DEKART Logon for Lotus Notes

Users Guide

Pages 41

2004

Annotation:

The following document contains a general description how to use Dekart Logon for Lotus Notes.

Contents

1 Terminology (Glossary)

Dekart Logon for Lotus Notes (DLLN) – Name of product.

KSD (Key Storage Device) – A device where personal information is stored (data necessary to access and work with a Citrix server). A KSD can be either smart card or USB token. The KSD can be secured with a PIN code, or can work without PIN.

PIN (Personal Identification Number) – A personal identification number that is used to access information stored on the KSD. The PIN code length can be from 4 to 8 characters, and should always be memorized, or be in the possession of only the KSD holder.

Biometric Authentication - user authentication based on verification of specific physical characteristics of the user by means of special biometric equipment. Biometric authentication can be based on verification of fingerprints, iris, voice, and other specific characteristics of human body.

Two-Factor Authentication - this is a process controlling the authenticity of the user's identity on the basis of the two following factors: *"Something You Have – for example, the KSD device"* and *"Something You Know — for example, the user name and password, PIN-code"*.

Three-factor authentication - is a process controlling the authenticity of the user's identity on the basis of the three following factors: *"Something You Have – for example, the KSD", "Something You Know — for example, the PIN code", "Something You are – for example, the user's BIO ID"*.

2 Purpose of Dekart Logon for Lotus Notes

Dekart Logon for Lotus Notes enables secure access (three-factor) to Lotus Notes and Lotus Notes resources.

3 General Description

Dekart Logon for Lotus Notes is a software and hardware solution that enables secure user access to Lotus Notes, and Lotus Notes resources. The solution utilizes strong (three-factor) authentication, and enables temporary blocking of access to Lotus Notes, so that only authorized users are able to work with Lotus Notes resources.

Security principles of Dekart Logon for Lotus Notes

1. Security is enabled for Dekart Logon for Lotus Notes due to the use of a KSD (PIN Code protected) that stores the users ID-file, password for Lotus Notes and user's BIO ID. This method does not require the user to store this information on the computers hard drive, thereby increasing the level of security.
2. The user is authorised to access the secured resources (Notes database(s)) only after he connects the KSD to the computer or workstation, enters correct PIN code and passes biometric verification procedure (voice, fingerprint etc.). When the KSD is removed from a workstation running Lotus Notes v.5.09, access to the database and Notes session is automatically terminated, and the ID file is closed. In Lotus Notes v.6.0.1 and higher, detachment of the KSD, temporarily blocks the system (Logout).

3. After multiple wrong PIN code entries, the KSD will be blocked. ***Note. Various KSD's have different settings for rejection of erroneous PIN code entries, and vary from 3 to 10 attempts before blocking the KSD (see attachment)***.
4. DLLN, with the help of the KSD enables you to automatically generate complex passwords for Lotus Notes, based on random characters, thereby increasing the security level, and does not require the user to remember their password for Lotus Notes, but only just their PIN code for the KSD.

Features of Dekart Logon for Lotus Notes

1. Convenient for end-users - no need to remember complex passwords to enter Lotus Notes.
2. Mobility– ID-file and password for Lotus Notes are saved to the KSD, therefore, allows you to work with Lotus Notes resources from any workstation in the network. It is sufficient for you to connect your KSD and enter your PIN Code.
3. Flexibility – optionally, you can access Lotus Notes with a password, without using a KSD.
4. Compatibility- the KSD can be used not only for DLLN, but also other applications such as: Dekart Logon и Dekart Private Disk.

Product components

The product is delivered with a CD containing the application DLLN, and a KSD that enables you to securely access Lotus Notes, a users guide.

The KSD can be from any one of the below listed vendors, and products, depending on customer requirements, or suppliers.

- Aladdin eToken PRO;
- Aladdin eToken R2;
- Schlumberger Multiflex;
- Schlumberger Cryptoflex;
- Schlumberger Payflex;
- Rainbow iKey 1000;
- Rainbow iKey 2000;
- Rainbow iKey 2032;
- Rainbow iKey 3000;
- Eutron CryptoIdentity ITSEC;
- Eutron CryptoIdentity 4;
- Eutron CryptoIdentity 5;
- Datakey Model 310;
- Datakey Model 330;
- GemPlus GPK.

Attention! Before you purchase a USB token or smart card, please make sure that it has enough memory to store the identity keys of the user (ID file for Lotus Notes). Take into account that the part of KSD memory may be allocated to other data, e.g. BIO ID. You can determine the memory usage of the card and read the USB token or smart card using the Dekart Key Manager Utility, as well as delete all unnecessary information using Dekart Key Manager or format the token or smart card using a Key Formatting utility or Corporate Key formatting utility.

Note 1. Some KSD characteristics are described in an attachment to this guide.

Note 2. Dekart delivers KSD's without a PIN Code.

System requirements

Hardware requirements

- Personal computer, with a minimum of one port (COM, USB), for connection of a KSD.
- In the event a smart card is used as a KSD, then a PC/SC compatible smart card reader is also required.
- If the user prefers to use three-factor authentication, a biometric device should be used, i.g. BioLink U-Match Mouse.

Software Requirements

- Operating systems: Windows 98, NT4.0, 2000, ME, XP.
- Lotus Notes v.5.09, 6.0.1 and higher.
- KSD drivers.
- Drivers of biometric device.

Note. In Lotus Notes you must install a password (in the Set Password menu File->Tools->User ID in Lotus Notes v.5.09 or in Change Password menu File->Security->User Security in Lotus Notes v.6.0.1 and higher).

In addition to secure the database in Lotus Notes you must select the encryption option (Encryption Setting in File > Database, and select to Locally encrypt this database).

Attention!

In order to receive complete information regarding Lotus Notes and Domino (settings, procedures, features, etc.) you must contact IBM, or visit the Lotus web site www.lotus.com.

Detailed information about biometric devices, used for authentication (features, software etc) can be obtained from BioAPI Consortium at www.bioapi.org.

4 Installation of Dekart Logon for Lotus Notes

1. If you have previously installed eToken for Secure Logon (eT4LN), it is necessary to de-install it from Windows (in **Control Panel** > **Add or Remove Programs, select the product and click Uninstall**).
2. Before beginning the installation, it is necessary to close all open applications.
3. In order to enable three-factor authentication, the biometric device should be connected and its drivers should be installed. ***Note: If the user hasn't previously installed the software working with biometric devices, then BioAPI Framework should be installed on the computer before installing device drivers (the BioAPI Framework can be downloaded from www.bioapi.org, Implementation section).***
4. In order to install Dekart Logon for Lotus Notes, you must launch LNLogon.exe. The program will check to ensure that the following guidelines have been adhered to:
   - If Lotus Notes, or KSD device drivers have not been installed, the program will display an error message, and the installation process will be terminated.
   - If Lotus Notes has already been launched, you will receive an error message and the program loading process will be terminated.
5. If all loading requirements have been fulfilled, you will see an window that displays the below figure, and you should then press **Next**.

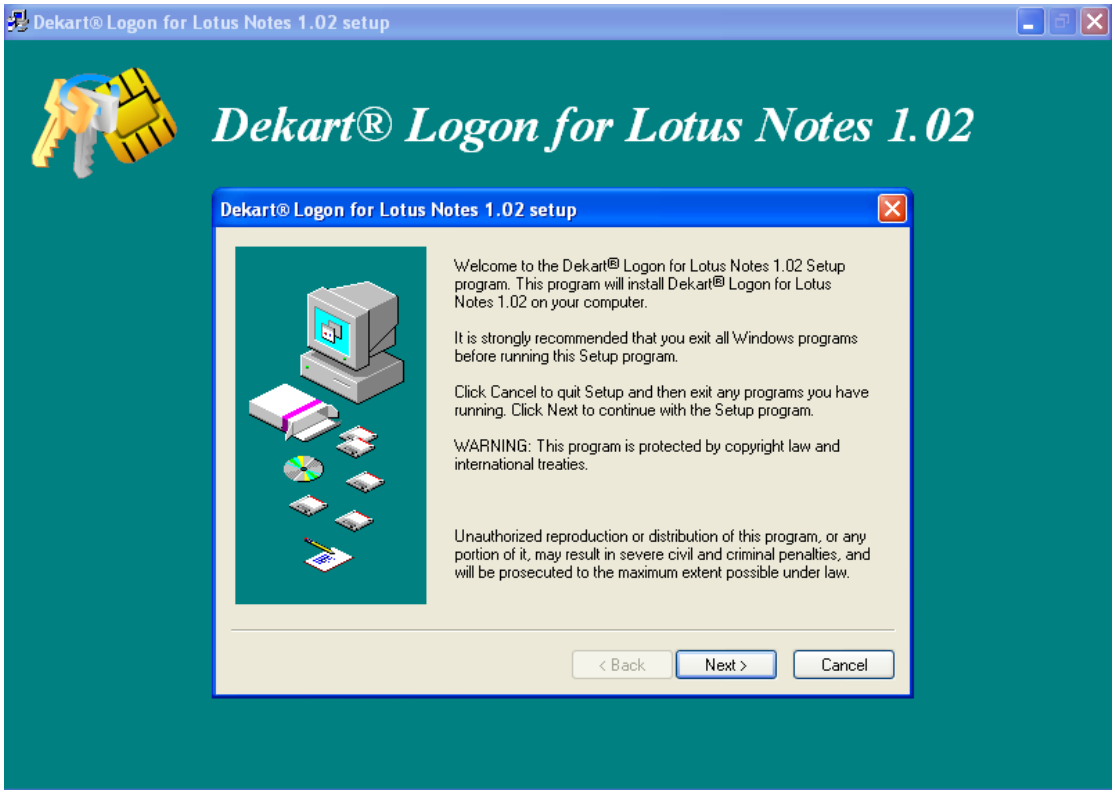

Figure 1

6. You will then see the Dekart licensing agreement. In order to continue, the user must agree with the terms in order to proceed with the installation

