dekart

MAKE IT SECURE

USER GUIDE

DEKART
PASSWORD CARRIER

Table of Contents

1 License and trademarks information

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.

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

2 Dekart SRL contact information

For information about Dekart or any of our products, please contact us at the following email addresses or feel free to visit our web site.

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

2.1 Dekart Password Carrier purpose and features

Dekart Password Carrier is a solution that allows you to securely store the private information used to authenticate yourself on websites or in certain Windows applications, and automatically fill in the selected forms. Dekart Password Carrier has an intuitive interface, and the ability to store the information without your intervention ("training" mode), memorizing the sites you visit, as well as the texts you type.

The data gathered by Dekart Password Carrier are encrypted with the AES algorithm and stored on a removable device or fixed disk. Whenever you open a page after previously visiting it, Dekart Password Carrier will automatically fill in all the forms (if any). You can override this setting, by disabling the automatic filling of specific (or all) fields.

Dekart Password Carrier is able to generate cryptographically strong passwords, which you can use for your accounts.

The program's ability to create encrypted backup copies of your data (as well as restore the data from

a backup copy) is useful too.

Dekart Password Carrier employs three-factor authentication (see Biometric authentication in Dekart Password Carrier), this means that a PIN-code and a BIO ID are needed once the Key Storage Device is connected (see Terms and abbreviations).

Security principles of Dekart Password Carrier

1. Dekart Password Carrier stores the URLs of the sites you visit, the names of the applications you use, as well as the authentication data on a PIN-code protected Key Storage Device. Your BIO ID resides there too. This means that you no longer have to remember your passwords, or write them on papers, etc. Due to the fact that Dekart Password Carrier employs three-factor authentication, the risk of privacy exposure is virtually nil, even if your Key Storage Device is lost or stolen.
2. In order to access the protected resources, you have to launch Dekart Password Carrier and enter the correct PIN-code (and perform the biometric authentication, if you have previously enabled it).
3. If the computer is left unattended (ex: the mouse was not moved, or no button was pressed for 5 minutes), Dekart Password Carrier will deactivate itself. To activate the program, you must enter the PIN code..
4. If you restart or hibernate your computer without quitting Dekart Password Carrier first, the program will shut itself down, clearing the memory areas that contained the information about your accounts.

Features of Dekart Password Carrier

Besides automatically collecting your passwords, storing them in an encrypted form, and transparently feeding them to the web-browser, Dekart Password Carrier provides other features you'll find useful:

- *Generate strong passwords*: the program can generate complex passwords that you can copy and paste into registration forms. Not only that it will make your accounts practically immune to brute-forcing, but it also guarantees that all your accounts will have distinct passwords (which is an attacker's worst nightmare);
- *Easy registration of new accounts*: Dekart Password Carrier allows you to define a custom user profile, the data from which will be automatically filled in when signing up on a site. You are no longer forced to spend time entering details such as address, phone number or your name. This also helps you to avoid accidental typos;
- *Freedom of movement*: this password management tool runs on *any* version of Windows which is in common use, and does *not* require administrative privileges. Thus you can be sure that you can stay connected to the world, regardless of your location;
- *Anti-phishing*: free phishing protection is what you automatically get as soon as you start using Dekart Password Carrier. Illicit sites that were designed to resemble authentic ones might fool the human eye, but they will *not* be processed by Dekart Password Carrier. Manually crafted Windows applications that mimic another application will not trick you either;
- *Keylogger protection*: since form-filling is done automatically, no keyboard typing is required. Keyloggers *(being a common problem of public terminals or computers in internet cafes)* will no longer be able to memorize user credentials, helping you to avoid identity theft;
- *Encrypted backup*: back yourself up by making an encrypted copy of the key, which can be used if your original key was lost or stolen. The data are encrypted with Dekart's NIST-certified implementation of the strongest algorithm available today – AES 256-bit;
- *Ease of use*: the program works in the background and doesn't get in your way when you work. In addition, you can temporarily disable it with only two mouse-clicks;
- *Easy customization*: Dekart Password Carrier can be trained to work with non-standard web-sites;
- *Flexibility* – The same Key Storage Device may be used for other Dekart applications (such as Dekart Logon, or Dekart Private Disk Multifactor), as well as for programs developed by other

vendors.

Note. Dekart Password Carrier is compatible with:
1. Internet Explorer (v.4 and above), and IE–based browsers such as Maxthon;
2. FireFox, Mozilla, SeaMonkey, if the IE Tab (http://ietab.mozdev.org/) extension is installed ;
3. various Windows applications that use STANDARD forms (ex: Client Lotus Notes, 1C:Enterprise, all Dekart's products PIN code forms, etc.);
4. Adobe Acrobat v.7.0, 8.0.

3 Terms and abbreviations

Dekart Password Carrier (DPC) – the name of the program.

Key Storage Device (KSD) – a device on which personal information is stored (usernames and passwords for various web-sites or Windows applications that require authentication). Password Carrier can be used with the following types of devices:

- USB flash drives;
- External hard disks;
- Flash memory cards (SD - Secure Digital, MMC - Multimedia Card, CF - Compact Flash, MS - Memory Stick, etc.);
- External devices that are detected as removable drives by the system, ex: PDAs, certain models of digital cameras, digital audio players such as the iPod;
- An encrypted file on the system's hard disk.

Additionally, a PIN code can be used to enhance the privacy of the data contained within the Key Storage Device. The program's interface uses the 'KSD' abbreviation, while the manual uses the extended version.

PIN (Personal Identification Number) – a secret number that gives you access to the Key Storage Device. The PIN code can be 4 to 8 symbols long.

BIO ID – A biometric ID – information that contains data about a person's unique features (ex: fingerprint, voice or retina). The size of the BIO ID is variable; a fingerprint requires about 600 bytes of data, while a voice key-phrase may take up to 30 Kbytes.

Biometric authentication – the process of authenticating a person by analyzing its unique features, using special biometric hardware. Biometric authentication can be carried out by processing one's fingerprint, voice, retina, or other biological characteristics.

