HAL E-BANK MANUAL

QUALIFIED DIGITAL CERTIFICATE ONE FOR ALL

Hal E-Bank version: 17.X.X.21

Content of Manual

The manual consists of eight content sections and two sub-sections. The current section is highlighted on the list. The manual's content sections are also available online at www.halcom.rs.

Table of Contents

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 at your bank or by mail. Then you will receive PIN and PUK codes for unlocking the locked digital certificate (see Chapter 3). 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. You can find a list of all the banks you can enter by using the digital certificate ONE FOR ALL on the web page *www.halcom.rs*.

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.

```
        PISNO POTRDILO O ISTOVETNOSTI DIGITALNEGA POTRDILA

Spodaj podpisani izjavljam, da so podatki iz tega izpisa
digitalnega potrdila podatki, ki povezujejo mene osebno s podatki
za preverjanje mojega elektronskega podpisa, katerih namen je
moje varno elektronsko poslovanje.


IZPIS VSEBINE DIGITALNEGA PODPISA:

        Version: V3
        Certificate serial number: 0553 A3
        Signature algorithm: RSA-SHA1
        Issuer:
         C=SI
         O=Halcom
         CN=Halcom CA PO 2
        Valid from: Sep 22 08:56:07 2009 GMT
        Valid to: Sep 22 08:56:07 2012 GMT
        Subject:
         Email=janez.novak@halcom.si
        G=Janez
        S=Novak
        CN=Janez Novak
        1.3.6.1.4.1.5939.2.2=#16083331383734353137
        O=HALCOM D.D.
        1.3.6.1.4.1.5939.2.3=#16083433333533313236
        C=SI
        Public key: 1024 Bits (rsaEncryption)
          3081 8902 8181 0085 C00F AF6E 2BB8 A057 7F56
          1946 3651 DEAB 1B58 7985 DBA1 221C D247 1150
          F082 772F 620E D62B AD59 5639 1822 492D 7BD4
          852E 0130 3C34 E6C3 C51D 3702 FEDA 2738 F8E5
          A577 4FBB 8B4C 0BB3 FCE5 8AEA B8F8 1F1D 0CBF
          C3B2 3ACF 1C85 7318 6781 68AF 3895 BF64 27F0
          60F2 A521 00CE 1F73 07FC ED3F 00C5 D1CE 31A0
          F907 D77D 33AE 54CB E902 0301 0001
        Thumbprint algorithm: SHA-1
        Thumbprint: 0ED9 6171 74E0 8AE9 FF84 A107 EB29 34FC E054 FE43


Datum in čas generiranja izpisa: 07.10.2009 ob 12:39

Ime in priimek podpisnika ter osebna davčna številka podpisnika:

_____

Lastnoročni podpis in datum podpisa:

_____
```

