

HAL E-BANK MANUAL
QUALIFIED DIGITAL CERTIFICATE
ONE FOR ALL



Hal E-Bank version: 21.X.X.01

Content of Manual

The manual consists of several content sections. The current section is highlighted on the list. The manual's content sections are also available online at www.eng.halcom.si/support.

1. PAYMENTS
2. CROSS-BORDER PAYMENTS AND OPERATIONS WITH FOREIGN CURRENCIES
3. REMOTE SIGNING
4. ADDRESS BOOK
5. QUALIFIED DIGITAL CERTIFICATE ONE FOR ALL
6. REVIEW OF BALANCE, TRANSACTIONS AND STATEMENTS
7. BANK NOTICES AND MESSAGES TO BANK
8. ADDITIONAL TOOLS AND SETTINGS
9. FILE EXCHANGE
10. E-INVOICES
11. SEPA DIRECT DEBIT
12. SDD REFUSALS AND MANDATES

Table of Contents

Basic Terms and Secure Use of Digital Certificate	4
Printout of Certificate of Identity and Exporting Digital Certificate	5
Renewal of Qualified Digital Certificate ONE FOR ALL	8
When and How to Revoke Qualified Digital Certificate.....	9
Unblocking of Locked Qualified Digital Certificate	10
Unblocking Locked Digital Certificate with Nexus Personal Program	10
Unblocking of Locked Digital Certificate with Program for Unlocking UnblockPIN.exe	12
Changing PIN Code.....	13
Changing PIN Code in Electronic Bank	13
Changing PIN Code by Using Nexus Personal Program	14

Basic Terms and Secure Use of Digital Certificate

Qualified digital certificate (QDC) is a holder's identity card in electronic business. As we can entirely trust identity cards issued by administrative units, we can also entirely trust qualified digital certificates issued by a certificate authority. QDC are issued only by accredited certificate authorities, which operate in accordance with the valid legislation and by prescribed official procedures.

Detailed technical explanation on issuing and using QDC can be found in the document entitled Notification to users of qualified digital certificates, which is saved on the installation CD Halcom CA, while in continuation we give a few tips for secure use of QDC.

SECURE ELECTRONIC OPERATIONS

Level of electronic operations security depends also on the carrier or media, on which QDC holder holds its private key. Currently, the highest level of security is ensured by the so called secured media (smart cards and USB smart keys), whose main advantage is that a private key never leaves a media, as encrypting and digital signing takes place on the media itself.

The foundation for secure electronic operations is **secure behavior of users**, which includes equipment of a computer with adequate anti-virus programs and regular updating of software. Otherwise, security is dependent on respecting basic rules for secure handling of QDC and PIN code, as follows:

- PIN code should always be kept separately from a qualified digital certificate; it should not be written on visible places, accessible by everyone;
- It is recommended to regularly change a PIN code;
- Upon completing work with electronic bank, smart cards should not be kept in reader nor the USB key in the USB port;
- Digital certificates should not be lent to others (in the same way you would not lend your identity card, passport or bank card);
- In case of loss or abuse of digital certificate, the certificate will be immediately revoked.

You will receive your qualified digital certificate ONE FOR ALL by mail. The following day you will also receive PIN and PUK codes for unlocking the locked digital certificate (see below). PUK code should be kept in a secure place, as a locked digital certificate cannot be used any more without PUK code.

With the qualified digital certificate ONE FOR ALL you can do business with all the banks using the Hal E-Bank electronic bank. The same certificate can also be used to enter various e-portals (e.g. eDAVKI, AJPES, eVEM...). You can find a list of all the banks and portals which you can enter by using the digital certificate ONE FOR ALL on the web page <http://www.halcom.si/en/support/?action=showEntry&data=364>.

