USER GUIDE

DEKART PRIVATE DISK MULTIFACTOR

Table of Contents

1 Preface

Dekart Private Disk MultiFactor is a software and hardware system designed to provide secured access to confidential information by converting the data storage of both desktops and laptops into a "false-bottomed" structure. The product allows a third party to see only what lies on the surface, leaving the secret data well-hidden and invisible. A special personalized electronic device – the smart card or the **Token** key, or another similar device – provides access to the confidential information. Every legitimate product user should obtain such a device and keep it safe.

1.1 Operating Guide Structure

This *Guide* consists of the following chapters:

- Introducing Dekart Private Disk MultiFactor describes the purpose and the features of **Dekart Private Disk MultiFactor** and its integration with the removable devices.
- Dekart Private Disk MultiFactor Hardware and Software Requirements lists and describes PC software and hardware required for **Dekart Private Disk MultiFactor** to operate properly as well as the product software and hardware requirements.
- Dekart Private Disk MultiFactor Installation, Update and De-Installation describes in detail how to install, update and de-install the product and its auxiliary components.
- Operating Dekart Private Disk MultiFactor thoroughly describes all the aspects of operating the product’s use.
- Troubleshooting is devoted to detecting and eliminating possible the problems that may occur when in using the product operation. 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*.

1.2 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***.

1.3 Operating Guide Purpose

This *Operating Guide* is designed for **Dekart Private Disk MultiFactor** users and contains information about installing, operating and de-installing this product.

This *Guide* contains the list of computer hardware and software requirements required to provide the by the product to operate properlyproper operation of **Dekart Private Disk MultiFactor**. It also describes how to use all of the product system elements:

- Smart cards, corresponding readers, the **Token** devices, USB drives, etc.
- **Dekart Private Disk MultiFactor** program modules and the corresponding functions.

1.4 License and trademarks information

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 USE THE SOFTWARE; INSTEAD, RETURN THE PACKAGE TO THE COMPANY FROM WHICH YOU RECEIVED IT AND YOU WILL RECEIVE A FULL REFUND IF YOU: (A) DO NOT USE THE SOFTWARE AND (B) RETURN IT WITH PROOF OF PAYMENT WITHIN THIRTY (30) DAYS OF THE PURCHASE DATE.

1. DEFINITIONS. "Software" means (a) all of the contents of the files, disk(s), CD-ROM(s) or other media with which this Agreement is provided, including but not limited to (i) Dekart or third party computer information or software; (ii) related explanatory written materials or files ("Documentation"); and (iii) fonts; and (b) upgrades, modified versions, updates, additions, and copies of the Software, if any, licensed to you by Dekart (collectively, "Updates"). "Use" or "Using" means to access, install, download, copy or otherwise benefit from using the functionality of the Software in accordance with the Documentation. "Dekart" means Dekart SRL, having its legal address at Alba Iulia 75, Chisinau, MD 2071, Moldova, and / or its affiliates/branches.

2. GRANT OF LICENSE. As long as you comply with the terms of this Agreement, Dekart grants to You a non-exclusive, non-transferable right for Your internal use to Use the Software in a quantity necessary for its intended purposes described in the Documentation. The Software may include or be bundled with other software programs licenses under different terms and/or licensed by a vendor other than Dekart. Use of any software programs accompanied by a separate license agreement is governed by that separate license agreement. Any third party software that may be provided with the Software is included for use at Your option. Dekart is not responsible for any third party's software and shall have no liability for Your use of third party software.

2.1. With the STANDARD SINGLE-USER License Dekart grants you with the right to use the accompanying Dekart Software and any of its updates that you may receive on a single terminal connected to a single computer (i.e., with a single CPU). You may, however, install the Software on more than one computer provided you do not operate the Software on more than one computer or computer terminal at a time. In case the user needs to deploy the purchased software on several computers simultaneously another license has to be purchased, namely Multi-User License or the user may alternatively select to have a separate license key per each terminal.

2.2. MULTI-USER, NETWORK LICENSE. You may use the Software on a network only if a separate copy of the Software has been licensed from Dekart for each terminal and/or CPU capable of executing the Software. Otherwise, if you desire to use the Software on a network or multi-user system, or to install the Software on multiple single-user CPUs, you must first obtain written multi-user authorization (a "Multi-user License") from Dekart. Under a Multi-user License, you may install the Software on networks and/or multiple single-user CPUs, provided the total concurrent network usage or total number of network installations (whichever is greater), plus the total number of single-user installations, does not exceed the total number of machines/users authorized by Dekart. The Multi-User License Key consists of a standard combination of 25 symbols plus 5 more symbols which indicate the overall number of users authorized by Dekart with this particular license.

3. EVALUATION. If the Software is an evaluation version or is provided to You for evaluation purposes, then Your license to use the Software is limited solely to internal evaluation purposes in accordance with the terms of the evaluation offering under which You received the Software and expires 30 days from installation (or such other period as indicated by the Software) and the Software may cease to function. Upon expiration of the evaluation period, You must discontinue use of the Software and delete the Software entirely from Your system. The Software may contain an automatic disabling mechanism that prevents its use after a certain period of time, so You should back up Your system and take other measures to prevent any loss of files or data.

4. REFUNDS. Products that can be downloaded prior to the purchase are NOT refundable. Optionally, our technical support team can decide that an exception to the rule can be made, after an examination of the problem. You have the chance to 'try before you buy'. We would like to emphasize that the evaluation period is an important phase and we encourage you to explore the programs and try all their options before the purchase. If you have not tested the fully-functional, free evaluation versions that can be retrieved from our download site(s), PLEASE do so before you place your order to make sure that the product you are ordering is the product you need.

5. INTELLECTUAL PROPERTY RIGHTS. The Software and any copies that You are authorized by Dekart to make are the intellectual property of and are owned by Dekart. No title to or ownership of the Software is transferred to You. Dekart owns and retains all title and ownership of all intellectual property rights in the Software, including any adaptations or copies. You acquire only a license to use the Software. The structure, organization and code of the Software are the valuable trade secrets and confidential information of Dekart. The Software is copyright protected.

6. NON-DEKART PRODUCTS. The Software may include or be bundled with hardware or

other software programs licensed or sold by a vendor other then Dekart. Any such products are provided on and "AS IS" basis and are not warranted by Dekart. Any warranty service for non-Dekart products is provided by the product vendor in accordance with the applicable vendor warranty.

7. LIMITED WARRANTY. Dekart warrants to You that for ninety (90) days from date of purchase (the "Warranty Period): (a) the media on which the Software is stored will be free of defects; (b) the Software will substantially conform to the Documentation accompanying the Software. If the defective item(s) are returned to Dekart or if You send an error report(s) to Dekart within the Warranty Period, Dekart will at its sole discretion either resolve the problem(s), or replace the Software, or refund the license fees You paid for the Software. Any misuse or unauthorized modification of the Software voids this warranty. The warranty referenced above is Your sole and exclusive remedy and is in lieu of all other warranties, express or implied. The warranty referenced above does not apply to Software provided free of charge. Such Software is provided "AS IS" without any warranties of any kind. The Software is not designed, manufactured or intended for use of distribution with on-line control equipment in hazardous environments requiring fail-safe performance. Such as in the operation of nuclear facilities, aircraft navigation, communication, or control systems, direct life support machines, weapons systems, or other uses in which failure of the software could lead directly to death, personal injury, or serve physical or environment damage.

8. LIMITATION OF LIABILITY. IN NO EVENT WILL DEKART BE LIABLE TO YOU FOR ANY DAMAGES, CLAIMS OR COSTS WHATSOEVER OR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL DAMAGES, OR ANY LOST PROFITS OR LOST SAVINGS, EVEN IF AN DEKART REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS, DAMAGES, CLAIMS OR COSTS OR FOR ANY CLAIM BY ANY THIRD PARTY. THE LIMITATIONS AND EXCLUSIONS REFERENCED ABOVE APPLY TO THE EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION. DEKART'S AGGREGATE LIABILITY UNDER OR IN CONNECTION WITH THIS AGREEMENT SHALL BE LIMITED TO THE AMOUNT PAID FOR THE SOFTWARE, IF ANY. The above exclusions and limitations will not apply to claims relating to death or personal injury. In those jurisdictions that do not allow the exclusion or limitations damages, Dekart's liability shall be limited or excluded to the maximum extent allowed within those jurisdictions.

9. EXPORT RESTRICTION. You will comply fully with all applicable laws and regulations of United States and other countries ("Export Laws") to assure that Software is not: (a) exported, directly or indirectly, in violation of Export Laws; or (b) used for any purpose prohibited by Export Laws.

10. GOVERNING LAW. Any use of the program which is illegal under international or local law is forbidden by this license. Any such action is the sole responsibility of the person committing the action.

11. TERM. This Agreement becomes effective on the date You legally acquire the Software and will automatically terminate if You breach any of its terms. Upon termination of this

Agreement, You must destroy the original and all copies of the Software or return them to Dekart and delete the Software from Your system(s).

12. NO SPYWARE. The Dekart software does not contain spyware of any kind. It does not install any tracking software on your system, or collect personal information about you and your browsing habits. Dekart software does not "spy" on other programs you run or web sites you visit. We also don't serve monitor usage or serve ads from the client software. The Dekart software does not come bundled with any third party software.

13. ROOT CERTIFICATE INSTALLATION. In order to offer our users a secure connection environment a root CA certificate is installed into the Trusted Root Certificate Authorities store. Having this certificate installed the users can safely access our website via SSL/HTTPS connection protocols and send or receive any sensitive information (e.g. names, addresses, etc) without the threat for these data being seen. This allows our users to securely register their license keys at Dekart website, submit their support requests to Dekart and ensure the privacy of the information transmitted over the web. DEKART CERTIFICATE POLICY. We hold ourselves fully liable to our customers for the privacy of their personal information. You may rest assured that we will never, under any circumstances, voluntarily or willingly disclose any information to any third party. That is our guarantee to you.

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

DEKART SRL CONTACT INFORMATION

E-mail:

	for sales details:	sales@dekart.com
	for product support:	support@dekart.com
	for comments and feedback:	info@dekart.com
WWW:		www.dekart.com

1.5 How to Contact Dekart

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

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

2 Introducing Dekart Private Disk MultiFactor

This chapter describes the purpose and features of **Dekart Private Disk MultiFactor**: the explanation of the main aspects of strong user authentication provided by this product:

- Identification;
- Authentication;
- Strong Authentication;
- Two-Factor Authentication.

2.1 How Does Dekart Private Disk MultiFactor Protect Information?

To use **Dekart Private Disk MultiFactor** effectively, take the following preparatory steps:

1. **Study this Guide thoroughly**.
2. **Obtain an electronic Key**. Keep it safe, do not lose or damage the Key. You will not be able to access your data without this Key, just as you will not open the door to your home without the right Key. Do not entrust your Key to anyone else.
3. **Prepare the computer**. The preparation consists of , by installing the product onto the PC .
4. **If required, set the Personal Identification Number (PIN) by accessing the applicable dialog box to strengthen authorized access control to your virtual disk**. Only the right Key can provide access to the information stored on your virtual disk. Memorize your Key PIN and do not write it down where it can be easily discovered. **Dekart Private Disk MultiFactor** provides special utilities to change your PIN. For directions on changing your PIN, Operating Dekart Private Disk MultiFactor. Be sure not to forget the PIN and keep it secure. If a third party finds out your **Token** PIN and has your **Token** Key, they will be able to access your data.

Thereafter, you can start working with **Dekart Private Disk MultiFactor**. It is very easy, because the product modules do not change the way you normally work with the Windows operating system.

2.1.1 How Does the Product Protect the Workplace?

Let us consider how **Dekart Private Disk MultiFactor** locks the door to information during the temporary interruptions of work, for example, when you leave your office. The door can shut and lock automatically! But only under the two following conditions — the software must be set up in accordance with certain parameters and the Key must be removed. The software will detect this event and lock your virtual disks.

Naturally, you will have to insert the electronic Key and, if required, pass authenticatione yourself on when returning to your workplace.

For more details on re-authentication after returning to your workstation, see Operating

Dekart Private Disk MultiFactor.

2.1.2 How Does the Product Protect Confidential Data?

Dekart Private Disk MultiFactor allows you to create virtual secret disks in Windows and work with them as with conventional disks. A virtual Private Disk MultiFactor is no more than a usual file — a so-called *disk image file*, storing all of the encrypted data. After accessing the image file by means of **Dekart Private Disk MultiFactor**, the operating system detectsermines it as a normal disk and assigns to it a corresponding letter to it. For example, if your system had drives defined by the letters **C:** and **D:**, then the letters X**:, Y:** or any other will appear upon accessing the Private Disk MultiFactor. All of the programs that you are accustomed to working with will not be affected in any way when using a standard and virtual disks. For them, this will be just another hard disk. The image file of a virtual disk can have any name, extension, and access path (even a network paths are valid as well). Accessing the Private Disk MultiFactor and working with the secret data are is only possible only when the right electronic Key is available. This device stores the cryptographic data encryption key and the full name of the virtual Private Disk MultiFactor image file.

Installing **Dekart Private Disk MultiFactor** is easy, and should not take longer than 5 minutes. **Dekart Private Disk MultiFactor** is easy to operate — upon loading it will prompt two modes of access to Private Disk MultiFactors.

1. **Simplified automatic mode.** In this mode, inserting the electronic Key into the reader or attaching it to the USB port is enough to access the Private Disk MultiFactor. Disk access is discontinued when the Key is removed. In this mode, one-factor authentication is used and the security is not as strong as in the mode that follows.
2. **Strong authentication mode.** In this mode, two-factor authentication is used to access the Private Disk MultiFactor. The distinguishing feature from the simplified mode is that this mode provides strong protection: even if a third party obtains your Key, they will be unable to take advantage of it without your PIN.

Encrypting confidential information is easy — simply transfer it from any media (other disks or the same computer, or floppies, Zip drives, etc.) to the Private Disk MultiFactor and remember to store your new confidential data on this disk too, while storing non-sensitive information on any other disks. The ***Advanced Encryption Standard*** (***AES)*** in ***CBC*** mode with 256 bit key length is used as the virtual disk encryption algorithm. *Is this encryption key reliable*? Yes! According to the estimates of *Bruce Schneier*, *Applied Cryptography*, fitting the encryption key 128 bit long requires 4.2x10^22 processors performing 256 million encryption operations per second. But even in this case, the key will be cracked in a year.

For more details on operating the product, please refer to Operating Dekart Private Disk MultiFactor.

2.2 Dekart Private Disk MultiFactor Capabilities

Dekart Private Disk MultiFactor has the following capabilities:

- Standard ***AES*** in ***CBC*** mode with 256 bit key length is used as an encryption algorithm.
- The electronic Key with the cryptographic hashing function **SHA** is used to generate random chains.
- The minimum volume of a virtual secret disk is 1 MB, the maximum volume is 2.1 GB under **Windows 95**, **Windows 98**, **Windows ME** and 1 TB under **Windows NT**, **Windows 2000**, **Windows 2003, Windows XP**.
- PIN length: the minimum PIN length is 0 alphanumeric symbols and the maximum length is 8 symbols.
- Smart card readers complying with the *PC/SC* specifications are supported.

2.3 Dekart Private Disk MultiFactor Components

Dekart Private Disk MultiFactor consists of the following mandatory components:

- the CD with the product program modules,
- *Operating Guide*.

The following optional components can also be shipped with **Dekart Private Disk MultiFactor** package (depending upon the delivery option):

- one of the following sets of the electronic Keys (depending upon the delivery option):
- Microsoft software for smart cards support,
- the **RTE** containing drivers and utilities for the **eToken** Key support,
- smart card reader or USB Token drivers.

2.4 Supported key storage and biometric devices

Dekart Private Disk MultiFactor supports the following devices:

Key Devices:

USB tokens

* ActivCard ActivKey USB token series
* Aladdin eToken R2 USB token series
* Aladdin eToken PRO USB token series
* Algorithmic Research MiniKey USB token series
* Eutron CryptoIdentity ITSEC USB token series
* Eutron CryptoIdentity 4 USB token series
* Eutron CryptoIdentity 5 USB token series
* Rainbow iKey 1000 USB token series

* Rainbow iKey 2000 USB token series
* Rainbow iKey 3000 USB token series
* ruToken USB token series

Smart cards

* ACOS1 smart card series
* Algorithmic Research PrivateCard smart card series
* Athena ASECard smart card series
* Datakey Model 310 smart card series
* Datakey Model 330 smart card series
* GemPlus GPK smart card series
* GemPlus MPCOS EMV smart card series
* Giesecke & Devrient STARCOS S smart card series
* Giesecke & Devrient STARCOS SPK smart card series
* Schlumberger Cryptoflex smart card series
* Schlumberger Multiflex smart card series
* Schlumberger Payflex smart card series
* Siemens CardOS M 4 smart card series
* SMARTCOS smart card series

Other devices
USB flash drives, CD-R/RW disks and other portable storage devices

You can use the electronic Key for simultaneous work with several applications.

Smart card readers

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

* ACS ACR series smart card readers
* Datakey DKR smart card reader series
* GemPlus GemPC smart card reader series
* OmniKey CardMan smart card reader series
* Schlumberger Reflex smart card reader series
* Towitoko CHIPDRIVE smart card reader series

Dekart Private Disk MultiFactor allows to share the smart card reader with different applications.

Biometric verification devices

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

* AET60 BioCARDKey

* BioLink U-Match MatchBook
* BioLink U-Match Mouse
* Precise Biometrics Precise 100 fingerprint and smart card reader series
* SCM SCR222 fingerprint reader
* Veridicom FPS100
* Veridicom FPS110
* Veridicom FPS200

Please, refer to the List of supported devices at www.dekart.com.

Note 1. Before you purchase a USB token or smart card, please make sure that it has enough memory to store the required user data. Please, take into account that the a part of Key memory may be allocated to other data, e.g. BIO ID. You can determine the memory usage of the card and read the USB token or smart card using the Dekart Key Manager Utility. This utility also allows you to , as well as delete all the unnecessary information

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

2.4.1 Using Electronic Keys with Different Applications

The current version of the electronic Key format allows you to use the electronic Key for simultaneous work with several applications, because one Key can store the data of several electronic Key-oriented software products. These can be the products can be developed by **Dekart,** or and other vendors.

Dekart software products generally utilize the ***Dekart Smart Key*** system specially designed by **Dekart** But sometimes the electronic Key can be used with the products of other companies. For example, if the **Cryptoflex for Windows 2000** smart card is shipped together with **Dekart Private Disk MultiFactor**, it can be simultaneously used by both standard **Windows 2000** applications and by **Dekart Private Disk MultiFactor**.

This feature allows the user of **Dekart Private Disk MultiFactor** to purchase the Key-oriented software from other vendors without paying extra for additional hardware compatible with the electronic Keys for **Dekart Private Disk MultiFactor**.

2.4.2 Using a Smart Card Reader with Different Applications

Dekart Private Disk MultiFactor allows you to share the smart card reader with different applications if one of the following conditions is met:

- The product operates with the control panel off. For more information about this mode, please refer to the section Connecting/Disconnecting the Virtual Secret Disk .

- The product is deactivated (See the section Product Operation Completion).

If any messages appear in the first mode, they can be simply closed by pressing ***Esc***, and the smart card can be further used further with a different application.

3 Dekart Private Disk MultiFactor Hardware and Software Requirements

Dekart Private Disk MultiFactor is a compact product integrated with the electronic Keys hardware produced by third parties.

This chapter describes the following:

- **Dekart Private Disk MultiFactor** PC hardware requirements.
- Operating systems with the corresponding service packs required for the product to run properly.

3.1 PC Hardware Requirements

Dekart Private Disk MultiFactor does not have any specific hardware requirements, most of the existing requirements target the operating system of your computer.

For **Dekart Private Disk MultiFactor** to run properly, a PC with the following minimum configuration is required:

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

In addition to this, the PC must be equipped with one of the following ports to connect the electronic Keys:

- A USB port, if the electronic Key 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.

One of the following hardware components is required if only the **Private Disk MultiFactor** software component has been purchased from **Dekart** (without electronic Keys and a corresponding reader):

- The **eToken R2** or the **eToken PRO** Key with sufficient memory capacity.
- Smart card reader complying with the *PC/SC* specification connected to the computer.
- If you prefer to use three-factor authentication, a biometric device is needed, e.g. BioLink U-Match Mouse.

3.2 PC Software Requirements

One of the following operating systems is required for **Dekart Private Disk MultiFactor** to run properly on a PC:

- Windows95 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 2003 (32- and 64-bit versions).
- Windows XP Professional, Home Edition (32- and 64-bit versions).