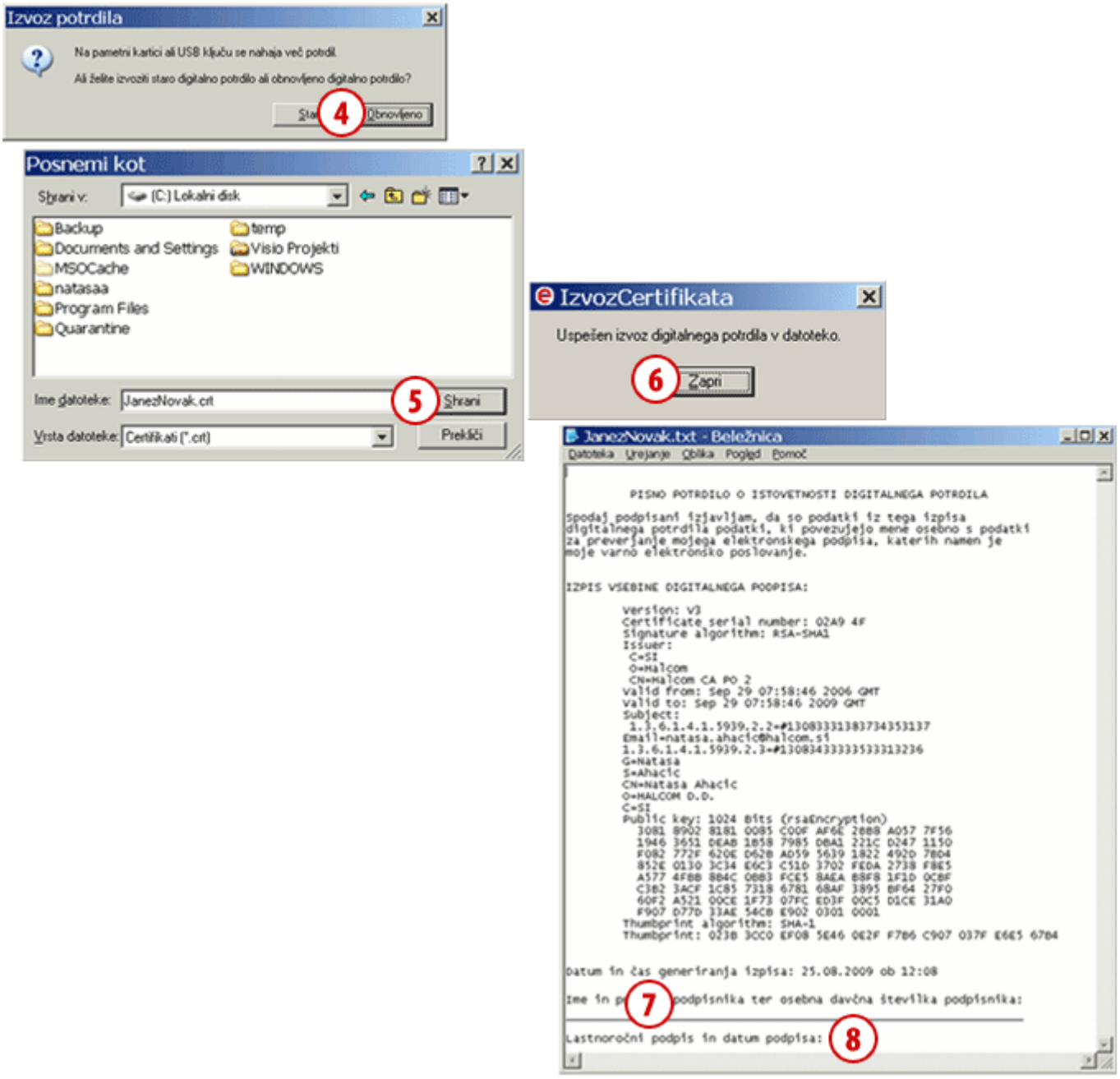
1. Write your name, surname, and a certificate holder's personal tax number on the certificate.
2. The certificate shall be equipped with the signature of digital certificate's holder.
3. Send the certificate to the bank, at which you submitted the documentation for electronic operations, as soon as 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). The program is saved on the electronic bank installation CD, while you can also download it on the web page *www.halcom.rs*. By using this program, you can create **identity certificate** (to file ImePriimek.**txt**), while at the same time you also export a **public part** of a digital certificate (to file ImePriimek.**crt**).

1 On the web page *www.halcom.rs*, start the exporting program by clicking the **Start** button.

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 **Confirm** 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.