Printout of Certificate of Identity and Exporting Digital Certificate

A bank shall enable you to use the electronic bank only after you submit a signed certificate of identity of your digital certificate (public part of digital certificate). You received a printed certificate by mail together with your digital certificate.

```

DIGITAL CERTIFICATE PROOF OF POSSESSION

I hereby certify that the information from this digital certificate
readout is the information that connects me personally with the certificate
which will be used for digital signature and authentication in secure online
banking and e-commerce purposes.

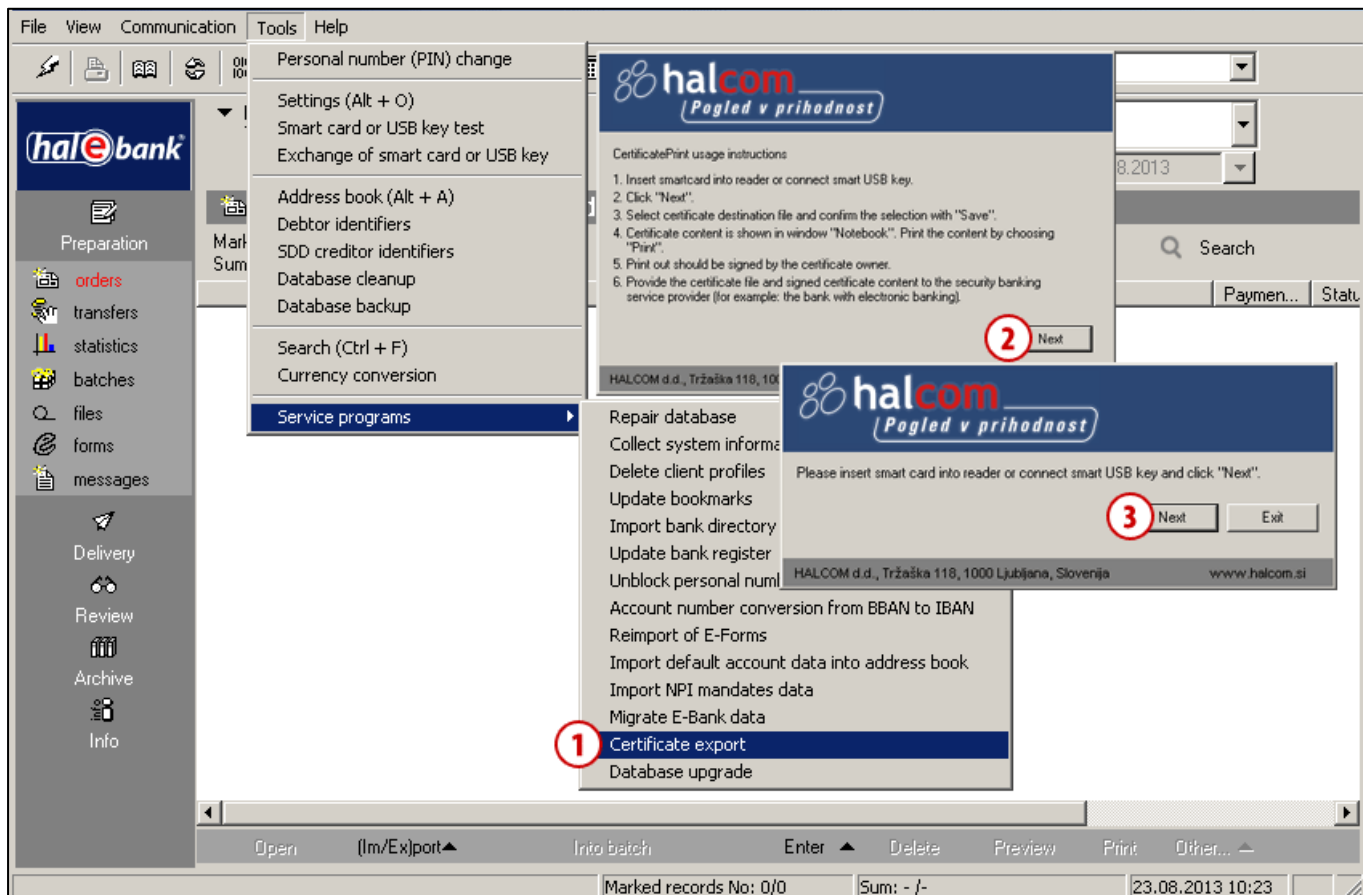
DIGITAL SIGNATURE READOUT:
Version: V3
Certificate serial number: 053E DA
Signature algorithm: RSA-SHA1
Issuer:
  C=SI
  O=Halcom
  CN=Halcom CA PO 2
Valid from: Aug 18 08:12:19 2009 GMT
Valid to: Aug 18 08:12:19 2012 GMT
Subject:
  1.3.6.1.4.1.5939.2.2=#13083536393439323433
  Email=testna.oseba@halcom.si
  1.3.6.1.4.1.5939.2.3=#13083433333533313236
  G=Testna
  S=Oseba
  CN=Testna Oseba
  O=HALCOM D.D.
  C=SI
  Public key: 1024 (rsaEncryption)
    3081 8902 8181 0089 48BF 6323 738C 606E A5B2
    29E0 A7A7 3D58 3345 0712 0800 3501 232F 2A55
    7EDD B940 E0A8 25DD 5A3C 1B23 F64C E556 2DE9
    C50E 3917 34D8 4D19 4729 9788 D7A6 F84A A6BE
    8B59 0610 690F 261B AEB8 B349 6990 3CCA 4A9A
    2AA8 D19D 55FC 7D15 39C5 A87F 995F 76DE AFF4
    5E16 262A 1C8C 209D 2388 A5F6 5255 8859 4BD5
    06BF 3794 4D75 0C79 5302 0301 0001
  Thumbprint algorithm: SHA-1
  Thumbprint: A998 35F4 6D19 7290 11EE F96C 833E 77A5 D3E6 C193

Date and time of readout generation: 15.12.2011 ob 14:13
Name and surname of the signer and the signer tax number:
_____

Certificate owner contact info:
Email address: _____
Telephone nr.: _____
Date: _____ signature: _____
    
```

1. Write your name, surname, and a certificate holder's personal tax number on the certificate.
2. Write your E-mail address and telephone number.
3. The certificate shall be equipped with the signature of digital certificate's holder.
4. Send the certificate to the bank, at which you submitted the documentation for electronic operations, as soon as possible.

