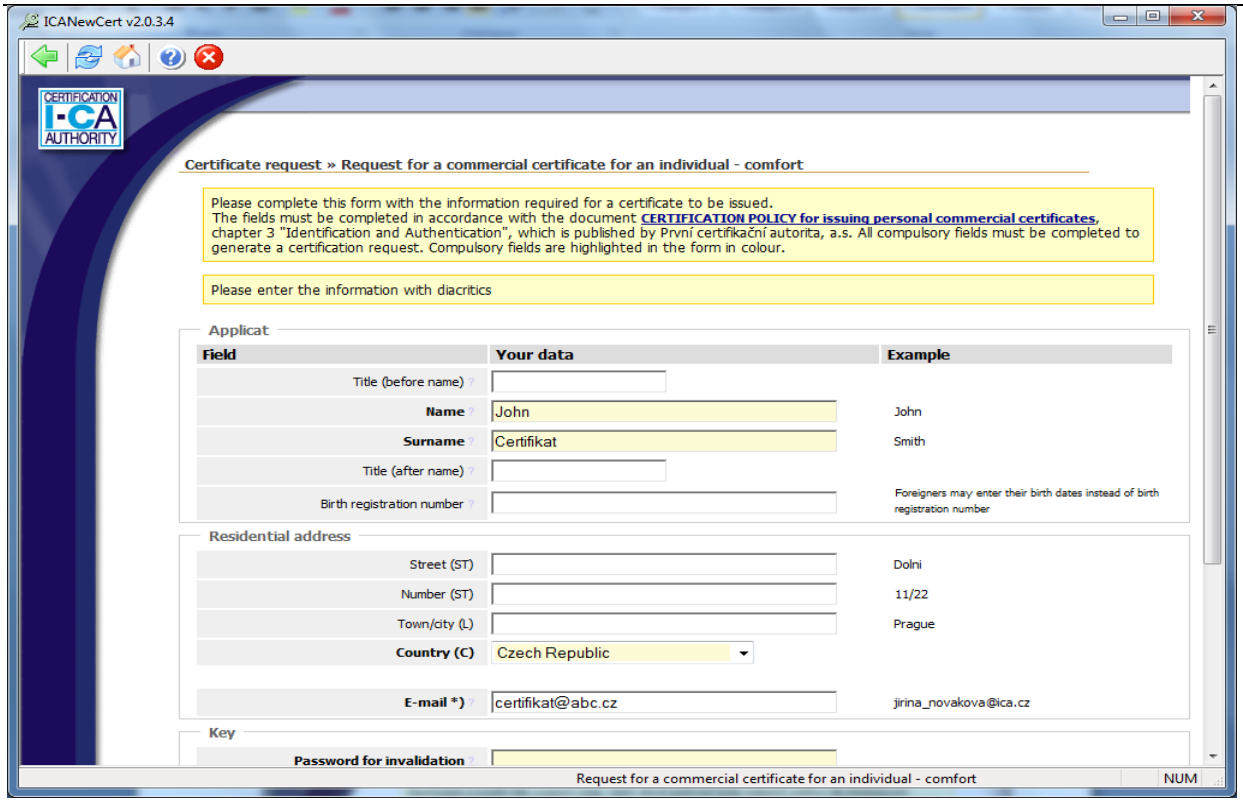


Figure 20 – Confirmation of data provided for the application