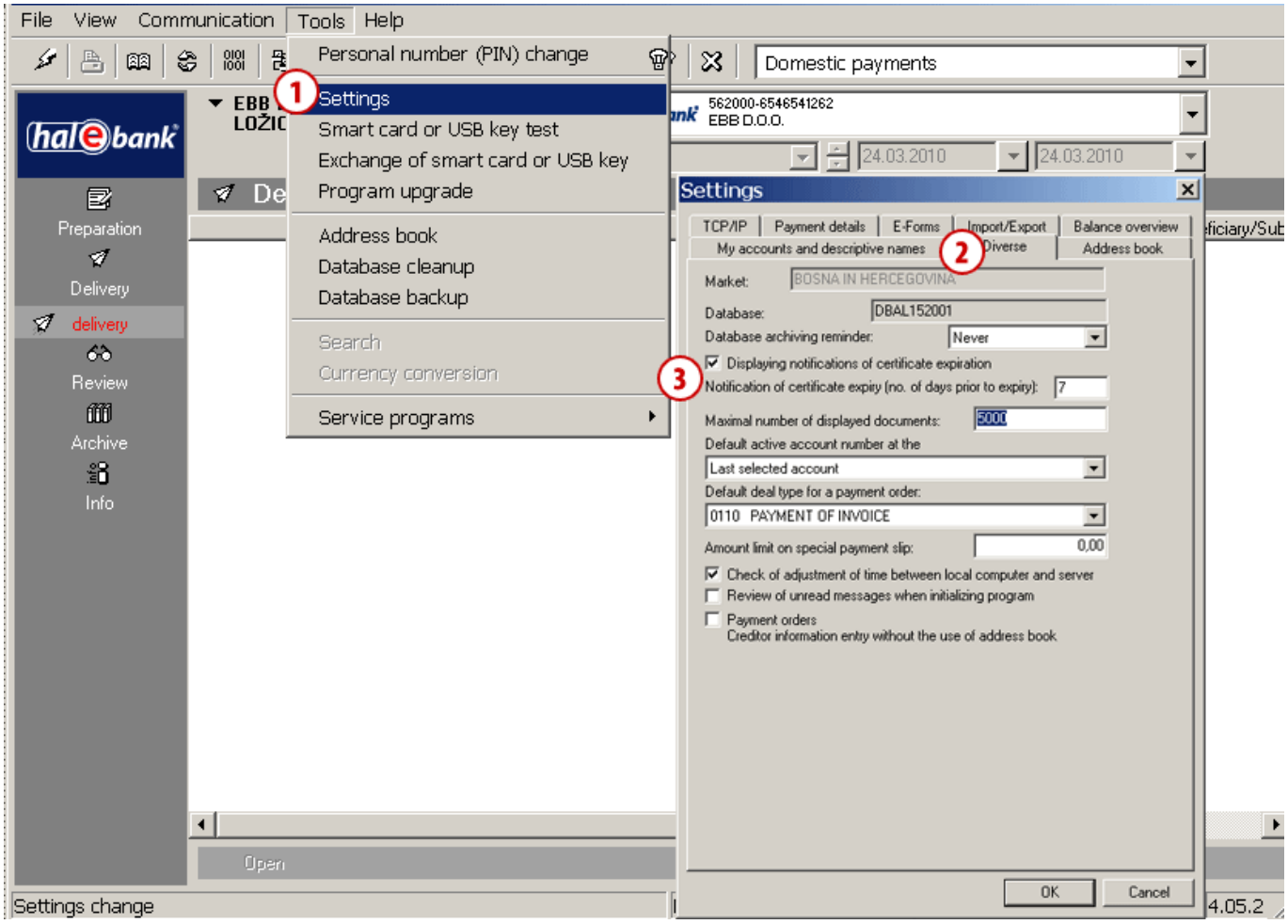
7 In the Notepad window, the certificate of identity for a digital certificate is written. **Name, surname and** certificate holder's **personal tax number** must be **added** into the certificate. The content of the certificate of identity is saved in text format to txt file (together with the .crt 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**.

Hal E-Bank notifies you 7 days prior to certificate expiration. The number of days can be set in the following way:



1. Select **Tools** and **Settings**.
2. Click the **Diverse** tab.
3. Check the »Displaying notifications of certificate expiration« check box and entred the number of days prior to expiry you wish to receive the notification.

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 *www.halcom.rs.* Based on properly completed request for revocation, Halcom CA will revoke a certificate and add it to the list of revoked digital certificates.