Two-factor authentication – the process of authenticating a person's identity, that relies on two factors: "*Something you have*" – ex: a Key Storage Device; and "*Something you know*" – ex: a PIN code.

Three-factor authentication – an enhanced version of the previous entry, that uses an additional, third factor: "*Something you are*" – ex: a person's BIO ID.

4 Introducing Dekart Password Carrier

This chapter contains the information about the purpose and features of **Dekart Password Carrier.**

Dekart Password Carrier offers you the ability to securely access web sites via an Internet browser,

as well as to use Windows applications that require authentication.

Dekart Password Carrier allows you to:
- Store authentication data on your Key Storage Device in order to access web sites or other resources that require authentication.
- Automatically fill forms with your personal data (on Internet sites and in Windows applications, as well as in Adobe Reader v. 7.0 and 8.0 documents).

How to start working with Dekart Password Carrier?

4.1 Dekart Password Carrier product's components

One **Dekart Password Carrier** package contains the following components:
- the application,
- documentation,
- the Key Storage Device (optional).

The Key Storage Device acts as the unique means of keeping the authentication data to access to web sites and Windows applications.

4.2 Dekart Password Carrier hardware and software requirements

Hardware requirements
- Personal computer, with at least one available port for the Key Storage Device.
- If you prefer to use three-factor authentication, a biometric device is needed, e.g. BioLink U-Match Mouse.

Software requirements
- Operating System: Windows 98, NT4.0, 2000, ME, XP.
- Microsoft Internet Explorer 4 (or newer).
- Key Storage Device drivers (usually provided with the product, or can be downloaded from the Key Storage Device manufacturer's web site).
- Drivers of biometric device.

Note. Dekart Password Carrier is compatible with:
1. ***Internet Explorer (v.4 and above), and IE–based browsers such as Maxthon;***
2. ***FireFox, Mozilla, SeaMonkey, if the IE Tab (http://ietab.mozdev.org/) extension is installed ;***
3. ***various Windows applications that use STANDARD forms (ex: Client Lotus Notes, 1C:Enterprise, all Dekart's products PIN code forms, etc.);***
4. ***Adobe Acrobat v.7.0, 8.0.***

Attention!
Detailed information about biometric devices, used for authentication (features, software etc.) can be obtained from the BioAPI Consortium at www.bioapi.org.
For more information about flash disks (OS requirements, drivers, etc.), contact the manufacturer.

4.3 Supported key storage and biometric devices

Dekart Password Carrier supports the following devices:

Key Storage Devices:

Dekart Password Carrier is a sophisticated tool that can work with a broad range of removable storage devices, among which:

- USB flash drives;
- hard disk;
- external hard disks;
- flash memory cards (SD - Secure Digital, MMC - Multimedia Card, CF-Compact Flash, MS - Memory Stick, etc.);
- external devices that are detected as removable drives by the system, ex: certain models of digital cameras, digital audio players such as the iPod, PDAs, etc.

Biometric verification devices:

- Dekart Software uses most types of BioAPI and HA API compatible biometric verification devices, for example:
- Precise Biometrics Precise 100 fingerprint and smart card reader series
- SCM SCR222 fingerprint reader
- BioLink U-Match MatchBook
- BioLink U-Match Mouse

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

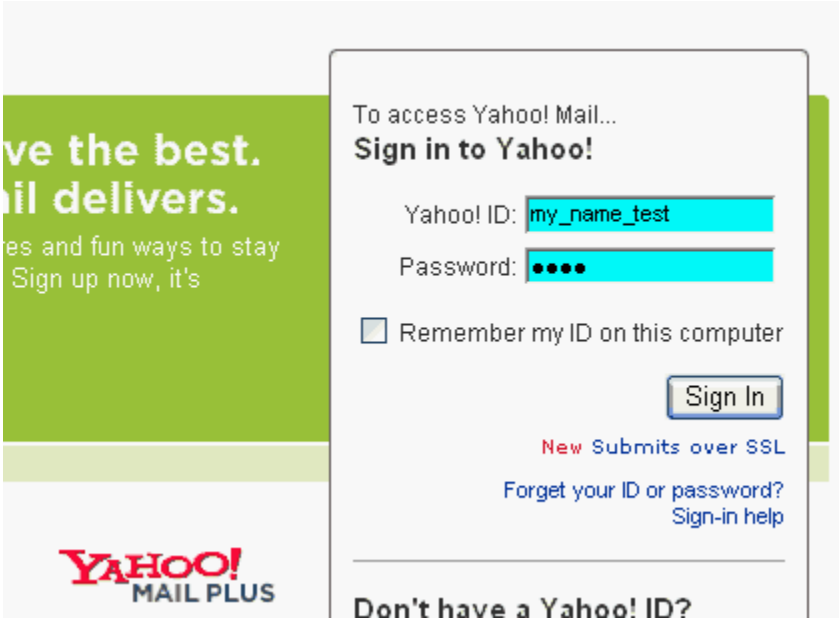
Note 1. If you wish to independently decide which Key Storage Device to use, make sure that it has plenty of space for all the components (the software, the private information – about 2 MB). Note that a certain area of the Key Storage Device may be taken by the BIO ID.

Note 2. Dekart delivers all Key Storage Devices without a predefined PIN code.

5 Quick Start for Dekart Password Carrier

Using **Dekart Password Carrier** does not require any special skills, as virtually everything is automated. Below is a short step-by-step guide.

1. Install Dekart Password Carrier as you would install any other Windows application. For more details, consult this section: Installing Dekart Password Carrier.
2. Migrate the software to the Key Storage Device (see Installing Dekart Password Carrier to a Key Storage Device. ***Note.*** By default, as a Key Storage Device, the removable disk will contain Password Carrier's program files, as well as your personal data (thus the program can be started directly from the Key Storage Device, on any computer).
3. To start using the application, run DPCarrier.exe (see Starting the application).
4. To "train" the system, you should (at least once) open a web-page or an application that contains forms, fill them in with the right values, then confirm your actions (ex: by pressing **OK**, **Next**, **Send**, etc.). All the typed-in details will be stored on the Key Storage Device.
5. Next time you run the same application or open the same web-page, the fields will be filled automatically (you will notice that the color of the fields changes to turquoise).

