DEKART Key Manager
version 1.06

Operating Guide

2004

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

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 of 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.*

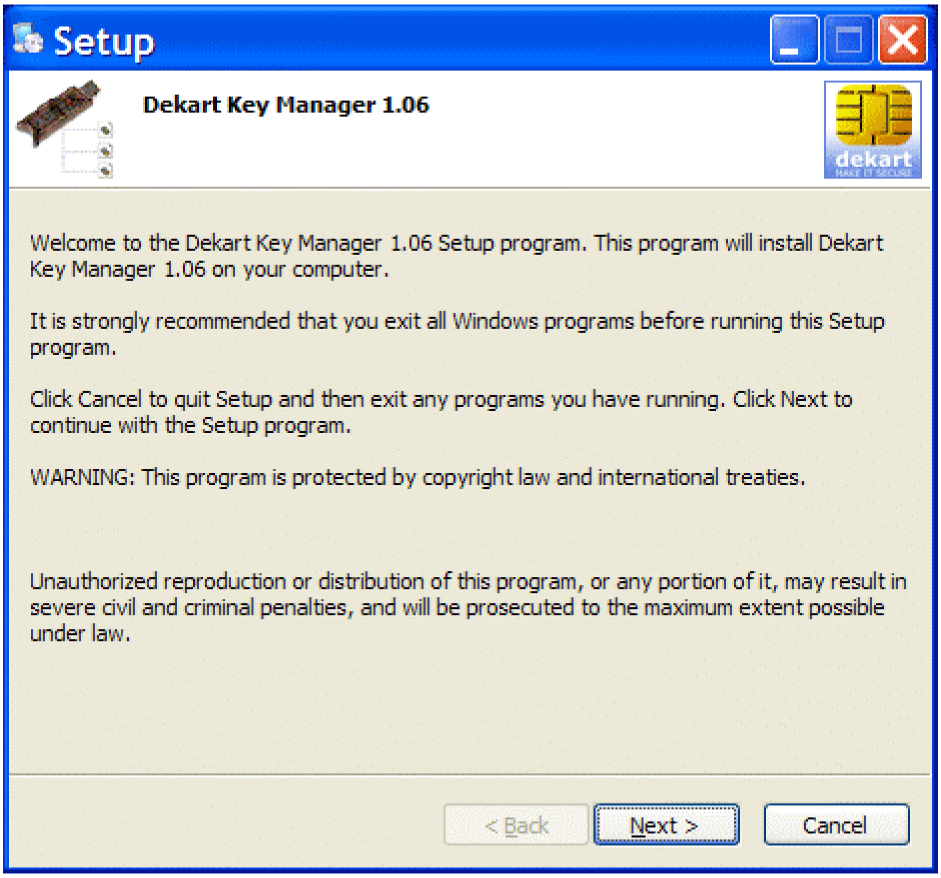
Note: To install the product components under Windows operating systems designed for corporate use — Windows NT, Windows 2000, Windows XP — it is necessary to log into the system as administrator. In Windows operating systems designed mainly for private use — Windows 95/98/ME, Windows XP Home — every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



Dekart Key Manager 1.06

Welcome to the Dekart Key Manager 1.06 Setup program. This program will install Dekart Key Manager 1.06 on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

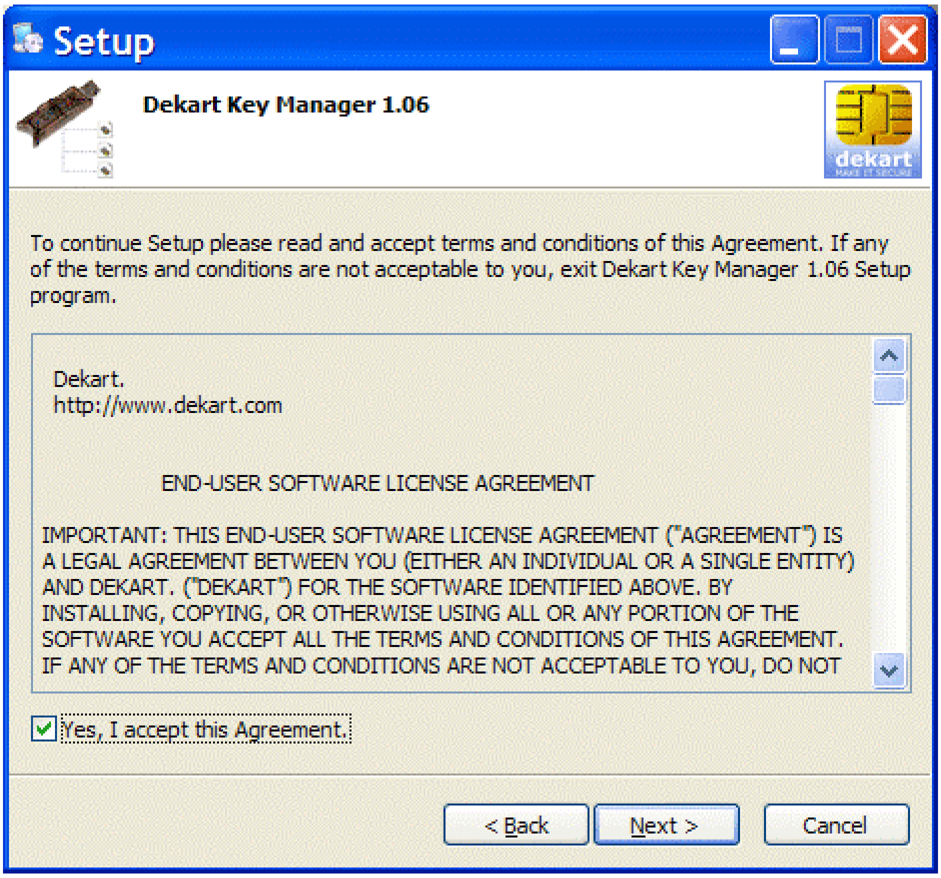
Click Cancel to quit Setup and then exit any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Figure 1
Dekart Key Manager welcome screen

3. Click *Next*. The ***End-User Software License Agreement*** will appear, as shown in Figure 2.



Setup

Dekart Key Manager 1.06

To continue Setup please read and accept terms and conditions of this Agreement. If any of the terms and conditions are not acceptable to you, exit Dekart Key Manager 1.06 Setup program.

Dekart.
http://www.dekart.com

END-USER SOFTWARE LICENSE AGREEMENT

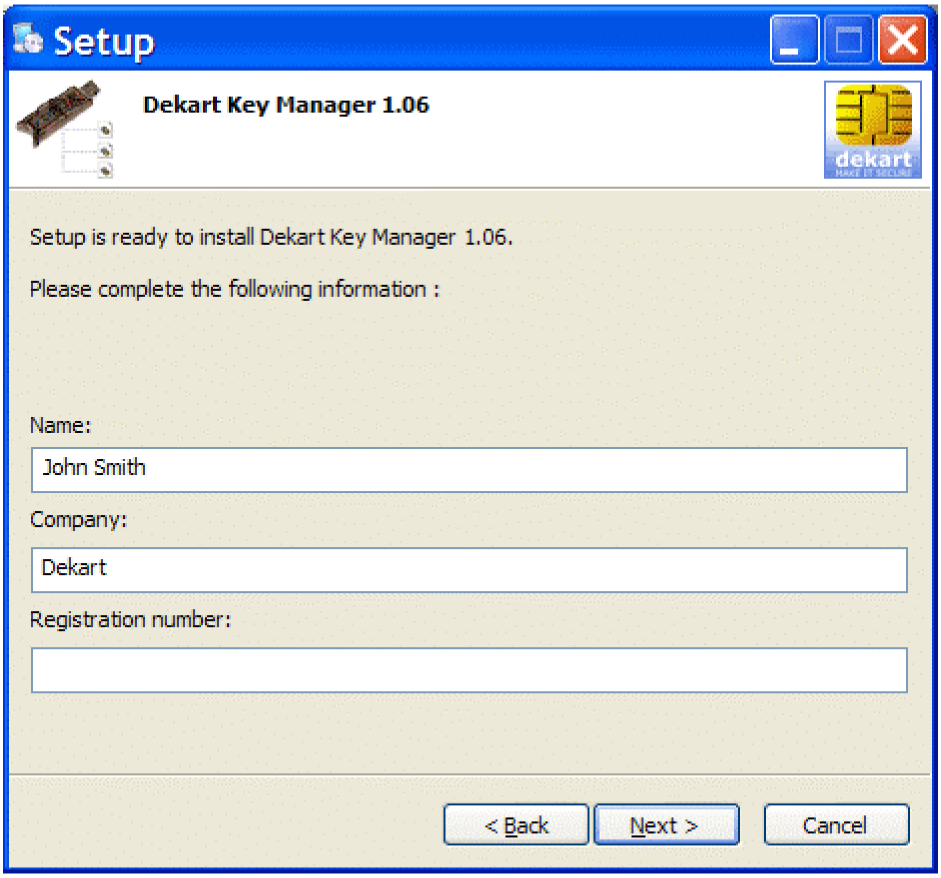
IMPORTANT: THIS END-USER SOFTWARE LICENSE AGREEMENT ("AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AND DEKART. ("DEKART") FOR THE SOFTWARE IDENTIFIED ABOVE. BY INSTALLING, COPYING, OR OTHERWISE USING ALL OR ANY PORTION OF THE SOFTWARE YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF ANY OF THE TERMS AND CONDITIONS ARE NOT ACCEPTABLE TO YOU, DO NOT

☑ Yes, I accept this Agreement.

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.



Setup is ready to install Dekart Key Manager 1.06.

Please complete the following information :

Name:

John Smith

Company:

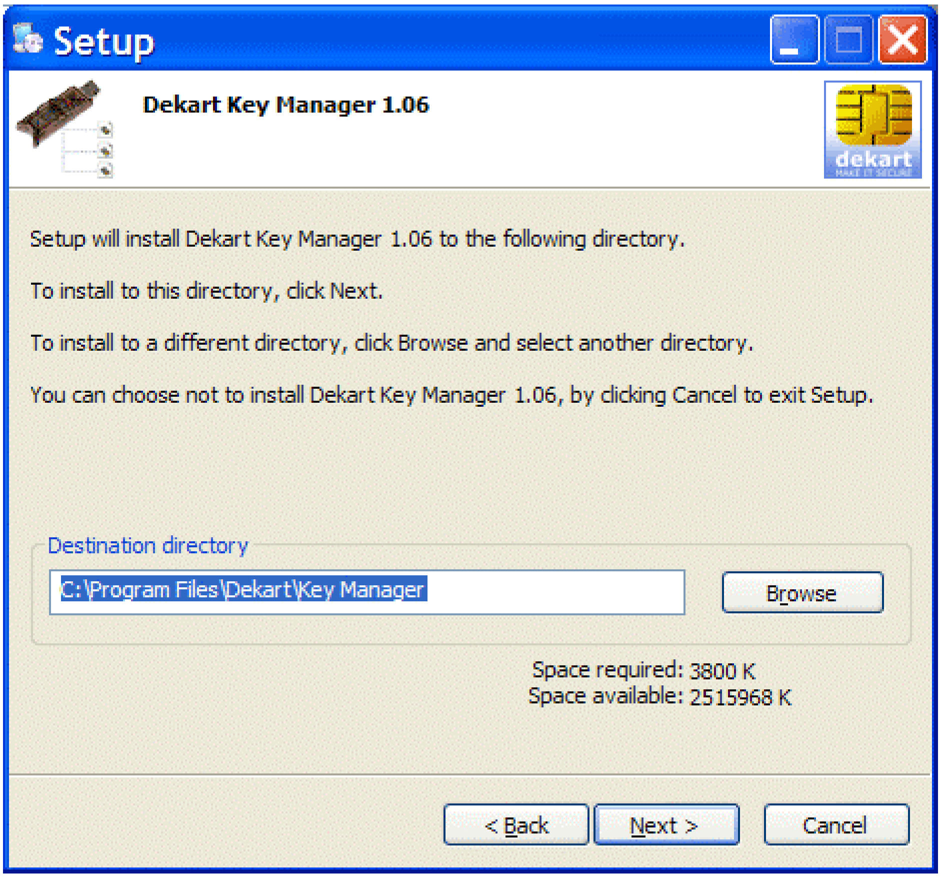
Dekart

Registration number:

Figure 3
Dekart Key Manager Registration window

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.



Setup will install Dekart Key Manager 1.06 to the following directory.

To install to this directory, click Next.

To install to a different directory, click Browse and select another directory.

You can choose not to install Dekart Key Manager 1.06, by clicking Cancel to exit Setup.

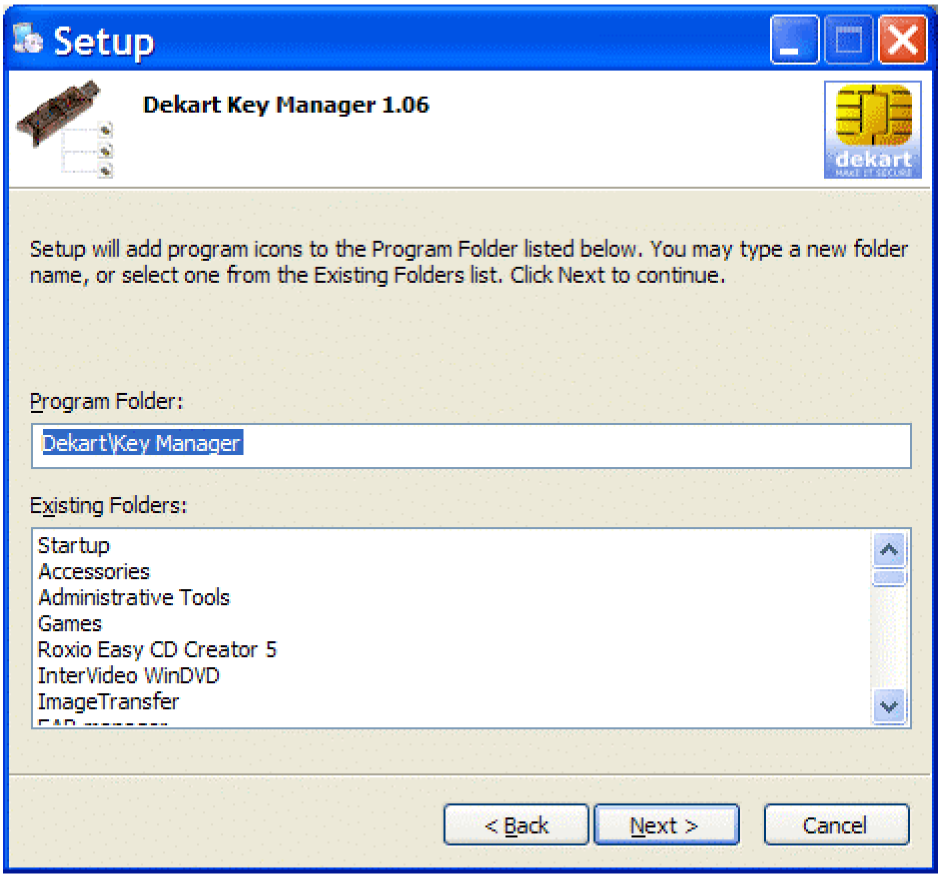
Destination directory

C:\Program Files\Dekart\Key Manager

Space required: 3800 K
Space available: 2515968 K

Figure 4
Dekart Key Manager destination location

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.



Setup

Dekart Key Manager 1.06

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the Existing Folders list. Click Next to continue.

Program Folder:

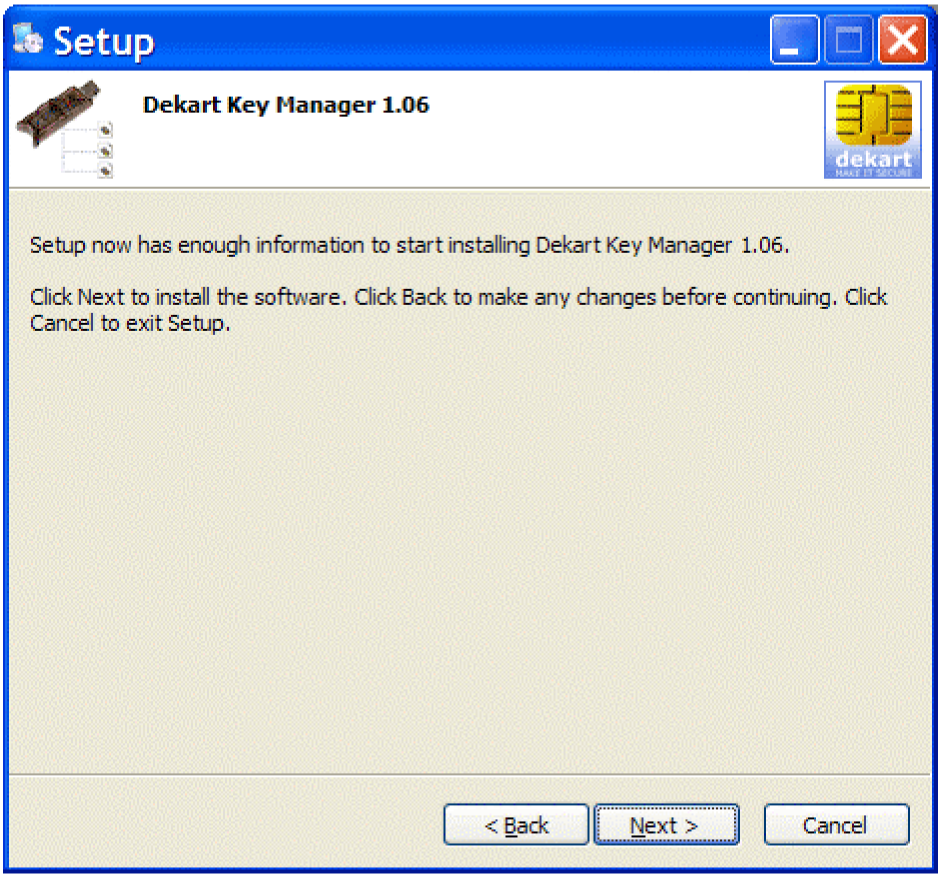
Dekart\Key Manager

Existing Folders:

Startup
Accessories
Administrative Tools
Games
Roxio Easy CD Creator 5
InterVideo WinDVD
ImageTransfer

Figure 5
Dekart Key Manager folder

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.

