



**dekart**  
MAKE IT SECURE

## **OPERATING GUIDE**

### **DEKART LOGON V. 2.20**

© 2004 Dekart

## 1 License and trademarks information

### **COPYRIGHT**

Copyright © Dekart SRL. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Dekart SRL, or its suppliers or affiliate companies.

### **DISCLAIMER**

Dekart SRL makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Dekart SRL reserved the right to revise this publication and to make changes to its content, at any time, without any obligation to notify any person or entity of such revisions or changes.

Further, Dekart SRL makes no representations or warranties with respect to any Dekart Logon software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Dekart SRL reserved the right to make changes to any and all parts of Dekart Logon software, at any time, without any obligation to notify any person or entity of such revisions or changes.

### **LICENSE AGREEMENT**

NOTICE TO ALL USERS: FOR THE SPECIFIC TERMS OF YOUR LICENSE TO USE THE SOFTWARE THAT THIS DOCUMENT DESCRIBES, CONSULT THE README.1ST, LICENSE.TXT, OR OTHER LICENSE DOCUMENT THAT ACCOMPANIES YOUR SOFTWARE, EITHER AS A TEXT FILE OR AS PART OF THE SOFTWARE PACKAGING. IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH THEREIN, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

### **DEKART SRL TRADEMARK ATTRIBUTIONS**

**Dekart Logon** is a trademark of Dekart SRL

All other registered and unregistered trademarks in this document are the sole property of their respective owners.

### **DEKART SRL CONTACT INFORMATION**

**E-mail:** for sales details: [sales@dekart.com](mailto:sales@dekart.com)  
for product support: [support@dekart.com](mailto:support@dekart.com)  
for comments and feedback: [info@dekart.com](mailto:info@dekart.com)  
**WWW:** [www.dekart.com](http://www.dekart.com)

## 2 Preface

**Dekart Logon** is a combined hardware-software solution intended for securing access the computer. The solution includes both the software program and the hardware device – [Key Storage Device \(KSD\)](#). A wide range of devices can act as a KSD, namely, smart cards, USB tokens, USB flash drives and many other devices, which memory can be used for storing

user credentials. The Key Storage Device is assigned to each user and presents its unique identifier for accessing the operating system on the computer protected by **Dekart Logon**.

### **The purpose of this guide**

This Operating Guide is intended for users of **Dekart Logon**. The Guide contains detailed description on how to install, administer and use **Dekart Logon**.

### **Documentation conventions**

New terms, key concepts, and guides' titles are *italicized* in this Guide.

The *greater than* (>) symbol is used to separate operations within one action.

Interface elements are ***bold-faced and italicized***.

### **Comments and feedback**

Please, send your comments, suggestions, remarks and other feedback with respect to Dekart Logon software and hardware issues and this operating guide to [support@dekart.com](mailto:support@dekart.com).

## **3 Introducing Dekart Logon**

This chapter contains the information about the purpose and features of **Dekart® Logon™** and defines the basic concepts of enhanced user authentication, provided by the software:

- o Identification.
- o Authentication.
- o Two-factor and three-factor authentication.

### **3.1 Dekart Logon purpose and futures**

**Dekart Logon** allows to:

- Identify an authorized user, granting strictly defined access to the resources.
- Identify the third-party user and prohibit access to the resources.

Such recognition is carried out by means of certain procedures: the users must let the system know who they are, i.e. *identify* themselves to the system, and next, they must *authenticate* into the system.

*Identification* is a control process that examines a unique user ID and determines whether this user is known to the system.

*Authentication* is a control process that checks the authenticity of the user identity, i.e. this process controls whether the user is the person they say they are. Usually, identification consists in entering a user name, and authentication is based on the user's knowledge of a secret password that must be entered from the personal computer keyboard.

Unfortunately, the standard authentication means of even the most protected Windows family of operating systems (Windows NT Workstation, Windows 2000/XP Professional) is based on the knowledge of two fixed values — the user name and password — and cannot guarantee reliable security if a third party learns these values.

Therefore, there is the need to replace the standard *one-factor* authentication with the so-called strong authentication. The *strong authentication* is based on, at least, two of the following three factors:

1. *Something you know*: for example, a user name and ID code.

2. *Something you have*: for example, a device such as a smart card or USB token that enables a system to verify whether it is present or not.
3. *Something you are*: for example, fingerprints, iris, voice, and other specific traits of your body. Conformity to these traits can be verified by the system during authentication.

If two factors are used to authenticate the user to the system, then this authentication is called *two-factor authentication*, if all three factors – *three-factor authentication*. **Dekart Logon** provides either two or three factor authentication for users of Windows OS family – for successful authentication the user requires a Key Storage Device, a PIN to this device, and, if biometric authentication is enabled, a successful biometric authentication. This type of authentication plays a major role in limiting access of the third-party users to the computer.

**Dekart Logon** also accomplishes another very important task — it allows to protect the computers left unattended by their respective users. Once successfully authenticated, the users often forget to lock their computers when they temporarily leave them, thus compromising valuable information. Once the user disconnects the Key Storage Device from the computer, **Dekart Logon** will automatically lock the computer.

The primary PIN code of the KSD should be changed after you install Dekart Logon and define the user who will own the KSD. These are the requirements to the PIN code:

- It must contain 1 to 8 alphanumeric symbols and be case-sensitive.
- It must be fairly strong and complicated (to make spying and guessing more difficult).
- It must be easy to remember. If you forget the PIN-code, you will not be able to access your computer and its resources.

## 3.2 Supported key storage and biometric devices

**Dekart Logon** supports the following devices:

### **Key Storage Devices:**

- ACOS1 card;
- ActivCard ActivKey USB token series;
- Aladdin eToken R2 USB token series;
- Aladdin eToken PRO USB token series;
- Algorithmic Research MiniKey USB token series;
- Algorithmic Research PrivateCard smart card series;
- Datakey Model 310 smart card series;
- Datakey Model 330 smart card series;
- Eutron CryptoIdentity ITSEC USB token series;
- Eutron CryptoIdentity 4 USB token series;
- Eutron CryptoIdentity 5 USB token series;
- GemPlus GPK smart card series;
- GemPlus MPCOS EMV smart card series;
- Giesecke & Devrient STARCOS S smart card series;
- Giesecke & Devrient STARCOS SPK smart card series;
- Rainbow iKey 1000 USB token series;
- Rainbow iKey 2000 USB token series;

- Rainbow iKey 3000 USB token series;
- Schlumberger Cryptoflex smart card series;
- Schlumberger Multiflex smart card series;
- Schlumberger Payflex smart card series;
- Siemens CardOS M 4 smart card series
- ruToken USB token series;
- USB flash drives, CD disks, etc.

**Smart card readers:**

Dekart Logon uses virtually all PC/CS compatible smart card readers, for example:

- Datakey DKR smart card reader series
- GemPlus GemPC smart card reader series
- OmniKey CardMan smart card reader series
- Schlumberger Reflex smart card reader series
- Towitoko CHIPDRIVE smart card reader series

**Biometric verification devices:**

Dekart Software uses most types of BioAPI and HA API compatible biometric verification devices, for example:

- Precise Biometrics Precise 100 fingerprint and smart card reader series
- SCM SCR222 fingerprint reader
- BioLink U-Match MatchBook
- BioLink U-Match Mouse

**Note 1.** Before you purchase a USB token or smart card, please make sure that it has enough memory to store the required user data. Please, 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.

**Note 2.** To store Dekart Logon data on the smart card or token you will need to format it using a Key Formatting utility or Corporate Key formatting utility. Registered customers can download the Key Formatting utility by providing the registration number for **Dekart Logon** at <https://www.dekart.com/download/> (please, use Internet Explorer browser to access the restricted download area). The use of USB flash drive enables users to use the strong authentication provided by **Dekart Logon** without the need to use any type of card formatting.

### 3.3 Dekart Logon products components

One **Dekart Logon** package contains the following components:

- A CD with the software installation module;
- One of the abovementioned Key Storage Devices (depending on the package type).
- *Operating Guide*.

The following optional components can also be delivered with **Dekart Logon** package (depending on the package type):

- Microsoft software for smart cards support.
- An **RTE** containing utilities and drivers for **eToken** KSD support.

Smart card reader drivers.

## 4 Dekart Logon hardware and software requirements

### Personal computer hardware requirements

**Dekart Logon** does not have any additional requirements to the hardware of the PC. These requirements are mainly defined by the operating system used on the given computer.

The following minimal hardware characteristics are required for the normal operation of

**Dekart Logon** (applies to Windows 95 OSR2.1):

- Intel Pentium 166 MHz processor.
- 16 MB RAM.
- 200 KB HDD.

In addition to this, the PC must be equipped with the following ports to connect hardware keys:

- A USB port, if the USB token or a smart card reader for the USB port is used
- A COM port, if a smart card reader for the COM port is used
- A PS/2 interface, if a smart card reader with the PS/2 interface is used

### Personal computer software requirements

Operating Systems:

- Windows 95 OSR2.1.
- Windows 98 SE.
- Windows Me.
- Windows NT 4 Workstation, Server with Service Pack 6a.
- Windows 2000 Professional, Advanced Server with Service Pack 3 or later.
- Windows XP Professional, Home Edition.

If you have separately purchased the KSD, i.e. not as the part of **Dekart Logon** package, then you will need to install the drivers and utilities required to work with this KSD on the specific operating system. To obtain the information and latest updates of the KSD drivers, please refer to the KSD vendor website and KSD dealer.

## 5 Installing, updating and un-installing Dekart Logon

**Note:** In order to install the PC product components under Windows operating systems designed for corporate use — Windows NT, Windows 2000, and Windows XP— it is necessary to logon to these computers as an administrator. In Windows operating systems designed mainly for private use — Windows 95/98, Windows XP Home Edition, every user has the required rights.

