dekart

MAKE IT SECURE

USER GUIDE

DEKART PRIVATE DISK

1 Preface

Dekart Private Disk is cost-effective and easy-to-use software which provides secure access to Document and Files on PC. **Dekart Private Disk** creates a virtual encrypted disk where user can place all important information, which can be accessed by entering the correct password.

1.1 Operating Guide purpose

This *Operating Guide* is designed for **Dekart Private Disk** users and contains information about installing, operating and de-installing **Dekart Private Disk**.
This *Guide* contains the list of requirements to provide the proper operation of **Dekart Private Disk**.

1.2 Operating Guide structure

This *Guide* consists of the following chapters:

- *Introducing Dekart Private Disk*describes the purpose and the features of **Dekart Private Disk**.
- *Dekart Private Disk hardware and software requirements* lists and describes PC software and hardware required for **Dekart Private Disk** to operate properly.
- *Dekart Private Disk installation, update and de-Installation* describes in detail how to install, update, and de-install **Dekart Private Disk** and its auxiliary components.
- *Using Dekart Private Disk* thoroughly describes all aspects of operating **Dekart Private Disk**.
- *Troubleshooting* is devoted to detecting and eliminating possible problems. All diagnostic messages and events causing them are listed, the troubleshooting measures are suggested.
- Glossary is an explanatory dictionary containing important terms used in this *Guide*.

1.3 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***.

1.4 License agreement

any express or implied warranties of merchantability or fitness for any particular purpose. Further, Dekart reserved the right to revise this publication and to make changes to its content, at any time, without any obligation to notify any person or entity of such revisions or changes.

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

LICENSE AGREEMENT

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

DEKART TRADEMARK ATTRIBUTIONS

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

1.5 How to contact Dekart

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

Technical Support
You can receive technical support for **Dekart Private Disk** contacting us at support@dekart.com.

Comments and suggestions
If you have ideas, suggestions, comments, critics or questions, we would love to hear from you about our software or documentation by email info@dekart.com.

Customer Service
For ordering or getting information about **Dekart** products please contact us by e-mail: sales@dekart.com.

2 Introducing Dekart Private Disk

This chapter describes the purpose and features of **Dekart Private Disk**.

2.1 How Dekart Private Disk protects your proprietary information

To start using **Dekart Private Disk,** please follow the instructions:

1. **Read this Guide**.
2. Install **Dekart Private Disk**

Once the installation is complete you can use the **Dekart Private Disk** software to create and access encrypted virtual disk.

2.1.1 How Dekart Private Disk protects your data

Dekart Private Disk creates virtual encrypted disk and user may use it as usual hard disk in Windows. User defines file-image and password for this encrypted disk. "Virtual disk" means that all files and folders after encryption go to file-image. User should specify this file-image and access password when it is necessary to connect a disk and get access to Files and Folders. Every disk has its own letter (C:, D:) in Windows. Virtual disk also has its letter which you define on creation.
All of the programs that you are accustomed to working with will not be affected in any way when using standard and virtual disks. For them, this will be just another hard disk. The file-image of a virtual encrypted disk can have any name, extension, and access path (even a network path is good). The password is the only way to access virtual encrypted disk.
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 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 256 bit long requires 4.2×10^{22} processors performing 256 million encryption operations per second. But even in this case, the key will be cracked in a year.
Installing **Dekart Private Disk** is easy, and should not take longer than a minute. **Dekart Private Disk** is easy to operate. Just point it on file-image and enter password. Now you can work with your data in the usual fashion in virtual disk.
For more details on operating **Dekart Private Disk**, please refer to chapter of this *Guide*, *Using Dekart Private Disk*.

2.1.2 How Dekart Private Disk protects your workplace

Let us consider how **Dekart Private Disk** locks the door to information during the temporary interruptions of work, for example, when you leave your office. You can disconnect virtual disk using a hot-key!
Of course on return you should again specify the file-image and access password to connect this disk again.
For more details on operating **Dekart Private Disk**, please refer to of this *Guide*, *Using Dekart Private Disk*.

2.2 Main features

Dekart Private Disk has the following characteristics:

- The ***Advanced Encryption Standard (AES)*** in ***CBC*** mode with 256 bit key length is used as an encryption algorithm.
- Cryptographic hashing function **SHA-1** 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 XP, Windows 2003**.

2.3 Dekart Private Disk components

Dekart Private Disk consists of the following mandatory components:
- Software **Dekart Private Disk**.
- This *Operating Guide*.

3 Dekart Private Disk hardware and software requirements

This chapter describes the following:
- **Dekart Private Disk** personal computer hardware requirements.
- Operating systems with the corresponding service packs required for **Dekart Private Disk** to run properly.

3.1 Personal Computer hardware requirements

For **Dekart Private Disk** to run properly, a PC with the following minimum properties is required (this applies mainly to the computers running Windows 95):
- Intel Pentium 166 MHz processor
- 16 MB RAM
- 2 MB or more free hard disk space

3.2 Personal Computer software requirements

Dekart Private Disk supports the following operating systems:
- 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.
- Windows XP Professional, Home Edition.

4 Dekart Private Disk installation, update and de-installation

Before installing, make sure that the PC meets the product hardware and software requirements indicated in the *Dekart Private Disk hardware and software requirements*.
Note: In order to install the product components under Windows operating systems designed for corporate use — Windows NT, Windows 2000, Windows XP — it is necessary to logon to the system as an administrator. In Windows operating systems designed mainly for private use — Windows 95/98/ME, Windows XP Home — every user has the required rights.

4.1 Installation

Note. In order to be able to install **Dekart Private Disk** on Windows NT, Windows 2000, Windows XP, you must have administrator privileges.
Do the following to install **Dekart Private Disk**:

1. Run PrvDisk.exe or Insert **Dekart Private Disk** product CD into the CD-ROM drive and SETUP.EXE. If you have downloaded the installation file from the Internet, please run PrvDisk.exe.
   Note. You can start the PrvDisk.exe module using command line with "/s" parameter (e.g., c:\PrvDisk_ru.exe /s). In this case the program will perform all required actions in silent mode (without displaying any information to the user).
2. The welcome screen will appear, as shown in Figure 1.

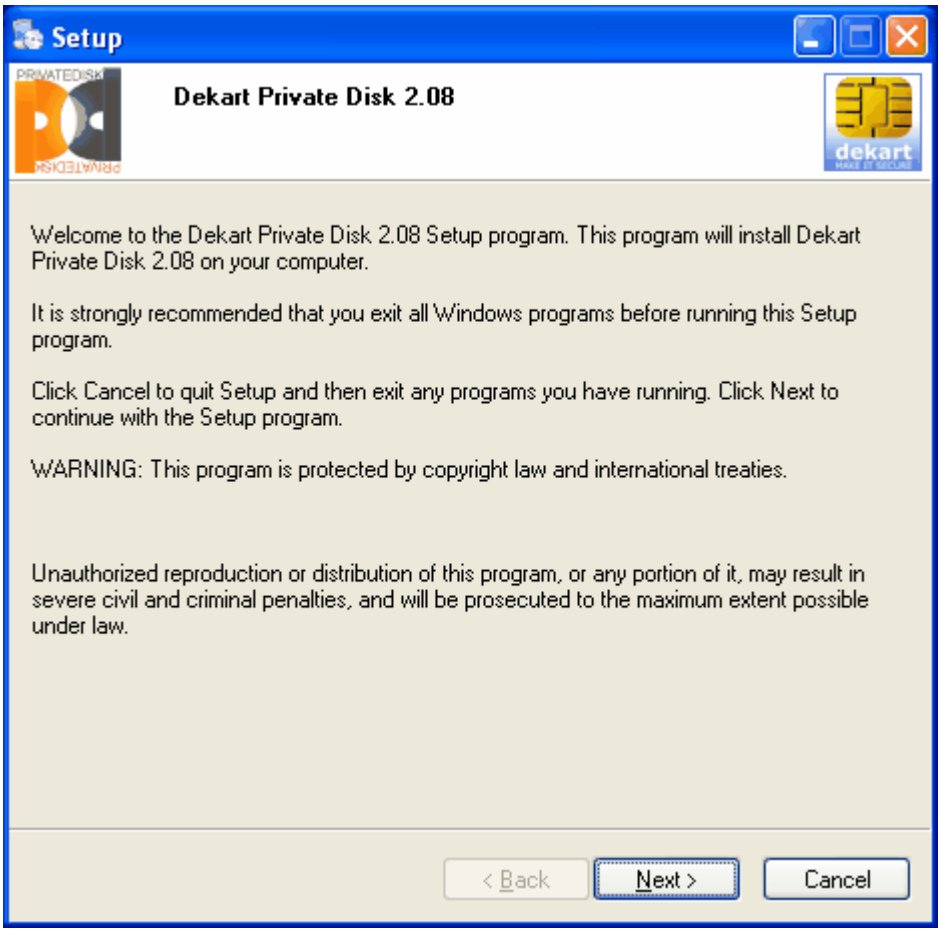

Figure 1
Dekart Private Disk welcome screen

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

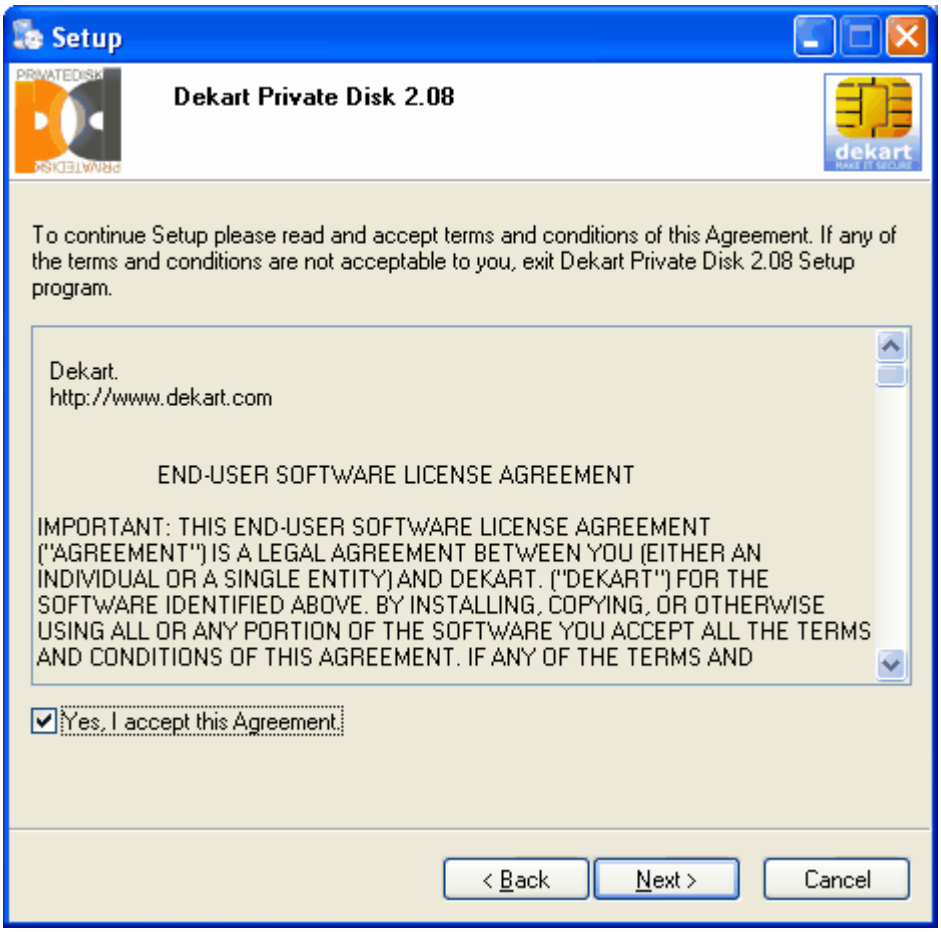

Figure 2
Dekart Private Disk license agreement

4. Carefully read the text of the license agreement between you, **Dekart Private Disk** end-user, and **Dekart**. Select ***Yes, I accept this agreement*** check box if you agree with the terms, and click ***Next***. The ***Registration*** window will appear, as shown in Figure 3.
   Note: If you do not agree with the terms of license agreement, *do not select* the check box and click ***Cancel***. In this case, **Dekart Private Disk** installation will be terminated.

