



User guide

proCertum CardManager

Version 1.56

Copyrights of this documentation and software described belong to **Asseco Data Systems S.A.** seated in Gdynia, Poland, ul. Żwirki I Wigury 15. The above rights are secured by act on copyright and derivate laws (Dz. U. No. 24, item 83, of 4th February 1994 with its following changes).

The following documentation is spread on the basis of granted license.

Table of contents

1.	Introduction.....	4
2.	Hardware and software requirements.....	5
3.	Installation process	6
4.	Getting proCertum CardManager application started.	11
4.1.	Options	14
5.	Secure profile.....	15
5.1.	Secure profile initialization	15
5.2.	Generating a new PIN code for the Secure card profile	17
5.3.	Changing the PIN code for the Secure profile	17
5.4.	Changing the PUK code for the Secure profile	18
5.5.	Saving the certificates for the Secure profile	19
5.6.	Removing the certificate from the Secure profile	19
5.7.	Certificate registration from the Secure profile.....	20
5.8.	Reviewing certificate details from the Secure profile	21
6.	Common profile	23
6.1.	Common profile initialization	23
6.2.	Generating a new PIN code for the Common profile	25
6.3.	Changing the PIN code for the Common profile	25
6.4.	Changing the PUK code for the Common profile.....	26
6.5.	Removing the certificate from the Common profile.....	27
6.6.	Certificate registration from the Common profile	27
6.7.	Certificate details from the Common profile.....	28
6.8.	Import of the certificate to the Common profile	29
7.	CryptoCertum Scanner	31
8.	Information about actualization	32
9.	Table of figures.....	33

1. Introduction

proCertum CardManager software is designed for managing profiles installed on a **cryptoCertum** card.

A user friendly interface makes it possible to generate PIN codes for certain certificates, delete certificates from a card by beginners on their own.

Main advantages:

- easy and intuitive handling of certificate profiles found on a cryptoCertum card;
- automatic identification of PCSC readers installed in the system;
- complete management of PIN codes of certificates installed on a card (PIN code amendment, new PIN code entry);
- independent deletion of a certificate from a cryptoCertum card;
- importing a non-qualified certificate onto a cryptoCertum card;
- registration of a certificate found on a cryptoCertum card in the user system;

2. Hardware and software requirements

Please find minimal hardware and software requirements enabling correct operation of **proCertum CardManager** application below:

- browser, Internet Explorer 5.5 (encryption power: 128-bit);
- processor Pentium® 800MHz;
- operating system Microsoft Windows 2000/XP/Vista;
- cryptographic card reader;
- cryptographic card;
- card reader drivers.

3. Installation process

proCertum CardManager application installer can be delivered in following forms:

- as a file **proCertumCardManagerSetup.exe** – usually distributed by Internet sources;
- as an integral part of other applications e.g.: Suscriptor, Auctor IC, cryptoCertum.

To start installation of **proCertum CardManager** application click twice on installer icon.



Figure 1: Installer icon

Note!

To start installation of **proCertum CardManager** application, double click **proCertumCardManagerSetup.exe** file icon (figure above) for one file distribution. For more file distribution double click setup.exe icon.

After the installation starts, the language, in which the installation will be done, is to be selected.

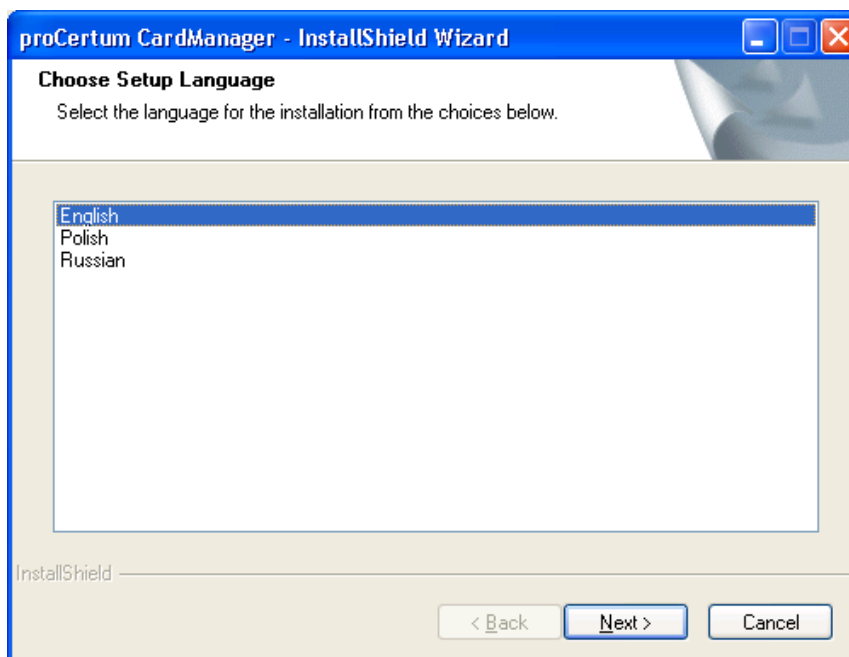


Figure 2: Window enabling the selection of the setup language

After the language is selected click **Next >** the opening window of the install creator starts.



Figure 3: Opening window of install creator

To continue the installation process click **Next >**. To cancel the installation process, click **Cancel**. Dialog window will be displayed, confirming and checking if the installation of **proCertum CardManager** application should be cancelled.

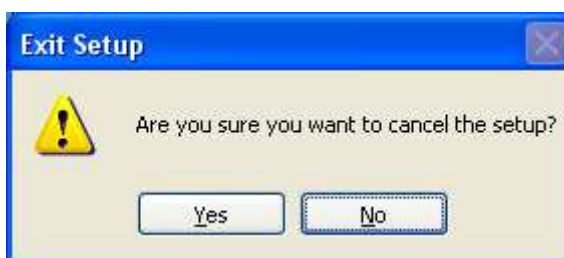


Figure 4: Dialog window – Cancellation of the setup

After clicking **Yes** the installation will be canceled. To return to the main window of the installer click **No**.

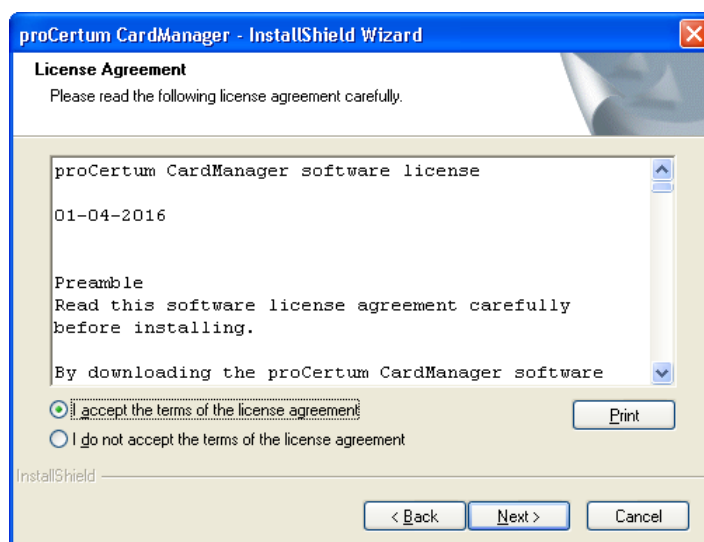


Figure 5: Installer window – License agreement

After you have clicked **Next >** read the license agreement in the installers window. After you have read the conditions, you must click on **I agree to License agreement conditions** and then click on **Next >**. Otherwise (after choosing an option **I do not agree to License agreement conditions**) license terms and conditions will be refused and further installation will not be possible.