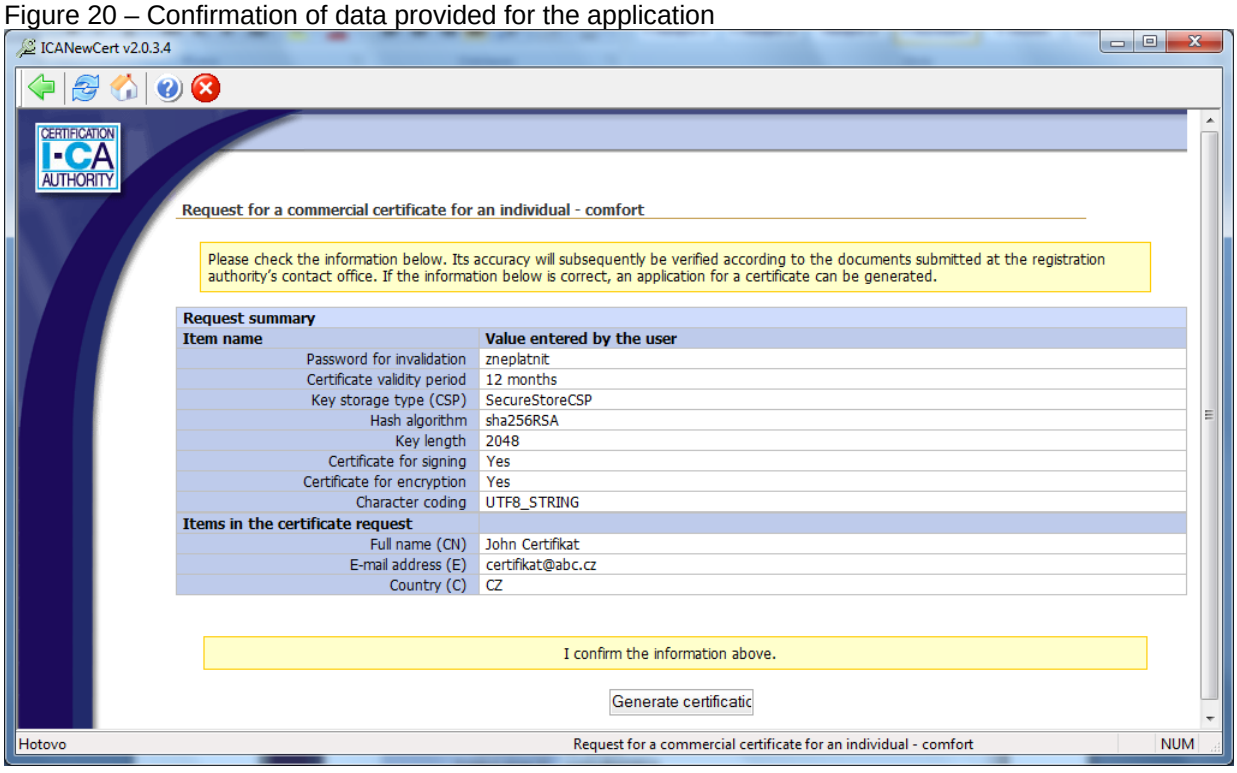
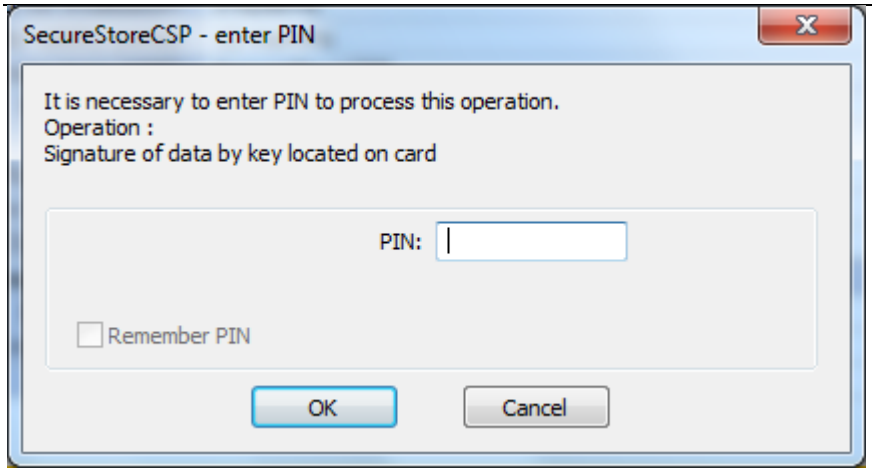


