COPYRIGHT
Copyright © 2003 Dekart. 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, or its suppliers or affiliate companies.

DISCLAIMER
Dekart 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 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 makes no representations or warranties with respect to any Dekart Key Manager software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Dekart reserved the right to make changes to any and all parts of Dekart Key Manager 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 DOCUMENTATION DESCRIBES, CONSULT THE README.TXT, 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 TRADEMARK ATTRIBUTIONS
All other registered and unregistered trademarks in this document are the sole property of their respective owners.

DEKART CONTACT INFORMATION
E-mail: for sales details: sales@dekart.com
for product support: support@dekart.com
for comments and feedback: info@dekart.com
WWW: www.dekart.com
TRADEMARKS

Trademarks of third party

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.
Contents

Preface ............................................................................................................................ 7
Operating Guide purpose ................................................................................................. 7
Operating Guide structure .............................................................................................. 7
Documentation conventions ........................................................................................... 7
Documentation set ........................................................................................................... 7
How to contact Dekart ..................................................................................................... 8

Chapter 1. Introducing Dekart Key Manager .............................................................. 10
Purpose ............................................................................................................................. 10
Main features .................................................................................................................. 10
Dekart Key Manager components ................................................................................. 10

Chapter 2. Dekart Key Manager hardware and software requirements ................. 11
Personal Computer hardware requirements ................................................................... 11
Personal Computer software requirements .................................................................... 11

Chapter 3. Dekart Key Manager installation, update and de-installation ............... 12
Installation ....................................................................................................................... 12
Re-installing Dekart Key Manager ................................................................................ 19
Updating Dekart Key Manager ..................................................................................... 19
Removing Dekart Key Manager .................................................................................... 19

Chapter 4. Using Dekart Key Manager ................................................................. 21
Getting started ............................................................................................................... 21
Viewing and backing up the contents of the hardware key ........................................... 21
Viewing the contents of the hardware key ................................................................... 22
Creating backup copies ............................................................................................... 25
Opening and viewing the backup copy ....................................................................... 26
Editing the contents of the hardware key .................................................................... 27
Copying the data to clipboard ...................................................................................... 27
Pasting the data from clipboard .................................................................................. 29
Copying the data from one hardware key to another .................................................... 30
Adding Dekart application data ................................................................................... 31
Deleting data from the hardware key .......................................................................... 32
Editing Dekart application data based on the context of the application .................... 34
Binary editing of Dekart application data ................................................................... 35
Creating the templates of the hardware key contents .................................................. 36
Managing the hardware key ........................................................................................ 36
Changing the PIN code ............................................................................................... 36
Changing administrator's PIN code ............................................................................ 38
Changing biometric identifier ...................................................................................... 38
Unblocking the PIN code ........................................................................................... 39
Editing the symbolic label ......................................................................................... 39
Searching the backup copies of the hardware key .................................................................41
Configuring Dekart Key Manager ..........................................................................................43
  Configuring the names of the applications ....................................................................44
  Embedding additional components ..............................................................................45
  Embedding additional components (plug-ins) for viewing and editing .......................45
  Formatting the hardware key .......................................................................................45
  Configuring the toolbar of the main window ..............................................................47
Safety recommendations for Dekart Key Manager .............................................................47
Closing Dekart Key Manager .............................................................................................47
Registering Dekart Key Manager ......................................................................................47
Dekart Key Manager technical support ............................................................................48

Chapter 5. Troubleshooting .................................................................................................51
  Possible problems ............................................................................................................51
  Diagnostic messages .......................................................................................................51

Glossary ...............................................................................................................................54
Preface

Dekart Key Manager is a versatile management tool for USB tokens and smart cards. It works with a wide array of devices from various vendors.

Dekart Key Manager simplifies the process of managing multifactor security solutions within the enterprise. This is a tool for administrators charged with the challenging task of managing hundreds, sometimes thousands, of USB tokens and smart cards.

Operating Guide purpose

This Operating Guide is designed for Dekart Key Manager users and contains information about installing, operating and de-installing Dekart Key Manager.

This Guide contains the list of software and hardware requirements to provide the proper operation of Dekart Key Manager.

Operating Guide structure

This Guide consists of the following chapters:

- Chapter 1 Introducing Dekart Key Manager describes the purpose and the features of Dekart Key Manager.
- Chapter 2 Dekart Key Manager hardware and software requirements lists and describes PC software and hardware required for Dekart Key Manager to operate properly.
- Chapter 3 Dekart Key Manager installation, update and de-Installation describes in detail how to install, update, and de-install Dekart Key Manager.
- Chapter 4 Using Dekart Key Manager thoroughly describes all aspects of using Dekart Key Manager.
- Chapter 5 Troubleshooting is devoted to detecting and eliminating possible problems. All diagnostic messages and events causing them are listed, the troubleshooting measures are suggested.
- Glossary is an explanatory dictionary containing important terms used in this Guide.