The next step will be the selection of the location, where the files of **proCertum CardManager** application should be installed. Defaults to: **C:\Program Files\Certum\proCertum CardManager**. After choosing of final destination, click **Next >**.

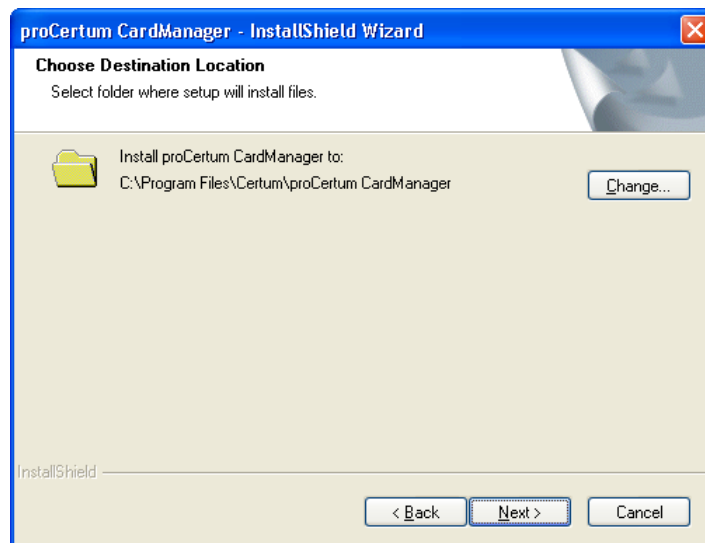


Figure 6: Installer Window– Choose Destination Location

You can change the destination location. To do that, click **Change..** Regular window of Windows explorer will be invoked.

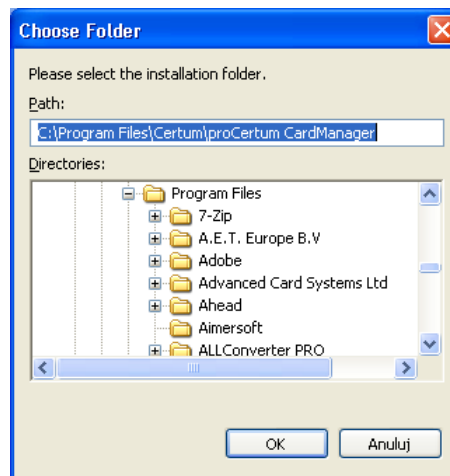


Figure 7: Dialog window – Select installation folder

To confirm the selection of proper folder, click **OK**. The button **Cancel** let you return to the window of application Choose Destination Location, without executing any changes.

After selecting destination folder and clicking on **Next >** install creator is ready for the installation of **proCertum CardManager** software. To get the installation process started click **Install**.

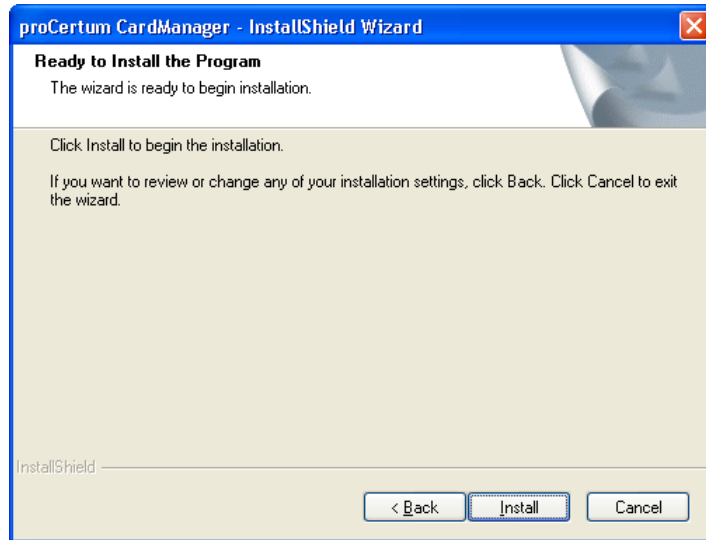


Figure 8: Installer window – Installation status

Installer starts copying process of application files.

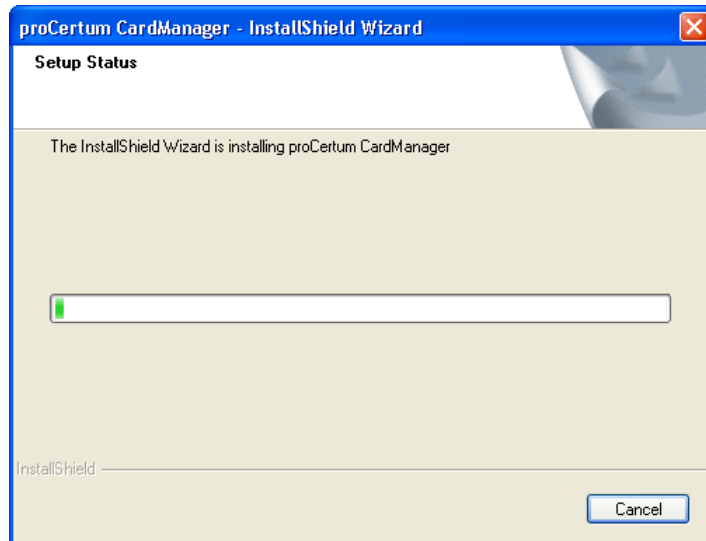


Figure 9: Installer window –Setup status



Figure 10: Installer window – Installation process completed

Clicking **Finish** closes the install creator of **proCertum CardManager** application and finishes its installation.

4. Getting proCertum CardManager application started.

To get the **proCertum CardManager** application started select from the **Start** menu **proCertum CardManager**. The main window of **proCertum CardManager** application will be displayed then.

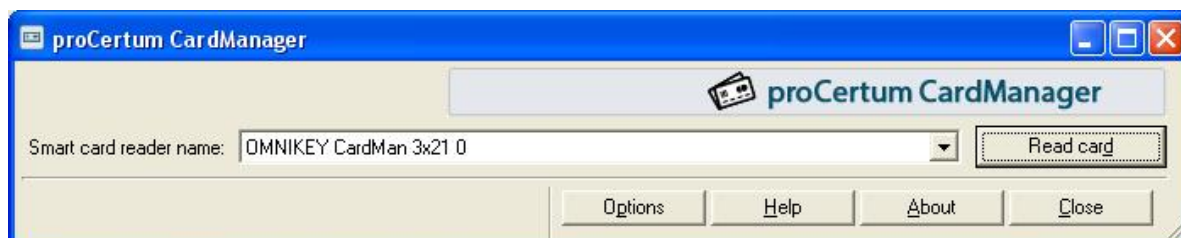


Figure 11: Main window of proCertum CardManager application

If there were more than one card readers installed on workstation, the user should select the proper reader first, which will cooperate with the program. To do that, select **the appropriate reader from the pull-down list**.

The button **Application info** enables checking the version number of the software, libraries used by **proCertum CardManager** as well as license.

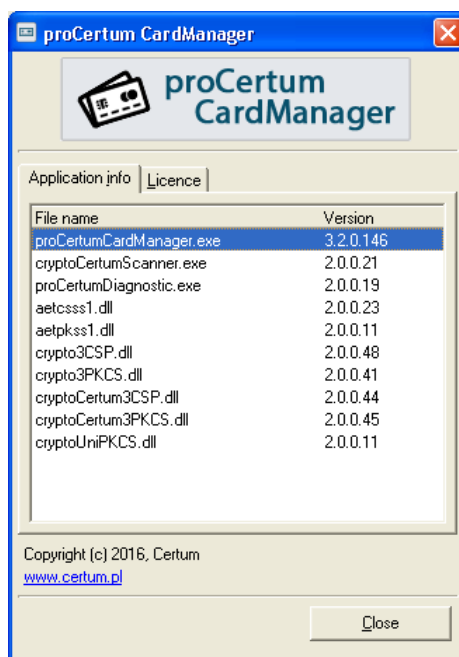


Figure 12: Informing window of proCertum CardManager application

In order to exit **proCertum CardManager** application you should press button **Close**.

proCertum CardManager application enables managing profiles found on the chip card.