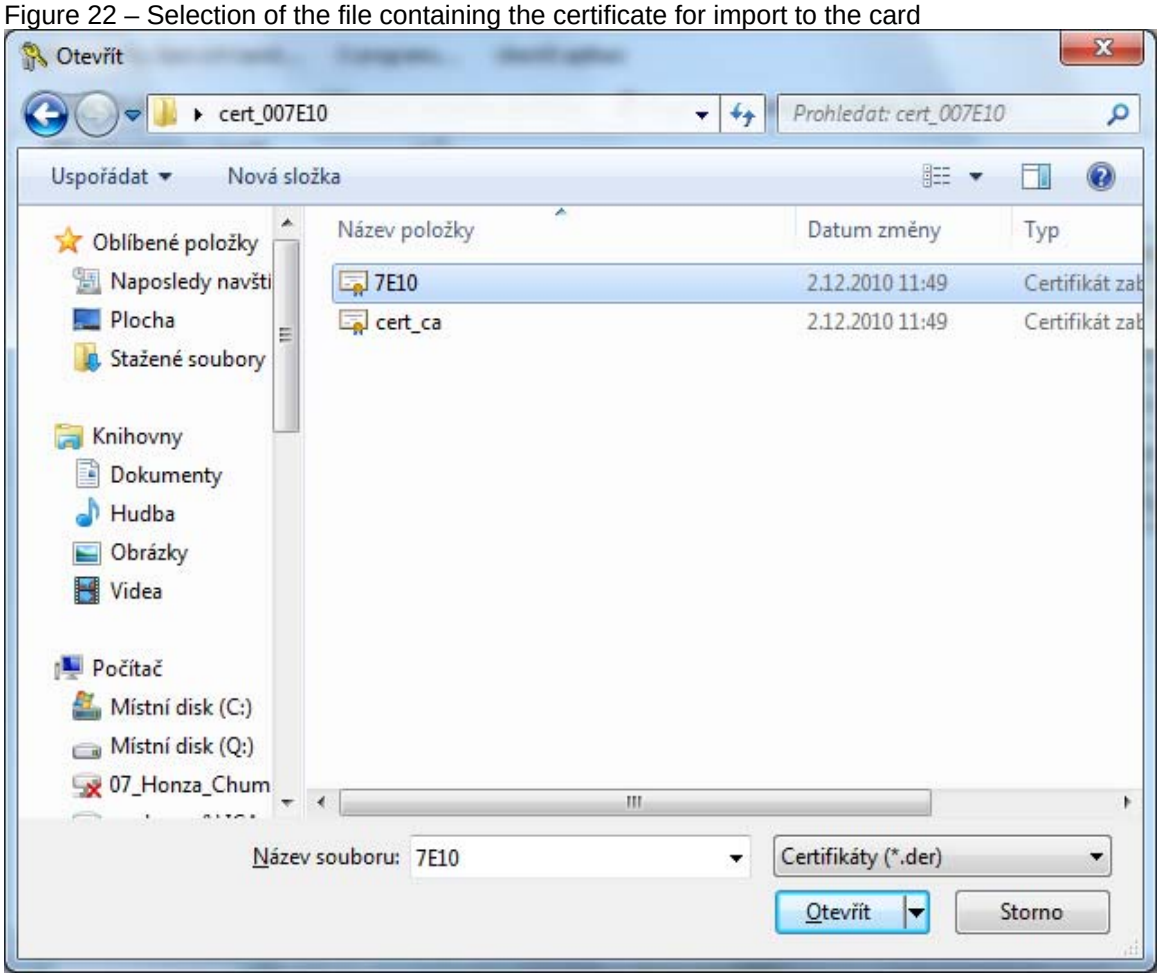
Figure 21 – Entering PIN to sign the application



7.2.2 Import of personal certificate

This feature allows importing the personal certificate from disc to the card. The certificate is imported in the .der format.
The imported certificate is saved to this repository on the card and it contains the keys to the certificate. If there is no repository with the corresponding keys on the card, the certificate will be stored to the card part marked as “Partner certificates”.

Figure 22 – Selection of the file containing the certificate for import to the card



7.2.3 Register personal certificates from Windows

This option will register all personal certificates from the card to the personal repository in Windows.