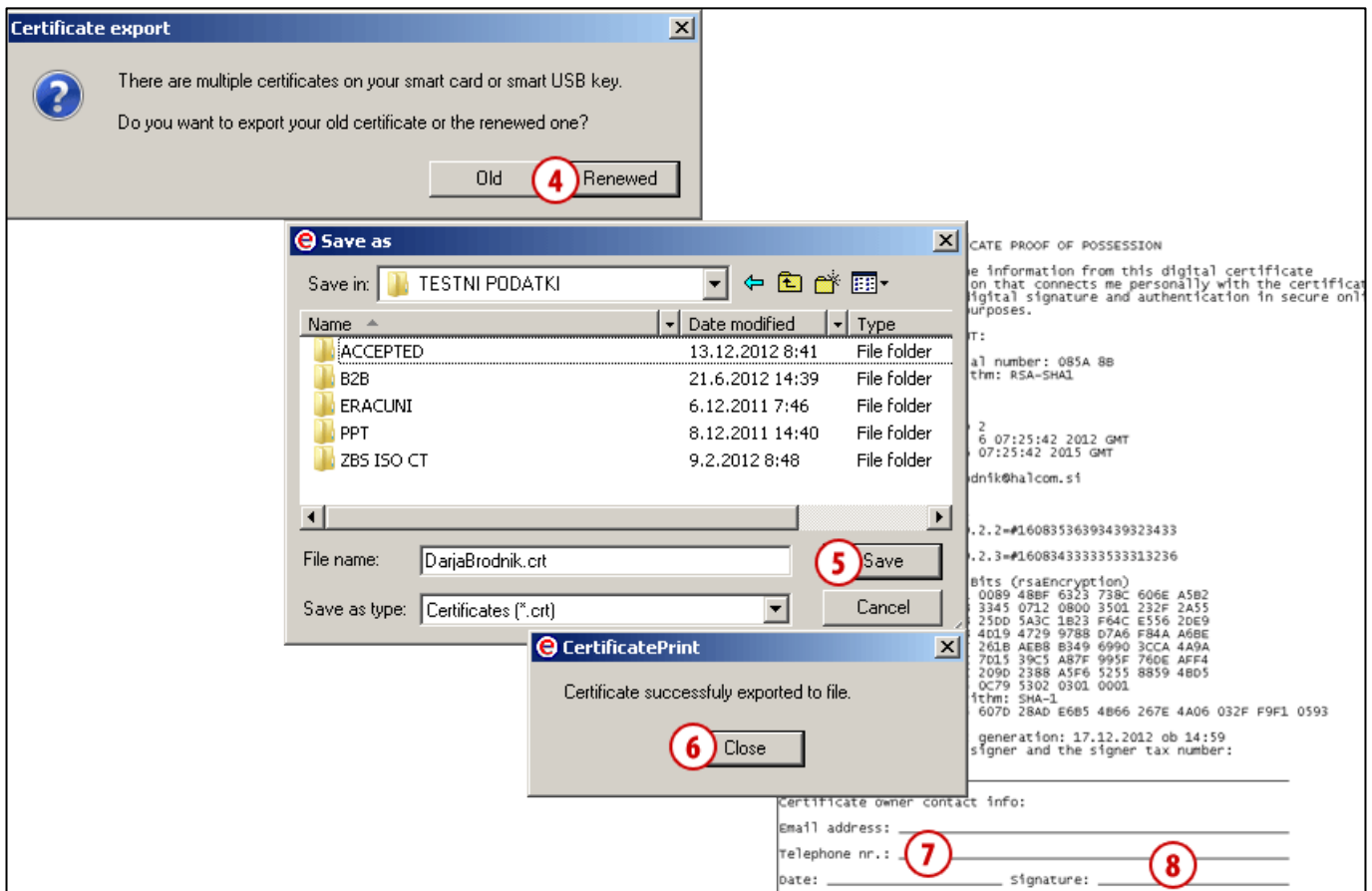
In case you need the identity certificate later on (for instance, you would like to conduct business electronically with another bank using the same digital certificate), you can print the identity certificate on your own by using the program for **writing out and exporting digital certificates** (IzvozCertifikata.exe). You run it via the Hal E-Bank Personal/Corporate program. By using this program, you can create **identity certificate** (to file lmePriimek.txt), while at the same time you also export a **public part** of a digital certificate (to file lmePriimek.crt).



- 1 In the Hal E-Bank Personal/Corporate program, you can run the program »Export of certificate« by clicking the »Tools« tab and then select »Service program«.
- 2 The instructions for exporting a digital certificate will appear which you confirm by clicking the **Next** button.

- 3 Enter a smart card into the reader or a key into the USB port; to continue, click the **Next** button.

Continued on next page ...



- 4 If you have an old and a renewed certificate saved on your smart card or on your USB key, select the one you want to export.
- 5 A new window will open, where you can specify the name and location where a public part of the digital certificate will be saved (file with the .crt ending). Confirm the selection by clicking the **Save** button.
- 6 Complete exporting of digital certificate by clicking the **Close** button.
- 7 In the Notepad window, the certificate of identity for a digital certificate is written.

Name, surname, certificate holder's personal tax number, e-mail address and telephone number must be added into the certificate. The content of the certificate of identity is saved in text format to txt file (together with the .crt file).

- 8 Printed certificate of identity shall be **personally signed** by a digital certificate holder. Afterwards, it has to be **sent** as soon as possible to the **selected provider of electronic services (bank)**.

Renewal of Qualified Digital Certificate ONE FOR ALL

Prior to expiration of its validity, **qualified digital certificates ONE FOR ALL** can be simply renewed. Renewal for the next three years is possible only once and with valid digital certificate.

1. If your e-mail address, stated in the documentation when ordering a digital certificate, is still valid, Halcom CA informs you about the expiration of your qualified digital certificate validity 30 days prior to the actual expiration. The letter also includes short instructions for renewal, which you can order at the web page <http://www.halcom.si/en/products/digital-certificate/renewal/>.
2. Upon payment of pro-forma invoice, which you receive upon ordering renewal, Halcom CA will send you instructions for continuation of the renewal procedure.