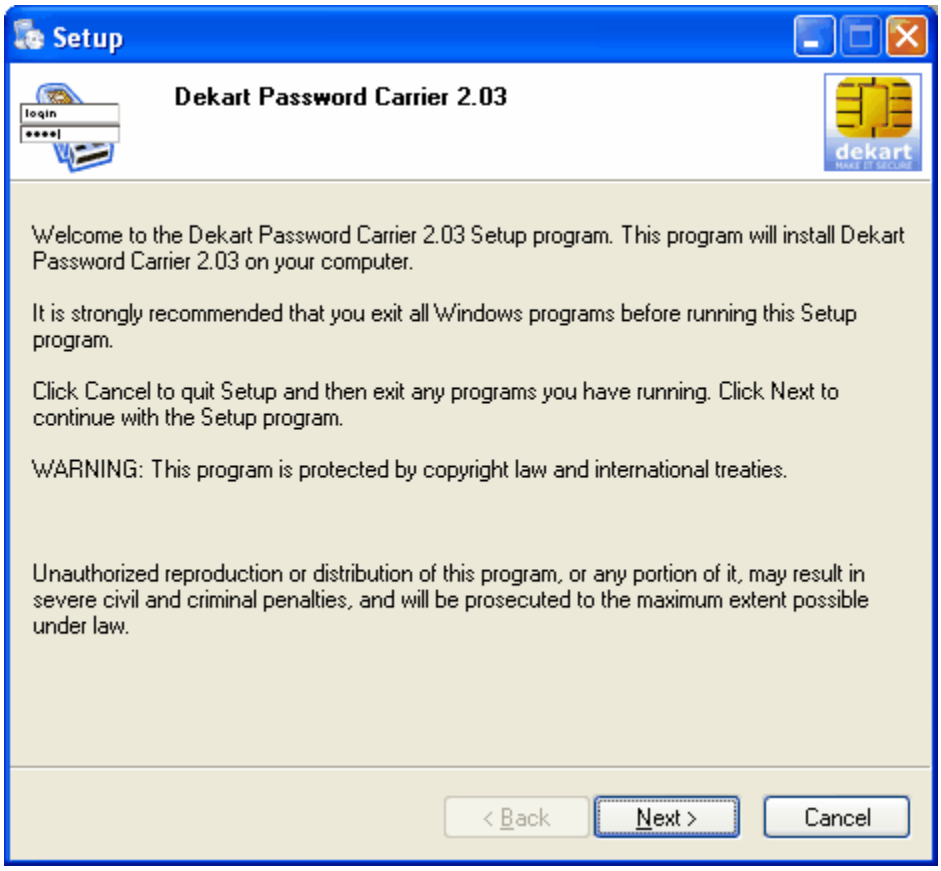


6 Installing, updating and uninstalling Dekart Password Carrier

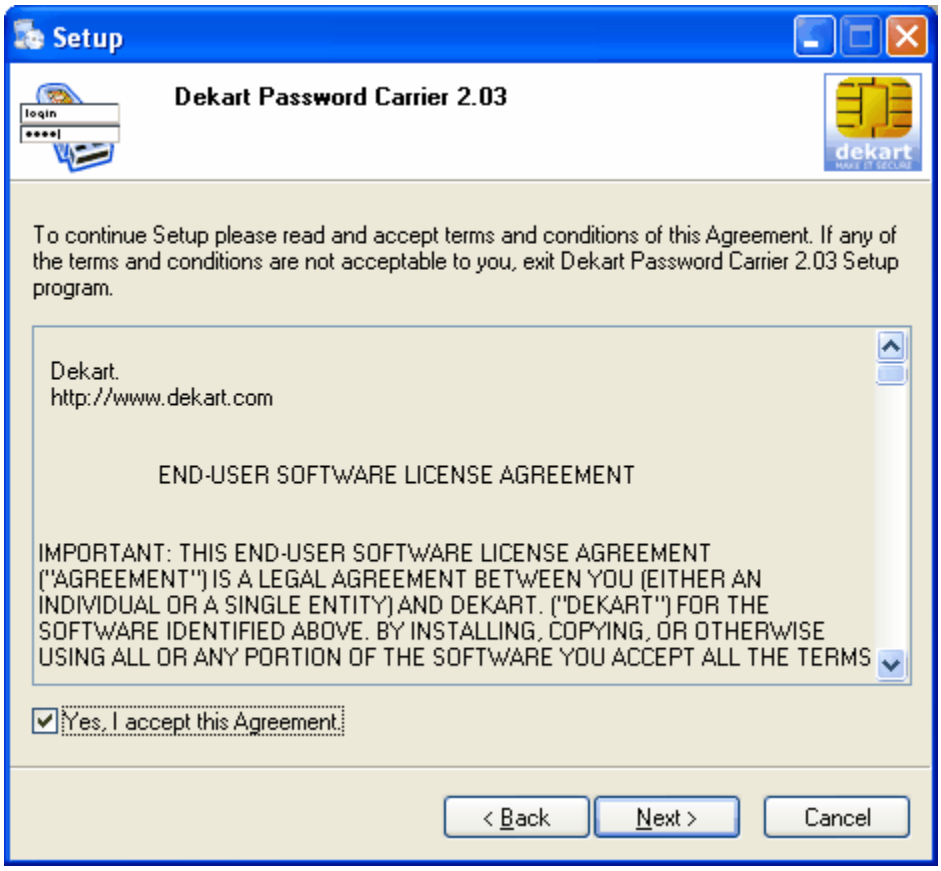
- Installing;
- Updating;
- Uninstalling.