7.2.4 Import of the pair of keys from backup (PKCS#8)...

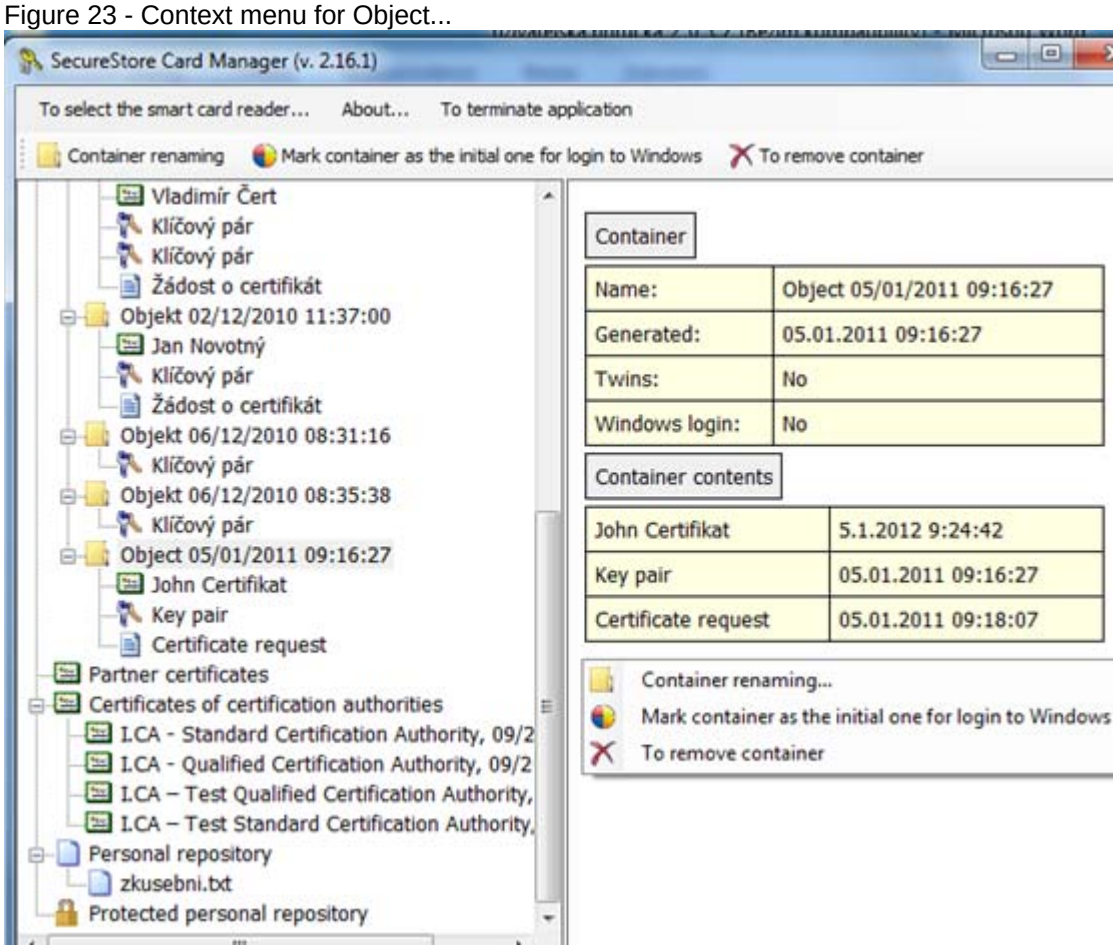
This option imports the keys, which were stored to the disc during the generation process of the application for a cryptographic certificate, to the card.

7.2.5 Import of the pair of keys (PKCS#12)...

This option imports the keys, which are stored in the PKCS#12 format on the disc, to the card.