When and How to Revoke Qualified Digital Certificate

Revocation of certificate can be requested by a certificate holder, a representative or a procurator of a legal entity at any time. However, the revocation must be requested in the following cases:

- When a legal entity or certificate holder changes some of the key data related to a certificate (name or surname, name of legal entity, and employment);
- Lost or stolen digital certificate;
- When it is found out or suspected that disclosure of key for signing or abuse of certificate had occurred.

HALCOM CA can revoke a certificate even without holder's request in cases of changes of holder's key data or upon a request by a competent court, minor offense judge or an administrative body.


In order to revoke a digital certificate, a completed Request for revocation must be sent to Halcom CA. The form can be found on the web page <http://www.halcom.si/en/products/digital-certificate/revocation-of-digital-certificate/>. Based on properly completed request for revocation, Halcom CA will revoke a certificate and add it to the list of revoked digital certificates.

Unblocking of Locked Qualified Digital Certificate

After three consecutive entries of wrong PIN code (Personal Identification Number), a qualified digital certificate locks itself. A locked digital certificate cannot be used until it is unblocked.

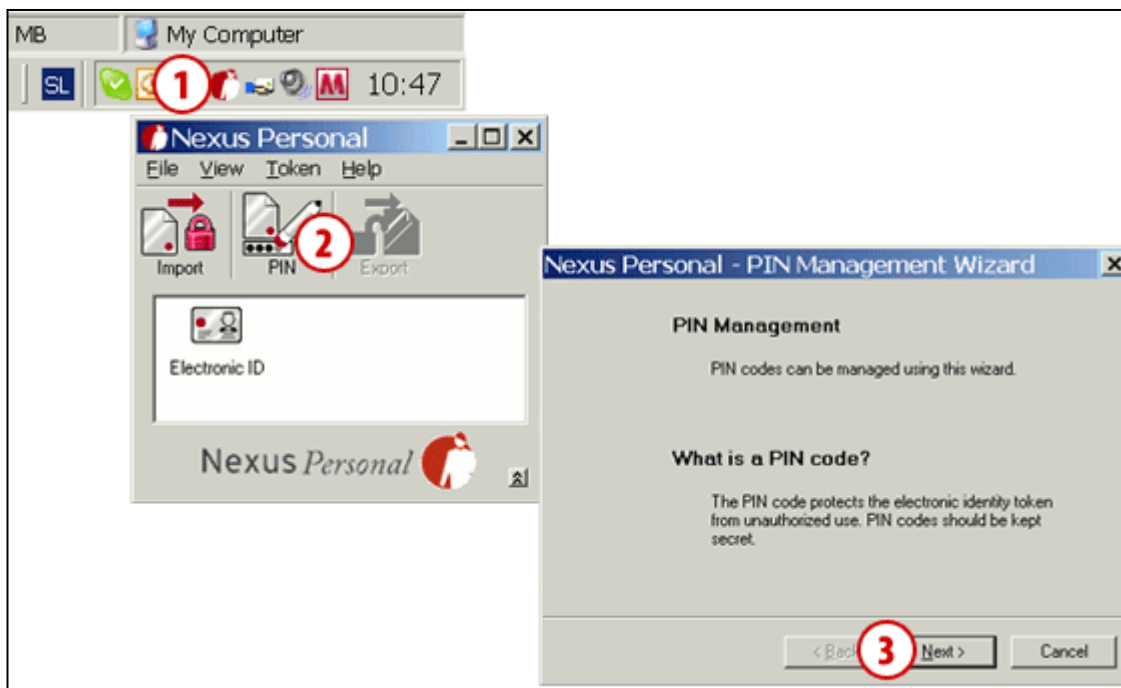
For unblocking a digital certificate, you need the PUK unlock code (Personal Unlock Key), which you received by mail together with the PIN code, and the Nexus Personal or UnblockPIN.exe programs.


You installed Nexus Personal on your computer together with the electronic bank or with the program

for using a digital certificate. If the program is installed on your computer, you will see the icon  in the bottom right corner on the taskbar. If you don't have the program, you can help yourself with the UnblockPIN.exe program, which can be downloaded from the web page

<http://www.halcom.si/en/support/?action=showEntry&data=337> (see instructions on Page12).