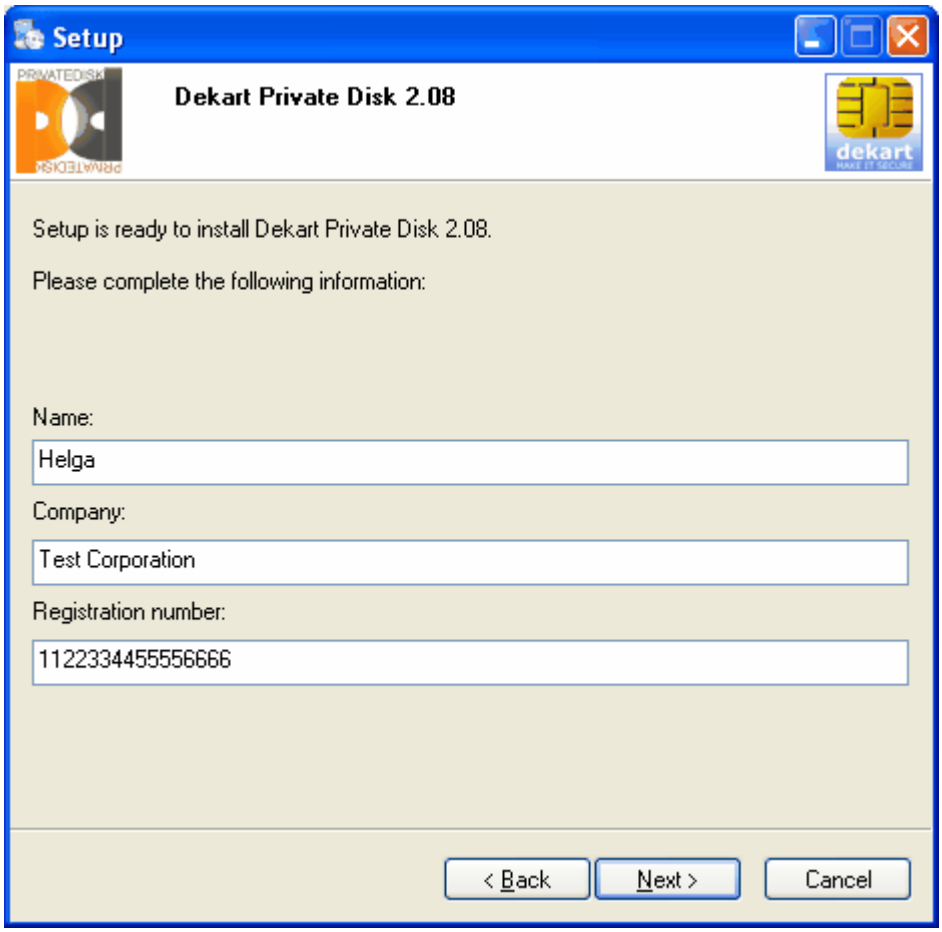

Figure 3
Dekart Private Disk Registration window

1. Fill out the fields in the registration window and click ***Next***. A product location selection screen will appear, as shown in Figure 4.
   Note: The serial (licence) or registration number of your **Dekart Private Disk** copy must be entered into the ***Registration Number*** field.

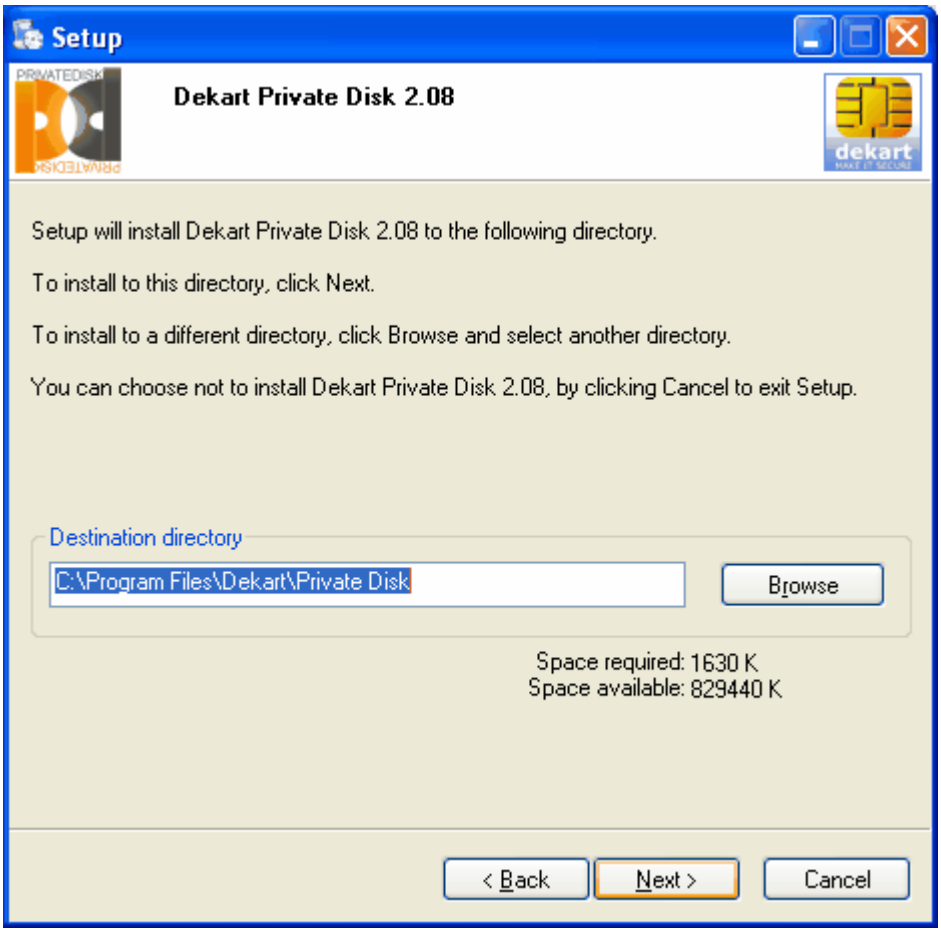

Figure 4
Dekart Private Disk destination location

6. Indicate the directory into which **Dekart Private Disk** should be installed on your computer and click ***Next***. A program folder selection screen will appear, as shown in Figure 5.

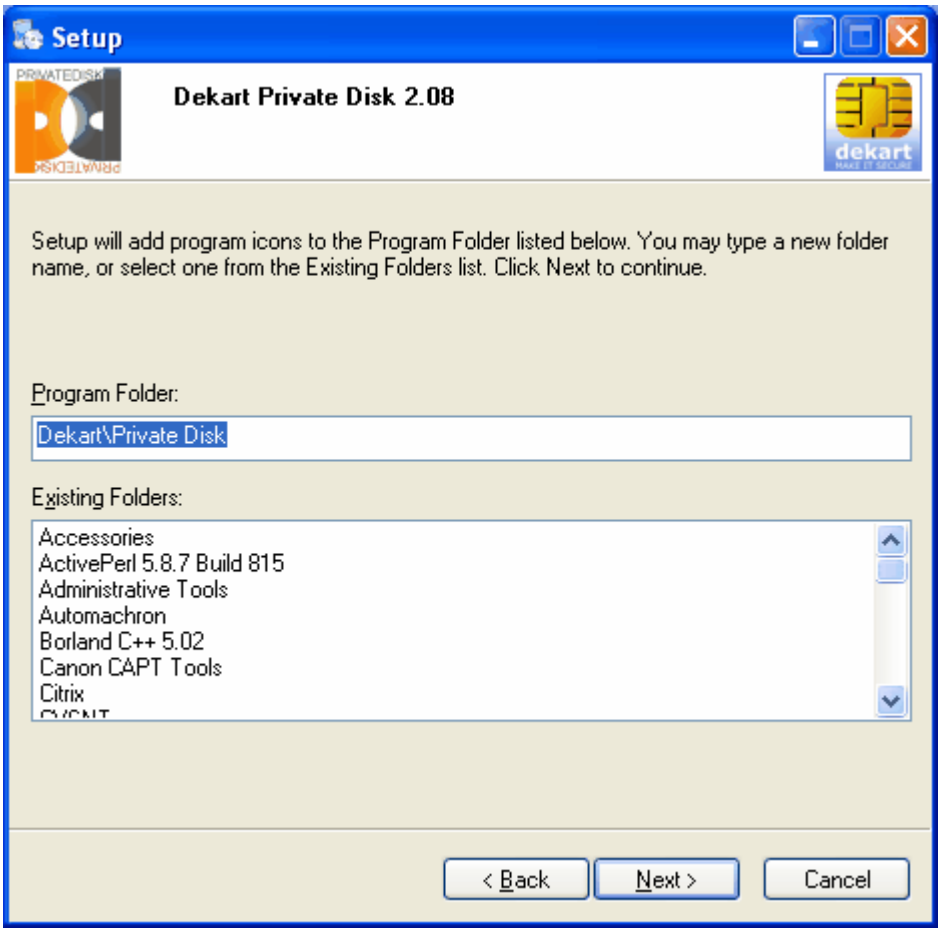

Figure 5
Dekart Private Disk folder

7. Indicate **Dekart Private Disk** folder name on your computer and click ***Next***. A ***Ready to Install*** window will appear, as shown in Figure 6.

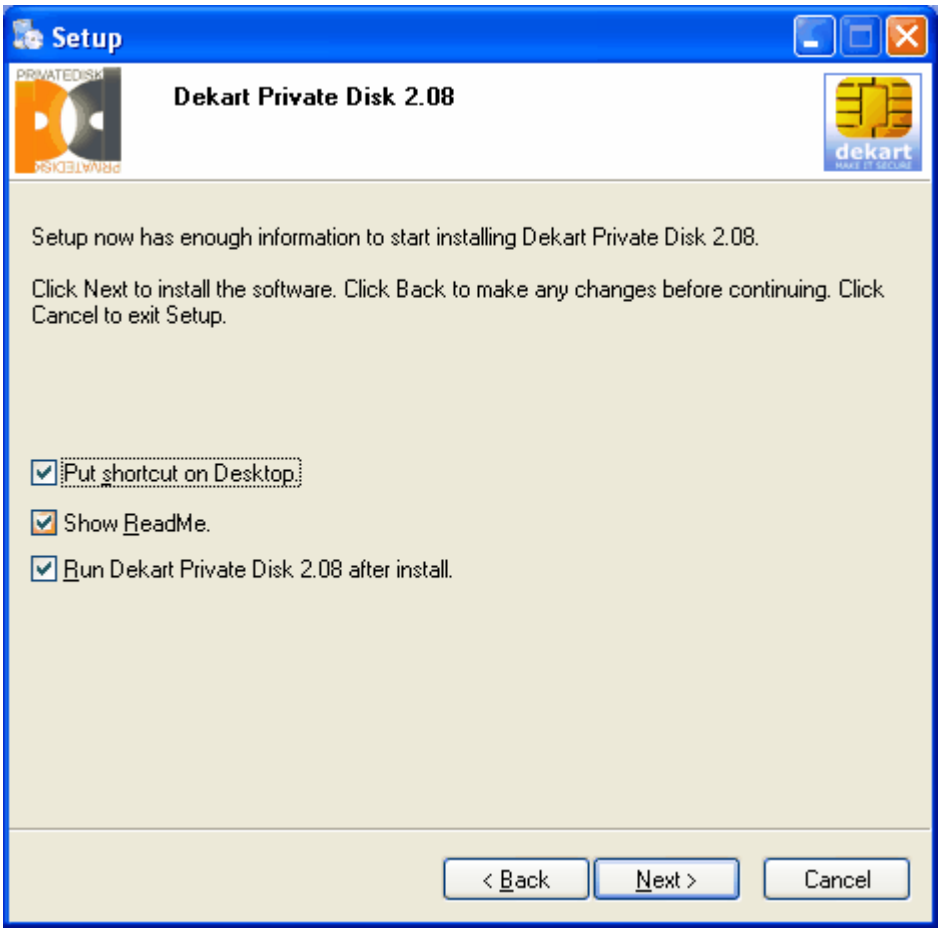

Figure 6
Ready to Install Dialog

8. Please, select the installation options (creating the application icon on desktop, displaying readme.txt, running Dekart Private Disk after installation) and click ***Finish***.
9. Wait until the installation completion window appears, as shown in Figure 7.

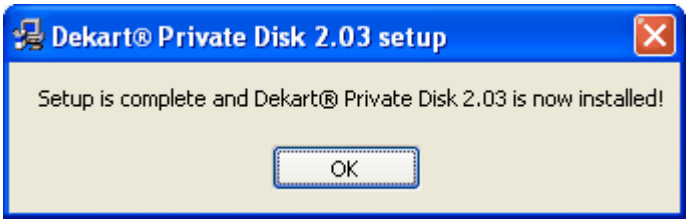

Figure 7
Setup complete

10. Click ***OK***.
11. All of the system changes enabled by the installation will take effect after restarting the computer. Restart the computer automatically now or by hand later.

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 to a removable drive (Flash drive), see Installation to removable disk

4.2 Re-installation of Dekart Private Disk

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

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

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

4.3 Updating Dekart Private Disk

Dekart Private Disk can be updated upon acquiring a newer version of the product.
To acquire a newer version of the product, please refer to **Dekart** technical support service and remember to indicate your registration number. The corresponding software can be downloaded from http://www.dekart.com or specially ordered.
To install the newer version of **Dekart Private Disk** on the computer, start the PrvDisk.exe or SETUP.EXE file from the product CD. The installation utility will find the current version of the product and will suggest that it be updated. Further actions are similar to those described in the *Installation* section of this chapter.

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

4.4 Removing Dekart Private Disk

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

1. Exit **Private Disk** (if it is active).
2. Choose **Uninstall** from **Private Disk** group at **Start Menu** (**Start > Programs > Dekart > Private Disk)**. OR Use ***Add/Remove Programs*** dialog from Control Panel to remove program ***(Start*** > ***Settings*** > ***Control Panel).***

After this the system will require to confirm the software removal, as shown in Figure 8.

Figure 8
Remove confirmation

3. On clicking ***Yes***, the system will remove program and report about the successful completion, as shown in Figure 9. **Note:** on clicking ***No***, de-installation is terminated.

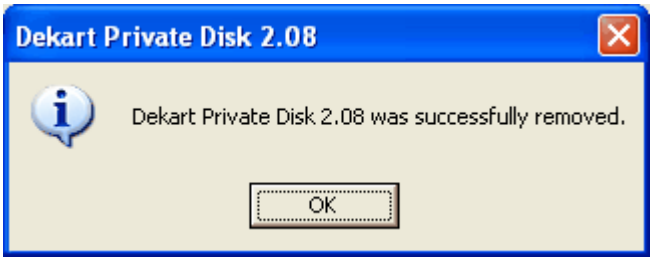

Figure 9
Remove complete

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

Note. If Private Disk was installed to a removable drive, you can uninstall it by deleting the **flash_disk:\..\Private Disk**\ 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 Using Dekart Private Disk

The main purpose of this chapter is familiarizing the user with main features and functions of **Dekart Private Disk**.