Note!

All the possible profiles, which can be found on the card, as well as all the possible options connected with the management of these profiles were discussed in the user guide. The availability of the profiles and the options depend on the kind of delivered card and the life cycle of the card. In practice, not all the described options will be available for the appropriate card.

To read the content from the card, click **Read card**.



Figure 13: Window of proCertum CardManager application with visible tabs of profiles

After the card was recognized, the number of the card and all the profiles found on the card are visible as active tabs. The button **More info >>** additionally displays a table with the list of the profiles and their versions.

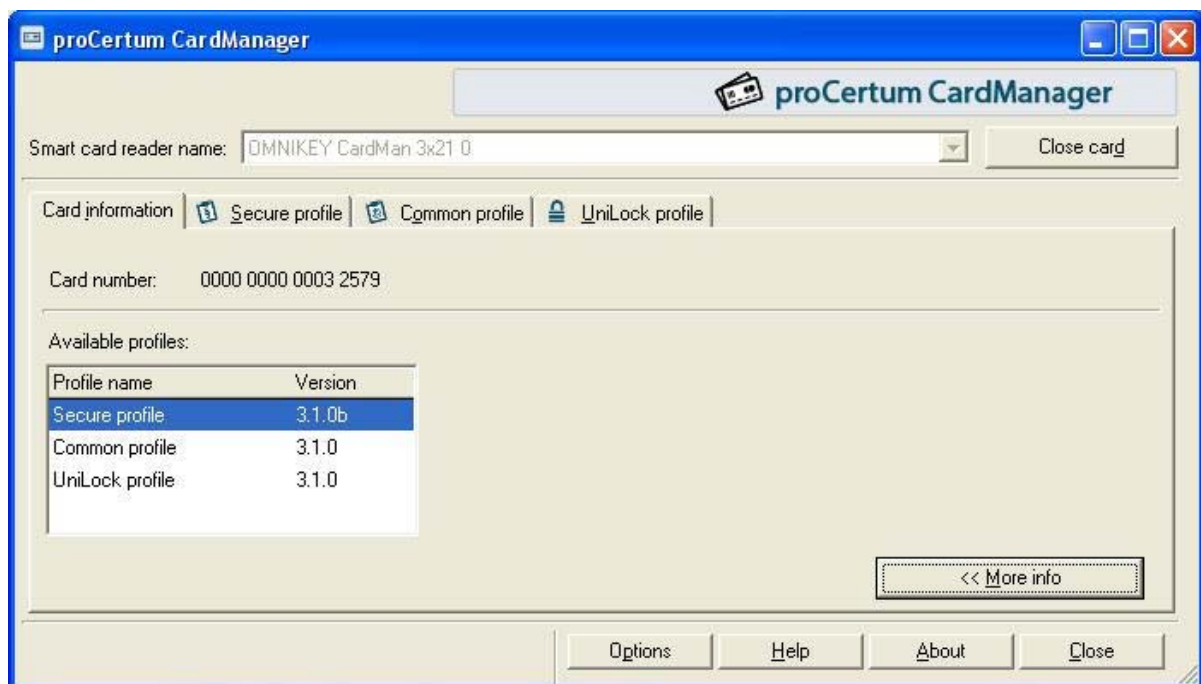



Figure 14: The tab after clicking on More information>>

The service of the appropriate profile is connected with choosing the tab which is corresponding to the profile. During the service, the program is using the file delivered with applications cooperating with this profile. In case of lack of any of the files, the message informing about the name of the file required for correct working of the application will be displayed.

	<p>Problem: Following message is displayed in the main window:</p> <div style="text-align: center;"></div> <p>Reason: The card was not inserted into the reader. Solution: Insert the chip card into the reader.</p>
---	---

	<p>Problem: The card is in the reader but we receive following message:</p> <div style="text-align: center;"></div> <p>Reason: The card was not inserted correctly into the reader. Solution: Insert the chip card into the reader.</p>
--	---

Note!

PIN/PUK term is being used in this Users guide. The PIN/PUK term means PIN/PUK for the card profile mentioned at that moment.

Each profile is separate from others and is protected with individual PIN and PUK code. Blocking of the PIN code or PUK code of one profile does not affect on the status of PIN codes and PUK codes of other profiles. Blocking of the PUK code of one profile is non reversible but it does not affect on other profiles.

Warning!

Three successive incorrect PIN entries will block the profile irreversibly.

PIN and PUK codes for the secure profile and Common profile should have between 4 to 8 marks. The exception is the PIN code for secure profile, which has to be composed of only digits. PIN and PUK codes for the UniLock profile should consist of 5 to 12 marks.

Note!

It is recommended, that PIN and PUK codes should use standard ASCII codes between 32 and 127.

Standard ASCII codes between 32 and 127 are digits, capital letters and small letters of English alphabet as well as following marks: !"#%&'()*+,-./:;<=>?@[]^_`{|}~.

The usage of non-standard marks (other than mentioned above, in particular polish diacritical marks) can affect the possibility of not verifying the entered code on the workstation under the control of other operating system or on the workstation with installed other codepage.

In case of entering non-standard codes, **proCertum CardManager** displays the message warning against possible consequences of this action.

4.1. Options

After pressing button **Options** button it will be displayed Panel which allows to control program options.

Following options are available:

Common profile options:

Show 'Remove Certificate' button – selecting this options will cause that in the tab common Profile will be visible **Remove certificate** allowing you to remove the selected certificate.

Enable PIN cache for CSP-based applications – selecting this option in CSP- based applications after the first providing of the correct PIN cache it will be automatically stored and used in subsequent attempts to use it without having to re-enter it by user.

Secure profile options:

Show 'Remove Certificate' button – selecting this options will cause that in the tab common Profile will be visible **Remove certificate** allowing you to remove the selected certificate.

Enable PIN cache for CSP-based applications - selecting this option in **CSP- based applications** after the first providing of the correct PIN cache it will be automatically stored and used in subsequent attempts to use it without having to re-enter it by user.

Options for storing the PIN cache is **enabled** by default. Whereas the options for deleting certificates are **disabled** by default. This means that the user who wants to delete the certificate will have firstly to turn on the appropriate option.

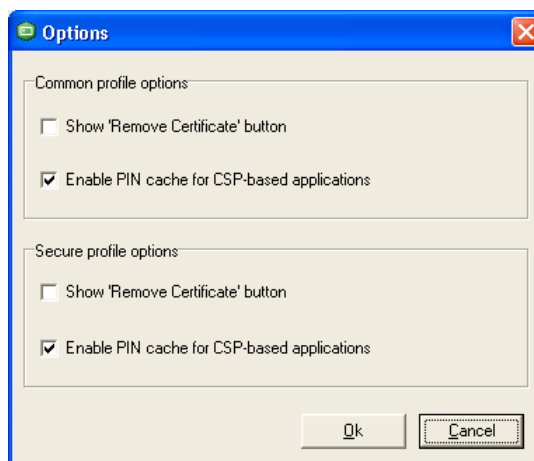


Figure 15: Options

5. Secure profile

If you want to manage a profile for qualified certificates select tab **Secure Profile**.