### 5.1 Installing Dekart Logon

Before installation you should take into account that you will need to know the user password and login to log into operating system.

**Note.** If you are installing the software on the computer under Windows 95/98 or Windows

Me, you will need the operating system setup disk during the installation procedure.

To install the software, do the following:

1. Close all running applications.
2. Connect the Key Storage Device to the computer and install the drivers (if this has not been previously done). To obtain the latest driver versions, please refer to the device vendors.
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 the BioAPI Framework should be installed on the computer before installing device drivers (the BioAPI Framework can be downloaded from [www.bioapi.org](http://www.bioapi.org), Implementation section).*
4. To install **Dekart logon**, run the setup program Logon.exe.
5. Select **Install Dekart Logon**
6. A welcome screen of the installation will appear, as shown in Figure 1.

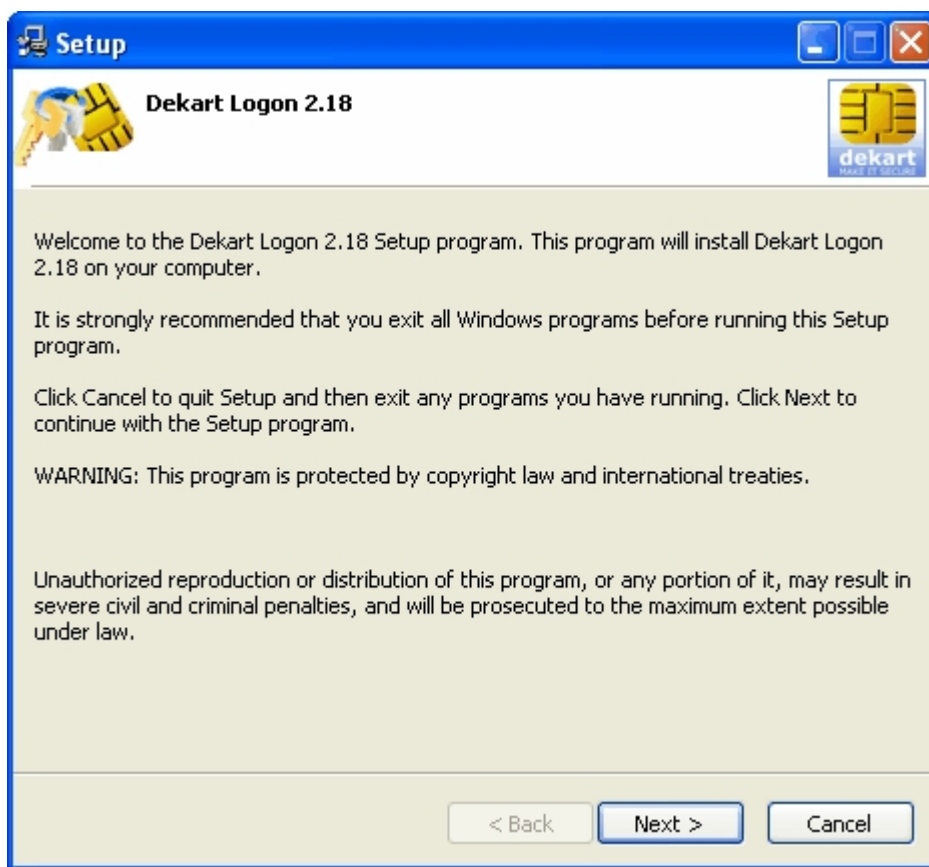


Figure 1

7. Click *Next*. The license agreement will appear, as shown in Figure 2.

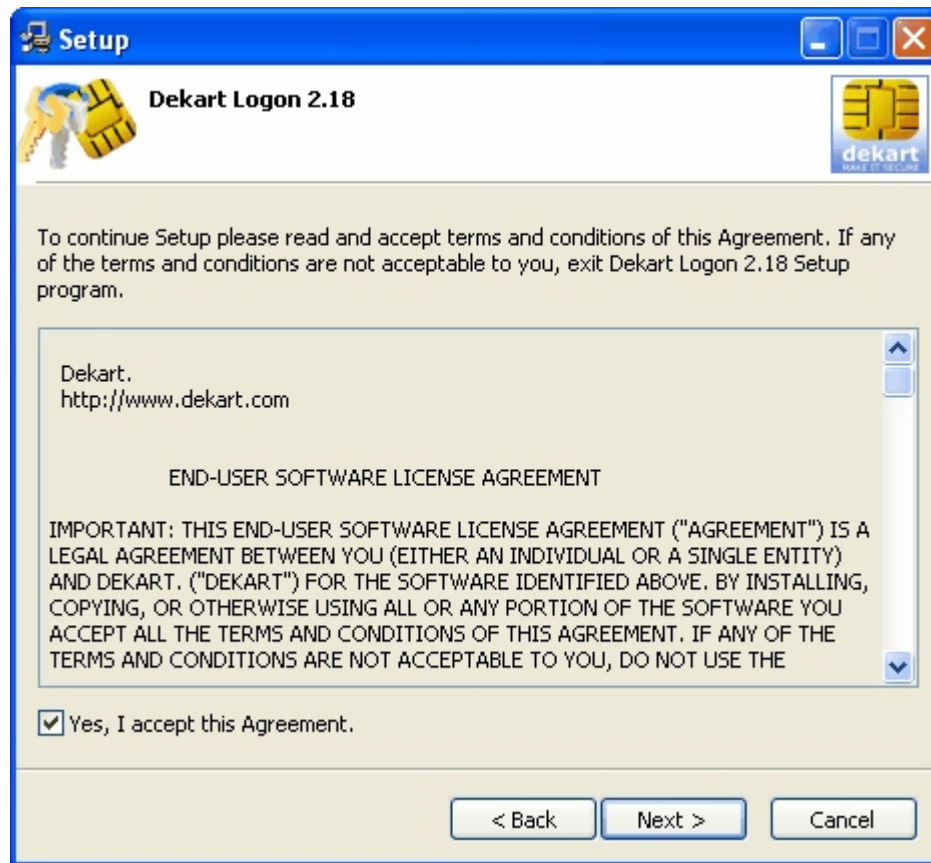


Figure 2

8. If you agree with the license agreement conditions, select the *Yes, I accept this agreement* checkbox, as shown in Figure 2 and click *Next*. (If you do not agree, please, cancel the installation).

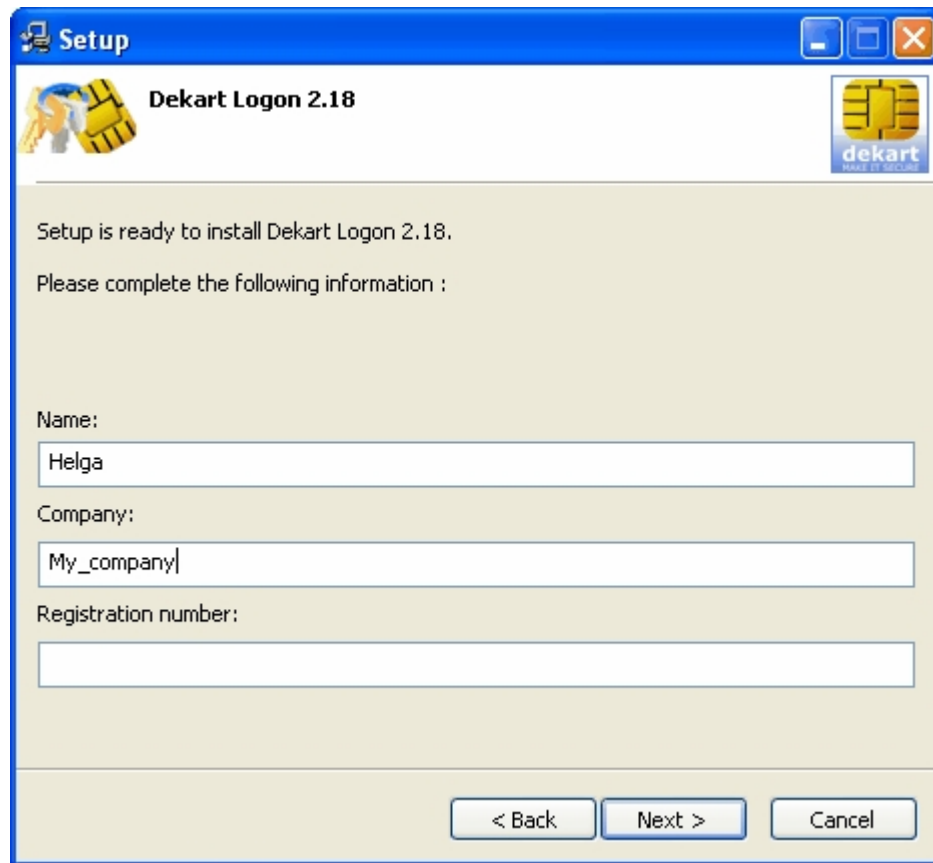


Figure 3

- 9 Please, enter your personal information and click *Next*. The dialog window asking for the **Start Menu** destination folder will appear.