5.1 Getting started

After successful Dekart Private Disk installation and Windows reboot, run Dekart Private Disk. To run Dekart Private Disk, select one of the following:

- Double-click the Desktop Private Disk icon, if you have created the application Desktop shortcut during Private Disk installation.
- Go to ***Start > Programs > Dekart > Private Disk > Private Disk***.
- Use Windows Explorer to select the Private Disk folder and double-click the application icon. **Note**. If Private Disk is installed to a removable drive, you can start

the application by double-clicking the program's icon in **flash_disk:\..\Private Disk** (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; Administrative privileges are not required if the program was previously launched by an administrator on the computer on which you wish to use it).

You will see program window and Private Disk icon (bulb) in system tray (where is the system clock and keyboard indicator) as shown in Figure 10.

Figure 10
Dekart Private Disk taskbar icon

5.2 Installation to 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'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 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 Dekart Private Disk control panel

Dekart Private Disk is managed using its Control panel, as shown in Figure 11.

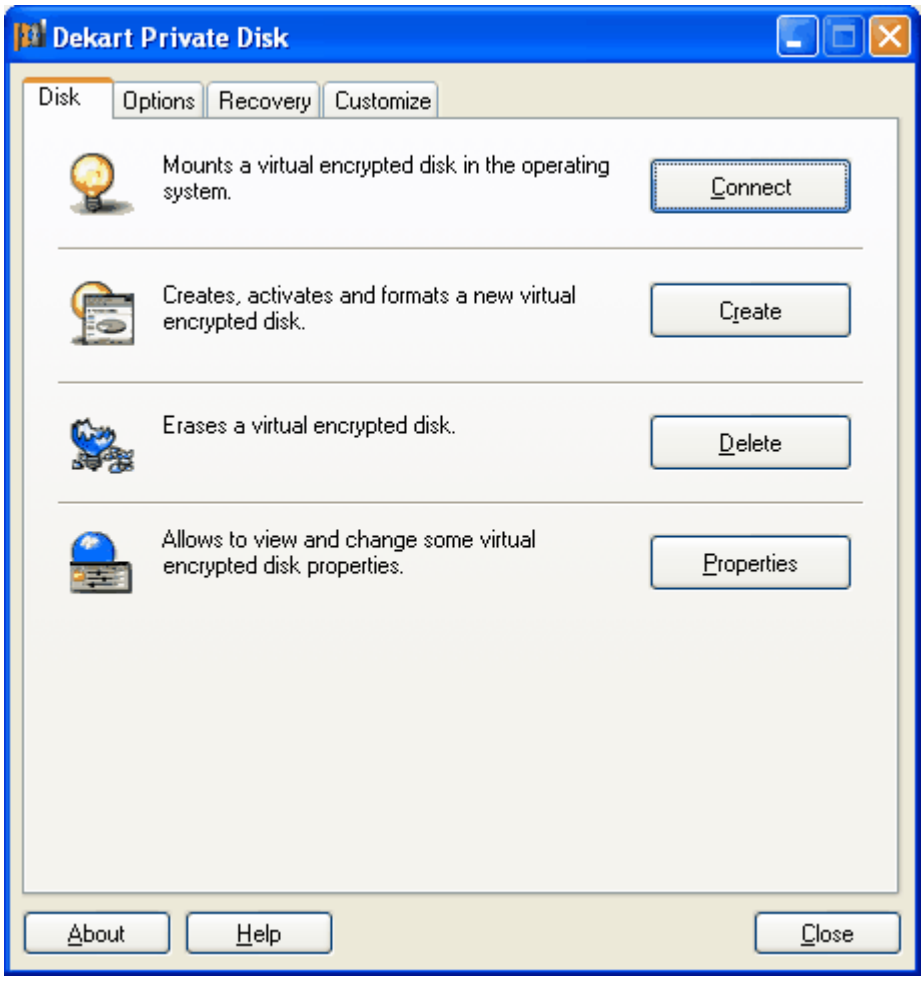

Figure 11
Dekart Private Disk control panel

You can activate Private Disk Control Panel with:
1. Double-click on Private Disk system icon (bulb).
2. Right - Click on **Dekart Private Disk** system icon (Figure 12) and choose ***Control Panel***.

Figure 12
Dekart Private Disk control panel

3. Run **Private Disk**, from Start menu (choose ***Start > Programs > Dekart > Dekart Private Disk > Private Disk)***. The control panel will appear, as shown in Figure 11.

5.4 Dekart Private Disk settings

You can configure the program to provide all required convenience.

5.4.1 Allow Dekart Private Disk to start automatically

You can allow Private Disk to run automatically on system start. Set ***Run automatically on System start*** flag to enable this (Figure 13).

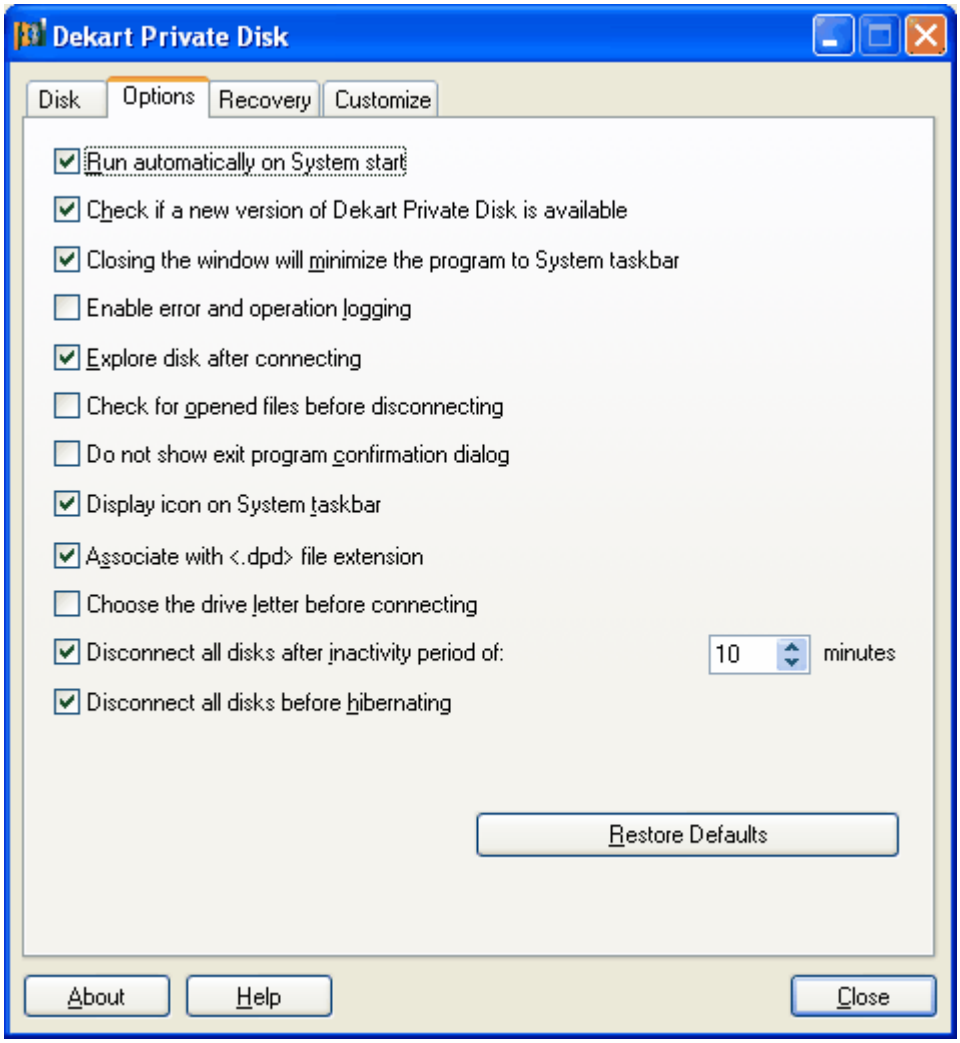

Figure 13
Options tab of the control panel

5.4.2 Enable/disable Dekart Private Disk icon

You can enable or disable **Private Disk** bulb icon. Set ***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 Control Panel to minimize when you click **Close** or **Exit** buttons. Set ***Closing the window will minimize the program to System taskbar*** flag to allow minimizing.

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

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

Note. We recommend enabling this option to avoid possible information loss triggered by the disk disconnection performed without closing running applications.

5.4.5 Allowing to automatically explore the disk after connecting

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

5.4.6 Allow to check for Dekart Private Disk updates

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

5.4.7 Disable Exit confirmation

You can enable or disable **Private Disk** to confirm **Exit**. Set ***Do not show exit program confirmation dialog*** flag to disable confirmation message.

5.4.8 Setting <.dpd> file extension for the file-image

You can associate Private Disk with file-images (*.dpd). Set ***Associate with <.dpd> file extension*** flag to allow associations. This allows mounting encrypted disk with double-clicking on file-images from Windows Explorer.

5.4.9 Enable program to ask drive letter before connecting

You can enable or disable **Private Disk** to ask user a drive letter before mounting virtual disk. Set ***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 the 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** 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 folder of the system disk, which will be further used to logging all mistakes and events triggered by the user's actions. If no checkbox is checked, the logging will not be enabled.

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

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

Once this option is enabled, Private Disk will automatically disconnect all the disks if you do not interract with the mouse/keyboard during the given time-interval. Before disconnecting, Private Disk 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's **Control Panel** allows you to enable or disable the disconnection of the virtual encrypted disk before hibernating. To do that, click ***Disconnect all disks before hibernating*** heckbox.

Once this option is enabled, Private Disk will automatically disconnect all the disks if you press **Start -> Turn off computer -> Hibernate**. Before disconnecting, Private Disk 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 menu to define the hot keys for automatic unmounting of all virtual encrypted disks and for automatic unmounting of all virtual encrypted disks on program exit. 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 system tray icon

The **Customize** tab of the Control Panel allows changing the icons of Private Disk appearing in system tray (both the "mounted" and "unmounted" state icons) and private disc file image (<.dpd> file extension). To do it, please, 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 may also use the default icons.

5.5 Creating a virtual encrypted disk

To create a virtual encrypted disk, do the following:

1. In **Dekart Private Disk** Control Panel, click ***Disk*** > ***Create***.

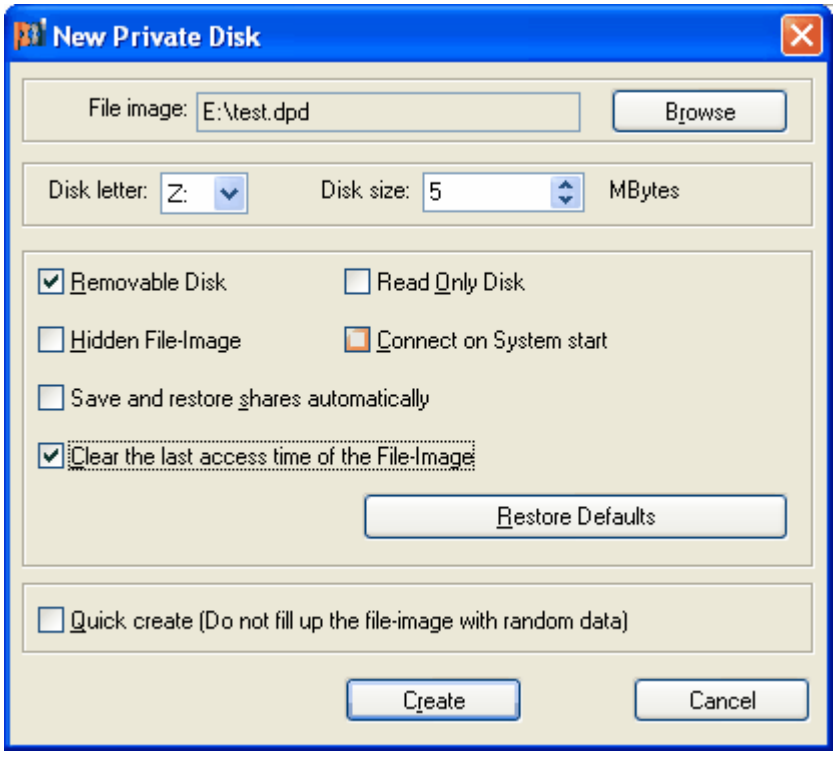

Figure 14
New disk creation window

2. You can do one of the following in the new disk creation window:
   - Click ***Cancel*** to cancel the new disk creation.
   - Click ***Browse*** to proceed with the new disk creation and indicate the full name of the file-image for the virtual secret disk in the ***File image*** field. A window will appear, as shown in Figure 15. Select an appropriate folder for the file image, indicate the name in the ***File Name*** field, and click ***Save***.