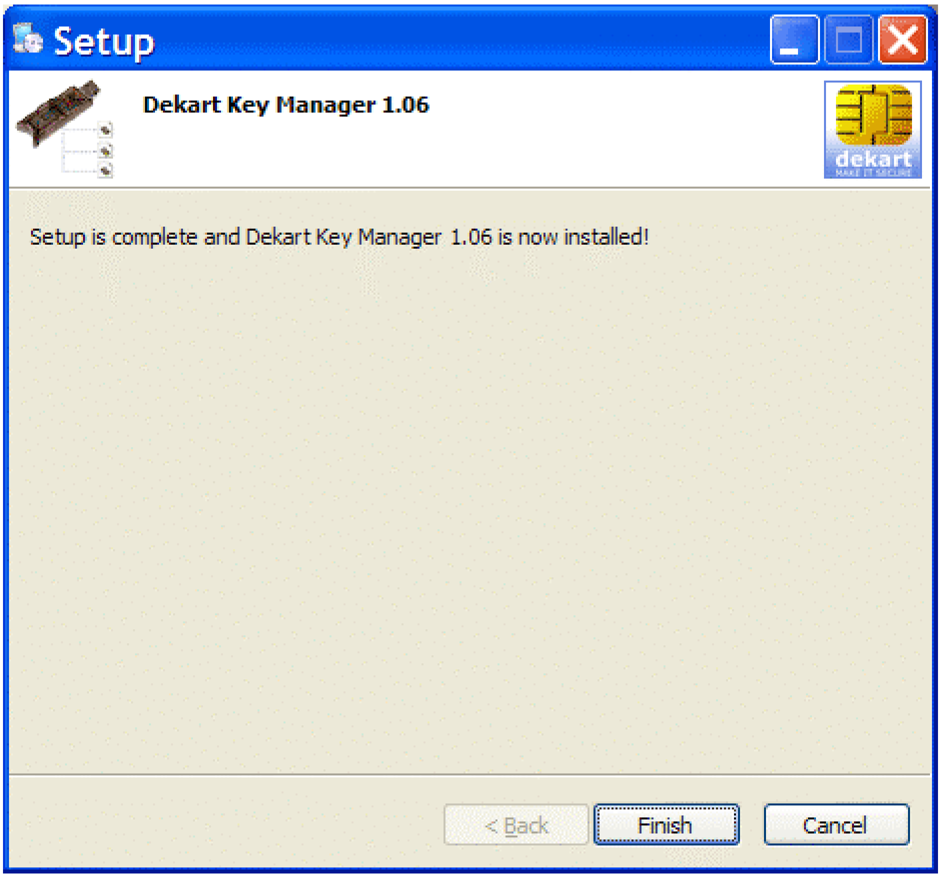


Setup now has enough information to start installing Dekart Key Manager 1.06.

Click Next to install the software. Click Back to make any changes before continuing. Click Cancel to exit Setup.

Figure 6
Ready to Install Dialog

8. Click ***Next*** to start copying **Dekart Key Manager** files.
9. Wait until the installation completion window appears, as shown in Figure 7.



Setup is complete and Dekart Key Manager 1.06 is now installed!

Figure 7
Setup complete

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.

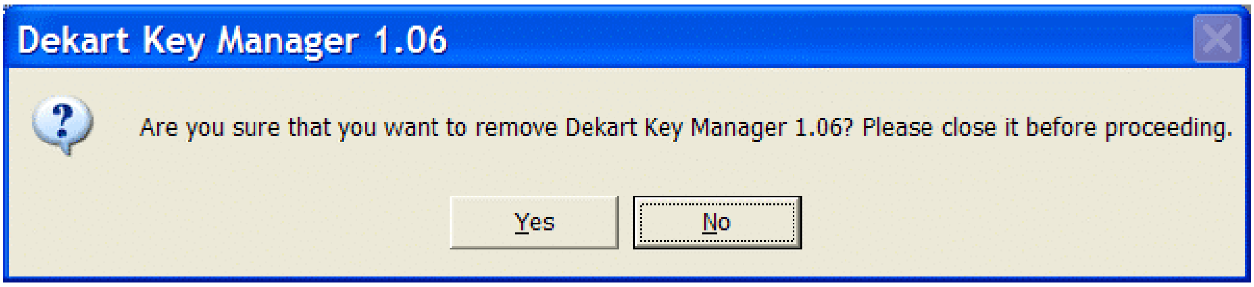
To acquire a newer version of the product, please contact **Dekart** at sales@dekart.com. The corresponding software can be downloaded from http://www.dekart.com or specially ordered.

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.

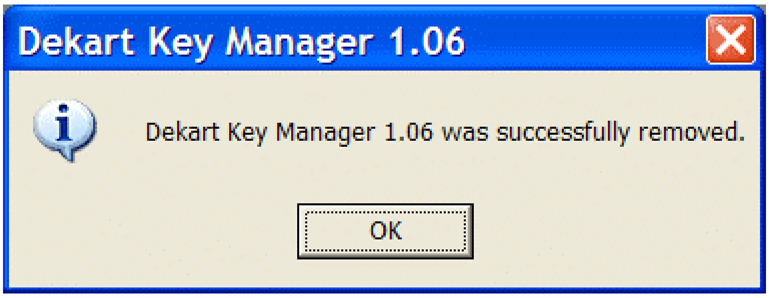


Are you sure that you want to remove Dekart Key Manager 1.06? Please close it before proceeding.

Figure 8
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.



Dekart Key Manager 1.06

Dekart Key Manager 1.06 was successfully removed.

Figure 9
Remove complete

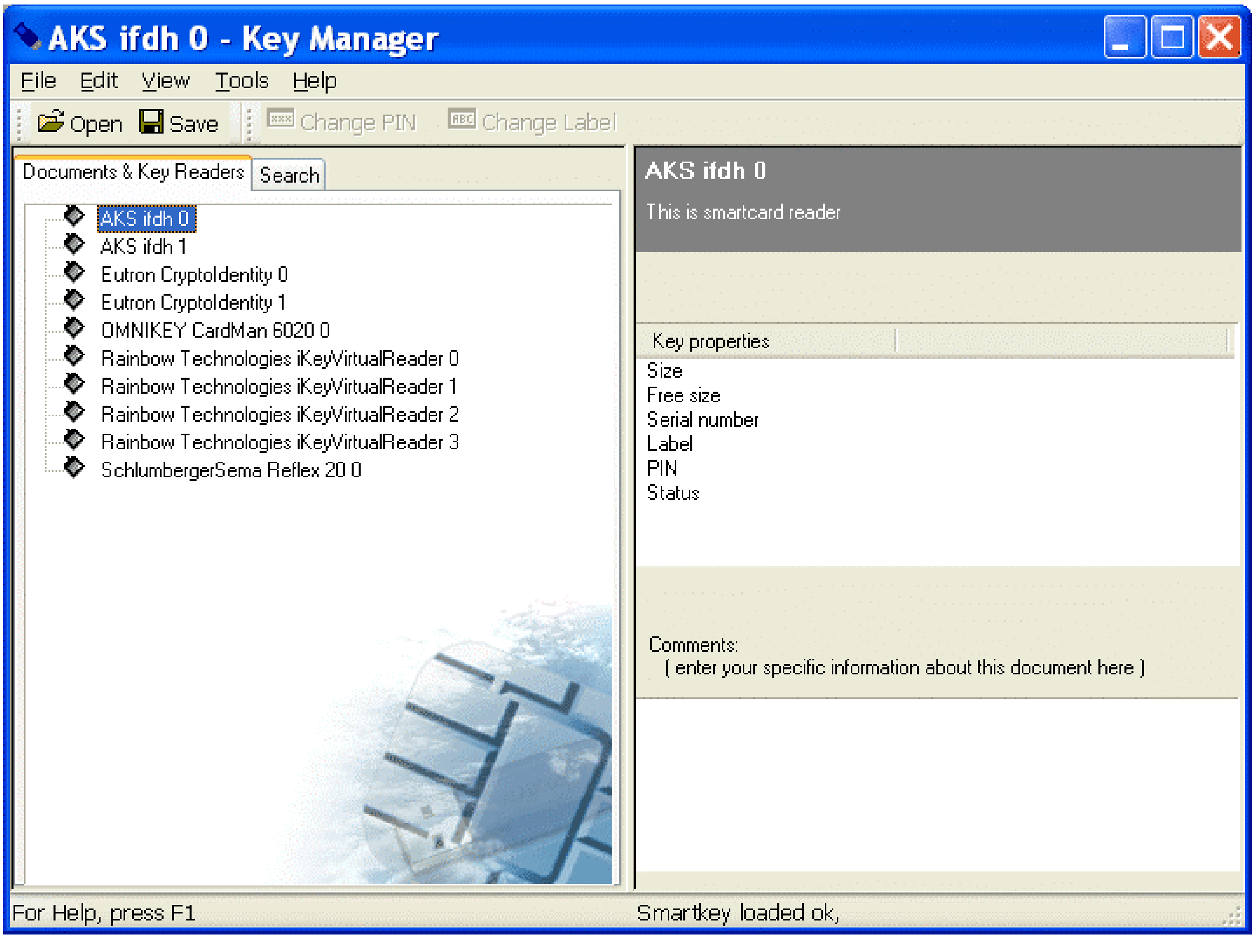
5. Click ***OK*** to complete the process.

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.


AKS ifdh 0 - Key Manager
File Edit View Tools Help
Open Save Change PIN Change Label
Documents & Key Readers
Search
AKS ifdh 0
AKS ifdh 1
Eutron CryptoIdentity 0
Eutron CryptoIdentity 1
OMNIKEY CardMan 6020 0
Rainbow Technologies iKeyVirtualReader 0
Rainbow Technologies iKeyVirtualReader 1
Rainbow Technologies iKeyVirtualReader 2
Rainbow Technologies iKeyVirtualReader 3
SchlumbergerSema Reflex 20 0
AKS ifdh 0
Key properties
Size
Free size
Serial number
Label
PIN
Status

This is smartcard reader

Comments:
[enter your specific information about this document here]

For Help, press F1

Smartkey loaded ok,

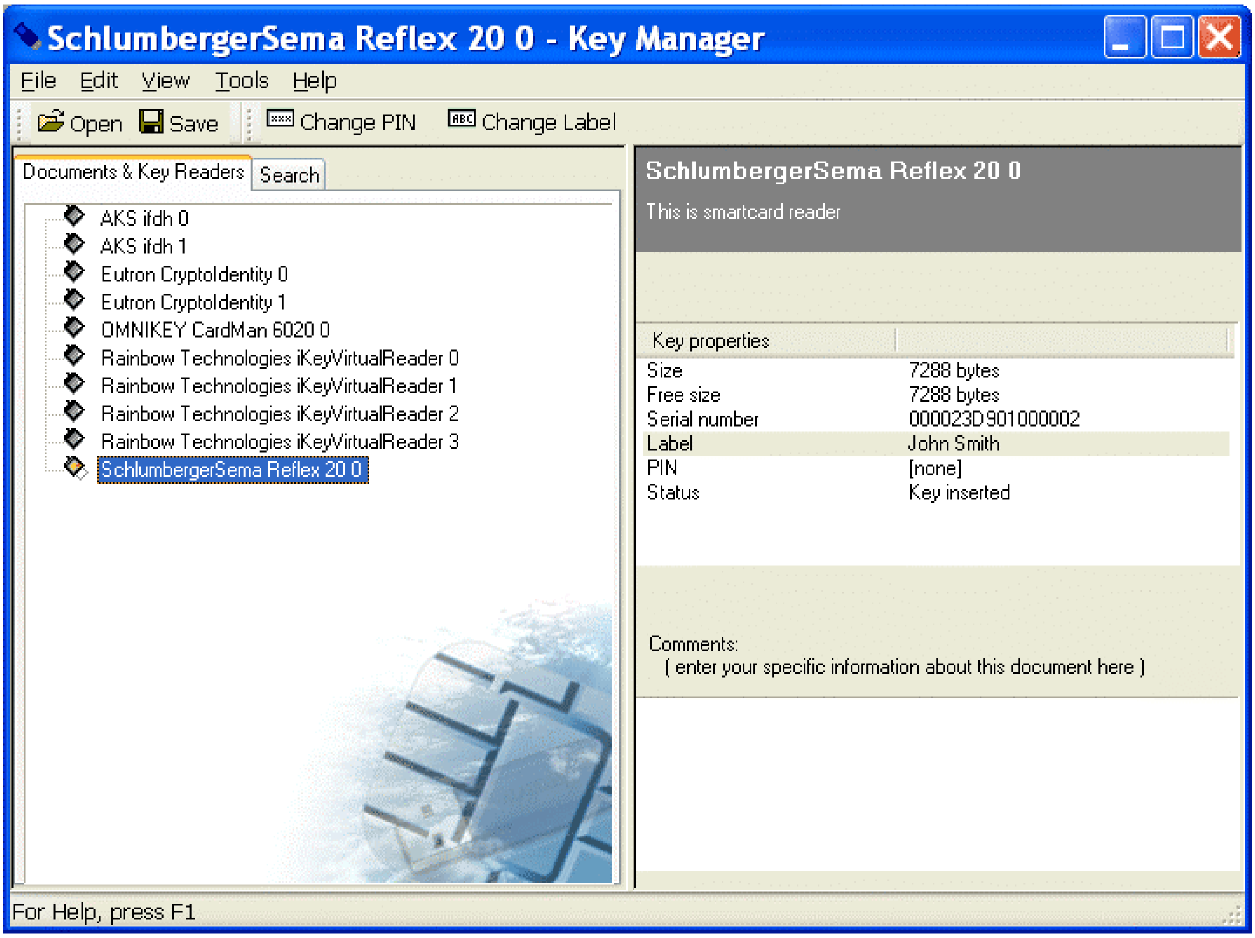
Figure 10
Main window of **Dekart Key Manager**

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.


SchlumbergerSema Reflex 20 0 - Key Manager
File Edit View Tools Help
Open
Save
Change PIN
Change Label
Documents & Key Readers
Search
AKS ifdh 0
AKS ifdh 1
Eutron CryptoIdentity 0
Eutron CryptoIdentity 1
OMNIKEY CardMan 6020 0
Rainbow Technologies iKeyVirtualReader 0
Rainbow Technologies iKeyVirtualReader 1
Rainbow Technologies iKeyVirtualReader 2
Rainbow Technologies iKeyVirtualReader 3
SchlumbergerSema Reflex 20 0

SchlumbergerSema Reflex 20 0

This is smartcard reader

Key properties	
Size	7288 bytes
Free size	7288 bytes
Serial number	000023D901000002
Label	John Smith
PIN	[none]
Status	Key inserted

Comments:
(enter your specific information about this document here)

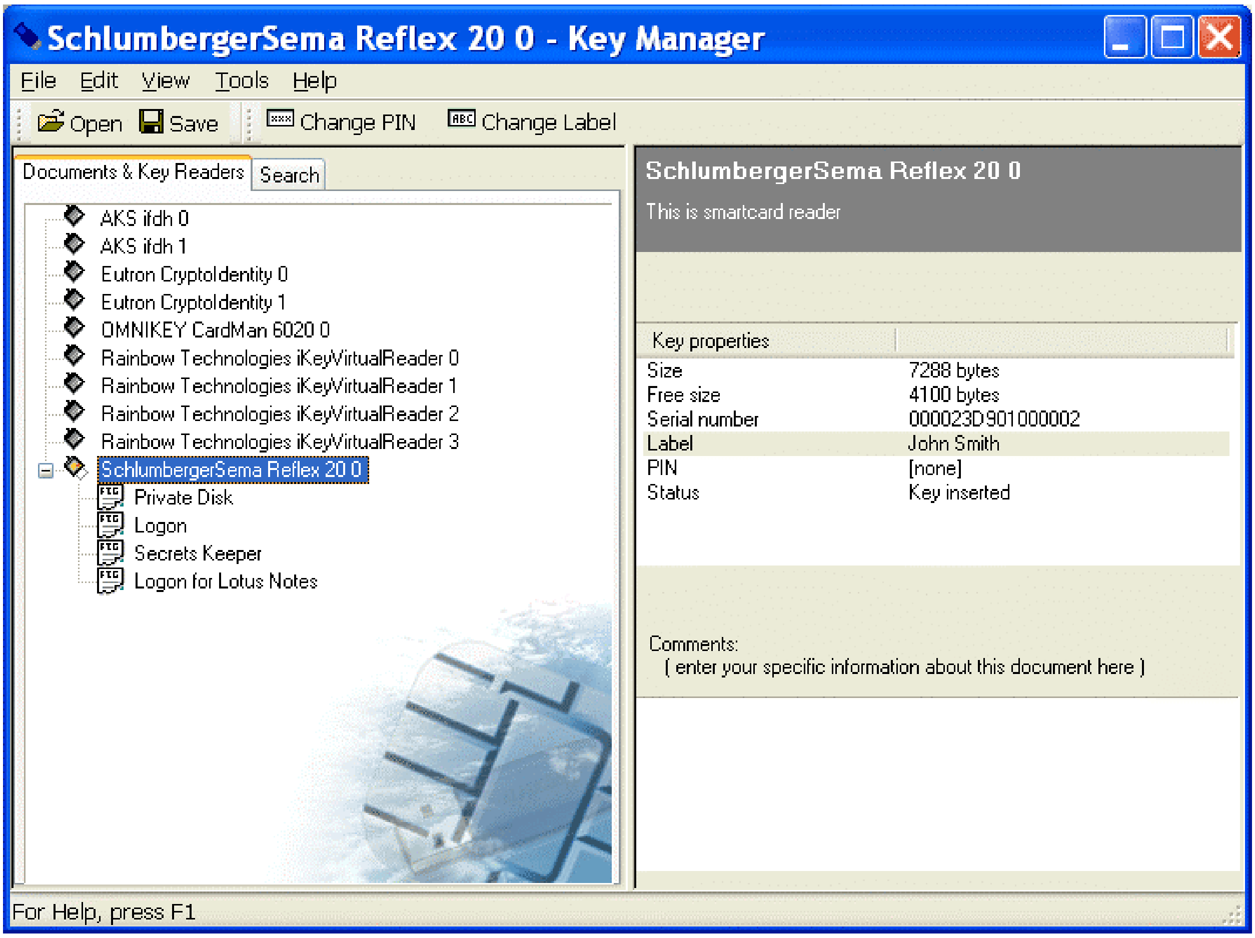
For Help, press F1

Figure 11
Empty 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).