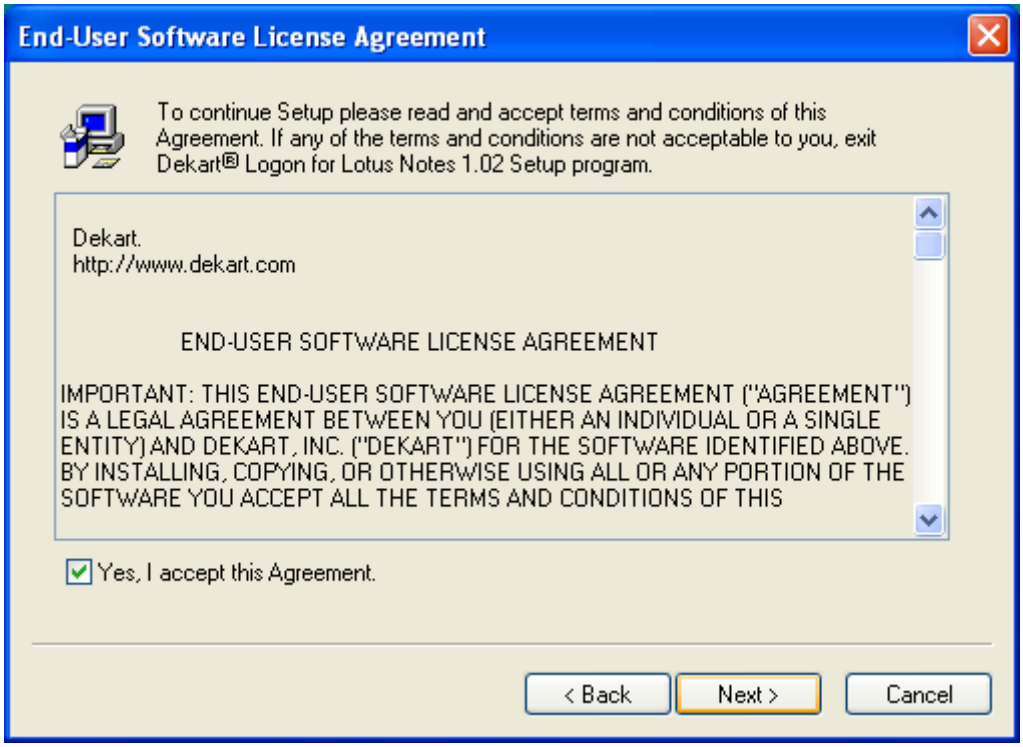

Figure 2

7. The next step in the installation process will require the user to enter the serial number of the DLLN product.

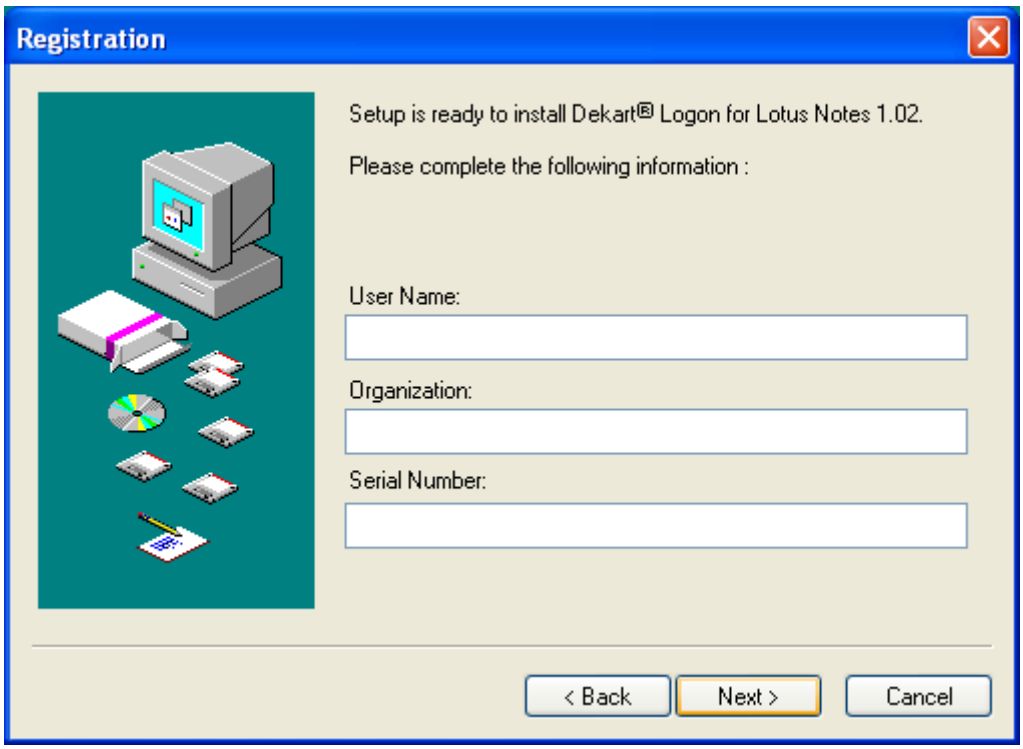

Figure 3

8. Next, the user must indicate the folder in the **Start Menu** where the DLLN administrator utility for Dekart Logon for Lotus Notes will be located.

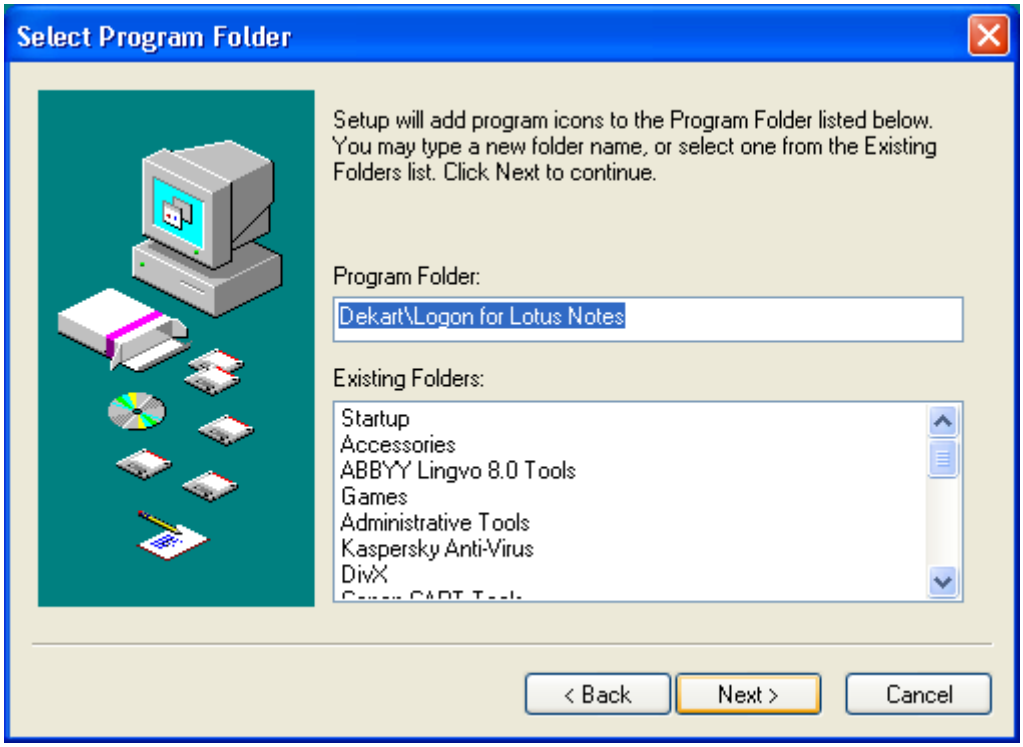

Figure 4

9. Upon completion of this step, it is necessary to select, and click on the **Finish** button.

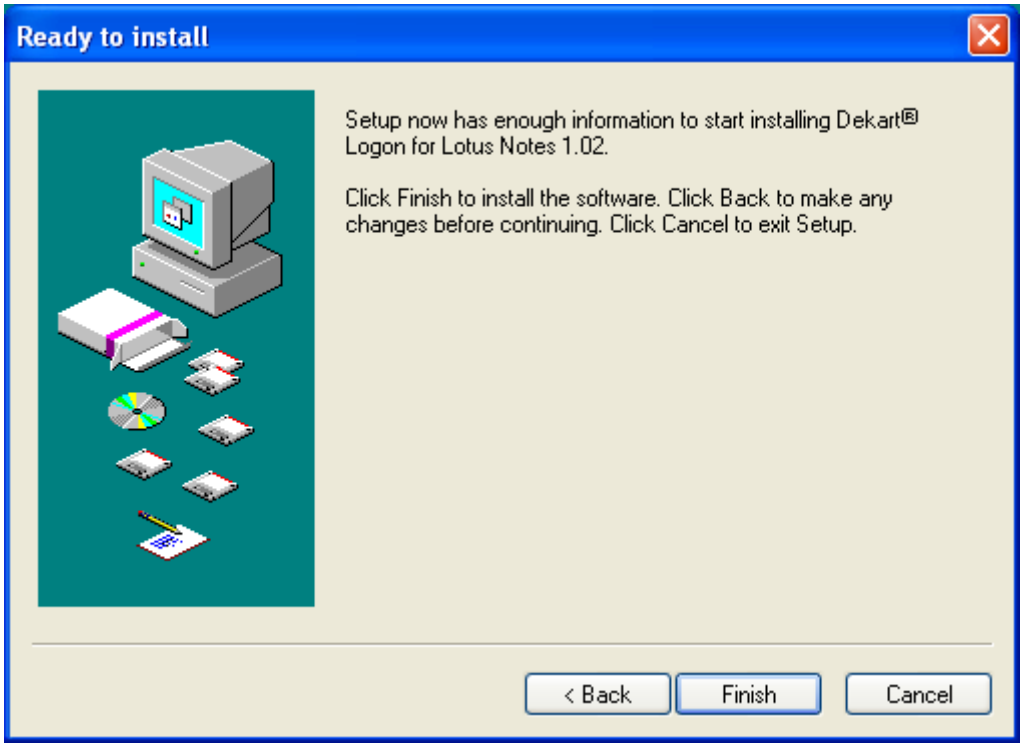

Figure 5

After this step, the program will copy all necessary files, and make changes to the INI-file of Lotus Notes, and the installation will be completed.

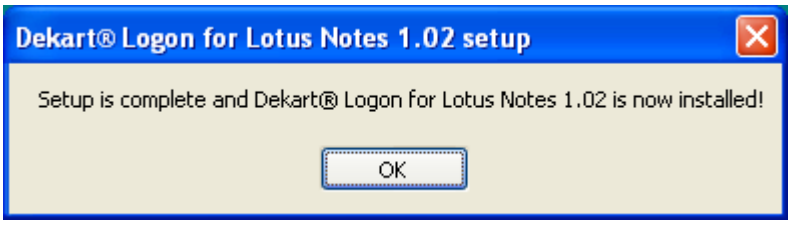

Figure 6

Note: Upon completion of the installation of Dekart Logon for Lotus Notes, it is necessary to restart your computer.

5 Update of Dekart Logon for Lotus Notes

1. After re-installing (updating) DLLN, the program automatically checks for a previous version of the application, and will collect all required system information.

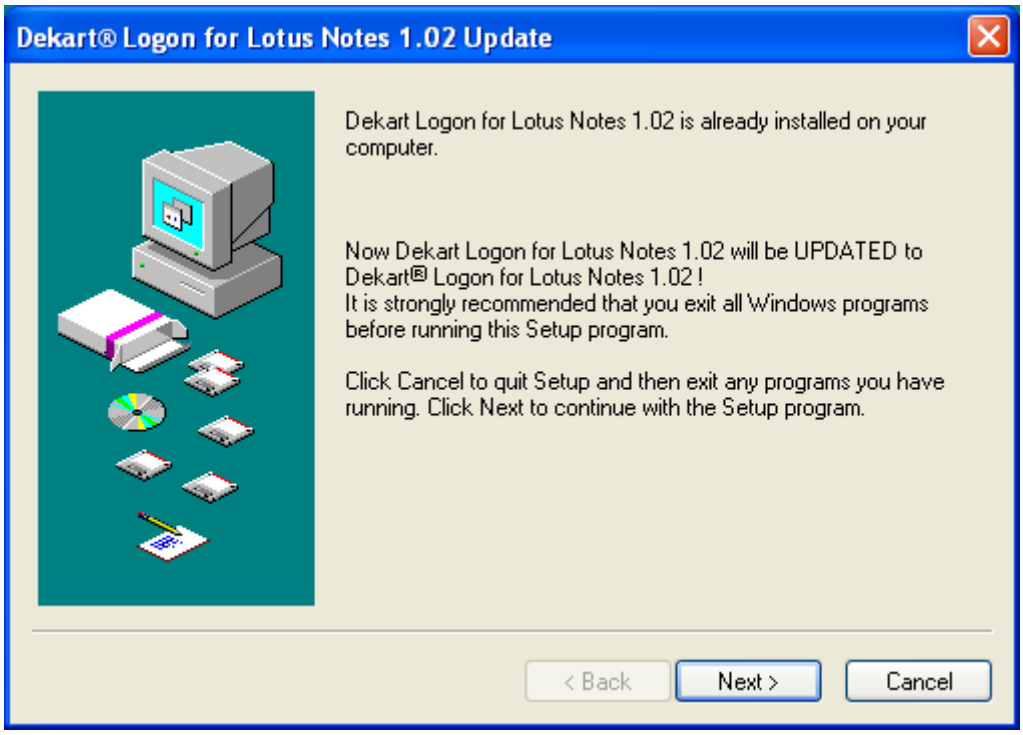

Figure 7

2. In order to continue with the update process, you must click on the **Next** button, after which you will see the Dekart licensing agreement, which the user must accept.
3. In order to complete the process of updating DLLN, you must click on the **Finish** button.