6.1 Installing Dekart Password Carrier

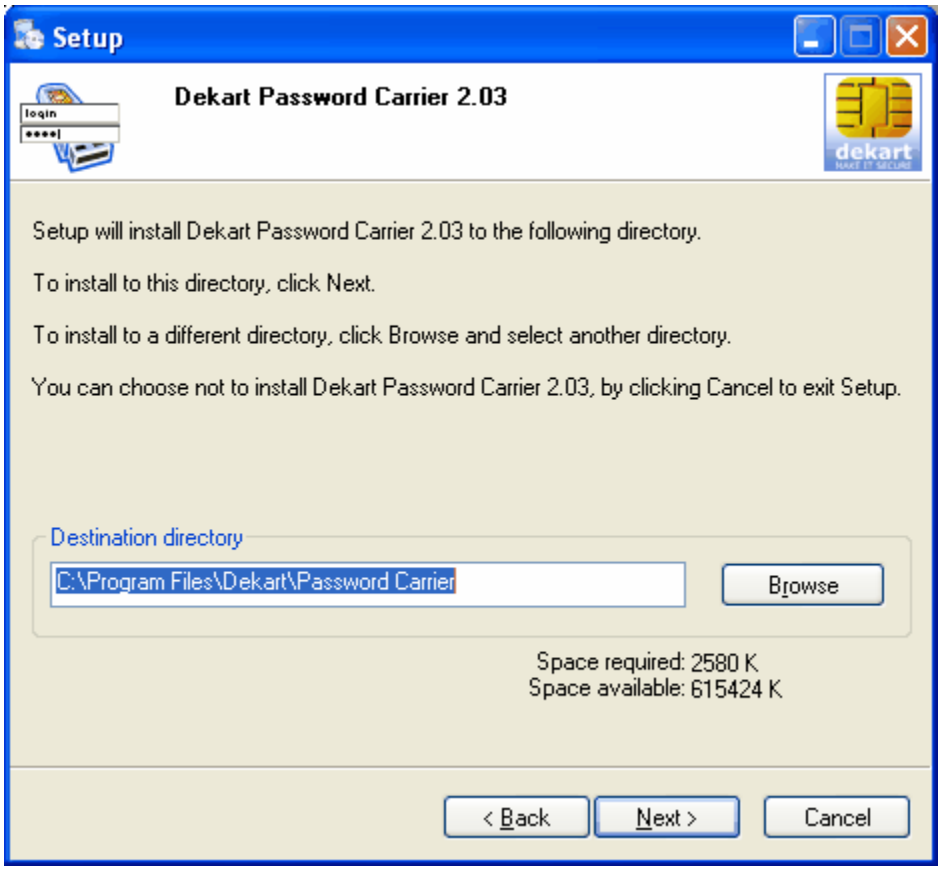
1. Before beginning the installation of the software, you must close all the open applications. Make sure that the device you intend to use as a Key Storage Device is properly connected and configured.
2. In order to enable three-factor authentication, the biometric device should be connected and its drivers should be installed.
3. In order to install Dekart Password Carrier you must launch the program: DPCarrier.exe.
4. In the appearing window select **Next**.



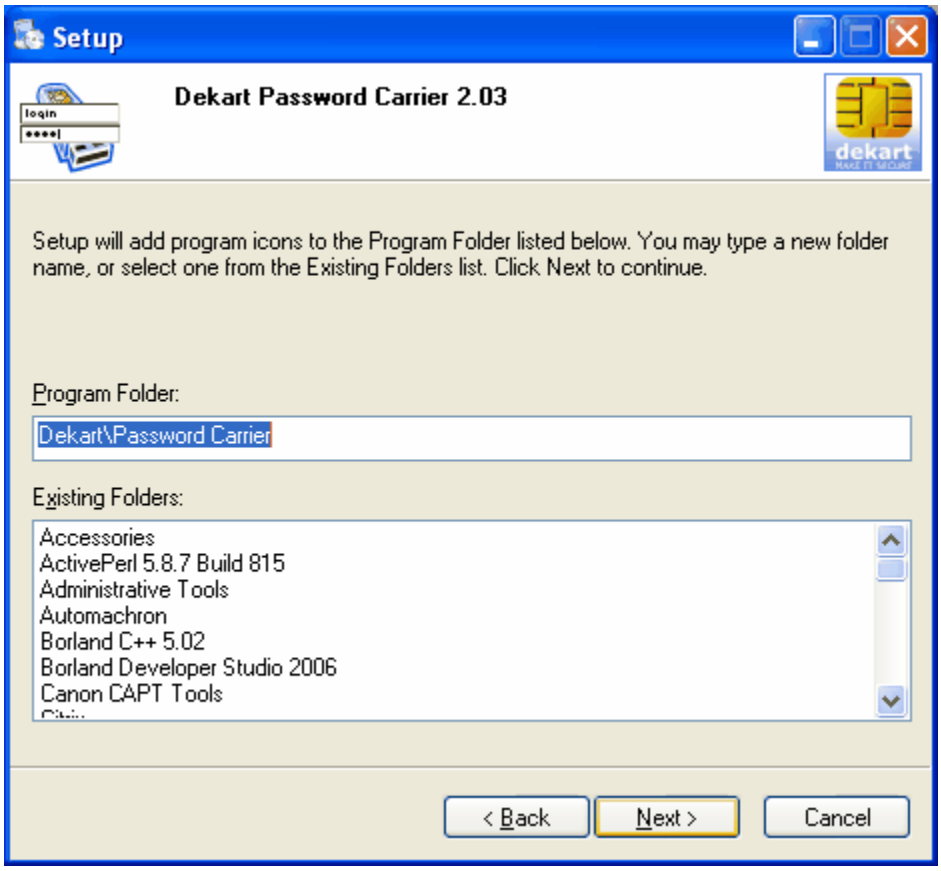
5. The license agreement window appears. You must accept the license agreement before you can proceed with the installation.