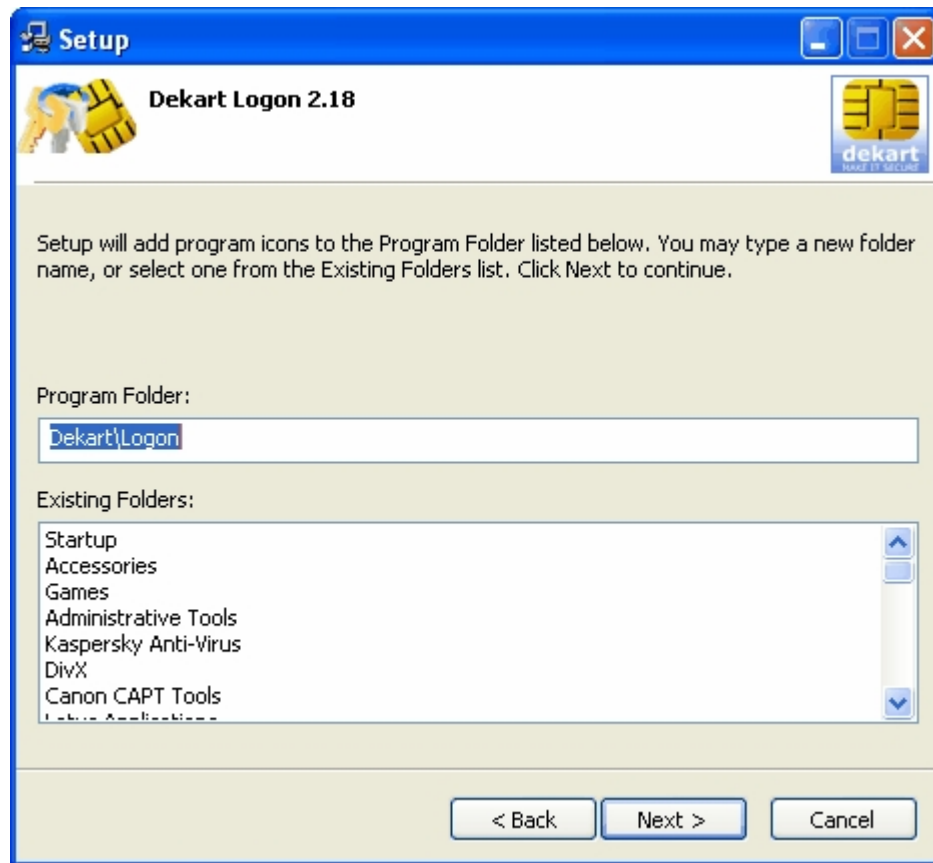


Figure 4

10. Indicate the folder name and click *Next*.

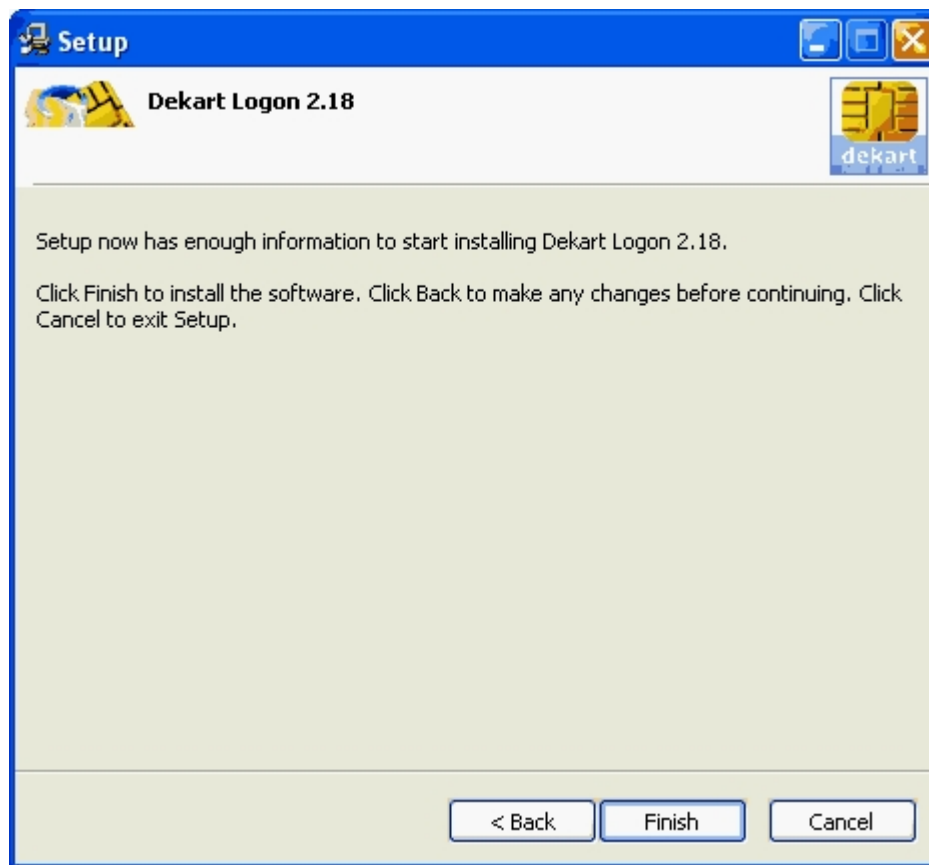


Figure 5

11. After you click **Finish**, all files necessary for software operation will be copied into the system directory.
12. If the installer request the installation of additional components, locate the folder containing the copy of your operating system installation CD in the corresponding request window or insert the installation Windows CD into the CD-ROM drive. Follow the software instructions.

To make Dekart logon work in automatic mode, please, activate it: After you have successfully installed Dekart Logon, the Dekart Logon Admin will start in the [activation](#) mode. All further steps are described in section [Activating Dekart Logon](#). You can close the window and return to this procedure later.

All system changes enabled by the installation will take effect after computer reboot. Please, reboot your computer.

## 5.2 Re-installing Dekart Logon

The user can re-install Dekart Logon. For example, this can be necessary in the following cases:

- The operating system has been re-installed.
- The product functionality has been damaged for some reason (deletion of several modules, etc.)

To re-install the product, start the Logon.exe file. Further actions are similar to those described in the [Product Installation section](#) of this chapter.

## 5.3 Updating Dekart Logon

To update **Dekart Logon** please obtain the latest version from [Dekart](#). The software allows for automatic notification about the software updates. To start an update, click the "To download the new version click here" message. The Dekart download page with all latest versions will appear. Select Dekart Logon, the language and download the latest version.

Once you have obtained the latest version of the software, run Logon.exe and follow the instructions. The program will locate the current version of **Dekart Logon** and will suggest performing update. Further actions are similar to those described in the [Product Installation section](#) of this chapter.

## 5.4 Deleting Dekart Logon

In order to uninstall the software, please do the following:

1. Go to **Start Menu**, select **Programs**, locate the folder you have entered in step 10 when [installing](#) the program, and click **Uninstall** (alternatively, you can go to **Control Panel**, select **Add or Remove Programs**, select the program name in the list and press the **Uninstall** button).
2. Click Yes to confirm your intention to uninstall the software.

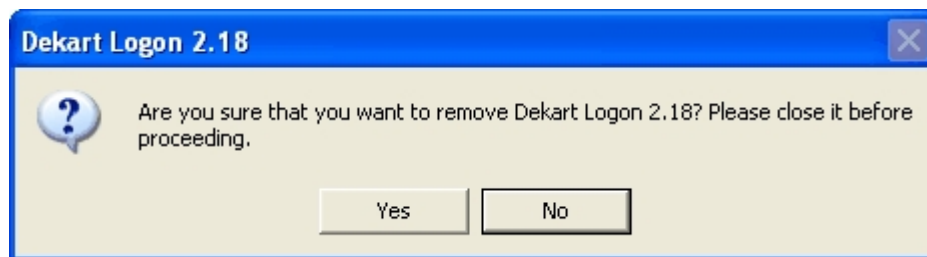


Figure 6

3. Restart your computer.

During the software removal all previously installed copies of the **Dekart Logon** will be deleted. All users currently registered in the system will remain valid and will be able to log into the system without **Dekart Logon**. However, remember that the first logon after uninstalling the product requires the user password.

## 6 Working with Dekart Logon

After you successfully install **Dekart® Logon™**, you need to make your computer ready for using enhanced authentication system. First of all, you will need to change the passwords for Windows users, making them more complicated, less predictable and vulnerable, then copy user account data to their Key Storage Devices, which significantly enhances the users' security and protection. You will then be able to change user account information and **Dekart Logon** settings depending on security policy implemented by your company or organization. Operating the software includes two major tasks:

- **Management:**

- [Adding the new user account to the KSD.](#)

- [Deleting the user account from the KSD.](#)

- [Adding or changing user biometric identifier on the KSD.](#)

- [Changing KSD label.](#)

- [Changing the PIN-code of the Key Storage Device.](#)

- [Changing user password.](#)

- [Configuring Dekart Logon behavior on KSD removal event.](#)

- **Enhanced user authentication:**

- [Two- or three-factor authentication.](#)

- [Operating system locking.](#)

### 6.1 Running Dekart Logon Admin

All configuration routines are performed using **Dekart Logon Admin**. To start **Dekart Logon Admin**, do the following:

1. Go to **Start** menu, select **Settings -> Control Panel**. The dialog window will appear as shown in Figure 7.



Figure 7

2. To start administration utility, double click the **Dekart Logon Admin** icon.
3. Or go to **Start Menu**, select **Programs**, go to the folder containing the program, select **Logon Administrator**.