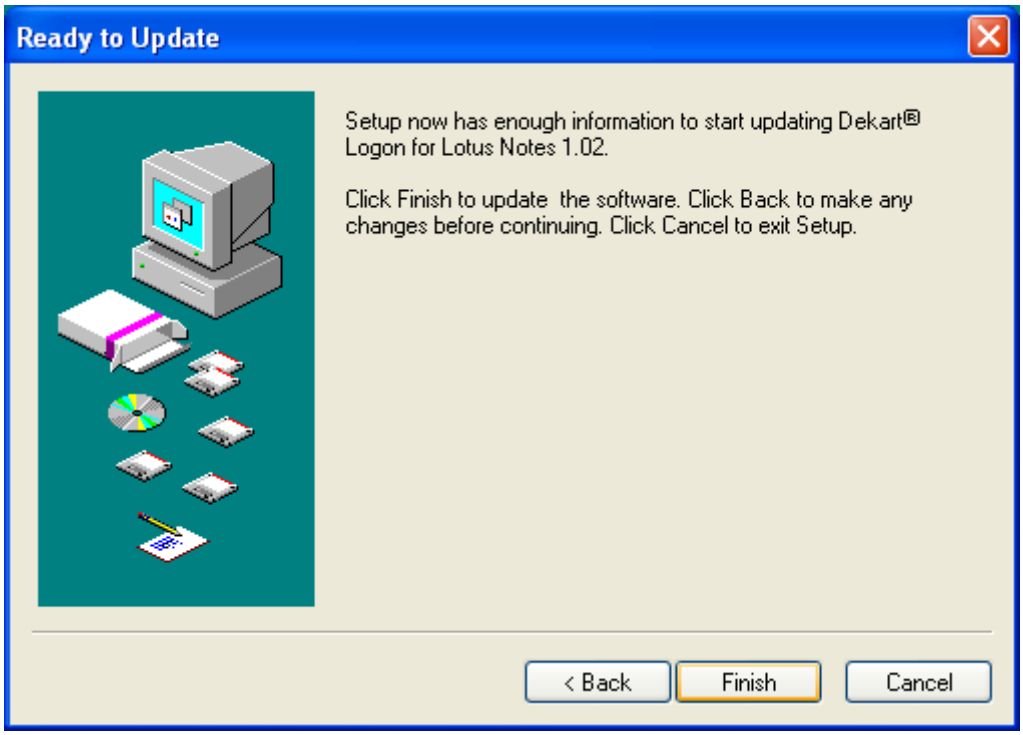

Figure 8

The program will overwrite all previous files, and in the case of a newer version of DLLN, the program will install all updated files.

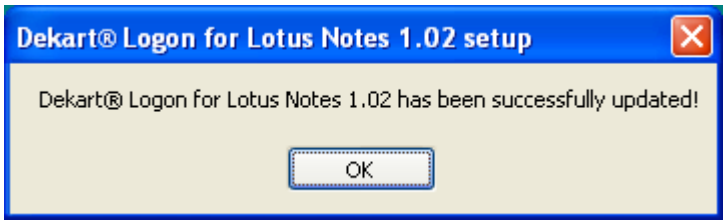

Figure 9

Note. After updating Dekart Logon for Lotus Notes, it is necessary to reload your computer.

6 De-installation (removal) of Dekart Logon for Lotus Notes

In order to de-install DLLN:

1. In the **Start Menu**, select **Programs**, indicate the folder name that was entered in step 8 of the installation procedure (see para.4), select **Uninstall** (alternatively, in **Control Panel** select **Add or Remove Programs** and press the **Uninstall** button).

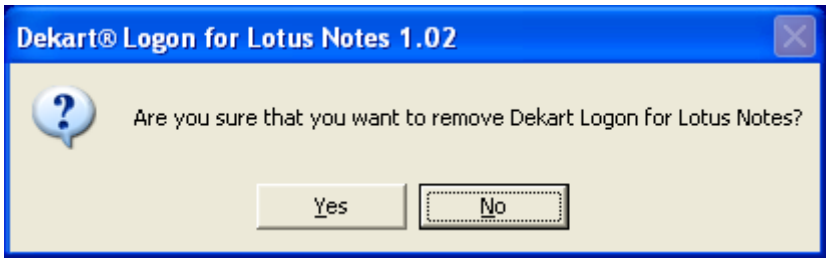

Figure 10

The user must confirm their intent to de-install (remove) Dekart Logon for Lotus Notes, press the **Yes** button.

2. After successful completion of the de-installation process, you will see the following message:

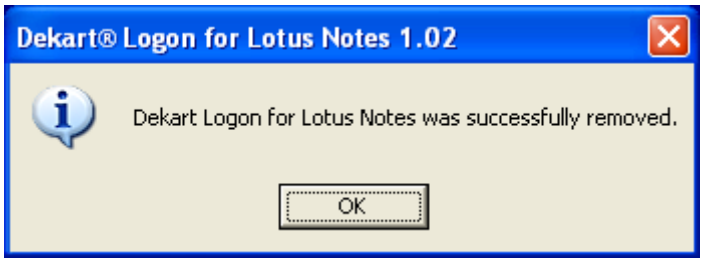

Figure 11

7 KSD Administrator Utility

The KSD Administrator Utility enables you to prepare the KSD device for access by a specified user to Lotus Notes, and to service during operation.

The main window in the program displays a table containing all KSD connected to computer, the label or identifier (*KSD Label or ID*) and login for Lotus Notes (*KSD Information*). The buttons, perform the following functions:

Key Storage Device and Biometric ID operatiosns:

Verify PIN	The PIN-code for verification
Change PIN	Changes the PIN-code
Change Label	Changes the label of the KSD
Clear KSD	Clears the KSD of all Lotus Notes data
Change BIO ID	Change biometric identifier

Lotus Notes operations:

Change ID file	Changes the ID file on the KSD
Detach ID file	Saves to disk the ID file from the KSD
Show [Notes PASSWORD]	Displays on screen the password for Lotus Notes
Change [Notes PASSWORD]	Changes the password for Lotus Notes

Close	Closes the window (application)

Launching the Utility

1. Launching the utility can be done in the following way: In the **Start Menu** select Programs and further select the folder where the application is located (see step 8 in para.4).

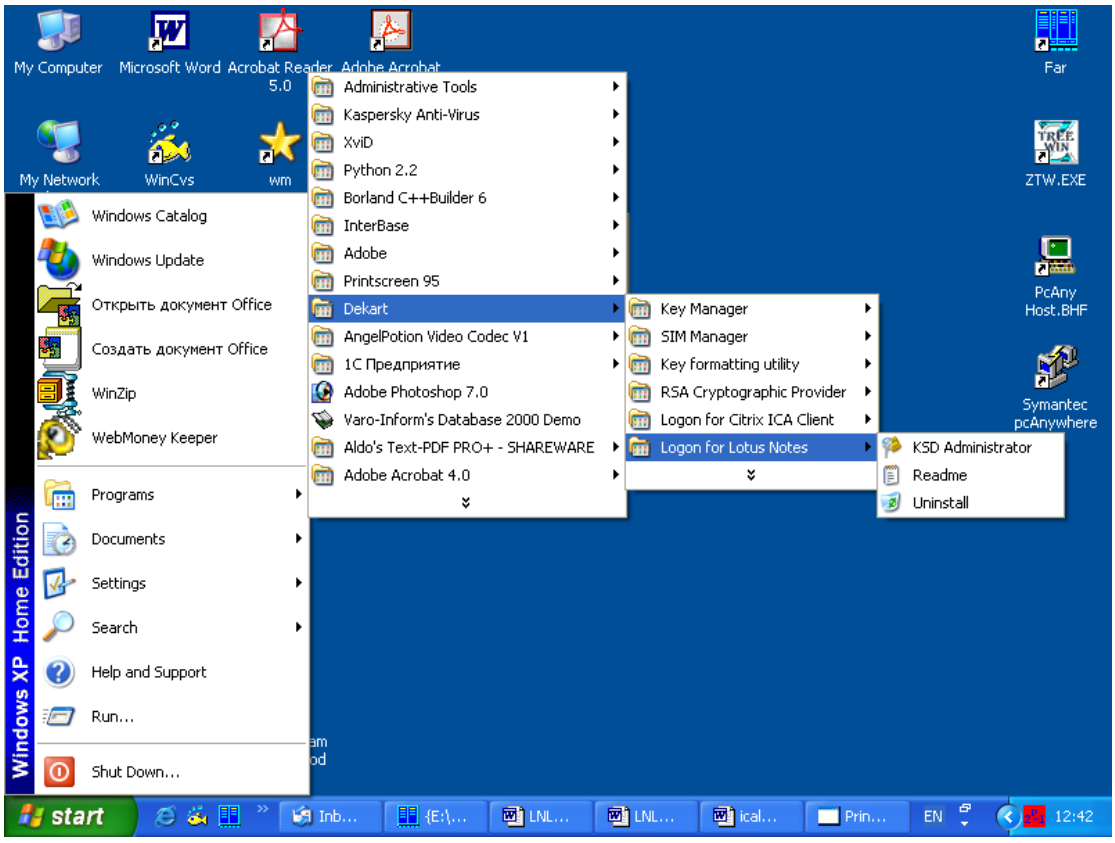

Figure 12

The main window of the program appears.

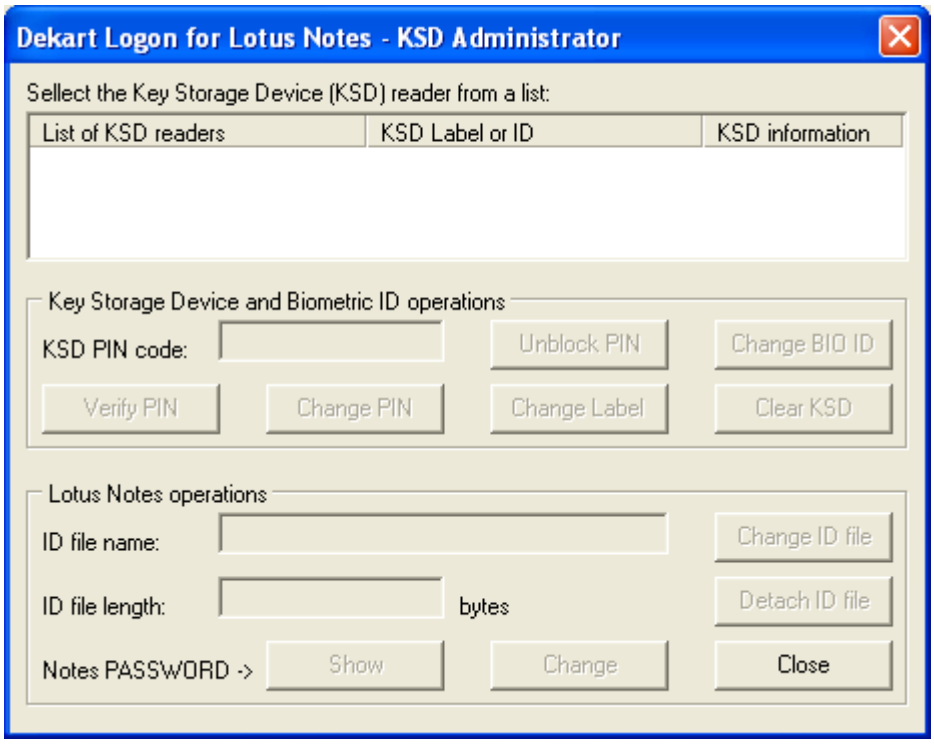

Figure 13

2. The user must connect their KSD to the computer. In the list (*List of KSD readers*) information concerning all KSD's connected to computer will be appeared.