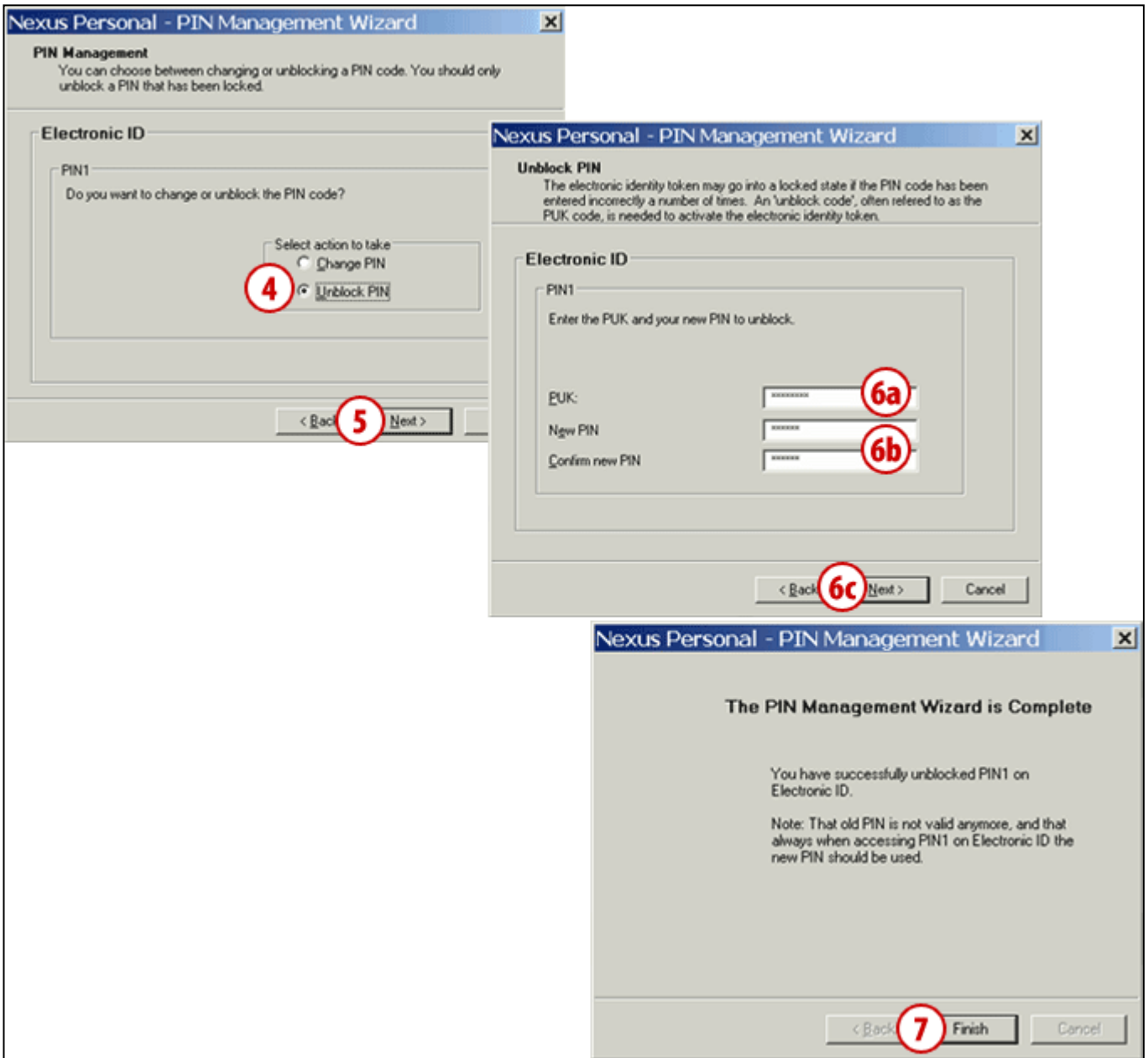
Unblocking Locked Digital Certificate with Nexus Personal Program



- 1 Start the Nexus Personal program by double clicking the icon  on the taskbar.
- 2 In the window which opens, click the PIN icon.

- 3 A warning will open, which you confirm by clicking the **Next** button.

Continued on next page ...



- 4 In the new window, select the unlocking possibility (**Unblock PIN**).
- 5 Confirm by clicking the **Next** button.
- 6 In the first field, enter the PUK unlock code, which you received by mail together with the PIN code (**6a**). In the bottom two fields, enter the new PIN code, which should be comprised of 6 to 8 characters (**6b**). Confirm the entry by clicking the **Next** button (**6c**).