If the electronic Keys have been purchased separately from **Dekart Private Disk MultiFactor**, for example, as a part of a different product, then one of the following software components must be installed on the PC:

- **eToken** Key software — **RTE** (**eToken** Run Time Environment) version 2.65 or higher. The latest version of the **RTE** software can be downloaded from Aladdin Knowledge Systems Web site at www.ealaddin.com.

  Microsoft Windows Installer (*MSI*) is required to install the **RTE** under Windows 95/98/NT. This permits the system to run the MSI files (this is the format of the *RTE* installation module). It can be downloaded from http://support.microsoft.com/downloads/.
- The electronic Key and biometric device software for the corresponding Windows OS (the drivers and utilities set). For more details and new versions of software, refer to the vendor of the reader or to the Web site of the company producing the readers.

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

4 Dekart Private Disk MultiFactor Installation, Update and De-installation

Note: In order to install the product components under Windows operating systems designed for corporate use — Windows NT, Windows 2000/2003, Windows XP — he process must be carried out by an a user with administrator privileges.

This chapter thoroughly describes the user actions during the process of **Dekart Private Disk MultiFactor**'s components installation:

- First, the auxiliary product components are installed into the system — the electronic Key, biometric device.
- Next, the main product components are installed.

This chapter also describes the user actions during **Dekart Private Disk MultiFactor** update and de-installation.

4.1 Product Installation

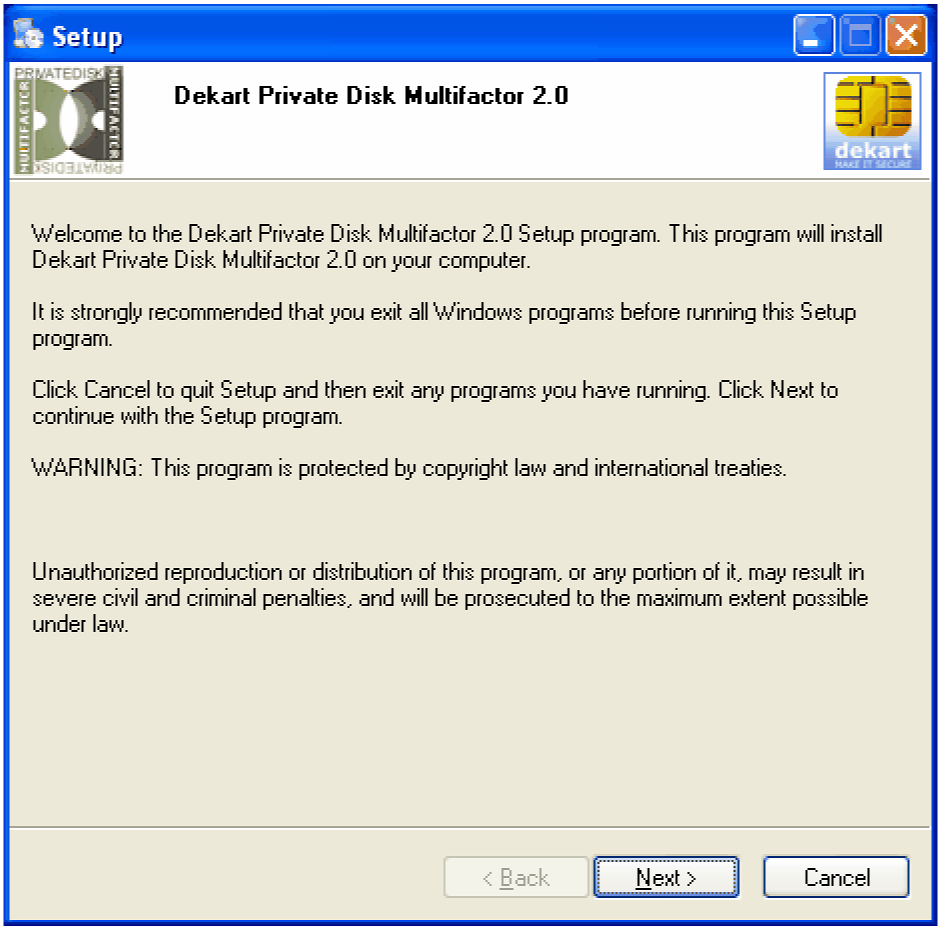
Note: In order to install the product components on a computer running Windows NT, Windows 2000/2003, Windows XP, the process must be carried out by an a user with administrator privileges.

Note: Before beginning the installation of the software, you must close all the open applications. If you intend to use a USB flash disk If you intend to use a USB flash disk as a Key, make sure that is properly connected and configured.

Note: In order to enable three-factor authentication, the biometric device should be connected and its drivers should be installed.

Do the following to install **Dekart Private Disk MultiFactor**:

1. Insert **Dekart Private Disk MultiFactor** product CD into the CD-ROM drive. The product installation module will run automatically. The installation menu will appear on the screen. If this menu does not appear, launch the SETUP.EXE module from the CD manually. If you have downloaded the installation file from the Internet, please run PrvDiskmf.exe
2. The installation program’s installation will appear.



Welcome to the Dekart Private Disk Multifactor 2.0 Setup program. This program will install Dekart Private Disk Multifactor 2.0 on your computer.

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

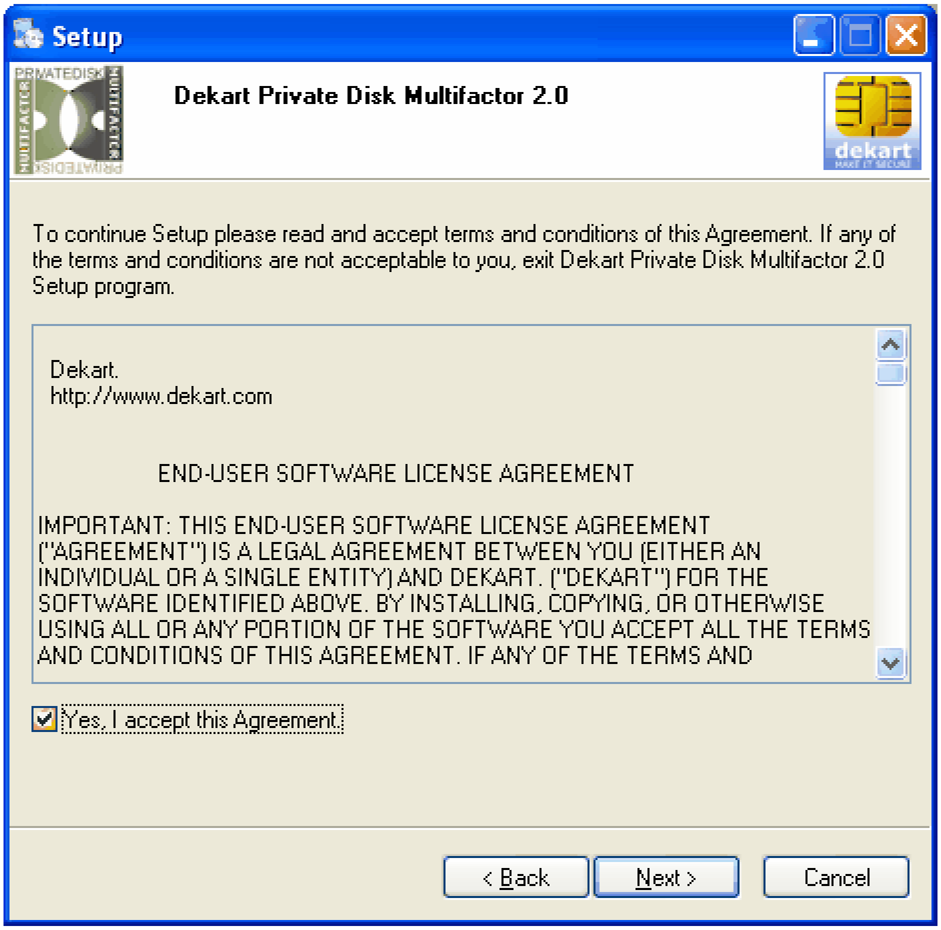
Click Cancel to quit Setup and then exit any programs you have running. Click Next to continue with the Setup program.

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.

Dekart Private Disk MultiFactor installation program welcome screen

3. Click ***Next*** on the welcome screen. The ***License Agreement*** window will appear.



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 Private Disk Multifactor 2.0 Setup program.

Dekart.
http://www.dekart.com

END-USER SOFTWARE LICENSE AGREEMENT

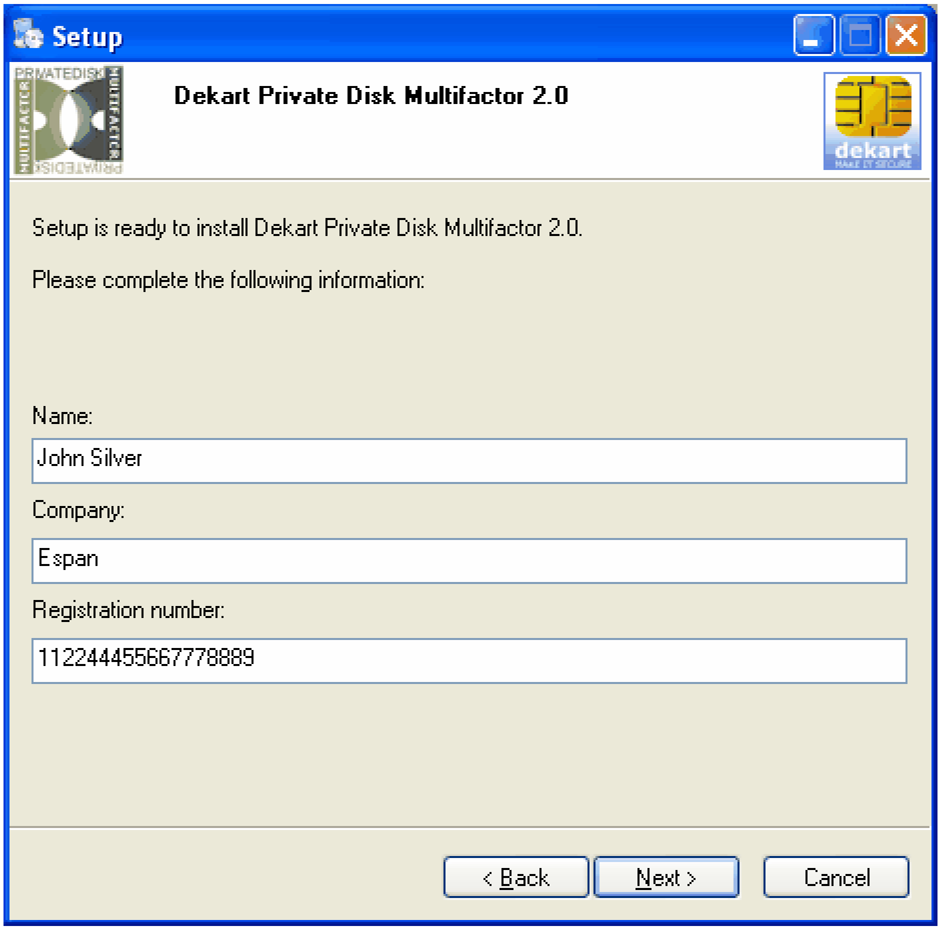
IMPORTANT: THIS END-USER SOFTWARE LICENSE AGREEMENT ("AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AND DEKART. ("DEKART") FOR THE SOFTWARE IDENTIFIED ABOVE. BY INSTALLING, COPYING, OR OTHERWISE USING ALL OR ANY PORTION OF THE SOFTWARE YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF ANY OF THE TERMS AND

☑ Yes, I accept this Agreement

Dekart Private Disk MultiFactor License Agreement window

4. Carefully read the text of the license agreement between you, the **Dekart Private Disk MultiFactor** 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.

   Note: If you do not agree with the terms of the license agreement, *do not select* the check box and click ***Cancel***. In this case, the product installation will be terminated.



Setup is ready to install Dekart Private Disk Multifactor 2.0.

Please complete the following information:

Name:
John Silver

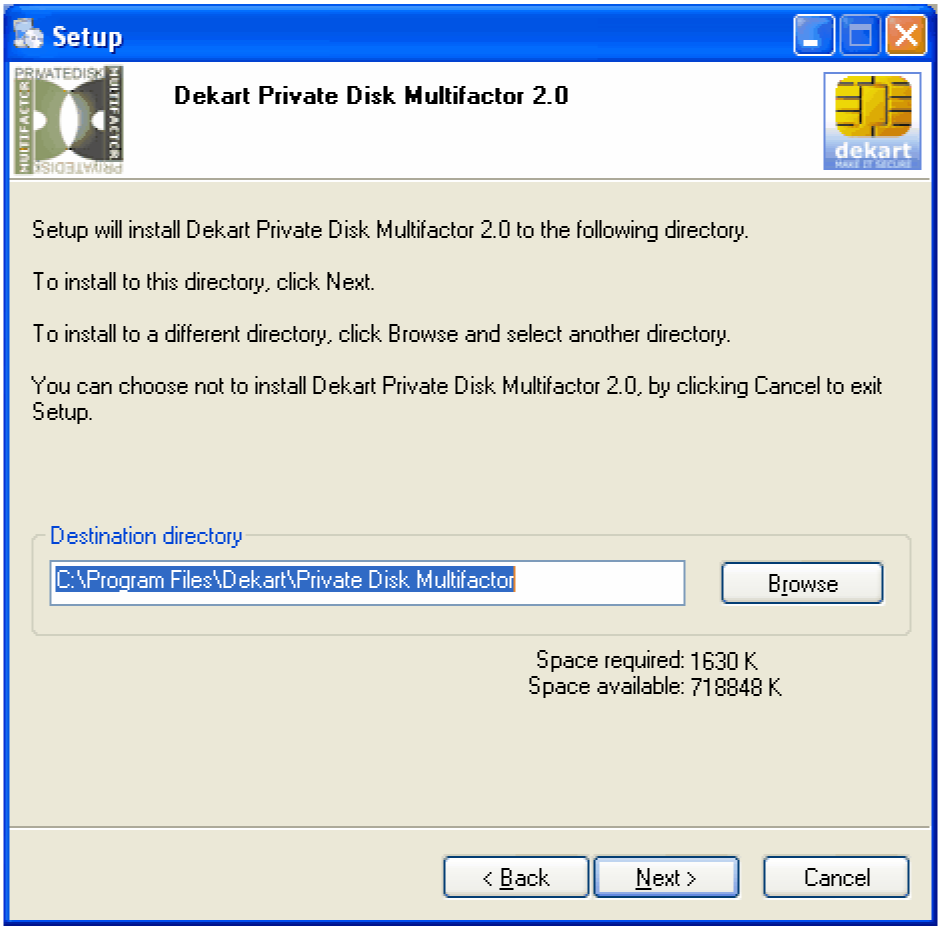
Company:
Espan

Registration number:
1122444555667778889

Dekart Private Disk MultiFactor registration window

5. Fill out the fields in the registration window and click ***Next***. A product location selection screen will appear.

   Note: The registration number of your **Dekart Private Disk MultiFactor** copy must be entered into the ***Registration Number*** box. You can find this number on the product box.



Setup will install Dekart Private Disk Multifactor 2.0 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 Private Disk Multifactor 2.0, by clicking Cancel to exit Setup.

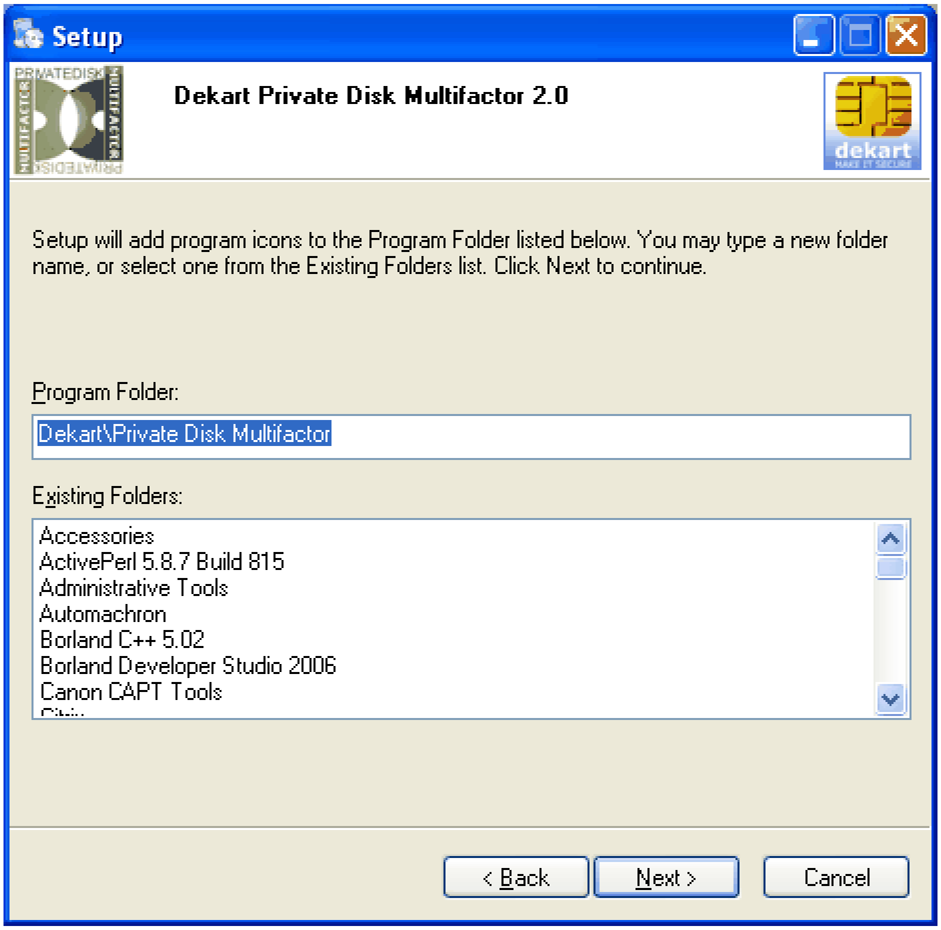
Destination directory

C:\Program Files\Dekart\Private Disk Multifactor

Space required: 1630 K
Space available: 718848 K

Dekart Private Disk MultiFactor installation path

6. Indicate the directory to which **Dekart Private Disk MultiFactor** should be installed on your computer and click ***Next***. A program folder selection screen will appear.



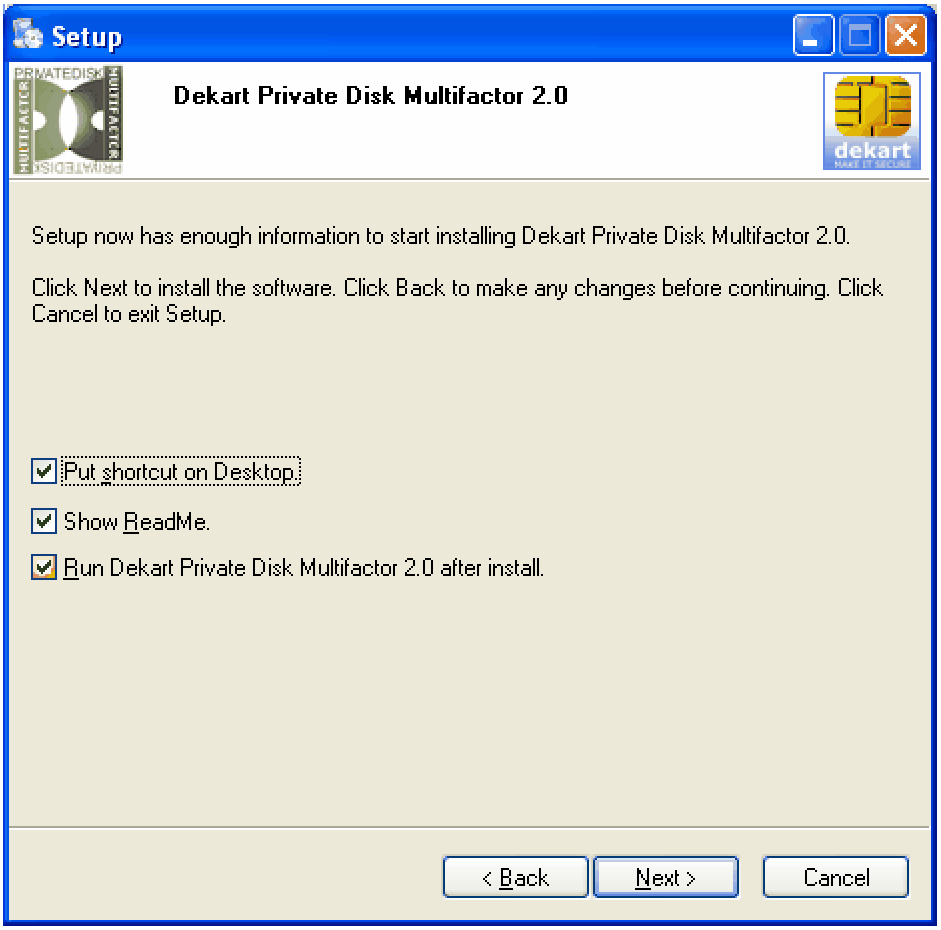
Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the Existing Folders list. Click Next to continue.