7.3 Context menu for Object

Figure 23 - Context menu for Object...



7.3.1 Renaming a container

This option allows renaming a selected container.

7.3.2 Marking a container as the initial one for login to Windows

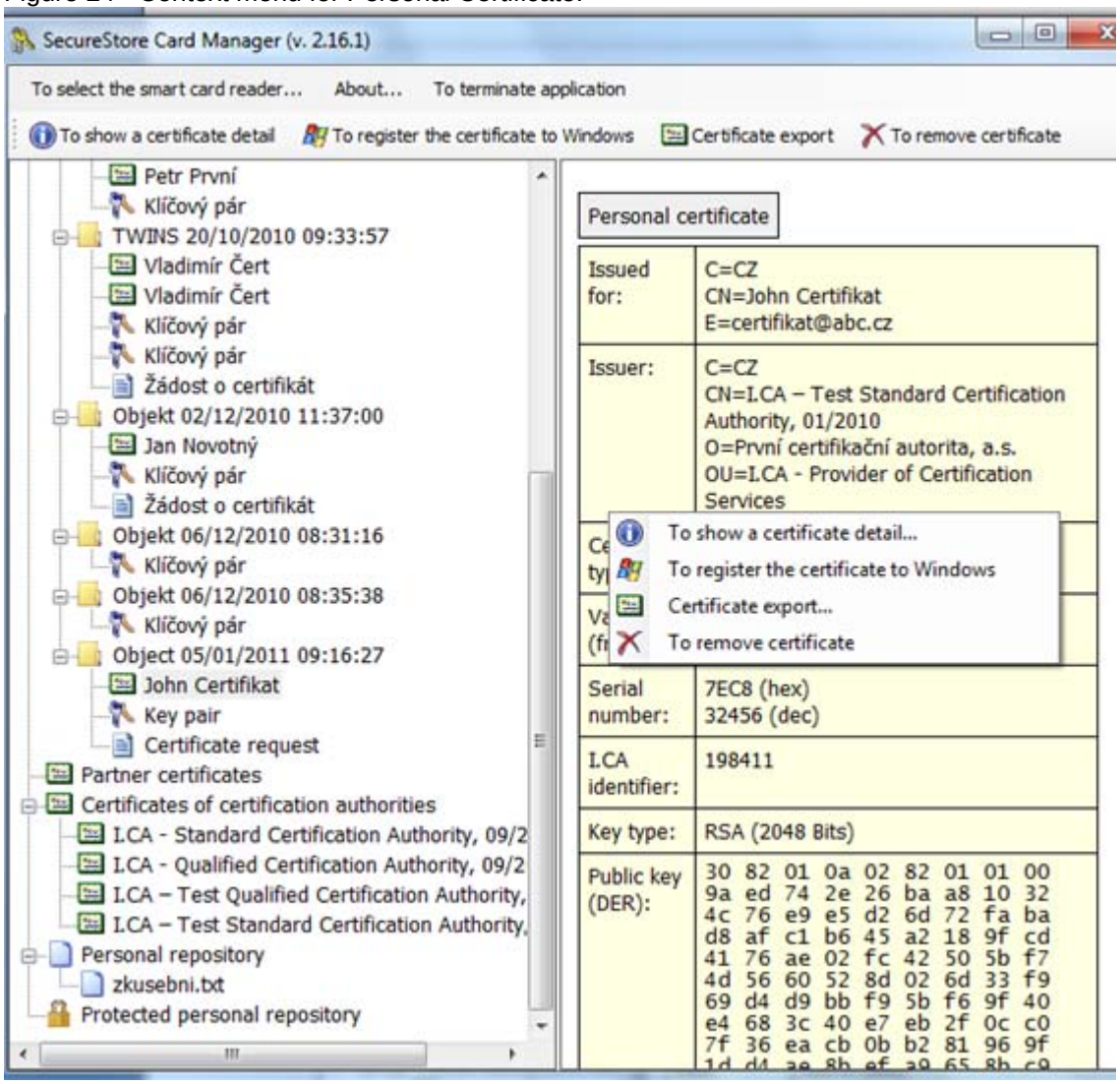
This option allows marking a selected container as the initial one for login to Windows. The certificate and key from this container will be used for login to Windows.