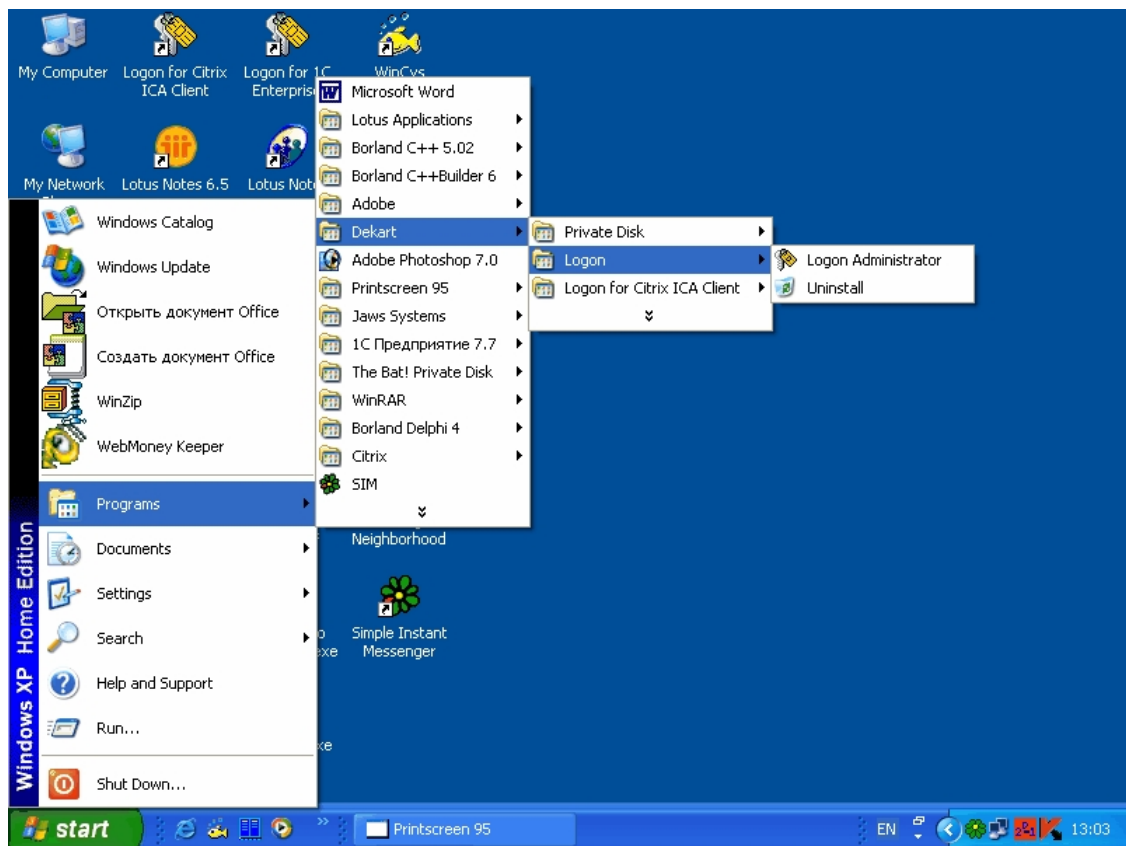


Figure 8

The *Dekart Logon Admin* window will appear.

4. Connect the Key Storage Device to the computer.

## 6.2 Activating Dekart Logon

If you haven't activated Dekart Logon immediately after installing it, then you will have to do it when running *Dekart Logon Admin* for the first time. The program window (provided the KSDs are connected to the computer) will be the following

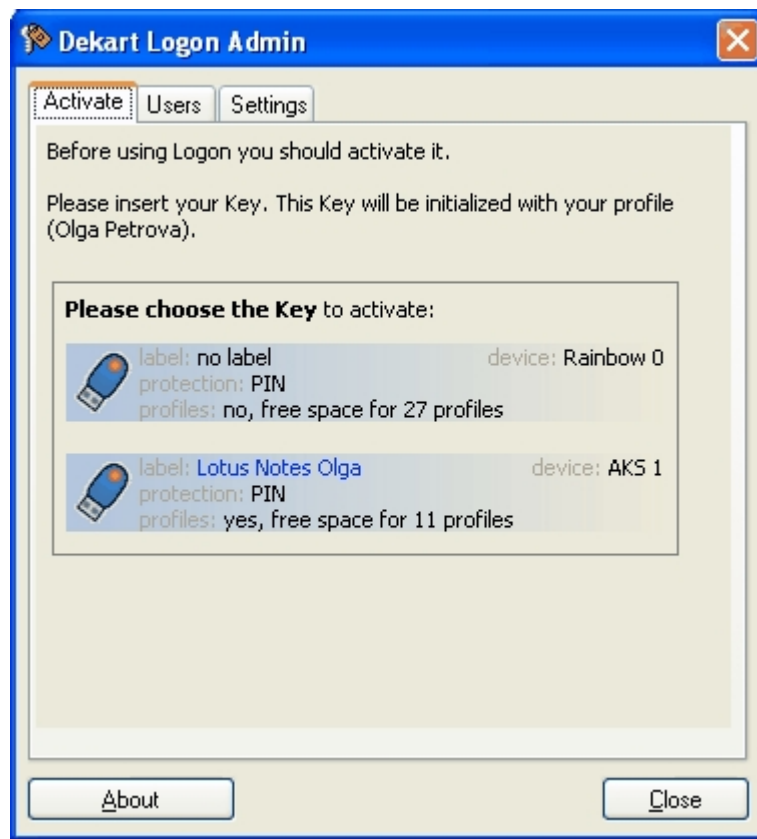


Figure 9

Please, do the following: click to select the KSD to be used for user authentication. The user account data will then be written to the KSD, which will be further used for accessing the operating system.

In case the Key Storage Device is PIN code protected, the administration utility will ask you to enter the PIN code (Figure 10).



Figure 10

***ATTENTION! KSD will block upon multiple wrong PIN code entries. Please, be careful.***

**Note 1.** Dekart delivers KSD without the predefined PIN code; no PIN verification will occur. **Note 2.** In case the BIO ID is stored on the KSD, the software will automatically detect it and attempt to conduct biometric authentication.

After successful authentication, the software will prompt you to enter the password used to access Windows, which will be further stored on the KSD. Please, enter the password in the required field and click the **Activate** button.

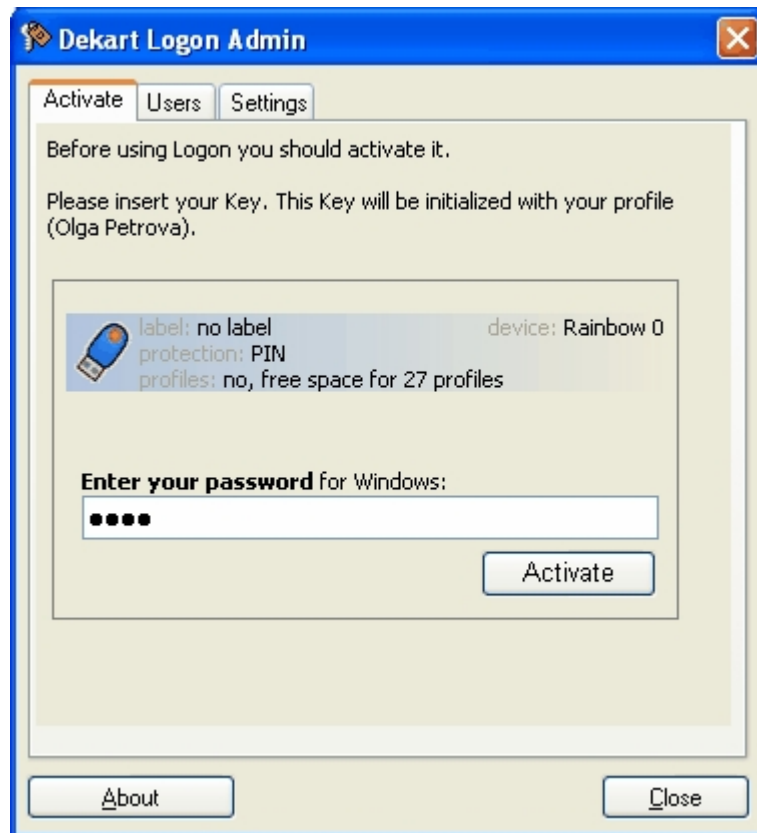


Figure 11

After successful activation you will see the following message (Figure 12).

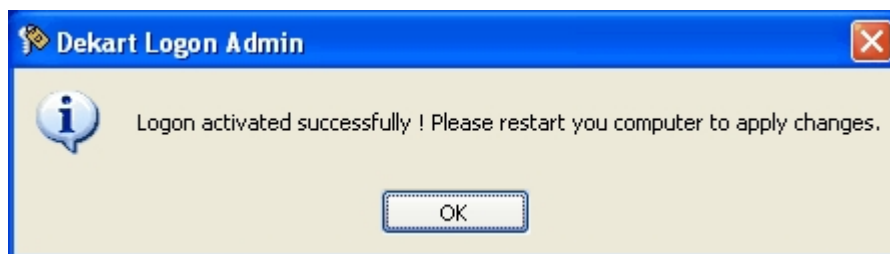


Figure 12

Click **OK** and restart your computer to make **Dekart Logon** function in automatic mode.

## 6.3 Administering Dekart Logon

**Dekart Logon** enhances the standard security of personal computer under Windows operating system. The software administration routines consist in managing user accounts and system security options.

Using administrative functions you can add and delete user accounts, change parameters of the KSD etc.

## 6.4 Administering Dekart Logon - preliminary steps

Run **Dekart Logon Admin** utility. After you connect the Key Storage Device to the computer the following changes will apply to the main window (see Figure 13).