Documentation conventions

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

In this Guide, the greater than (>) symbol is used to separate the operations within one action. Interface elements are bold-faced and italicized.

Documentation set

- Operating Guide designed for Dekart Key Manager users.
How to contact Dekart

To order the products, request information about the products, receive technical support, etc., please refer to Dekart.

• Technical Support
  You can receive technical support for Dekart Key Manager contacting us at support@dekart.com

• Comments and suggestions
  If you have ideas, suggestions, comments, critics or questions, we would like to hear from you about our software or documentation by e-mail: info@dekart.com.

• Customer Service
  For ordering or getting information about Dekart products please contact us by e-mail: sales@dekart.com
Chapter 1. Introducing Dekart Key Manager

This chapter describes the purpose and features of Dekart Key Manager.

Purpose

Dekart Key Manager creates back up copies of the USB tokens or smart cards and stores them in protected files. The protected files can be stored in a secure location. If the user loses the key device, Dekart Key Manager will create a replacement copy from a back up. The user will not lose valuable data or access to protected resources.

Dekart Key Manager enables you to browse, interpret and edit content of the memory of a USB token or a smart card. It gives the administrator complete knowledge about all Dekart applications that store data on the key. Data can be moved from one key to another, edited and stored back on the key.

Main features

Dekart Key Manager has the following features:

- works with the majority of devices produced by leading smart card and USB token vendors.
- displays all smart card readers and USB tokens that have been previously installed in the system.
- displays properties of inserted smart cards and USB tokens and Dekart applications’ data.
- backs up and restores Dekart applications’ data from the USB tokens or smart cards.
- allows to change PIN and label of the USB token or smart card, unblock PIN.
- powerful search tool.
- supports pluggable viewers of applications’ data.

Dekart Key Manager components

Dekart Key Manager consists of the following components:

- Software Dekart Key Manager.
- This Operating Guide.
Chapter 2. Dekart Key Manager
hardware and software requirements

This chapter describes the following:

- **Dekart Key Manager** personal computer hardware requirements.
- Operating systems with the corresponding service packs required for **Dekart Key Manager** to run properly.

**Personal Computer hardware requirements**

For **Dekart Key Manager** to run properly, a PC with the following minimum properties is required (this applies mainly to the computers running Windows 95):

- Intel Pentium 166 MHz processor
- 16 MB RAM
- 2 MB or more free hard disk space

A smart card reader or USB token complying with *PC/SC (Personal Computer/Smart Card)* specification is required.

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

- A USB port, if a 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**

**Dekart Key Manager** supports the following operating systems:

- Windows 95 OSR2.1
- Windows 98 SE
- Windows Me
- Windows NT4 Workstation, Server with Service Pack 6
- Windows 2000 Professional, Advanced Server with Service Pack 3 or higher
- Windows XP Professional, Home Edition

In addition, you must install drivers for the smart card readers, or USB tokens being utilized on your PC.
Chapter 3. Dekart Key Manager installation, update and de-installation

Before installing, make sure that the PC meets the product hardware and software requirements indicated in chapter 2 of this Guide, Dekart Key Manager hardware and software requirements.

Note: To install the product components under Windows operating systems designed for corporate use — Windows NT, Windows 2000, Windows XP — it is necessary to log into the system as administrator. In Windows operating systems designed mainly for private use — Windows 95/98/ME, Windows XP Home — every user has the required rights.

Installation

Note: To be able to install Dekart Key Manager on Windows NT, Windows 2000, Windows XP, you must have administrator privileges.

The following steps must be performed to install Dekart Key Manager:

1. Insert Dekart Key Manager product CD into the CD-ROM drive and run SETUP.EXE. If you have downloaded the installation file from the Internet, please run KeyMan.exe (English version).

2. The welcome screen will appear, as shown in Figure 1.

![Setup window](image)

Figure 1
Dekart Key Manager welcome screen
3. Click **Next**. The *End-User Software License Agreement* will appear, as shown in Figure 2.

![Dekart Key Manager license agreement](image)

**Figure 2**

**Dekart Key Manager** license agreement

4. Carefully read the text of the license agreement between you, **Dekart Key Manager** end-user, and **Dekart**. Select **Yes, I accept this agreement** check box if you agree with the terms, and click **Next**. The **Registration** window will appear, as shown in Figure 3.