7.3.3 Removing a container

This option allows deleting a container from the card, including the certificates and keys it contains.

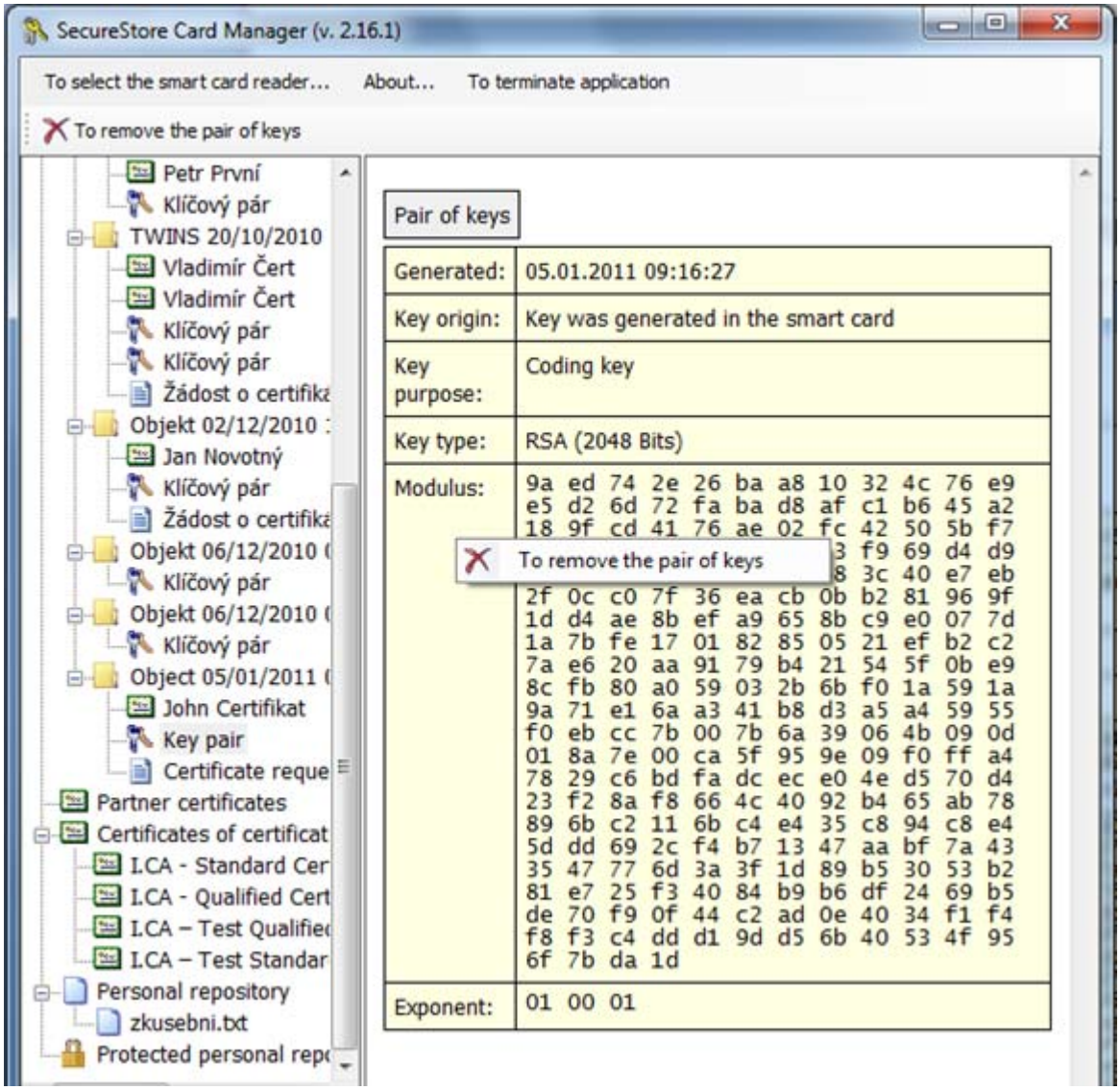
7.4 Context menu for Personal Certificate