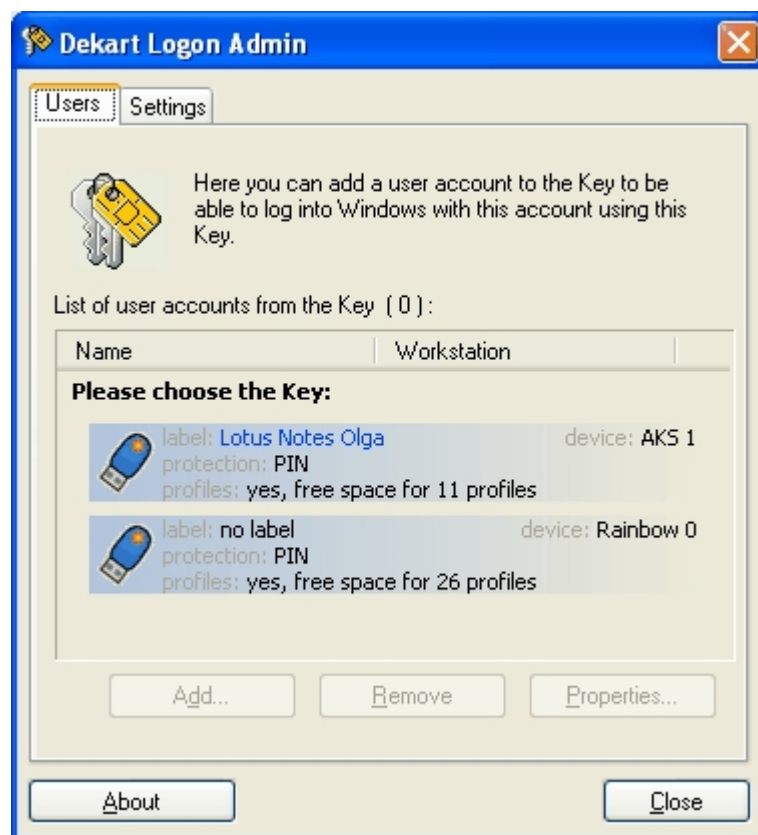


Figure 13

Click to select the device currently in use and conduct the two- or three-factor authentication if required (the software will prompt you to enter the PIN code to the device and provide the biometric identifier). The **Users** tab will automatically display (Figure 14).

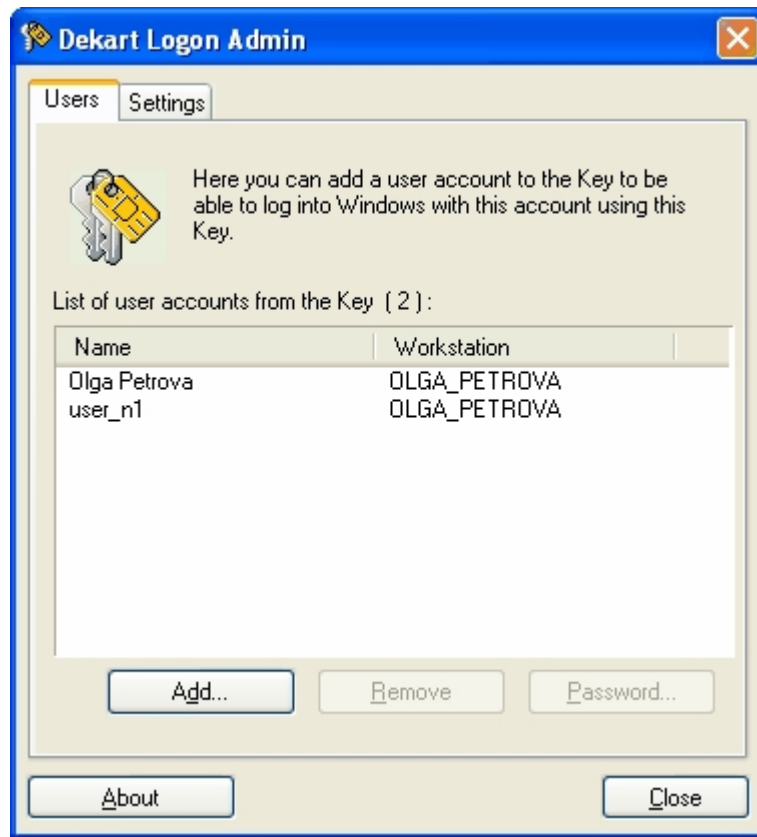


Figure 14

The *Users* tab of the administration window contains the list of user accounts stored on the KSD, thus offering the following options:

- **Add** — add user accounts.
- **Remove** — delete user accounts.
- **Password** — change system password.

**Note.** When you activate the utility, the user account is automatically stored on the KSD.

The *Settings* tab (Figure 15) of the administration window allows to do the following with the KSD (*Key settings*):

- **Change PIN** – change the PIN-code of the Key Storage Device.
- **Change BIO ID** – add and/or change user's biometric identifier.
- **Change label** – change label of the Key Storage Device.

You can also define the behavior of **Dekart Logon** upon Key Storage Device removal event (*Key removal behavior*) and enable specific system behavior for additional security (*Additional security*).



Figure 15

## 6.5 Adding user accounts

**Dekart Logon Admin** enables you to add user accounts on KSD. The user account details contain the following: a) computer name or domain name, or an empty field; b) username; c) user password. The user data can then be read from the KSD during the authentication procedure. This leads to the following benefits:

- Secure two- and three-factor authentication.
- User convenience — no need to manually enter the user name and password during the Windows logon procedure.

**Dekart Logon** allows storing multiple user accounts on one Key Storage Device (depending on its memory size). This allows using KSD in the following situations and cases:

1. You can use one Key Storage Device containing several user accounts to access your personal computer under different names, to access different domains or even several computers. The ability to store multiple accounts on a single device becomes necessary when there is a need to create multiple environments on a single computer.
2. You can use one KSD to access all network computers with installed **Dekart Logon** if you have corresponding access rights.

**Note.** Every computer involved in KSD based authentication must have its unique name. When you (or anyone else) change the computer name, please, take into account that the Key Storage Devices belonging to users of this computer will no longer allow to access this computer until they update the user account data stored on them. To avoid such confusing situation, please, delete all account data from the KSD before applying any changes to

computer names and then add them again.

To add a user account, do the following:

1. Follow the instructions provided in "[Administering Dekart Logon - preliminary steps](#)".
2. Select **Users** tab and click **Add**. The dialog window will appear, as shown in Figure 16.

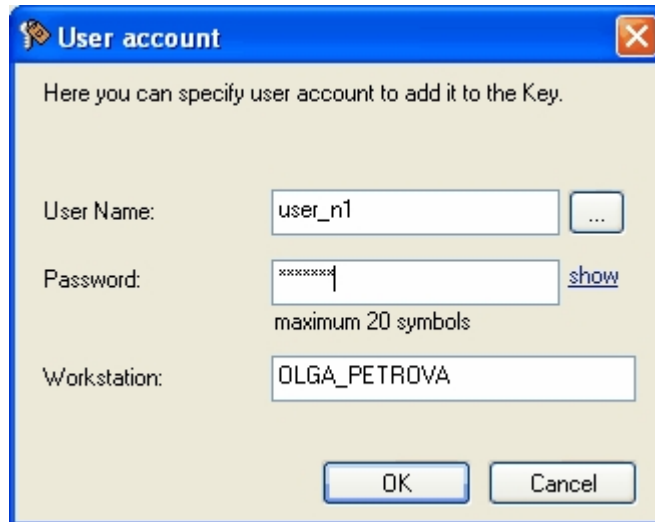


Figure 16

3. Enter your username in the **User Name** field and password in the **Password** field. The **Workstation** field may contains either the computer name or domain name in the "\\domain\_name" format (two backslashes and the domain name) or may be left empty for access to all computers with the installed **Dekart Logon**.

**Note:** In Windows NT like systems (Windows NT/2000/XP), you can enter the domain name after the user name in the Username field «username@domainname».

4. Click **OK**.

## 6.6 Deleting user accounts

To delete a user account from the Key Storage Device memory, do the following:

1. Follow the instructions provided in the "[Administering Dekart Logon - preliminary steps](#)" section.
2. Use **Users** tab to select the user account to be deleted and click **Remove**. The software will prompt you to confirm the removal procedure.  
**Note.** Please, be careful when deleting a user account currently in use (you have just used to access Windows). In case it is a single user account on your computer and you have previously configured Dekart Logon to allow only KSD based logon, you will not be able to access the system in the future.
3. Click **OK** to delete user account.

## 6.7 Changing user password

To change user passwords both in the system and on the Key Storage Device for the computer and for the domain, please do the following:

1. Follow the instructions provided in the "[Administering Dekart Logon - preliminary steps](#)" section.
2. Use **Users** tab to select the necessary user and click **Password....** The following window will appear:



Figure 17

3. Please, enter the new password in both fields.  
**Note 1.** The password length should not exceed 20 characters. The password has to be rather complicated to ensure that any malicious password guessing will not succeed. The statistics is that up to 33% of all passwords can be easily guessed by unauthorized parties. That's why we recommend not choosing passwords that have anything to do with your name, surname, birthdates or even your old passwords. Generally speaking, the stronger the password - the stronger the security.  
**Note 2.** If the company security policy requires implementing strong password policies on Windows NT/2000/XP operating systems, the attempt to set up a simple password using **Dekart Logon** will be unsuccessful.
4. To use the automatically generated password click [Generate password](#) link.
5. Click **Change**. The password change will apply both to user account and to the KSD.

## 6.8 Changing the password of the current user account

To change the password used to access the system, do the following:

1. Click Ctrl+Alt+Del. Then click **Change password...** in the appearing **Windows security** window. The following window will appear:



Figure 18

2. Enter the PIN-code in the required fields and the new password twice. To use the automatically generated password click [Generate password](#) link.
3. Click **Change**. The password change will apply both to user account and to the KSD.

## 6.9 Changing the PIN code

**Dekart Logon** allows to define and manage the Key Storage Device PIN-code, used to access **Dekart Logon** user credentials. The PIN-code protected devices provide strong authentication, as they cannot be used without knowing the PIN code by any other than KSD holder user. There are two reasons to change the KSD PIN-code:

- As there is no predefined PIN code on the new KSD, it should be set up to provide the required level of security.
- The PIN code can be changed at regular time intervals as defined by the respective company security policy.
- The PIN code should be changed if it has become available to the third-party, i.e. if it has been stolen.