SchlumbergerSema Reflex 20 0 - Key Manager
File Edit View Tools Help
Open Save Change PIN Change Label
Documents & Key Readers
Search
For Help, press F1

- AKS ifdh 0
- AKS ifdh 1
- Eutron CryptoIdentity 0
- Eutron CryptoIdentity 1
- OMNIKEY CardMan 6020 0
- Rainbow Technologies iKeyVirtualReader 0
- Rainbow Technologies iKeyVirtualReader 1
- Rainbow Technologies iKeyVirtualReader 2
- Rainbow Technologies iKeyVirtualReader 3
- SchlumbergerSema Reflex 20 0
  - Private Disk
  - Logon
  - Secrets Keeper
  - Logon for Lotus Notes

SchlumbergerSema Reflex 20 0

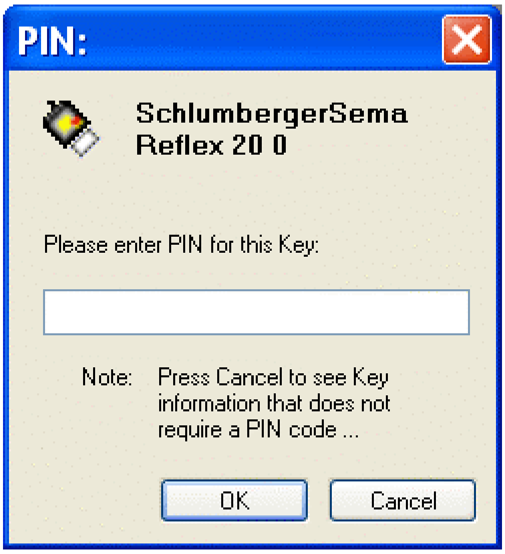
This is smartcard reader

Key properties	
Size	7288 bytes
Free size	4100 bytes
Serial number	000023D901000002
Label	John Smith
PIN	[none]
Status	Key inserted

Comments:
(enter your specific information about this document here)

Figure 12
Hardware key with application data

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).



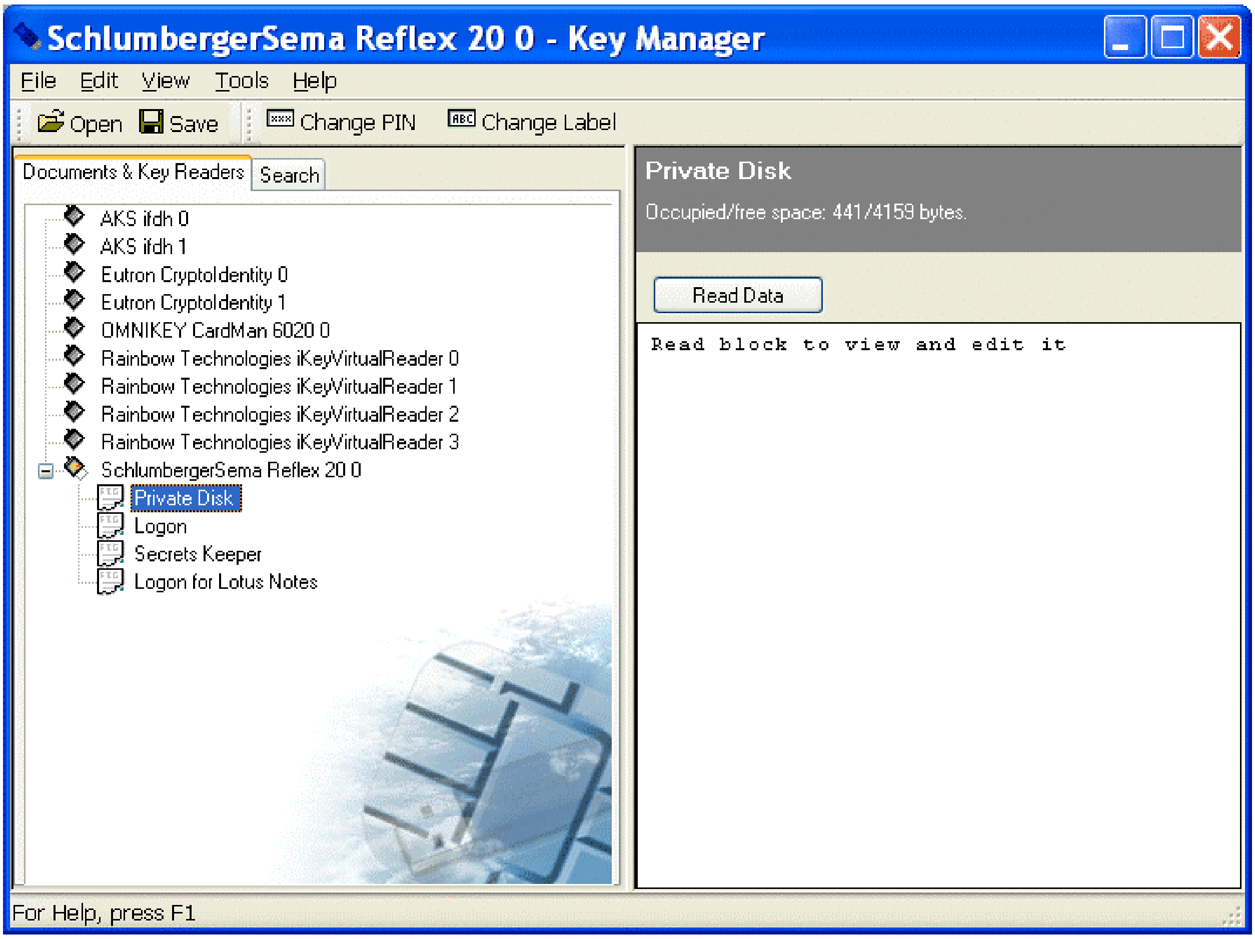
SchlumbergerSema Reflex 20 0

Please enter PIN for this Key:

Note: Press Cancel to see Key information that does not require a PIN code ...

Figure 13
Entering PIN code

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).


SchlumbergerSema Reflex 20 0 - Key Manager
File Edit View Tools Help
Open Save Change PIN Change Label
Documents & Key Readers
Search
AKS ifdh 0
AKS ifdh 1
Eutron CryptoIdentity 0
Eutron CryptoIdentity 1
OMNIKEY CardMan 6020 0
Rainbow Technologies iKeyVirtualReader 0
Rainbow Technologies iKeyVirtualReader 1
Rainbow Technologies iKeyVirtualReader 2
Rainbow Technologies iKeyVirtualReader 3
SchlumbergerSema Reflex 20 0
Private Disk
Logon
Secrets Keeper
Logon for Lotus Notes
Read Data
For Help, press F1

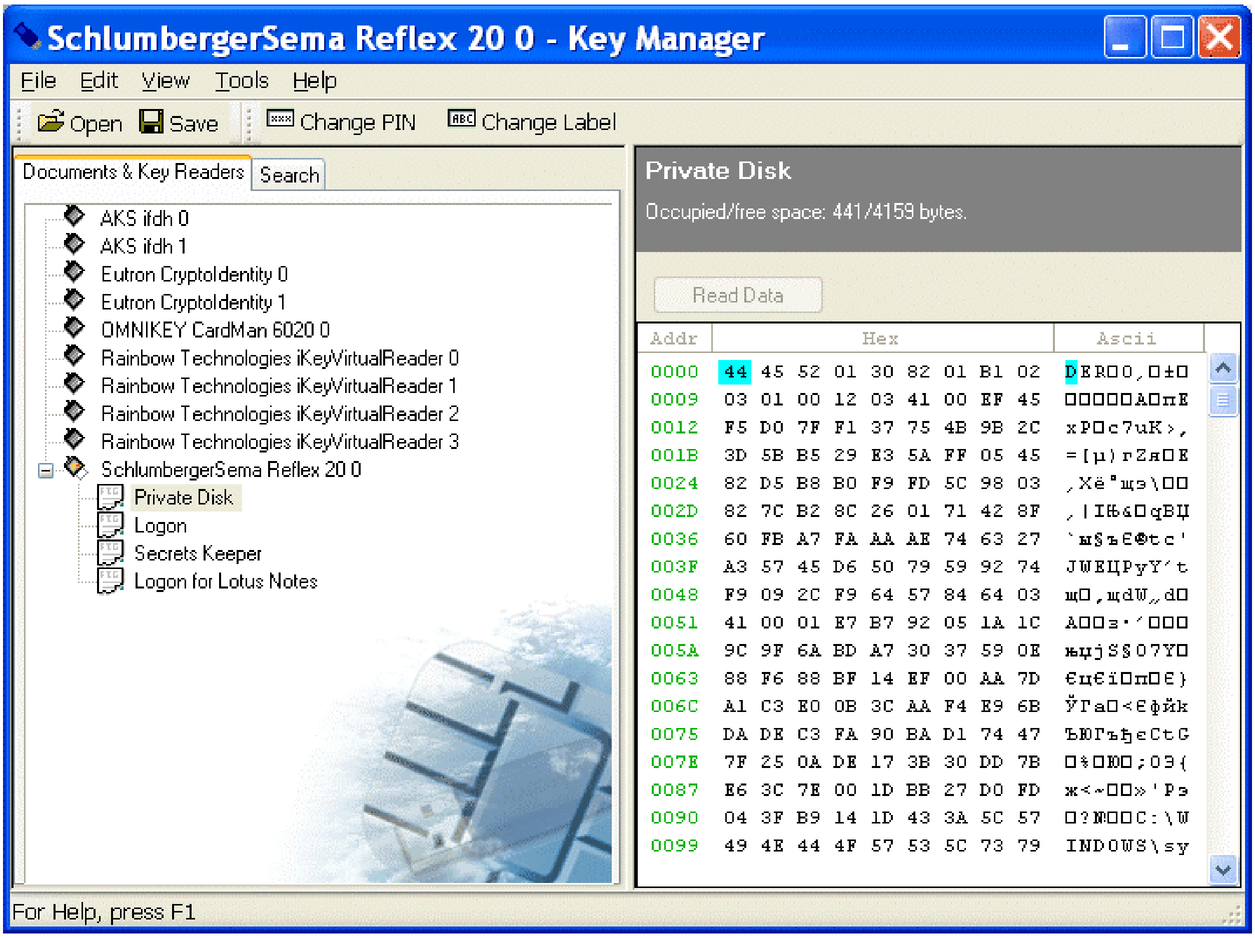
Private Disk

Occupied/free space: 441/4159 bytes.

```
Read block to view and edit it
```

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).


SchlumbergerSema Reflex 20 0 - Key Manager
File Edit View Tools Help
Open Save Change PIN Change Label
Documents & Key Readers
Search
AKS ifdh 0
AKS ifdh 1
Eutron CryptoIdentity 0
Eutron CryptoIdentity 1
OMNIKEY CardMan 6020 0
Rainbow Technologies iKeyVirtualReader 0
Rainbow Technologies iKeyVirtualReader 1
Rainbow Technologies iKeyVirtualReader 2
Rainbow Technologies iKeyVirtualReader 3
SchlumbergerSema Reflex 20 0
Private Disk
Logon
Secrets Keeper
Logon for Lotus Notes
Private Disk
Read Data
For Help, press F1

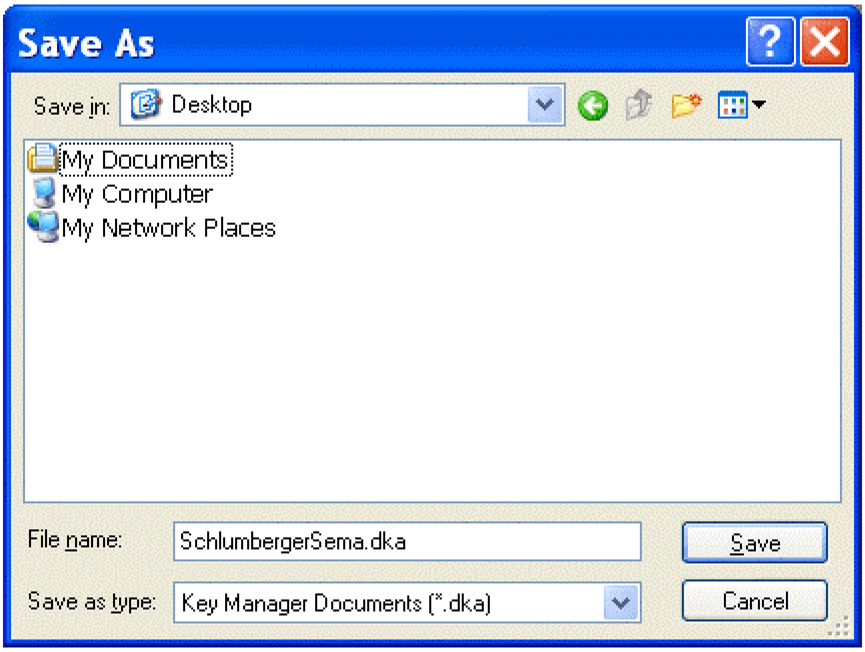
Occupied/free space: 441/4159 bytes.

```
Addr            Hex                    Ascii
0000  44 45 52 01 30 82 01 B1 02  DER□0‚□±□
0009  03 01 00 12 03 41 00 EF 45  □□□□□A□пE
0012  F5 D0 7F F1 37 75 4B 9B 2C  хР□с7uK›,
001B  3D 5B B5 29 E3 5A FF 05 45  =[µ)гZя□E
0024  82 D5 B8 B0 F9 FD 5C 98 03  ‚Хё°щэ\□□
002D  82 7C B2 8C 26 01 71 42 8F  ‚|ІЊ&□qBЏ
0036  60 FB A7 FA AA AE 74 63 27  `ы§ъЄ®tc'
003F  A3 57 45 D6 50 79 59 92 74  ЈWEЦPyY’t
0048  F9 09 2C F9 64 57 84 64 03  щ□,щdW„d□
0051  41 00 01 E7 B7 92 05 1A 1C  A□□з·’□□□
005A  9C 9F 6A BD A7 30 37 59 0E  њџjѕ§07Y□
0063  88 F6 88 BF 14 EF 00 AA 7D  €ц€ї□п□Є}
006C  A1 C3 E0 0B 3C AA F4 E9 6B  ЎГа□<Єфйk
0075  DA DE C3 FA 90 BA D1 74 47  ЪЮГъђєСtG
007E  7F 25 0A DE 17 3B 30 DD 7B  □%□Ю□;0Э{
0087  E6 3C 7E 00 1D BB 27 D0 FD  ж<~□□»'Рэ
0090  04 3F B9 14 1D 43 3A 5C 57  □?№□□C:\W
0099  49 4E 44 4F 57 53 5C 73 79  INDOWS\sy
```

Figure 15
Displaying application data

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).



Save in: Desktop

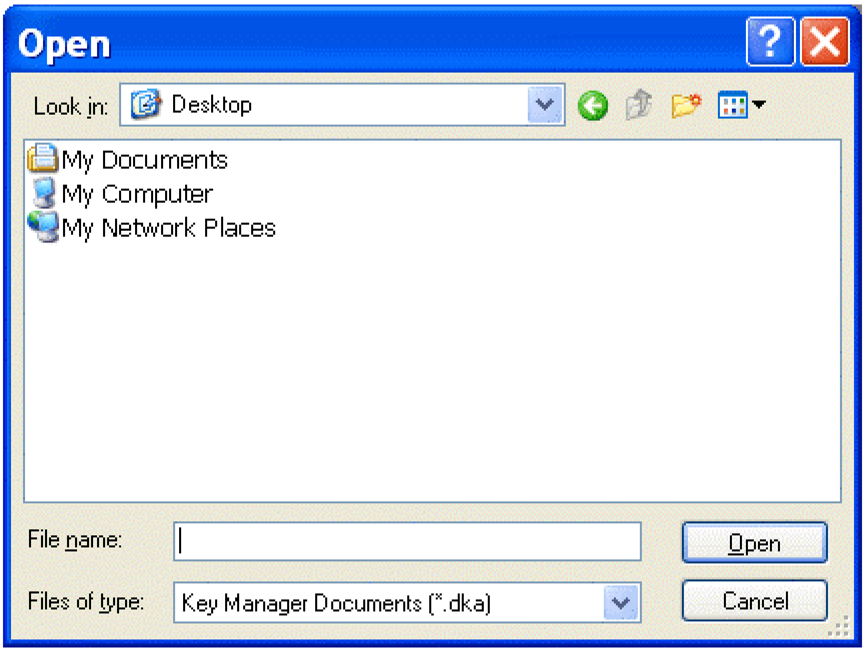
File name: SchlumbergerSema.dka

Save as type: Key Manager Documents (*.dka)

Figure 16
Specifying the location for backup copy

Opening and viewing the backup copy

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



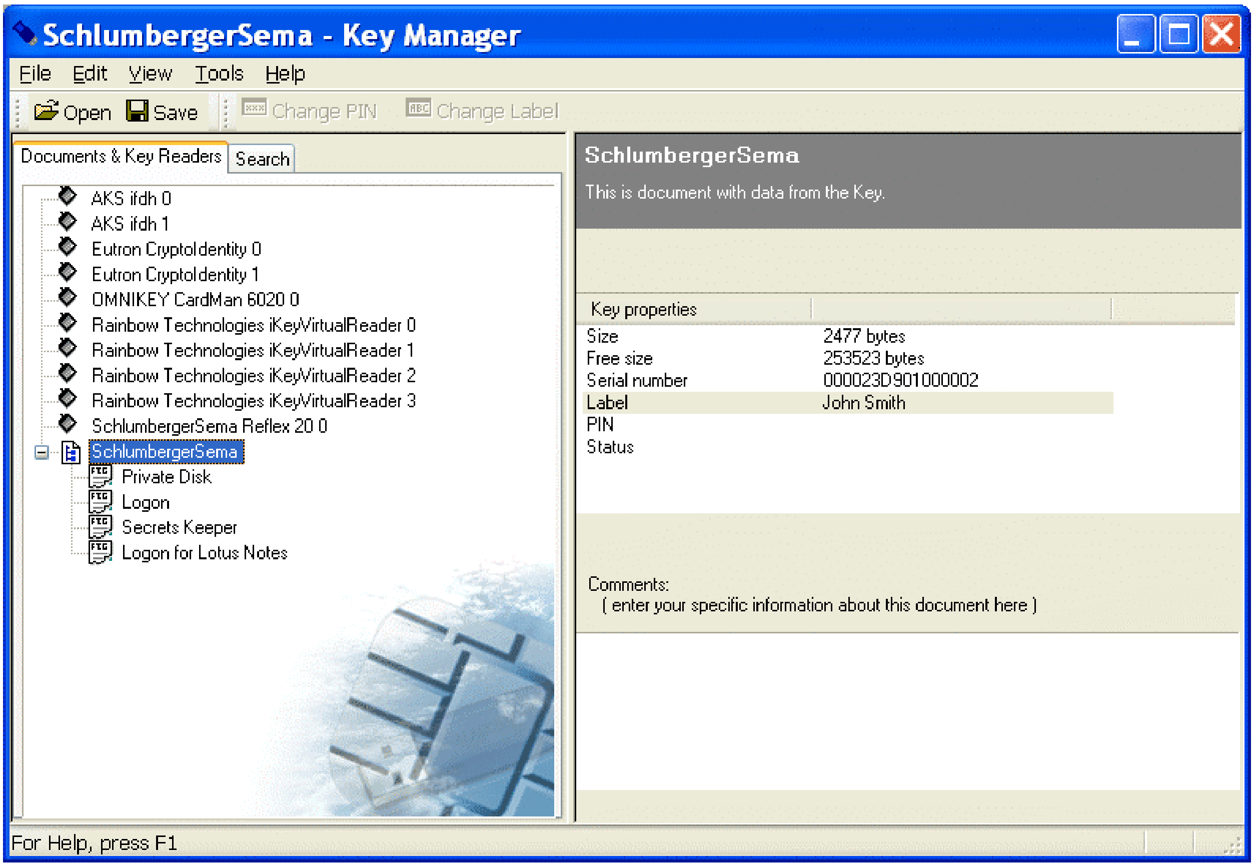
Look in: Desktop

File name:

Files of type: Key Manager Documents (*.dka)

Figure 17
Opening backup copy

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).