Program Folder:
Dekart\Private Disk Multifactor

Existing Folders:
Accessories
ActivePerl 5.8.7 Build 815
Administrative Tools
Automachron
Borland C++ 5.02
Borland Developer Studio 2006
Canon CAPT Tools

Dekart Private Disk MultiFactor folder

7. Indicate **Dekart Private Disk MultiFactor** folder name on your computer and click ***Next***. A ***Ready to Install*** window will appear.



Setup now has enough information to start installing Dekart Private Disk Multifactor 2.0.

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

☑ Put shortcut on Desktop.

☑ Show ReadMe.

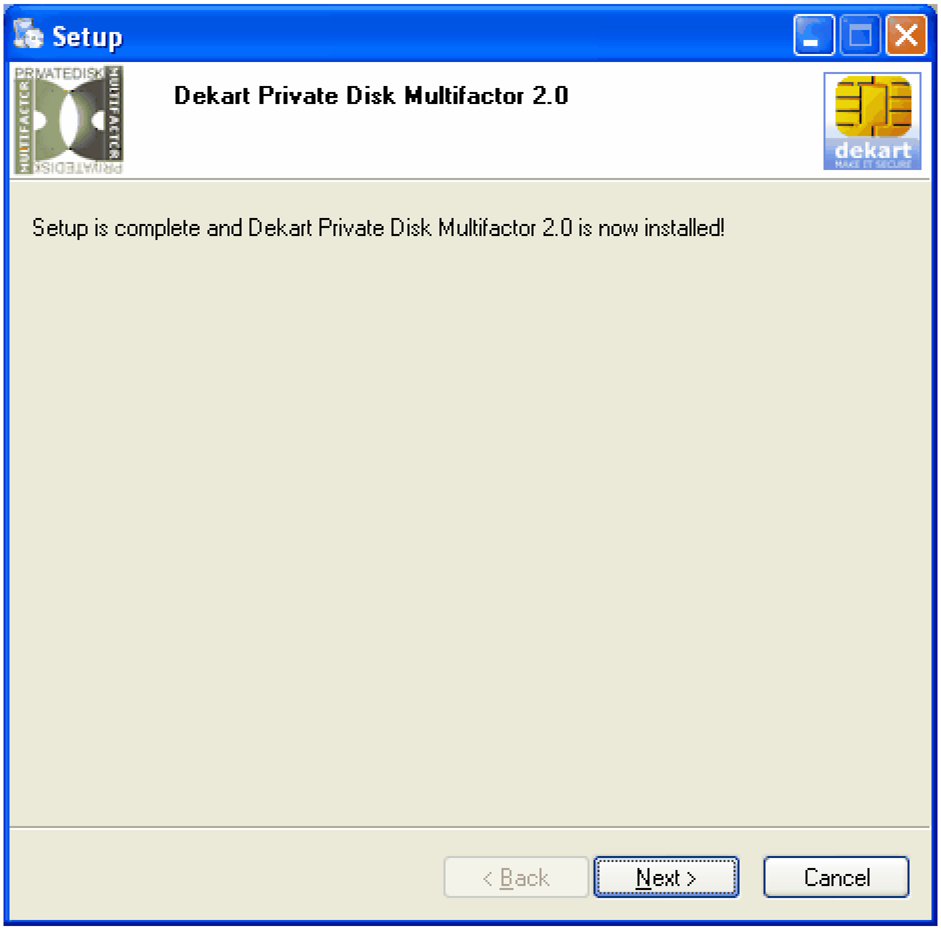
☑ Run Dekart Private Disk Multifactor 2.0 after install.

Starting the installation

8. Please, select the installation options (creating the application icon on desktop, displaying readme.txt, running Dekart Private Disk MultiFactor after installation) and click ***Next*** to start copying the product files.

   Note: If any additional system components need to be installed during the installation, insert the Windows operating system CD into the CR-ROM drive or indicate the folder with the copy of this CD. Follow directions on the screen.

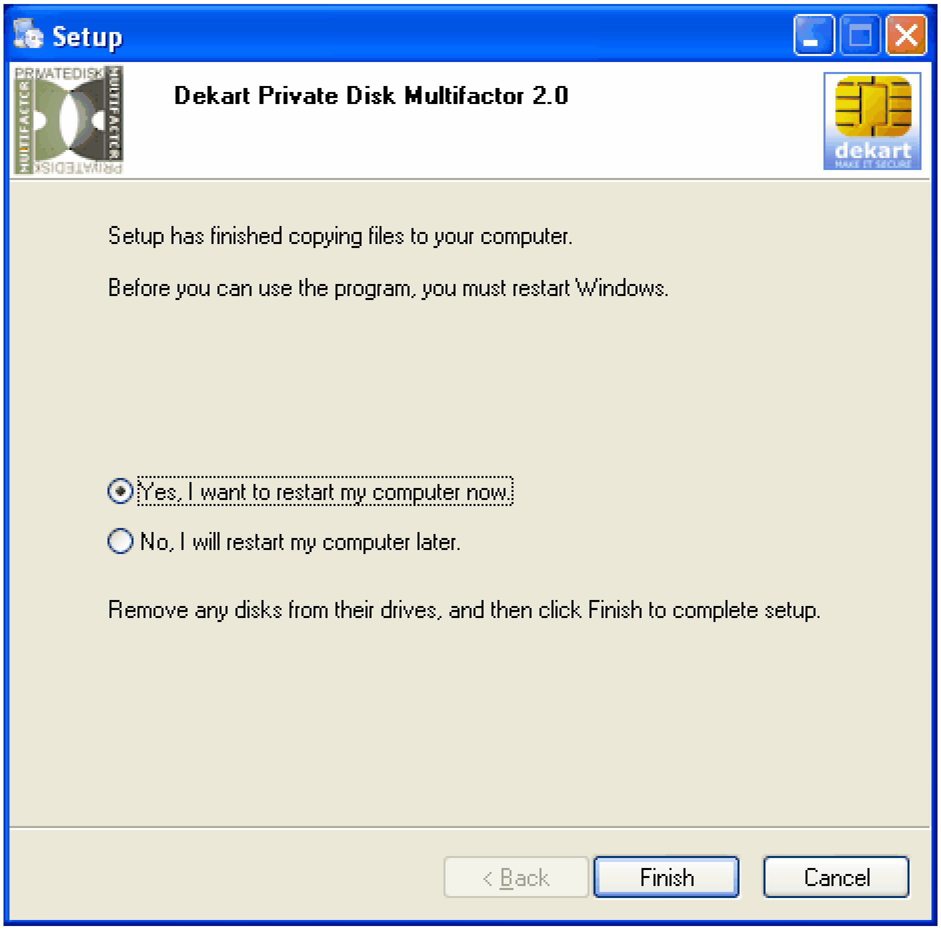
9. Wait until the installation completion window appears.



Setup is complete and Dekart Private Disk Multifactor 2.0 is now installed!

Installation completion window

10. Click ***Next***.
11. All of the system changes enabled by the installation will take effect after restarting the computer. Restart the computer automatically now (select **Yes)** or restart it manually later (select **No)**. Click ***Finish***.



Setup has finished copying files to your computer.

Before you can use the program, you must restart Windows.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

Restart invitation window

If you have selected the ***Create the desktop icon***, the application icon will then appear on your Desktop.

Note. If you wish to install Private Disk Multifactor to a removable drive (Flash drive), see Installation to removable disk

4.2 Re-Installing Dekart Private Disk MultiFactor

The user can re-install **Dekart Private Disk MultiFactor**. This may be necessary in the following cases:

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

To re-install the product, start the SETUP.EXE file from the **Dekart Private Disk MultiFactor** product CD and select ***Install Dekart Private Disk MultiFactor*** from the main menu or run PrvDiskmf.exe. Further actions are similar to those described in the Product Installation section of this chapter.

After re-installing, please, restart your computer.

4.3 Updating Dekart Private Disk MultiFactor

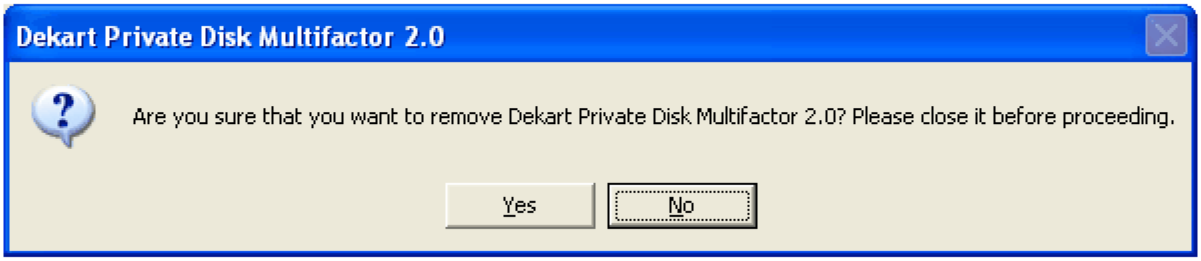
Dekart Private Disk MultiFactor can be updated when a newer version of the product is available.
An updated version of the product can be copied from our site: http://www.dekart.com. You can also obtain it by contacting our support team and providing your registration number.
A notification about a newer version will pop-up when you start the program. By clicking the link in the pop-up window, you will be redirected to the download section of our site.
The "check for updates" feature can be disabled by clearing the respective checkbox in the "Options" tab. To install the newer version of the product on the computer, start the SETUP.EXE file from the product CD of the newer version of **Dekart Private Disk MultiFactor** and select ***Install Dekart Private Disk MultiFactor*** from the main menu or run PrvDiskmf.exe. The installation utility will find the current version of the product and will suggest you to update it. Further actions are similar to those described in the Product Installation section of this chapter.
After the update, please, restart your computer.

Note. If **Dekart Private Disk MultiFactor** was previously installed on the removable drive, you need to perform actions described in the section Installation to removable disk

4.4 De-Installing Dekart Private Disk MultiFactor

Under certain conditions, you may need to de-install **Dekart Private Disk MultiFactor**. Do the following to de-install it with the standard Windows OS facilities:

1. Exit **Private Disk MultiFactor** (if it is active).
2. Choose **Uninstall** from the **Private Disk MultiFactor** group in the **Start Menu** (**Start > Programs > Dekart > Private Disk MultiFactor)**. OR Use the ***Add/Remove Programs*** dialog from Control Panel to remove the program ***(Start*** > ***Settings*** > ***Control Panel).***
3. After this the system will ask you to confirm the product de-installationyor intention.

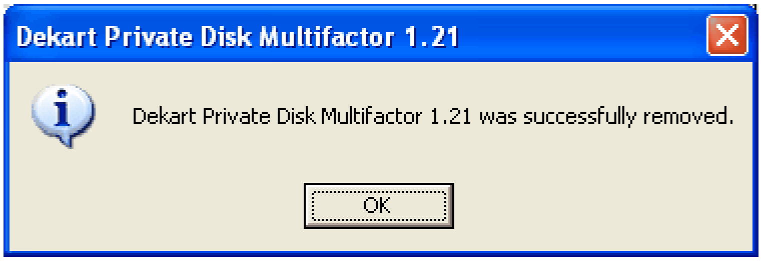

Dekart Private Disk Multifactor 2.0

Are you sure that you want to remove Dekart Private Disk Multifactor 2.0? Please close it before proceeding.

Dekart Private Disk MultiFactor de-installation confirmation

4. Upon clicking ***Yes***, the system will delete the previously installed product modules and report about the successful de-installation completion.

Note: Clicking ***No***, will cancel the de-installation procedure.


Dekart Private Disk Multifactor 1.21

Dekart Private Disk Multifactor 1.21 was successfully removed.

Dekart Private Disk MultiFactor de-installation completed

5. Click ***OK*** in the de-installation completed window.

Note: Use the same procedure to delete the electronic Key drivers.

Note. If **Private Disk MultiFactor** was installed to a removable drive, you can uninstall it by deleting the **flash_disk:\..\Private Disk MultiFactor** folder (the path to the program's folder on the removable disk will be the same as the path you chose at step#5 during the installation except the disk's letter).

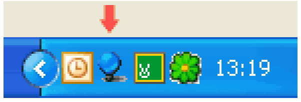
5 Operating Dekart Private Disk MultiFactor

The main goal of this chapter is to make the user of **Dekart Private Disk MultiFactor** acquainted with its use and functionality.

Note: To avoid errors during the operation of the electronic Key, do not remove the Key from the computer while there are active data exchange processes between the computer and the electronic Key. Data exchange is indicated by the flashing LED of the reader or the **Token** Key or the Flash Drive.

5.1 Getting Started

After the product is successfully installed and Windows has restarted, **Dekart Private Disk MultiFactor** will run automatically. **Dekart Private Disk MultiFactor** icon will appear in the system tray on the right side of the task bar.



Dekart Private Disk MultiFactor icon on the right side of the task bar

5.2 Installation to a removable disk

To make the program fully mobile, use the ***Install to removable disk*** function.

1. Start the application.

2. Connect the removable disk to the computer.
3. Right-click Private Disk Multifactor's icon in the system tray, choose ***Install to removable disk***.
4. Select the letter that corresponds to the removable disk from the list and press **OK**

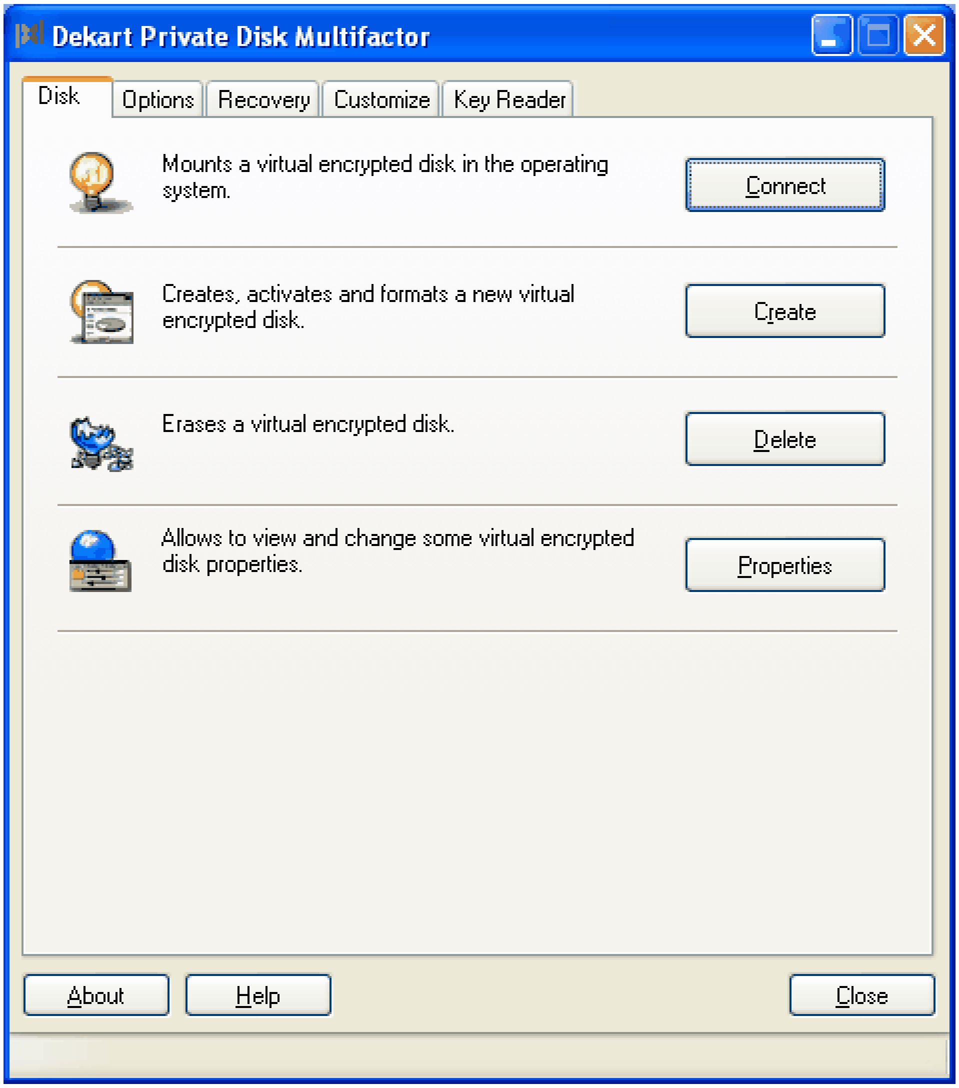
All the required files will be copied to the removable disk; as a result, you will be able to run Private Disk Multifactor on other computers without having to install the program.

Note 1: The path to the program's folder on the removable disk will be the same as the path you chose at step#5 during the installation (except the disk's letter).

Note 2: Administrative privileges are not required if the program was previously launched by an administrator on the computer on which you wish to use it.

5.3 Accessing Dekart Private Disk MultiFactor's Control Panel

Dekart Private Disk MultiFactor is controlled through its Control Panel.



Mounts a virtual encrypted disk in the operating system.

Creates, activates and formats a new virtual encrypted disk.

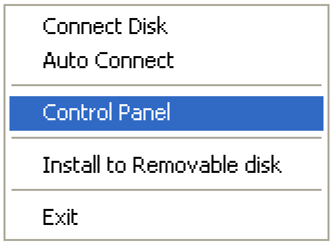
Erases a virtual encrypted disk.

Allows to view and change some virtual encrypted disk properties.

Dekart Private Disk MultiFactor Control Panel

To activate the Control Panel, do one of the following:

1. Double click **Dekart Private Disk MultiFactor**'s icon on the right side of the task bar. The Control Panel will appear.
2. Right-click **Dekart Private Disk MultiFactor**'s icon to activate the system menu. Select the ***Control Panel*** element from this menu. The Control Panel will appear.



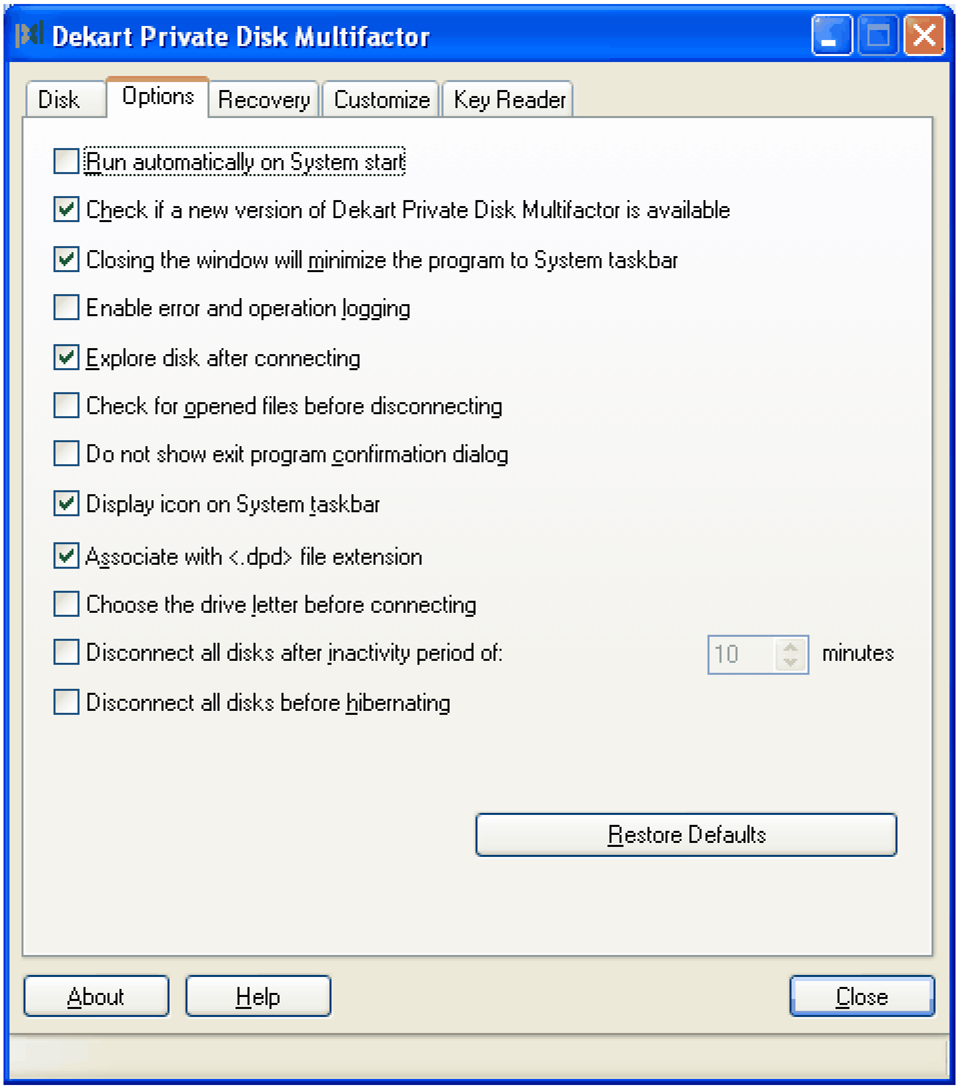
System menu

3. To launch **Private Disk MultiFactor**, do the following: ***Start* > *Programs* > *Dekart Private Disk MultiFactor* > *Private Disk MultiFactor***. The Control Panel will appear.