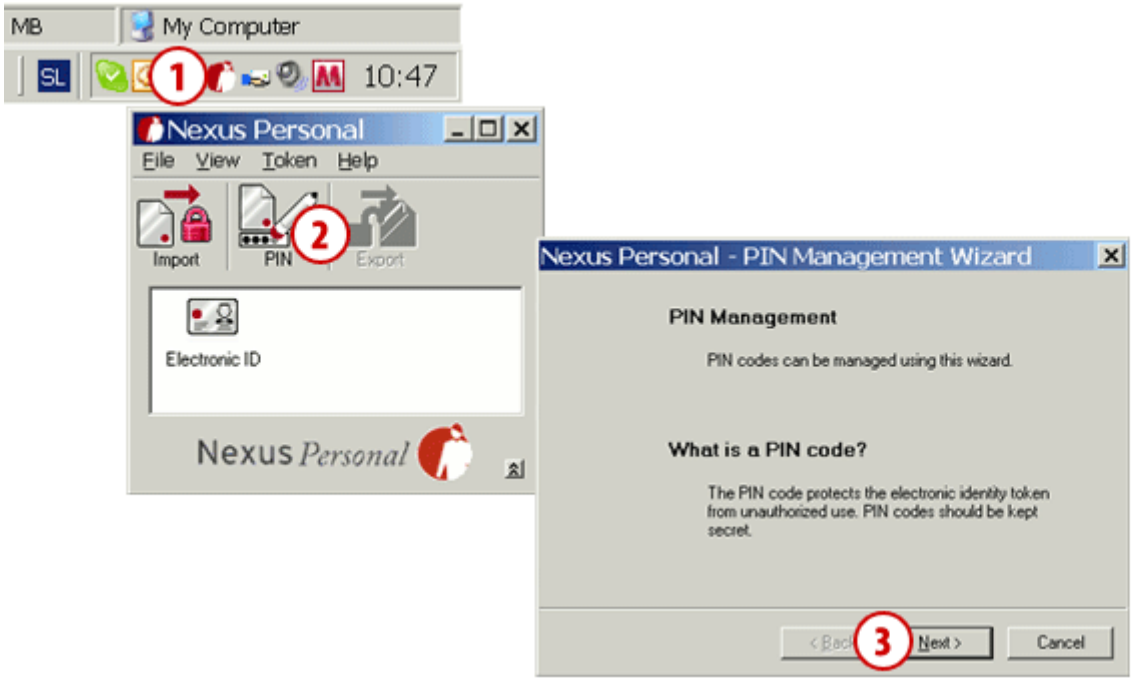
Unblocking of Locked Qualified Digital Certificate

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.