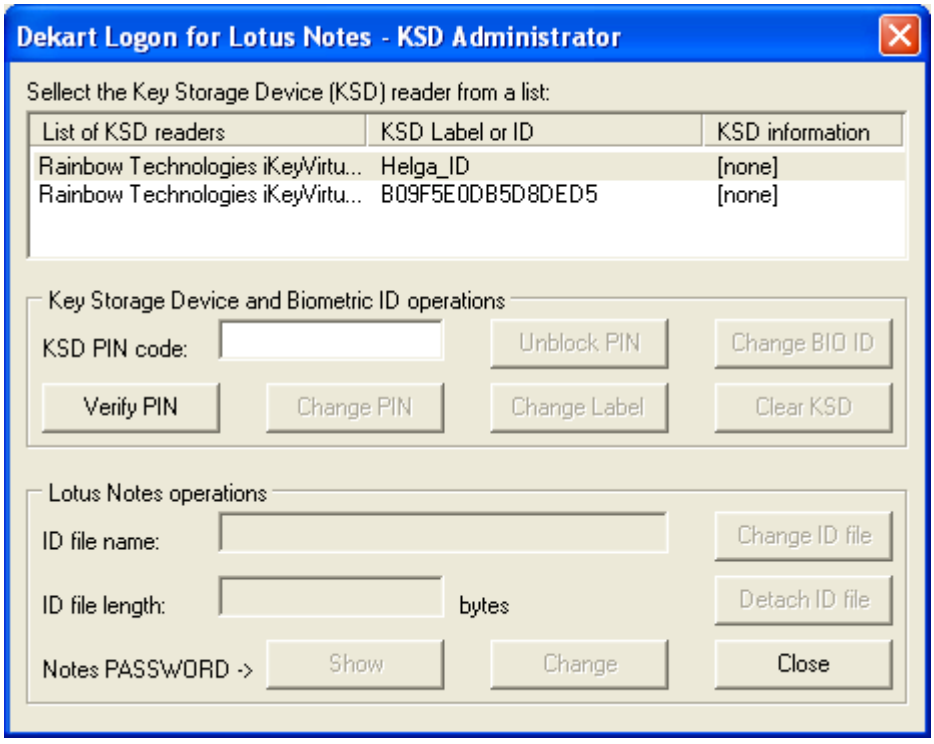

Figure 14

3. With the aid of your mouse, select the needed KSD (in this event the **Verify PIN** button is activated).

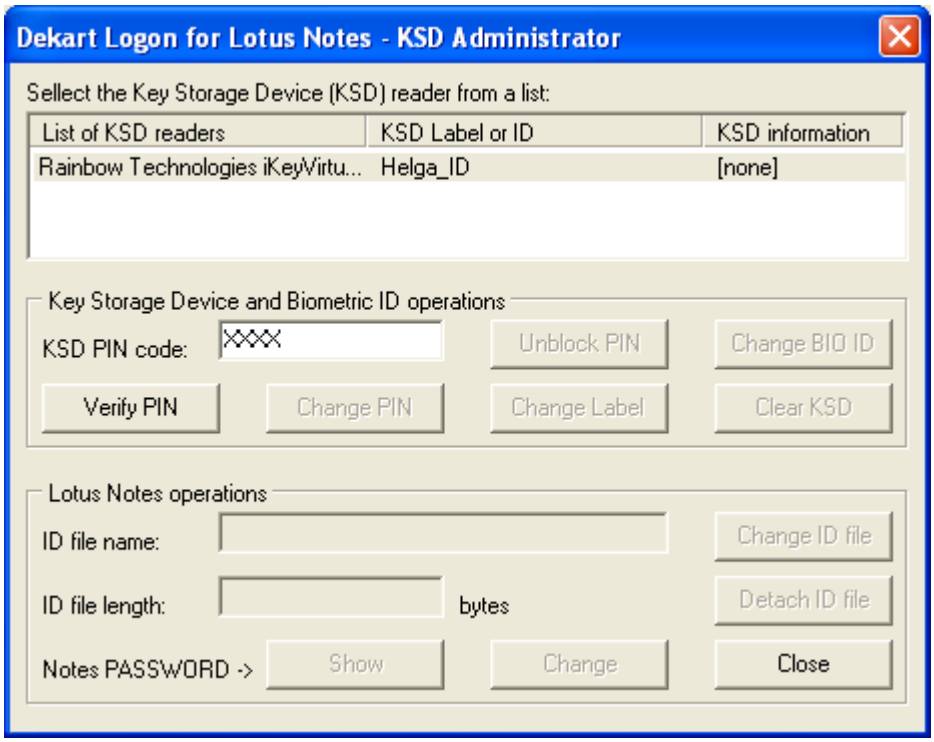

Figure 15

4. In the field **KSD PIN code**, the user must indicate the PIN-code and press the **Verify PIN** button.

Attention! Several incorrect PIN-code entries will result in a blocked KSD!
The number of incorrect entries allowed is dependent on the KSD type, and is indicated in the attachment.

Note: Dekart delivers KSD's without a PIN Code, in this case "Verify PIN" is not required for KSD's delivered by Dekart.

Upon successful verification of the PIN-code, several buttons become available in the main menu:

- During preparation of the KSD for use with DLLN (utilizing a new KSD) - **Change PIN, Change Label, Change ID file, Change BIO ID** (Figure 16**);**
- While servicing a KSD that is in use, - all buttons, except **Verify PIN,** the fields **ID file name** and **ID file length** are automatically displayed (Figure 17).

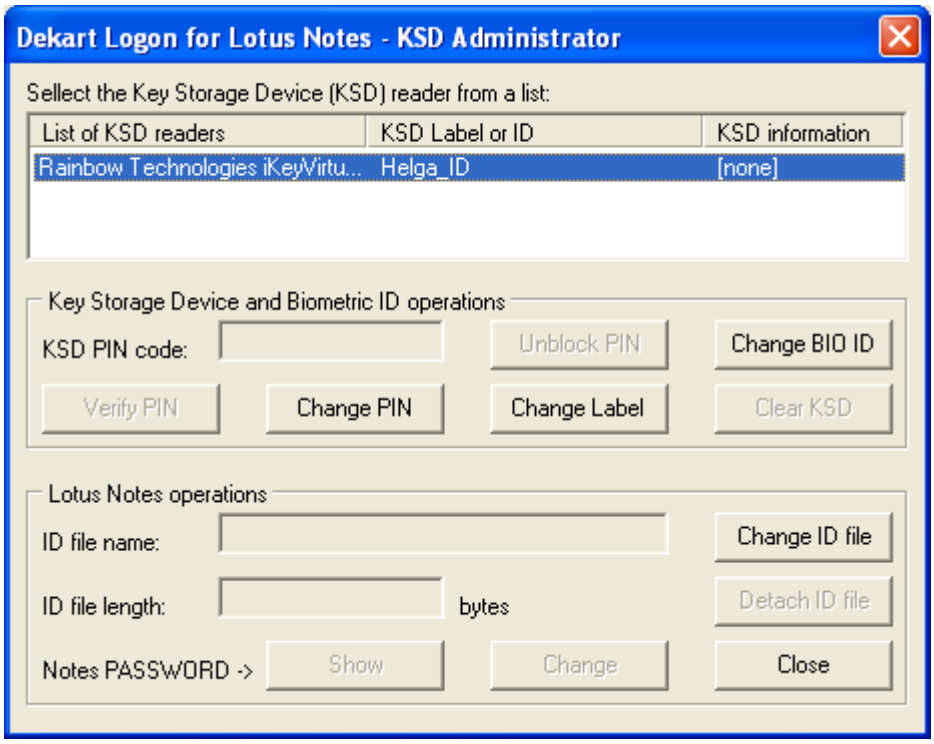

Figure 16

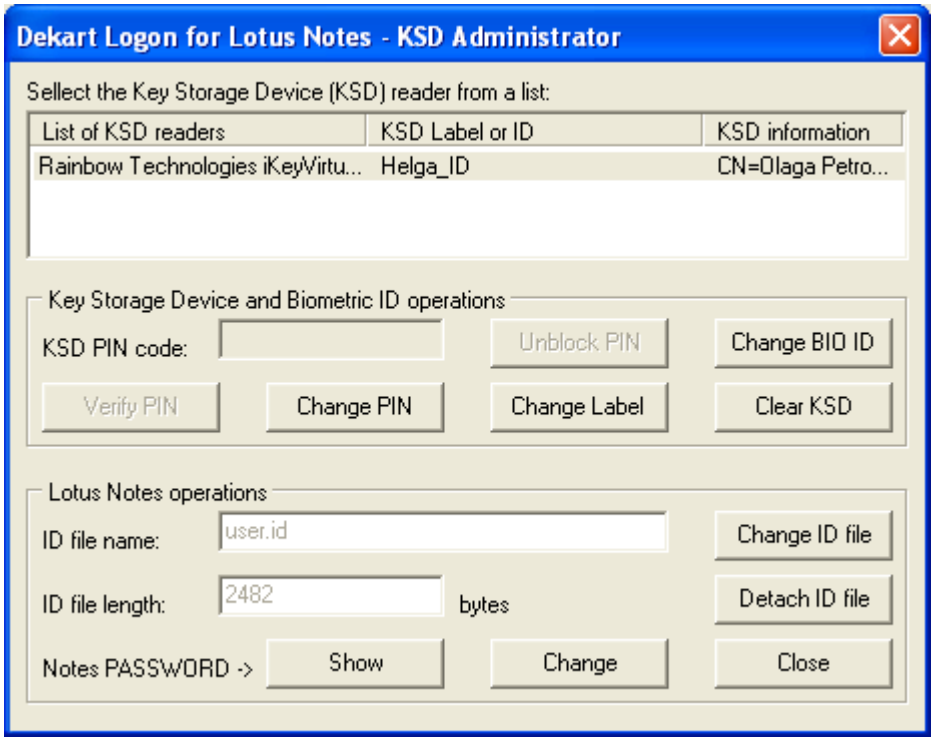

Figure 17

Note: If the BIO ID is stored on the KSD, the software will automatically detect it and will attempt to conduct biometric authentication.

Preparing the KSD for use

After launching the utility, connecting a new KSD the program will display the following window:

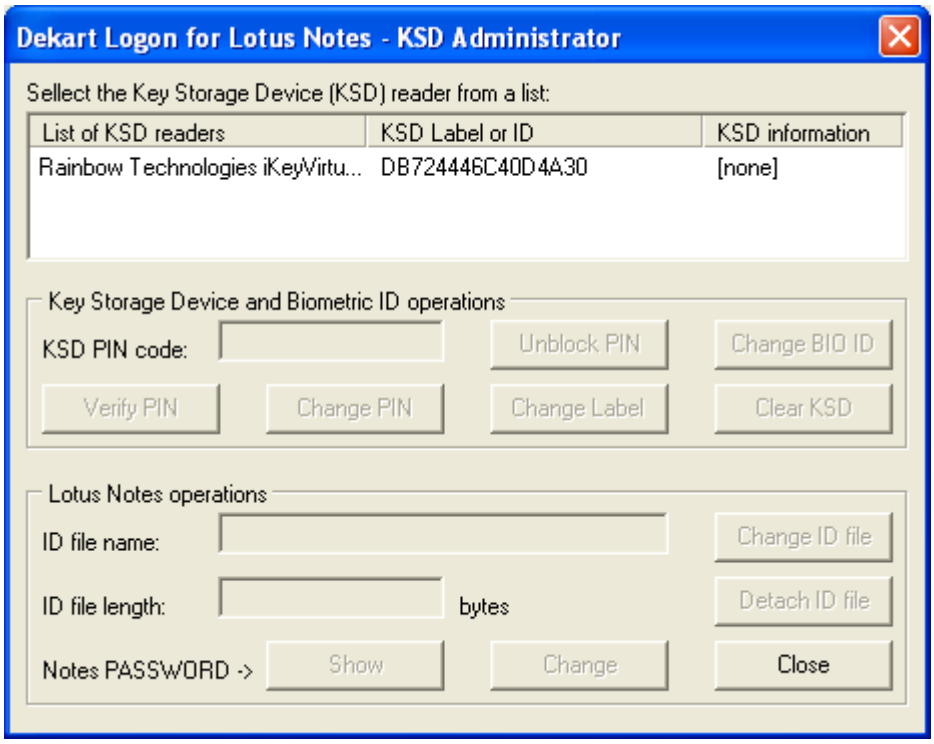

Figure 18

Note. If the KSD is new, then in the field KSD Label or ID, the serial number of the KSD is displayed. In the future, the user can change this parameter.

1. The user must select the KSD in the *List of KSD readers* with their mouse.

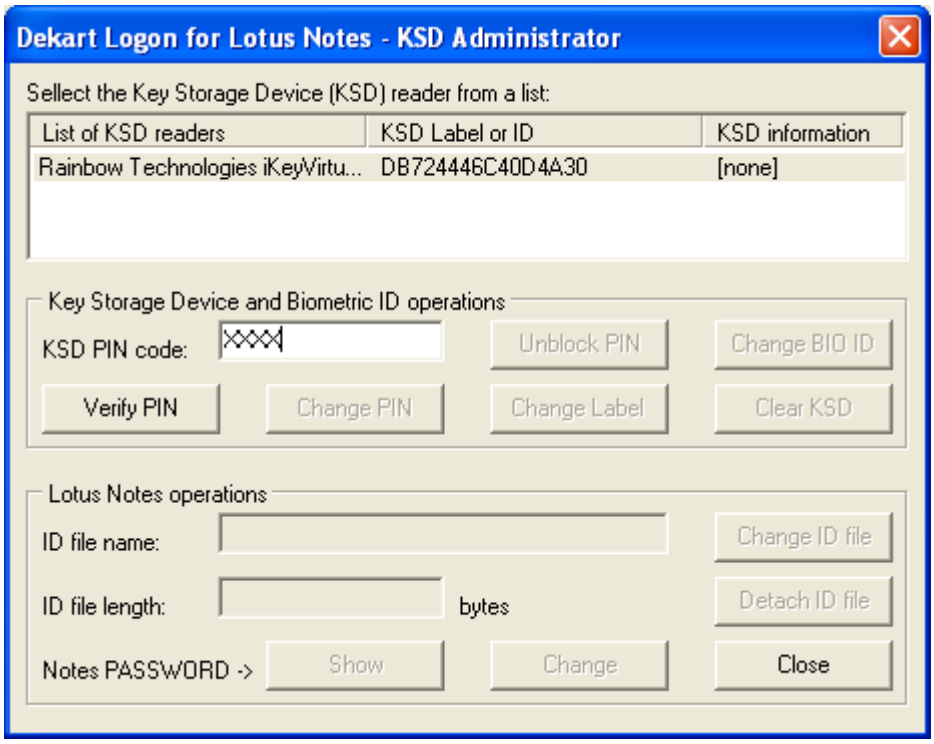

Figure 19

In the event the specified KSD is secured with a PIN-code, it is necessary to enter the PIN code, and press **Verify PIN.**

This activates the **Change PIN, Change Label, Change ID file, Change BIO ID** buttons (see Figure 16).