SchlumbergerSema

This is document with data from the Key.

Key properties	
Size	2477 bytes
Free size	253523 bytes
Serial number	000023D901000002
Label	John Smith
PIN	
Status	

Comments:
(enter your specific information about this document here)

Figure 18
Displaying backup copy

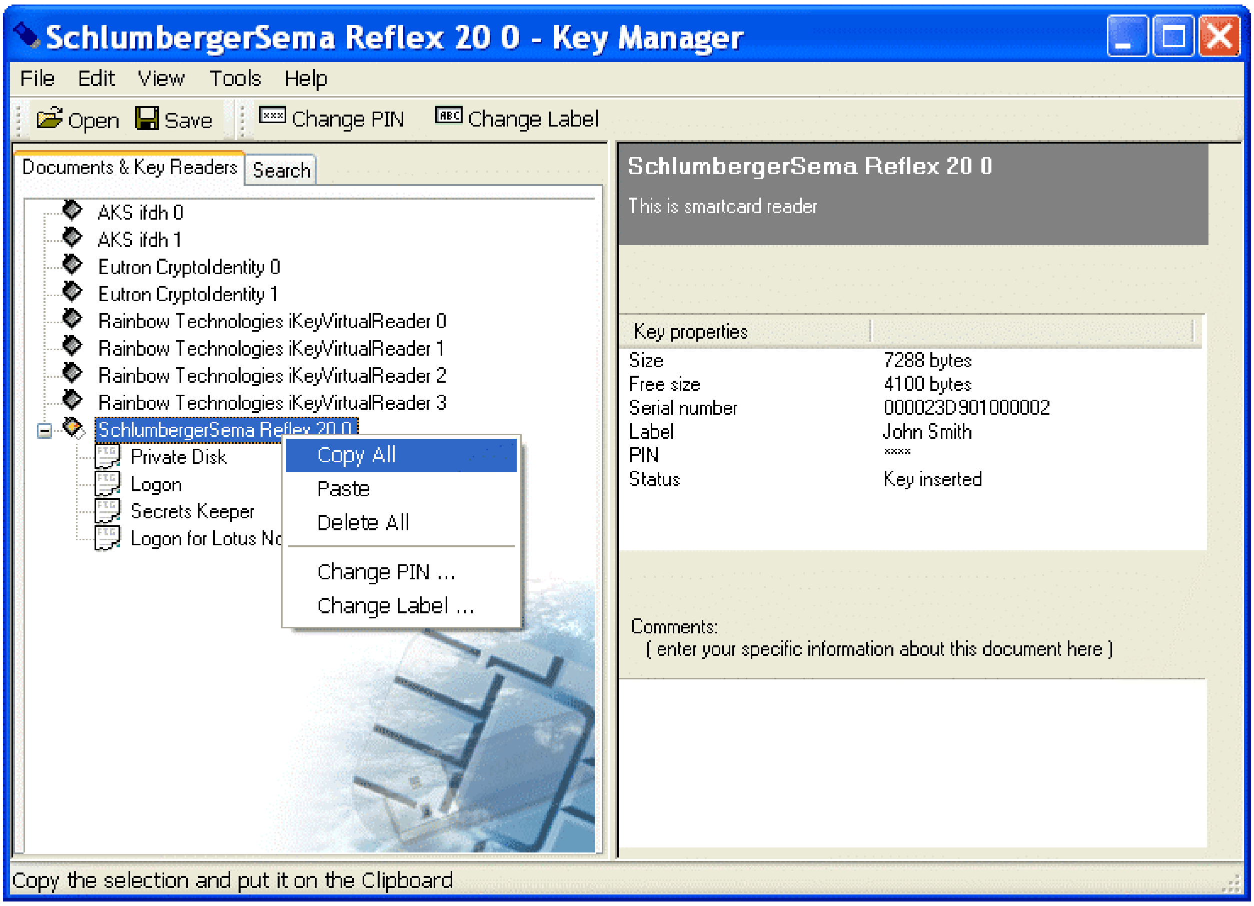
Editing the contents of the hardware key

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.



SchlumbergerSema Reflex 20 0

This is smartcard reader

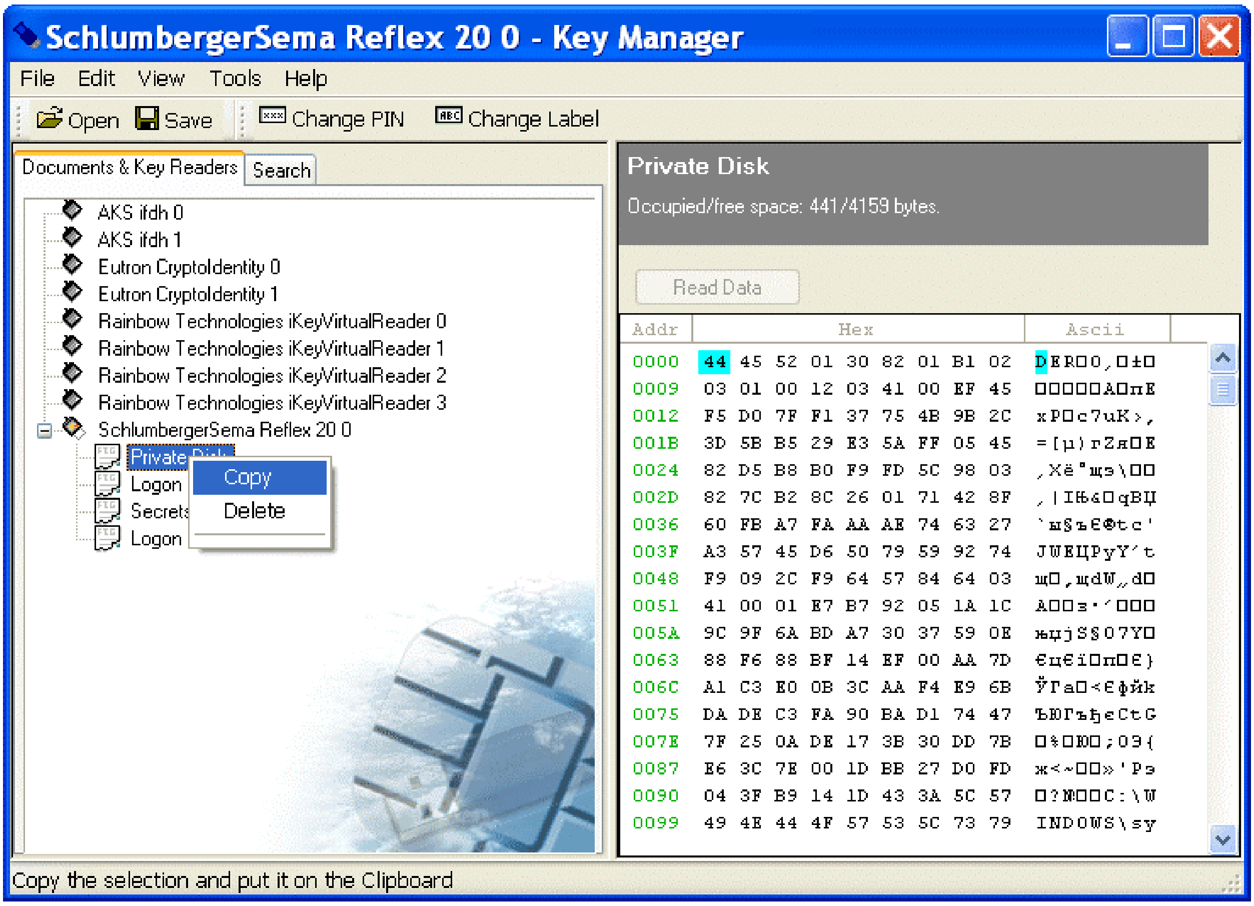
Key properties	
Size	7288 bytes
Free size	4100 bytes
Serial number	000023D901000002
Label	John Smith
PIN	****
Status	Key inserted

Comments:
(enter your specific information about this document here)

Copy the selection and put it on the Clipboard

Figure 19
Copying all data to clipboard

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.


SchlumbergerSema Reflex 20 0 - Key Manager
File
Edit
View
Tools
Help
Open
Save
Change PIN
Change Label
Documents & Key Readers
Search
AKS ifdh 0
AKS ifdh 1
Eutron CryptoIdentity 0
Eutron CryptoIdentity 1
Rainbow Technologies iKeyVirtualReader 0
Rainbow Technologies iKeyVirtualReader 1
Rainbow Technologies iKeyVirtualReader 2
Rainbow Technologies iKeyVirtualReader 3
SchlumbergerSema Reflex 20 0
Private Disk
Logon
Secrets
Logon
Copy
Delete
Read Data

Private Disk

Occupied/free space: 441/4159 bytes.

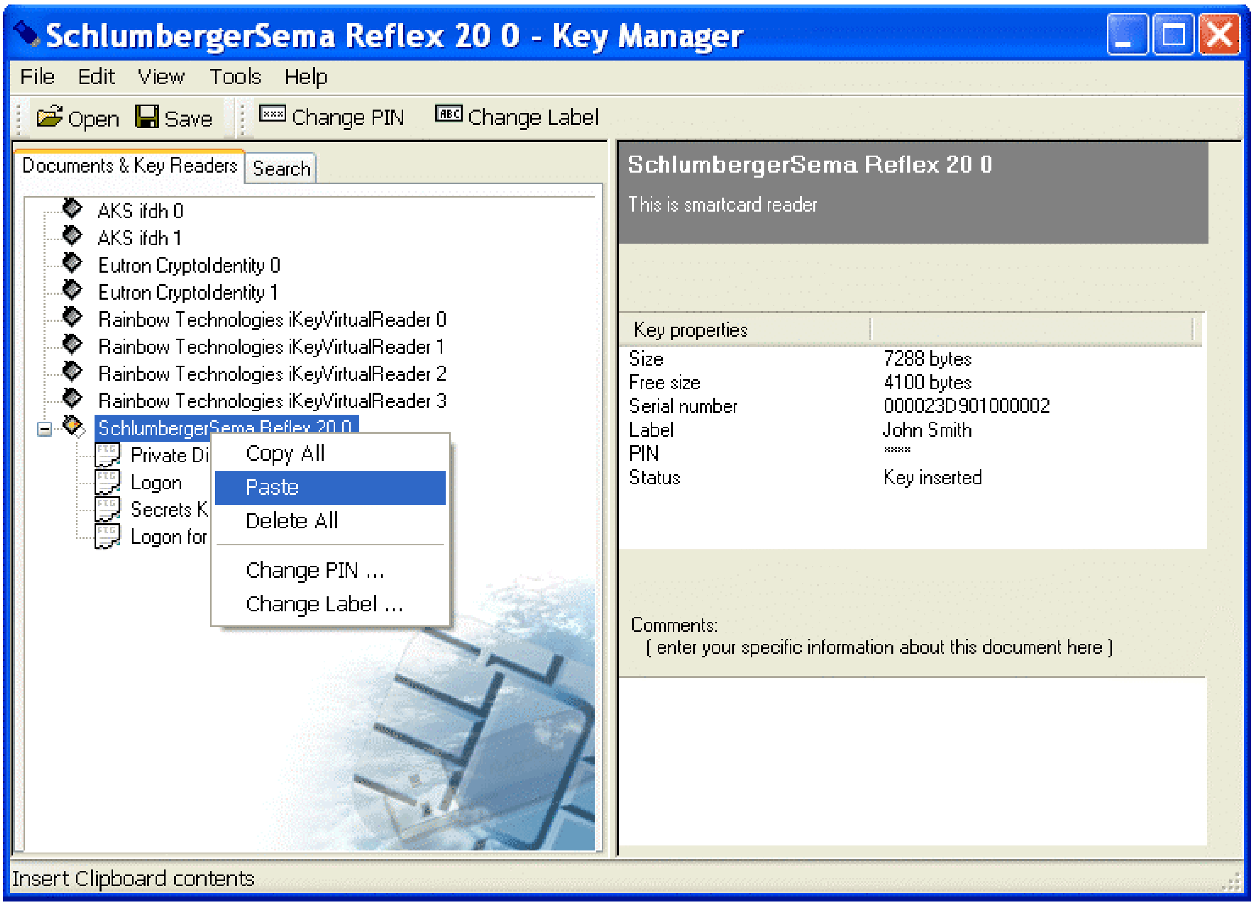
```
Addr   Hex                            Ascii
0000   44 45 52 01 30 82 01 B1 02     DER□0,□±□
0009   03 01 00 12 03 41 00 EF 45     □□□□□A□пE
0012   F5 D0 7F F1 37 75 4B 9B 2C     хР□с7uK›,
001B   3D 5B B5 29 E3 5A FF 05 45     =[µ)гZя□E
0024   82 D5 B8 B0 F9 FD 5C 98 03     ,Хё°щэ\□□
002D   82 7C B2 8C 26 01 71 42 8F     ,|ІЊ&□qBЏ
0036   60 FB A7 FA AA AE 74 63 27     `ы§ъЄ®tc'
003F   A3 57 45 D6 50 79 59 92 74     JWEЦPyY’t
0048   F9 09 2C F9 64 57 84 64 03     щ□,щdW„d□
0051   41 00 01 E7 B7 92 05 1A 1C     A□□з·’□□□
005A   9C 9F 6A BD A7 30 37 59 0E     њџjЅ§07Y□
0063   88 F6 88 BF 14 EF 00 AA 7D     €ц€ї□п□Є}
006C   A1 C3 E0 0B 3C AA F4 E9 6B     ЎГа□<Єфйk
0075   DA DE C3 FA 90 BA D1 74 47     ЪЮГъђєСtG
007E   7F 25 0A DE 17 3B 30 DD 7B     □%□Ю□;0Э{
0087   E6 3C 7E 00 1D BB 27 D0 FD     ж<~□□»'Рэ
0090   04 3F B9 14 1D 43 3A 5C 57     □?№□□C:\W
0099   49 4E 44 4F 57 53 5C 73 79     INDOWS\sy
```

Copy the selection and put it on the Clipboard

Figure 20
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.


SchlumbergerSema Reflex 20 0 - Key Manager
File Edit View Tools Help
Open Save Change PIN Change Label
Documents & Key Readers Search
AKS ifdh 0
AKS ifdh 1
Eutron CryptoIdentity 0
Eutron CryptoIdentity 1
Rainbow Technologies iKeyVirtualReader 0
Rainbow Technologies iKeyVirtualReader 1
Rainbow Technologies iKeyVirtualReader 2
Rainbow Technologies iKeyVirtualReader 3
SchlumbergerSema Reflex 20 0
Private Di
Logon
Secrets K
Logon for
Copy All
Paste
Delete All
Change PIN ...
Change Label ...
Insert Clipboard contents

SchlumbergerSema Reflex 20 0

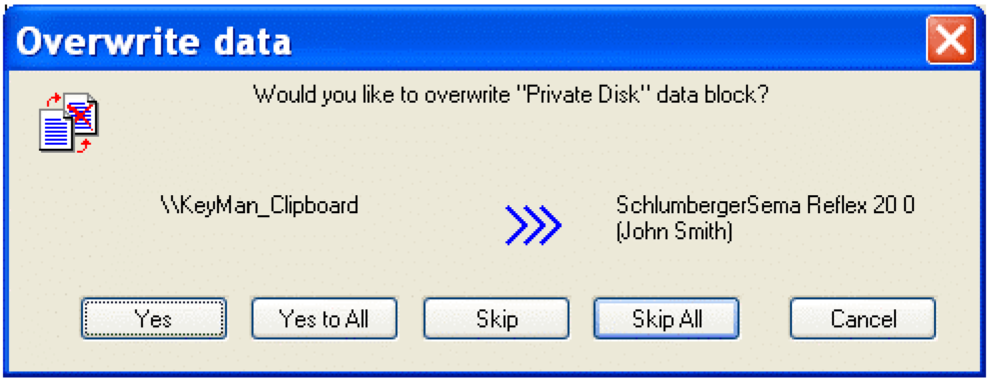
This is smartcard reader

Key properties	
Size	7288 bytes
Free size	4100 bytes
Serial number	000023D901000002
Label	John Smith
PIN	****
Status	Key inserted

Comments:
(enter your specific information about this document here)

Figure 21
Pasting the data from clipboard

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



Would you like to overwrite "Private Disk" data block?

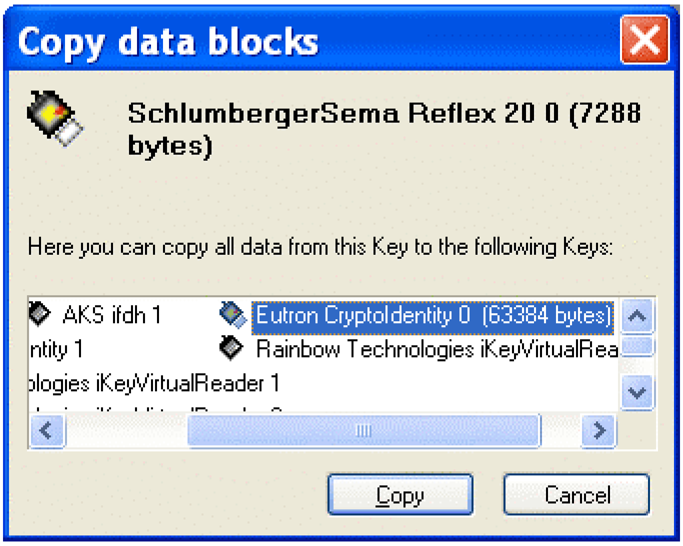
\\KeyMan_Clipboard

SchlumbergerSema Reflex 20 0
(John Smith)

Figure 22
Overwrite data warning message

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).