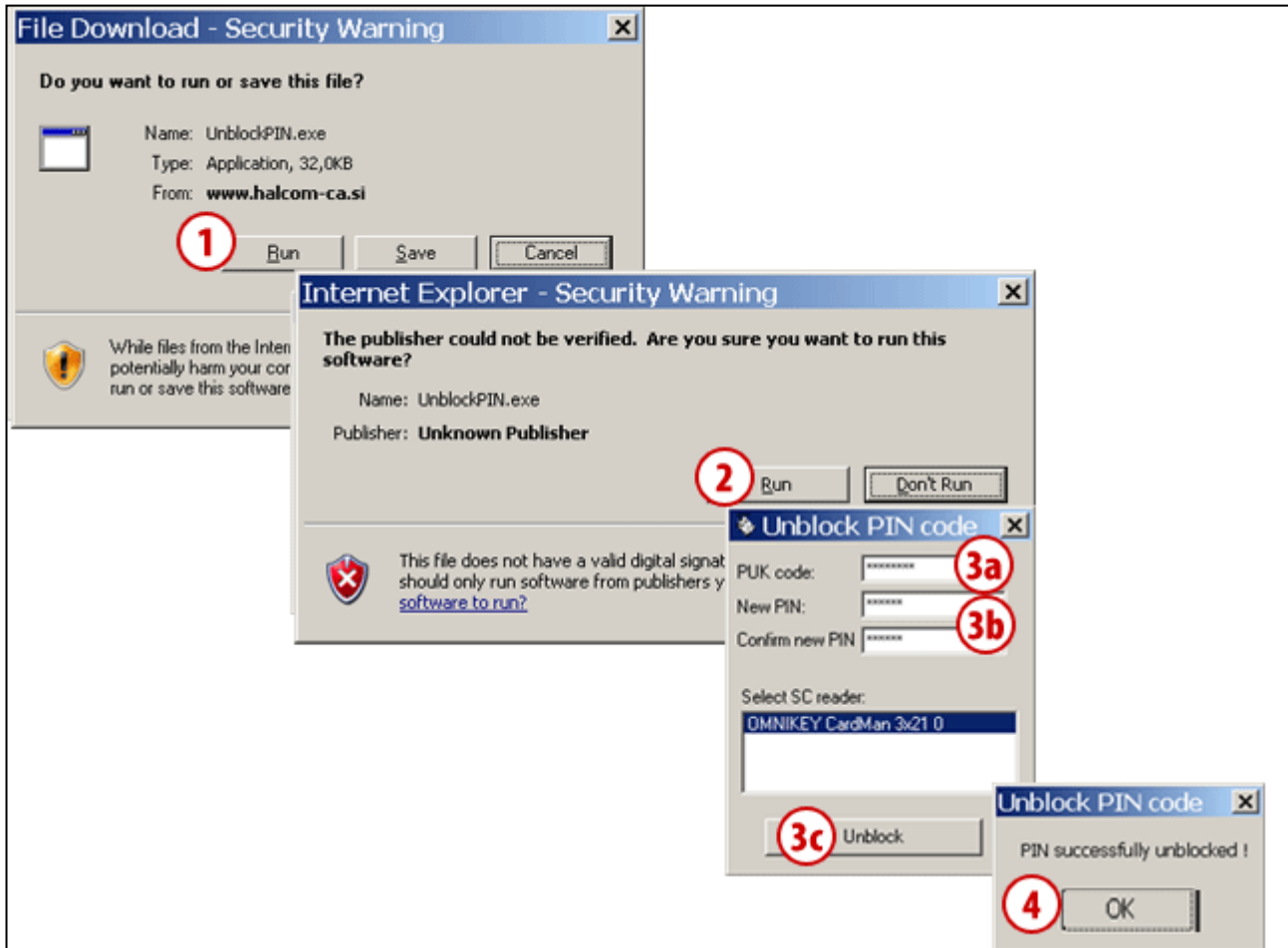
- 7 Confirm the message on successful unblocking of the digital certificate by clicking the **Finish** button; the certificate is successfully unblocked.

WARNING

If you try to unblock a digital certificate with the wrong PUK code for three consecutive times, a digital certificate will be automatically destroyed. You will have to order a new card or USB key.

Unlocking of Locked Digital Certificate with Program for Unlocking UnblockPIN.exe

The program for unlocking (UnblockPIN.exe) is saved on the electronic bank installation CD, but it can also be downloaded from the web page www.eng.halcom.si/support.



- 1 On the web page www.eng.halcom.si/support, start the program for unlocking a digital certificate by clicking the **Start** button.
- 2 Confirm starting of the program by clicking the **Start** button.
- 3 In the first field, enter the PUK unlock code, which you received by mail together with the PIN code (3a). In the bottom two fields, enter the new PIN code, which should be comprised of 6 to

8 characters (3b). Confirm the entry by clicking the **Unlock** button (3c).

- 4 Confirm the message on successful unblocking of the digital certificate; the certificate is successfully unblocked.