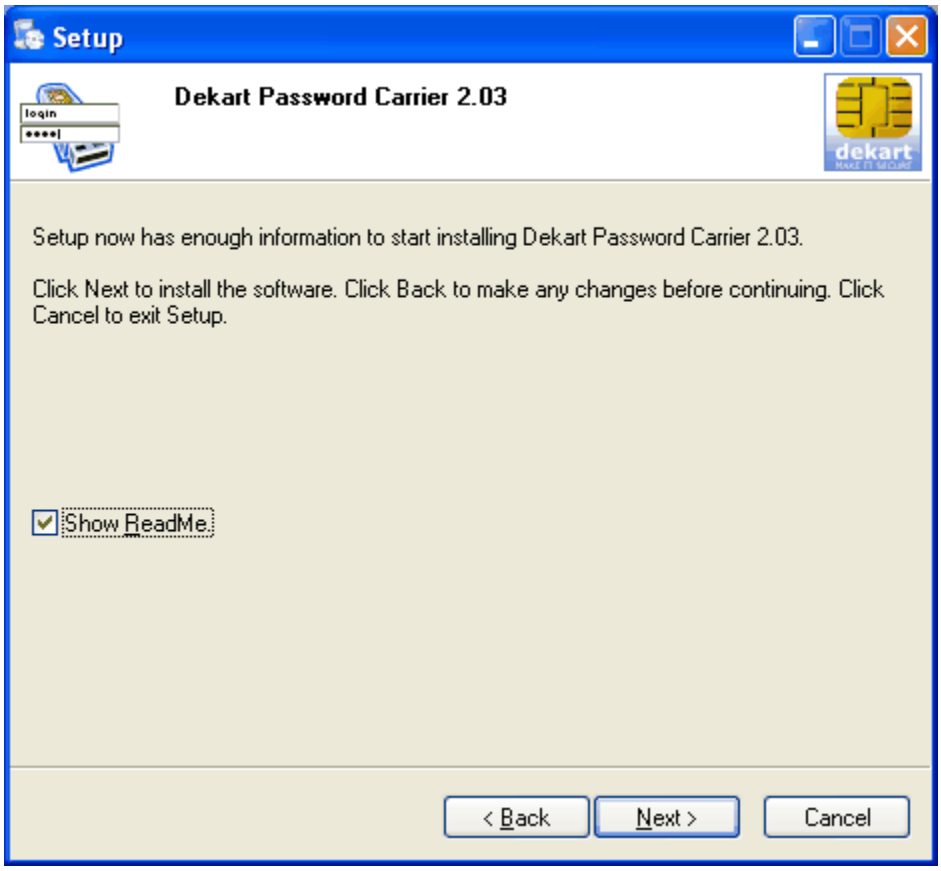
6. You must then select the folder, where the Dekart Password Carrier software is to be installed. ***Note: do not install the program directly to the removable device, it should be installed to the system's hard disk. For details, see*** ***Installing Dekart Password Carrier on a removable device***



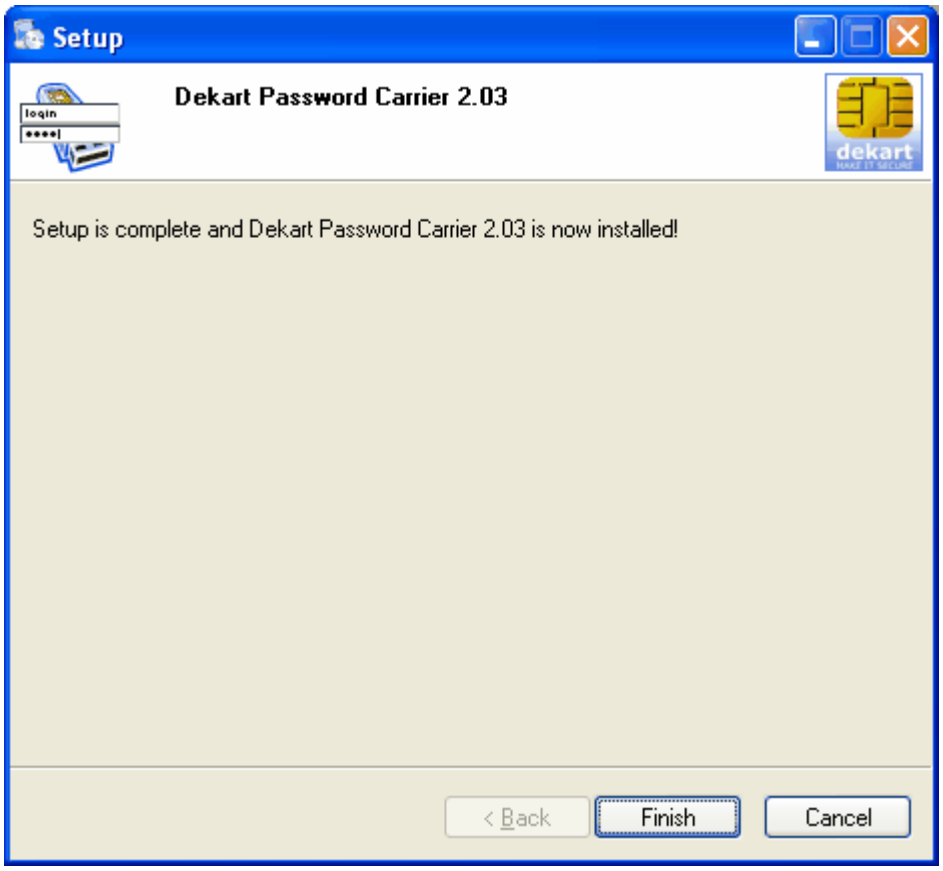
7. You must then select the folder in the **Start Menu**, where the Dekart Password Carrier software is to be added.



8. The next step in the installation process requires that you press **Next**. Click the *Show ReadMe* checkbox to view additional information about Password Carrier.



9. The final step in the installation process requires that you press **Finish**.

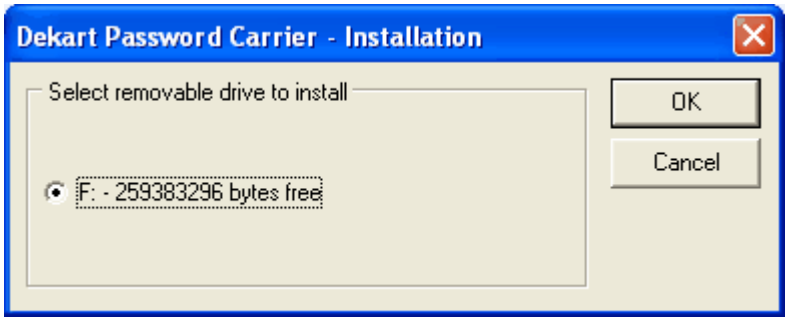


After this process is completed, the program will copy the necessary files, and the installation procedure will be complete.