5.4 Dekart Private Disk MultiFactor settings

You can configure many of the program's settings so that it meets your needs.

1. Activate the Control Panel.
2. Select the ***Options*** tab.



□ Run automatically on System start

☑ Check if a new version of Dekart Private Disk Multifactor is available

☑ Closing the window will minimize the program to System taskbar

□ Enable error and operation logging

☑ Explore disk after connecting

□ Check for opened files before disconnecting

□ Do not show exit program confirmation dialog

☑ Display icon on System taskbar

☑ Associate with <.dpd> file extension

□ Choose the drive letter before connecting

□ Disconnect all disks after inactivity period of: 10 minutes

□ Disconnect all disks before hibernating

The *Options* tab of the Control Panel

5.4.1 Allow Dekart Private Disk MultiFactor to start automatically

Dekart Private Disk MultiFactor automatic launching upon starting the computer can be enabled and disabled on the ***Options*** menu of the Control Panel. To enable the option, check the ***Run automatically on System start*** checkbox.

5.4.2 Enable/disable Dekart Private Disk MultiFactor's icon

You can enable or disable **Private Disk Multifactor**'s bulb icon. Set the ***Display icon on System taskbar*** flag to enable bulb icon.

5.4.3 Minimize Control Panel when clicking Close or Exit buttons

You can allow the Control Panel to be minimized when you click **Close** or **Exit**. Set the ***Closing the window will minimize the program to System taskbar*** flag to allow minimizing.

5.4.4 Checking for currently opened files before the disk's disconnection

Go to Private Disk Multifactor's Conrol Panel, select the ***Options*** tab and check the ***Check for opened files before disconnecting*** checkbox. When this option is enabled, the program will display a warning message when the disk is about to be disconnected, informing the user that there are files currently opened on the disk and allowing them to save all the changes before proceeding with the disconnection of the disk. Otherwise, the disk will be disconnected without prompting the user to save their changes.

Note. We recommend enabling this option to avoid possible data loss..

5.4.5 Automatically exploring the disk when it is connected

The program can be set up to be automatically explore a virtual disk in Windows Explorer after it has been connected. To enable this, go to Private Disk MultiFactor's Control Panel, select the ***Options*** tab and check the ***Explore disk after connecting*** checkbox.

5.4.6 Automatically check for Dekart Private Disk MultiFactor updates

You can allow Private Disk Multifactor to check for updates if an Internet connection is available. Set the ***Check if a new version of Dekart Private Disk is available*** flag to check for Updates automatically.

5.4.7 Disable the exit confirmation

You can configure **Private Disk Multifactor** to show confirm dialog when you **Exit**. Set the ***Do not show exit program confirmation dialog*** flag to disable the confirmation. .

5.4.8 Associating Private Disk MultiFactor with the <.dpd> file extension

You can associate Private Disk Multifactor with encrypted file-images (*.dpd). Set the ***Associate with <.dpd> file extension*** flag to do this. This allows encrypted disks to be mounted by double-clicking on file-images in Windows Explorer.

5.4.9 Choosing a drive letter before connecting an image

You can enable or disable **Private Disk Multifactor** to ask the user to choose a drive letter before mounting virtual disk. Set the ***Choose the drive letter before connecting*** flag to enable this prompt. If this option is enabled the program will ask you to enter the drive letter every time you mount a disk.

5.4.10 Enabling/disabling event and error logging

Select the ***Options*** tab of the Control panel menu to enable or disable **Dekart Private Disk Multifactor** error and event logging. After you select the ***Enable error and operation logging*** checkbox, dk_pdapi.log and dk_pd.log files will appear in the root directory of the system disk. These files will contain details about errors and events triggered by the user's actions. If the checkbox is not checked, the logging mode is not enabled.

5.4.11 Enabling/Disabling the 'disconnect at time-out' option

The ***Options*** tab of Private Disk Multifactor's **Control Panel** allows you to enable or disable the disconnection of the virtual encrypted disk on timeout. To do that, click the ***Disconnect all disks at time-out*** heckbox, indicating the time interval (in minutes) in the scrollbox on the right.

Once this option is enabled, Private Disk Multifactor will automatically disconnect all the disks if you do not interact with the mouse/keyboard during the given time-interval. Before disconnecting, Private Disk Multifactor will check whether any files located on any of the disks are currently open (if this option is enabled). If this is true, you will be notified and given the chance to close all the open files. On the other hand, if this option is disabled, the disks will be dismounted even if certain files on them are being accessed.

5.4.12 Enabling/Disabling the 'disconnect before hibernating' option

The ***Options*** tab of Private Disk Multifactor's **Control Panel** allows you to enable or disable the disconnection of the virtual encrypted disk before hibernating. To do that, click the ***Disconnect all disks before hibernating*** checkbox.

Once this option is enabled, Private Disk Multifactor will automatically disconnect all the disks if you press **Start -> Turn off computer -> Hibernate**. Before disconnecting, Private Disk Multifactor will check whether any files located on any of the disks are currently open (if this option is enabled). If this is true, you will be notified and given the chance to close all the open files. On the other hand, if this option is disabled, the disks will be dismounted even if certain files on them are being accessed.

5.4.13 Configuring "Hot Keys"

Select the ***Customize*** tab of the Control Panel to define the hot key that will automatically dismount all the virtual encrypted disks; and the hotkey that will automatically dismount all the virtual encrypted disks and exit the program. To do this, enter the desired key combination in the ***Dismount all disks*** and ***Dismount all disks and exit the program*** fields or use the default settings.

5.4.14 Changing the Private Disk MultiFactor system tray icon

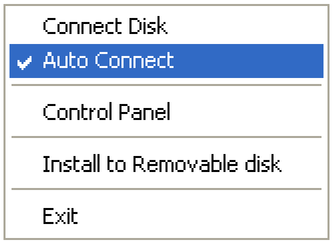
The **Customize** tab of the Control Panel allows you to change the system tray icons used by Private Disk Multifactor (both the "mounted" and "unmounted" state icons) and icon that corresponds to Private Disk Multifactor file images (the <.dpd> file extension). To do this, click the **Change** button for the icons "***No connected disks status icon***:", "***Connected disks status icon:***" and ***"Private Disc File image:"***..

Here you can either select icons offered by Private Disk or **Browse** the file you would like to choose the icons from.

You can restore to the default settings by pressing ***Restore Defaults***.

5.4.15 Enabling/Disabling Dekart Private Disk MultiFactor's Auto Connect Mode

Dekart Private Disk MultiFactor’s automatic connection/disconnection mode can be enabled via the system menu. If the option is enabled, the disks will be automatically connected or disconnected when a key is inserted or removed.. Right-click **Dekart Private Disk MultiFactor’s** icon to activate the system menu

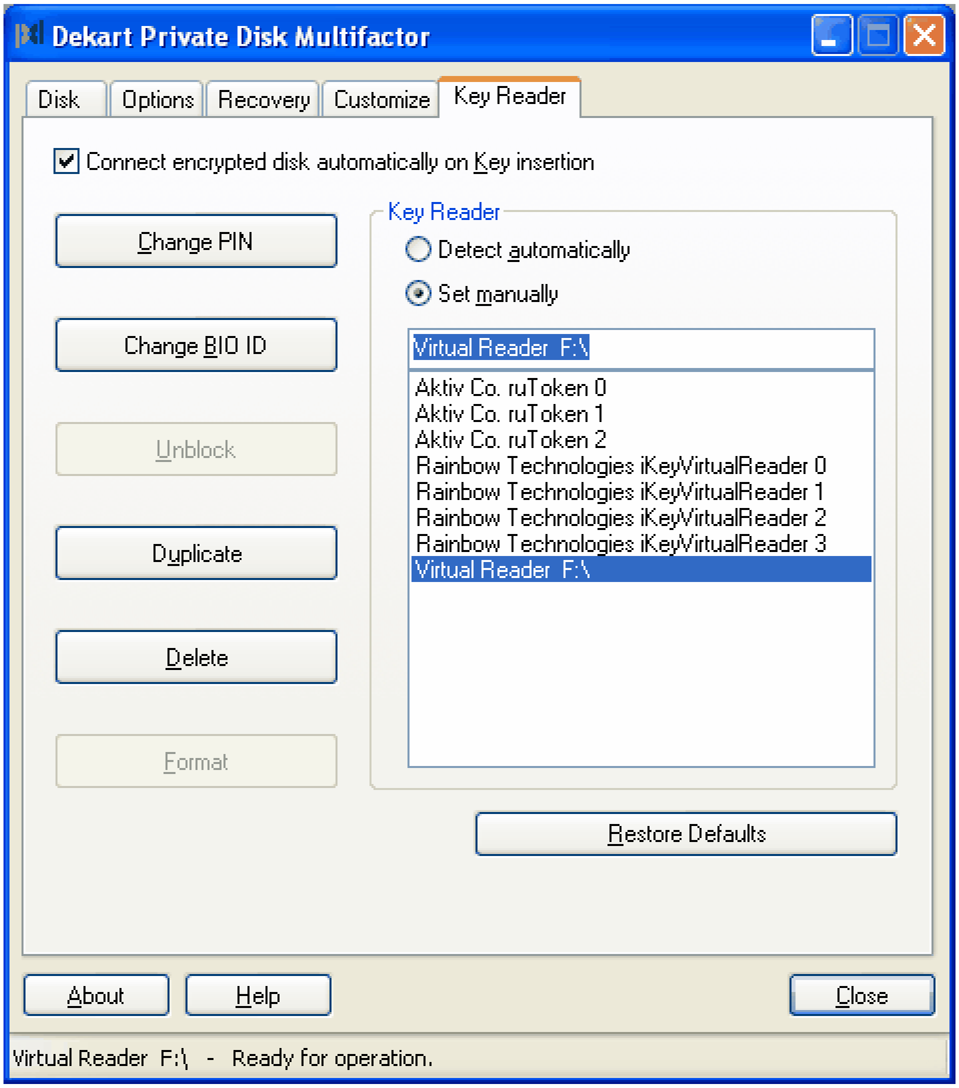


Dekart Private Disk MultiFactor Control Panel System menu

To enable the option, check ***Auto Connect***; unchecking the option will disable it.

5.5 Key Selection

If several electronic Keys are present in the system, you can select a specific Key on the ***Key Reader*** tab of the Control Panel. To select a Key, select the desired **Key** from the list.



☑ Connect encrypted disk automatically on Key insertion

Key Reader

○ Detect automatically

● Set manually

Virtual Reader F:\

Aktiv Co. ruToken 0
Aktiv Co. ruToken 1
Aktiv Co. ruToken 2
Rainbow Technologies iKeyVirtualReader 0
Rainbow Technologies iKeyVirtualReader 1
Rainbow Technologies iKeyVirtualReader 2
Rainbow Technologies iKeyVirtualReader 3
Virtual Reader F:\

Virtual Reader F:\ - Ready for operation.

The *Key Reader* tab of Control Panel

5.6 Key Activation

To start using Dekart Private Disk MultiFactor, you will need to perform the following **obligatory** operation - activate your electronic Key. To activate your Key, please, connect your Key to the computer and, in case the Key is protected, perform the two- or three-factor authentication (enter the PIN code and present your biometric identifier)..

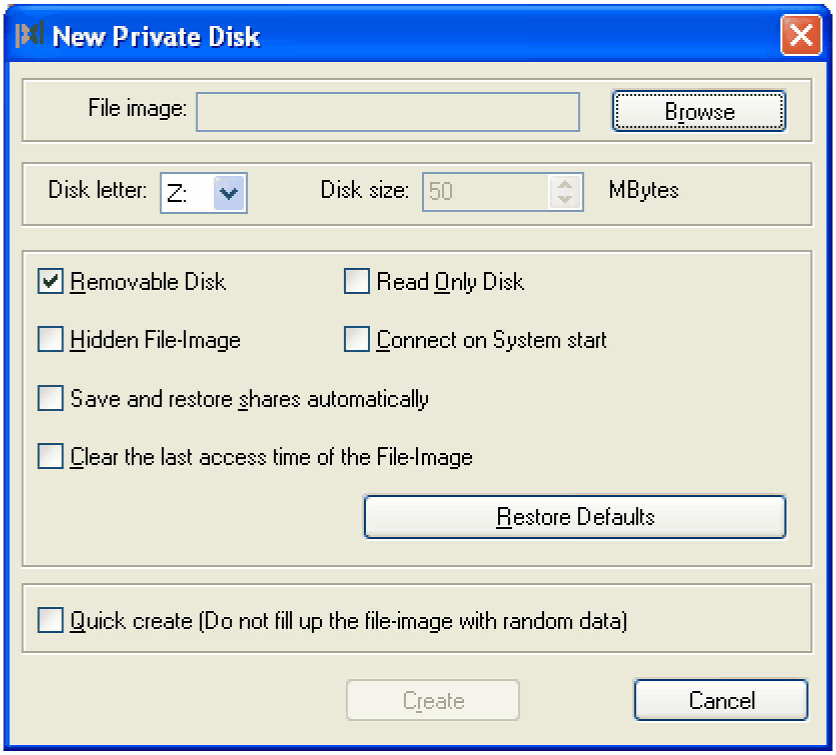
5.7 Creating Virtual Secret Disk

To create a virtual secret disk, do the following:

1. In **Dekart Private Disk MultiFactor**'s Control Panel, click ***Disk*** > ***Create***.
2. Connect the Key to the computer when required. If the Key is PIN-protected, the PIN will be requested. Enter the proper PIN.

Note: For directions on changing the PIN, see the section Setting and Changing Virtual Disk Access PIN of this chapter.

Note: If **Dekart Private Disk MultiFactor** data were previously recorded to this electronic Key, a virtual disk creation confirmation request will follow. By clicking ***Yes***, you can lose the existing secret disk associated with your electronic Key. **Think carefully before doing this!** By clicking ***No***, you will cancel the virtual disk creation process. Upon clicking **Yes**, all the information about the previous disk will be deleted and the new disk creation window will appear.



File image:

Disk letter: Z: Disk size: 50 MBytes

☑ Removable Disk   □ Read Only Disk

□ Hidden File-Image   □ Connect on System start

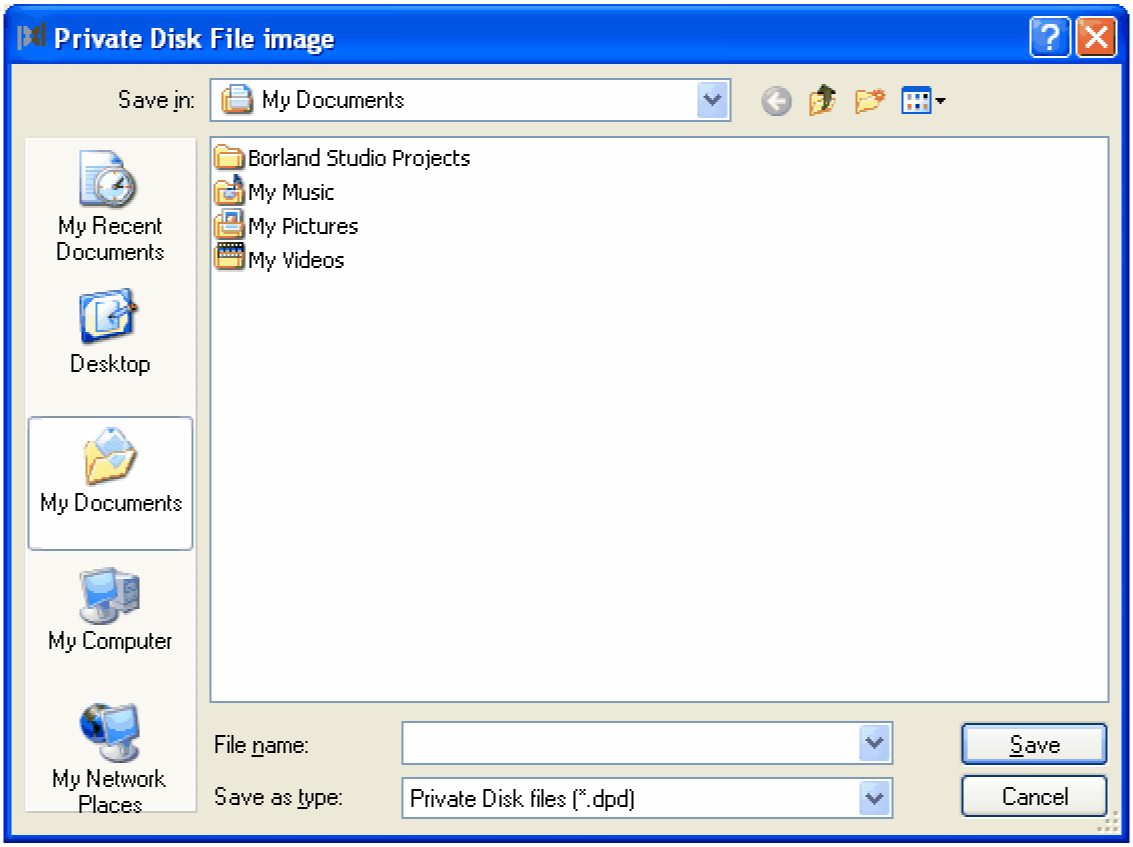
□ Save and restore shares automatically

□ Clear the last access time of the File-Image

□ Quick create (Do not fill up the file-image with random data)

The new disk creation window

3. You can do one of the following in the new disk creation window:
   - Click ***Cancel*** to cancel the creation of the new disk.
   - Click ***Browse*** to proceed with the creation of the new disk, then indicate the full name of the image file for the virtual disk in the ***File image*** field. A window will appear. Select an appropriate folder for the image file, indicate the name in the ***File Name*** field, and click ***Save***.



Private Disk File image

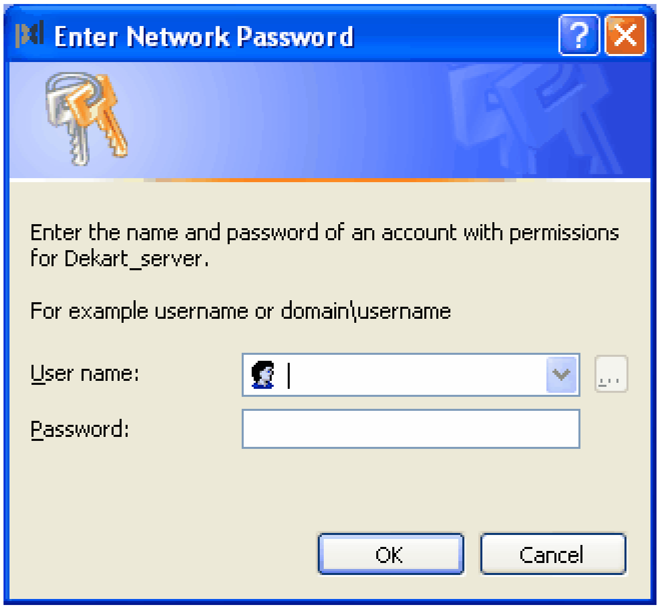
Save in: My Documents

File name:

Save as type: Private Disk files (*.dpd)

Creating an image file

Dekart Private Disk MultiFactor can request a network resource access password if the image file is stored on the network disk.



Enter Network Password

Enter the name and password of an account with permissions for Dekart_server.