Copy data blocks

SchlumbergerSema Reflex 20 0 (7288 bytes)

Here you can copy all data from this Key to the following Keys:

AKS ifdh 1

Eutron CryptoIdentity 0 (63384 bytes)

ntity 1

Rainbow Technologies iKeyVirtualRea

ologies iKeyVirtualReader 1

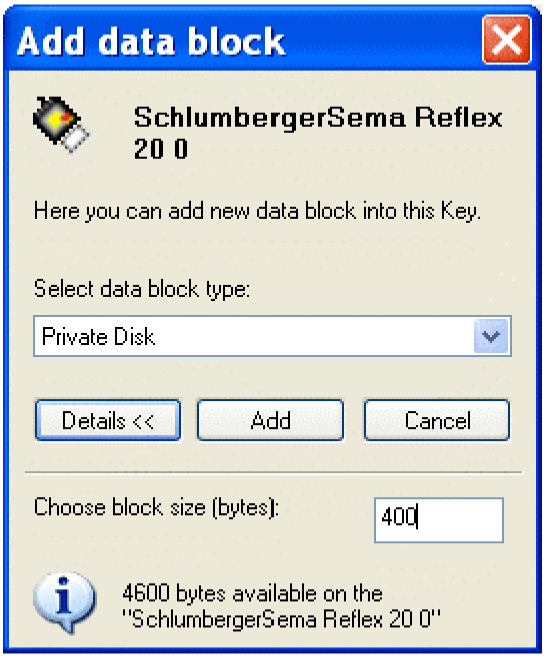
Figure 23
Copying the contents of the hardware key to another key

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).



Here you can add new data block into this Key.

Select data block type: Private Disk

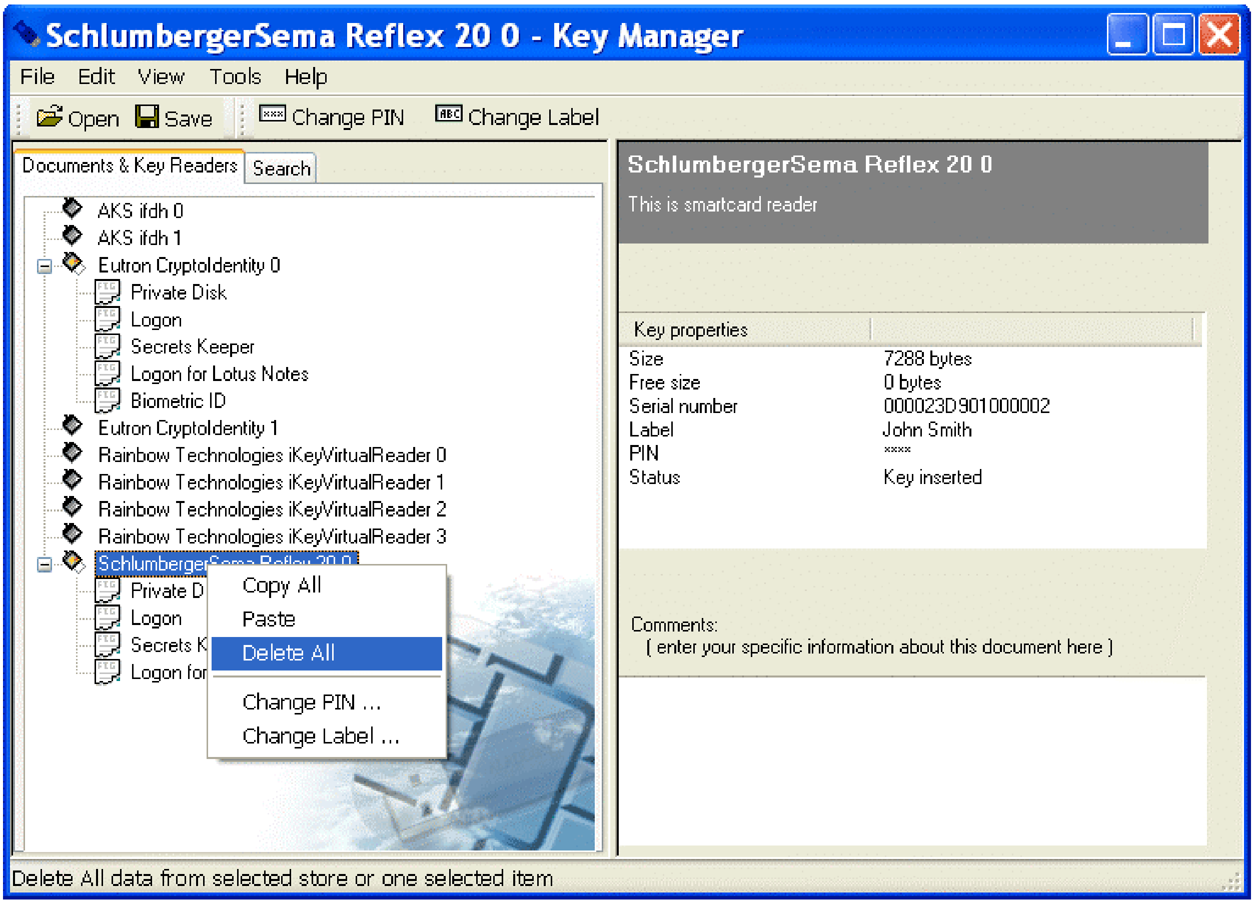
Choose block size (bytes): 400

4600 bytes available on the "SchlumbergerSema Reflex 20 0"

Figure 24
Adding the data of the selected application

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.



SchlumbergerSema Reflex 20 0

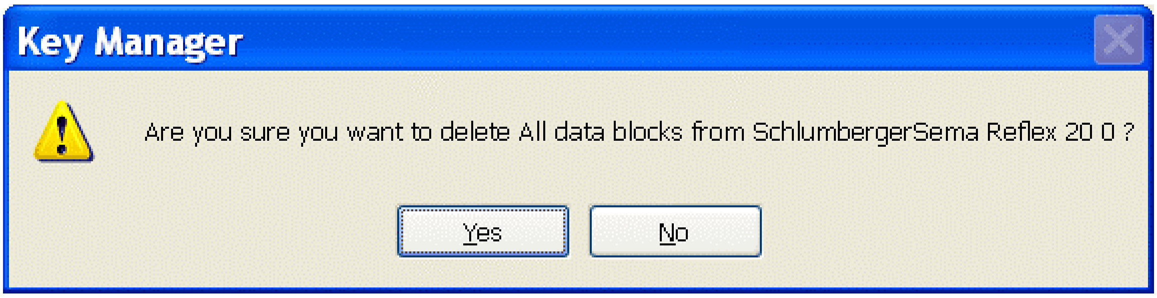
This is smartcard reader

Key properties	
Size	7288 bytes
Free size	0 bytes
Serial number	000023D901000002
Label	John Smith
PIN	****
Status	Key inserted

Comments:
(enter your specific information about this document here)

Delete All data from selected store or one selected item

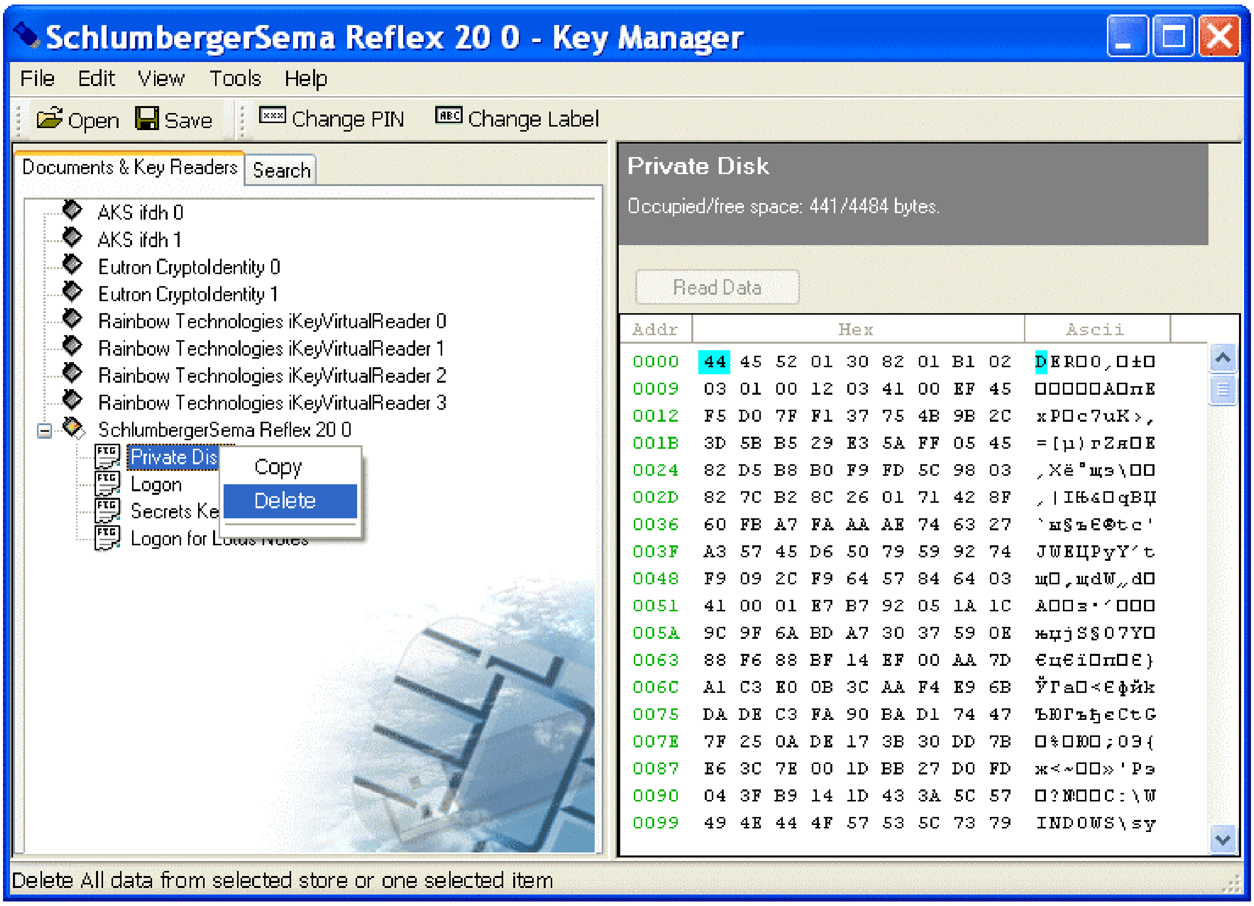
Figure 25
Deleting all data from the hardware key



Are you sure you want to delete All data blocks from SchlumbergerSema Reflex 20 0 ?

Figure 26
Data deletion warning message

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.

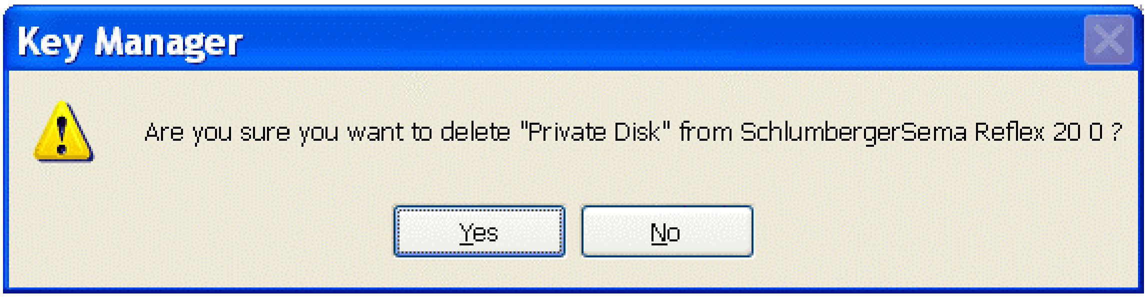

SchlumbergerSema Reflex 20 0 - Key Manager
File
Edit
View
Tools
Help
Open
Save
Change PIN
Change Label
Documents & Key Readers
Search
AKS ifdh 0
AKS ifdh 1
Eutron CryptoIdentity 0
Eutron CryptoIdentity 1
Rainbow Technologies iKeyVirtualReader 0
Rainbow Technologies iKeyVirtualReader 1
Rainbow Technologies iKeyVirtualReader 2
Rainbow Technologies iKeyVirtualReader 3
SchlumbergerSema Reflex 20 0
Private Dis
Logon
Secrets Ke
Logon for Lotus Notes
Copy
Delete
Private Disk
Read Data

Occupied/free space: 441/4484 bytes.

```
Addr  Hex                          Ascii
0000  44 45 52 01 30 82 01 B1 02   DER□0,□±□
0009  03 01 00 12 03 41 00 EF 45   □□□□□A□пE
0012  F5 D0 7F F1 37 75 4B 9B 2C   хР□с7uK>,
001B  3D 5B B5 29 E3 5A FF 05 45   =[µ)гZя□E
0024  82 D5 B8 B0 F9 FD 5C 98 03   ,Хё°щэ\□□
002D  82 7C B2 8C 26 01 71 42 8F   ,|IЊ&□qBЏ
0036  60 FB A7 FA AA AE 74 63 27   `ы§ъЄ®tc'
003F  A3 57 45 D6 50 79 59 92 74   JWEЦPyY't
0048  F9 09 2C F9 64 57 84 64 03   щ□,щdW„d□
0051  41 00 01 E7 B7 92 05 1A 1C   A□□з·'□□□
005A  9C 9F 6A BD A7 30 37 59 0E   њџjS§07Y□
0063  88 F6 88 BF 14 EF 00 AA 7D   €ц€ї□п□Є}
006C  A1 C3 E0 0B 3C AA F4 E9 6B   ЎГа□<Єфйk
0075  DA DE C3 FA 90 BA D1 74 47   ЪЮГъђєСtG
007E  7F 25 0A DE 17 3B 30 DD 7B   □%□Ю□;0Э{
0087  E6 3C 7E 00 1D BB 27 D0 FD   ж<~□□»'Рэ
0090  04 3F B9 14 1D 43 3A 5C 57   □?№□□C:\W
0099  49 4E 44 4F 57 53 5C 73 79   INDOWS\sy
```

Delete All data from selected store or one selected item

Figure 27
Deleting application data

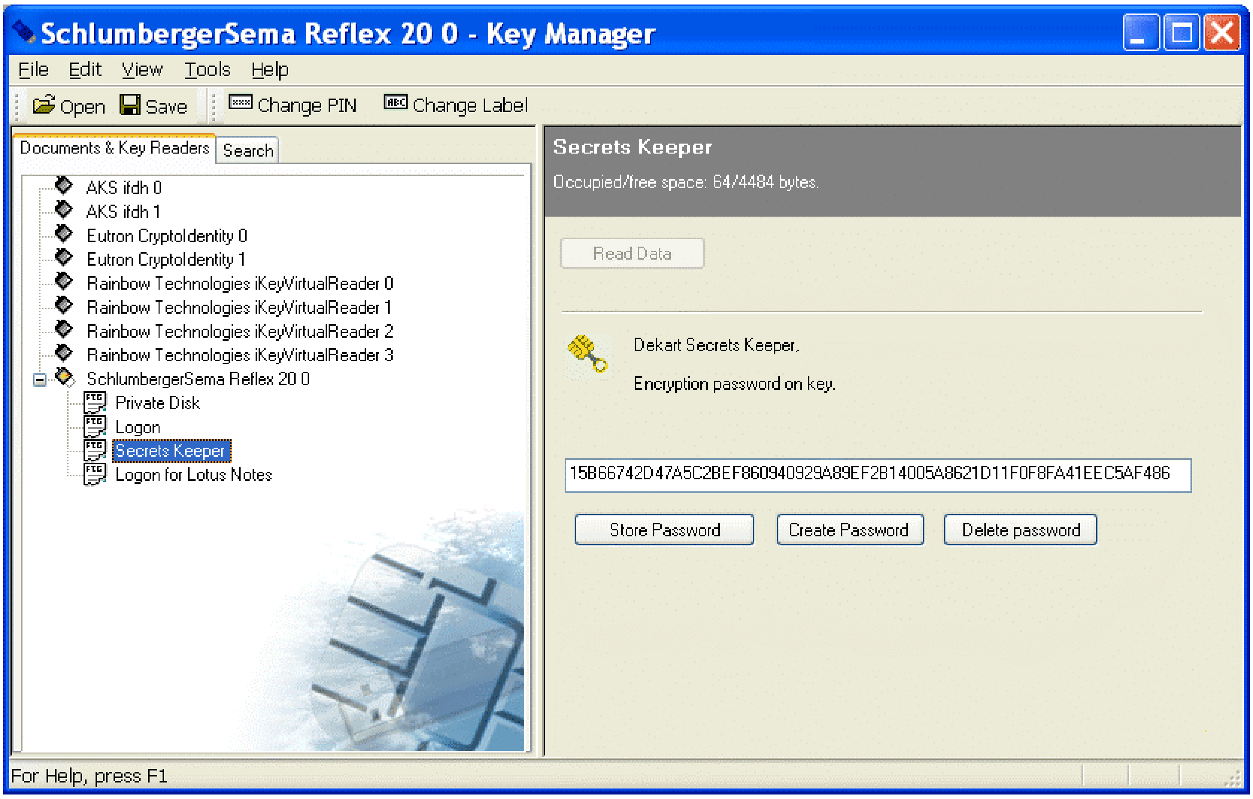


Are you sure you want to delete "Private Disk" from SchlumbergerSema Reflex 20 0 ?

Figure 28
Application data deletion warning message

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.



Occupied/free space: 64/4484 bytes.

Dekart Secrets Keeper,

Encryption password on key.