To change the PIN code of the Key Storage Device, do the following:

1. Follow the instructions provided in "[Administering Dekart Logon - preliminary steps](#)".
2. Go to **Settings (Key settings)** and click **Change PIN**.



Figure 19

3. Fill in the required fields, as shown in Figure 19. If you want to use the KSD without the PIN code, check the **Remove PIN** checkbox (Figure 20).



Figure 20

4. Click **OK**. All changes will be written onto Key Storage Device memory.

## 6.10 Changing Key Storage Device label

**Dekart Logon** allows changing the label of the Key Storage Device. The KSD label may contain the name of the KSD holder or any other personal information. To change the KSD label, do the following:

1. Follow the instructions provided in the "[Administering Dekart Logon - preliminary steps](#)" section.

2. Go to *Settings (Key settings)* and click *Change Label*.



Figure 21

3. Fill in the required field as shown in Figure 21 and click *Change*.

## 6.11 Configuring Dekart Logon behavior on Key Storage Device removal event

After successful authentication you get the access to your computer. You may set up the computer to prohibit access to your desktop to anyone but you, especially if you often need to temporarily leave your workplace. Even if you leave your computer for a short time, we recommend that you lock the computer, e.g. by using the Screensaver with enabled **Password protect** option on Windows 9x, or using the **Control + Alt + Del** and **Workstation Lock** on Windows 2000/XP, and further authentication to the saved session upon returning to your workplace.

**Dekart Logon** allows to perform all actions mentioned above automatically. It allows monitoring the KSD removal/insertion events and locking the computer if required. Whenever you leave your computer, you may restrict any access to it by simply disconnecting the KSD. To unlock the computer and return to your current session, it is enough to connect the KSD to the computer.

To enable KSD removal/insertion monitoring, do the following:

1. Follow the instructions provided in "[Administering Dekart Logon - preliminary steps](#)".
2. Go to *Settings* tab and select one of the available options from the **Key removal behavior** list:

### Windows NT/2000/XP:

- **No action** – no action will be taken on Key Storage Device removal event.
- **Lock WorkStation** – the computer will be temporarily locked.
- **Force Logoff** – all open application will be closed and the application will trigger a user Logoff event.



Figure 22

**Windows 9x:**

- **No action** – no action will be taken on Key Storage Device removal event.
- **Activate Screen Saver** – the screensaver will be activated and will temporarily block access to the computer.

To enable all selected changes click the Ctrl+Alt+Del key combination, select **Lock** or **LogOff...** (Windows NT/2000/XP) or restart your computer (Windows 9 ).

## 6.12 Enabling additional security mode

To configure the application to allow only two- or three-factor authentication, do the following:

1. Follow the instructions provided in the "[Administering Dekart Logon - preliminary steps](#)" section.
2. Go to **Settings (Additional security)** tab and check the **Allow logon only with Key** checkbox if you want to access the system by using the Key Storage Device only (without the option of manually entering the password).

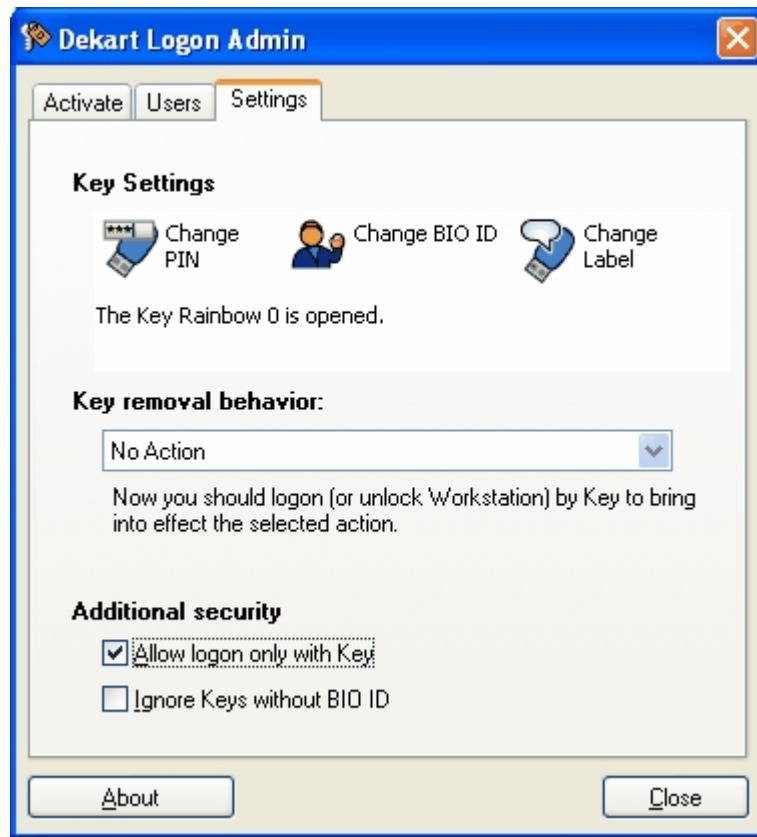


Figure 23

If you enable the **Ignore Keys without BIO ID** option, **Dekart Logon** will authorize users only with devices containing users' biometric identifiers.

**Note.** To enable this feature, you will need to write your biometric identifier onto the KSD. Otherwise, the software will display a warning message.

## 6.13 Adding biometric identifier to the KSD

To enable the three-factor authentication, you will need to store your biometric identifier on the KSD.

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

To add BIO ID, please do the following.

1. Follow the instructions provided in the "[Administering Dekart Logon - preliminary steps](#)" section.
2. Go to **Settings (Key settings)** tab and click **Change BIO ID**.

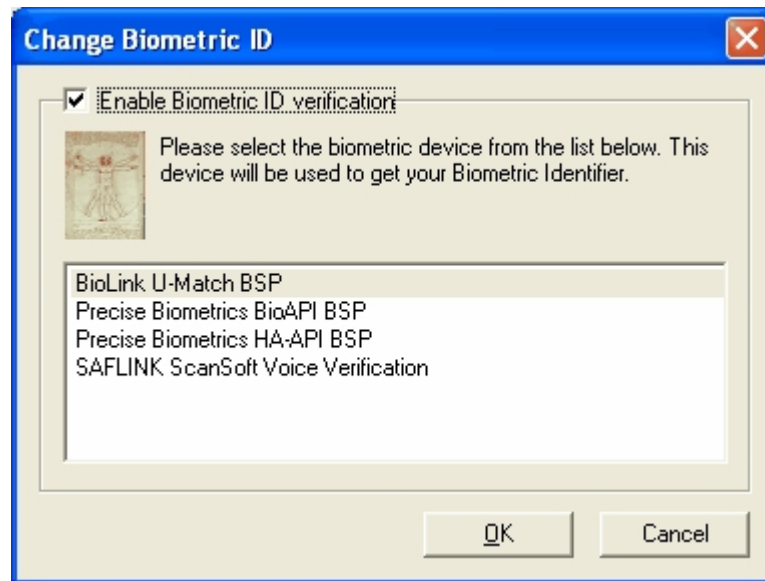


Figure 24

3. Check the **Enable Biometric ID verification** checkbox and select the biometric device from the list.
4. 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 will be stored on the KSD.

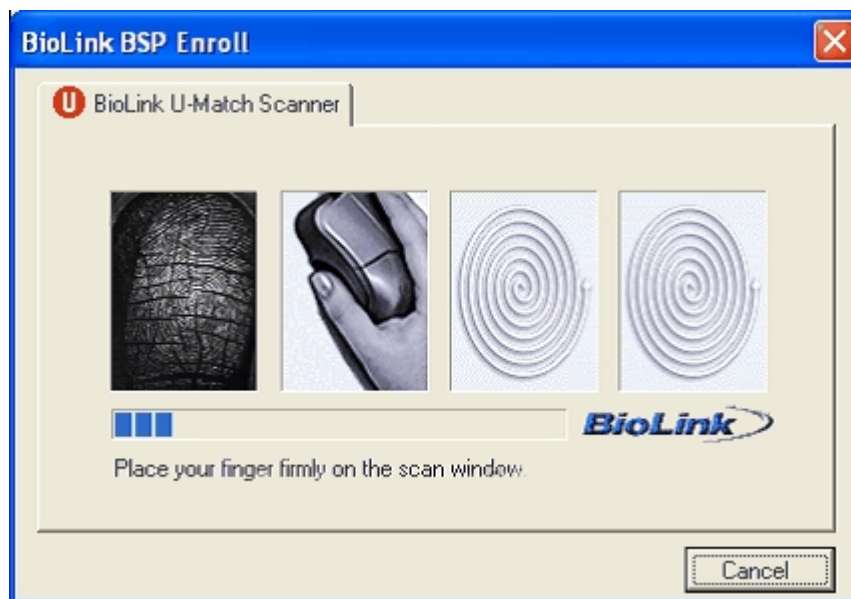


Figure 25

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, it is then stored on the KSD.



Figure 26

## 6.14 Changing the biometric identifier on the KSD

To change the BIO ID (if it has been previously stored on the KSD), please do the following:

1. Follow the instructions provided in "[Administering Dekart Logon - preliminary steps](#)".
2. Go to **Settings (Key settings)** tab and click **Change BIO ID**.
3. Select the biometric device from the list ([see also](#)).
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** window.

## 6.15 Using Dekart Logon

This section describes the features of **Dekart Logon**, most widely used in the day-to-day routines:

- [Authentication](#).