For example username or domain\username

User name:

Password:

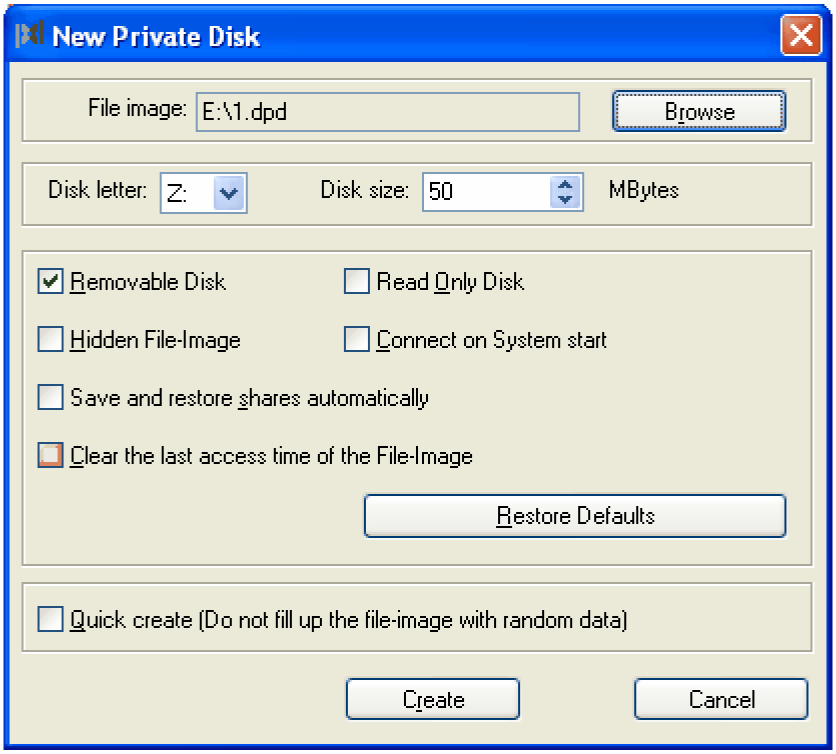
Network resource access password request

Enter the password into the ***Password*** field and click ***OK***.

If the file with the same name already exists in the folder you specified, you will be asked if you wish to overwrite the existing file. **Note:** By clicking ***Yes*** and overwriting the existing file, you will lose the existing virtual disk associated with this file. **Think carefully before doing this!** Upon clicking ***No***, the image file creation will be terminated. In this case, you will have to indicate a different image file name to continue the creation of the disk..

4. Select the virtual disk’s from the ***Disk letter*** field of the *new disk creation* window. Select the desired secret disk volume in megabytes in the ***Disk size*** field (depending upon the free disc space where the image file will be located). You may immediately set up some options for the newly created secret disk or do it later (look at Changing properties of the virtual encrypted disk). To set up the disk's properties during new disk creation process, check the following checkboxes:
   - ***Removable Disk*** – the newly created disk will have the < Removable> status;
   - ***Hidden File-Image*** – the disk's file-image will be <hidden>;
   - ***Read Only Disk*** - the disk will have the <Read only> status;
   - ***Save and restore shares automatically*** - allows to save and restore network access rights to the contents of the encrypted disk;
   - ***Connect on System Start*** - this disk will be connected when Windows starts. In this case, the "***Run automatically on System Start***" will be enabled in the Options tab of Private Disk’s Control panel .
   - ***Clear the last access time of the File-Image*** – once the disk is disconnected, its time of last access will be changed to the time of its creation. This means that one will be unable to determine when was the last time the encrypted disk was used.

   Press ***Create to start the*** image file creation process.



File image: E:\1.dpd

Disk letter: Z: Disk size: 50 MBytes

☑ Removable Disk ☐ Read Only Disk

☐ Hidden File-Image ☐ Connect on System start

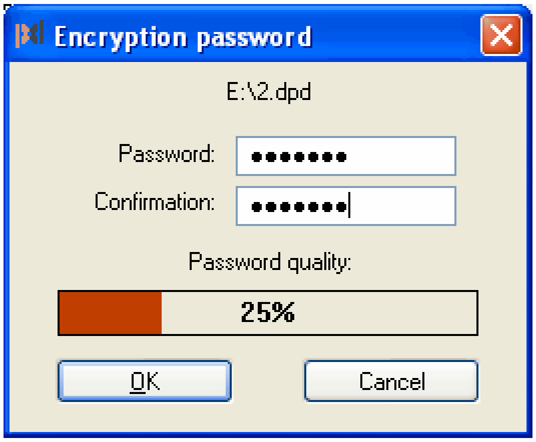
☐ Save and restore shares automatically

☐ Clear the last access time of the File-Image

☐ Quick create (Do not fill up the file-image with random data)

Image file creation

If a Key is not attached to the computer, the program will ask you to enter a password. Enter the password in the ***Password*** field, then enter the same password in the ***Confirmation*** field



Encryption password

E:\2.dpd

Password: ●●●●●●●

Confirmation: ●●●●●●●

Password quality:

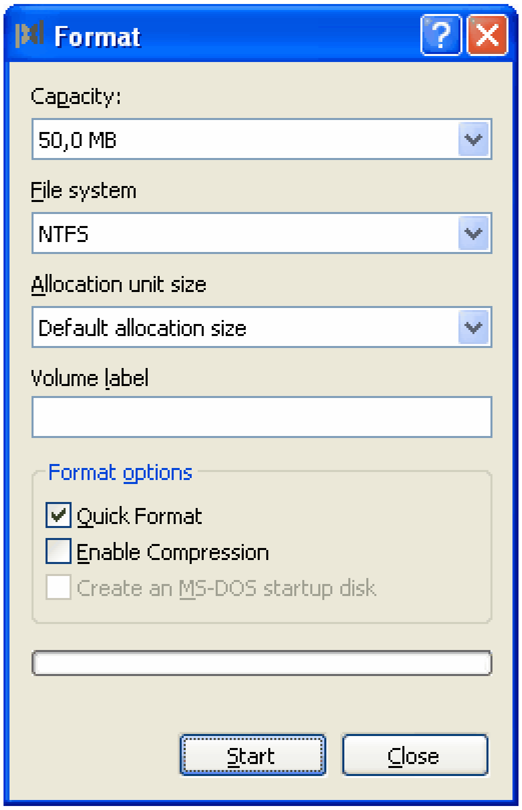
25%

Note: The entered password must be at least 5 symbols long (not longer than 64 symbols) otherwise, an insufficient password length message will appear. The **Dekart Private Disk MultiFactor** access password can consist of alphanumeric symbols, and it is **case-sensitive**. Enter the password carefully.

For more information about choosing a strong password, please refer to the section R *ecommendations for ensuring Dekart Private Disk MultiFactor security*.

Note. If the entered password and password confirmation do not match, **Dekart Private Disk MultiFactor** will ask you to enter the password again.

When the image file is created, you will be asked to format the new disk..



Capacity: 50,0 MB

File system: NTFS

Allocation unit size: Default allocation size

Volume label:

Format options

☑ Quick Format

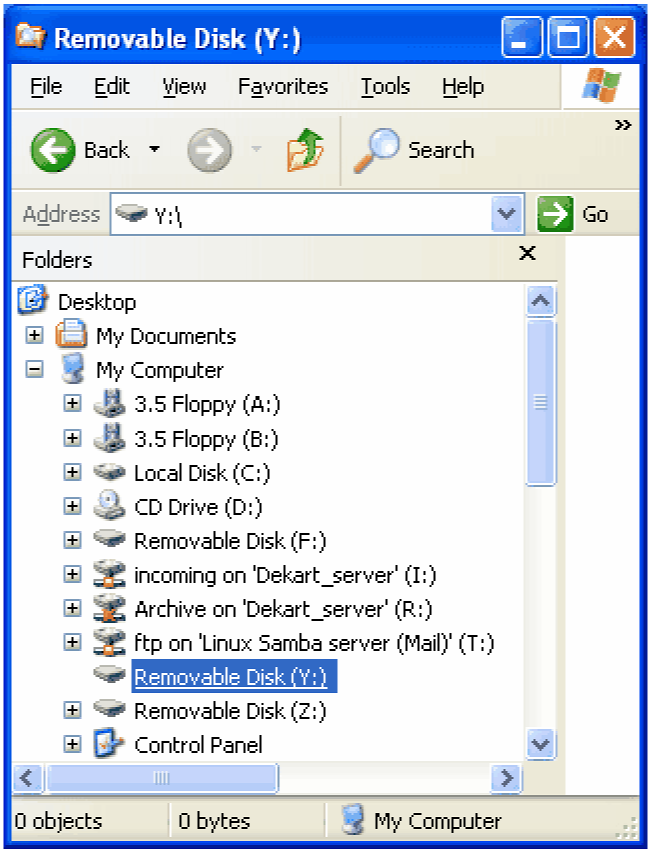
□ Enable Compression

□ Create an MS-DOS startup disk

Virtual disk format dialog

5. To format the disk, click ***Start*** and wait for the process to complete. When the disk is formatted, close the ***Format*** dialog box to finish the disk creation process. The virtual is now ready for use. Its icon will appear in ***My Computer***

   Note: If you click ***Close*** and cancel the disk format process, the virtual disk will not be created



The created disk can now be used

5.8 Recommendations for ensuring Dekart Private Disk MultiFactor security

In order to enhance the protection of your proprietary information, we advise that you follow the recommendations listed below.

Tip#1. Never write the PIN code down, you need to remember it!

Tip#2. Create backup copies of your virtual encrypted disks at a regular interval. This will allow you to restore your data in case the file-images are lost or corrupted (see *Backing up virtual encrypted disk data* and *Restoring virtual encrypted disk data* sections).

Tip#3. Backup your Key. If for any reason your break or lose your Key, the backup Key will help you decrypt your data (see Creating the Electronic Key Duplicate).

Tip#4. When leaving your workplace unattended, even if this is for a short period of time, don't forget to unmount all the mounted virtual encrypted (see *Mounting/unmounting virtual encrypted disk* section).

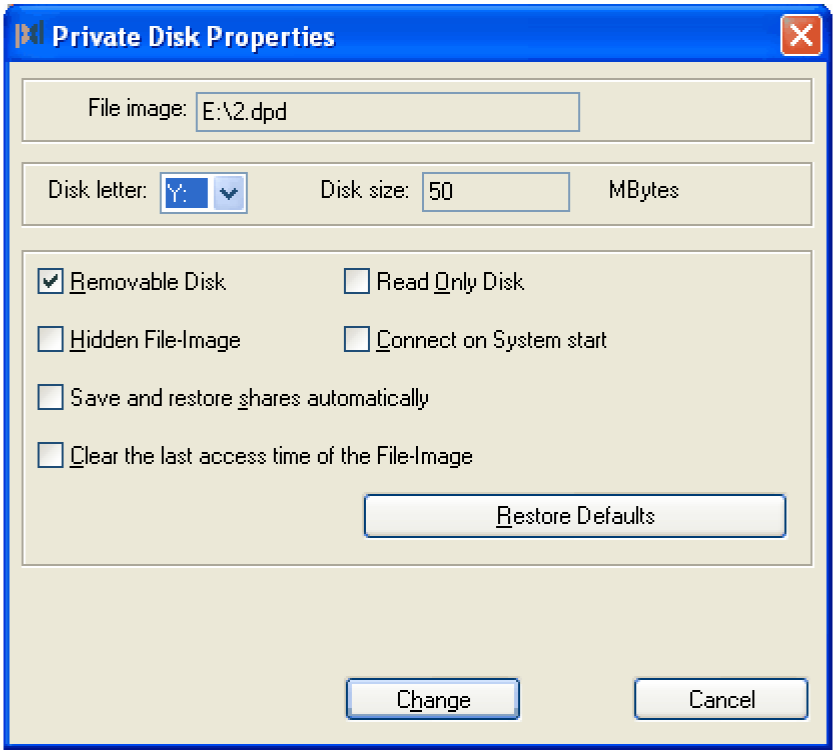
Tip#5. To provide a greater level of protection for your encrypted data, define a white-list of applications that are allowed to access the contents of the virtual drive (see Managing the list of applications which are allowed to access the encrypted disk section).

Tip#6. To make sure the encrypted data cannot be recovered, erase the unused encrypted images using Private Disk's special feature (see Deleting virtual encrypted disk section). In this case, the encrypted image will be filled with random data before being deleted

Tip#7. The length of your password should not be too short. The optimal length – 8 random symbols, including upper-case and lower-case letters, digits, punctuation marks etc. Never write the password down, remember it!

5.9 Changing Virtual Secret Disk Properties

To change the name of the Private Disk MultiFactor image file (or its path) or the logical name (letter) identifying the secret disk in the system, access **Dekart Private Disk MultiFactor** Control Panel and click ***Disk*** > ***Properties***. The ***Private Disk MultiFactor Properties*** window will appear.



Private Disk Properties

File image: E:\2.dpd

Disk letter: Y:

Disk size: 50 MBytes

☑ Removable Disk

☐ Read Only Disk

☐ Hidden File-Image

☐ Connect on System start

☐ Save and restore shares automatically

☐ Clear the last access time of the File-Image

Disk properties window

➢To set up the disk's properties check the following checkboxes:

- ***Removable Disk*** – the newly created disk will have the < Removable> status;
- ***Hidden File-Image*** – the disk's file-image will be <hidden>;
- ***Read Only Disk*** - the disk will have the <Read only> status;
- ***Save and restore shares automatically*** - allows to save and restore network access

rights to the contents of the encrypted disk;

- ***Connect on System Start*** - this disk will be connected when Windows starts. In this case, the "***Run automatically on System Start***" will be enabled in the Options tab of Private Disk's Control panel .
- ***Clear the last access time of the File-Image*** – once the disk is disconnected, its time of last access will be changed to the time of its creation. This means that one will be unable to determine when was the last time the encrypted disk was used

➢ Enter new values in ***File image*** and ***Disk letter*** fields (See the Creating Virtual Secret Disk section) and click ***Change***.

➢ Click ***Cancel*** to stop changing the disk properties.

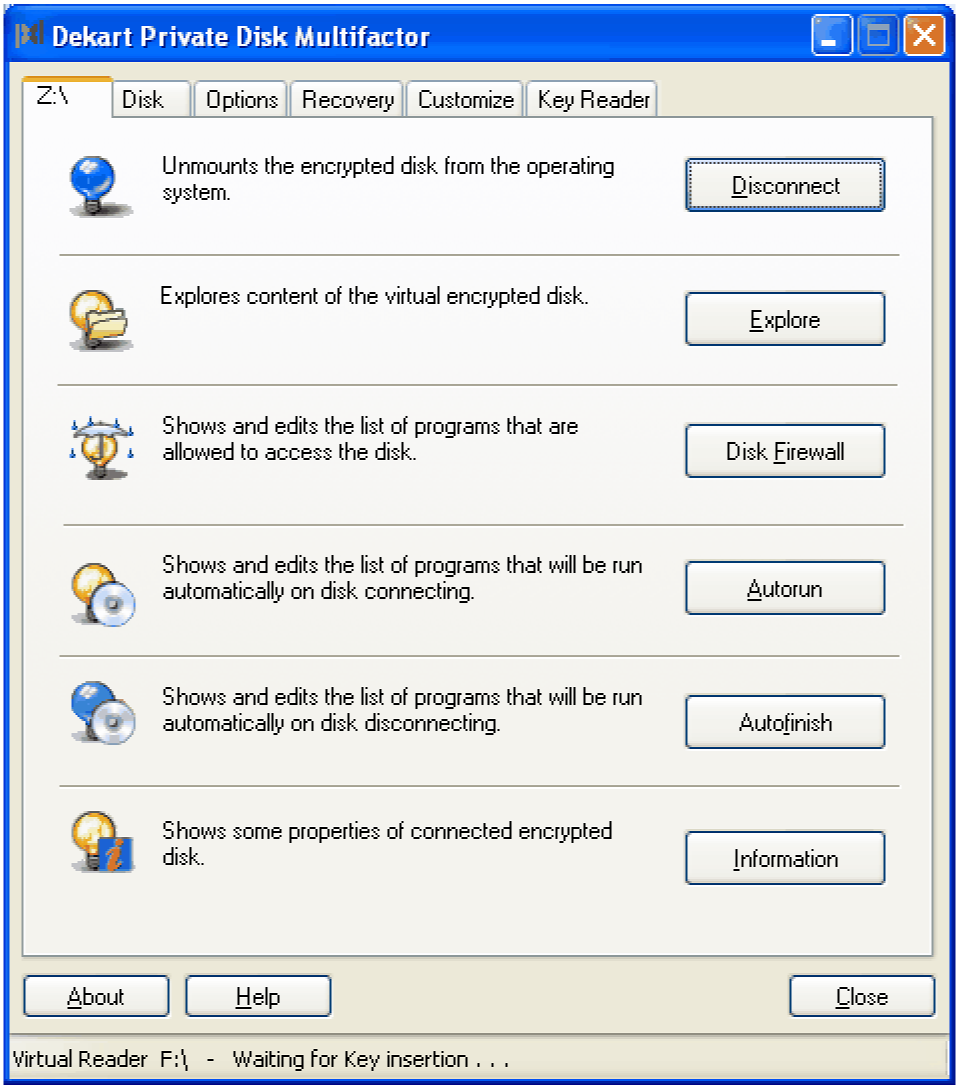
Note: The value in the ***Disk Size*** field containing the information about the disk volume cannot be changed.

5.10 Connecting/Disconnecting the Virtual Secret Disk

Before a virtual secret disk can be used, it must be *connected* first. Connecting the virtual disk can be done in two ways — manually, via the Control Panel, or automatically.

1. **Connecting a disk via the Control Panel.** In this case, click ***Disk*** > ***Connect*** in the Control Panel. The electronic Key must be activated. Otherwise, **Dekart Private Disk MultiFactor** will remind you to do it .

   When the Key is attached, the disk becomes visible to the system and it can be used like any other drive on your computer.



Unmounts the encrypted disk from the operating system.

Explores content of the virtual encrypted disk.

Shows and edits the list of programs that are allowed to access the disk.

Shows and edits the list of programs that will be run automatically on disk connecting.

Shows and edits the list of programs that will be run automatically on disk disconnecting.

Shows some properties of connected encrypted disk.

Virtual Reader F:\ - Waiting for Key insertion . . .

Connecting the virtual disk

If the file-image of the virtual encrypted disk is password protected, the software will ask you to enter the access password. After entering the password, the disk becomes visible to the system and it can be used like any other drive on your computer.

Note: If the image file is located on a network drive, the network resource access password request may follow. Enter the password into the ***Password*** field and click ***OK***.

Note: If the "**Associate with <.dpd> file extension"** option was set, you can connect the encrypted virtual disk by double clicking the file-image in **Windows Explorer**.

In this mode you can use the virtual secret disk without an electronic Key. To finish working with the virtual secret disk (i.e, *disconnect it*), click ***Disk*** > ***Disconnect***.

You can also connect/disconnect a virtual encrypted disk using a popup menu. To access this menu, please right click the Private Disk MultiFactor systray icon. Select the desired action from the menu items list. In case there are several connected disks, please select the desired disk letter in the ***Disconnect Disk*** menu to disconnect that disk. To disconnect all the currently connected disks at once, click ***Disconnect all disks.***

Another way to disconnect the virtual drives is to automate the process, by enabling the *Disconnect all disks at time-out* and/or the *Disconnect all disks at standby* options in Private Disk's settings. In this case, the drives will be dismounted either when the system is inactive for a defined period of time, or when the computer hibernates.

Note: To prevent possible data loss, close all the applications that access files on the disk before disconnecting it.

2. **Connecting a disk automatically.** In this case, it is necessary to activate the mode of automatic virtual secret disk connection upon inserting the electronic Key and disconnection upon Key removal. Do one of the following to close **Dekart Private Disk MultiFactor's** Control Panel:

   o Press ***Esc***.

   o Click the *minimize* button in the top right corner of the Control Panel.

   From this point on, using the private disk will only be possible with the electronic Key attached. The disk is disconnected immediately if the Key is removed. Upon attaching the Key, the virtual disk is automatically connected or the PIN is requested by **Dekart Private Disk MultiFactor** if the disk access is PIN-protected (See the Setting and Changing Virtual Disk Access PIN section of this chapter)

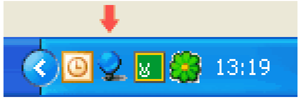
Note: To prevent possible data loss, close all the applications that access files on the disk before disconnecting it.

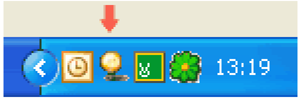
5.10.1 Connecting a disk with Drag'n'Drop

A disk can be connected via the Drag'n'Drop mechanism. To do that, click on an image file with your mouse and drag it onto Private Disk MultiFactor's Control panel or Private Disk MultiFactor's shortcut or Private Disk MultiFactor's icon. When the file is dropped, the disk connection dialog will be activated.

5.10.2 Virtual Secret Disk's Status

Dekart Private Disk MultiFactor icon is located in the system tray on the right side of the task bar. It indicates the current status of the virtual secret disk — *disk disconnected* or *disk connected*.





Virtual secret disk's status

To change the status from "Disconnected" to "Connected", activate the corresponding electronic Key.

To change the status from "Connected" to "Disconnected", i.e. to finish your work with the secret disk, simply remove, or deactivate the electronic Key.

Note: Do not disconnect the secret disk if any application is currently accessing it. First, close the application, then, disconnect the disk.