15B66742D47A5C2BEF860940929A89EF2B14005A8621D11F0F8FA41EEC5AF486

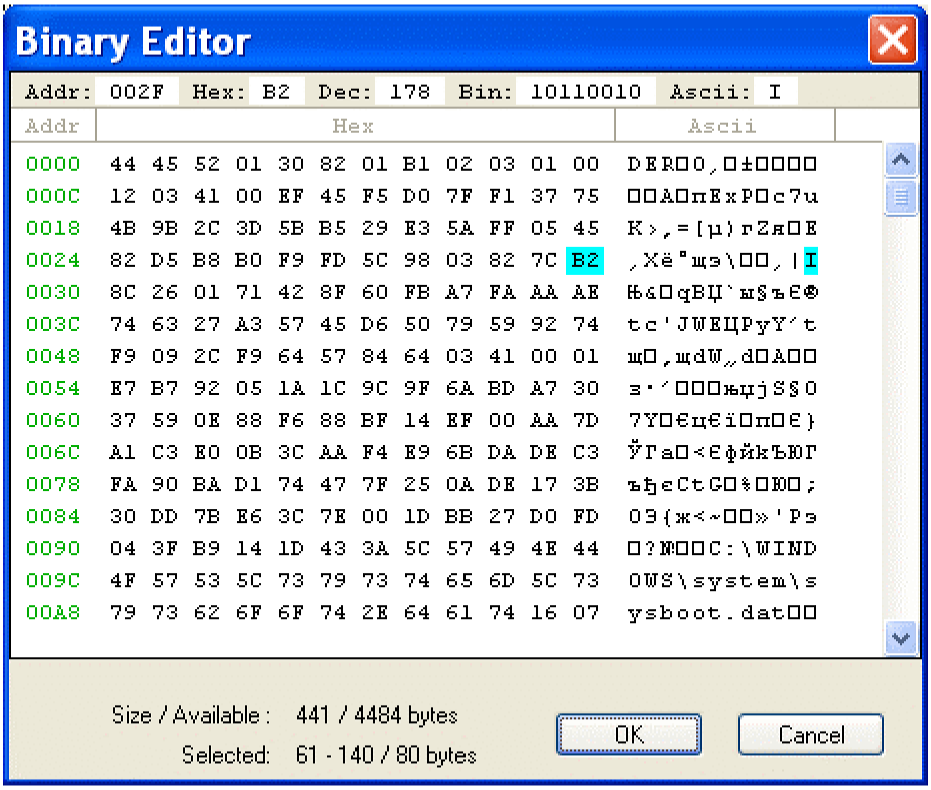
Figure 29
Editing data of the separate application

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.



```
Addr: 002F  Hex: B2  Dec: 178  Bin: 10110010  Ascii: I

Addr  Hex                                  Ascii
0000  44 45 52 01 30 82 01 B1 02 03 01 00  DER□0,□±□□□□
000C  12 03 41 00 EF 45 F5 D0 7F F1 37 75  □□A□пExP□с7u
0018  4B 9B 2C 3D 5B B5 29 E3 5A FF 05 45  K>,=[µ)гZя□E
0024  82 D5 B8 B0 F9 FD 5C 98 03 82 7C B2  ,Xё°щэ\□□,|I
0030  8C 26 01 71 42 8F 60 FB A7 FA AA AE  Њ&□qBЏ`ы§ъЄ®
003C  74 63 27 A3 57 45 D6 50 79 59 92 74  tc'JWEЦPyY't
0048  F9 09 2C F9 64 57 84 64 03 41 00 01  щ□,щdW„d□A□□
0054  E7 B7 92 05 1A 1C 9C 9F 6A BD A7 30  з·'□□□њџjЅ§0
0060  37 59 0E 88 F6 88 BF 14 EF 00 AA 7D  7Y□€ц€ї□п□Є}
006C  A1 C3 E0 0B 3C AA F4 E9 6B DA DE C3  ЎГа□<ЄфйkЪЮГ
0078  FA 90 BA D1 74 47 7F 25 0A DE 17 3B  ъђєСtG□%□Ю□;
0084  30 DD 7B E6 3C 7E 00 1D BB 27 D0 FD  0Э{ж<~□□»'Рэ
0090  04 3F B9 14 1D 43 3A 5C 57 49 4E 44  □?№□□C:\WIND
009C  4F 57 53 5C 73 79 73 74 65 6D 5C 73  OWS\system\s
00A8  79 73 62 6F 6F 74 2E 64 61 74 16 07  ysboot.dat□□
```

Size / Available : 441 / 4484 bytes

Selected: 61 - 140 / 80 bytes

Figure 30
Editing binary data

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.

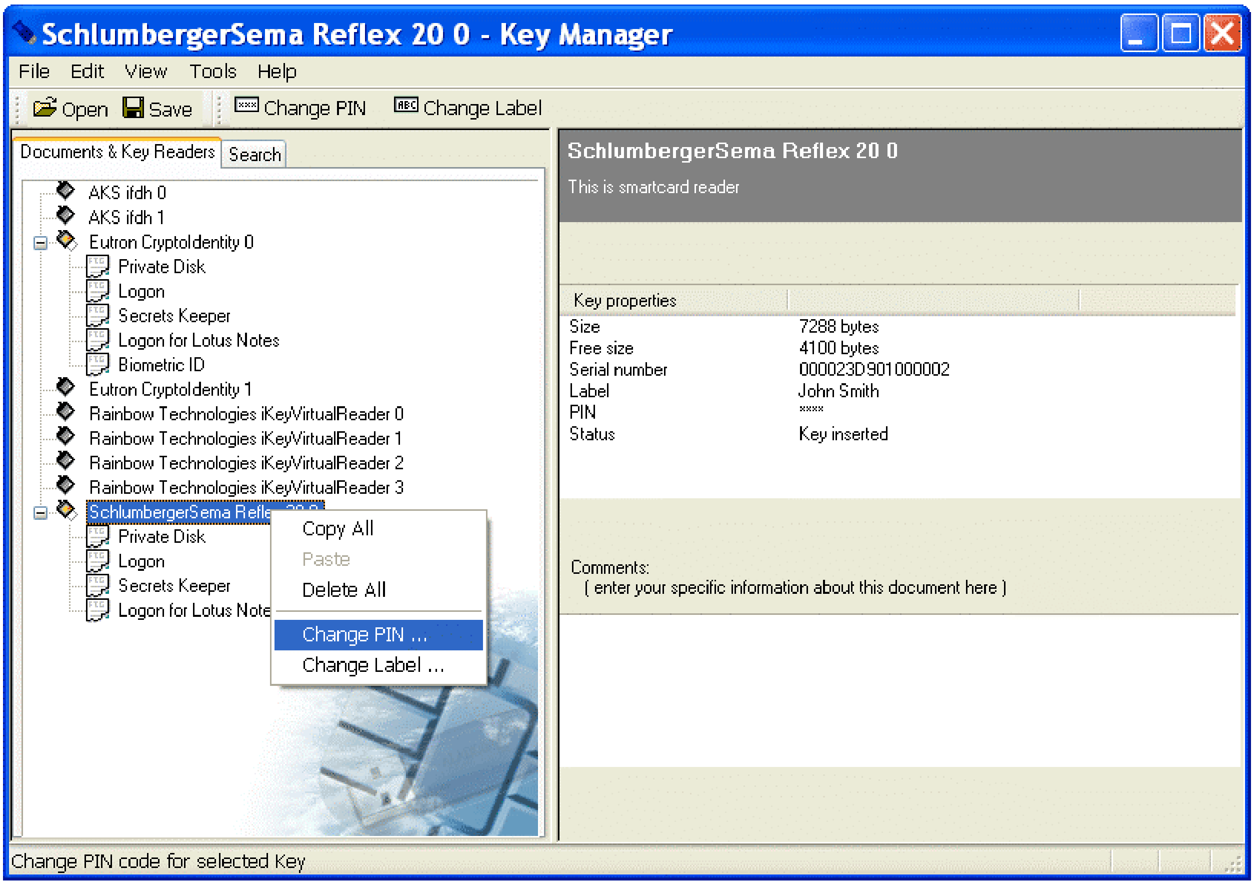
To create a template, go to ***File > New*** menu of the main window. Creating, editing and copying the templates are identical to working with the hardware key (see *Viewing the contents of the hardware key* section and *Editing the contents of the hardware key* section).

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).



SchlumbergerSema Reflex 20 0

This is smartcard reader

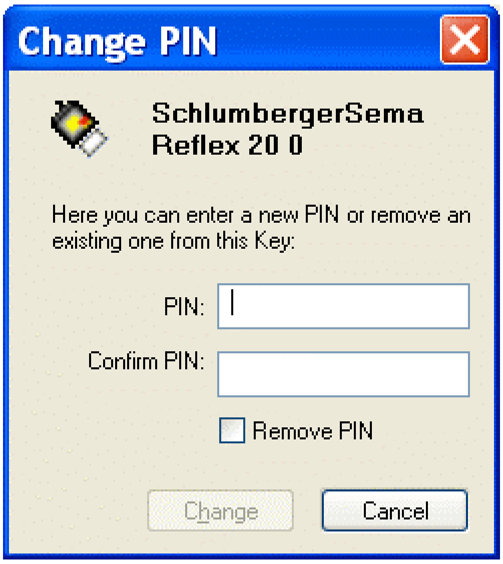
Key properties	
Size	7288 bytes
Free size	4100 bytes
Serial number	000023D901000002
Label	John Smith
PIN	****
Status	Key inserted

Comments:
(enter your specific information about this document here)

Change PIN code for selected Key

Figure 31
Changing the PIN code of the hardware key

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.

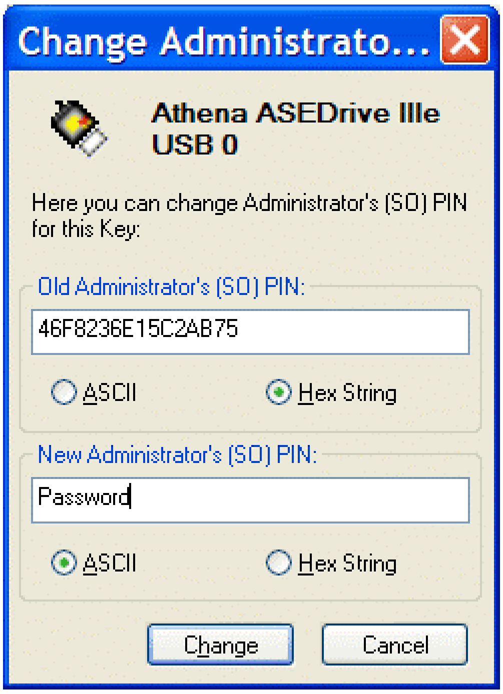


Here you can enter a new PIN or remove an existing one from this Key:

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).



Athena ASEDrive IIIe USB 0

Here you can change Administrator's (SO) PIN for this Key:

Old Administrator's (SO) PIN: 46F8236E15C2AB75

○ ASCII ● Hex String

New Administrator's (SO) PIN: Password

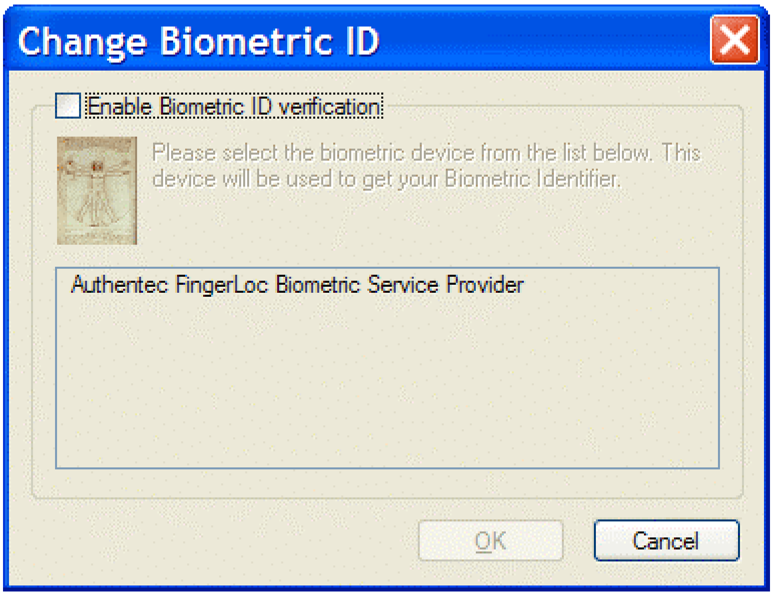
● ASCII ○ Hex String

Figure 33
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).



Change Biometric ID

□ Enable Biometric ID verification

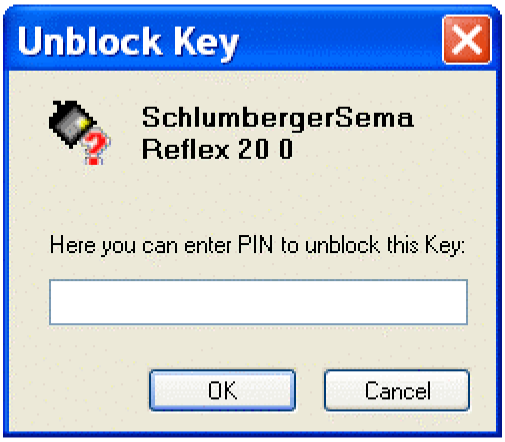
Please select the biometric device from the list below. This device will be used to get your Biometric Identifier.

Authentec FingerLoc Biometric Service Provider

Figure 34
Changing biometric identifier

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).



Unblock Key

SchlumbergerSema
Reflex 20 0

Here you can enter PIN to unblock this Key:

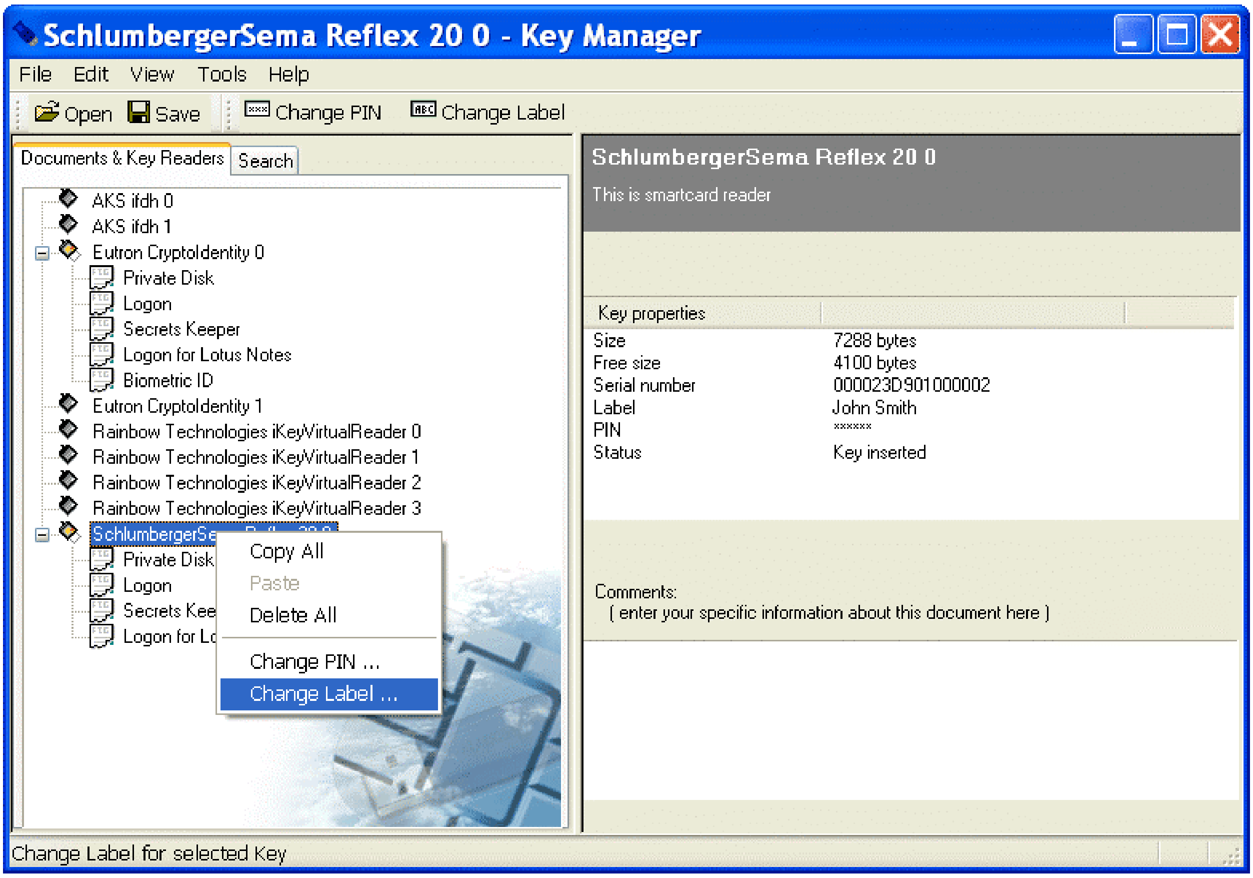
Figure 35
Unblocking the hardware key

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).



SchlumbergerSema Reflex 20 0 - Key Manager
File Edit View Tools Help
Open Save Change PIN Change Label
Documents & Key Readers Search
AKS ifdh 0
AKS ifdh 1
Eutron CryptoIdentity 0
Private Disk
Logon
Secrets Keeper
Logon for Lotus Notes
Biometric ID
Eutron CryptoIdentity 1
Rainbow Technologies iKeyVirtualReader 0
Rainbow Technologies iKeyVirtualReader 1
Rainbow Technologies iKeyVirtualReader 2
Rainbow Technologies iKeyVirtualReader 3
SchlumbergerSe
Private Disk
Logon
Secrets Kee
Logon for Lo
Copy All
Paste
Delete All
Change PIN ...
Change Label ...

SchlumbergerSema Reflex 20 0

This is smartcard reader

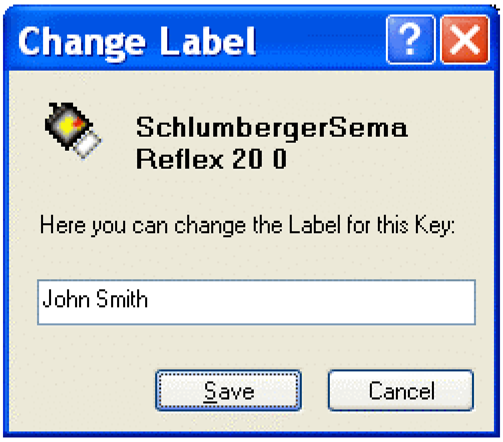
Key properties	
Size	7288 bytes
Free size	4100 bytes
Serial number	000023D901000002
Label	John Smith
PIN	******
Status	Key inserted

Comments:
(enter your specific information about this document here)

Change Label for selected Key

Figure 36
Changing the symbolic label

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.



Here you can change the Label for this Key:

John Smith

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).