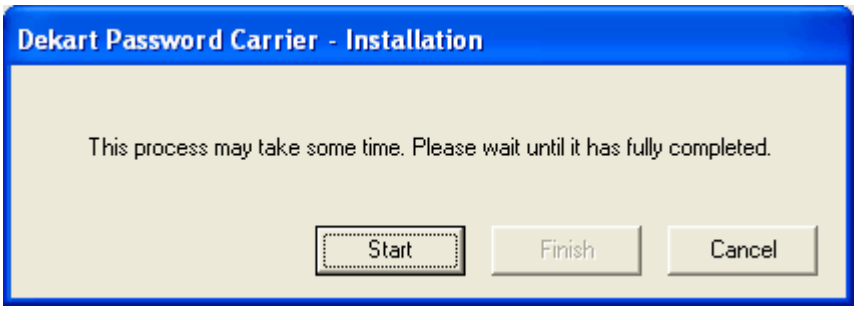
6.2 Installing Dekart Password Carrier to a removable device

To do this, follow these steps:

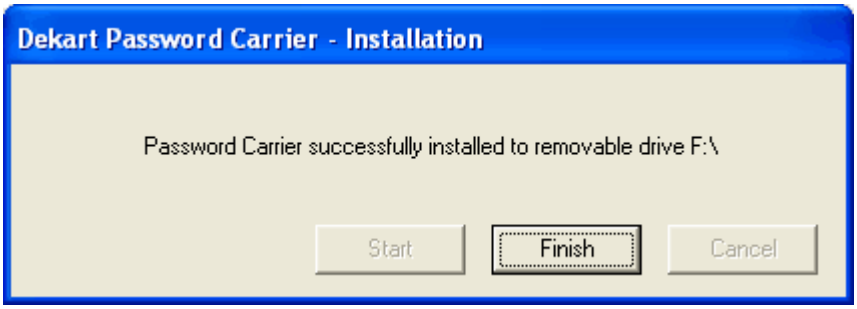
1. Install Dekart Password Carrier.
2. Open the **Start** menu, go to: ***Programs\Dekart\Password Carrier***, and choose **Install to removable device**.
3. In the opened window select the removable device which you will use as a Key Storage Device and press ***OK***.



4. In the opened window press ***Start***.



5. There will appear a notification message that the software was successfully installed on the Key Storage Device. Press the ***Finish*** button.



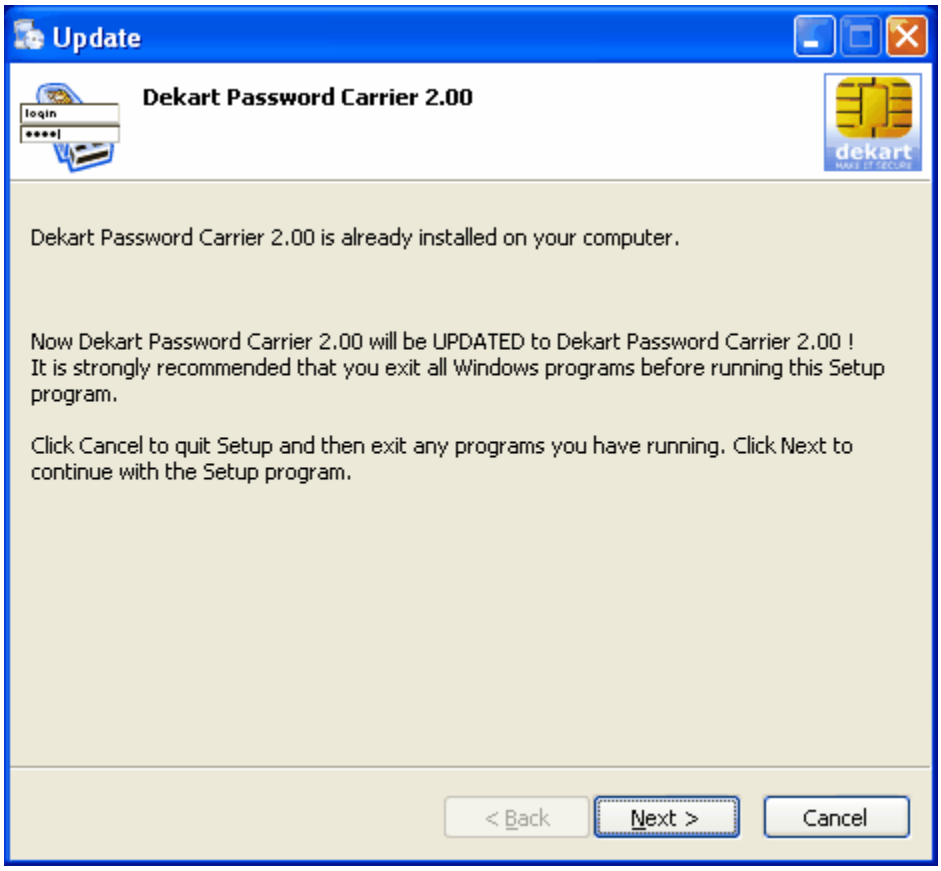
Note 1. Make sure that there are no read\write operations involving the removable device before disconnecting it from the computer (most of the Flash disks have a LED that indicates whether the device is in use or not)..

Note 2. Make sure that there are no read\write operations involving the removable device before disconnecting it from the computer. For example, most of the Flash disks have a LED that indicates whether the device is in use or not.