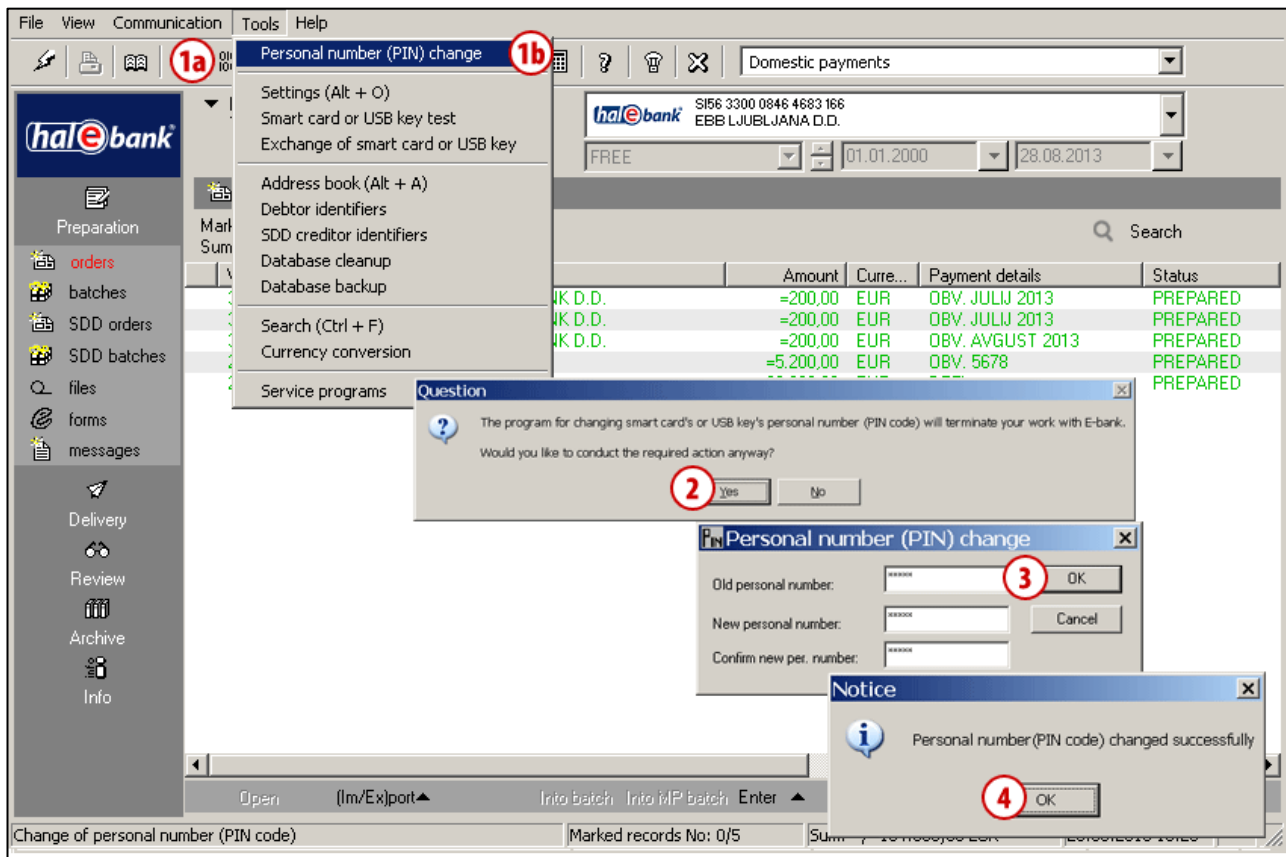
WARNING

If you try to unblock a digital certificate with the wrong PUK code for three consecutive times, a digital certificate will be automatically destroyed. You will have to order a new card or USB key

Changing PIN Code


PIN code can be changed in two ways; in electronic bank itself or by using the **Nexus Personal** program.

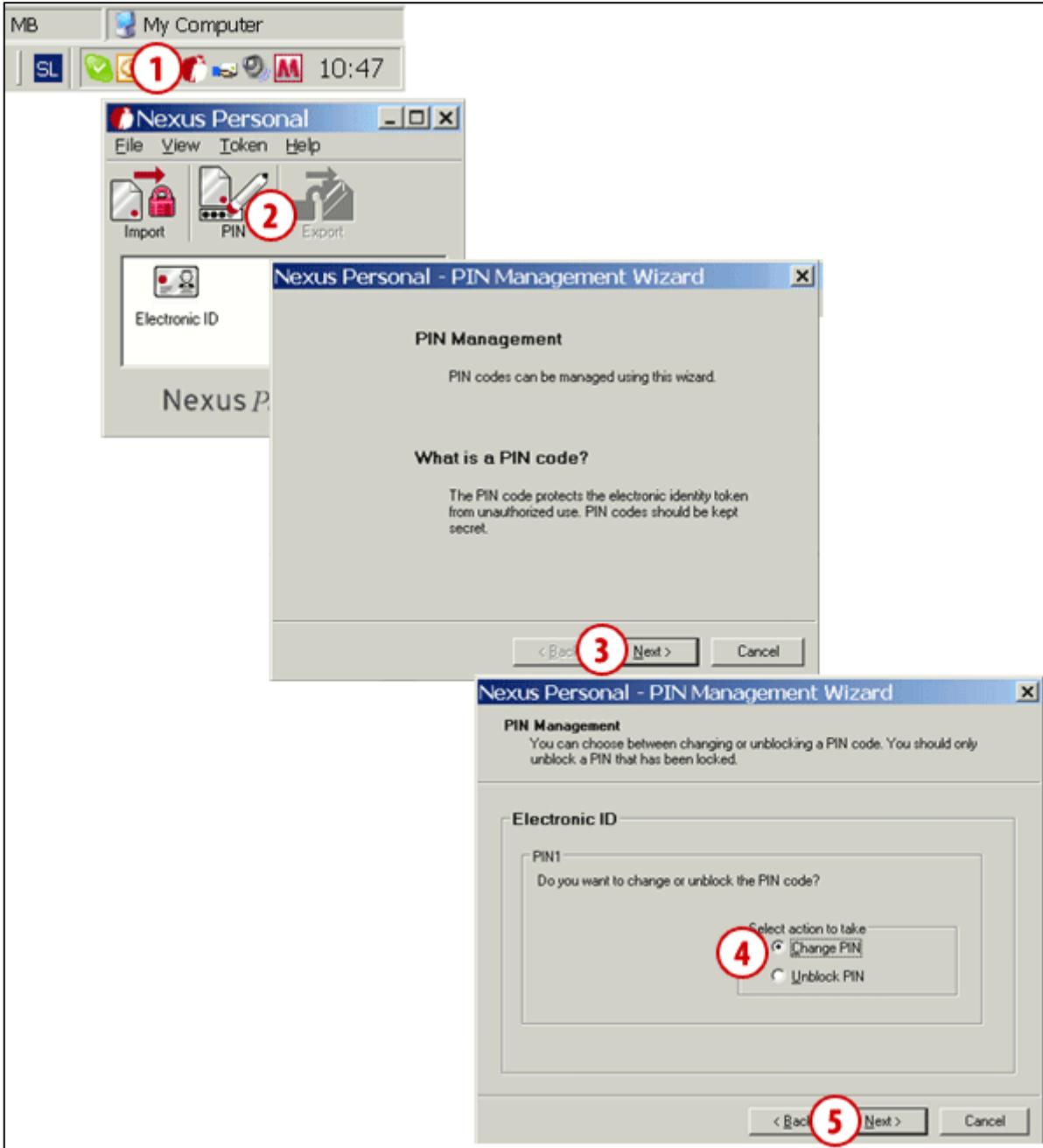
Changing PIN Code in Electronic Bank




- 1 On the toolbar, click the »Change personal number (PIN code)« icon (1a), or follow the menu selection **Tools** and select the **Personal number (PIN) change** option (1b).
- 2 A warning will appear that the program for changing personal number will stop the work with electronic bank. Confirm the warning and the electronic bank program will close.
- 3 The window for changing PIN code will open, where you enter the old PIN code and the new PIN code twice. The new PIN code should be comprised of 6 to 8 characters. Confirm the entry by clicking the **Confirm** button.
- 4 The program reports on the successful change of PIN code. Confirm the notification by clicking the **OK** button. Start the electronic bank and continue working with the new PIN code.