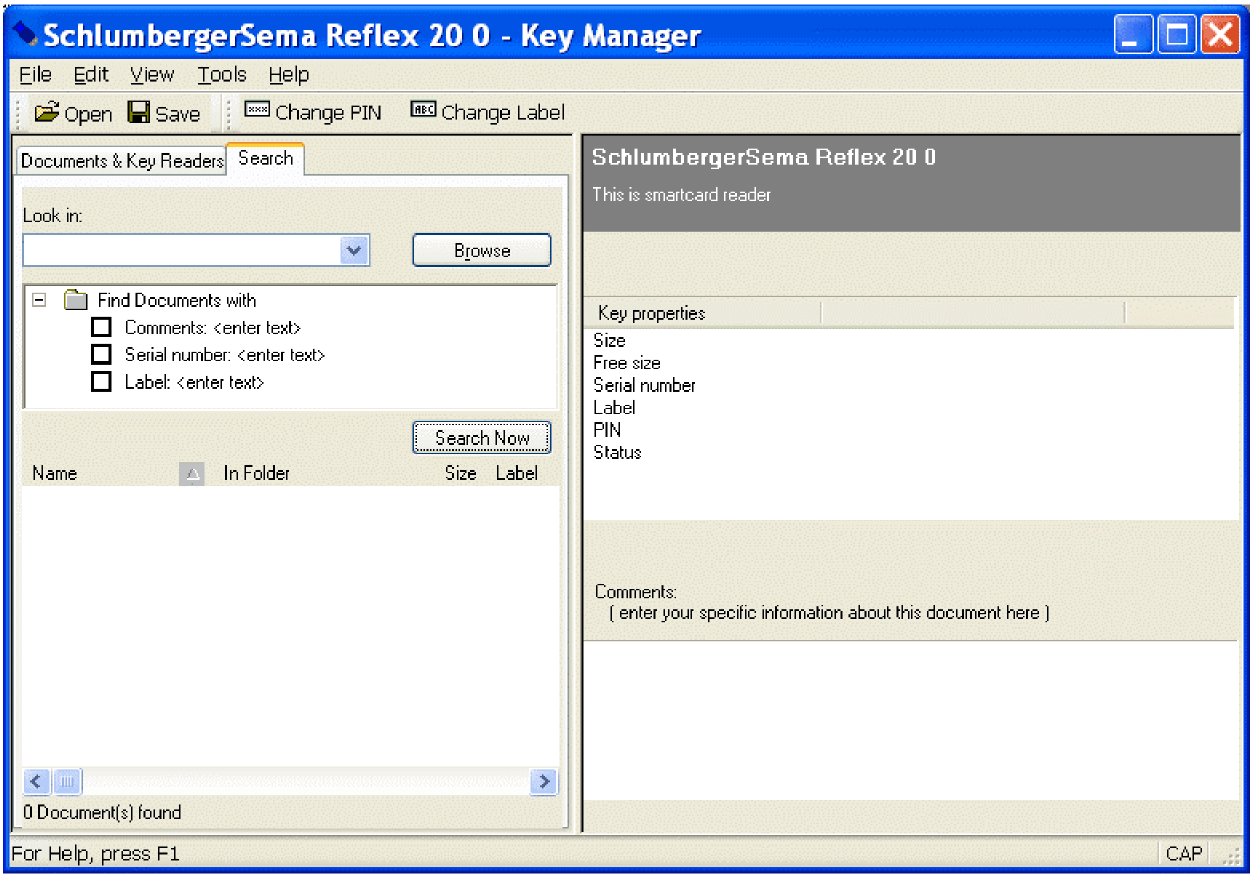
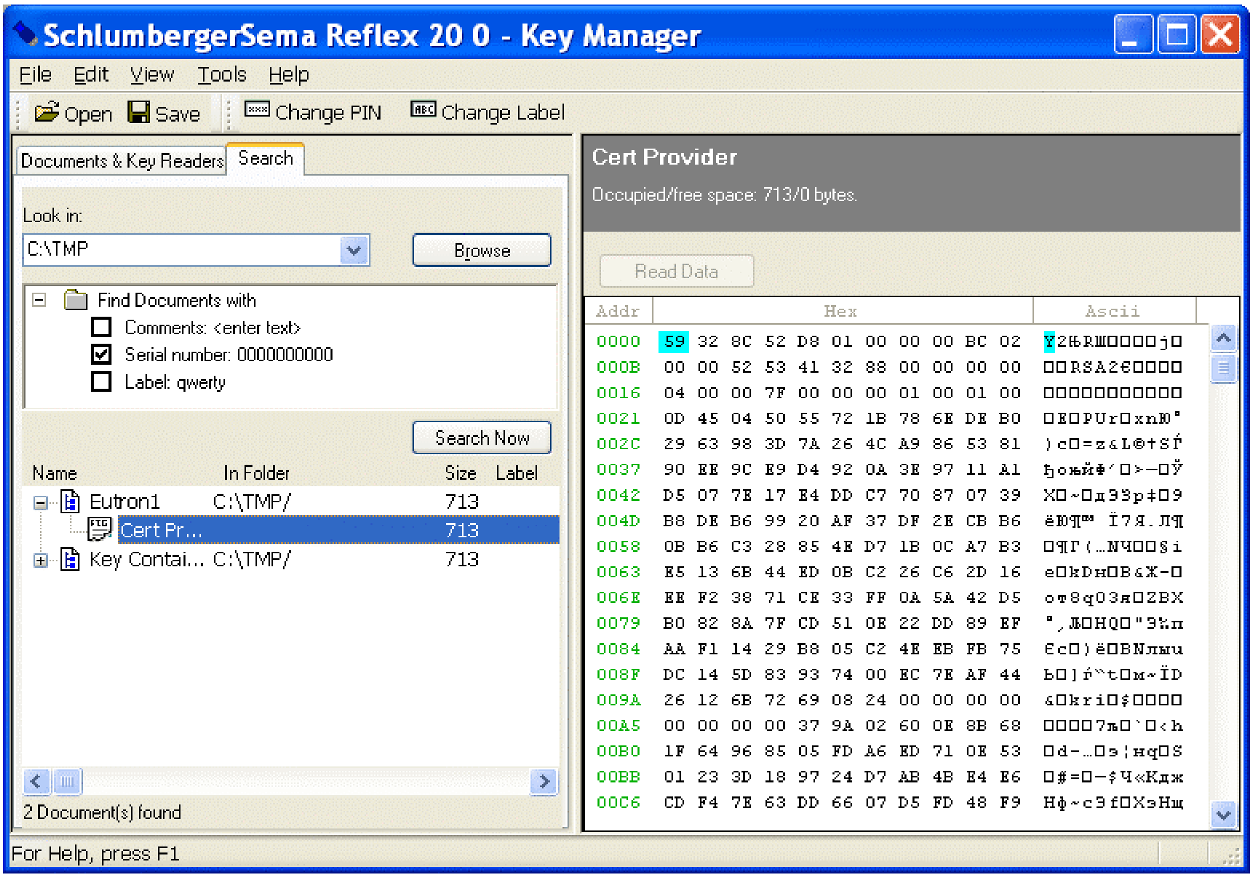

SchlumbergerSema Reflex 20 0 - Key Manager
File Edit View Tools Help
Open Save Change PIN Change Label
Documents & Key Readers Search
Look in:
Browse
Find Documents with
Comments: <enter text>
Serial number: <enter text>
Label: <enter text>
Search Now
Name In Folder Size Label
0 Document(s) found
SchlumbergerSema Reflex 20 0
This is smartcard reader
Key properties
Size
Free size
Serial number
Label
PIN
Status
Comments:
(enter your specific information about this document here)
For Help, press F1
CAP

Figure 38
Searching the backup copy

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).


SchlumbergerSema Reflex 20 0 - Key Manager
File Edit View Tools Help
Open Save Change PIN Change Label
Documents & Key Readers
Search
Browse
Search Now
Read Data
For Help, press F1

Look in: C:\TMP

⊟ Find Documents with
- □ Comments: <enter text>
- ☑ Serial number: 0000000000
- □ Label: qwerty

Name	In Folder	Size	Label
⊟ Eutron1	C:\TMP/	713	
Cert Pr...		713	
⊞ Key Contai...	C:\TMP/	713	

2 Document(s) found

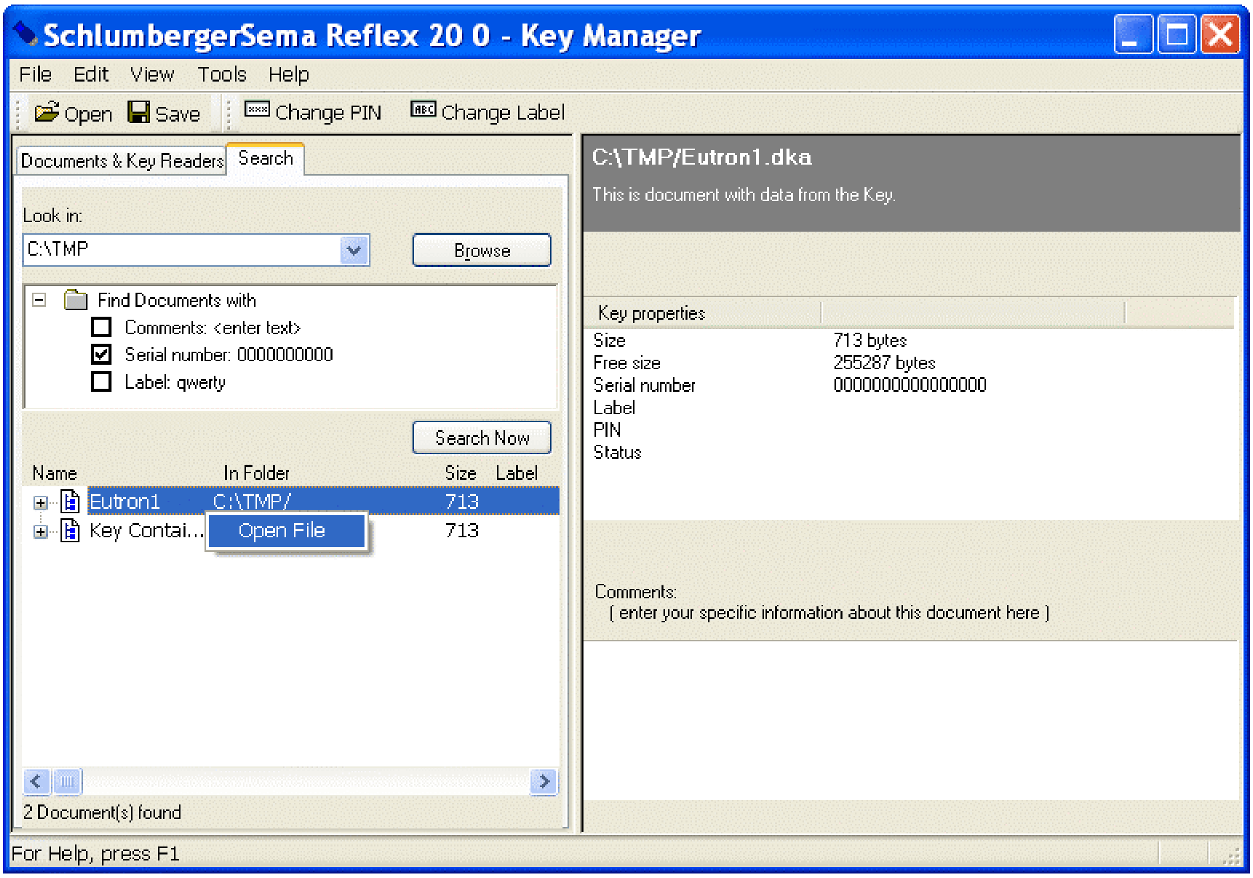
Cert Provider

Occupied/free space: 713/0 bytes.

```
Addr              Hex                    Ascii
0000  59 32 8C 52 D8 01 00 00 00 BC 02   Y2ЊRШ□□□□j□
000B  00 00 52 53 41 32 88 00 00 00 00   □□RSA2€□□□□
0016  04 00 00 7F 00 00 00 01 00 01 00   □□□□□□□□□□□
0021  0D 45 04 50 55 72 1B 78 6E DE B0   □E□PUr□xnЮ°
002C  29 63 98 3D 7A 26 4C A9 86 53 81   )c□=z&L©†SЃ
0037  90 EE 9C E9 D4 92 0A 3E 97 11 A1   ђoњйФ’□>—□Ў
0042  D5 07 7E 17 E4 DD C7 70 87 07 39   Х□~□дЭЗp‡□9
004D  B8 DE B6 99 20 AF 37 DF 2E CB B6   ёЮ¶™ Ї7Я.Л¶
0058  0B B6 C3 28 85 4E D7 1B 0C A7 B3   □¶Г(…NЧ□□§і
0063  E5 13 6B 44 ED 0B C2 26 C6 2D 16   е□kDн□В&Ж-□
006E  EE F2 38 71 CE 33 FF 0A 5A 42 D5   от8qО3я□ZBХ
0079  B0 82 8A 7F CD 51 0E 22 DD 89 EF   °‚Љ□НQ□"Э‰п
0084  AA F1 14 29 B8 05 C2 4E EB FB 75   Єс□)ё□ВNлыu
008F  DC 14 5D 83 93 74 00 EC 7E AF 44   Ь□]ѓ“t□м~ЇD
009A  26 12 6B 72 69 08 24 00 00 00 00   &□kri□$□□□□
00A5  00 00 00 00 37 9A 02 60 0E 8B 68   □□□□7љ□`□‹h
00B0  1F 64 96 85 05 FD A6 ED 71 0E 53   □d–…□э¦нq□S
00BB  01 23 3D 18 97 24 D7 AB 4B E4 E6   □#=□—$Ч«Kдж
00C6  CD F4 7E 63 DD 66 07 D5 FD 48 F9   Нф~cЭf□ХэHщ
```

Figure 39
Search results

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).


SchlumbergerSema Reflex 20 0 - Key Manager
File Edit View Tools Help
Open Save Change PIN Change Label
Documents & Key Readers
Search
Browse
Search Now
Open File
For Help, press F1

Look in: C:\TMP

Find Documents with
- ☐ Comments: <enter text>
- ☑ Serial number: 0000000000
- ☐ Label: qwerty

Name	In Folder	Size	Label
Eutron1	C:\TMP/	713	
Key Contai...		713	

2 Document(s) found

C:\TMP/Eutron1.dka

This is document with data from the Key.

Key properties	
Size	713 bytes
Free size	255287 bytes
Serial number	0000000000000000
Label	
PIN	
Status	

Comments:
(enter your specific information about this document here)

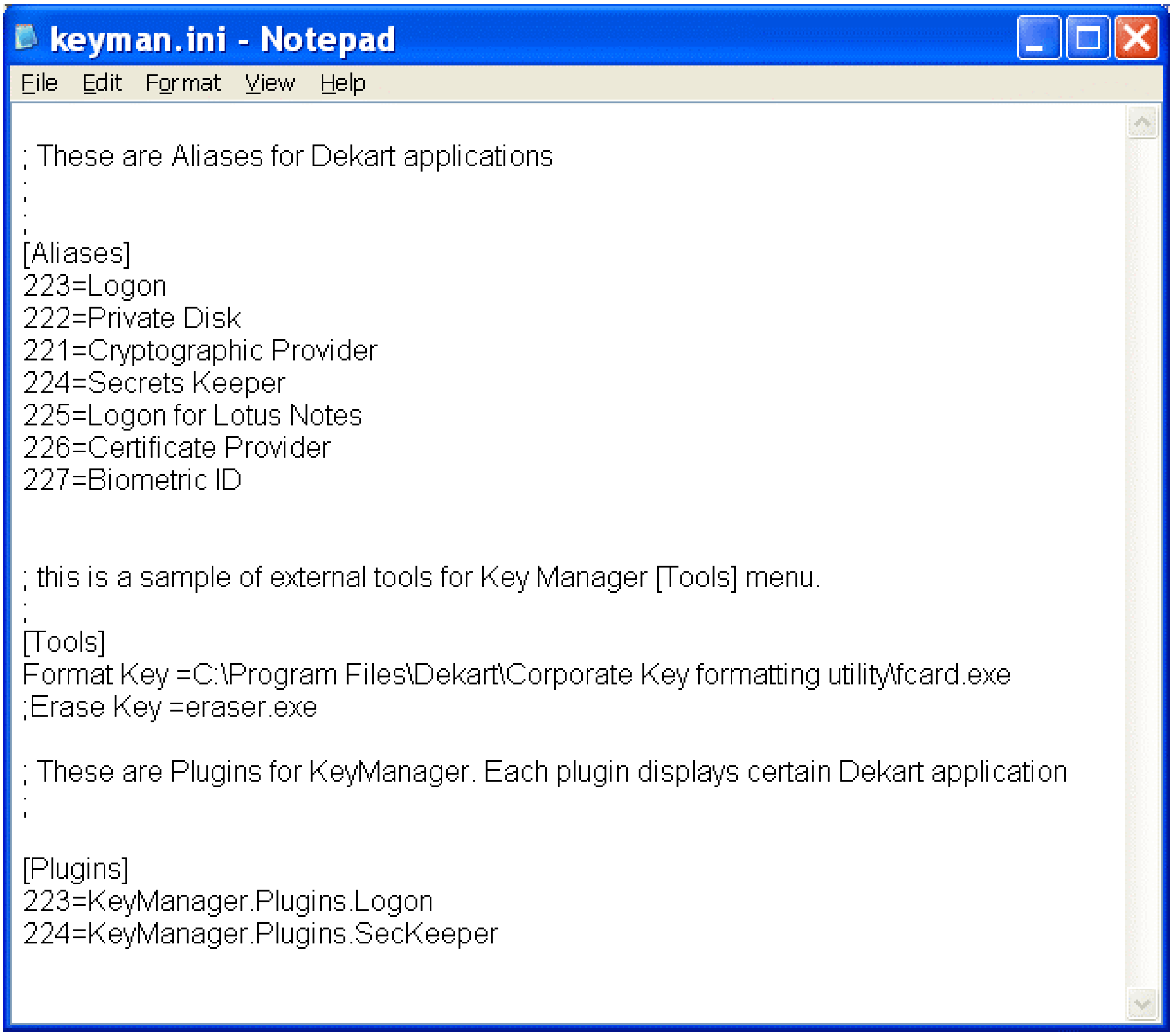
Figure 40
Opening the backup copy found

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).



```
; These are Aliases for Dekart applications
;
;
[Aliases]
223=Logon
222=Private Disk
221=Cryptographic Provider
224=Secrets Keeper
225=Logon for Lotus Notes
226=Certificate Provider
227=Biometric ID


; this is a sample of external tools for Key Manager [Tools] menu.
;
[Tools]
Format Key =C:\Program Files\Dekart\Corporate Key formatting utility\fcard.exe
;Erase Key =eraser.exe

; These are Plugins for KeyManager. Each plugin displays certain Dekart application
;

[Plugins]
223=KeyManager.Plugins.Logon
224=KeyManager.Plugins.SecKeeper
```