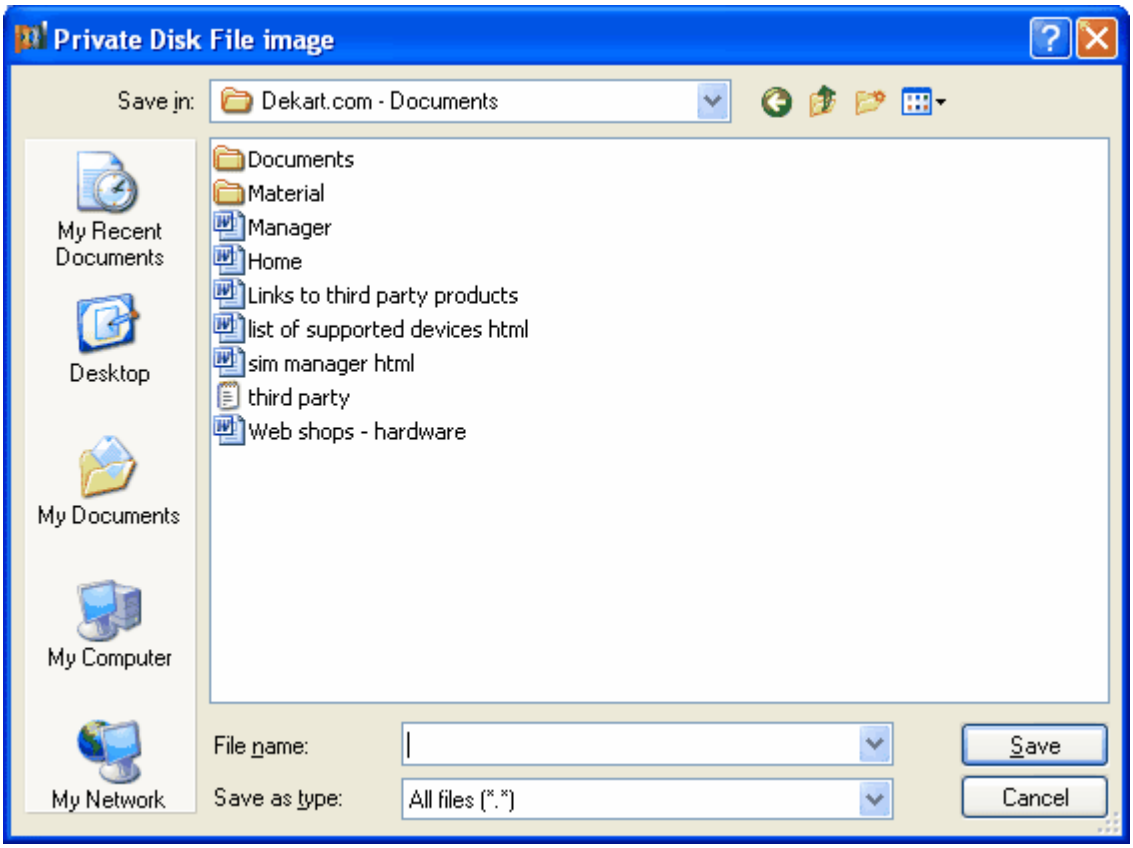

Figure 15
Creating a file-image

Dekart Private Disk can request a network resource access password if the file-image is to be stored on the network disk, as shown in Figure 16.

Figure 16

Network resource access password request

Enter the username and password into the ***User name*** and ***Password*** fields and click ***OK***. If the file with the same name already exists in the folder you specified, the confirmation that you wish to overwrite request window will appear, as shown in Figure 17..

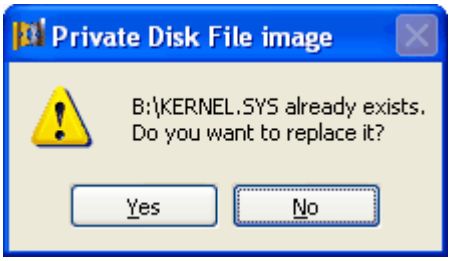

Figure 17
File overwriting confirmation request

Note: By clicking ***Yes*** and overwriting the existing file, you can lose the existing virtual encrypted disk associated with this file. **Think carefully before doing this!**
Upon clicking ***No***, the file-image creation will be terminated. In this case, you will have to indicate a different file-image name in the window shown in Figure 15 to continue disk creation.

2. Select the disk letter that will identify the disk in the system in the ***Disk letter*** field of the new disk creation window (Figure 14). Select the desired secret disk volume in megabytes in the ***Disk size*** field (depending upon the free disc space where the file-image 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 at operating system start. In this case, the "***Run automatically on System Start***" will be enabled in the Options tab of Private Disk Control panel (Figure 13).
   - ***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.
4. Click ***Create.*** You will be asked to enter the password that protects the encrypted disk. Enter the password in the ***Password*** field, then enter the same password in the ***Confirmation*** field.

Figure 18
Entering the a virtual disk access password

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** access password can consist of alphanumeric symbols, and it is **case-sensitive**. Enter the password carefully.

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

Note 1. If the entered password and password confirmation do not match, **Dekart Private Disk** will convey this to the user and ask to enter the password again. Please enter the matching values in the ***Password*** and ***Confirm Password*** fields.

Note 2. The password's strength is analyzed from the cryptographic point of view, and the result of the analysis is shown in the ***Password quality*** bar. The estimated quality is represented by a numerical value (between 0 and 100%) and by changing the color of the bar (green corresponds to a strong password, while red corresponds to a weak one).

5. You can speed up the disk creation process by using the ***Quick create*** option. In this case, the file image will not be filled with random data ("junk").
6. Click ***OK***. File-image creation process will start. Its progress will be indicated in a special window, as shown in Figure 19.

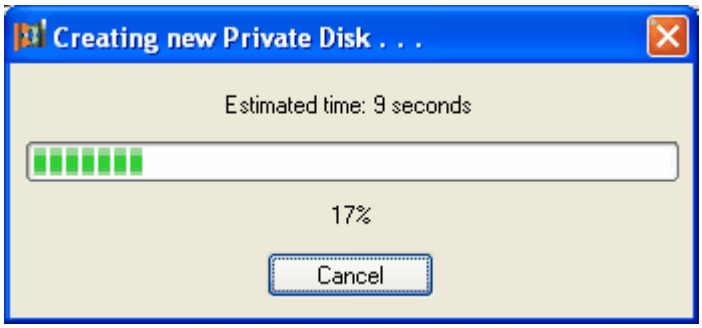

Figure 19

File-image creation process

To stop this process, press ***Cancel***. In this case, the window shown in Figure 20 will appear requesting either to confirm (***Yes***) or to cancel (***No***) creation process termination.

Figure 20
File-image creation process termination

You can do one of the following:

- Click ***No*** to continue creating the file-image.
- Click ***Yes*** to terminate this process.

When the file-image is created, the request will follow to format it, as shown in Figure 21.

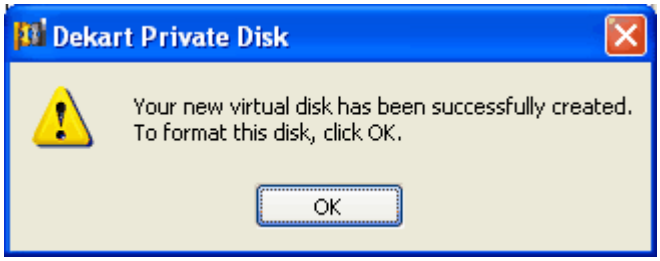

Figure 21
Created secret disk formatting request

7. To start formatting click ***OK.*** A format dialog box will appear, as shown in Figure 22.

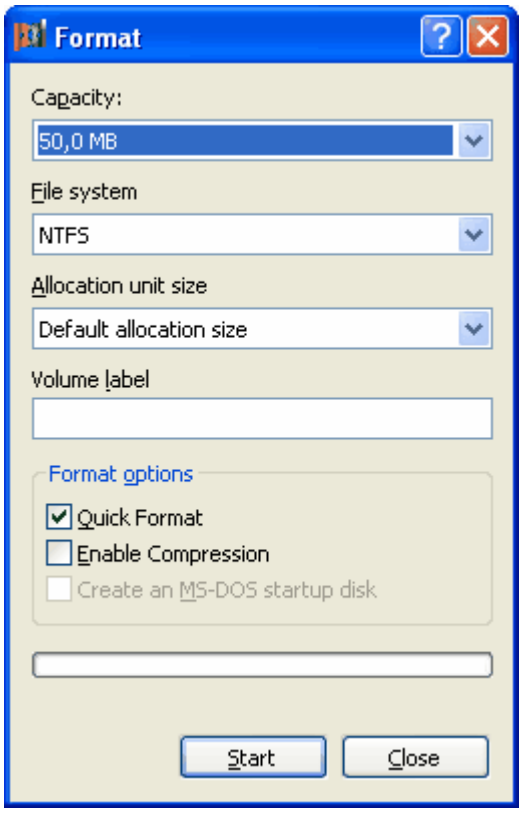

Figure 22
Format dialog box

8. Choose the desired format parameters (or leave them by default) and click ***Start.*** A Format warning message will appear on the screen notifying you that all virtual disk data will be deleted. .

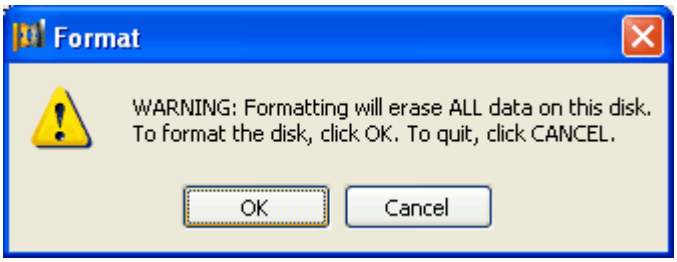

Figure 23
Format warning message

9. Click ***OK*** and wait until the disk is formatted. When it is formatted, close the ***Format*** dialog box to finish the disk creation process. Only at this point, the virtual disk creation is completed. It will be automatically enabled and ready to work. Its icon will appear in the ***Windows Explorer*** window, as shown in Figure 24.

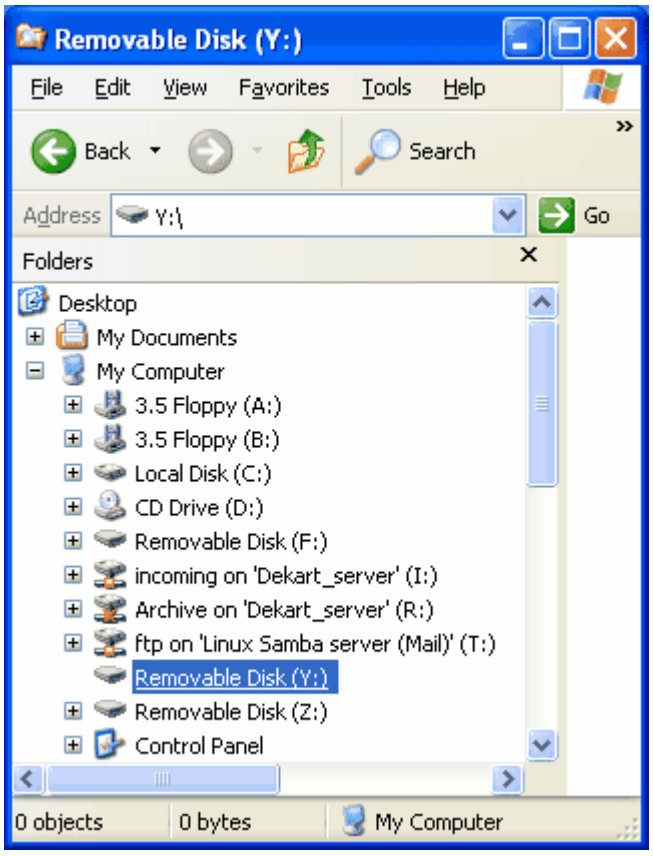

Figure 24
Information about virtual disk appearance

Note: If you click ***Cancel*** and cancel disk formatting, the virtual disk creation process will be interrupted and cancelled.

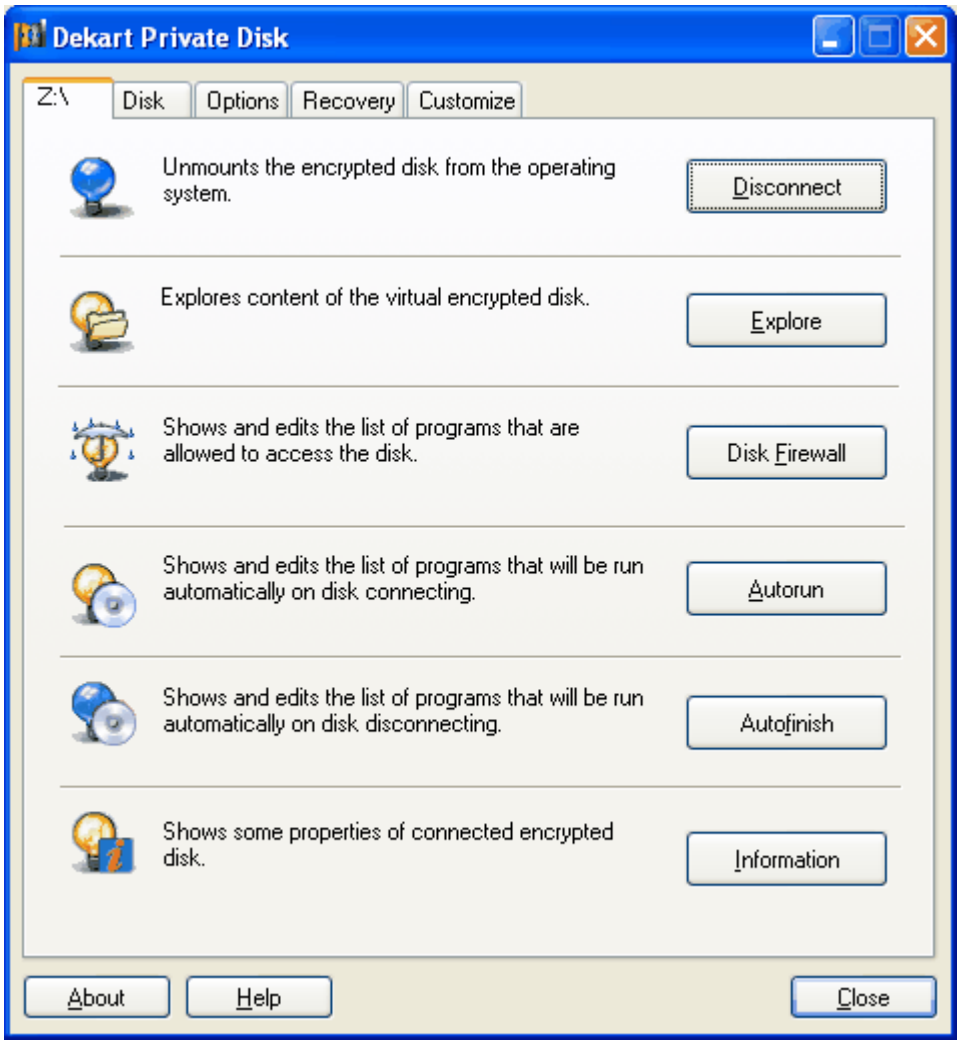

Figure 25
Created disk ready to work

5.6 Recommendations for ensuring Dekart Private Disk security

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

Tip#1. The length of password to access your virtual encrypted disk should have enough length. The optimal length – 8 random symbols, including upper-case and lower-case letters, digits, punctuation marks etc. Neither write the password down, nor leave this paper behind your computer, try 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. Create backup copies of the encryption keys. In case you forget the password for

accessing the encrypted disk, the backup copy of the encryption key will allow you to decrypt the data (see *Creating backup copy of the encryption key* and *Restoring the encryption key of the virtual encrypted disk from the backup copy*).