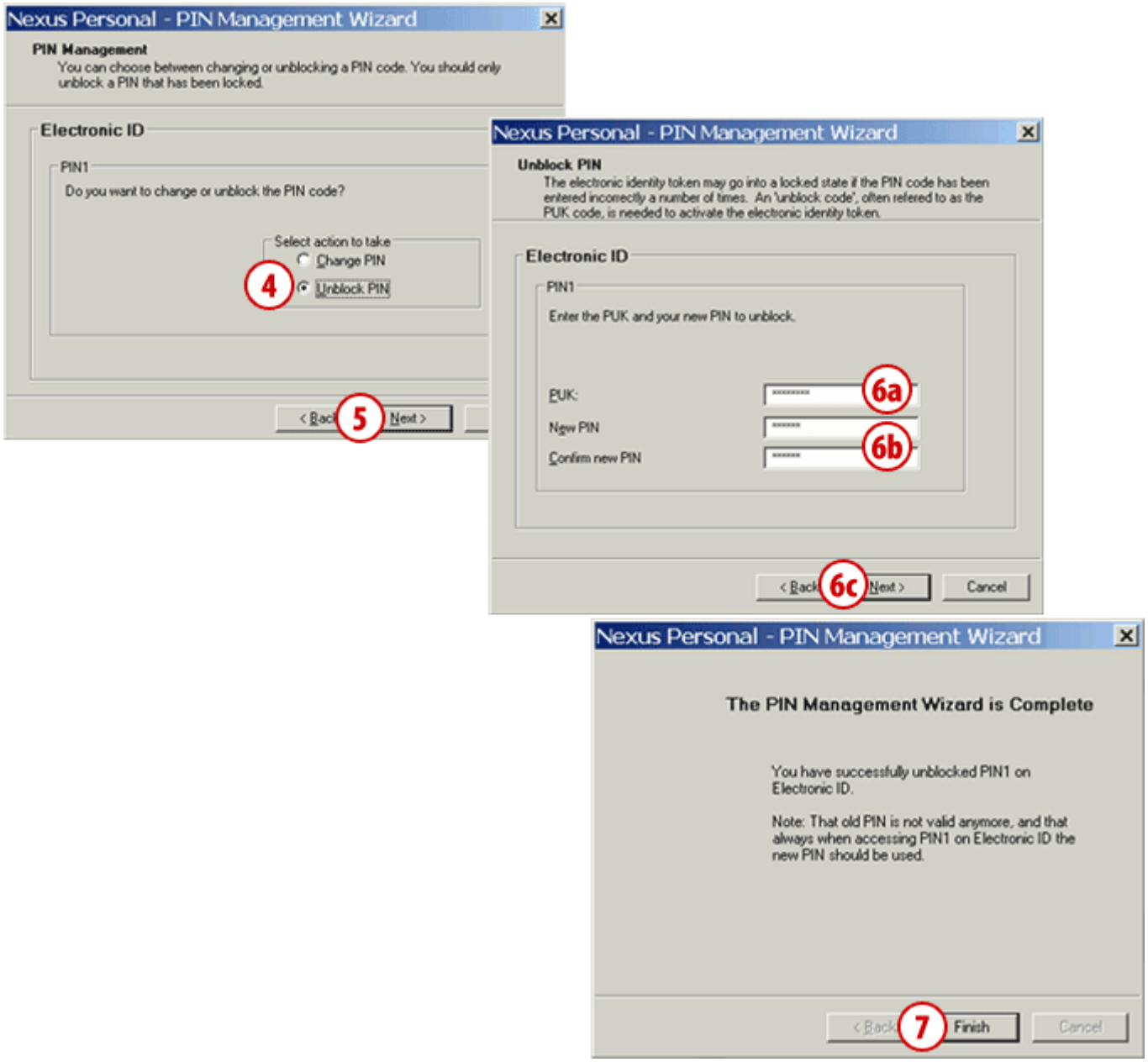
You installed **Nexus Personal** on your computer together with the electronic bank or with the program for using a digital certificate. If the program is installed on your computer, you will see the icon in the bottom right corner on the taskbar. If you don't have the program, you can help yourself with the **UnblockPIN.exe** program, which can be downloaded from the web page *www.halcom.rs* (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)**.