- [Operating system lock.](#)

## 6.16 Authentication

**Dekart Logon** replaces the standard Windows authentication procedure with its own, allowing the user to select between the one-factor, two-factor and three-factor authentication. In certain cases, the user can authenticate by standard means, for example, if **Dekart Logon** has just been installed on the computer, or the user has not yet obtained a Key Storage Device. To enable standard authentication, please do the following:

1. Turn on the computer.
2. Enter your *User name* and *Password* in the dialog window, as shown in Figure 27.

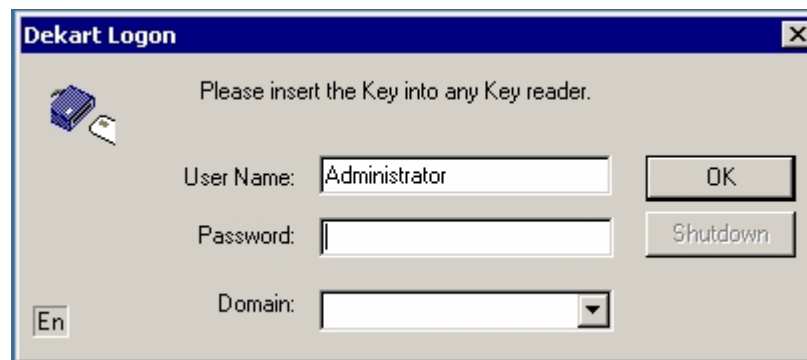


Figure 27

**Note.** You only have three attempts to enter the authentication data. After three consecutive wrong entries, the user authentication is not available unless the computer is restarted.

3. Click **OK**. Standard authentication is completed.

Once you have installed **Dekart Logon** on your computer and have securely stored your user account on the Key Storage Device, you are able to access the system using strong two- or three-factor authentication (using the PIN code and biometric identifier) in the following way:

1. Turn on the computer. In the dialog box that appears, as shown in Figure 27, connect the Key Storage Device to the computer.

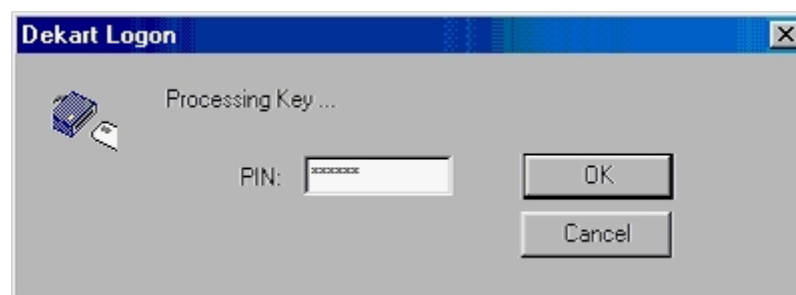


Figure 28

2. Enter the PIN code into the *PIN* field, as shown in Figure 28, click **OK**.

**Note. Please, be careful** — the KSD will block up on multiple wrong PIN code entries

and all information stored on it will become inaccessible. The number of allowable incorrect entries varies according to the KSD manufacturer, and the application.

3. If the [biometric identifier is stored on the KSD](#), the software will automatically detect it and will attempt to start biometric authentication (scan the fingerprint, speak the key phrase etc.). If your biometric identifiers do not match with the biometric templates stored on the KSD, the software will prompt you to repeat the biometric authentication. This ensures that no one but you will be able to access your computer, even if your KSD is lost or stolen.

## 6.17 Locking your operating system

You may set up the computer to prohibit access to your desktop to anyone but you, especially if you often need to temporarily leave your workplace unattended. Even if you leave your computer for a short time, we recommend that you lock the computer to ensure that no one will have access to it while you are away. You can lock your computer by using a Screensaver on Windows 9x (with **Password protect** option enabled), or using the **Control + Alt + Del** and **Workstation Lock** on Windows 2000/XP. To return to the saved session, you will need to conduct authentication by entering your username and password.

**Dekart Logon** allows performing all actions mentioned above automatically. It allows monitoring the KSD removal/insertion events and locking the computer if required.

Whenever you leave your computer, you may restrict any access to it by simply disconnecting the KSD. To unlock the computer and return to your current session, it is enough to connect the KSD to the computer. To configure the behaviour of **Dekart Logon** on KSD removal event, please follow the instructions described in section

["Configuring Dekart Logon behavior on Key Storage Device removal event"](#)

## 6.18 Terminating Windows NT/2000/XP session

**Dekart Logon** allows to terminate a user session on Windows NT/2000/XP in the following way:

1. Click **Control + Alt + Del** key combination. The following window will appear (Figure 29).

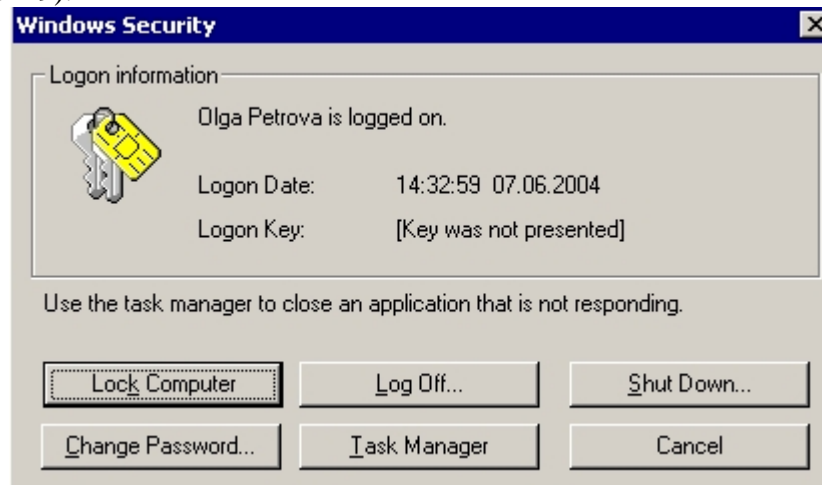


Figure 29

2. You can choose one of the following actions:
  - **Lock computer** – Temporarily locks the computer.
  - **Log Off...** - Closes your user account but the computer remains on for easy access the next time you log on.
  - **ShutDown...** - This action shuts down Windows so that you can safely turn off the computer power. Many computers turn the power off automatically.
  - **Change Password** – Enables to change the user password for current user account.
  - **Task Manager** – Runs **Task Manager**. Windows Task Manager provides information about computer performance and displays details about programs and processes running on your computer.
  - **Cancel** – Closes current window.
3. If you press the **ShutDown...**, button the following window will appear (Figure 30).



Figure 30

4. Please, select one of the following available actions:
  - **Log Off...** - Closes your user account but the computer remains on for easy access the next time you log on.
  - **Restart** – Restarts your computer.
  - **ShutDown...** - Shuts down Windows so that you can safely turn off the computer power. Many computers turn the power off automatically.
  - **Stand By** – Puts your computer on standby. Standby is a state in which your monitor and hard disks turn off, so that your computer uses less power.
  - **Hibernate** – Puts your computer in hibernation. Hibernation is a state in which your computer shuts down to save power but first saves everything in memory on your hard disk.
5. Click **OK** to terminate your current session.

## 6.19 Getting information about the product

Click the **About** button to view information about **Dekart Logon**. The following window will appear:



Figure 31

**Note.** If you use an unregistered copy of **Dekart Logon** the *About Dekart Logon* window will display empty registration fields as shown in Figure 32.

## 6.20 Registering Dekart Logon

To register the program, if this has not been done during the installation procedure, go to the *About Dekart Logon* window, and enter the registration information in the proper fields.

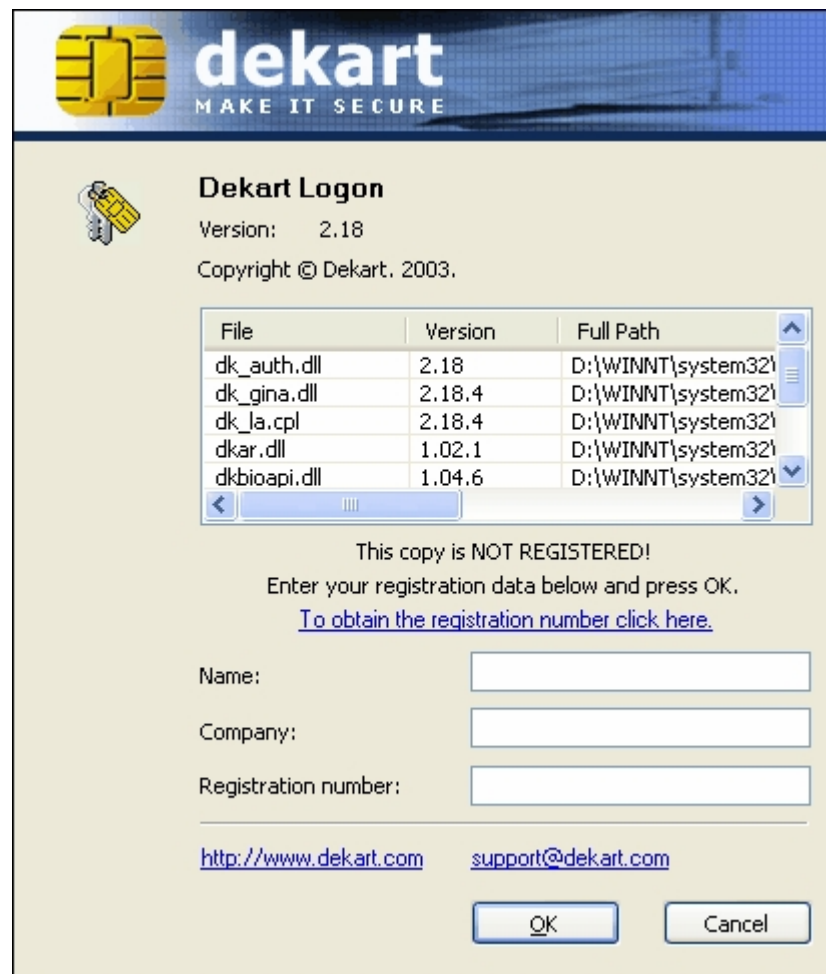


Figure 32

Please, obtain a registration number at [Software Registration \(Register\)](http://www.dekart.com) page at [www.dekart.com](http://www.dekart.com). In case you use licensed Dekart software, please, submit your license key to receive your registration number to your 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.