**Note:** If you do not agree with the terms of license agreement, *do not select* the check box and click **Cancel**. In this case, **Dekart Key Manager** installation will be terminated.
5. Fill out the fields in the registration window and click Next. A product location selection screen will appear, as shown in Figure 4.

**Note:** The serial (licence) number of your Dekart Key Manager copy must be entered into the **Serial Number** field.
6. Indicate the directory into which Dekart Key Manager should be installed on your computer and click Next. A program folder selection screen will appear, as shown in Figure 5.
7. Indicate Dekart Key Manager folder name on your computer and click Next. A *Ready to Install* window will appear, as shown in Figure 6.
8. Click **Next** to start copying **Dekart Key Manager** files.

9. Wait until the installation completion window appears, as shown in Figure 7.
10. Click *Finish*.

11. All of the system changes enabled by the installation will take effect after restarting the computer. Restart the computer.
Re-installing Dekart Key Manager

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

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

To re-install Dekart Key Manager, start the KeyMan.exe or SETUP.EXE file from the Dekart Key Manager product CD. Further actions are similar to those described in the Installation section of this chapter.

Updating Dekart Key Manager

Dekart Key Manager can be updated upon acquiring a newer version of the product.

To acquire a newer version of the product, please contact Dekart at sales@dekart.com. The corresponding software can be downloaded from http://www.dekart.com or specially ordered.

To install a newer version of Dekart Key Manager on the computer, start the KeyMan.exe or SETUP.EXE file from the product CD. The installation utility will locate the current version of the product and will suggest that it be updated. Further actions are similar to those described in the Installation section of this chapter.

Removing Dekart Key Manager

Under certain conditions, you may need to remove Dekart Key Manager. Do the following to remove it with standard Windows OS facilities:

1. Exit Dekart Key Manager.
2. Choose Uninstall from Key Manager group at Start menu (Start > Programs > Dekart > Key Manager). OR Use Add/Remove Programs dialog from Control Panel to remove program (Start > Settings > Control Panel).
3. After this the system will require that you confirm the software removal, as shown in Figure 8.

![Figure 8](remove_confirmation.png)

Remove confirmation

4. On clicking Yes, the system will remove the program and report about the successful completion, as shown in Figure 9.

Note: on clicking No, de-installation is terminated.
5. Click **OK** to complete the process.
Chapter 4. Using Dekart Key Manager

The main purpose of this chapter is to familiarize the user with the main features and functions of Dekart Key Manager.

Getting started

After successful installation of Dekart Key Manager its icon will appear in Start menu: Start > Programs > Dekart > Key Manager > Key Manager. After running Dekart Key Manager the main window of the application will appear, as shown in Figure 10.

![Main window of Dekart Key Manager](image)

Figure 10
Main window of Dekart Key Manager

Viewing and backing up the contents of the hardware key

This section describes how to view the application data and hardware key service data, as well as back up the data stored on the hardware key and view backup copies.
Viewing the contents of the hardware key

After starting Dekart Key Manager the window shown in Figure 10 will appear. In the left part of the window the list of smart card readers and USB tokens is displayed. The right panel of the window contains the information about the current state of the selected smart card reader or USB token, as well as the contents of the smart card or USB token that has been connected.

To start viewing the contents of the hardware key, the user has to connect it. Figure 11 displays the empty contents of the hardware key.

The right panel of the window displays all basic characteristics of the hardware key:

- **Size** – total volume of the hardware key memory
- **Free Size** – free portion of hardware key memory, available for Dekart applications
- **Serial Number** – unique serial number of the hardware key
- **Label** – symbolic label of the hardware key
- **PIN** – shows if the hardware key is PIN code protected
- **Status** – current state of the hardware key (connected or disconnected)

If the user connects a hardware key containing Dekart application data, the list of these applications will automatically display in the left side of the window (Figure 12).
If the hardware key is PIN code protected, Dekart Key Manager will require user to enter correct PIN code before starting any operations with the hardware key (Figure 13).
To view the data of the application, the name of this application has to be selected in the left side of the window. The right panel will display the portion of hardware key memory occupied by this specific application, as well as the free memory available to its data (Figure 14).

![Image of SchlumbergerSema Reflex 200 Key Manager window](image)

**Figure 14**
Viewing the information about the application

To view the data of the selected application, press the **Read Data** button. The read data will display in the right panel (Figure 15). Display format will depend on the additional component for viewing the data, which is separately implemented for each application (see **Embedding additional components for viewing and editing** section).
Creating backup copies

To create a backup copy of the hardware key contents, use the left side of the window to select the hardware key or any of its applications to be backed up and then go to File > Save As ... menu. Use the dialog window to specify the location to store the backup copy of the hardware key (Figure 16).
Opening and viewing the backup copy

To open a backup copy select **File > Open …** menu. The following dialog will appear (Figure 17):

The contents of the backup copy will display in the same way as the contents of the smart card or USB token (see **Viewing the contents of the hardware key** section), only that the file icon in the left part of the window will appear and all the operations will apply to the file (Figure 18).
Editing the contents of the hardware key

Dekart Key Manager allows to:

- edit application data;
- copy the data to clipboard;
- paste the data from clipboard;
- delete selected data;
- add data.