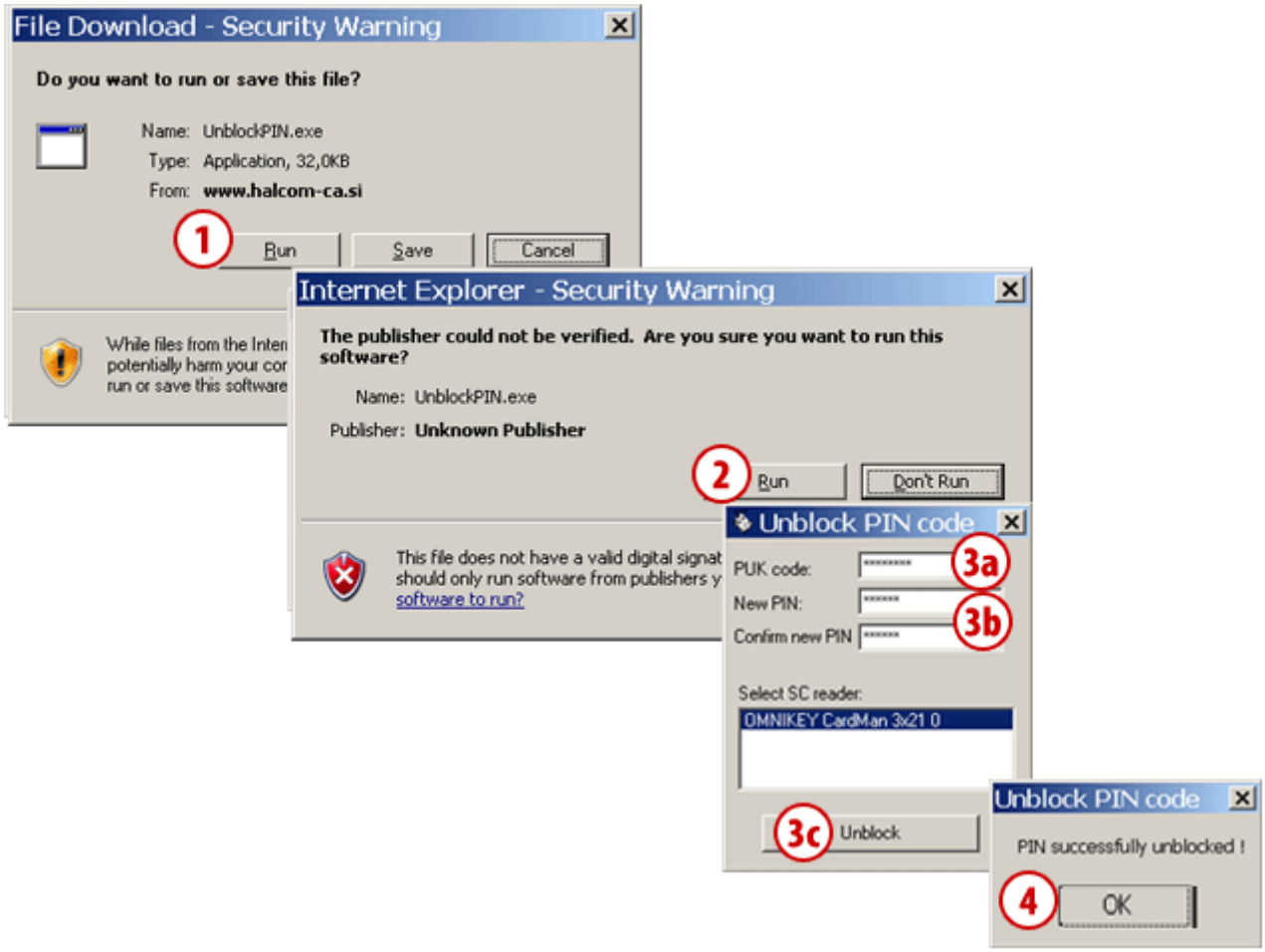
7 Confirm the message on successful unblocking of the digital certificate by clicking the **Finish** button; the certificate is successfully unblocked.

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.

Unblocking 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.halcom.rs*.



1. On the web page *www.halcom.rs*, 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 **Unblock** button **(3c)**.
4. Confirm the message on successful unblocking of the digital certificate; the certificate is successfully unblocked.