Changing PIN Code by Using Nexus Personal Program

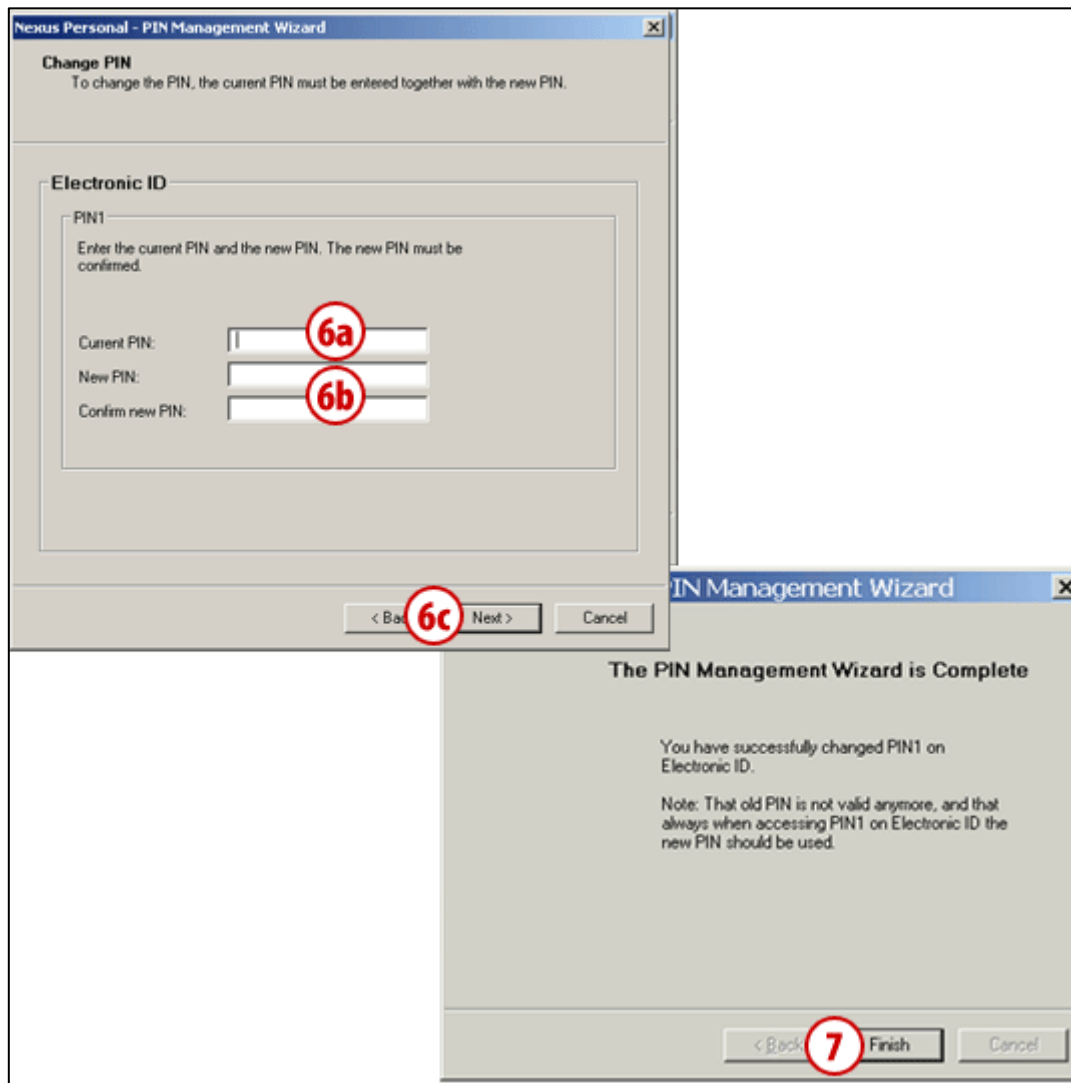
You installed the **Nexus Personal** program on your computer together with the software for using a digital certificate or during the installation of the electronic bank. If the program is installed on your computer, you will see the icon  in the bottom right corner on the taskbar.



- 1 Start the **Nexus Personal** program by double clicking the icon  on the taskbar.
- 2 In the window which opens, click the **PIN** icon.
- 3 A warning will open, which you confirm by clicking the **Next** button.

- 4 In the new window, select the change of personal number (**Change PIN**).
- 5 Confirm by clicking the **Next** button.

Continued on next page ...



6 In the first field, enter the personal number you are using **(6a)**. In the bottom two fields, enter the new PIN code, which should be comprised of 6 to

8 characters **(6b)**. Confirm the entry by clicking the **Next** button **(6c)**.
7 Confirm the message on successful change of PIN code by clicking the **Finish** button.