## 6.21 Adding User's Logo

If desired, you can change the Dekart Logo appearing on start up to your own logo. To change Dekart logo, please, do the following:

1. [Activate](#) Dekart Logon (if you haven't previously done it).
2. Run regedit utility (located in WINDOWS or WINNT directory).
3. Go to [HKEY\_LOCAL\_MACHINE\SOFTWARE\Dekart\Logon], create new string value (New -> String Value).
4. Assign a name "Logo Picture" to the new string value .
5. Write a complete path to the .bmp file of the new logo.

**Note.** Required logo size is 413x65 pixels. The logo will be displayed "as is" - without any resizing.

## 7 Troubleshooting

This chapter contains:

1. **Diagnostic Messages List.** These messages result from wrong user actions or **Dekart Logon** hardware or software errors during the software operation.
2. **Message identification numbers.** These numbers are used to identify possible problems when users contact Dekart Support Department.
3. **Message explanation list.** These descriptions are given in the *Explanation* column of the Diagnostic Messages table.
4. **On-Message Actions List.** The actions to be carried out on receiving a certain message are given in the *Action* column of the *Diagnostic Messages* table.

If any contingencies occur during **Dekart Logon** installation and operation and the user does not know how to handle the situation, the *Diagnostic Messages* table can be used as follows:

5. The *Message* column contains the message received from a user.
6. The *Explanation* column contains the descriptions of the reason for this message.
7. The *Action* column contains the descriptions of the actions that should be taken to handle the corresponding situation.
8. The "###" column contains the unique message id required only when contacting technical support service. These numbers are used for error identification when contacting Dekart Support service.

The *Diagnostic Messages* table is provided below.

**Diagnostic Messages table. Dekart Logon Admin messages.**

##	Message	Source	Explanation	Action
01-01	An error occurred while loading SmartKey.dll. Key management functions cannot be executed.	At Logon Admin startup	The SmartKey.dll library has not been found. Dekart Logon will not function without this library.	Install Dekart Smartkey. For additional information, please contact technical support service.
01-03	This User already exists.	Add User dialog	The username you are trying to add already exists in the system.	Please, enter another username.
01-05	Exceeded the available number of accounts for this Key.	Add User dialogs	The number of user accounts that can be stored on one KSD is limited to 18.	Please, delete unnecessary user accounts from the KSD or use another KSD.
01-05	Exceeded the available number of accounts for this Key.	Add User dialogs	The number of user accounts that can be stored on one KSD is limited to 18.	Please, delete unnecessary user accounts from the KSD or use another KSD.
01-10	An error occurred while writing to the Key.	Add User, Delete User dialogs	Error writing information to the KSD. The key may already contain 18 user accounts and adding a new user account is impossible.	Disconnect and then connect the KSD again. Connect another KSD, if necessary. Exit the program and start it again, repeat the action which caused this error. Please, contact technical support service if the problem appears to happen again.
01-12	The password you entered is incorrect.	Delete User dialog	You have changed the system password without changing the password on the KSD.	Please, use the system utilities to make the system password match with the one stored on the KSD and repeat the operation. Change the password again, if necessary.
01-14	The PIN you entered is incorrect.	Add User, Delete User dialogs	The PIN code you have entered does not match with the code required to access the KSD. You may have connected the wrong KSD.	Try entering the PIN code again. Make sure you have connected the right KSD. Disconnect and then connect the KSD again. If the problem persists, please contact technical support service.
01-15	The password you entered is incorrect.	Add User dialogs	The password you have entered does not match with the password of the user being copied.	Please, enter correct password.

**Diagnostic Messages table. Dekart Logon messages.**

##	Message	Source	Explanation	Action
02-01	Incorrect User name or password.	OS logon dialog	The password and username you have entered do not correspond to user account of the operating system.	Enter correct user account data or connect the KSD containing correct data.
02-02	Local User profile has not been found on this Key.	OS logon dialog	The KSD you have connected does not contain a user account of this PC. You may have connected the wrong KSD.	Make sure you have connected the right KSD. Disconnect and then connect the KSD again. If the problem persists, please contact technical support service.
02-03	The PIN you entered is incorrect.	OS logon, Screen Saver dialogs	The PIN code you have entered does not match with the code required to access the KSD. You may have connected the wrong KSD.	Try entering the PIN code again. Make sure you have connected the right KSD. Disconnect and then connect the KSD again. If the problem persists, please contact technical support service.
02-04	The Key is blocked.	OS logon, Screen Saver dialogs	You have used all three attempts to enter the wrong PIN code and this lead to KSD blocking.	Connect another KSD or contact technical support to receive instructions on how to unblock the KSD.
02-05	The Key you connected has not been initialized.	OS logon, Screen Saver dialogs	The KSD you have connected does not contain the license for <b>Dekart Logon</b> .	Connect another KSD or contact technical support service.
02-06	Unidentified Key or reader error.	OS logon, Screen Saver dialogs	Unknown error while reading the data from the KSD. Possible reason – hardware error (USB token, smart card or smart card reader failure).	Disconnect and then connect the KSD again. Try to repeat the action which led to this error. If the problem persists, please contact technical support service.
02-07	The Key is blocked. Format the Key to unblock it.	OS logon, Screen Saver dialogs	The KSD has been blocked and requires reformatting.	Connect another KSD or contact technical support service.
02-08	To unlock this workstation current User should insert the Key or enter their password.	Screen Saver dialog	The PC can be unlocked using the KSD or password of the current user only.	Connect another KSD or enter the user password.
02-09	The password you entered is incorrect.	Screen Saver dialog	The password you have entered does not match with the password of the current user.	Enter correct data or connect the KSD, containing correct user account data.



## 8 Glossary

*Application Programming Interface (API)* - a software interface used for interaction between the application and the operating system.

*BIOS* - the Basic Input/Output System is an OS-independent software designed for hardware operation support. An essential set of routines in a PC, which is stored on a chip and provides an interface between the operating system and the hardware.

*BIOS Setup Utility* - the utility for managing BIOS settings.

*COM-port* - PC serial communication port.

*International Organization for Standardization (ISO)* - International Organization for Standardization

*IRDA-port* - standard port for infrared data transmission and printing developed by the Infrared Data Association.

*ISO 7816* - list of requirements to the readers' physical properties and smart card data exchange protocols.

*Key Storage Device (KSD)* - the device used to store key information. The KSD may be a smart card, USB token, USB Drive etc. Dekart Logon uses the KSD to store user account data and user's biometric identifier. The KSD may be PIN code protected.

*Microsoft Windows Installer (MSI)* - the Microsoft Windows Installer (MSI) is a new installation service, enabling efficient installation and configuration of applications. For example, if an installation is unsuccessful, the installer restores the original state of the computer. MSI is built into Windows 2000 and Windows Millennium, and is freely available as a redistributable file for Windows 95/98 and NT 4.0.

*PCMCIA-port* - the port conforming with the PCMCIA specifications (Personal Computer Memory Card International Association)

*Personal Computer/Smart Card (PC/SC)* - smart card readers' specifications supported by **DekartLogon**.

*PIN-code* - the *Personal Identification Number* is used to confirm the authorization to access the data stored on the *hardware key*.

*PS/2-port* - the port used to connect the keyboard and the mouse to the PC.

*Universal Serial Bus (USB)* - the Universal Serial Bus can be used to connect and disconnect peripheral devices without opening the PC case and even without shutting down the computer.

The USB automatically detects these devices and configures the corresponding software.

*Authentication* - this is a control process checking the authenticity of the user's identity, i.e. this process checks whether the user is the person he claims to be.

*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.

*One-Factor or Standard Authentication* - a process controlling the authenticity of the user identity by standard means of the OS on the basis of a single factor: *Something You Know* – the user name and password.

*Two-factor Authentication* - a process controlling the authenticity of 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* - 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*".

*KSD monitor*- a subsystem of **Dekart Logon** used to ensure additional computer security. It controls whether the Key Storage Device is available in the key reader or the USB port and locks the computer access when the key is removed.

*Driver* - a software designed to control data input/output and interface, the applications/OS and the device connected to the PC.

*Identification* - a control process using a unique identifier to determine whether the specific user is known to the system.

*Logon* - a special process resulting in user authentication into the OS according to the user name and the password. After successful completion of this process, the user gains access to the OS according to the rights granted to that user.

*Smart Card* - a plastic card with an embedded microchip including the secured memory block with special hardware implementing the encryption algorithms — techniques for secret information encrypting/decoding. The smart card is connected to the computer by means of a special device — the smart card reader.

*Smart Card Reader* - this is a device used to operate smart cards. The reader can be both internal (connected as a standard 3,5" floppy disk drive) and external (connected by means of one of the following ports: *COM, PS/2, USB, PCMCIA, IRDA*, etc.)

***StrongLogin*** - this is a login process supplemented with strong authentication means, for example, the means of **DekartLogon**.

***ScreenSaver*** - this is a dynamic or a static picture appearing on the PC screen after the key strokes or mouse movement have not been detected for a certain amount of time. It is used for two purposes: to save the screen from discoloration and prevent the computer from an unauthorized access.