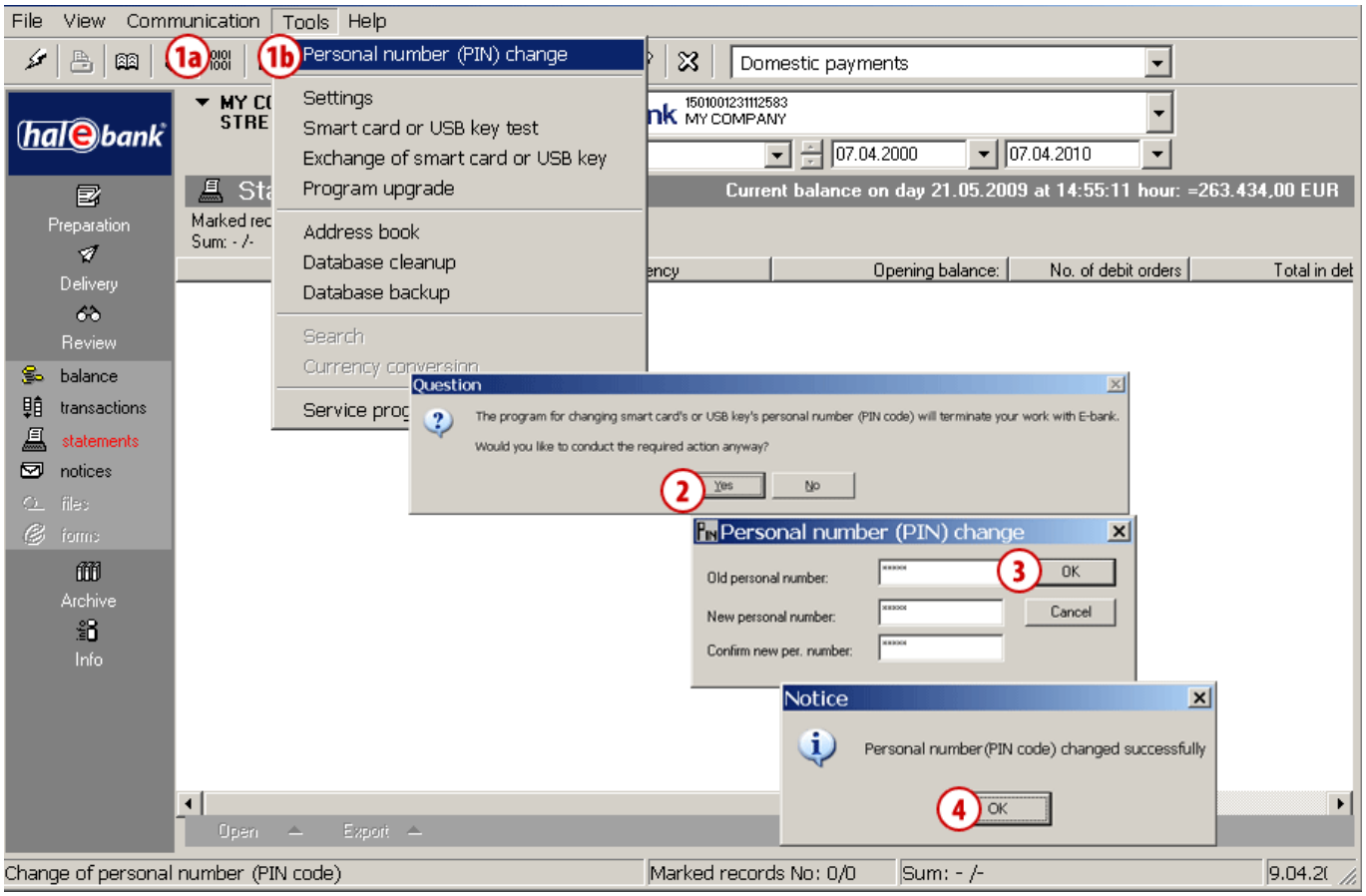
WARNING

- *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.