As a result a window informing about the chosen card profile and a certificate list located on this profile will be displayed.

Note!

For managing **Secure Profile**, Authentication Module might be required.

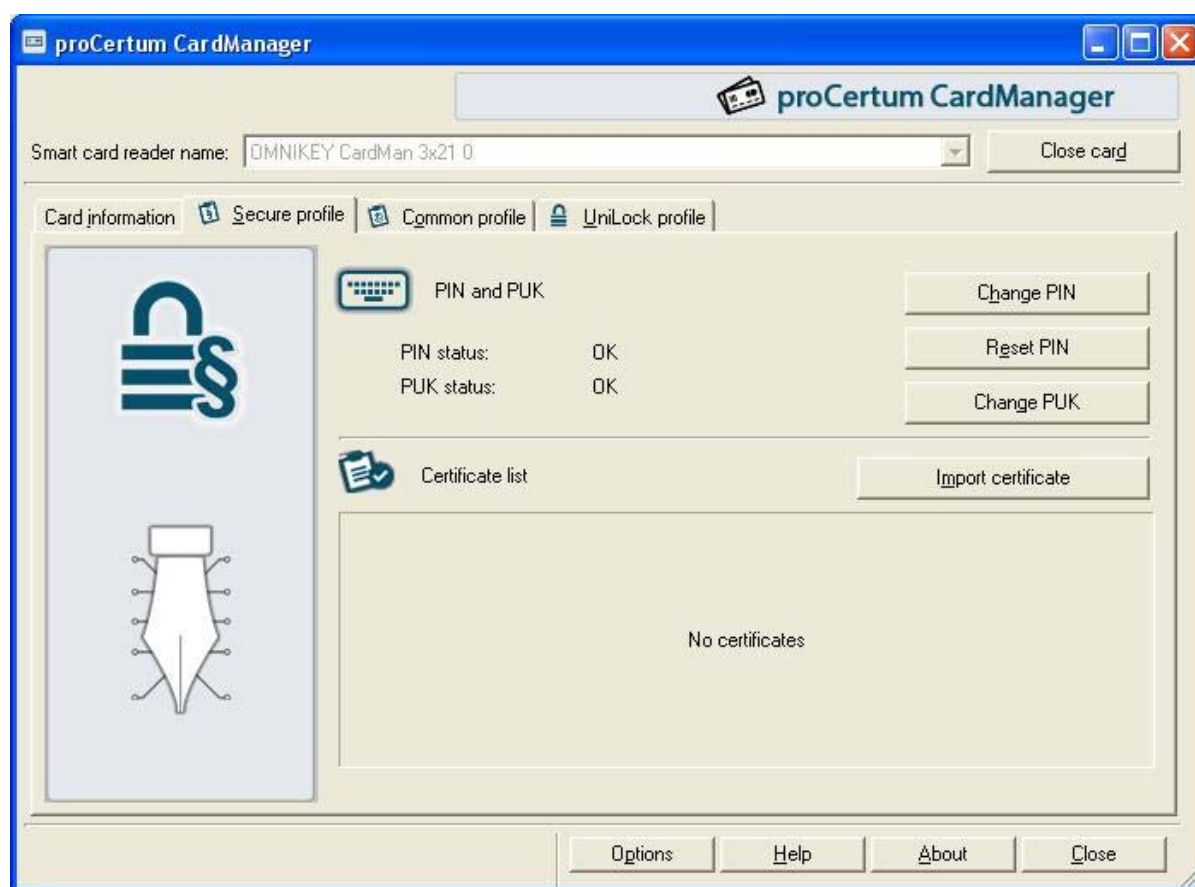


Figure 16: The tab of the Secure profile

5.1. Secure profile initialization

Note!

User usually receives card with already initialized profiles. Therefore the user does not have to initialize the profiles.

Chip card can be also delivered with non-initialized profile. It means that the tab with the name of the profile will appear in the main window of **proCertum CardManager** application. The profiles can be non-initialized aside from the others.

When the profile is not initialized, it means that it is empty and there were no PIN or PUK codes defined for this profile.

Non-initialized profile cannot be used (you cannot for example generate a pair of keys or save certificate). During the initialization process the user defines PIN and PUK codes for the profile. Applications supporting operation of cryptographic cards do not detect non-initialized profile.

To initialize the profile, click **Init profile** and then define a new PUK and a new PIN code. You will be asked to confirm the entered code each time. To accept changes click OK. After initialization of the profile it is ready to work.

Warning!

Second initialization of the profile is impossible. It is also not possible to restore the status to the status before the initialization.