2. Press the button **Change ID file.** The dialog window *Change ID file - Select ID file* (see Figure 20) is activated.

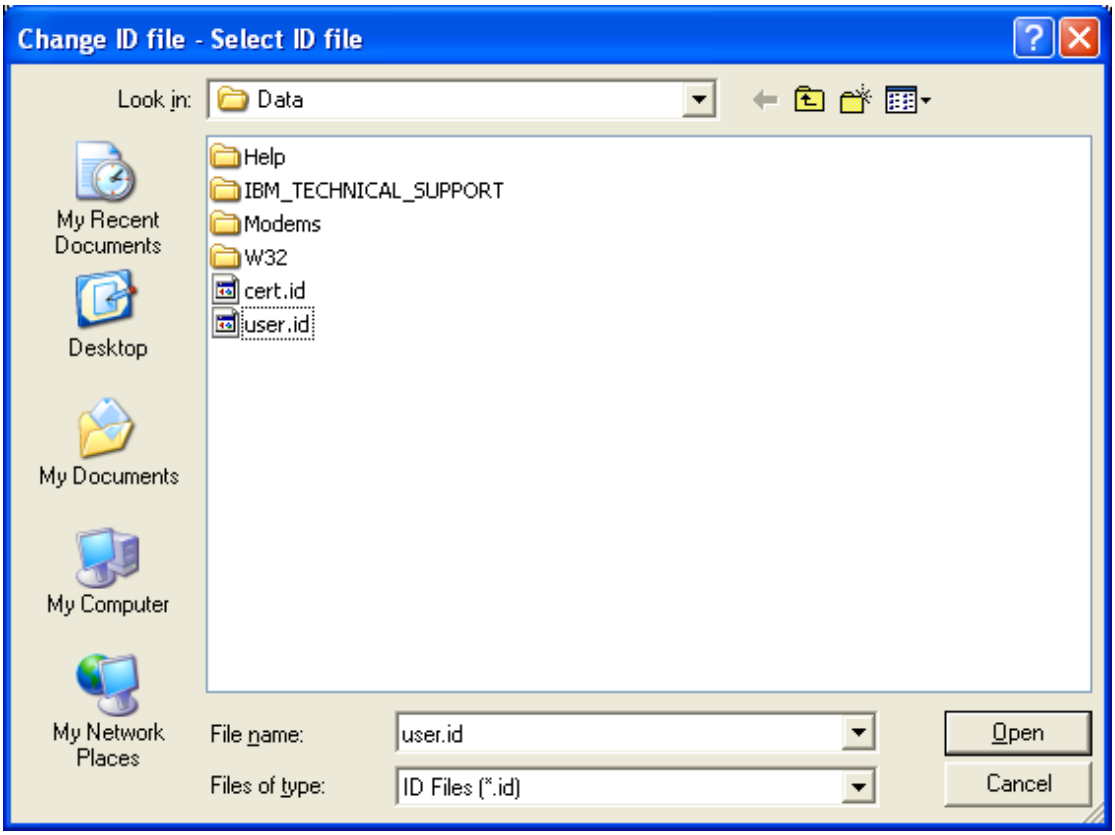

Figure 20

3. The user must indicate the file user.id (see Figure 20) and press the **Open** button. The dialog *Initialize Notes – Select "notes.ini"* appears. It is necessary to select the file notes.ini and press the **Open** button.

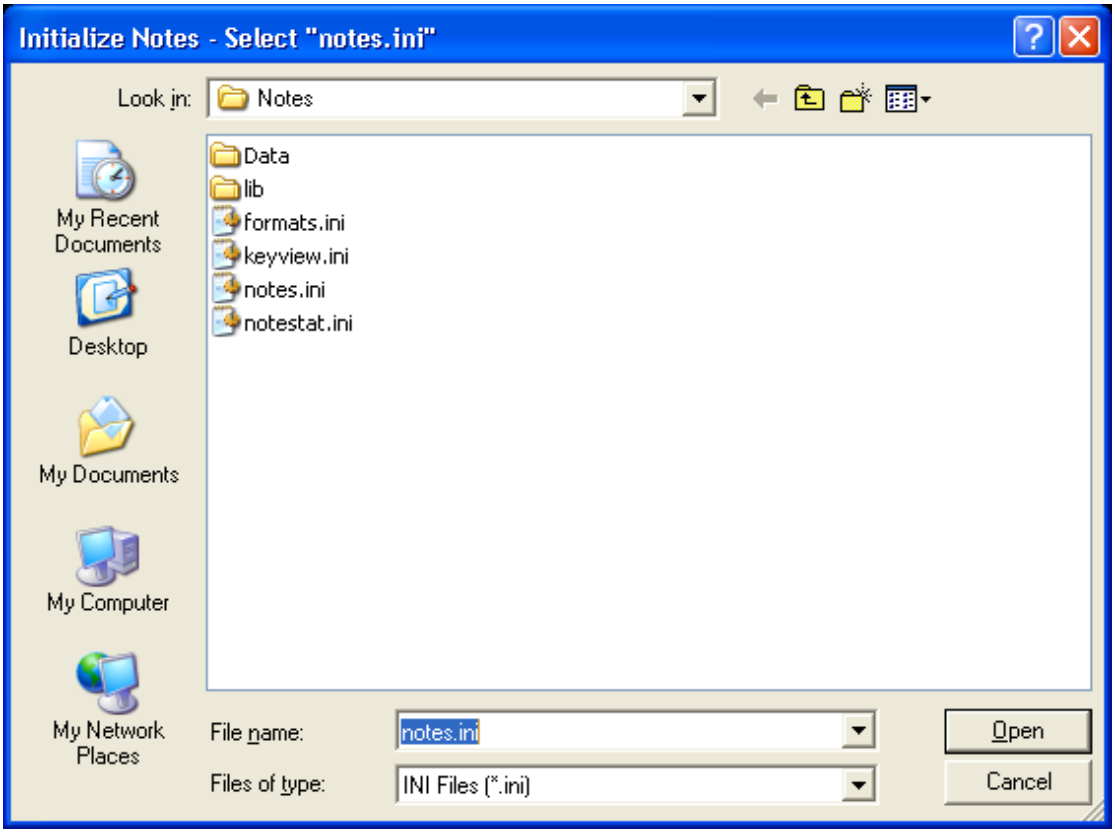

Figure 21

4. After indicating the file to be initialized, you will be prompted for the password for Lotus Notes (ID file). The user must then enter their password, and press **OK.**

Figure 22

After successful completion of this procedure, the window will appear as indicated below (see Figure 23) – all buttons are activated, except **Verify PIN**, and the **ID file name, ID file length** fields are displayed.

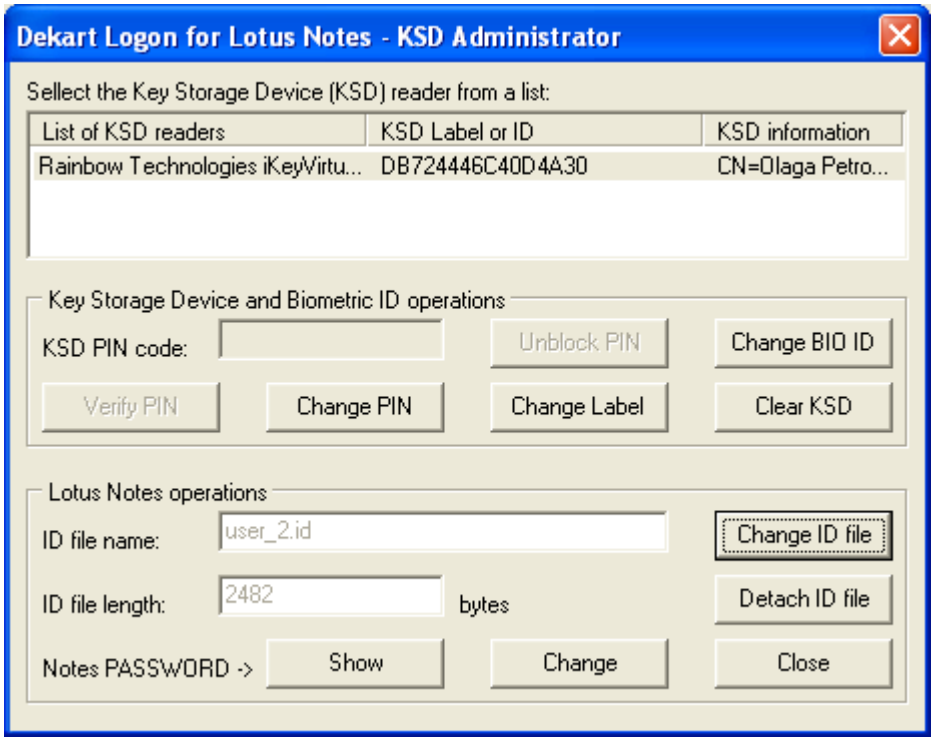

Figure 23

Upon the completion of this process, the KSD is ready for use.

Note: In order to raise the level of security, it is recommended that a PIN code will be established by user using the "Change PIN" function.

Adding BIO ID to KSD

In order to enable three-factor authentication, the KSD should store user's biometric identifiers.

Note: The biometric device choice is determined by the physiological characteristics of user and the location of his computer.

In order to add BIO ID do the following:

1. Click the **"Change BIO ID"** button in program window. The window with the list of installed drivers for biometric devices will appear.

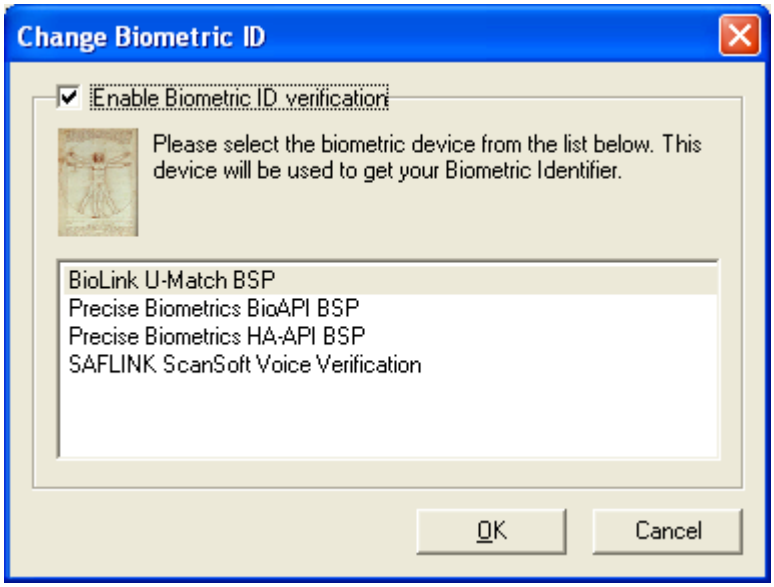

Figure 24

2. Check the **"Enable Biometric ID verification"** checkbox and choose the biometric device from the list.

3. If the fingerprint scanner is used, e.g. BioLink U-Match, the user will be required to provide his fingerprints for scanning for several times. As soon as the scanning procedure is complete, the user's BIO ID is stored on the KSD.