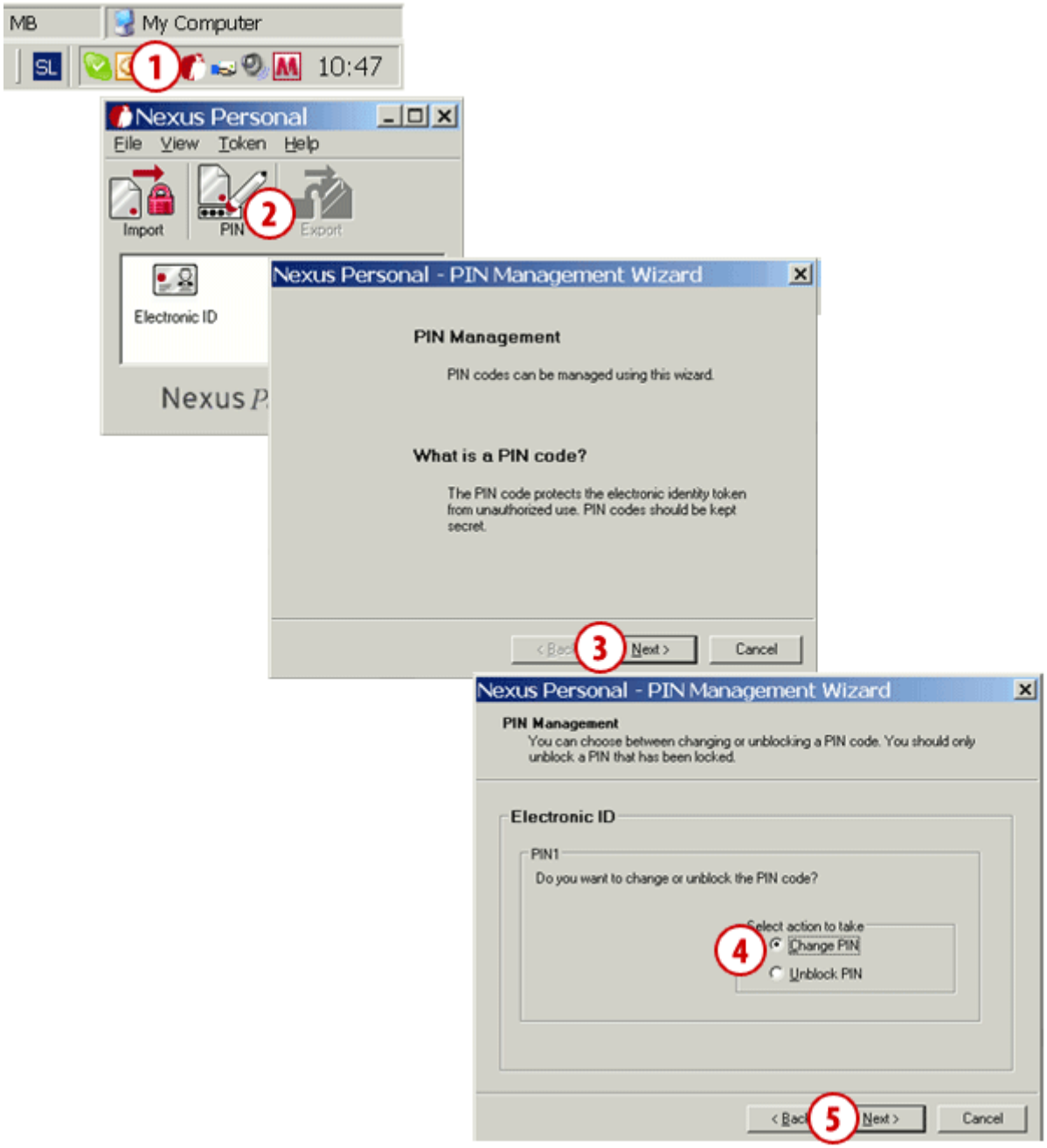
Changing PIN Code in Electronic Bank



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 code) 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.

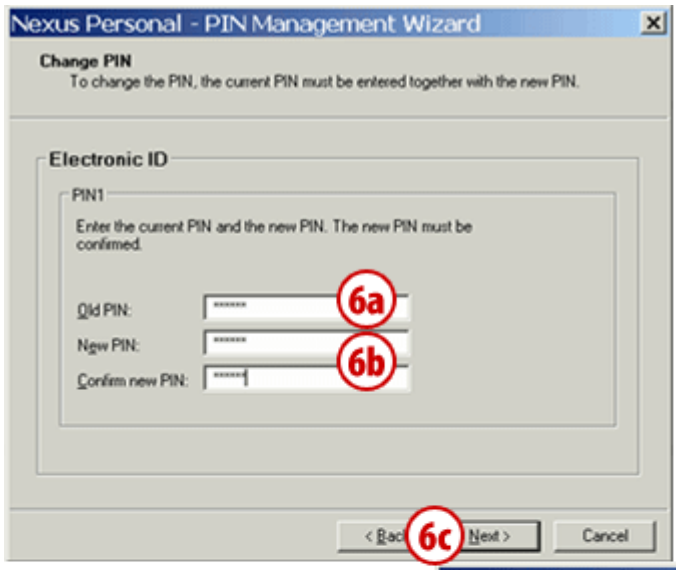
Changing PIN Code by Using Nexus Personal Program

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.