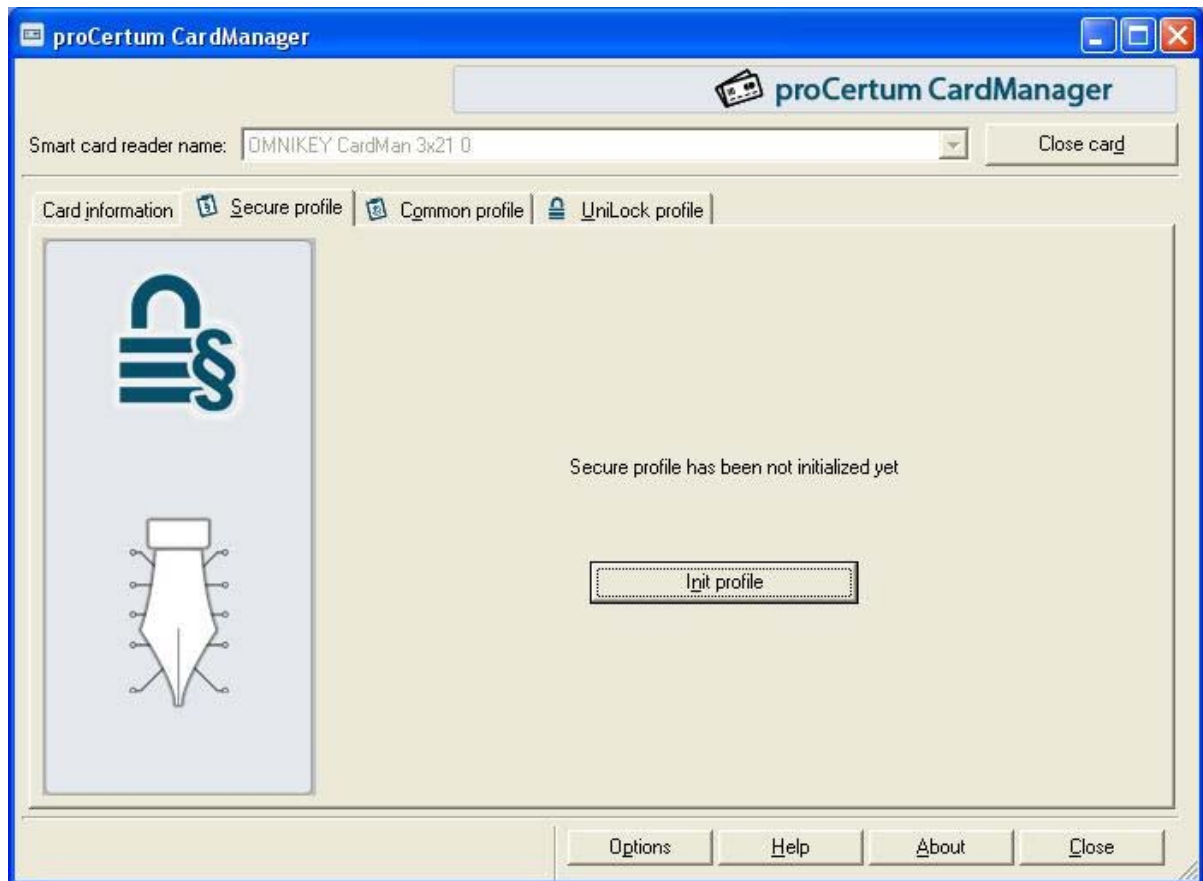


Figure 17: The tab of the Secure profile – non-initialized profile

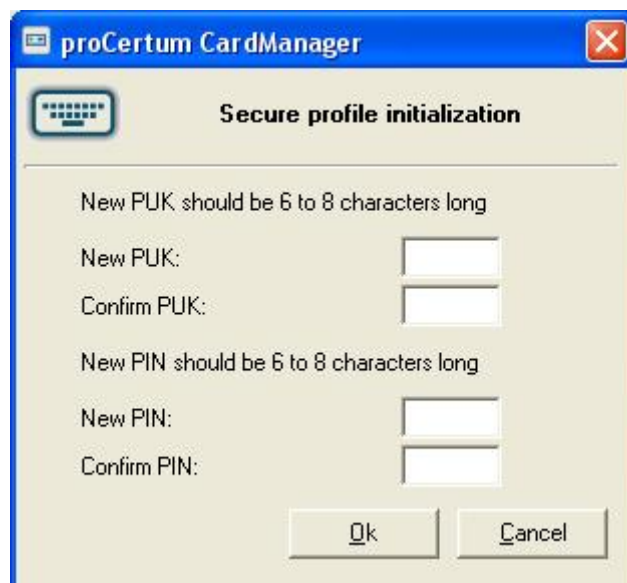


Figure 18: Dialog window –Secure profile initialization

5.2. Generating a new PIN code for the Secure card profile

Defining a new PIN code is certainly required for the correct usage of the card.

During the first start of the **proCertum CardManager** application with a new card, it is required to define a new PIN code.

To generate a new PIN code click on **New PIN**. The following window will appear:



Figure 19: Dialog window – Generating a new PIN code for the Secure profile

The user will be asked to enter the PUK code and to define a new PIN code. Furthermore the user will be asked to confirm the entered code. To confirm the entered PIN click **OK**. To quit from generating new PIN code and to save previous settings click **Cancel**. The **proCertum CardManager** application will confirm the correctness of entered data.



Figure 20: Window informing about the accomplishment of the operation of generating the new PIN code.

5.3. Changing the PIN code for the Secure profile

To change the PIN code, select **Change PIN**. Following window should appear:



Figure 21: Dialog window – Changing the PIN code for the Secure profile

You will be asked to enter the old PIN code and to enter the new one. You will be also asked to confirm the entered code. To accept entered PIN click **OK**. If you want to quit and save previous settings, click **Cancel**. The **proCertum CardManager** will confirm the correctness of executed changes.



Figure 22: Window informing about successful operation of changing the PIN code

5.4. Changing the PUK code for the Secure profile

To change the PUK code, click **Change PUK**. The following window will appear:



Figure 23: Dialog window – Changing the PUK code for the Secure profile

You will be asked to enter the old PUK code and to enter the new one. You will be also asked to confirm the entered code. To accept the entered PIN code click **OK**. If you want to quit and save previous settings, click **Cancel**. The **proCertum CardManager** will confirm the correctness of executed changes.



Figure 24: Window informing about completed operation of generating new PUK code

5.5. Saving the certificates for the Secure profile

If already generated private key is found in the Secure profile, it is possible to save the certificate with the public key fitting to the mentioned private key to this profile. To commit this action click **Save certificate**. The window enabling saving certificate to Secure profile will appear.



Figure 25: Dialog window – Saving certificate to the secure profile

After selecting the file (operated formats: .cer, .der), entering correct PIN code and clicking on **OK**, the certificate will be saved to the secure profile.

5.6. Removing the certificate from the Secure profile

To remove certificate, select the required certificate from the **Certificates List** and then click on **Remove certificate**. The following window will appear:

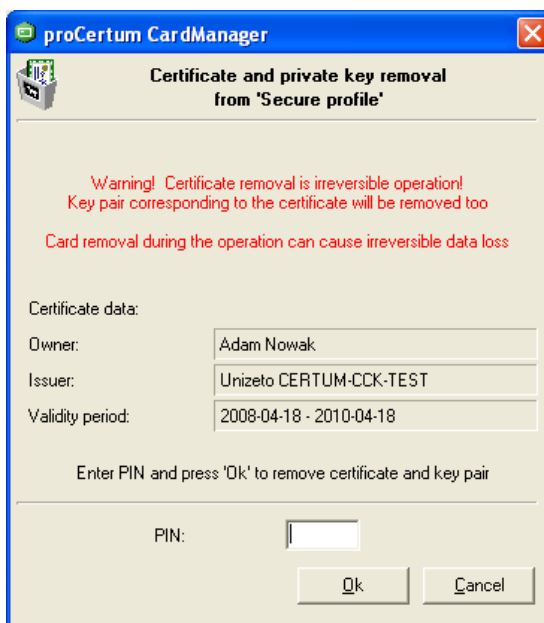


Figure 26: Dialog window – Removing the certificate and the private key from the secure profile

Enter the PIN code in the PIN field and confirm removing the certificate by clicking **OK**. To quit from removing the certificate, click on **Cancel**. The **proCertum CardManager** application will confirm the correctness of committed changes.



Figure 27: Window informing about completed operation of removing certificate

Warning!

Operation of removing certificate is irreversible! The pair of keys corresponding to the certificate will be removed too. Second installation of certificate can be performed by Certification Authority.

5.7. Certificate registration from the Secure profile

Certificate registration is possible, when the component and **cryptoCertumCSP** library component was installed on the workstation. These components are installed automatically during the standard registration.

To register certificates, click **Register** certificates. The **proCertum CardManager** application confirms completed operation of the registration.



Figure 28: Window informing about completed operation of the certificate registration.

Note!

The above procedure registers all the certificates found on the card in the operating system Windows system. Therefore all the certificates saved on the card can be visible for example in mail programs of the operating system Windows.

5.8. Reviewing certificate details from the Secure profile

For detailed description of the certificate select the certificate from the **Certificates list** and then click on **Show certificate details**. The window with the following three tabs will appear:

- General;
- Details;
- Certification path.

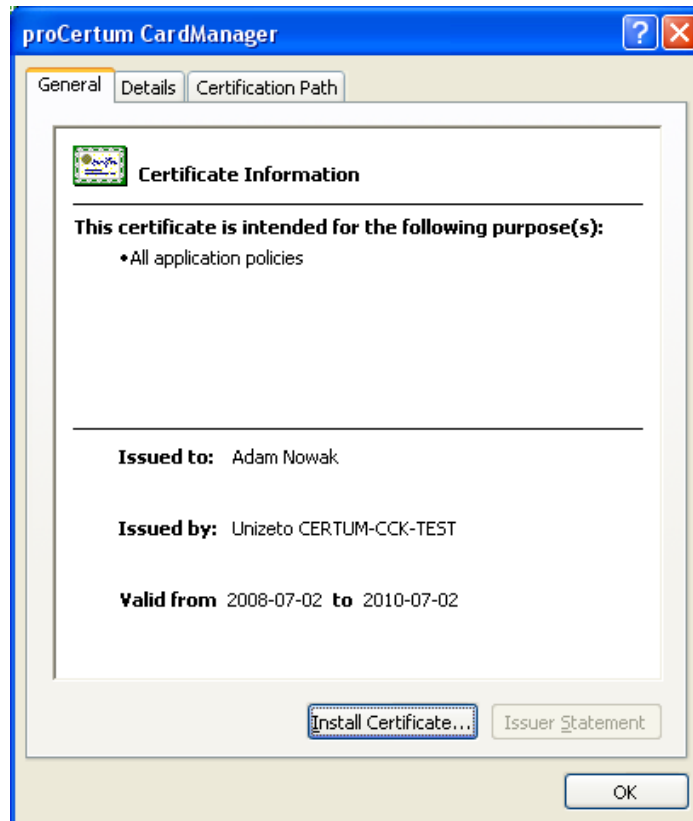


Figure 29: Dialog window – Information about certificate

To become familiar with the individual data, click the proper tab.