5.11 Exploring a virtual encrypted disk

After you mount the encrypted disk, you can use Windows Explorer to view the contents of the encrypted disk and work with the information it contains. You can run Windows Explorer in the following two ways:

1. Go to the Disk properties windows, click **Explore**
2. Right-click the application icon in the system tray, select the ***Explore disk*** menu and select the required disk letter if there are several disks connected.

5.12 Managing the list of applications which are allowed to access the encrypted disk (Disk Firewall feature)

Private Disk MultiFactor enables you to control which applications are allowed to access the encrypted disk and which applications are not. To use this feature, follow these steps:

1. Connect the disk
2. Switch to the disk's tab on the **Control Panel** (***Disk_name:***\).
3. Press the **Disk Firewall** button

The ***Allowed Programs*** window will appear. To add an application to the ***List of allowed programs*** press **Add,** then indicate the program you wish to allow to access the disk. You can add more applications by repeating this procedure. Press **OK** when you are done.

To remove a program from the ***List of allowed programs***, open the ***Disk Firewall*** window, select the applications and press **Delete**. Press **OK** when you are done.

Note. To activate Disk Firewall, check the ***Enable Disk Firewall*** option. Unchecking the option will de-activate Disk Firewall, while the list of selected applications will be reserved.

When dismounting the disk, Private Disk MultiFactor will notify you about the changes you made and ask you to confirm them, by entering the password of the encrypted disk.

The new settings will be applied next time you connect the disk.

5.13 Managing the programs that are automatically started when a disk is mounted or dismounted

Private Disk MultiFactor allows you to define programs that will be automatically started when a disk is mounted or dismounted.

Autorun.
To edit the list of the programs that start automatically when the encrypted disk is mounted, go to **Control Panel** (***Disk_name:***) and click the **Autorun** button. The ***Autorun programs*** window will appear.

To add a new program to the list, click **Add**. The ***Add a program to autorun*** window will appear. Select the files to be run after the disk is mounted and click **OK**. They will then appear in the **List of programs to autorun** (***Autorun programs*** window) on disk mounting.

To delete a program from the list, select it and click **Delete**.

Note: To activate Autorun, check the ***Enable Autorun*** option. Unchecking the option will de-activate Autorun, while the list of selected applications will be reserved.

After you are finished editing the list of programs, click **OK**.

Autofinish.
To edit the list of the programs that start automatically when the encrypted disk is dismounted , go to **Control Panel** (***Disk_name:***) and click the **Autofinish** button. The ***Autofinish programs*** window will appear.

To add a new program to the list, click **Add**. The ***Add a program to autofinish*** window will appear. Select the files to be run after the disk is dismounted and click **OK**. They will then appear in the **List of programs to autofinish** (***Autofinish programs*** window) on disk unmounting.

To delete a program from the list, select it and click **Delete**.

Note: To activate Autofinish, check the ***Enable Autofinish*** option. Unchecking the option will de-activate Autofinish, while the list of selected applications will be reserved.

After you are finished editing the list of programs click **OK**.

When dismounting the disk, Private Disk MultiFactor will notify you about the changes you made and ask you to confirm them, by entering the password of the encrypted disk.

5.14 Managing the list of files which are automatically opened when the disk is connected

Private Disk MultiFactor can automatically open certain files (ex: MS Word documents, pictures, or programs) when the virtual encrypted disk is connected.

Managing the list of files which are started automatically is described in the Managing the list of applications which are allowed to access the encrypted disk section.

5.15 Sharing a Secret Disk in a network

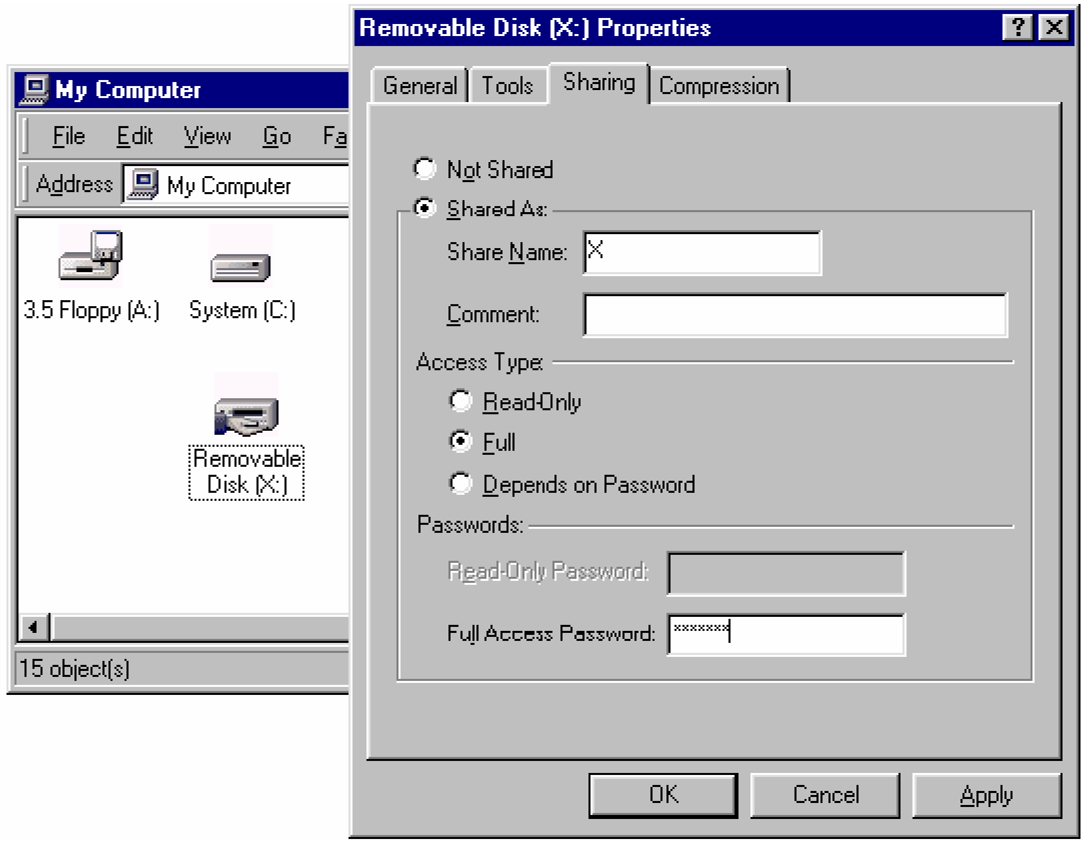
Dekart Private Disk MultiFactor supports the shared use of the virtual private disk's data in a network. To allow other users to access the secret data, the disk must be mounted on the computer where the image file is located (See the section Connecting/Disconnecting the Virtual Secret Disk above). Then, the shared access must be setup with the help of the standard Windows OS utilities (as it is done with the sharing of a conventional drive).

Note: The virtual secret disk can be available for shared network use only if it is connected to the computer storing the image file. When the Key is removed or the disk is deactivated, disk access will be immediately disabled for all users and the currently processed data can be lost. Do not deactivate such a disk unless all users are off the system and the disk is properly shut down.

Note: Only one electronic Key has to be connected to the computer storing the image file of the virtual secret disk shared among several users. Electronic Keys are not required for other users.

To enable disk sharing, do the following (this example applies to Windows 98):

1. Double click ***My Computer***.
2. In the appearing ***My Computer*** window, select the virtual secret disk and right-click it. Select ***Properties***. Click the ***Sharing*** button. Setup values in the ***Shared As***, ***Access Type*** fields and click ***Apply***.



Removable Disk (X:) Properties

○ Not Shared

● Shared As:

Share Name: X

Comment:

Access Type:

○ Read-Only

● Full

○ Depends on Password

Passwords:

Read-Only Password:

Full Access Password: *******

Setting up shared virtual disk access

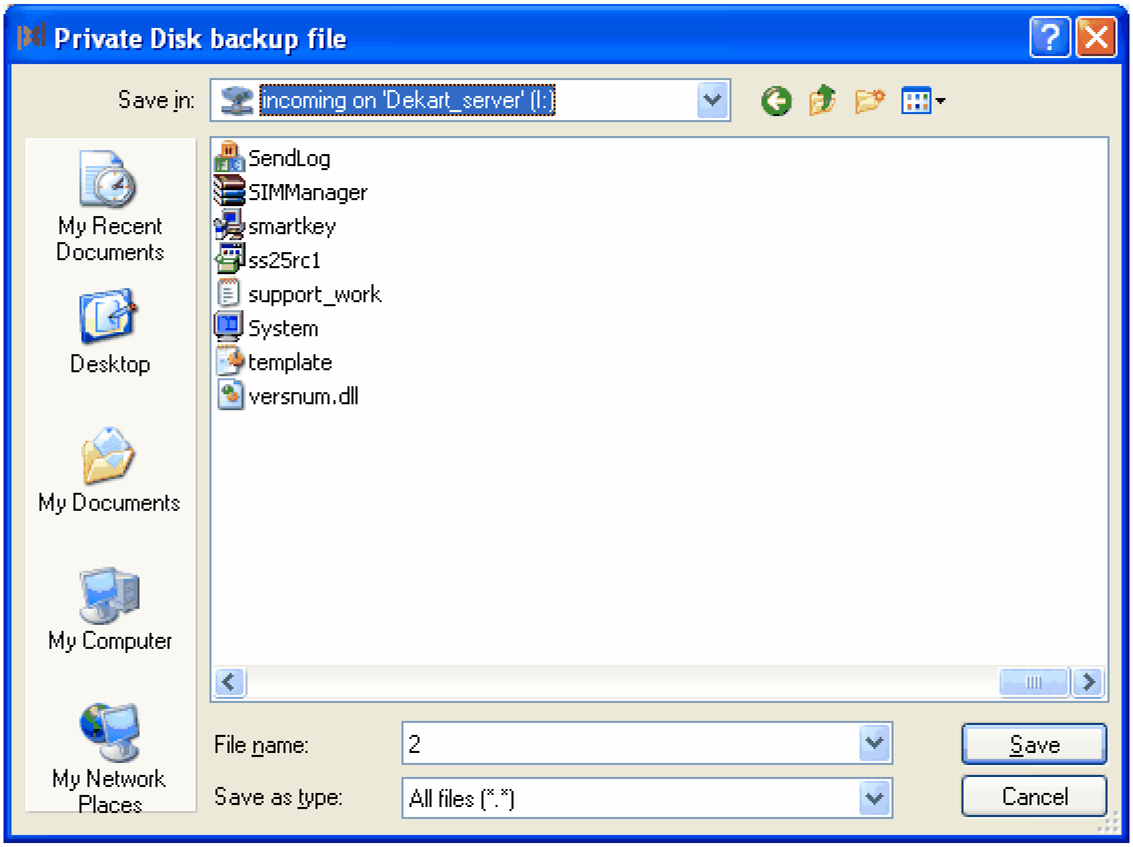
5.16 Backing up a Virtual Secret Disk

Dekart Private Disk MultiFactor allows you to back up a virtual secret disk's data. A b ackup copy can be used to recover important data when the encrypted image has been damaged or accidentally deleted.

A backup copy is compressed and encrypted. Encryption is implemented by means of an electronic Key and a special alternative access password. This password helps you restore the data even if the electronic Key used to encrypt the virtual disk data backup copy has been lost.

To create a backup copy, do the following:

1. Click ***Recovery*** > ***Backup*** in the Control Panel.
2. Connect the secret disk as described in the section Connecting/Disconnecting the Virtual Secret Disk.
3. The ***Private Disk MultiFactor backup file*** window will appear.



Private Disk backup file

Save in: incoming on 'Dekart_server' (I:)

SendLog
SIMManager
smartkey
ss25rc1
support_work
System
template
versnum.dll

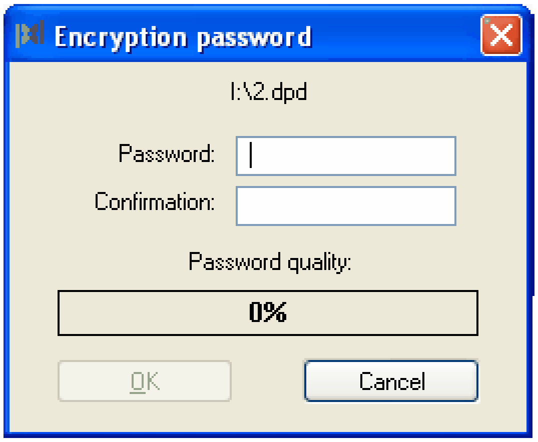
File name: 2

Save as type: All files (*.*)

Backing up a virtual disk

4. Select the folder in which the disk backup copy will be stored, enter the backup copy file name in the ***File Name*** field, click ***Save***.

   The software will ask you to enter and confirm the backup copy alternative access password.



Encryption password

I:\2.dpd

Password:

Confirmation:

Password quality:

0%

Entering the backup copy alternative access password.

5. Enter the alternative password in the ***Password*** field, then re-enter it in the ***Confirmation*** field. The entered password must be at least 8 symbols long. Otherwise, an insufficient password length message will appear.

Click ***OK***, enter a password which is at least 8 symbols long in the ***Password*** field, then re-enter it in the ***Confirm Password*** field, click ***OK***.

If the original password and the confirmation password do not match, **Dekart Private Disk MultiFactor** will notify you about this.

Click ***OK***, enter the matching values in the ***Password*** and ***Confirm Password*** fields, click ***OK***.

Note: The **Dekart Private Disk MultiFactor** backup copy alternative access password can consist of alphanumeric symbols, and it is **case-sensitive**. Enter the password carefully.

5.17 Restoring a Virtual Secret Disk

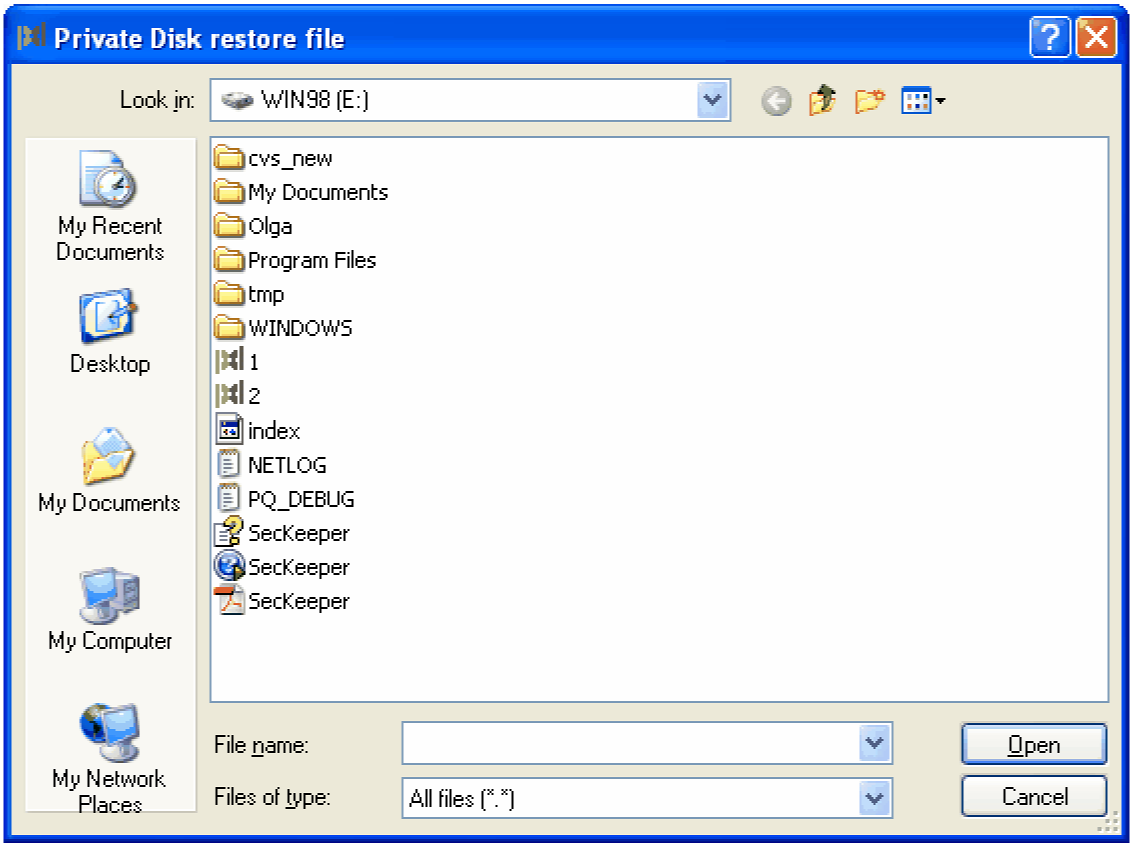
Dekart Private Disk MultiFactor allows you to restore a virtual secret disk from a previously created backup copy (see the section Backing up Virtual Secret Disk Data above).

Note: The data of a backup copy can be restored to the original secret disk, as well as to any other existing or newly created secret disk, if the alternative access password is entered correctly and the size of the restored data does not exceed the capacity of the virtual disk of destination. This feature allows you to restore data even if both the image file and the electronic Key of the original secret disk have been lost.

Note: If an existing virtual secret disk is intended to store the data recovered from a backup copy, *all of its current data will be lost upon backup data recovery* (replaced by the backup copy data). **Be careful!**

To restore data using a backup copy, do the following:

1. Click ***Recovery* > *Restore*** in the product Control Panel .
2. Connect the secret disk as described above in the section Connecting/Disconnecting the Virtual Secret Disk or create a new disk, as described in the section Creating Virtual Secret Disk.
3. The ***Private Disk MultiFactor restore file*** window will appear.



Look in: WIN98 (E:)

Files of type: All files (*.*)

Virtual disk data recovery using a backup copy

4. Select a folder storing the disk backup copy, enter the backup copy file name in the ***File Name*** field, click ***Open***.

   If the activated electronic Key is not an electronic Key used in creating this backup copy, the software will request to enter an alternative access password.

   Note: The alternative backup copy access password can consist of alphanumeric symbols and it is **case-sensitive**. Enter the password carefully.

   Before the data recovery process starts, **Dekart Private Disk MultiFactor** warns that all data will be deleted from the current virtual disk.

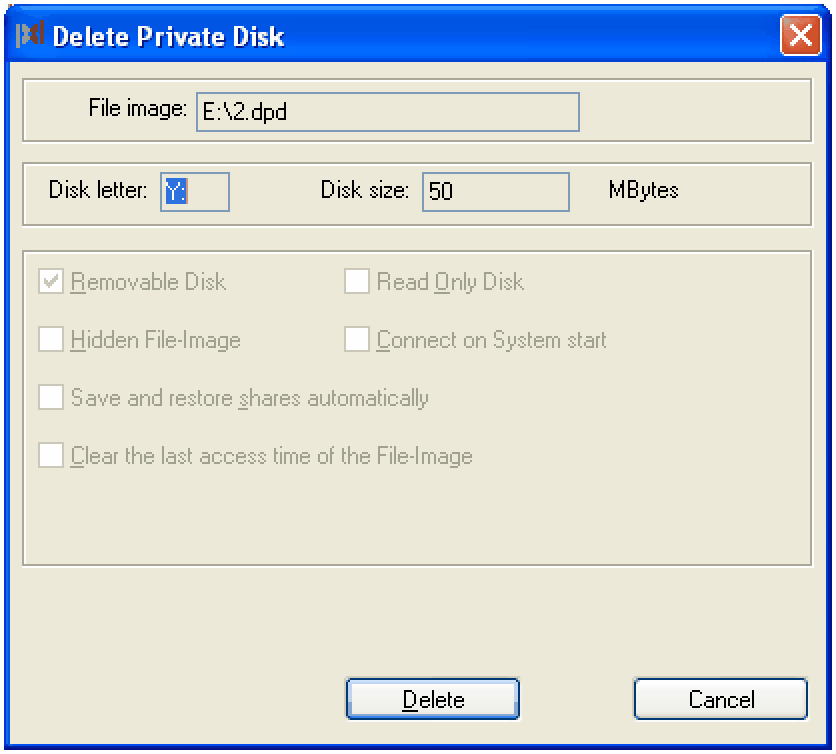
5. After clicking ***Yes***, all of the current disk data are deleted, and the virtual private disk data recovery process is initiated.

5.18 Deleting a Virtual Secret Disk

To delete virtual secret disk, do the following:

1. Disconnect the secret disk (if it is connected) as described in the Connecting/Disconnecting the Virtual Secret Disk section.
2. In **Dekart Private Disk MultiFactor** Control Panel, click ***Disk*** > ***Delete***.

3. The window with the request to enter the file name of the disk to be deleted will appear.
4. Activate your Key or enter the password in the appeared window. The window with the information about the disk to be deleted will appear.