Copying the data to clipboard

To copy all contents of the hardware key to clipboard, the hardware key should be opened (see Viewing the contents of the hardware key section). After right-clicking the selected hardware key, the context menu will appear, as shown in Figure 19. Select Copy from the context menu. After this selection all data will be copied to Clipboard.

The same result can be achieved through Edit > Copy command of the main window.
To copy data of the specific application to clipboard, open the hardware key (see Viewing the contents of the hardware key section), select the required application and right-click on its name to view the context menu (Figure 20). After you select *Copy* from the context menu all data will be copied to clipboard.

The same result can be achieved through *Edit > Copy* command of the main window.

Figure 19

Copying all data to clipboard
Copying data of the application to clipboard

**Pasting the data from clipboard**

To paste the data from clipboard to hardware key, open the hardware key (see *Viewing the contents of the hardware key* section), select it and right-click on its name to view the context menu (Figure 21). After you select *Paste* from the context menu all data will be copied from clipboard.

The same result can be achieved through *Edit > Paste* command of the main window.
Pasting the data from clipboard

The following warning message will appear if the application data already exists on the hardware key (Figure 22).

Copying the data from one hardware key to another

To copy data from one hardware key to another, open the source hardware key (see Viewing the contents of the hardware key section), select it and go to Edit > Copy To … menu of the main window. The window with the list of the available hardware keys will appear (Figure 23). The following warning message will appear if the application data already exists on the hardware key (Figure 22).
To copy data of the specific application from one hardware key to another, open the source hardware key (see Viewing the contents of the hardware key section), select the required application and go to Edit > Copy To … menu of the main window. The window with the list of the available hardware keys will appear (Figure 23). The warning message will appear if the application data already exists on the hardware key (Figure 22).

Adding Dekart application data

To manually add the data of the specific application to the hardware key, open the source hardware key (see Viewing the contents of the hardware key section), select the required application and go to Edit > Add … menu of the main window. The window with the list of applications (see Configuring the names of the applications section), which can be added to the hardware key, will appear (Figure 24).

After the application has been added, Dekart Key Manager allocates the required part of the hardware key memory, defined for each application separately. The selected data block will be initialized with zero value, which can be manually edited in the future (see Editing and copying application data section).
Deleting data from the hardware key

To delete the data from the hardware key, open the hardware key (see Viewing the contents of the hardware key section), right-click on its name and select Delete All from the context menu (Figure 25). The deletion warning message will appear (Figure 26). After confirmation all data will be deleted.

The same result can be achieved through Edit > Delete … command of the main window.
To delete all data of the specific application from the hardware key, open the hardware key (see Viewing the contents of the hardware key section), select the required application, right-click on its name and select **Delete** from the context menu (Figure 27). The deletion warning message will appear (Figure 28). After confirmation the application data will be deleted.

The same result can be achieved through **Edit > Delete …** command of the main window.
Editing Dekart application data based on the context of the application

Some applications allow viewing and editing their data in common (user) mode (Figure 29). The user mode is automatically turned on when the application data is opened (see Viewing the contents of the hardware key section). The user mode is invoked through use of embedded components, specially implemented for each application. The procedure of embedding these components is described in Embedding additional components for viewing and editing section.
Editing data of the separate application

**Binary editing of Dekart application data**

To edit the data of a specific application in hexadecimal mode, open the source hardware key (see *Viewing the contents of the hardware key* section), select the required application and go to *Edit > Binary editor* ... menu of the main window. The binary data editor will appear (Figure 30).

This editor allows editing separate hexadecimal values, copying separate data blocks to clipboard, pasting from clipboard, deleting data.

**Note:** Binary editing is a very critical operation and may lead to serious data losses, if it is performed by a person having not enough expertise in the subject.
Creating the templates of the hardware key contents

The fact that Dekart Key Manager works with file backup copies allows creating templates of the hardware key contents, which can be further used as the basis for issuing a large number of common key data, with all necessary personalization.

To create a template, go to File > New menu of the main window. Creating, editing and copying the templates are identical to working with the hardware key (see Viewing the contents of the hardware key section and Editing the contents of the hardware key section).