Tip#4. Leaving your workplace even for a short period of time take care to unmount all mounted virtual encrypted disks (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 that encrypted data cannot be recovered, erase the unused encrypted images using Private Disk's special feature (see Deleting virtual encrypted disk section).

5.7 Changing virtual encrypted disk properties

To change the logical name (letter) identifying the secret disk in the system, disks parameters or access password please open **Dekart Private Disk** Control Panel and click ***Disk*** > ***Properties***. Indicate the name of the file image of the encrypted disk in the appearing dialog window.

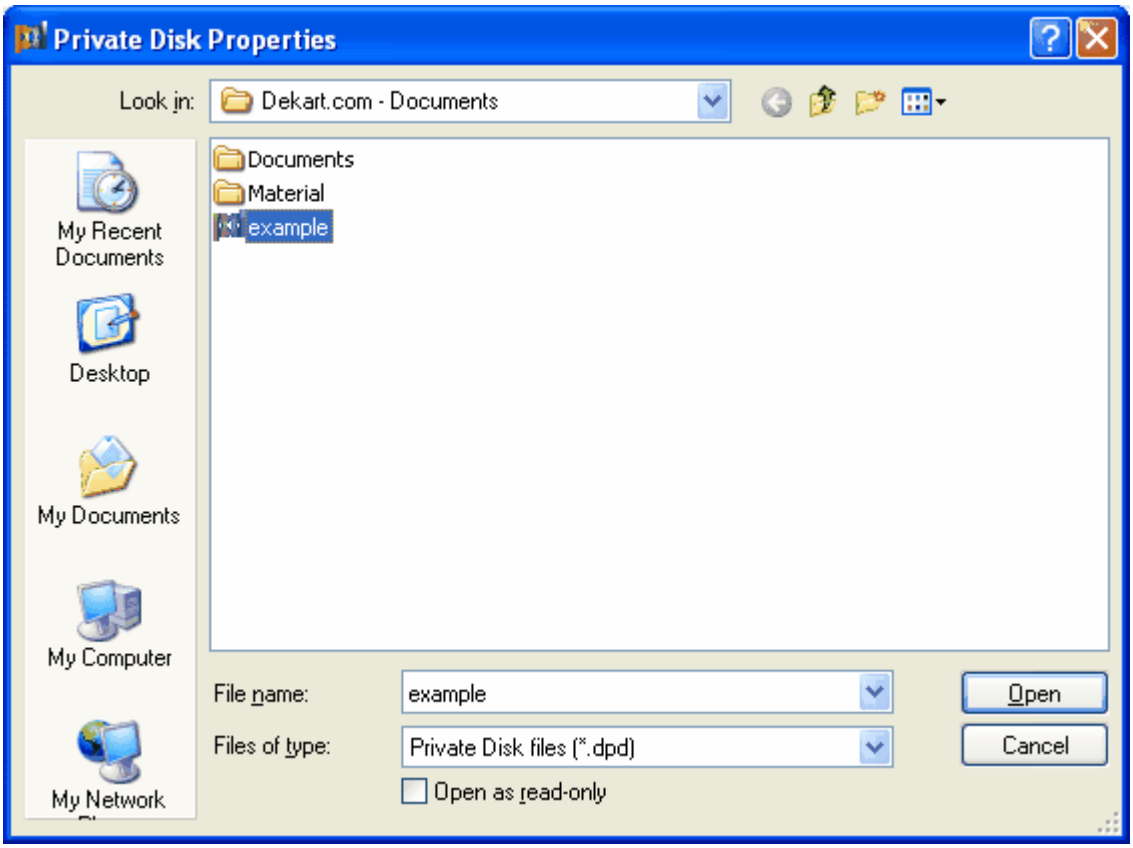

Figure 26
Choosing file-image

You will be prompted to enter your password.

Figure 27
Entering access password for changing disk properties

After successful password verification the ***Private Disk Properties*** window will appear, as shown in Figure 28.

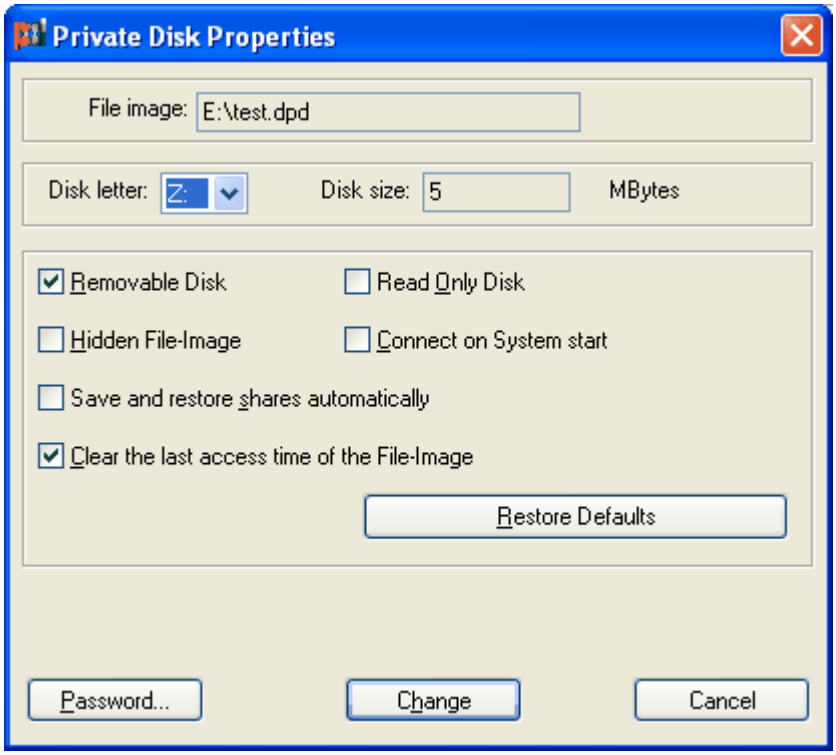

Figure 28
Disk properties window

You can do one of the following:

- Click ***Cancel*** to stop changing the disk properties.
- Enter new value in ***Disk letter*** field (See the *Creating a virtual encrypted disk* section in this chapter) a.
- Set ***Hidden File-Image*** check box if you want to hide disk's file-image.
- Set ***Read Only Disk*** check box if you want to connect the virtual disk in read-only mode.
- Set ***Removable Disk*** check box to make virtual disk "Removable" or unset the check

box make virtual encrypted disk "Fixed" (this could be needed if you want to move your Outlook Express mail base to virtual encrypted disk or want to enable Recycle Bin on this disk).

- Check the ***Connect at Ssystem Start*** checkbox for the secret disk's automatic connection on operating system start.
- Set ***Save and restore shares automatically*** checkbox to save and restore network access rights to the contents of the encrypted disk.
- Check the ***Clear the last acess time of the File-Image*** checkbox to reset the last access time of the encrypted image to the time of its creation when the disk is disconnected.
- Click ***Password*** if you want to change access password to encrypted disk. In the appeared dialog enter new access password and confirm it.

To apply the changes click ***Change***.

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

5.8 Mounting/unmounting virtual encrypted disk

5.8.1 Mounting/unmounting virtual encrypted disks

To start working with the virtual secret disk, it must be *connected (mounted)* first, i.e. it must become recognizable for the computer's Windows system. Mounting the virtual disk (permitting to access it) can be carried out in following way. In the Control Panel of the **Dekart Private Disk** click ***Disk*** > ***Connect.*** In appeared **Connect Private Disk** dialog please select the file-image of the virtual encrypted disk and click **Open**. The software will require to enter access password, as shown in Figure 29.

Figure 29
Entering access password for virtual encrypted disk

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

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

To finish working with the virtual secret disk (*disconnection*), click ***Disk*** > ***Disconnect***.

There is a possibility to work with several virtual encrypted disks at one time. For this click **Disk**>**Connect** and select another file-image.

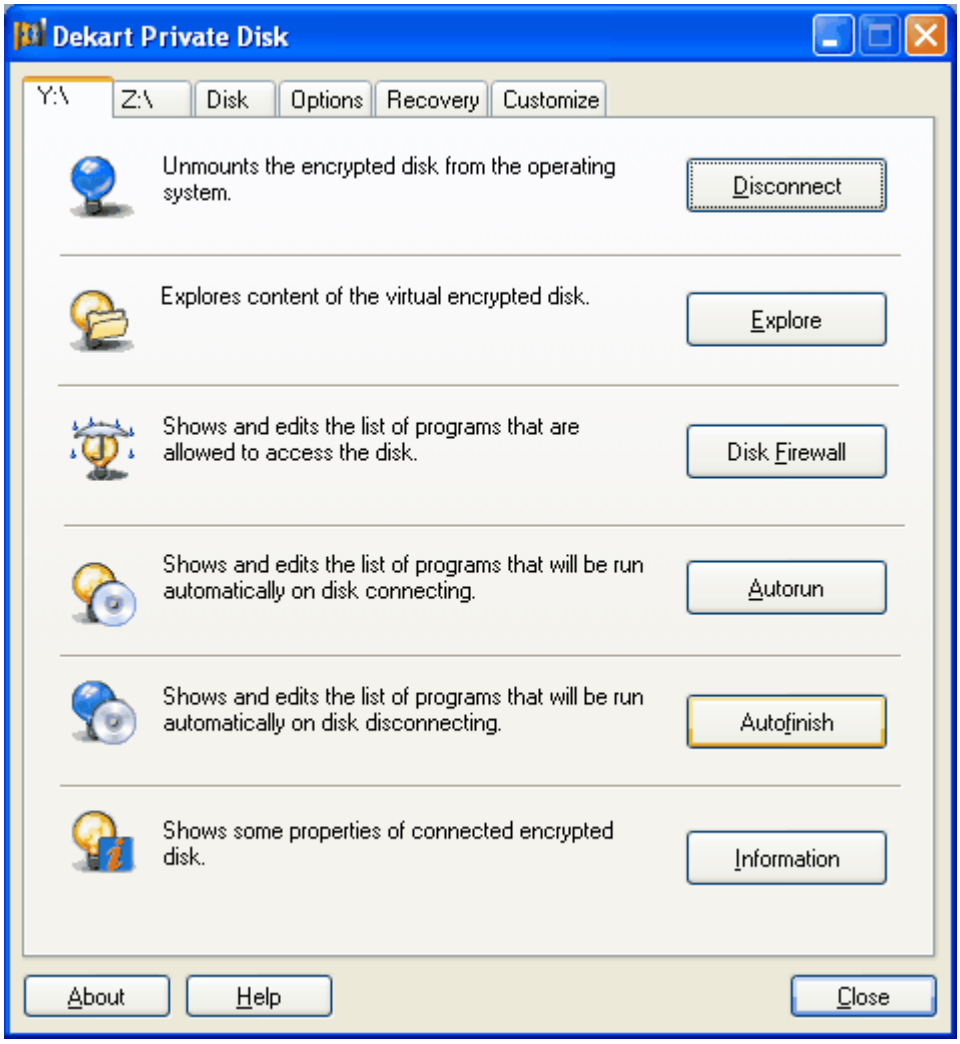

Figure 30
Working with several virtual encrypted disks at one time.

Note: If on connecting new virtual encrypted disk its disk symbol is occupied the software will display dialog for choosing another letter (see Figure 31) Select another disk symbol and click ***OK***.

Figure 31
Choosing another letter for virtual encrypted disk

To stop working with the virtual encrypted disk click ***Disk > Disconnect***.

You can also connect/disconnect virtual encrypted disk using a popup menu. To access this menu, please right click the Private Disk systray icon. Select the desired action from the menu items list (Figure 32). In case there are several connected disk, please select the desired disk letter in the ***Disconnect Disk*** menu to disconnect this disk.

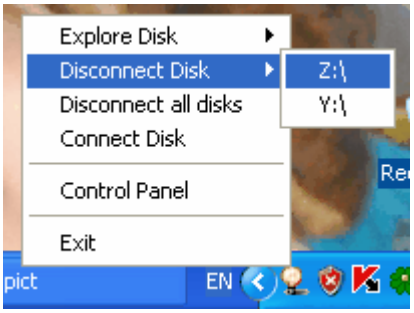

Figure 32
Mounting/unmounting virtual disk using popup menu

To disconnect all the currently connected disk at once, click ***Disconnect all disks.***

The third 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 stand by* 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 losses, close all applications using data on the disk before disconnecting the disk.

5.8.2 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's Control panel or Private Disk's shortcut or Private Disk's icon. When the file is dropped, the disk connection dialog will be activated.