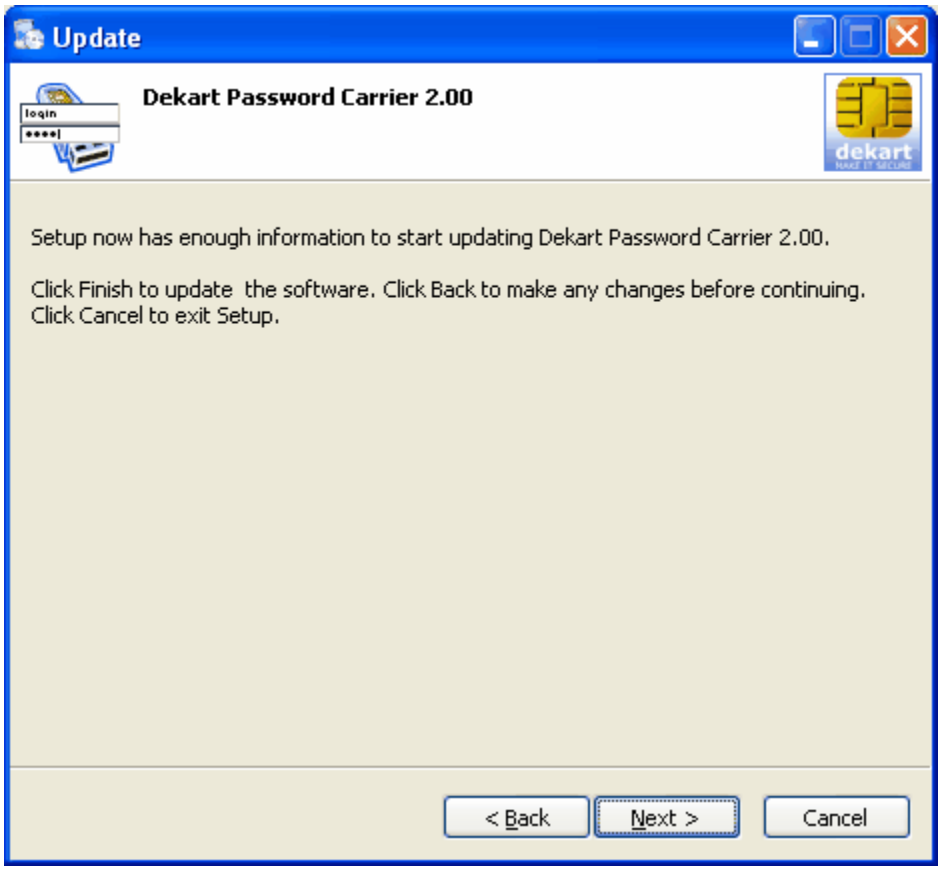
6.3 Updating Dekart Password Carrier

To update **Dekart Password Carrier** please obtain the latest version from Dekart.

1. Next time you launch the setup program, the installation program will automatically check for the presence of an earlier version, and will display all the necessary information in a separate picture (see below).

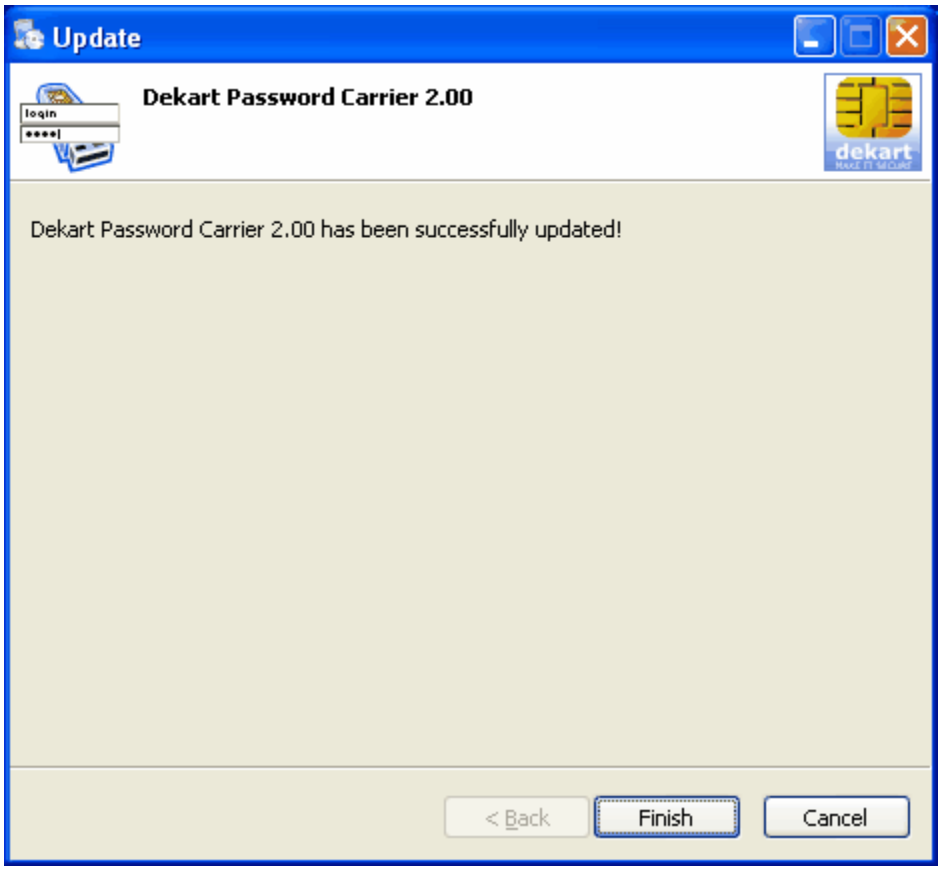


2. In order to continue the process, press **Next**. You must accept the license agreement before you can proceed with the update.



Upon the completion of the above steps, the program will copy the installation files. In the event that you are updating the application, all updated files will then be copied.

3. Click the **Finish** button to finalize the update process.



Note 1: After updating Dekart Password Carrier, it is necessary to restart your computer.

Note 2: To update the software located on a removable device, you have to repeat the steps described in the "Installing Dekart Password Carrier on a Flash disk" chapter once the update is complete.