Figure 24 - Context menu for Personal Certificate.

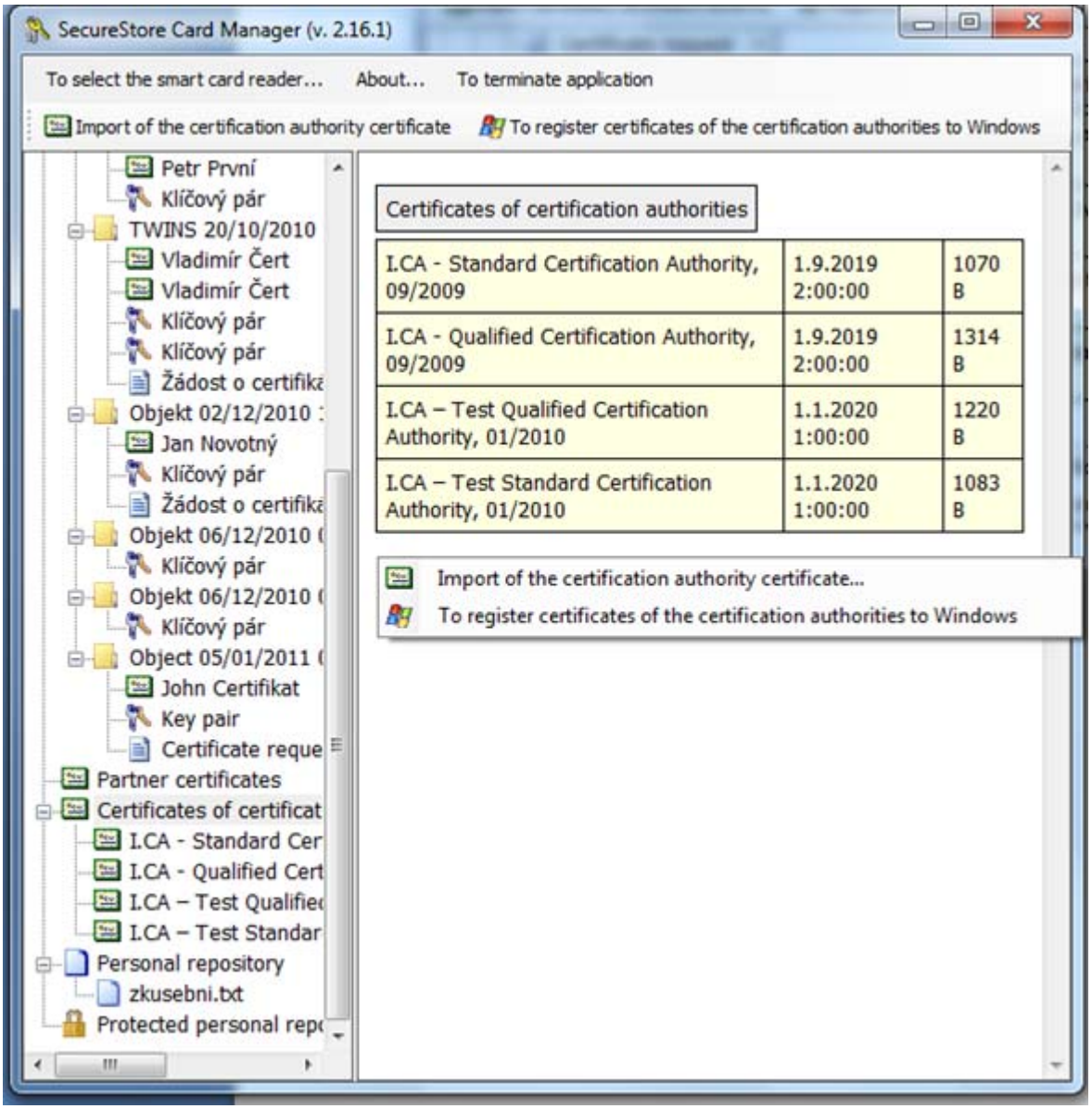


Context menu will open for the selected Personal Certificate.

7.5 Context menu for the pair of keys



7.6 Context menu for the CA Certificates folder



8. Concepts

- Certification authority
  ...is an independent trustworthy entity issuing the certificate to the client. The certification authority guarantees the unambiguous link between the client and his/her certificate.

- Registration authority
  ...is the contact office for communication with clients. In particular, it accepts applications for certificates and delivers certificates to the clients. These offices verify identity of the applicant for certificate and compliance of the application with the presented documents. Registration authorities do not issue certificates; they only apply for them at the central office of I.CA.

- Cryptographic operations
  ... are operations using the keys for encryption and decryption. In case of the chip card, the so-called asymmetric cryptography is used: a pair of keys is used for encryption and decryption, as well as for generation and verification of electronic signature.

- Electronic signature
  ... is the data in electronic form; they are attached to the data message or are connected to it in a logic manner and they enable verification of identity of the undersigned person in relation to the undersigned message.

- Data for generation of electronic signature
  ... are the unique data used by the undersigning person to generate electronic signature (within the meaning of the Act on Electronic Signature); they include the private key of the appropriate asymmetric cryptographic algorithm (here RSA).

- Chip card
  ... is a tool for a safe saving of the private user key and a tool to generate electronic signature. On the chip card, there are private keys, certificates of certification authorities, client certificates and other data as well.

- PIN and PUK
  ... is the protection of access to the card, i. e., when saving data to the card or using private keys from the card. Protecting codes can be set up on the card in advance and the user will receive those values in the so-called PIN envelope, or the client will set up the PIN and PUK values in the card himself/herself.

- PIN envelope
  ... is a letter that the client can receive together with the card. PIN envelope belongs to the particular card; it includes the unambiguous card identification and the PIN and PUK values. The PIN envelope is not supplied with every card.

- Repository
  ... is the storage space on a medium (disc, chip card) where the pair of keys is saved together with the certificate. The chip card may contain up to 8 various repositories at a time. The chip card repository has its unique name. The SIGNATURE type of repositories does not allow generating backups of keys when generating the application for certificate. All certificates for which the key backups are generated are saved to the OTHERS type of repositories.

- Application for certificate
  ... starts with filling out the form that includes data about applicant. The generated public key of the applicant is attached to the information provided by the applicant in the request form and the whole structure is signed by the applicant private key. Application for certificate is the digital data that contain all information needed to issue the certificate. The user can generate the application for certificate by means of the ComfortChip programme or at the webpage of I.CA www.ica.cz.

- Certificate
  .... is an analogy of the identity card; the client proves his/her identity by it in electronic communication. Acquisition of the certificate is very similar to the standard procedures for issuance of the identity card. I.CA provides those services through the network of contact offices – registration authorities that implement requirements of their clients. The certificate is unambiguously linked with the pair of keys that the user utilises in his/her electronic communication. The pair of keys consists of the so-called public key and private key.

- Public key
  ... is the public part of the user pair of keys; it is intended to verify the electronic signature and to encrypt if need be.

- Private key
  ... is the secret part of the user pair of keys; it is intended to generate electronic signature and to decrypt if need be. It is necessary to ensure the highest security for the use of the private key. Therefore, the chip card is used for storing the key. The private key used for decryption must be saved for the whole existence period of the encrypted documents and messages. The user can save this key on the card and we recommend storing it also in a back-up medium.

- Validity period of the certificate
  Every certificate is issued for a definite period. The validity period is indicated in every certificate. The certificate used for electronic signature is useless after expiry of its validity period. The certificate used for encryption must be stored even after expiry of its validity period so that the older messages may be decrypted.