Managing the hardware key

Apart from the fact that Dekart Key Manager allows editing the contents of the hardware keys, it enables user to change some attributes of the hardware key, these being the PIN code and symbolic label.

Changing the PIN code

To change the PIN code for accessing the hardware key, open the hardware key (see Viewing the contents of the hardware key section), right-click on its name and select Change PIN ... from the context menu (Figure 31).
The dialog window offering to change or remove the PIN code will appear (Figure 32). The same result can be achieved through Tools > Change PIN … command of the main window.

Figure 32
Changing the PIN code of the hardware key
Changing administrator's PIN code

To change the administrator's PIN code (also called "issuer's key" or "security officer's key"), allowing to change or unformat the key storage device, please, open the key storage device contents (see Viewing the contents of the key storage device section) and select Tools > Change Administrator's PIN. Enter the old administrator's code and the new administrator's PIN code. Both old and new PIN codes can be entered in both usual text mode (a password or a common digits' PIN) – please, check the ASCII checkbox, or in hexadecimal mode – provided that you check the Hex String checkbox (Figure 33).

![Figure 33](image)

Changing administrator's PIN code

**Note:** Please, be very attentive when entering your old and new administrator's PIN codes. Entering wrong administrator's PIN code may lead to final blocking of the key storage device, which means that the key storage device would no longer allow any formatting or unformatting.

Changing biometric identifier

To change the biometric identifier stored on the key storage device, please open the key storage device (see Viewing the contents of the key storage device section) and select Tools > Change BIO ID. Check the Enable Biometric ID verification checkbox, select biometric device from the list of devices installed on your computer, click OK and follow the instructions of biometric device software package (Figure 34).
Unblocking the PIN code

To unblock the PIN code for accessing the hardware key, open the hardware key (see *Viewing the contents of the hardware key* section) and go to **Tools > Unblock** menu. The following window will prompt user to enter correct PIN code for unblocking the hardware key (Figure 35).

**Note:** Entering wrong PIN code will permanently block the hardware key, which will then require complete re-formatting (see *Formatting hardware key* section).

Editing the symbolic label

Every hardware key may be assigned a symbolic label, which can be used for different purposes, e.g. for defining the hardware key holder attributes or for identifying and distinguishing between the hardware keys if the user uses more than one key.
To edit the symbolic label, open the hardware key (see Viewing the contents of the hardware key section), right-click on its name and select **Change Label** … command (Figure 36).

The dialog window for editing the symbolic label will appear (Figure 37). The same result can be achieved through **Tools > Change Label** … command of the main window.

![Figure 36](image1)

**Figure 36**
Changing the symbolic label

![Figure 37](image2)

**Figure 37**
Editing symbolic label
Searching the backup copies of the hardware key

Dekart Key Manager enables the user to search the backup copies of the hardware keys using different search criteria. To open the search window, activate the Search tab in the left side of the main window (Figure 38).

![Figure 38 Searching the backup copy](image)

To start a search, define the necessary folder in the Look in field, and set the search criteria – define the desired contents of the backup copy: comments of the copy (Comments), serial number of the hardware key (Serial number) and the symbolic label of the hardware key (Label). These fields are not obligatory and can be used separately or together at the same time. If several fields are selected, the search will be based on all of them. The search will return the results that contain the values of these fields as part of a larger string too. The search results will display in the lower left part of the main window. (Figure 39).
Viewing the contents of the backup copies found is identical to viewing the contents of the hardware keys (see *Viewing the contents of the hardware key* section). To open the backup copy in the main list of the hardware keys (*Documents & Key Readers* tab of the main window), right-click on the selected backup copy and select *Open File* from the context menu (Figure 40).

![Figure 39](image_url)

*Figure 39*

**Search results**
Configuring Dekart Key Manager

Dekart Key Manager enables you to use additional (external) utilities to work with hardware keys, e.g. the utility for formatting the hardware keys.

The configuration settings of Dekart Key Manager are stored in the keyman.ini file. After successful installation of Dekart Key Manager, this file contains default settings defining the normal work of the application. These settings can be optionally changed. This may become necessary in several cases – the new application data is written to the smart card, another external utility is added, the new utility for viewing and editing the hardware keys is used.

Editing the keyman.ini file can be done by using the standard Windows text editors, e.g. using Notepad (Figure 41).
Configuring the names of the applications

The [Aliases] section of the configuration file keyman.ini defines the symbolic names of the application data blocks, i.e. the names of the applications using these data blocks (Figure 41). These names are displayed in the left part of the main window when the hardware key contents is being viewed (see Viewing the contents of the hardware key section). This allows defining the ownership between the application and its data block. The data blocks without the symbolic names will display the application digital identifier. To change digits to names the symbolic name for the given data block should be defined in the [Aliases] section of the configuration file keyman.ini.