6. Common profile

To manage a profile for non-qualified certificates, select the **Common Profile** tab. As a result of this action, the window informing about chosen card profile and certificate list available on this profile will be shown.

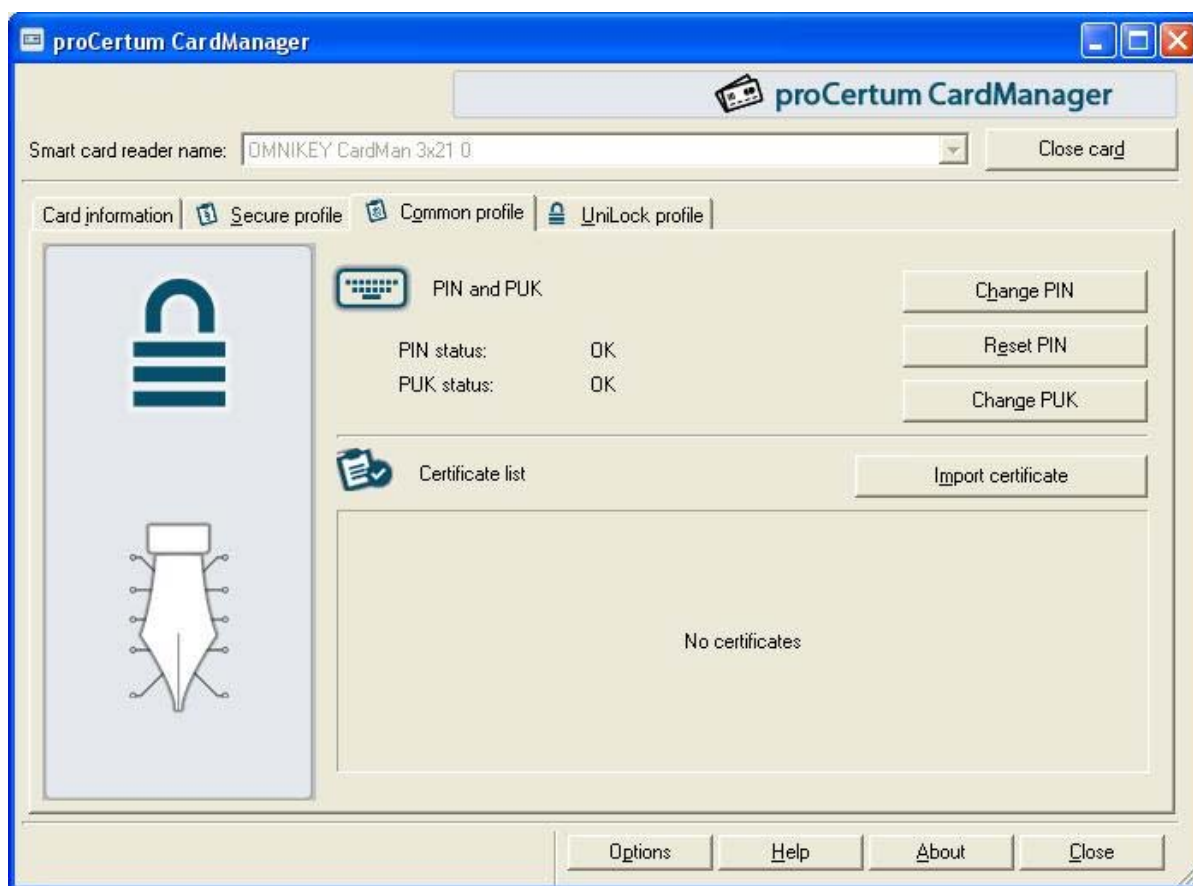


Figure 30: Tab of the Common profile

6.1. Common profile initialization

Note!

User usually receives card with already initialized profiles. Therefore the user does not have to initialize the profiles.

Chip card can be also delivered with non-initialized profile. It means that the tab with the name of the profile will appear in the main window of **proCertum CardManager** application. The profiles can be non-initialized aside from the others.

When the profile is non-initialized, it means that it is empty and there were no PIN or PUK codes defined for this profile.

Non-initialized profile cannot be used (you cannot for example generate a pair of keys or save certificate). During the initialization process the user defines PIN and PUK codes for the profile. Applications supporting operation of cryptographic cards do not detect non-initialized profile.

To initialize the profile, click **Initialize profile** and then define a new PUK and a new PIN code. You will be asked each time to confirm the entered code. To accept changes click **OK**. After initialization of the profile it is ready to work.

Warning!

Second initialization of the profile is impossible. It is not also possible to restore the status to the status before the initialization.