5.8.3 Virtual encrypted disk status

Dekart Private Disk 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 connected* (bulb is on) or *disk disconnected* (bulb is off), as shown in Figure 33.

Figure 33
Virtual secret disk status

To change the status from "Disconnected" to "Connected", connect the disk as described in the section *Mounting/unmounting virtual encrypted disk*).
To change the status from "Connected" to "Disconnected", disconnect the disk as described in the section *Mounting/unmounting virtual encrypted disk*).
Note: Do not disconnect the secret disk if any application is currently working with it. First, close the application, next, disconnect the disk.

5.9 Exploring 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 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.

5.10 Managing the programs to be automatically run on disk mounting or unmounting

Private Disk allows to define programs to be automatically run on the disk mounting or disk unmounting event.

Autorun.
To edit the list of the programs to be automatically run from the encrypted disk, 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 the 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 programs' list click **OK**.

Autofinish.
To edit the list of the programs to be automatically run from the encrypted disk on the disk unmounting event, 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 mounted and click **OK**. They will then appear in the **List of programs to autofinish** (***Autofinish programs*** window) on disk unmounting.

To delete the 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 programs' list click **OK**.

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

5.11 Managing the list of applications which are allowed to access the encrypted disk

Private Disk 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 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.

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

Private Disk 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.

5.13 Viewing the parameters of the virtual disk

To view the parameters of the currently connected encrypted disk, press the **Information** button (**Control Panel** > ***Disk_name:***\). The pop-up window will contain details about the specified disk.

5.14 Starting Dekart Private Disk from command line

Dekart Private Disk could be started from the command line prompt:

..\PrvDisk.exe [\options][:parameter]

You can specify the following options when working with Dekart Private Disk from command line:

/minimize	start the program minimized to system tray;
/path:YourFileImage	activate virtual encrypted disk from this file-mage (*YourFileImage*);
/password:YourPassword	connect virtual encrypted disk using the password *YourPassword*;
/symbol:DiskSymbol	connect encrypted disk under the specified disk symbol (disk letter) *DiskSymbol*;
/dismount	disconnect all virtual encrypted disks;
/dismount:DiskSymbol	disconnect the specified encrypted disk using it's disk symbol *DiskSymbol*;
/unload	disconnect all encrypted disks and close the program without confirmation;
/nosystray	hide system tray icon at the right side of the task bar;
/nohotkeys	disable Dekart Private Disk's hotkeys;
/noexitdialog	do not display exit confirmation dialog at program closing**;**
/logfile	create error log-files in the system disk root (e.g. in the "C:\"): dk_pd.log and dk_pdapi.log;
/properties:YourFileImage	change properties of a virtual encrypted disk from this file-image;
/ROD	set Read Only Disk property to a virtual encrypted disk;
/RD	set Removable Disk property to a virtual encrypted disk;
/HFI	set Hidden File-Image property to a virtual encrypted disk;
/CSS	set Connect on System start property to a virtual encrypted disk;
/passwordnew:YourNewPassword	change a virtual encrypted disk password to the given password;
/create:YourFileImage	create a virtual encrypted disk in this file-image;
/size:DiskSize	create a virtual encrypted disk with the given size;
/FS:FAT|FAT32|NTFS	create a virtual encrypted disk with the given File System (*FAT* or *FAT32* or *NTFS);*
/erase:YourFileImage	erase a virtual encrypted disk with the given file-image *YourFileImage;*
/script:YourScriptFile	execute in turn all commands written in the given script file *YourScriptFile.*

Command line samples:

1. Create disk

PrvDisk.exe /create:C:\disk.dpd /passwordnew:12345 /RD /HFI /symbol:Z /size:100 /FS:FAT /minimize

2. Connect disk

PrvDisk.exe /path:C:\disk.dpd /password:12345 /minimize

3. Disconnect disk

PrvDisk.exe /dismount:Z

4. Change disk properties

PrvDisk.exe /properties:C:\disk.dpd /password:12345 /passwordnew:67890 /RD /symbol:Y /minimize

5. Erase disk

PrvDisk.exe /erase:C:\disk.dpd /password:67890 /minimize

6. Execute script

PrvDisk.exe /script:C:\script.txt

where file script.txt contains::

```
/create:C:\disk.dpd /passwordnew:12345 /RD /HFI /symbol:Z /size:100
/FS:FAT /minimize
/dismount:Z

/path:C:\disk.dpd /password:12345 /minimize
/dismount:Z

/properties:C:\disk.dpd /password:12345 /passwordnew:67890 /RD /symbol:Y
/minimize
/path:C:\disk.dpd /password:67890 /minimize
/dismount:Y
/erase:C:\disk.dpd /password:67890 /minimize
```

Note: In case you use long folder and file names, please use the quotation marks "" to write these parameters, e.g. **/path:"my secret data.dpd".**

5.15 Encrypted disk sharing

Dekart Private Disk supports the shared use of the virtual secret disk data in a network. To allow other users to access the secret disk data, it must be connected to the computer where the file-image is located (See the section *Mounting/unmounting virtual encrypted disk* above). Next, the shared use must be setup with the help of the standard Windows OS utilities (similarly to the shared use of a conventional drive).

Note: When the disk is deactivated, disk access will be immediately disabled for all users and the currently processed data can be lost.

To enable disk sharing, do the following (this example is for Windows XP):

- Double click ***My Computer***.
- In the appearing ***My Computer*** window, select the virtual secret disk and right-click it. Select ***Properties***. Click the ***Sharing*** button shown in Figure 34. Setup values in the ***Shared As***, ***Access Type*** fields and click ***Apply***.

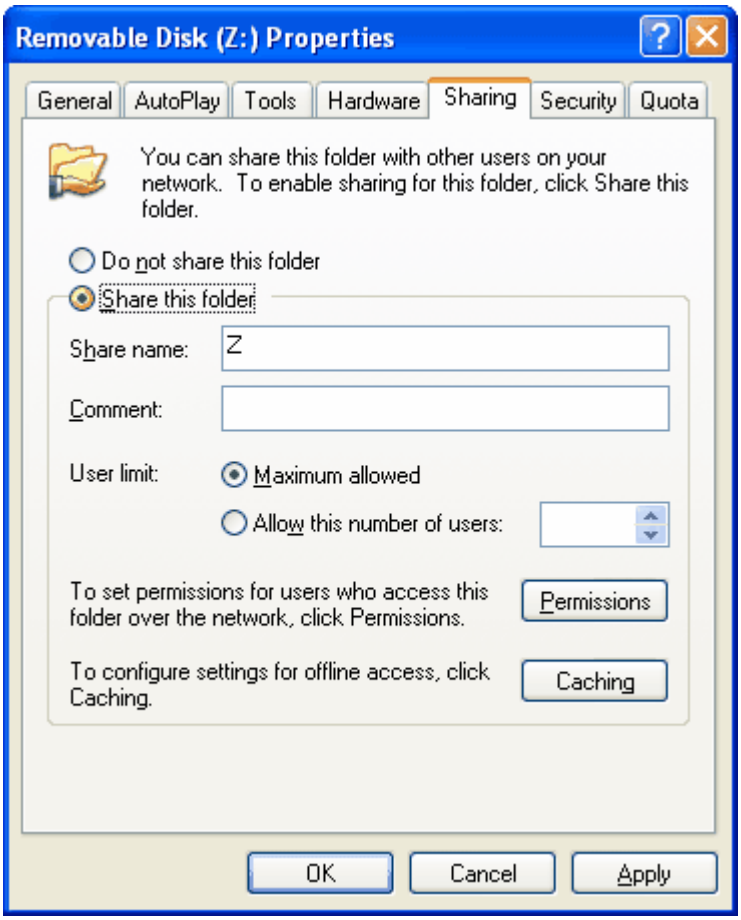

Figure 33
Setting up shared virtual disk access

5.16 Backing up virtual encrypted disk data

Dekart Private Disk allows backing up the virtual secret disk data. Backup copy aids in full disk recovery if it has been damaged or accidentally deleted.
A backup copy is stored compressed and encrypted. Encryption is implemented by means of an encryption password and a special alternative access password. Alternative access password allows restoring the data.
To create a backup copy, do the following:

1. Click ***Recovery*** on the **Dekart Private Disk** Control Panel.
2. Press ***Backup*** button.
3. Indicate the location and the name of the image of the virtual encrypted disk.
4. When asked, enter the password of the encrypted disk.
5. The ***Private Disk backup file*** window will appear, as shown in Figure 35.

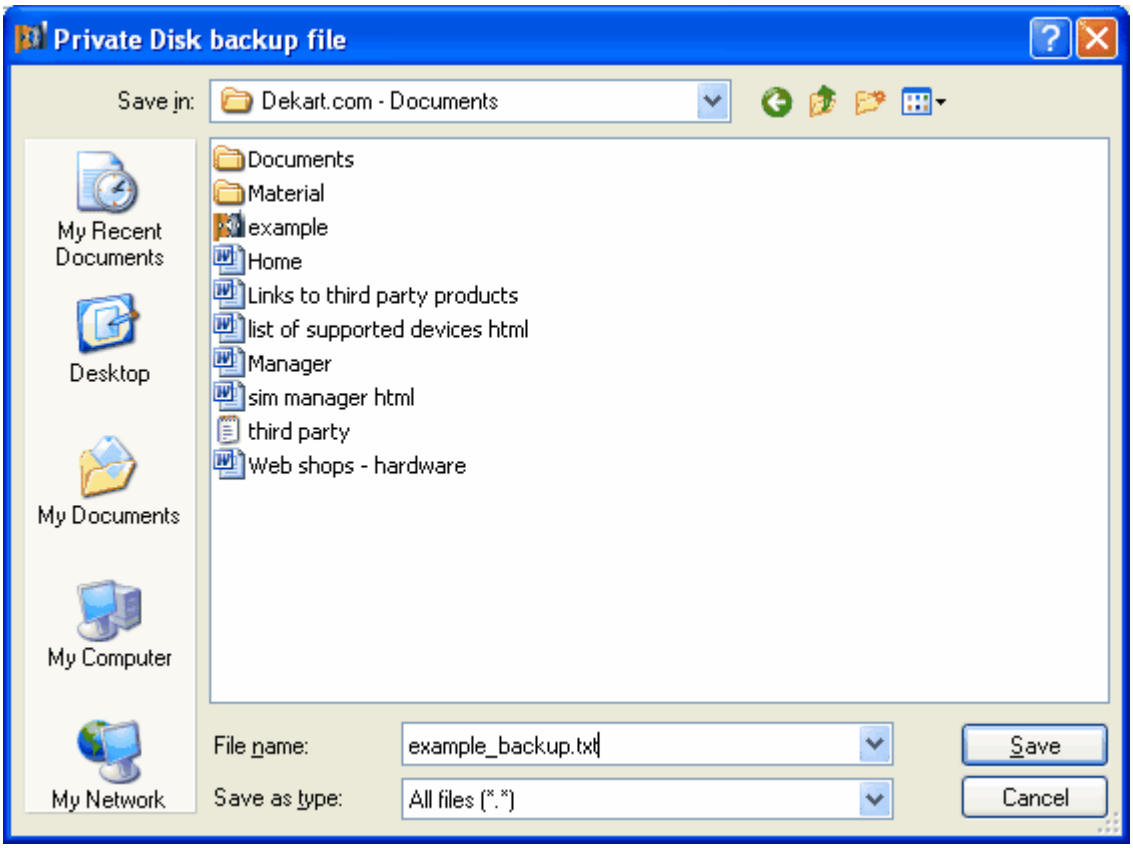

Figure 35
Backing up virtual disk data

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

5.17 Restoring virtual encrypted disk data

Dekart Private Disk allows to restore the virtual secret disk data using the previously created backup copy (see the section *Backing up virtual encrypted disk data* above).
To restore data using a backup copy, do the following:

1. Connect the secret disk as described above in the section *Mounting/unmounting virtual encrypted disk* or create a new disk, as described in the section *Creating a virtual encrypted disk*. This disk will contain the data restored from a backup copy.

Note: Backup copy data 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 volume of the restored data does not exceed the capacity of the virtual disk of destination. This feature allows to restore data even the file-image of the original secret disk have been lost. Moreover, the backup copy data can ***only*** be restored to a virtual secret disk. 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!**

2. Click ***Disk > Restore*** in the **Dekart Private Disk** Control Panel.

The ***Private Disk restore file*** window will appear, as shown in Figure 36.