Example:

[Aliases]
223=Logon
222=Private Disk
221=Cryptographic Provider
224=Secrets Keeper
Embedding additional components

The [Tools] section of the configuration file keyman.ini is intended for defining the applications, which can be further run from the Tools menu.

Embedding an additional component will require entering complete path to the application including its command line parameters. The following example illustrates the use of command line to embed the additional component:

[Tools]
Format Key = C:\Program Files\Dekart\Key formatting utility\efcard.exe “AKS ifdh 0”

Embedding additional components (plug-ins) for viewing and editing

The [Tools] section of the configuration file keyman.ini is intended for defining additional applications for viewing and editing data blocks in common user mode. Every application may have a separate utility for viewing and editing besides the binary data editor (see Binary editing of Dekart application data section).

The basic installation package of Dekart Key Manager contains utilities for common viewing of most recent Dekart applications. If the utility for viewing the required application is not available in the basic package, request the information from Dekart sales department using sales@dekart.com.

Additional viewing tools are the ActiveX components. Therefore, the additional component should be registered in the operating system: copy the component file into the Dekart Key Manager folder and run Regsvr32.exe filename.ocx command, where the filename.ocx is the component’s name.

The registration can be done only by the administrator of the operating system or by any user with administrator privileges.

Formatting the hardware key

Before using the hardware keys they need to be formatted with a special utility, Dekart Corporate key formatting utility, which can be either separately used or optionally embedded into Dekart Key Manager (see Embedding additional components section).

The main window of Dekart Corporate key formatting utility is shown in Figure 42. This utility is intended for formatting hardware keys for use with Dekart applications. It also allows unformatting the hardware keys which have already been formatted for Dekart applications (if it is allowed by the hardware key).
Dekart Corporate key formatting utility enables user to simultaneously format more than one hardware key (hold down the Ctrl key and define the keys to be formatted using the left mouse button). Before starting formatting or unformatting, the formatting parameters should be defined. To define the formatting parameters, click the Options ... button to view the following window (Figure 43):
The utility can optionally format all memory of the hardware key (*Occupy all free space*), or only a fixed portion of memory (*Occupy*), or even reserve a fixed portion of memory for other purposes (*Reserve*). Some of the hardware keys allow erasing all data from their memory before formatting (*Clear all Key’s data*), but others may require the formatter to clear all data and display a warning message. Some of the hardware keys also require a special password before formatting, namely, the *Issuer Key* (*Use formatting password*).

**Configuring the toolbar of the main window**

*Dekart Key Manager* toolbar in the upper part of the main window is designed for ease of work with the application (Figure 44). Some of the toolbars can be optionally added or removed by using the *View* menu of the main window. The *View > Split* command allows splitting the right and the left panels of the main window.

![Dekart Key Manager toolbar](image)

**Figure 44** *Dekart Key Manager* toolbar

**Safety recommendations for Dekart Key Manager**

To provide better protection of confidential information, please take into account the following recommendations.

*First*. Make sure the backup copies of the hardware keys are stored in encrypted archives or on encrypted disks.

*Second*. Store the backup copies of the hardware keys on external storage devices and make sure these devices are stored in a secure place, e.g. safe.

*Third*. Protect the hardware keys with PIN codes. This will lower the security risk in case the hardware keys are lost or stolen.

*Fourth*. Anytime you leave your workplace, disconnect all connected hardware keys.

**Closing Dekart Key Manager**

To close *Dekart Key Manager* use the standard *Windows* methods or use the *File > Exit* command.

**Registering Dekart Key Manager**

In order to be eligible to software updates and *Dekart* support, the *Dekart Key Manager* should be registered in *Dekart* database.

Please, obtain a registration number at Software Registration (Register) 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 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.

In order to register the application, if this has not been done during the installation procedure, it is necessary to go to the window About Dekart Key Manager, and enter the registration information in the proper fields.

![Figure 45](image)

*About Dekart Key Manager* window with the registration form

**Note:** The user shall present the registration number of the products every time he contacts Dekart support team or updates Dekart Key Manager.

**Dekart Key Manager technical support**

If any contingencies or problems occur during Dekart Key Manager operation and the user does not know how to handle the situation, he is welcome to contact Dekart support team at support@dekart.com provided that he presents his Name and Registration number. To do this, go to the About Dekart Key Manager (Figure 45) window, click the support@dekart.com link. This will open the email composer window with all information about the software versions (Figure 46). Describe your problem and send us your request.
Figure 46
Chapter 5. Troubleshooting

This chapter contains:

- **Diagnostic Messages List.** These messages result from incorrect user actions or **Dekart Key Manager** hardware or software errors during the software operation. For convenience, messages are given alphabetically in the *Message* column of the *Diagnostic Messages* table.