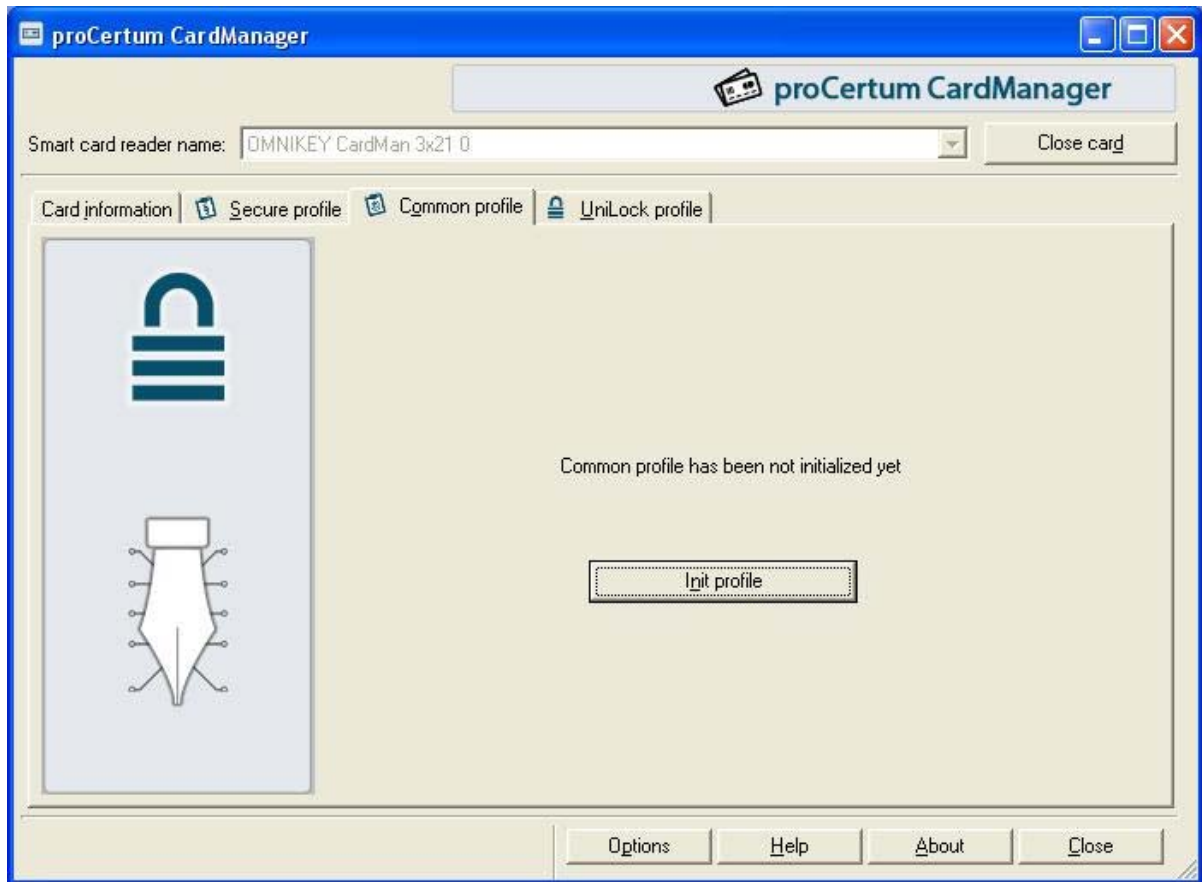


Figure 31: Tab of Common profile – non-initialized profile



Figure 32: Dialog window –Common profile initialization

6.2. Generating a new PIN code for the Common profile

To generate a new PIN code, click on **New PIN**. The following window will appear:



Figure 33: Dialog window – Generating a new PIN code for the Common profile

The user will be asked to enter the PUK code and to define a new PIN code. Furthermore the user will be asked to confirm the entered code. To confirm the entered PIN click **OK**. To quit from generating new PIN code and to save previous settings click **Cancel**. The **proCertum CardManager** application will confirm the correctness of entered data.



Figure 34: Window informing about successful operation of generating the new PIN code

6.3. Changing the PIN code for the Common profile

To change the PIN code, click **Change PIN**. The following window will appear:



Figure 35: Dialog window – Changing the PIN code for the Common profile

You will be asked to enter the old PIN code and to enter the new one. You will be also asked to confirm the entered code. To accept the entered PIN click **OK**. If you want to quit, click **Cancel**. The **proCertum CardManager** will confirm the correctness of executed changes.

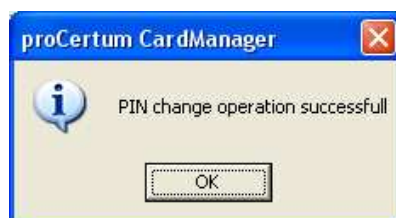


Figure 36: Window informing about successful operation of generating the new PIN code

6.4. Changing the PUK code for the Common profile

To change the PUK code, click **Change PUK**. The following window will appear:

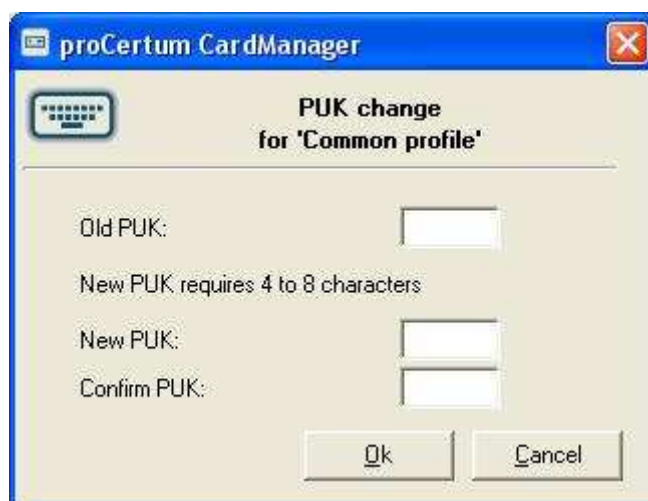


Figure 37: Dialog window– Changing the PUK code for the Common profile

You will be asked to enter the old PUK code and to enter the new one. You will be also asked to confirm the entered code. To accept the entered PIN code, click **OK**. If you want to quit and save previous settings, click **Cancel**. The **proCertum CardManager** will confirm the correctness of executed changes.



Figure 38: Window informing about successful operation of generating the new PUK code

6.5. Removing the certificate from the Common profile

To remove certificate, select the required certificate from the **Certificate List** and then click **Remove certificate**. The following window will appear

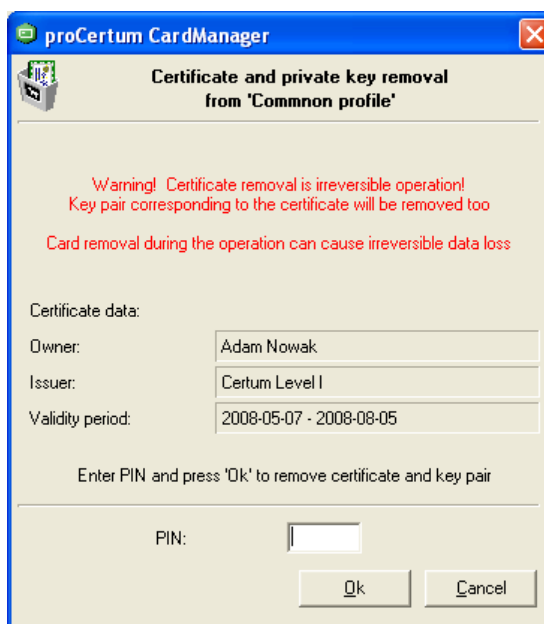


Figure 39: Dialog window – Certificate and private key removal from the Common profile

Enter the PIN code in the PIN field and confirm removing the certificate by clicking **OK**. To quit from removing the certificate, click **Cancel**. The **proCertum CardManager** application will confirm the correctness of committed changes.



Figure 40: Window informing about completed operation of removing certificate

Warning!

Operation of removing the certificate is irreversible! The pair of keys corresponding to the certificate will be removed too. Second installation of certificate can be performed by Certification Authority.

6.6. Certificate registration from the Common profile

The certificate registration is possible, when the **library crypto3CSP** component was installed on the workstation. Components are installed automatically during the standard installation. Additionally, the installation of **Common Electronic Signature** might be required (if it was attached to installation CD).

The certificate registration can be performed by selecting the function **Register certificates**. The **proCertum CardManager** will confirm the registration.



Figure 41: Window informing about completed operation of the certificate registration

Note!

The above procedure registers all the certificates located on the card in the operating system Windows. Therefore all the certificates saved on the card can be visible for example in mail programs of the operating system Windows.

6.7. Certificate details from the Common profile

For detailed description of the certificate select the certificate from the **Certificate list** and then click **Show certificate details**. The window with the following three tabs will appear:

- General;
- Details;
- Certification path.

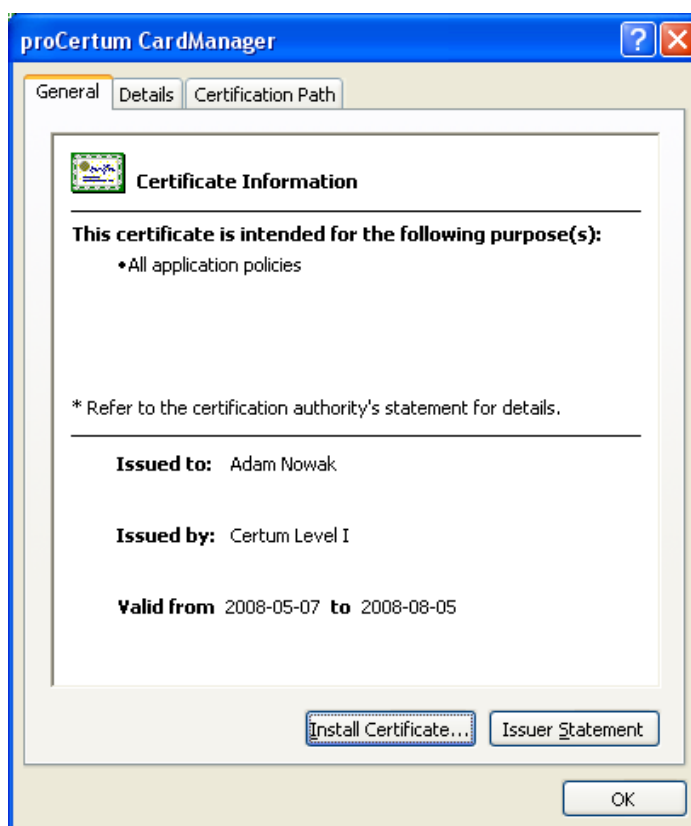


Figure 42: Dialog window – Information about certificate

To become familiar with the individual data, click on the proper tab.