Delete Private Disk

File image: E:\2.dpd

Disk letter: Y: Disk size: 50 MBytes

☑ Removable Disk ☐ Read Only Disk

☐ Hidden File-Image ☐ Connect on System start

☐ Save and restore shares automatically

☐ Clear the last access time of the File-Image

Disk deletion window

4. To delete the disk, click ***Delete***. The deletion confirmation request will appear.

   Note: Upon clicking ***Cancel***, the disk deletion process is terminated.

5. Click ***Yes*** to proceed with the virtual secret disk deletion operation, click ***No***, to cancel it.

   Note: If the image file is located on a network drive, the network resource access password request may follow. Enter the password into the ***Password*** field and click ***OK***.

5.19 Creating backup copy of the encryption key

Dekart Private Disk MultiFactor allows you to create a backup copy of the encryption key of the virtual encrypted disk. The backup copy can be used to restore the disk in the cases when the password is lost, or if the file-image has been accidentally corrupted if the operating system failed unexpectedly.

The backup copy is stored in encrypted form. To encrypt the backup copy, a special alternative access password, independent from the disk access password, is used.

To create a backup copy, do the following:

1. In **Dekart Private Disk MultiFactor**'s Control Panel click **Recovery**.
2. Press **Copy.**
3. Select the folder and the filename of the virtual encrypted disk file-image.

4. Enter the password to access the virtual encrypted disk.
5. The *Save encryption key* window will appear.
6. Select a folder to store the disk backup copy, enter the backup copy file name in the ***File Name field***, click ***Save***. The software will ask you to enter and confirm the backup copy alternative access password.
7. Enter the alternative password in the ***Password*** field and re-enter it in the ***Confirmation*** field. The entered password must be at least 5 symbols long. Otherwise, an insufficient password length message will appear.

Note. The **Dekart Private Disk MultiFactor** backup copy alternative access password can consist of alphanumeric symbols, and it is **case-sensitive**. Enter the password carefully.

5.20 Restoring the encryption key of the virtual encrypted disk from a backup copy

Dekart Private Disk MultiFactor allows you to restore the encryption key of the virtual encrypted disk using a previously created backup copy of the encryption key, thus restoring access to the encrypted disk itself (see the *Creating backup copy of the encryption key* section) .

To restore the encryption key from a backup copy, do the following:

1. In the Control Panel click **Recovery**.
2. The ***Open encryption key*** window will appear.
3. Select the folder where the encryption key backup copy is stored, enter the backup copy file name in the ***File Name*** field, click ***Open***.
4. The software will ask you to enter an access password for the encryption key backup copy.

   Note. The alternative backup copy access password can consist of alphanumeric symbols and it is **case-sensitive**. Enter the password carefully.

5. The software will ask you to select the folder and the name of the file-image, for which the encryption key should be restored.
6. Enter the new password in the ***Password*** field to access the file-image of the encrypted disk (independent from the password to access the encryption key backup copy) and re -enter it in the ***Confirmation*** field. The entered password must be at least 5 symbols long. Otherwise, an insufficient password length message will appear.

5.21 Forgotten password recovery

Dekart Private Disk MultiFactor allows you to recover the password of an encrypted disk, if you have partially forgotten it, by using a Brute-force attack method.

To start the password recovery attempt, please, do the following:

1. Go to the Control Panel, click ***Recovery*** > ***Password....***
2. The *Secret disk file image* window will appear.
3. Select the directory where the file-image of the encrypted disk is located, click on this file and click **Open**.
4. You will be prompted to enter the password properties - alphabet (password symbols) and password length.
5. Specify the alphabet (types of symbols), which you recall to have been used in your password, the password length and click **OK**. If you used any special characters that are not shown, enter them in the ***Extension*** field (e.g. Cyrillic symbols or umlauts) .
6. You will be asked to confirm the password properties entered at the previous step. Click **OK**.
7. The password recovery process window will appear.
8. Click **OK**.

You can stop the password recovery process by pressing the **Cancel** button. The software will allow you to save the current state of this process in order to continue the recovery from this saved state. If you agree, you will be able to start from the saved state next time you run the password recovery process again.

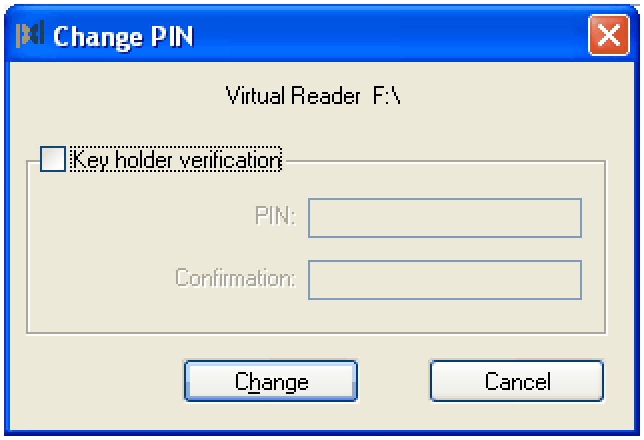
Note. The risk that a third party person will break your password and access your private data is minimized, provided that you follow our Recommendations for ensuring Dekart Private Disk security. Please read the How to recover a lost password guide for more details.

5.22 Setting and Changing a Virtual Disk's Access PIN

To avoid unauthorized access to the virtual disk, the Key PIN can be added. Setting and using the PIN allows you to implement strong two-factor Key user authentication, thus enhancing the security of Private Disk MultiFactor.

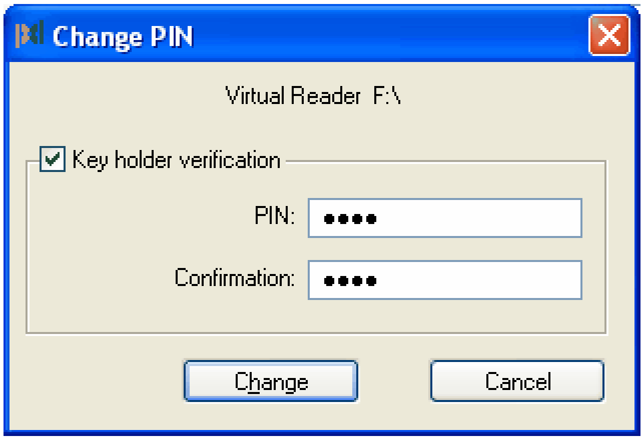
To set or change the disk access PIN, do the following:

1. Activate your Key.
2. In **Dekart Private Disk MultiFactor's** Control Panel, click ***Key Reader*** > ***Change PIN***. If the key is not PIN-protected, the ***Change PIN*** window will appear.



Change PIN window

3. Select the ***Key holder verification*** check box to enable the disk access PIN (if the checkbox is not selected, a PIN is not used to access the virtual disk). The ***PIN*** and ***Confirm PIN*** fields are active when the checkbox is selected.



Change PIN

Virtual Reader F:\

☑ Key holder verification

PIN: ●●●●

Confirmation: ●●●●

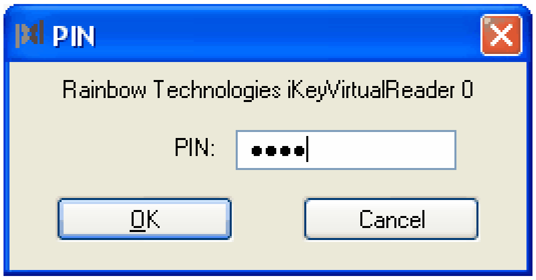
Accessing the PIN field and the Confirm PIN field

Note: By clicking ***Cancel***, you can cancel setting or changing the PIN.

4. Enter the PIN in the ***PIN*** and ***Confirm PIN*** fields (0 to 8 symbols), click ***Change***. If the values entered in the ***PIN*** and ***Confirm PIN*** fields do not match, the software will inform you about this.

   Click ***OK*** and enter the same values in the ***PIN*** and ***Confirm PIN*** fields, click ***Change***. From this point on, using the Key will be possible only if the right PIN is entered.

   The PIN request will appear whenever the smart card is inserted into the reader or the **Token** is attached to the computer.



PIN

Rainbow Technologies iKeyVirtualReader 0

PIN: ●●●●

PIN request window

Enter the private disk's access PIN and press ***Enter***. Pressing ***Esc*** cancels the PIN entry attempt.

Note: The PIN can consist of digits and symbols and it is **case-sensitive**. **Be careful entering the PIN — the electronic Key (smart-cartd or Token) is blocked after three consecutive wrong entries and cannot be used further until unblocked.**

Note: eToken R2 cannot be blocked after three consecutive wrong PIN entries.

5.23 Electronic Key Unblocking

The electronic Key is blocked after some consecutive wrong PIN entries (**eToken R2**, USB flash drive are not blocked), and the corresponding private disk becomes unavailable for further work. To make it available, the Key must be unblocked. The only way to unblock the Key is to know the right PIN. The Key cannot be unblocked if you do not know or have forgotten the right PIN.

To unblock the electronic Key, do the following:

1. In ***Dekart Private Disk MultiFactor***'s Control Panel, click ***Key Reader*** > ***Unblock*** (this menu option becomes available when a blocked smart card is inserted into the reader or a blocked **Token** is attached to the computer). The PIN request will follow.
2. Enter the PIN. If the entered PIN is correct, the Key is unblocked. If the entered PIN is wrong, an error message will appear.

   Note: The PIN can consist of digits and symbols, and it is **case-sensitive**. Enter the PIN carefully.
3. If the entered PIN is wrong, you can try to enter it again.

Note: After three consecutive wrong PIN entries to unblock the electronic Key, the Key permanently blocks its data about the private disk. The Key can still be used to create and operate other private disks after it is formatted. You can obtain the formatting utility from http://www.dekart.com/products/card_management/key_manager/.

5.24 Creating an Electronic Key Duplicate

For security reasons, you can create an electronic Key duplicate. If your main electronic Key becomes damaged or if you lose it, you can use its duplicate to access the private disk.

To create an valid electronic Key duplicate, do the following:

1. Activate your Key.
2. In **Dekart Private Disk MultiFactor**'s Control Panel, click ***Key Reader*** > ***Duplicate***.
3. When the request appears, select the original electronic Key from the list and attach a duplicate Key to the computer. This is the duplicate electronic Key, to which the data will be copied.

   Note: The PIN may be requested while handling PIN-protected electronic Keys (see the section Setting and Changing Virtual Disk Access PIN).

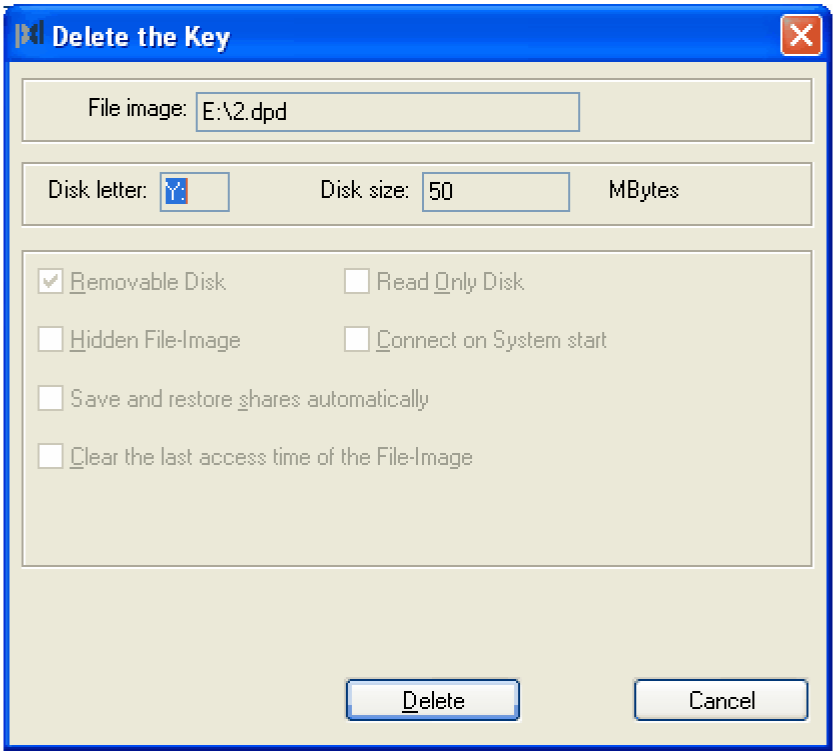
5.25 Electronic Key Data Deletion

Sometimes, it is necessary to delete **Dekart Private Disk MultiFactor** data from an electronic Key.

To permanently delete all of the electronic Key data, do the following:

1. Activate your Key; the Electronic Key data deletion window will appear on the screen.

2. In **Dekart Private Disk MultiFactor** Control Panel, click ***Key Reader*** > ***Delete*** .



File image: E:\2.dpd

Disk letter: Y: Disk size: 50 MBytes

☑ Removable Disk □ Read Only Disk

□ Hidden File-Image □ Connect on System start

□ Save and restore shares automatically

□ Clear the last access time of the File-Image

Electronic Key data deletion window

3. Click ***Delete***. The deletion confirmation request will follow.

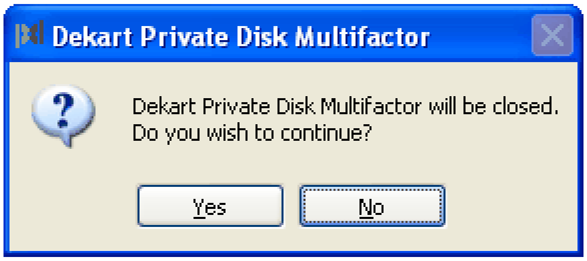
   Note: Clicking ***Cancel*** cancels the electronic Key data deletion process.

4. Click ***Yes*** to proceed with the data deletion operation, click ***No*** to terminate it.

5.26 Exiting Private Disk Multifactor

You can quit **Dekart Private Disk MultiFactor** in one of the following ways:

1. Right-click the **Dekart Private Disk MultiFactor**'s systray icon to activate system menu. Select ***Exit***.
   Note: If Private Disk was installed to a flash drive, use the ***Exit and safely remove hardware*** option.
   Note: If you wish to use the flash disk after quitting Private Disk MultiFactor, use the standard ***Exit*** option.
2. If you unchecked the ***Closing the window will minimize the program to System taskbar*** checkbox in the ***Options*** menu, click the ***Exit*** button**,** or use the close window button in the top right corner of the window, or press *Alt* + *F4*.
   A confirmation request will follow.


Dekart Private Disk Multifactor

Dekart Private Disk Multifactor will be closed.
Do you wish to continue?

Work completion confirmation

Click ***Yes*** to close the program, click ***No*** to cancel.

5.27 Biometric authentication

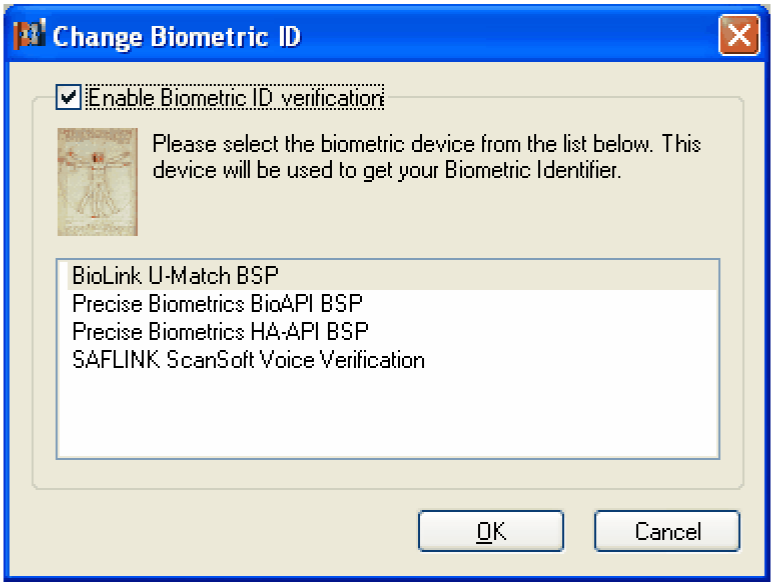
If the three-factor authentication is enabled (the **Enable Biometric ID verification** checkbox is checked in the **Change Biometric ID** window), biometric authentication will be performed after the user activates the Key**,** and the PIN of the Key is successfully verified (if the Key is PIN protected)**.** The software will automatically read the biometric identifier stored on the Key and will ask the user to provide their biometric data (scan the fingerprints, pronounce the authentication phrase etc.). In case the BIO ID provided by the user does not match the template stored on the Key, the user will be asked to repeat the biometric authentication. The authentication routine is successful only when the data provided by the user are identical to the biometric template stored on the Key. This approach ensures that only an authorized user can get access to the secret data. Thus, even if the Key is lost or stolen, no unauthorized user will get access to the secret disk.

5.27.1 Adding a BIO ID to the Key

In order to enable three-factor authentication, the Key should contain the user's biometric identifier.

In order to add a BIO ID, follow theses steps:

1. Click the ***Key Reader*** > ***Change BIO ID***. The window with the list of installed drivers for biometric devices will appear.



Change Biometric ID

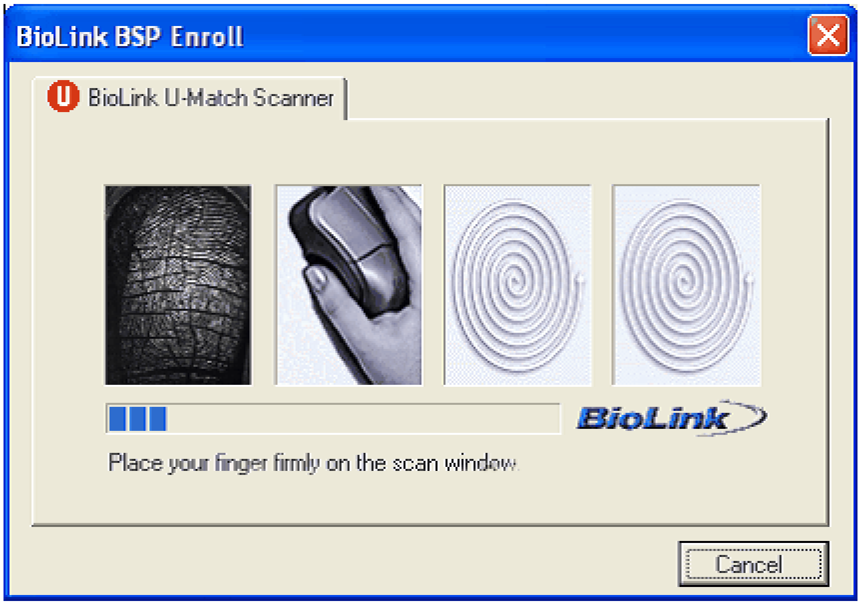
☑ Enable Biometric ID verification

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

- BioLink U-Match BSP
- Precise Biometrics BioAPI BSP
- Precise Biometrics HA-API BSP
- SAFLINK ScanSoft Voice Verification

Selecting a biometric device

2. Check the **"Enable Biometric ID verification"** checkbox and select the biometric device from the list.
3. If a fingerprint scanner is used, e.g. BioLink U-Match, the user will be asked to press their fingers against the scanner several times. As soon as the scanning procedure is complete, the user's BIO ID is stored on the Key.