- **Message Explanation List.** These descriptions are given in the *Explanation* column of the *Diagnostic Messages* table.

- **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.

### Possible problems

If any contingencies occur during **Dekart Key Manager** installation and hardware connection and the users do not know how to handle the situation, they can contact the Dekart support team at support@dekart.com provided that they present their Name and Registration number.

### Diagnostic messages

If any contingencies occur during **Dekart Key Manager** installation and hardware connection and the user does not know how to handle the situation, the *Possible Problems* table can be used as follows:

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

The diagnostic messages table is listed below.
## Table 1. Diagnostic messages table

<table>
<thead>
<tr>
<th>##</th>
<th>Message</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Data block could not be erased. You should delete data block instead of erasing its contents.</td>
<td>(Binary editor of the data block). Compete deletion of data block is not allowed. The data block size may not be zero.</td>
<td>Delete the data block partially. To completely change data block contents use the following command set: select all, paste. Copy all new data to clipboard before applying these commands.</td>
</tr>
<tr>
<td>02</td>
<td>Not enough free space for new data block.</td>
<td>There is not enough free space on the hardware key for the new data block.</td>
<td>You may not write new data block onto the full hardware key. If there is a free portion of memory on the hardware key, try to decrease the size of the data block.</td>
</tr>
<tr>
<td>03</td>
<td>Keyman.ini not found...</td>
<td>Configuration file Keyman.ini was not found in the source folder of Key Manager.</td>
<td>Re-install the application</td>
</tr>
<tr>
<td>04</td>
<td># attempts left ...</td>
<td>The PIN code request dialog displays the number of remaining PIN code entry attempts.</td>
<td>Be careful with wrong PIN code entries, otherwise the hardware key will block after # of wrong entries.</td>
</tr>
<tr>
<td>05</td>
<td>No files were found.</td>
<td>(Search tab) File search did not produce any results.</td>
<td>Try searching again or change search criteria.</td>
</tr>
<tr>
<td>06</td>
<td>You are trying to paste data (# bytes) to this data block. The resulting size has exceeded the maximum allowed size (# bytes) for this data block. Operation aborted.</td>
<td>(Binary editor of the data block). Attempting to paste from clipboard # bytes of data. Not enough space to perform this operation.</td>
<td>Try to paste smaller size data. The data block allowed sizes are specified in the &quot;Size \ Available&quot; field.</td>
</tr>
<tr>
<td>07</td>
<td>The Document could not be loaded. Too many opened files.</td>
<td>The document can not be opened. Too many documents opened at the same time.</td>
<td>Re-start Key Manager and try to open the document again.</td>
</tr>
<tr>
<td>08</td>
<td>An error occurred while loading Viewer Plug-in (#) for #.</td>
<td>Error loading Viewer Plug-in (#) for # data.</td>
<td>The Viewer Plug-in for this data block is not available or has been incorrectly installed. Re-install the application.</td>
</tr>
<tr>
<td>09</td>
<td>An error occurred while executing: #</td>
<td>Error calling external utility</td>
<td>Check the name and path to the external utility in keyman.ini file.</td>
</tr>
<tr>
<td>10</td>
<td>KeyMan.ini does not contain [Tools] section or KeyMan.ini not found</td>
<td>File KeyMan.ini not found or the [Tool] section is unavailable.</td>
<td>The KeyMan.ini file, section [Tool] contains data about external utilities. Re-install the application or add this section.</td>
</tr>
<tr>
<td>11</td>
<td>Unknown error with the Key!</td>
<td>Hardware key processing error.</td>
<td>Repeat the operation.</td>
</tr>
<tr>
<td>12</td>
<td>The Key is blocked!</td>
<td>(Right-hand information panel in hardware key status bar). Hardware key is blocked.</td>
<td>Unblock the hardware key by entering correct PIN code. Conventionally, the hardware key accepts only three PIN code entry attempts.</td>
</tr>
<tr>
<td>13</td>
<td>The Key is finally blocked! It should be reformatted to reuse.</td>
<td>(Right-hand information panel in hardware key status bar). Hardware key is permanently blocked. Reformatting the card is required.</td>
<td>To be able to use the hardware key, it has to be reformatted.</td>
</tr>
<tr>
<td>14</td>
<td>The Key you connected has not been formatted!</td>
<td>(Right-hand information panel in hardware key status bar). Hardware key is not formatted.</td>
<td>Before using the hardware key with Dekart applications the...</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td>Error Message</td>
<td>Solution</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>15</td>
<td>Unidentified Key or reader error!</td>