- Commercial Standard Certificates
  Standard Certificates represent personal certificates suitable for common use. They are issued for natural or legal persons based on the duly completed application for certificate; the application is handed over to the contact office of I.CA along with presentation of the required documents needed to verify the applicant's identity.

- Commercial Comfort Certificates
  Comfort certificates represent personal certificates whose main difference from the standard certificates consists in the chip card that is a part of this service. It works as a medium for safe data storage to generate an electronic signature and for a safe creation of electronic signature. This service is mainly intended for corporate purposes; however, it is rendered to natural and legal persons, too.

- Qualified certificate
  .... is strictly governed by Act no. 227/2000 Coll., and is exclusively intended for the electronic signature area. Generation, administration and use of a qualified certificate are governed by special relevant certification policies.

- Client Commercial Certificate
  ... is issued to natural or legal persons based on the duly completed application for certificate; the request is handed over to the contact office of I.CA along with presentation of the required documents needed to verify the applicant's identity. Validity period of these certificates always depends on the length of the cryptographic key used.

- Client certificate
  ... is issued to the client of I.CA based on the duly completed application for certificate; the request is handed over to the contact office of I.CA along with presentation of the required documents needed to verify the applicant's identity. In case of I.CA, the certificate may be either commercial or qualified.

- Certificate of certification authority
  ... is used to verify authenticity and trustworthiness of client certificates. By its installation on his/her PC, the user declares his/her trust in such certification authority to the operation system. In real terms, it means that if a user receives a message that is electronically signed with the certificate signed by this certification authority, the system accepts it as a trustworthy one. Otherwise, the message appears as untrustworthy.

- Certificate for login to Windows
  Certificate for login to Windows must include specific data. Therefore, it is not possible to use any certificate for login to Windows. On request, the I.CA registration authority will issue the right certificate for login. The card repository containing the login certificate must be marked for authentication. Only one repository may be marked for authentication on the card.

- List of public certificates (commercial)
  ... is a list of certificates issued by I.CA for which their owners agreed to make them public. There are no “testing” certificates and no certificates for which their owner did not give his/her consent with publication.

- List of public certificates (qualified)
  ... is a list of certificates issued by I.CA. Publication of these certificates is regulated by Act no. 227/2000 Coll., on Electronic Signature.

- Certification authorities supported by the card
  Every chip card issued by I.CA contains a defined list of the so-called supported certification authorities whose certificates may be saved on the card.

- Certificate renewal – “subsequent” certificate
  ... is issued to the client after the expiry date of the primary certificate. A subsequent certificate is issued only in case the client does not request changes in the previous certificate items. If he/she requests such changes, it will not be a subsequent certificate, but another primary one. If the subsequent certificate is being issued before the validity of the primary certificate expires, presence of the customer at the I.CA registration authority is not necessary. The client will just send the electronically signed application for issuance of a subsequent certificate in the standardised electronic form using the valid certificate.

- Usage of the key
  - **DigitalSignature (digital signature)** – primarily, this attribute (bit) is set up if the certificate is to be used in association with digital signature, except when assuring non-repudiation, signatures of certificates and lists of certificates invalidated by the certification authority.
    Usage: At present, it is necessary to adjust this bit in cases when the user intends to use his/her private key associated with the issued certificate generally to generate a digital signature (for example, when using the certificate within the safe electronic mail).
  - **NonRepudiation (indisputability)** – this attribute is set up if the public key (through verification of a digital signature) is to be used for proving responsibility for a certain activity of the undersigned person.
    Usage: At present, it is necessary to adjust this bit especially in case of qualified certificates when the user intends to use his private key associated with the issued certificate generally to generate an electronic signature.
  - **KeyEncipherment (key encryption)** – this attribute is set up if the public key is to be used for transfer of cryptographic keys.
    Usage: It is necessary to set up this bit if the user intends to use the certificate for encryption purposes within the secure electronic mail. It is also necessary to set up this bit in the MS Outlook environment, if the user does not have other certificate that can be used for encryption.
  - **DataEncipherment (data encryption)** – this attribute is set up if the public key is to be used for data encryption (except for cryptographic keys).
    Usage: Generally, it is necessary to set up this bit if the public key included in the certificate will be used for encryption of general data, for example documents. For the purposes of a secure electronic mail, it is not necessary to set it up.

- PKCS#12 format
  The RSA keys and certificate can be saved to a single file in the so-called PKCS#12 format that is defined by the PKCS#12 standard. In this format, it is possible for example to export the RSA key certificate from the Windows repository if the private key export is permitted. Contents of the file are protected with a password. This file has a pfx or p12 suffix.