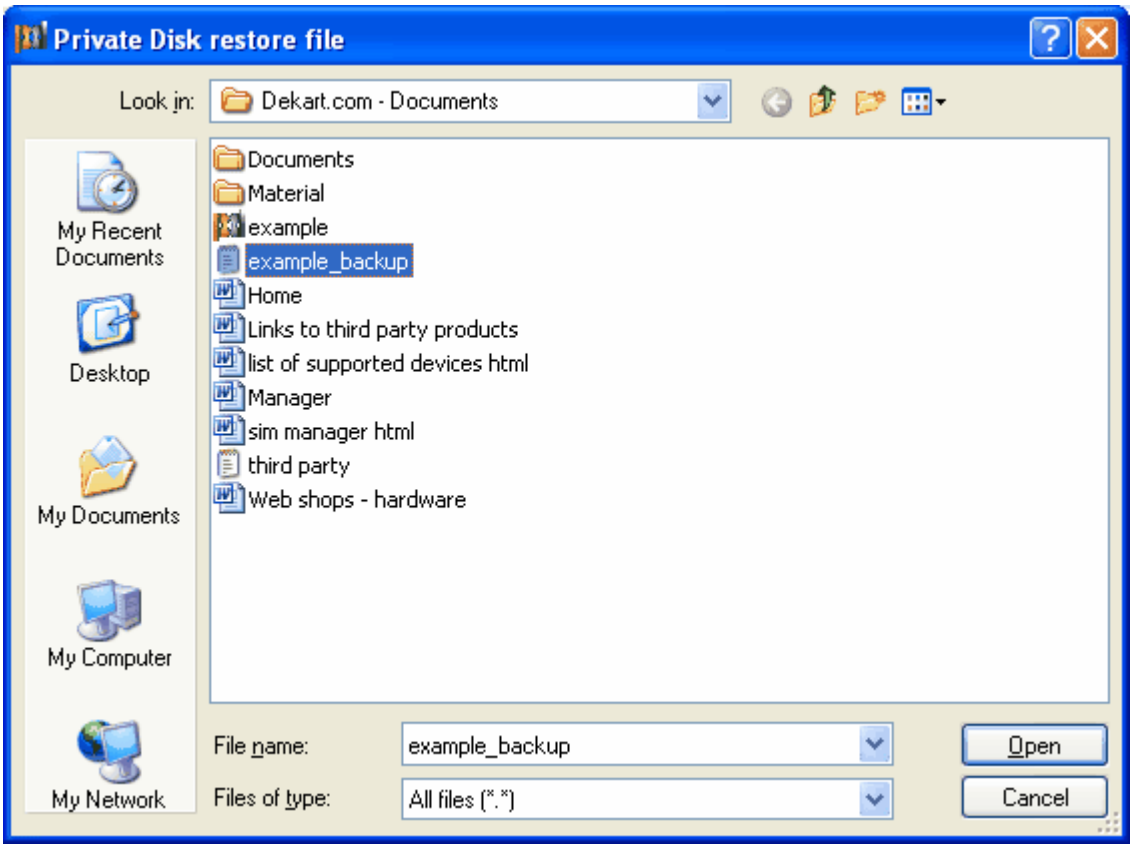

Figure 36
Virtual disk data recovery using a backup copy

3. Select a folder storing the disk backup copy, enter the backup copy file name in the ***File Name*** field, click ***Open***.
   If the activated virtual disk doesn't correspond to 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 data recovery, **Dekart Private Disk** warns that all data will be deleted from the current virtual disk, as shown in

Figure 37.

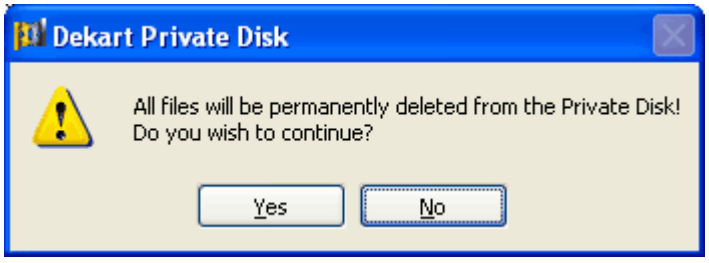

Figure 37
Virtual disk data deletion warning

4. On clicking ***Yes***, all of the current disk data are deleted, and the virtual secret disk data recovery process starts.

5.18 Deleting virtual encrypted disk

Deleting virtual encrypted disk means permanently erasing all information stored on it and eliminating its recovery.
To delete the virtual encrypted disk, do the following:

1. Unmount encrypted disk (if it is mounted) as described in *Mounting/unmouting virtual encrypted disk* section.
2. In **Dekart Private Disk** 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. After file name entering the window with the request to enter the password will appear.

Then the window with the information about the disk to be deleted will appear.

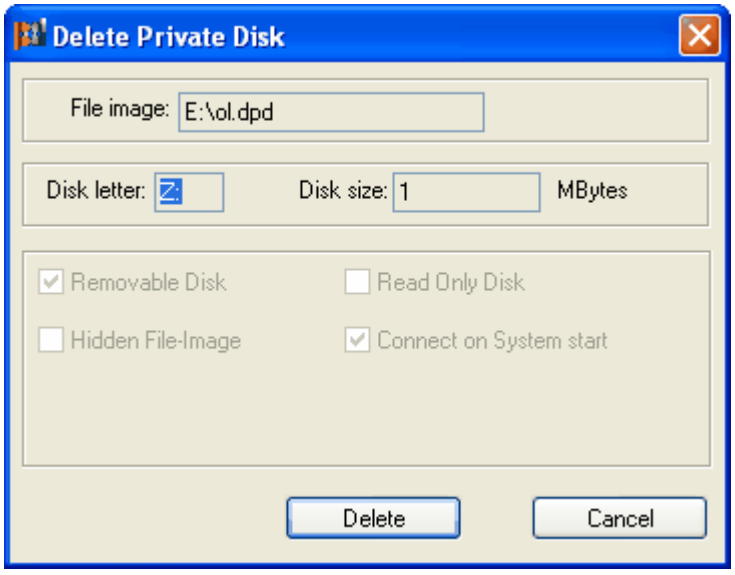

Figure 38
Disk deletion window

5. To delete the disk, click ***Delete***. The deletion confirmation request will appear.
   Note. On clicking ***Cancel***, the disk deletion process is terminated.

Figure 39
Disk deletion confirmation

6. Click ***Yes*** to proceed with the virtual encrypted disk deletion, click ***No***, to cancel it.

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

5.19 Creating backup copy of the encryption key

Dekart Private Disk allows creating backup copy of the encryption key of the virtual encrypted disk. The backup copy allows restoring the disk in the cases of password loss or if the file-image has been accidentally corrupted during the operating system failure.
The backup copy is stored in encrypted form. To encrypt the backup copy a special password of alternative access, independent from disk access password, is used. This password is used for data recovery.
To create backup copy, do the following:
1. In **Dekart Private Disk** Control Panel click **Recovery**.

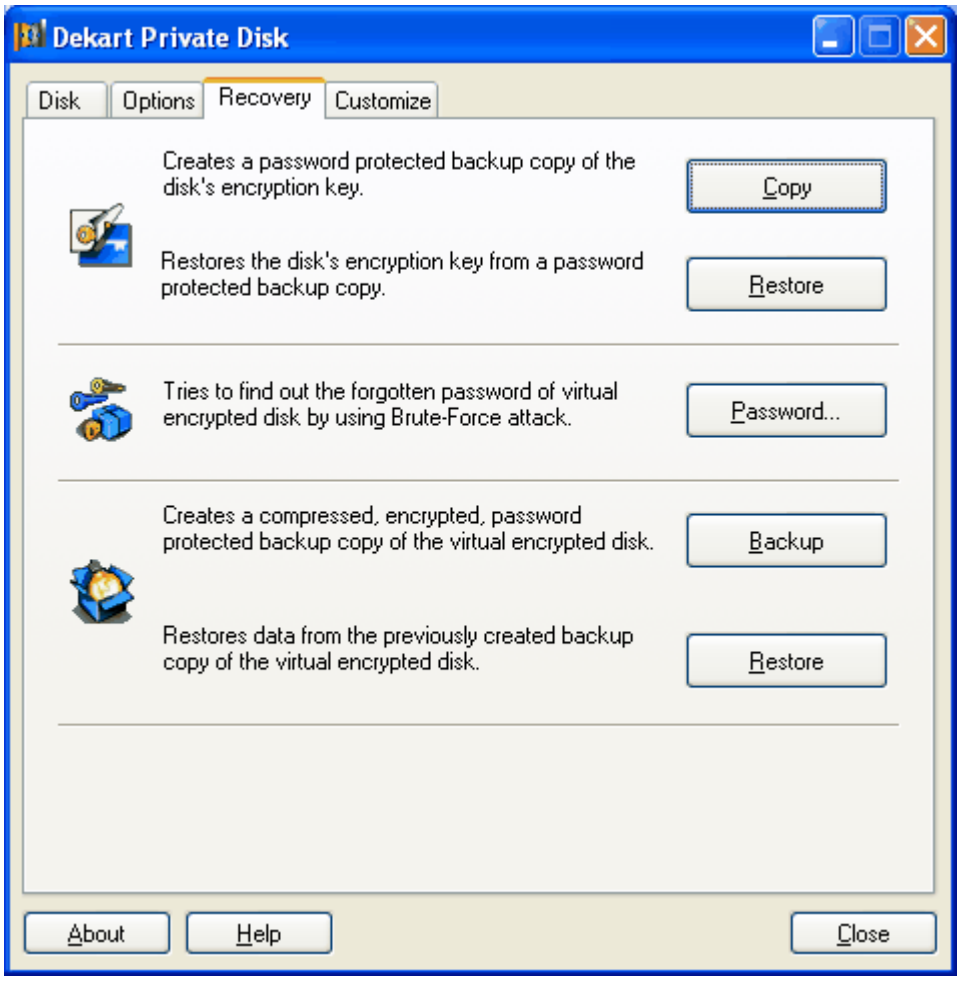

Figure 40
Create and restore encryption key window

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, as shown in Figure 41.

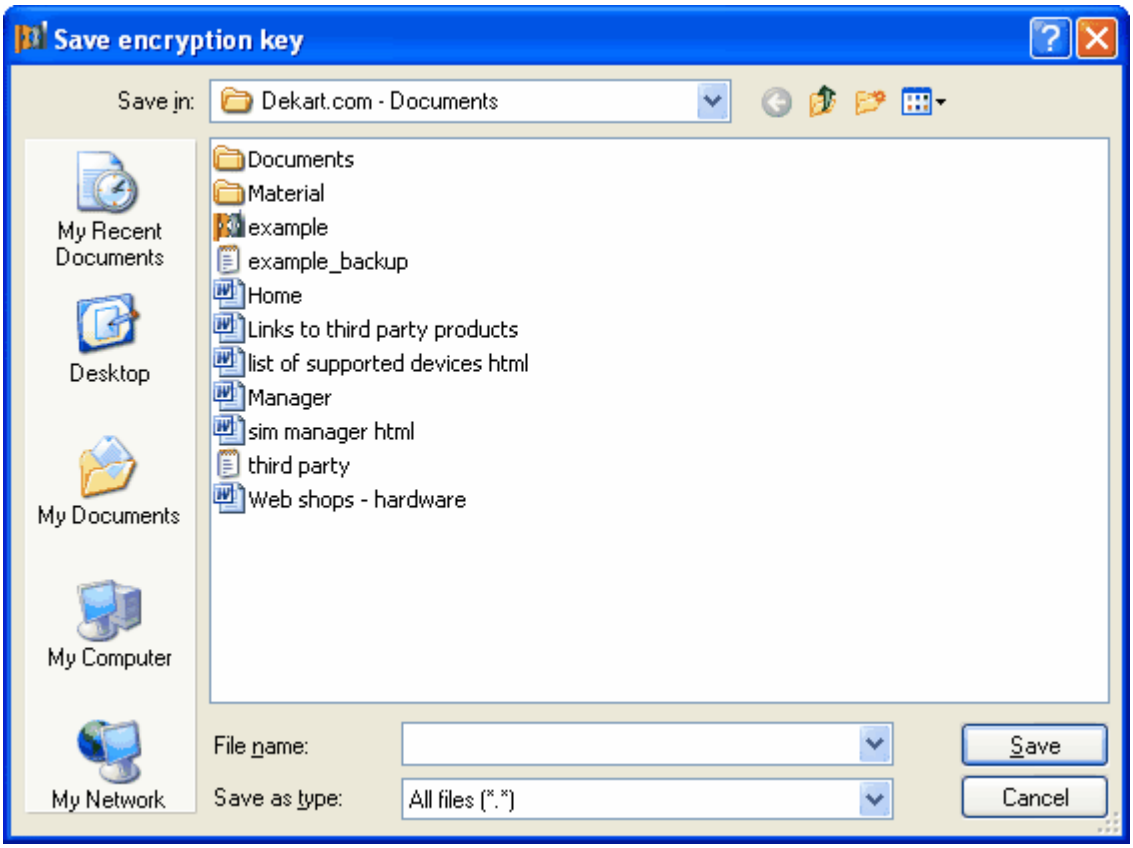

Figure 41
Creating backup copy of the encryption key

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 require 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 to ensure accuracy. The entered password must be 5 or more symbols long. Otherwise, an insufficient password length message will appear.

Note. The **Dekart Private Disk** 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 the backup copy

Dekart Private Disk allows restoring 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 the backup copy, do the following:
1. In Control Panel click **Recovery**.
2. The ***Open encryption key*** window will appear, as shown in Figure 42.