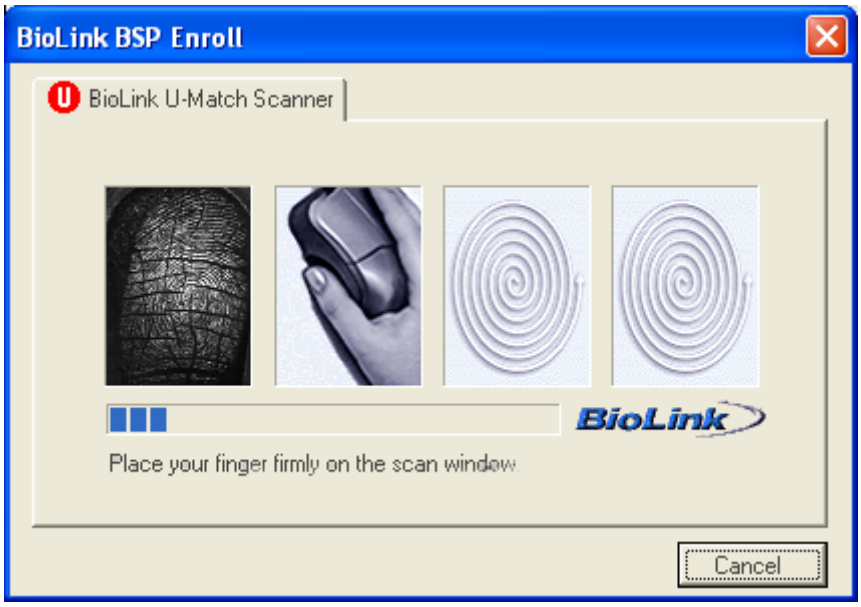

Figure 25

If the voice recognition device is used, e.g. SAFLINK Scansoft Voice Verification, the user will be required to speak the key phrase into a microphone to create his voice template (Figure 26). After the voice template is created, the information is stored on the KSD.

Figure 26

Servicing the KSD

After launching the utility, connecting the KSD, entering correct PIN code and successful biometric verification, the program window appears as indicated in Figure 17.

The user can then perform the following operations with the KSD:

- Change the PIN-code;
- Change the label of the KSD;
- Clear the KSD;
- Change the ID-file;
- Change BIO ID;
- Save the ID-file from the KSD to disk;
- Display the Lotus Notes password on the screen;
- Change the password for Lotus Notes.

Changing the PIN code

In order to change the PIN code, it is necessary to perform the following steps:

1. Launch the program.

2. Press the **Change PIN** button. The following dialog window appears (see Figure 23).

Figure 27

3. In the field *new PIN code,* enter the new PIN-code, or leave it blank (to work without a PIN code), and press **OK**.

Note: The PIN-code can be from 4 to 8 characters.

4. The program with then prompt you to confirm your PIN code, then press **OK**.

Figure 28

Upon completion of this procedure, you will see the following message:

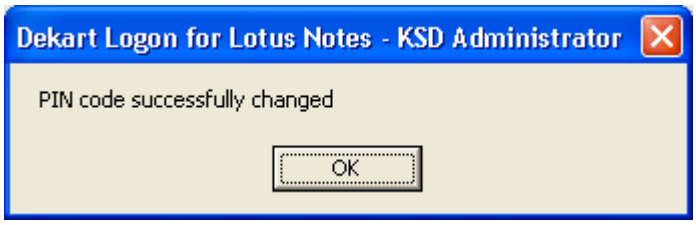

Figure 29

Changing the BIO ID

In order to change BIO ID (if it has been previously stored on the KSD) do the following:

1. Launch the program.
2. Click the **"Change BIO ID"** button in the program window. The ***Change Biometric ID*** window with the list of installed drivers of biometric devices will appear, as shown in Figure 24.

3. Select the biometric device from the list.
4. Depending on the type of the selected device enter the required biometric information (fingerprint, voice). After the succession of biometric scans, the template will be stored on the KSD.

   Note: In order to stop using biometric authentication, the user should uncheck the Enable Biometric ID verification checkbox in the Change Biometric ID windows.

Changing the label for the KSD

The KSD label contains information about the specified user/owner of the device. This information can be the name of the user, or other personal information. In order to change the label for the KSD you must:

1. Launch the program.
2. Press the button **Change Label.** The following dialog window appears (Figure 30).

Figure 30

3. In the field *new Label* you must indicate the new label for the KSD, and press **OK**. In order to clear the label, in *new Label* you should leave the field blank, and press **OK**.

Note: The length of the label for the KSD cannot be greater than 32 characters.

Clearing the KSD

Attention! Executing the "clear KSD" function will erase all data pertaining to Lotus Notes from the KSD (ID file and password)!

In order to clear the KSD, it is necessary to perform the following steps:

1. Launch the program.
2. Press **Clear KSD.** The program will ask you to confirm the process (Figure 31).

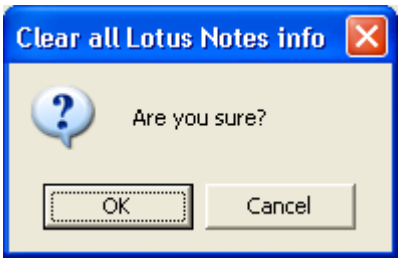

Figure 31

3. In order to proceed, press **OK**. After completion of the operation, the window will appear as shown on Figure 16.

Changing the ID file

In order to change the ID file, the user must:

1. Launch the program.
2. Press **Change ID file.** The *Change ID file - Select ID file* window appears (see Figure 20).
3. The user must indicate the file user.id (see Figure 20) and press **Open**.
4. The dialog window *Initialize Notes – Select "notes.ini"* appears (see Figure 21). It is required that you select the file notes.ini and press **Open**.
5. After you indicate that file that is to be initialized, you will be asked for the Lotus Notes Password (see Figure 22). The user must enter the password and press **OK.**

Saving the ID-file to disk

In order to save the ID file to disk, the user must perform the following steps:

1. Launch the program.
2. Press **Detach ID file.** The dialog window *Detach ID file - Select ID file* appears (see Figure 32).

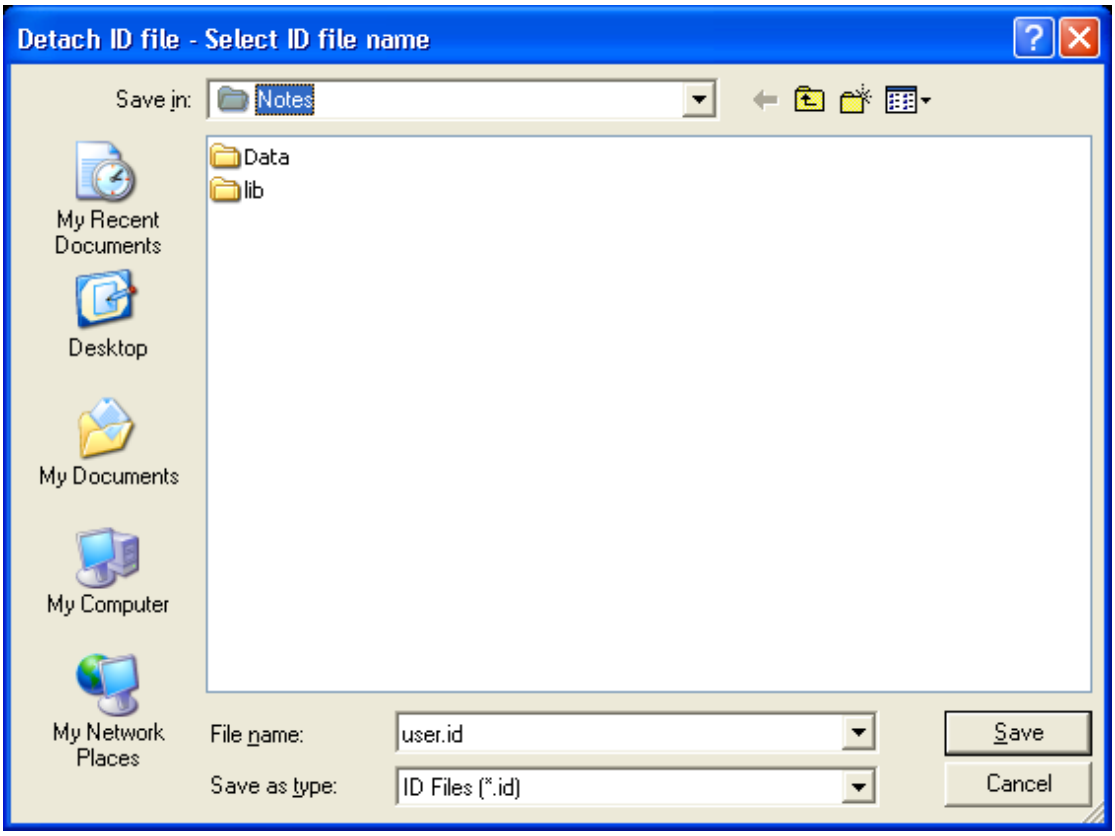

Figure 32

3. Indicate the name of the file where the ID file from the KSD is to be saved, and press **Save.**

Display Lotus Notes password

In order to display the password for Lotus Notes on the screen:

1. Launch the program.
2. Press **Notes PASSWORD -> Show.** The program displays a warning and asks you to confirm the operation.

Figure 33

3. If the user presses **OK**, then the password for Lotus Notes will be displayed on the screen.

Figure 34

Changing the password for Lotus Notes

In order to change the password for Lotus Notes:

1. Launch the program.
2. Press **Notes PASSWORD -> Change.** The below dialog appears:

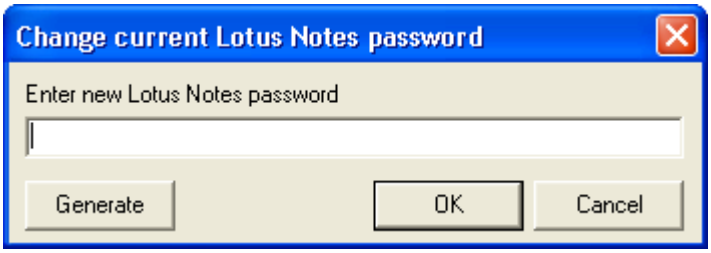

Figure 35

3. The user can utilize the function *Generate new Lotus Notes password,* and will then be able to generate a password automatically (variation 1), or manually (variation 2).

   Variation 1 In order to automatically generate a password for Lotus Notes, you must press **Generate (**Figure 35). Figure 36 displays the resulting password.

Figure 36

   Variation 2 In the field *new Lotus Notes password* enter the desired password for Lotus Notes, and press **OK.**

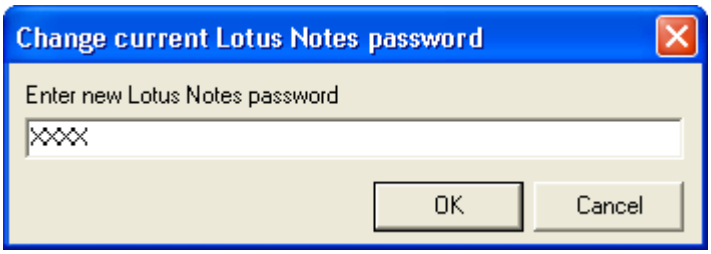

Figure 37

In response to a prompt from the program, you will be asked to confirm the password (see Figure 38).

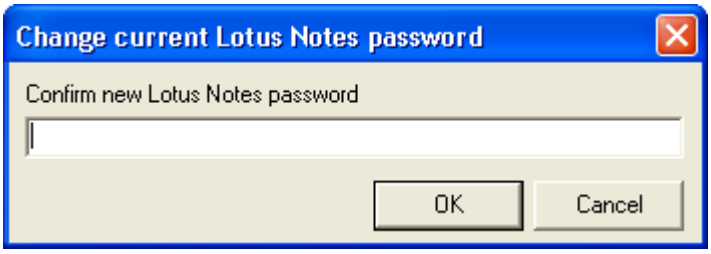

Figure 38

Note: The length of the password is determined by Lotus Notes, and cannot be longer than 64 characters.

4. A dialog will appear: *Initialize Notes – Select "notes.ini"* (see Figure 21). Select the filenotes.ini and press **Open**.

Accessing information about Dekart Logon for Lotus Notes

Press **F1** or right-click the title bar of the program window. Choose "About" from the menu bar (Figure 39).