<td>(Right-hand information panel in hardware key status bar). Unknown hardware key type or smart card reader error.</td>
<td>Disconnect and then reconnect the hardware key and repeat the operation.</td>
</tr>
<tr>
<td>16</td>
<td>An error occurred while reading data from the Key!</td>
<td>Error reading data from the hardware key.</td>
<td>Restart the application and repeat the operation.</td>
</tr>
<tr>
<td>17</td>
<td>An error occurred while deleting # from the Key!</td>
<td>Error deleting data from the hardware key.</td>
<td>Restart the application and repeat the operation.</td>
</tr>
<tr>
<td>18</td>
<td>An error occurred while writing # to the Key!</td>
<td>Error writing data to the hardware key.</td>
<td>Restart the application and repeat the operation.</td>
</tr>
<tr>
<td>19</td>
<td>An error occurred while loading smartkey.dll</td>
<td>Error loading smartkey.dll library</td>
<td>smartkey.dll library has not been installed or PC/SC subsystem does not work on this computer.</td>
</tr>
<tr>
<td>20</td>
<td>Please enter PIN for the Key</td>
<td>(Right-hand information panel in hardware key status bar). Enter correct PIN code.</td>
<td>The user has cancelled entering PIN code while connecting the hardware key. Disconnect and then connect again the hardware key, enter PIN code.</td>
</tr>
<tr>
<td>21</td>
<td>An error occurred while #</td>
<td>Error processing the hardware key. Error description: #</td>
<td>Check if there is enough free space on hardware key to perform this operation. Repeat the operation.</td>
</tr>
<tr>
<td>22</td>
<td>Not enough free space on the Key!</td>
<td>Not enough free space in the hardware key memory.</td>
<td>The operation requires a free portion of memory on the hardware key.</td>
</tr>
<tr>
<td>23</td>
<td>An error occurred while changing PIN</td>
<td>Error changing PIN code.</td>
<td>Restart the application and repeat the operation.</td>
</tr>
</tbody>
</table>
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Programming Interface (API)</strong></td>
<td>This is a software interface used for interaction between the OS and an application.</td>
</tr>
<tr>
<td><strong>Basic Input/Output System (BIOS)</strong></td>
<td>The PC Basic Input/Output System is an OS-independent software designed for hardware operation support. This is 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.</td>
</tr>
<tr>
<td><strong>International Organization for Standardization (ISO)</strong></td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>This is a control process checking the authenticity of the users identity, i.e. this process checks whether the user is the person they claim to be.</td>
</tr>
<tr>
<td><strong>Biometric Authentication</strong></td>
<td>This is the user authentication based on examining specific physical traits of the user by means of special biometric equipment. Biometric authentication can be based on examining fingerprints, iris, voice, and other specific traits of the user's body.</td>
</tr>
<tr>
<td><strong>Two-Factor Authentication</strong></td>
<td>This is a process controlling the authenticity of the users identity on the basis of the two following factors: Something You Know — for example, the user name and password. Something You Have – for example, the eToken device.</td>
</tr>
<tr>
<td><strong>Driver</strong></td>
<td>This is software designed to control data input/output and interface the applications/OS and the device connected to the PC.</td>
</tr>
<tr>
<td><strong>Identification</strong></td>
<td>This is a control process using a unique identifier to determine whether the specific user is known to the system.</td>
</tr>
<tr>
<td><strong>One-Factor or Standard Authentication</strong></td>
<td>This is 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.</td>
</tr>
<tr>
<td><strong>Registration</strong></td>
<td>The process resulting in user authentication using his login and password pair. If the registration is successful, the user is granted access to the OS within the limit of his privileges.</td>
</tr>
<tr>
<td><strong>Hardware key</strong></td>
<td>A smart card or USB token where personal information is stored. The hardware key can be PIN code protected, or can work without PIN.</td>
</tr>
<tr>
<td><strong>Encryption key</strong></td>
<td>Specially built numerical sequence used to transform the source information into the encrypted data using a special algorithm.</td>
</tr>
<tr>
<td><strong>PIN (Personal Identification Number)</strong></td>
<td>Personal identification number that is used to access information stored on the hardware key. The PIN code length can be from 4 to 8</td>
</tr>
<tr>
<td>Identification Number</td>
<td>characters, and should always be memorized, or be in the possession of only the hardware key holder.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------------------</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer.</td>
</tr>
<tr>
<td>SW</td>
<td>Software</td>
</tr>
</tbody>
</table>