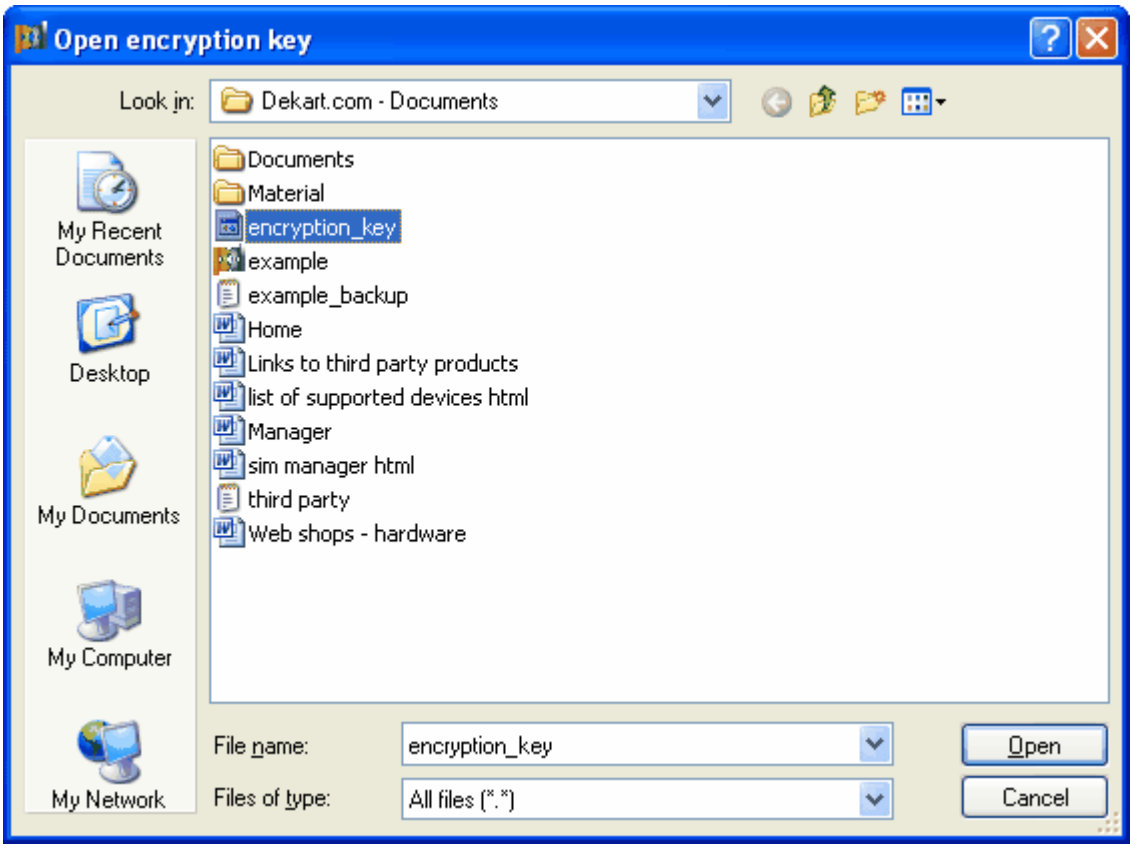

Figure 42
Restoring the encryption key from the backup copy

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 request 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 request to select the folder and the filename 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 to ensure accuracy. The entered password must be 5 or more symbols long. Otherwise, an insufficient password length message will appear.

5.21 Forgotten password recovery

Dekart Private Disk allows to recover the password to the encrypted disk you have partially forgotten by using a Brute-force attack method.

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

1. Go to 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.

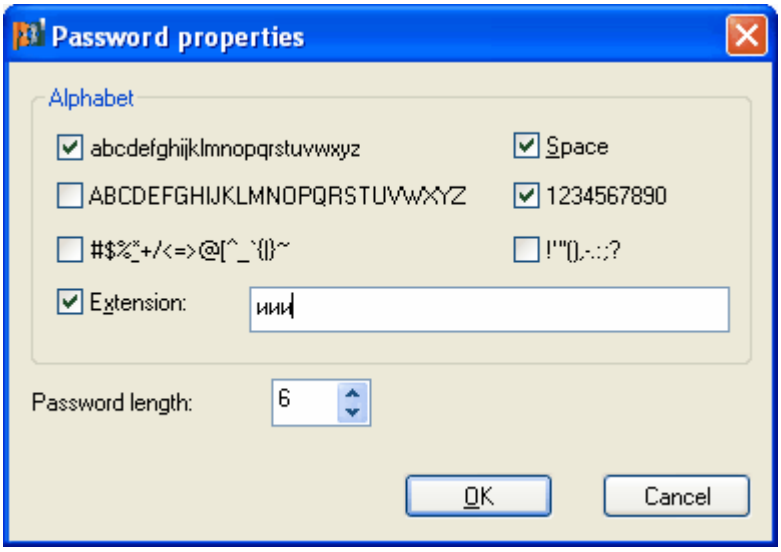

Figure 43
Password properties window

5. Specify the alphabet (types of symbols), which you suppose to have been used in your password, the password length and click **OK**. Please, specify the symbols not mentioned above in the ***Extension*** field (e.g. cyrillic symbols)
6. The prompt window asking you to confirm the password properties choice will appear. 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.

5.22 Closing Dekart Private Disk

To finish the work with **Dekart Private Disk** do one of the following:

1. Right-click the **Dekart Private Disk** systray icon to activate system menu. Select ***Exit***. **Note 1.** If Private Disk was installed to a flash drive, use the ***Exit and safely remove hardware*** option. **Note 2.** If you wish to use the flash disk after quitting Private Disk, 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.

3. The confirmation screen will appear, as shown in Figure 44.

Figure 44
Close program confirmation screen

Click ***Yes*** to close **Dekart Private Disk**, click ***No*** to continue work.

Note. If the virtual encrypted disk is active, the disk is deactivated (dismounted) upon work completion.

5.23 Registering Dekart Private Disk

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

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

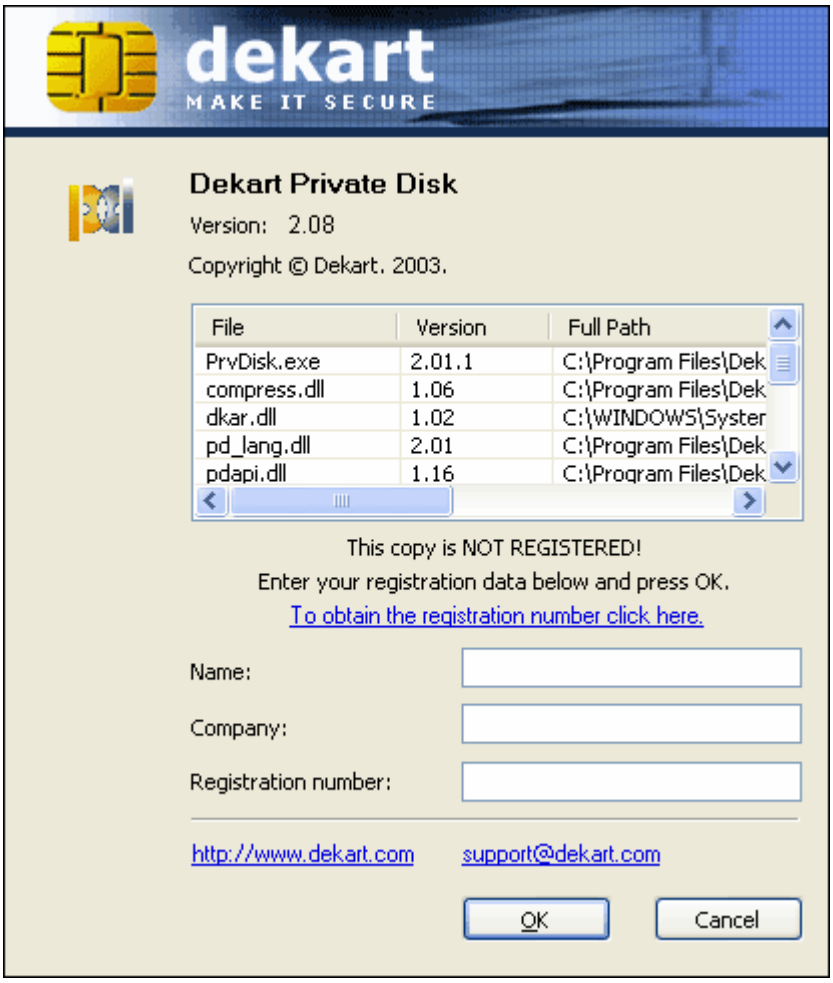

Figure 45
About Dekart Private Disk window with the registration form

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

5.24 Dekart Private Disk technical support

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

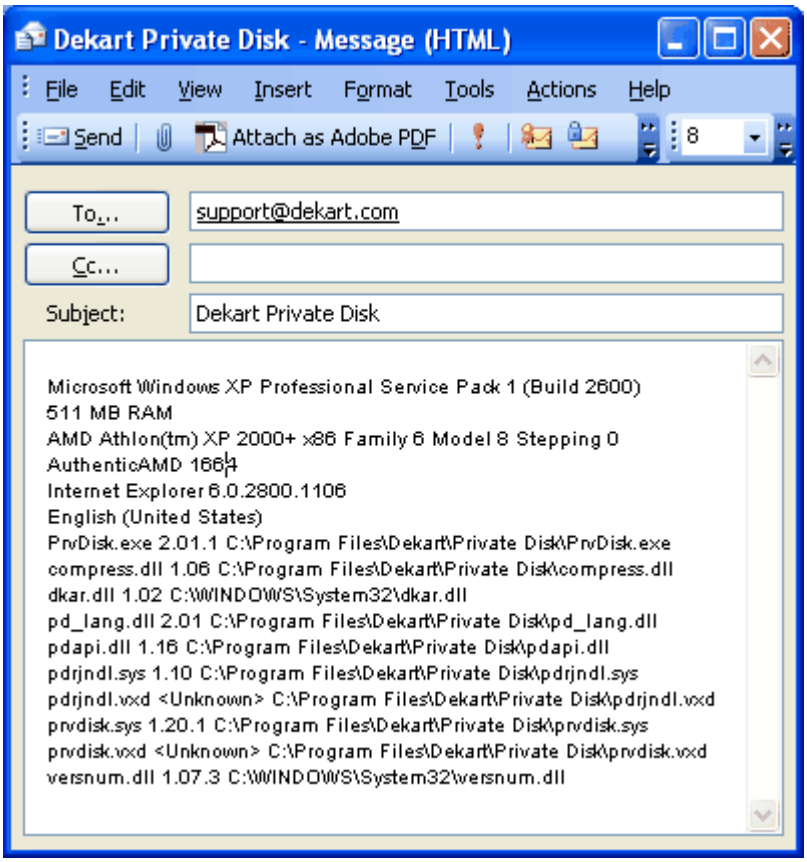

Figure 46
Email composer window with all information about the software versions

6 Troubleshooting

This chapter contains:

- **Diagnostic Messages List**. These messages result from wrong user actions or **Dekart Private Disk** hardware or software errors during the software operation. For convenience, messages are given alphabetically in the *Message* column of the *Diagnostic Messages* table.
- **Message Explanation List**. These descriptions are given in the *Explanation* column of the *Diagnostic Messages* table.
- **On-Message Actions List**. The actions to be carried out on receiving a certain message are given in the *Action* column of the *Diagnostic Messages* table.

6.1 Possible problems

If any contingencies occur during **Dekart Private Disk** installation and hardware connection and the user does not know how to handle the situation, he is welcome to contact Dekart support team at support@dekart.com provided that he presents his Name and Registration number

6.2 Diagnostic messages

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

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

The diagnostic messages table is listed below.

Diagnostic messages table.

##	Message	Explanation	Action
01	Unable to connect the Private Disk!	The symbol for the disk being installed has been allocated to another drive or has an illegal value.	In disk properties, change the symbol identifying the disk in the operating system (see the section *Dekart Private Disk options tab* section in chapter 4).
		Operating system error	Exit all applications and restart the computer.
07	This Operating System is not supported!	**Dekart Private Disk** is not supported by the current operating system.	Contact **Dekart Private Disk** technical support service.
08	Unable to activate help!	**Help** system is not available.	This can occur due to the following reasons: the help file of **Dekart Private Disk**, **PrvDisk.hlp** is missing or **WinHelp** system is not installed in Windows. Refer to **Dekart Private Disk** technical support service.
09	Unable to backup the Private Disk!	Virtual disk read error.	Use special utilities to check the virtual secret disk. There may be file system errors – try to fix them.
		Backup file write error.	Use the special utilities to check the hard disk to which you attempted to write the backup copy. It may have bad sectors or disk file systems errors, or there is not enough disk space. Try to solve these problems or find another disk storage unit.
11	Unable to create the Private Disk!	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, use special utilities (for example, **Norton Disk Doctor**) to check whether your hard disk storing the file-image has bad sectors or file system errors. Try to fix them or select another disk storage unit. The symbol indicating the disk being created can have an illegal value. To solve this problem, correct the **LASTDRIVE** instruction in the **config.sys** system file and reboot your computer.
14	Unable to restore the Private Disk!	Wrong backup copy alternative access password was entered.	Enter the right backup copy alternative access password.
		Virtual disk write error.	Use special utilities to check the virtual secret disk. It may have file system errors.
		Backup file read error.	Use special utilities to check the hard disk storing the backup copy. It may have bad sectors or disk file systems errors.
		The memory capacity of the recovered data exceeds the volume of the connected virtual disk.	Create a new virtual disk with more free space.

7 Glossary

Term	Description
Application Programming Interface (API)	This is a software interface used for interaction between the *OS* and an application.
Basic Input/Output System (BIOS)	The *PC* Basic Input/Output System is an OS-independent software designed for hardware operation support. This is an essential set of routines in a PC, which is stored on a chip and provides an interface between the operating system and the hardware.
International Organization for Standardization (ISO)	International Organization for Standardization
Authentication	This is a control process checking the authenticity of the users identity, i.e. this process checks whether the user is the person they claim to be.
Biometric Authentication	This is the user authentication based on examining specific physical traits of the user by means of special biometric equipment. Biometric authentication can be based on examining fingerprints, iris, voice, and other specific traits of the user's body.
Two-Factor Authentication	This is a process controlling the authenticity of the users identity on the basis of the two following factors: Something You Know — for example, the user name and password. Something You Have – for example, the *eToken* device.
Encryption key	Specially built numerical sequence used to transform the source information into the encrypted data using a special algorithm.
Driver	This is software designed to control data input/output and interface the applications/*OS* and the device connected to the *PC*.
Identification	This is a control process using a unique identifier to determine whether the specific user is known to the system.
One-Factor or Standard Authentication	This is a process controlling the authenticity of the user identity by standard means of the *OS* on the basis of a single factor: Something You Know – the user name and password.
Registration	The process resulting in user *authentication* using his login and password pair. If the registration is successful, the user is granted access to the OS within the limit of his privileges.