6.8. Import of the certificate to the Common profile

To import the certificate, click **Import certificate**. The following window should appear:



Figure 43: Dialog window – Details of the certificates imported to the Common Profile

You should enter here the localization of certificate in the file with the extension **.pfx** or **.p12**.



Figure 44: Dialog window – Selection of the file with the certificate

Furthermore the user should enter password protecting the private key and the PIN code. To accept the operation, click **OK**.

In order to quite from the procedure of import the certificate, click **Cancel**. The imported certificate will be available at **Certificate list**.

Note!

The required length of the key for the imported certificate depends on the kind of the card and can consist of bites between 768 and 1024 or between 768 and 2048.

7. CryptoCertum Scanner

To get the **CryptoCertum CardManager** applications started please select from the **Start** menu **CryptoCertum Scanner**. It will be displayed in **tray**.



Figure 45: CryptoCertum Scanner in tray

To configure **CryptoCertum CardManager** click icon using right mouse button. 4 options will be displayed then:

- **Run proCertum CardManager** – selecting this option will cause installing of program proCertum CardManager.
- **Register Common profile certificate**– selecting this option will cause automatic certificate's registration from Common profile after inserting a card. Certificate will be installed in the Windows certificate storage.
- **Register Secure profile certificate** – selecting this option will cause automatic certificate's registration from Secure profile after inserting a card. Certificate will be installed in the Windows certificate storage.
- **Check expiration date of nonqualified certificates** – selecting this option will cause proof of expiration data of nonqualified certificates.
- **Check expiration date of qualified certificates** – selecting this option will cause proof of expiration data of qualified certificates.
- **Autorun after logon** - selecting this option will cause application start after second system login or second profile login.
- **Close** – this option closes application.

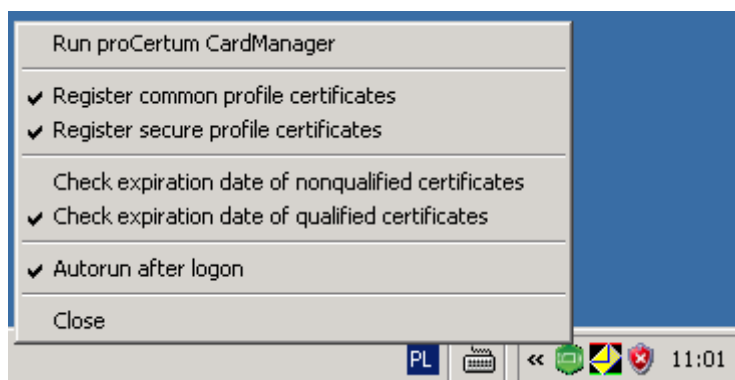


Figure 46: CryptoCertum Scanner – options

8. Information about actualization

In **proCentrum CardManager** application there is a mechanism that informs about **new version of application**. This mechanism starts when the application is opened. When the new version is available the following information will be shown:

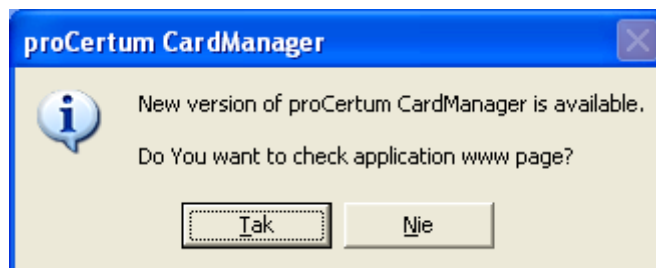


Figure 47: Window informing about new version of application

After clicking **Yes** the window with **www.page** will be opened. The new version of application will be available for downloading from the **www.page**. To make the mechanism work, the computer must be connected to the Internet.



Figure 48: www page with new version of proCertum CardManager

9. Table of figures

Figure 1: Installer icon.....	6
Figure 2: Window enabling the selection of the setup language.....	6
Figure 3: Opening window of install creator.....	7
Figure 4: Dialog window – Cancellation of the setup.....	7
Figure 5: Installer window – License agreement.....	7
Figure 6: Installer Window– Choose Destination Location.....	8
Figure 7: Dialog window – Select installation folder.....	8
Figure 8: Installer window – Installation status.....	9
Figure 9: Installer window –Setup status.....	9
Figure 10: Installer window – Installation process completed.....	10
Figure 11: Main window of proCertum CardManager application.....	11
Figure 12: Informing window of proCertum CardManager application.....	11
Figure 13: Window of proCertum CardManager application with visible tabs of profiles.....	12
Figure 14: The tab after clicking on More information>>.....	12
Figure 15: Options.....	14
Figure 16: The tab of the Secure profile.....	15
Figure 17: The tab of the Secure profile – non-initialized profile.....	16
Figure 18: Dialog window –Secure profile initialization.....	16
Figure 19: Dialog window – Generating a new PIN code for the Secure profile.....	17
Figure 20: Window informing about the accomplishment of the operation of generating the new PIN code.....	17
Figure 21: Dialog window – Changing the PIN code for the Secure profile.....	18
Figure 22: Window informing about successful operation of changing the PIN code.....	18
Figure 23: Dialog window – Changing the PUK code for the Secure profile.....	18
Figure 24: Window informing about completed operation of generating new PUK code.....	19
Figure 25: Dialog window – Saving certificate to the secure profile.....	19
Figure 26: Dialog window – Removing the certificate and the private key from the secure profile.....	20
Figure 27: Window informing about completed operation of removing certificate.....	20
Figure 28: Window informing about completed operation of the certificate registration.....	20
Figure 29: Dialog window – Information about certificate.....	22
Figure 30: Tab of the Common profile.....	23
Figure 31: Tab of Common profile – non-initialized profile.....	24
Figure 32: Dialog window –Common profile initialization.....	24
Figure 33: Dialog window – Generating a new PIN code for the Common profile.....	25
Figure 34: Window informing about successful operation of generating the new PIN code.....	25
Figure 35: Dialog window – Changing the PIN code for the Common profile.....	25
Figure 36: Window informing about successful operation of generating the new PIN code.....	26
Figure 37: Dialog window– Changing the PUK code for the Common profile.....	26
Figure 38: Window informing about successful operation of generating the new PUK code.....	26
Figure 39: Dialog window – Certificate and private key removal from the Common profile.....	27
Figure 40: Window informing about completed operation of removing certificate.....	27
Figure 41: Window informing about completed operation of the certificate registration.....	28
Figure 42: Dialog window – Information about certificate.....	28
Figure 43: Dialog window – Details of the certificates imported to the Common Profile.....	29
Figure 44: Dialog window – Selection of the file with the certificate.....	29

Figure 45: CryptoCertum Scanner in tray	31
Figure 46: CryptoCertum Scanner – options	31
Figure 47: Window informing about new version of application	32
Figure 48: www page with new version of proCertum CardManager	32