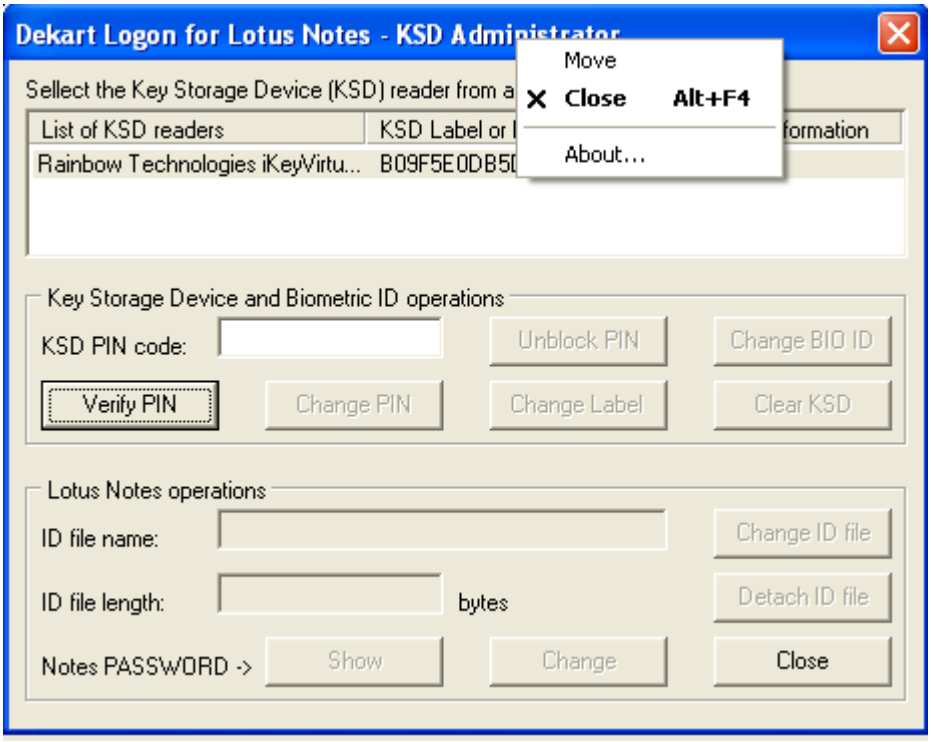

Figure 39

The *About Dekart Logon for Lotus Notes* window will appear (Figure 52). If you are using the unregistered version of the product, then the *About Dekart Logon for Lotus Notes* window shown in Figure 54 will appear.

8 Work with Dekart Logon for Lotus Notes

Working with **Dekart Logon for Lotus Notes** can be broken down into two steps. First (preparatory) consisting of preparing the KSD for use (see para.7). The second step specifically provides security for the user while working with Lotus Notes:

• Authentication of users of Lotus Notes.

• Temporarily blocking access to Lotus Notes.

Access to Lotus Notes

DLLN replaces the standard means of authenticating to Lotus Notes with its own method of strong authentication.

- Upon launching Lotus Notes, the user will see dialog window generated by DLLN.

Figure 40

- The user must enter a PIN Code, and press **OK.**

Attention! Multiple incorrect PIN code entries will result in the KSD being blocked!

- After successful verification of the PIN code the user will be required to provide his BIO ID, if the BIO ID is stored on the KSD and the **"Enable Biometric ID Verification"** checkbox has been checked.
- If desired, the user can also access Lotus Notes with their password. In order to do this, the user should select **Work without KSD**, after which the standard Lotus Notes dialog window will appear (see Figure 41 for version 5.09 and Figure 42 for version 6.0.1 and higher).

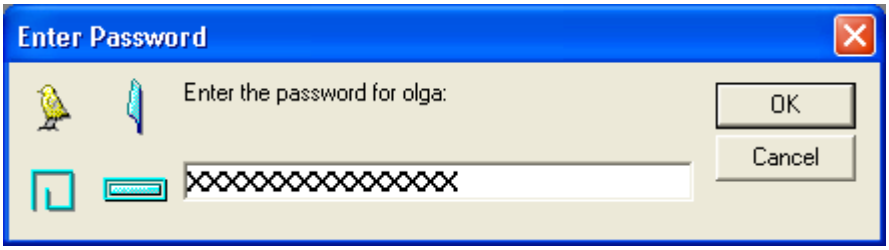

Figure 41

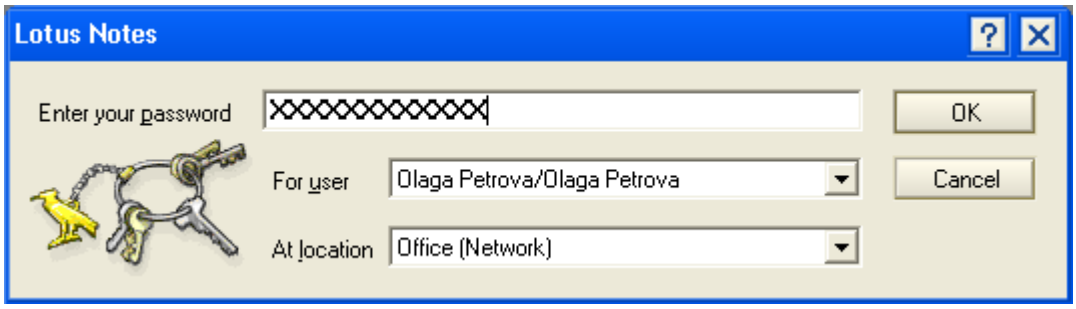

Figure 42

Temporary blocking/restricting access to Lotus Notes (Logout)

If the user has to step away from their workplace, DLLN allows them to secure their Lotus Notes databases, by removing their KSD, either from the USB port, or smart card reader. In this case, Lotus Notes v.5.09 will close (block) the open database and ID file. The below message then appears (see Figure 43).

Figure 43

Note: The characteristics necessary for securing the database «Address book» in Lotus Notes v.5.09 are provided for in the attachment.

In Lotus Notes v.6.0.1 and higher the program will also close the ID-file of the user, and Lotus Notes will enter the temporary block mode (see Figure 44).

Figure 44

Only the user who invoked Logout will be able to Logon to Lotus Notes!

Any action that requires the Lotus Notes ID-file, after removal of the KSD, will result in the following message:

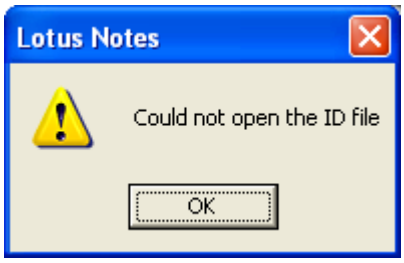

Figure 45

In order to continue working (going from Logout to Logon mode) the user will have to insert their KSD and enter their PIN-code when prompted (see Figure 40).

Note 1: If using a KSD that is not secured with a PIN-code it is possible to go from Logout to Logon mode, by simply inserting the KSD in the appropriate port/reader.

Note 2: In order to continue working with Lotus Notes v.5.09, any user other than the holder of the KSD will have to enter a new ID-file (selecting Switch ID… in the Menu File > Tools).

Operations of Dekart Logon for Lotus Notes

In the menu **Actions,** the user must select **Dekart Logon for LN Tools>.** The screen displays a popup menu with a list of allowable actions **(**Figure 46**).**

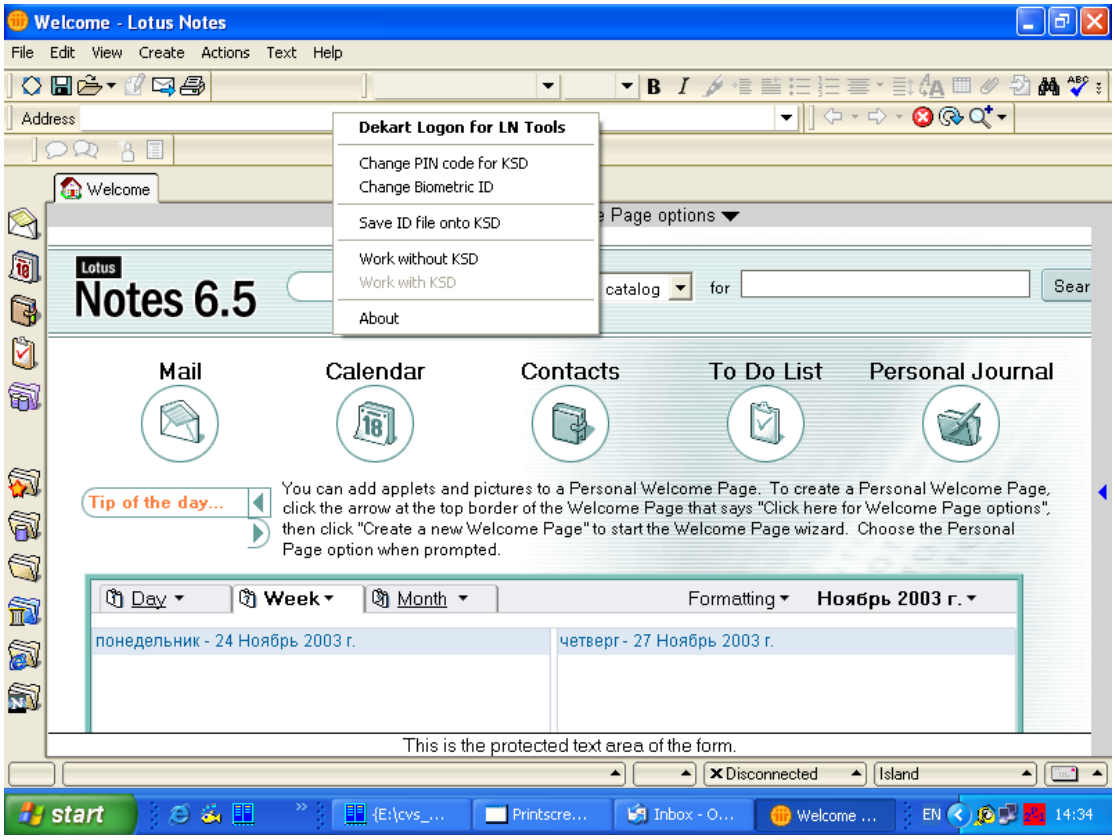

Figure 46

- Changing the PIN Code;

- Changing the BIO ID;
- Storing the ID-file on the KSD;
- Working with the KSD;
- Working without the KSD;
- Receiving information about the product.

Changing the PIN-code

Changing the PIN-code takes place from the menu **Actions > Dekart Logon for LN Tools>** select **Change PIN code for KSD.** Further actions follow the procedures outlined in para**.7**:

1. The dialog that appears in the window (Figure 27) in the field *new PIN code* requires that a new PIN-code be entered, or leave the field empty (in order to work without a PIN-cod), and press **OK**.
2. When prompted by the program (Figure 28) the user must confirm the new PIN-Code, and press **OK**. After successful completion of the operation, the following message appears (Figure 47).

Figure 47

Changing the BIO ID

Changing the BIO ID takes place from the menu **Actions > Dekart Logon for LN Tools>** select **Change Biometric ID.** Further actions follow the procedures outlined in para**.7**.

Changing work modes

Changing work mode “Working with the KSD” to ”Working without the KSD”

If while working with Lotus Notes (“Working with KSD” mode) the user wishes to interrupt their session without closing Lotus Notes, or wishes to work directly with ID-files that are stored on the hard drive, user must do the following:

- In the menu **Actions > Dekart Logon for LN Tools>** select **Work without KSD**. The on-screen message will display the following prompt:

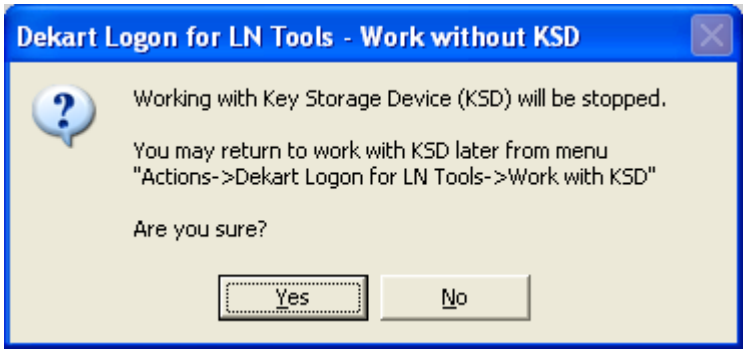

Figure 48

- When you press **Yes** you will see the following message (see Figure 49 for Lotus Notes v.5.09, and Figure 50 for Lotus Notes v.6.0.1).