Figure 41
Editing configuration file

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
```

225=Logon for Lotus Notes
226=Certificate Provider
227=Biometric ID

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.

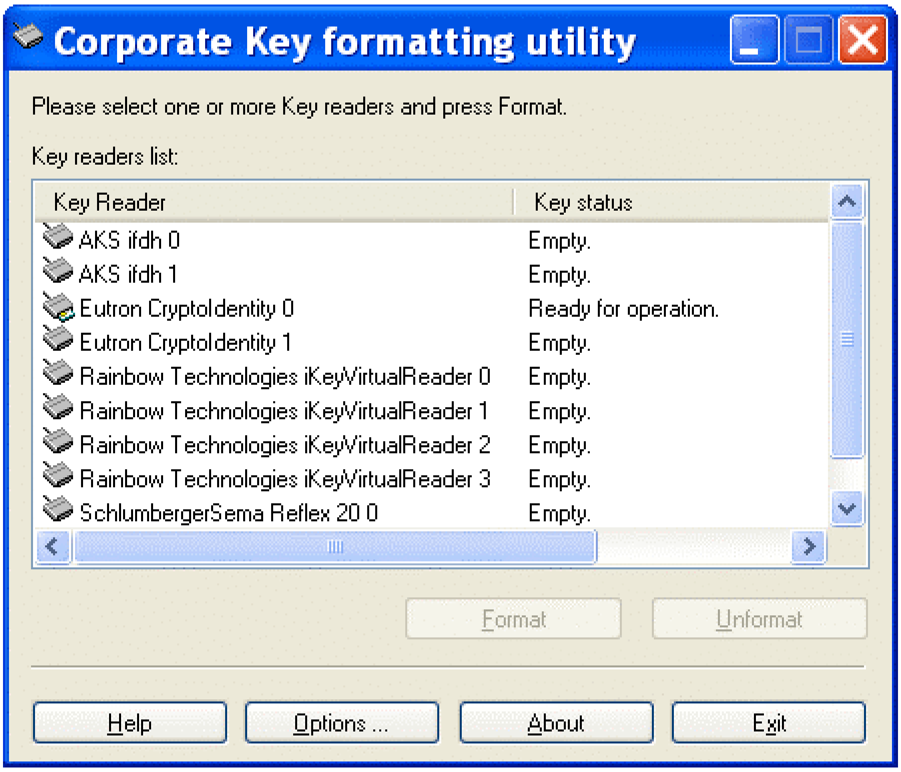
Additional viewing tools are the ActiveX components. Therefore, the additional component should be registered in the operating system: copy the component file into the **Dekart Key Manager** folder and run *Regsvr32.exe filename.ocx* command, where the *filename.ocx* is the component’s name.

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).



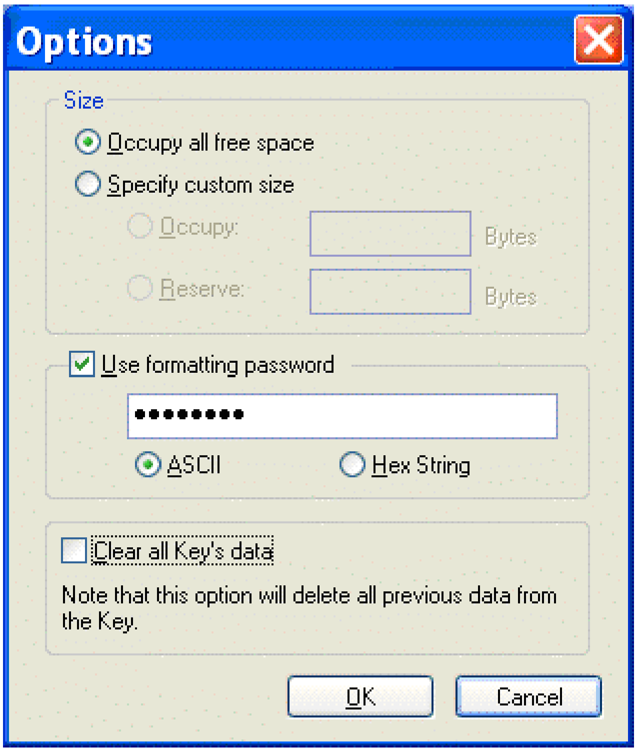
Please select one or more Key readers and press Format.

Key readers list:

Key Reader	Key status
AKS ifdh 0	Empty.
AKS ifdh 1	Empty.
Eutron CryptoIdentity 0	Ready for operation.
Eutron CryptoIdentity 1	Empty.
Rainbow Technologies iKeyVirtualReader 0	Empty.
Rainbow Technologies iKeyVirtualReader 1	Empty.
Rainbow Technologies iKeyVirtualReader 2	Empty.
Rainbow Technologies iKeyVirtualReader 3	Empty.
SchlumbergerSema Reflex 20 0	Empty.

Figure 42
Main window of **Dekart Corporate key formatting utility**

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):



Size

● Occupy all free space

○ Specify custom size

○ Occupy: Bytes

○ Reserve: Bytes

☑ Use formatting password

●●●●●●●●●

● ASCII ○ Hex String

□ Clear all Key's data

Note that this option will delete all previous data from the Key.

Figure 43
Setting up formatting parameters

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.

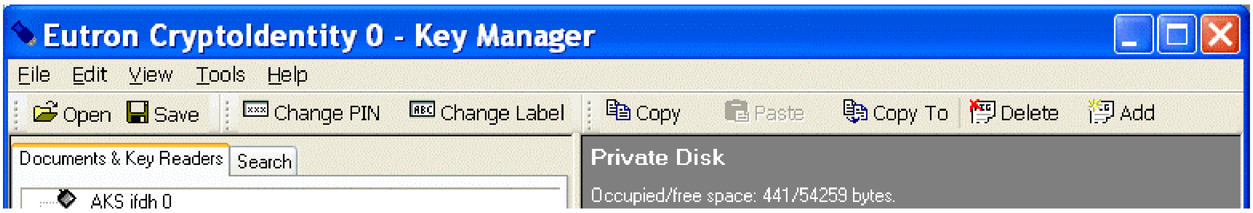

Eutron CryptoIdentity 0 - Key Manager
File Edit View Tools Help
Open Save Change PIN Change Label Copy Paste Copy To Delete Add
Documents & Key Readers Search
AKS ifdh 0
Private Disk
Occupied/free space: 441/54259 bytes.

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.

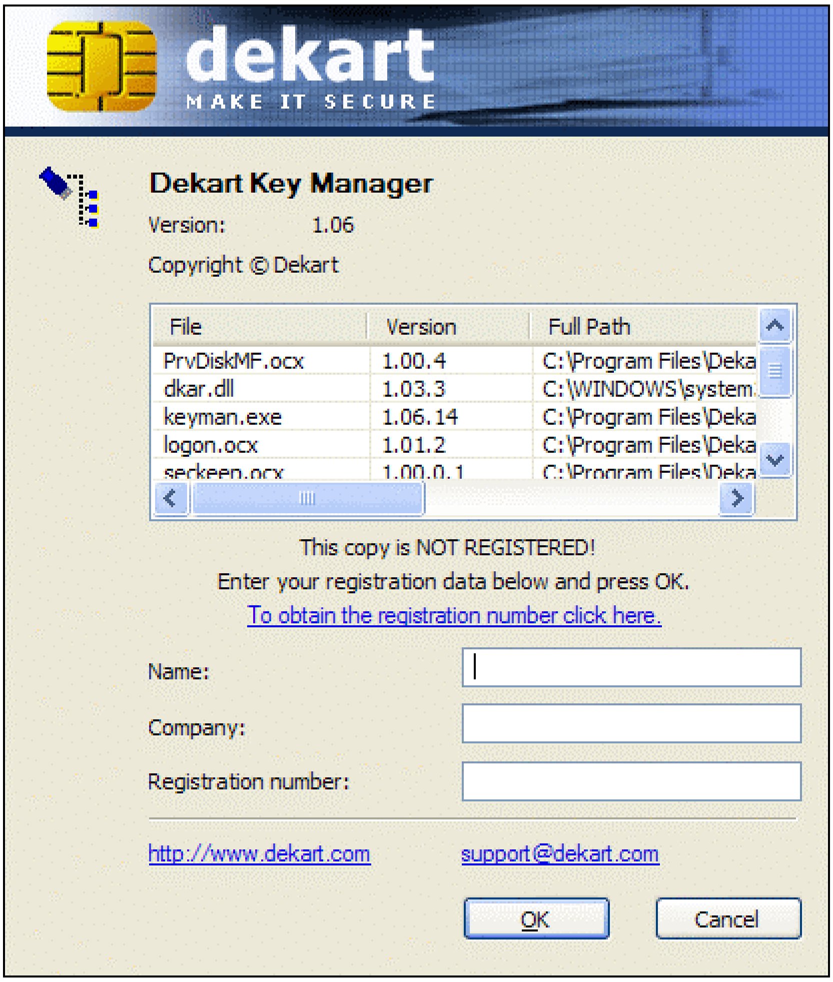
Registering Dekart Key Manager

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. 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.



Dekart Key Manager

Version: 1.06

Copyright © Dekart

File	Version	Full Path
PrvDiskMF.ocx	1.00.4	C:\Program Files\Deka
dkar.dll	1.03.3	C:\WINDOWS\system
keyman.exe	1.06.14	C:\Program Files\Deka
logon.ocx	1.01.2	C:\Program Files\Deka
seckeep.ocx	1.00.0.1	C:\Program Files\Deka

This copy is NOT REGISTERED!

Enter your registration data below and press OK.

To obtain the registration number click here.

Name:

Company:

Registration number:

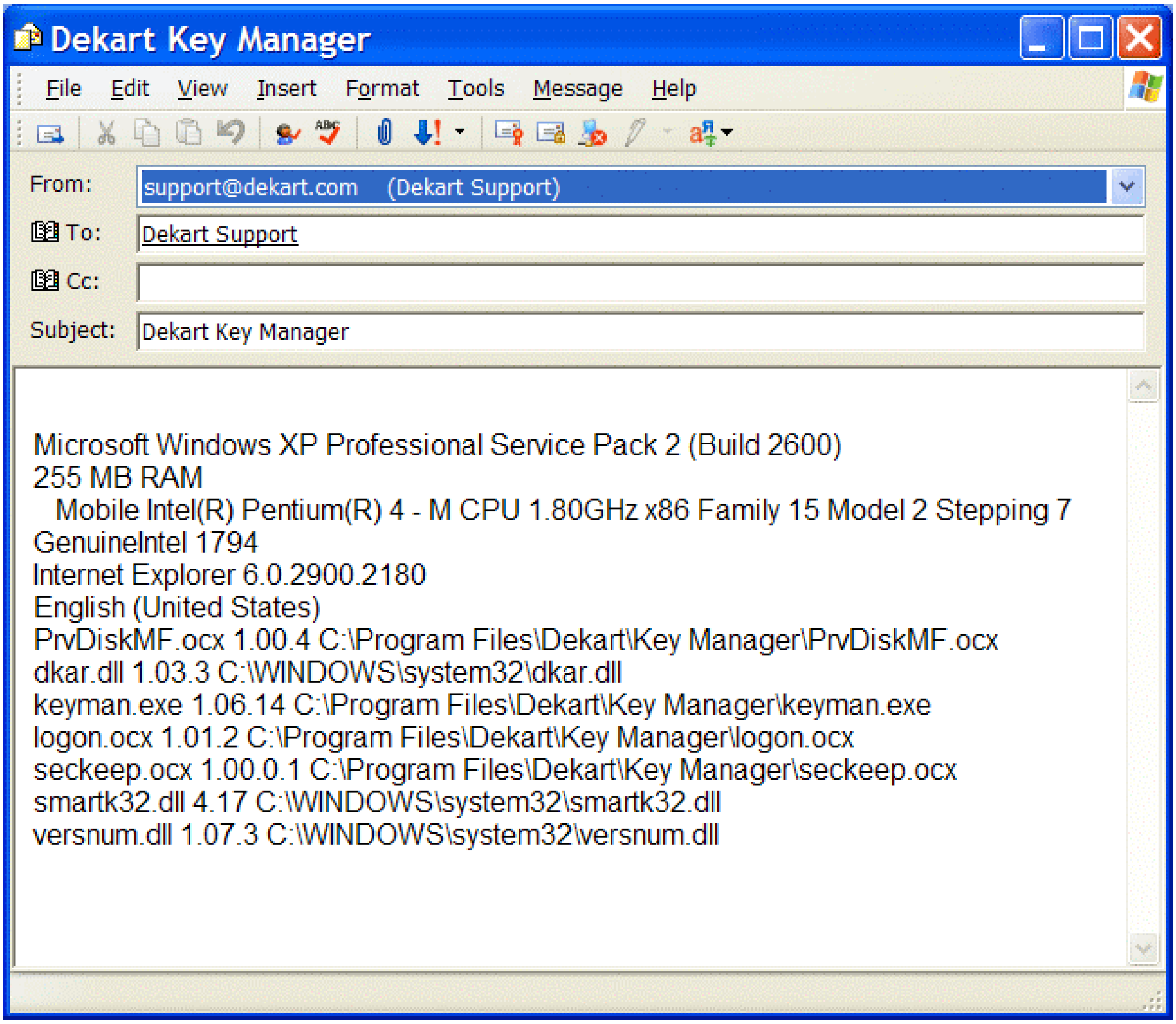
http://www.dekart.com support@dekart.com

Figure 45
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.



From: support@dekart.com (Dekart Support)

To: Dekart Support

Cc:

Subject: Dekart Key Manager

```
Microsoft Windows XP Professional Service Pack 2 (Build 2600)
255 MB RAM
  Mobile Intel(R) Pentium(R) 4 - M CPU 1.80GHz x86 Family 15 Model 2 Stepping 7
GenuineIntel 1794
Internet Explorer 6.0.2900.2180
English (United States)
PrvDiskMF.ocx 1.00.4 C:\Program Files\Dekart\Key Manager\PrvDiskMF.ocx
dkar.dll 1.03.3 C:\WINDOWS\system32\dkar.dll
keyman.exe 1.06.14 C:\Program Files\Dekart\Key Manager\keyman.exe
logon.ocx 1.01.2 C:\Program Files\Dekart\Key Manager\logon.ocx
seckeep.ocx 1.00.0.1 C:\Program Files\Dekart\Key Manager\seckeep.ocx
smartk32.dll 4.17 C:\WINDOWS\system32\smartk32.dll
versnum.dll 1.07.3 C:\WINDOWS\system32\versnum.dll
```

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.

Table1. **Diagnostic messages table**

##	Message	Explanation	Action
01	Data block could not be erased. You should delete data block instead of erasing its contents.	(Binary editor of the data block). Compete deletion of data block is not allowed. The data block size may not be zero.	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.
02	Not enough free space for new data block.	There is not enough free space on the hardware key for the new data block.	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.
03	Keyman.ini not found...	Configuration file Keyman.ini was not found in the source folder of Key Manager.	Re-install the application
04	# attempts left ...	The PIN code request dialog displays the number of remaining PIN code entry attempts.	Be careful with wrong PIN code entries, otherwise the hardware key will block after # of wrong entries.
05	No files were found .	(Search tab) File search did not produce any results.	Try searching again or change search criteria.
06	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.	(Binary editor of the data block). Attempting to paste from clipboard # bytes of data. Not enough space to perform this operation.	Try to paste smaller size data. The data block allowed sizes are specified in the “Size \ Available” field.
07	The Document could not be loaded. Too many opened files.	The document can not be opened. Too many documents opened at the same time.	Re-start Key Manager and try to open the document again.
08	An error occurred while loading Viewer Plug-in (#) for #.	Error loading Viewer Plug-in (#) for # data.	The Viewer Plug-in for this data block is not available or has been incorrectly installed. Re-install the application.
09	An error occurred while executing: #	Error calling external utility	Check the name and path to the external utility in keyman.ini file.
10	KeyMan.ini does not contain [Tools] section or KeyMan.ini not found	File KeyMan.ini not found or the [Tool] section is unavailable.	The KeyMan.ini file, section [Tool] contains data about external utilities. Re-install the application or add this section.
11	Unknown error with the Key!	Hardware key processing error.	Repeat the operation.
12	The Key is blocked!	(Right-hand information panel in hardware key status bar). Hardware key is blocked.	Unblock the hardware key by entering correct PIN code. Conventionally, the hardware key accepts only three PIN code entry attempts.
13	The Key is finally blocked! It should be reformatted to reuse.	(Right-hand information panel in hardware key status bar). Hardware key is permanently blocked. Reformatting the card is required.	To be able to use the hardware key, it has to be reformatted.
14	The Key you connected has not been formatted!	(Right-hand information panel in hardware key status bar). Hardware	Before using the hardware key with Dekart applications, the

	been formatted!	hardware key status bar). Hardware key has not been formatted.	with Dekart applications, the hardware key has to be formatted.
15	Unidentified Key or reader error!	(Right-hand information panel in hardware key status bar). Unknown hardware key type or smart card reader error.	Disconnect and then reconnect the hardware key and repeat the operation.
16	An error occurred while reading data from the Key!	Error reading data from the hardware key.	Restart the application and repeat the operation.
17	An error occurred while deleting # from the Key!	Error deleting data from the hardware key.	Restart the application and repeat the operation.
18	An error occurred while writing # to the Key!	Error writing data to the hardware key.	Restart the application and repeat the operation.
19	An error occurred while loading smartkey.dll	Error loading smartkey.dll library	smartkey.dll library has not been installed or PC\SC subsystem does not work on this computer.
20	Please enter PIN for the Key	(Right-hand information panel in hardware key status bar). Enter correct PIN code.	The user has cancelled entering PIN code while connecting the hardware key. Disconnect and then connect again the hardware key, enter PIN code.
21	An error occurred while #	Error processing the hardware key. Error description: #	Check if there is enough free space on hardware key to perform this operation. Repeat the operation.
22	Not enough free space on the Key!	Not enough free space in the hardware key memory.	The operation requires a free portion of memory on the hardware key.
23	An error occurred while changing PIN	Error changing PIN code.	Restart the application and repeat the operation.

Glossary

Term	Description
Application Programming Interface (API)	This is a software interface used for interaction between the *OS* and an application.
Basic Input/Output System (BIOS)	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.
International Organization for Standardization (ISO)	International Organization for Standardization
Authentication	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.
Biometric Authentication	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.
Two-Factor Authentication	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.
Driver	This is software designed to control data input/output and interface the applications/*OS* and the device connected to the *PC*.
Identification	This is a control process using a unique identifier to determine whether the specific user is known to the system.
One-Factor or Standard Authentication	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.
Registration	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.
Hardware key	A smart card or USB token where personal information is stored. The hardware key can be PIN code protected, or can work without PIN.
Encryption key	Specially built numerical sequence used to transform the source information into the encrypted data using a special algorithm.
PIN (Personal Identification Number)	Personal identification number that is used to access information stored on the hardware key. The PIN code length can be from 4 to 8

Identification Number)	characters, and should always be memorized, or be in the possession of only the hardware key holder.

Term	**Description**
OS	Operating System
PC	Personal Computer.
SW	Software