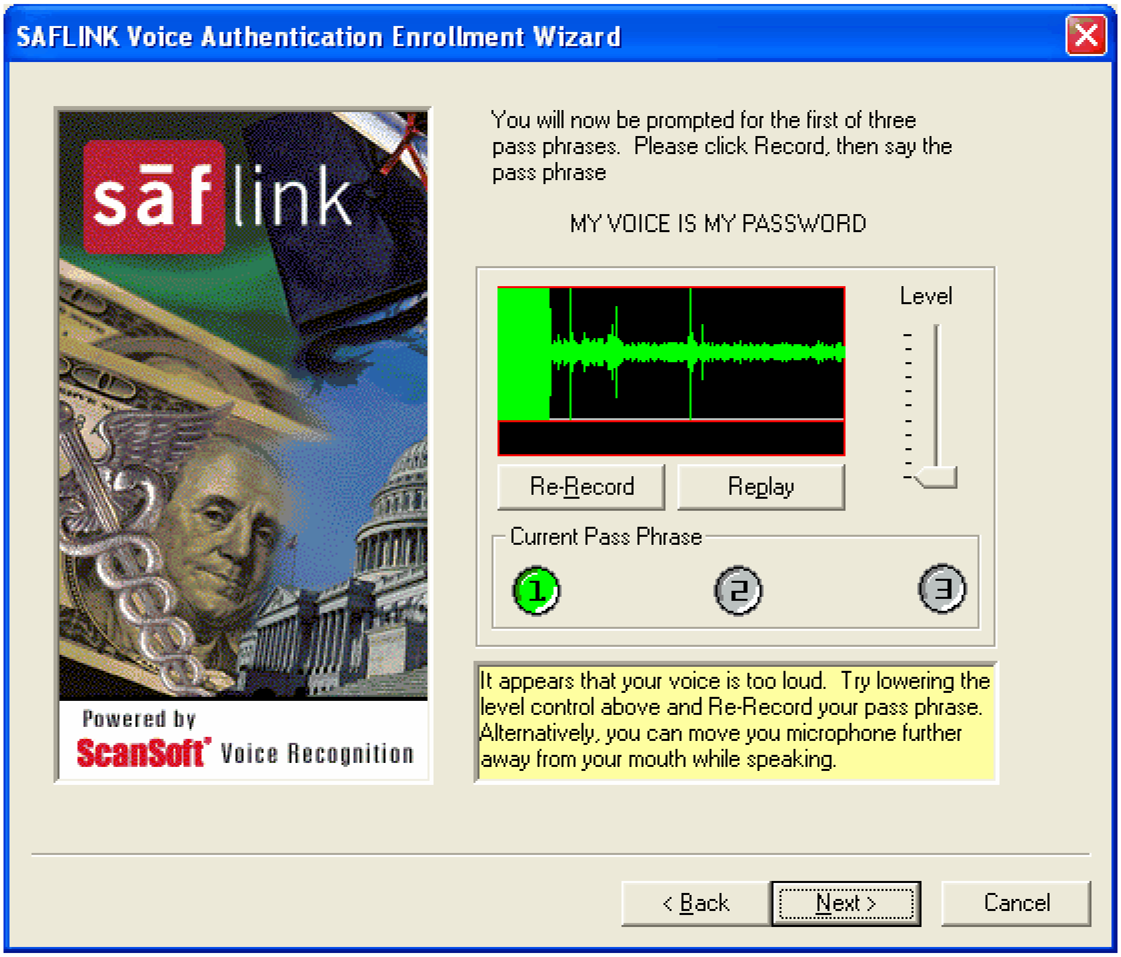
BioLink BSP Enroll

BioLink U-Match Scanner

Place your finger firmly on the scan window.

Presenting a biometric identifier - a fingerprint

If a voice recognition device is used, e.g. SAFLINK Scansoft Voice Verification, the user will be asked to pronounce the key-phrase. After the voice template is created, it is then stored on the Key.


SAFLINK Voice Authentication Enrollment Wizard
sāflink
Powered by ScanSoft Voice Recognition
Level
Re-Record
Replay
Current Pass Phrase
1
2
3
< Back
Next >
Cancel

You will now be prompted for the first of three pass phrases. Please click Record, then say the pass phrase

MY VOICE IS MY PASSWORD

It appears that your voice is too loud. Try lowering the level control above and Re-Record your pass phrase. Alternatively, you can move you microphone further away from your mouth while speaking.

Presenting a biometric identifier - a key phrase

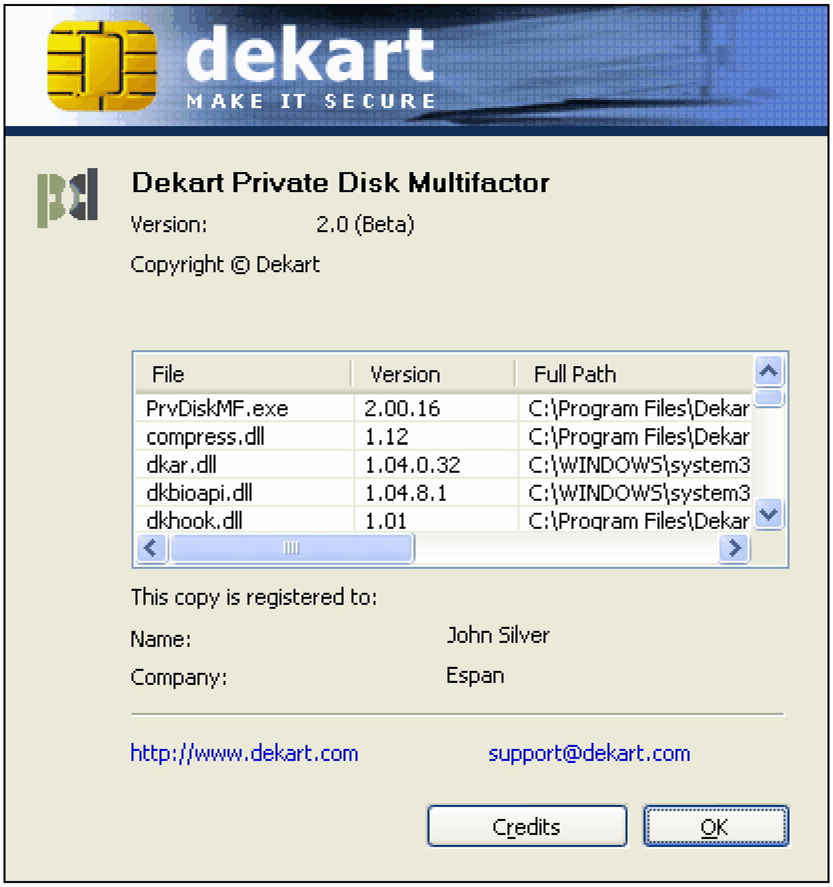
5.27.2 Changing the BIO ID

To change the BIO ID (if it has been previously stored on the Key), please follow the steps described in the Adding BIO ID to the Key section.

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

5.28 Viewing information about Dekart Private Disk MultiFactor

To view information about **Dekart Private Disk MultiFactor,** go to ***Dekart Private Disk MultiFactor's*** Control Panel, Click ***Help*** > ***About...***. The following window will appear:



Dekart Private Disk Multifactor

Version: 2.0 (Beta)

Copyright © Dekart

File	Version	Full Path
PrvDiskMF.exe	2.00.16	C:\Program Files\Dekar
compress.dll	1.12	C:\Program Files\Dekar
dkar.dll	1.04.0.32	C:\WINDOWS\system3
dkbioapi.dll	1.04.8.1	C:\WINDOWS\system3
dkhook.dll	1.01	C:\Program Files\Dekar

This copy is registered to:

Name: John Silver

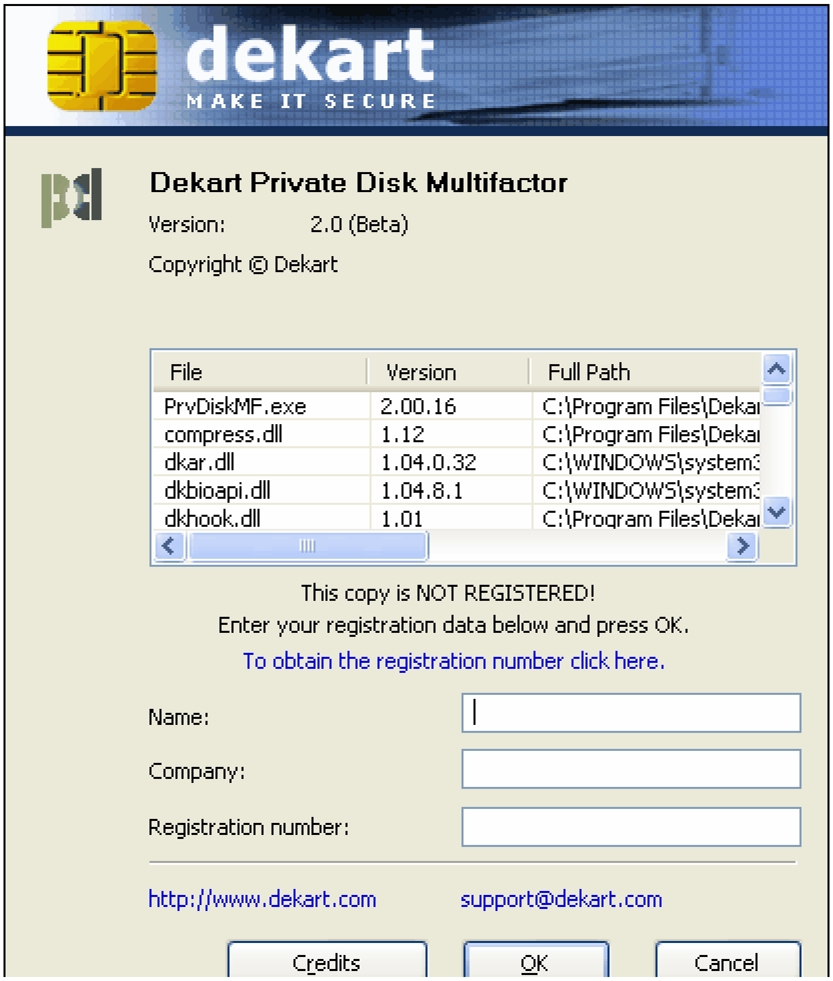
Company: Espan

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

The About dialog

5.29 Registering Dekart Private Disk MultiFactor

To register the product, please go to *Dekart Private Disk MultiFactor*'s Control Panel, Click ***Help*** > ***About...***. Please, fill in the required information into the fields.



Dekart Private Disk Multifactor

Version: 2.0 (Beta)

Copyright © Dekart

File	Version	Full Path
PrvDiskMF.exe	2.00.16	C:\Program Files\Dekar
compress.dll	1.12	C:\Program Files\Dekar
dkar.dll	1.04.0.32	C:\WINDOWS\system3
dkbioapi.dll	1.04.8.1	C:\WINDOWS\system3
dkhook.dll	1.01	C:\Program Files\Dekar

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

Registration form

Please, obtain a registration number at the *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.

6 Troubleshooting

This chapter contains:

- **List of Possible Problems**. The listed situations can occur during the hardware and software installation process. They are indicated in the *Situation* column of the *Possible Problems* table.
- **List of Troubleshooting tips**. These are actions that should be performed if a certain situation occurs during the hardware and software installation process. They are indicated in the *Solution* column of the *Possible Problems* table.
- **List of Diagnostic Messages**. These messages result from incorrect user actions or

hardware or software errors that occur while **Dekart Private Disk MultiFactor** is running. For convenience, messages are given in alphabetical order, in the *Message* column of the *Diagnostic Messages* table.

- **List of Message Explanations**. These descriptions are given in the *Explanation* column of the *Diagnostic Messages* table.
- **List of Troubleshooting Actions**. The actions that should be performed when a certain message from the *Diagnostic Messages* table is shown.

6.1 Possible Problems

If any contingencies occur during **Dekart Private Disk MultiFactor's** installation or hardware connection, please refer to the table of *Possible Problems*:

- The *Situation* column describes the problems that can occur during the software installation and hardware connection.
- The *Solution* column contains the descriptions of the actions that should be taken to handle the corresponding situation.

Possible Problems

Situation	**Solution**
1. The operating system cannot identify the smart card reader or the **Token** and suggests that it should be installed.	Cancel this action (click ***Cancel***) and install the reader/**Token** drivers. For drivers and consultation, refer to the reader/**Token** manufacturer or to **Dekart Private Disk MultiFactor** technical support (see item 8).
2. The operating system recognizes the reader/**Token**, the ready-to-work indicator glows when the smart card is inserted (the **Token** reader indicator glows when it is attached to the computer), but the smart card/**Token** is not read.	Try restarting the computer or replacing the smart card/**Token**
3. The operating system recognizes the reader, its indicator glows when the smart card is inserted, or the **Token** indicator glows when it is attached to the computer, but the smart card/**Token** does not read even after multiple computer restarts – carry out the actions as stated in item 1.	Install the reader drivers. For drivers and consultation, refer to the reader manufacturer or to **Dekart Private Disk MultiFactor** technical support service (see item 8).
4. The operating system recognizes the reader, its indicator glows when the smart card is inserted (or the **Token** indicator glows when it is attached to the computer), but the reader indicator starts flashing shortly after the card is inserted. or errors occur frequently during the program's operation.	Replace the smart card/**Token**, if the problems persist, make sure that the port to which the device is attached is properly-powered,..
5. The operating system recognizes the reader, **Dekart Private Disk MultiFactor** operates properly, but the mouse connected in series with the smart card reader does not work.	Install the reader driver – . For drivers and consultation, refer to the reader/Token manufacturer or to **Dekart's** technical support(see item 8).
6. The operating system does not recognize the smart card reader/**Token**.	Check the reader/**Token** connection to the ports, check the ports (refer to the computer vendor).

7. The computer ports and the reader connection are good, but the operating system does not recognize the smart card reader/**Token**.	Refer for drivers and consultation to the reader/**Token** manufacturer or to **Dekart‘s** technical support (see item 8).
8. In all the other cases, refer to **Dekart ‘s** technical support.	Please provide a detailed description of the problem

6.2 Diagnostic Messages

When a diagnostic message shows up while **Dekart Private Disk MultiFactor** is running, refer to the table below:

- The *Message* column contains the message shown on the screen.
- The *Explanation* column provides a detailed description of the error message.
- The *Action* column enumerates the measures that need to be taken.

Note: To disable the message, press ***Esc*** or remove the smart card from the reader or detach the Key from the computer.

Note: Before starting troubleshooting actions, always try to repeat the last operation.

The *Diagnostic Messages* table is given below.

Diagnostic Messages

Message	**Explanation**	**Action**
An error occurred while processing the Key!	The symbol of the disk being connected is used by another drive or has an illegal value.	Change the symbol identifying the disk in the operating system (see the section *Changing Virtual Secret Disk Properties*).
	Operating system error	Exit all applications and restart the computer.
	Hardware error (COM port, reader, or smart card/**Token** error).	Try to use a Key duplicate or check (replace) the COM port or the reader.
	Disk image file handling error.	Check whether the disk image file has been damaged or deleted or whether this file is currently used by another application.
No Key reader has been detected by the system!	The active smart card reader/ **Token** is not detected in the operating system when **Dekart Private Disk MultiFactor** is started.	Connect the reader/**Token** to the computer (or wait until the smart card reader/**Token** service is started) and try to re-start **Dekart Private Disk MultiFactor**. If the problem persists, refer to the section *Possible Problems* .
The Key is blocked!	The electronic Key has been blocked after three consecutive wrong PIN entries.	To continue using the electronic Key, the smart card/**Token** must be unblocked with the right PIN (see the section *Electronic Key Unblocking*).
The Key is empty!	The electronic Key does not contain any information about a virtual disk.	Create a new virtual disk (see the section *Creating Virtual Secret Disk*).
The PIN you entered is incorrect!	A wrong PIN was entered.	The right PIN must be entered to proceed.

The PIN you entered to unblock the Key is incorrect!	While unblocking the electronic Key, a wrong PIN was entered.	The right PIN must be entered to unblock the Key.
This Operating System is not supported!	**Dekart Private Disk MultiFactor** is not supported by the current operating system.	Refer to **Dekart’s** technical support.
Unable to activate help!	The **Help** system is not available.	This can occur due to the following reasons: the help file of **Dekart Private Disk MultiFactor**, **PrvDisk.hlp** is missing or **WinHelp** is not installed in Windows. Refer to **Dekart‘s** technical support.
Unable to backup the Private Disk MultiFactor!	The virtual disk cannot be read.	Check the virtual secret disk’s integrity. There may be file system errors – try to fix them.
	Backup file write error.	Check the integrity of the media to which you attempted to write the backup copy. It may have bad sectors, or there is not enough disk space. Try to solve these problems or find another disk storage unit.
Unable to restore Secret disk!	The size of the connected encrypted disk is smaller than the size of the backup.	Connect the encrypted disk of the required size and repeat the operation.
	Error while reading the backup copy file.	Check the integrity of the media containing your backup copy for bad sectors, or file system errors. Check if there is enough space on the disk.
	Error while writing the encrypted disk.	Check the integrity of the virtual disk, if there are any file system errors on the disk and try to fix them.
Unable to change to server mode!	Server mode cannot be activated.	Check if you have the administrator's rights required to start/stop Windows NT/2000/XP drivers and services. If you have the required rights, but the message recurs, refer to **Dekart Private Disk MultiFactor** technical support service.
Unable to create the Private Disk MultiFactor!	The virtual disk cannot be created.	Check if there is enough free disk space on your computer to create the virtual secret disk. If there is not enough free space, indicate the available secret disk volume in its properties (***Disk*** > ***Create*** > ***Disk size*** > ***… Mbytes***). If there is enough free space, check the integrity of the media and fix the errors that are revealed; or select another disk storage unit. The symbol indicating the disk being created can have an illegal value. If you are using Windows 9x, correct the **LASTDRIVE** instruction in the **config.sys** file and reboot your computer.
Unable to initialize the Key reader!	The reader/**Token** in use is not recognized by **Dekart Private Disk MultiFactor**.	In **Dekart Private Disk MultiFactor’s** menu, choose a smart card reader/ **Token** used via ***System*** > ***Key Reader***. If the problem persists, refer to the *Possible Problems* section.
Unable to load Windows Smart Card Service!	The Windows Smart Card Service cannot be started.	Ensure that the Windows Smart Card Service is installed on your computer. If it is not installed, contact the system administrator. If the problem persists, refer to **Dekart‘s** technical support.
Unable to restore the Private Disk MultiFactor!	Wrong backup copy alternative access password was entered.	Enter the right backup copy alternative access password.

	Virtual disk write error.	Check the integrity of the virtual secret disk. It may have file system errors.
	Backup file read error.	Check the integrity of the media storing the backup copy. It may have bad sectors or disk file systems errors.
	The memory capacity of the recovered data exceeds the size of the connected virtual disk.	Create a new virtual disk with more free space.
Unknown Key!	The inserted electronic Key is not for use with **Dekart Private Disk MultiFactor** or with its current version, or it is not formatted to work with Dekart applications.	**MultiFactor** Key or try to format the key using the Key Formatting Utility. If the problem persists, refer to **Dekart's** technical support.
You do not have sufficient administrative rights for this operation!	**Dekart Private Disk MultiFactor's** driver cannot be started.	Check whether you have sufficient privileges to start/stop **Dekart Private Disk MultiFactor's** drivers. If you have the required rights, but the message persists, refer to **Dekart's** technical support.
Not enough administrative privileges to perform this operation!	You don't have enough privileges to enable/disable Server mode.	Please, login as an administrator and repeat the operation.
Unsuccessful biometric registration!	Could not register the biometric identifier on the Key.	Repeat the operation. If the situation repeats, try using another biometric identification device.
Unsuccessful biometric verification!	The biometric identifier you have presented does not match the template stored on the Key.	Repeat the operation. If the problem persists, check your biometric device.
Key permanently blocked.	After multiple wrong PIN code entries attempting to unblock the Key, the Key is permanently blocked.	Re-format your **Key** using Key Formatting Utility**.**
Unknown key!	You have attempted to read/write data using a Key not supported by **Dekart Private Disk MultiFactor**	Use one of the Keys listed in the Supported devices section.

7 Glossary

Term	**Description**
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.

Driver
This is software designed to control data input/output and interface the applications/*OS* and the device connected to the *PC*.

Electronic Key
This can be either a *smart card* or the *Token or other similar device*.

eToken
This is a special device, also called *the eToken Key*, produced by Aladdin Knowledge Systems as a Key-ring style hardware device and employed by **Dekart Private Disk MultiFactor**. This is a full-scale analog of a smart card that can be attached to the *USB* port and used as a means for identifying a user.

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.

Personal Computer/Smart Card (PC/SC)
Smart card readers' specifications.

Personal Identification Number
See *PIN*

PIN
The *Personal Identification Number* is used for **Dekart Private Disk MultiFactor** user's virtual disk data access authentication. The PIN is set by the Key user by means of **Dekart Private Disk MultiFactor** facilities.

Plug-and-play
This is a standard designed by Microsoft, Intel, etc. in order to simplify connection of additional devices to the computer. The operating system (Windows 95, Windows 98, Windows 2000 Professional, Windows XP, Windows Me) identifies and sets up the peripheral device without any user interference or further manual parameter setting. Plug and Play (PnP) is a capability developed by Microsoft for its Windows 95 and later operating systems that gives users the ability to plug a device into a computer and have the computer recognize that the device is there.

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

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

Strong Authentication
This is a process controlling the authenticity of the users identity on the basis of at least two of the three following factors:
Something You Know — for example, the user name and password.
Something You Have – for example, the *Token* device.
Something You Are – for example, fingerprints or specific physical traits.

Three-Factor Authentication
This is a process controlling the authenticity of the users identity on the basis of three following factors:
Something You Know — for example, the user name and password.
Something You Have – for example, the *USB drive*.
Something You Are – for example, fingerprints or specific physical traits.

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 *CD* device.

Universal Serial Bus (USB)
The Universal Serial Bus can be used to connect and disconnect peripheral devices without opening the PC case and even without shutting down the computer. The *USB* automatically detects these devices and configures the corresponding software.

OS
Operating System

PC
Personal Computer.