Figure 49

Figure 50

In order to continue working with Lotus Notes, the user must indicate a new ID file in Lotus Notes v.5.09, it is necessary to select **Switch ID…** in menu **File > Tools**, however, in Lotus Notes v.6.0.1 – select **Switch ID…** in menu File **> Security** (this operation is performed automatically, if in window (Figure 50) the user presses **OK).**

Changing the work mode from "work without KSD" to "work with KSD"

If during Lotus Notes work session ("work without KSD" mode) the user wishes to begin working with the ID-file stored on the KSD, they must do the following:

- In the menu **Actions > Dekart Logon for LN Tools>** select **Work with KSD**. There will appear a prompt to enter the PIN code (see Figure 40).
- The user must enter their PIN code and press **OK.**

Attention! Multiple incorrect PIN-code entries will result in the blocking of your KSD. Great care must be taken to avoid this from happening!

Storing your ID-file on the KSD

In the event that while working with Lotus Notes, the ID file has been changed, it is necessary to save the new ID file on the KSD. In order to do this, go to the menu **Actions > Dekart Logon for LN Tools>,** select **Save ID file onto KSD.** The program will prompt you to confirm the operation.

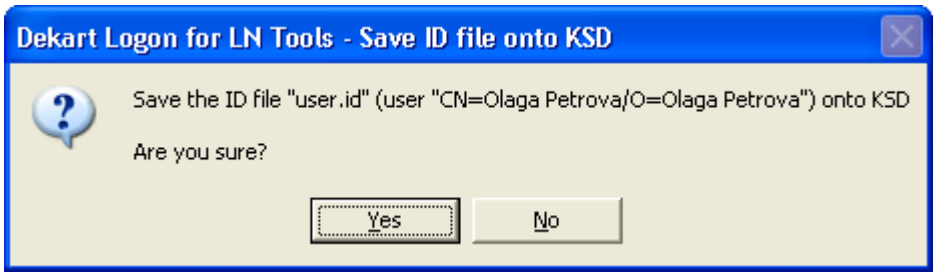

Figure 51

The user must press **Yes,** in order for the operation to be completed.

Viewing information about Dekart Logon for Lotus Notes

In order to view information about DLLN, go the menu **Actions > Dekart Logon for LN Tools>** select **About.** The following screen will appear**:** *About Dekart Logon for Lotus Notes.*

Note. If you are using the unregistered version of the product then the About Dekart Logon for Lotus Notes window shown in Figure 50 will appear.

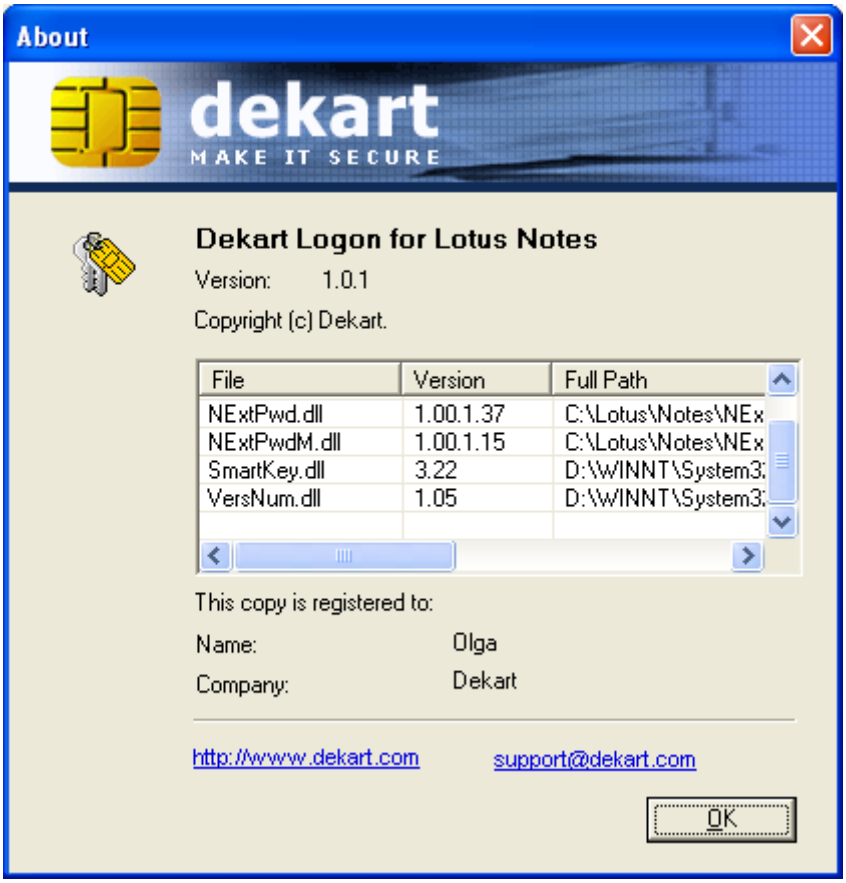

Figure 52

9 Biometric authentication in Dekart Logon for Lotus Notes

If the three-factor authentication is enabled (the **Enable Biometric ID verification** checkbox checked in the **Change Biometric ID** window), the biometric authentication will be required after the user starts **KSD Administrator,** launches **Lotus Notes,** and the PIN for the **KSD** is successfully verified (if the user has set the PIN protection for the KSD)**.** The software will automatically read the biometric templates stored on the KSD and will offer the user to provide his biometric data (scan the fingerprints, speak the authentication phrase etc.). In case the BIO ID provided by the user is not identical with the templates stored on the KSD, the user will be required to repeat the biometric authentication. Authentication routine will be finished only when the data provided by the user will be identical to the biometric templates stored on the KSD. The biometric approach ensures that only authorised user can get access to Lotus Notes.

10 Registering Dekart Logon for Lotus Notes

If you didn't register the product during installation, please register it by filling out the form in *About Dekart Logon for Lotus Notes window*.

Figure 53

Please, obtain a registration number at *Software Registration (Register)* page at **www.dekart.com.** In case you use licensed Dekart software, please, submit your license key to receive your registration number via email. If you use shareware programs, please, use Dekart *Buy on-line* page to purchase your registration number. After your transaction is processed, you will receive an email with the registration number.

Attachment

Device characteristics of KSD (PIN-codes, memory size)

Table 1

KSD name	PIN-code for applications/ device	Allowed wrong PIN code entries	Allowed attempts to unblock KSD	Memory size (kB)
Aladdin eToken PRO	PIN-code for applications	3	3	16, 32, 64
Aladdin eToken R2	PIN-code for device	∞	-	16, 32, 64
Schlumberger Multiflex	PIN-code for applications	3	3	4, 8
Schlumberger Cryptoflex	PIN-code for applications	3	3	8, 16
Schlumberger Payflex	PIN-code for applications	3	3	4
Rainbow iKey 1000	PIN-code for device	3	3	8, 32
Rainbow iKey 2000	PIN-code for device	10	0	8, 32
Rainbow iKey 2032	PIN-code for device	10	0	8, 32
Rainbow iKey 3000	PIN-code for applications	3	3	32
Eutron CryptoIdentity ITSEC	PIN-code for applications	3	3	32
Eutron CryptoIdentity 4	PIN-code for applications	3	3	8
Eutron CryptoIdentity 5	PIN-code for applications	3	3	32, 64
Datakey Model 310	PIN-code for device	10	0	8, 32
Datakey Model 330	PIN-code for device	10	0	8, 32
GemPlus GPK	PIN-code for applications	3	3	2, 4, 8, 16
ruToken	PIN-code for device	3	12	8, 16, 128

Note 1. Key storage device can have one PIN-code for all Dekart applications, and another PIN code for other applications, or a single PIN code for the device

Note 2. Most KSD's allowable incorrect PIN code entries are limited. Upon reaching the maximum allowable incorrect entries, the KSD is blocked. If during the unblocking you enter the correct PIN code, the KSD will function properly once again. IF DURING THE UN-BLOCKING OPERATION THE WRONG PIN CODE IS ENTERED, THE KSD WILL BE PERMANENTLY BLOCKED!

Special Aspects of securing the Lotus Notes v.5.09 database «Address book»

In Lotus Notes v.5.09 (without Dekart Logon for Lotus Notes) there exist problems in encrypting the Notes database (Address book). After enabling the encryption mode, launching Lotus Notes results in an error (see Figure 54 and Figure 55).

Figure 54

Figure 55

In order to avoid this from happening, you should enable encryption for the Notes database (address book) after installing Dekart Logon for Lotus Notes, and in the future use this feature only when DLLN is in the «Work with KSD» mode.

Error messages

Error Message	Possible reason	Remedy
Key Storage Device not found or not formatted for Lotus Notes Logon	KSD is not connected to the computer, or the device (smart card or USB key) is not formatted for DLLN.	• Connect the KSD to the computer. • If the KSD is connected, make certain that the contact with the USB port or smart card reader is good; remove and re-connect. • Format the KSD for DLLN.
ATTENTION! Bad	Wrong PIN code was entered.	It is necessary to repeat the

PIN code was entered!		operation, and enter the correct PIN code. **Attention! Multiple incorrect PIN code entries will result in blocking of the KSD!** **The number of allowable entries for the specific KSD is specified in Table 1.**
Key Storage Device is blocked	KSD is blocked.	In order to un-block the KSD it is necessary to contact the administrator. **Attention! If the incorrect PIN code is entered, the KSD will be permanently blocked!**
Key Storage Device is not formatted for Lotus Notes Logon	The KSD is not formatted for use with DLLN.	It is necessary to format the KSD, for use with DLLN.
Confirmed PIN does not match	During the Change PIN code procedure the PIN codes did not match.	It is necessary to repeat the operation, and ensure that both PIN code entries match.
PIN length must be at least 4 characters	Length of the PIN code must be at least four (4) characters long.	It is necessary to repeat the operation and enter a PIN code of at least four (4) characters long.
Invalid password was entered	Invalid password was entered.	It is necessary to repeat the operation and enter the correct password.
Password field can't be empty	Policy requires that a valid password must be entered.	It is necessary to repeat the operation and enter a **Password.**
Error: “Password do not match”	During the Change password procedure, the passwords do not match.	It is necessary to repeat the procedure and ensure that both password entries are identical.
Error: "Specified password is already in use”	During the Change password procedure, the password entered matches one that is already in use.	The user must enter a new password.
File: ... already exists. Overwrite it?	The file name already exists, and the user is prompted to overwrite the existing file.	In order to prevent loss of data, the user should indicate another file name.
The password and the confirmation data are	During the Change password procedure, the entered data	It is necessary to repeat the procedure and ensure that

not the same	does not match.	the same password has been entered in both fields.
Error writing data into KSD (Not enough free space on KSD)	An error occurred while writing to KSD. There might be not enough space on the KSD memory.	Please, use Dekart Key Manager to delete (or move to the local disk) the data from the KSD in order to write DLLN data.
Biometric verification failed!	The BIO ID provided by the user is not identical with the one stored on the KSD.	Repeat biometric verification procedure.

Note: In the event that an error occurs that is not identified in the above list, you should contact your administrator.

Window for KSD operations

During any operation pertaining to KSD operation, you will see the following window and message:

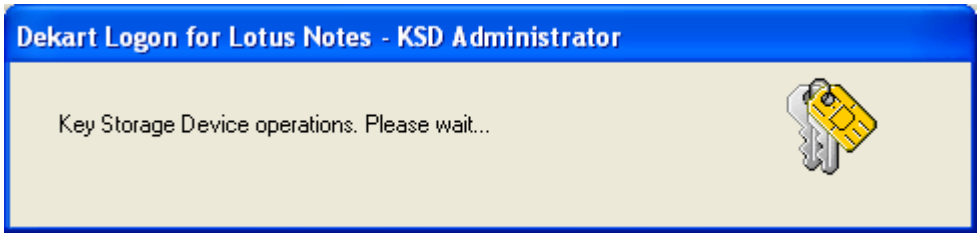

Figure 56

When the biometric information is read or written from the KSD, the following message appears.

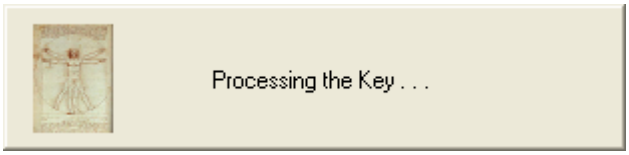

Figure 57