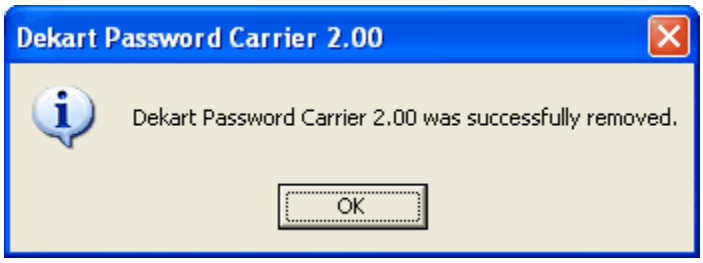
6.4 Uninstalling Dekart Password Carrier

In order to remove the software, follow these steps:

1. Select **Programs** in the **Start Menu**, locate the folder you have entered at step 7 when installing the program, select **Uninstall** (alternatively, you can go to **Control Panel**, select **Add or Remove Programs**, select the program name in the list and press the **Uninstall** button). The following message will appear:

In order to confirm your intention to remove Dekart Password Carrier press **Yes**.

2. After the successful completion of the de-installation process the following message will appear:



Note. To remove Dekart Password Carrier from the Key Storage Device, delete the folder <removable_device>:\Dekart\Password Carrier.

7 List of operations available in Dekart Password Carrier

Key Storage Device-related operations:

Change PIN	Change the PIN-code assigned to the Key Storage Device
Change Label	Change the current label of the Key Storage Device
Change BIO ID	Change the BIO ID assigned to the Key Storage Device

Operations that can be performed with the records stored on the Key Storage Device:

Backup Data to File	Create a backup copy of the data stored on the Key Storage Device
Restore Data from File	Restore the data from a previously made backup copy
Use Fixed Drive	Password Carrier will use a PIN-protected file on the system's hard disk

User Data Tuning:

User Profile Tuning	Create and edit the User Profile (i.e. define and store on the Key Storage Device typical data fields - Full Name, Address, email, phone, etc., default Login and Password)
Logon/Password Fine Tuning	Edit the status of a certain field (automatic – *Managed*, or manual - *Ignored*), or remove a field from a Key Storage Device, or edit Name or/and Password value in the selected field

Controlling the application:

Go To Collected Favorite	Open previously visited web-sites in the system's default browser and automatically fill in the fields of the existing forms.
Force Form Fill	Fill in the forms with data from your User Profile.
Managing (On/Off/Fill only)	Enable or disable automatic form filling (Internet browser & standard Windows applications)
Windows Filling (On/Off)	Enable or disable automatic Windows applications form filling
Exit	Quit the application
Exit & Eject	Quit the application and initiate the safe hardware removal procedure.

Other operations:

Make Safer Password	Generate a cryptographically strong password
About	See additional information about the software
Help	Open the Help file

8 Using Dekart Password Carrier

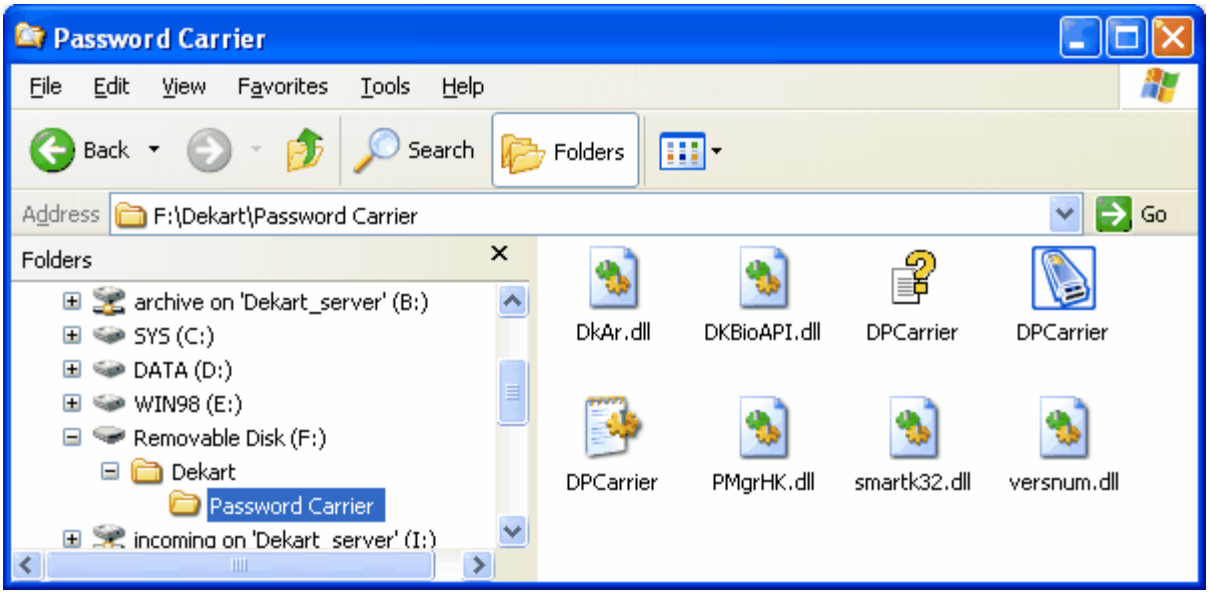
Password Carrier can be started from a removable drive, as well as from a fixed one (such as the system's hard disk). Your private data may reside on a removable device, or on a fixed drive. The table below illustrates the possible use cases:

Start Password Carrier from	**Store your data on**
A removable drive	A removable drive
A removable drive	A fixed disk
A fixed disk	A removable drive
A fixed disk	A fixed disk

8.1 Starting the application

Start from removable device

1. Connect the Key Storage Device to your computer.
2. Open ***<removable_device>:\Dekart\Password Carrier*** in Windows Explorer and run DPCarrier.exe.



Start from hard disk

The program can be started in one of the following ways:

- Go to **Start Menu** \ *Programs*, select the folder you chose at step 7 when installing the program (see Installing Dekart Password Carrier), then run the program.

- In Windows Explorer, open the folder indicated at step 6 of the installation process (see Installing Dekart Password Carrier), then run the program.

When the program is launched for the first time, the following window will show up if the Key Storage Device is not PIN-protected:

We strongly recommend you to enable PIN code protection and press the Set PIN button. In this case the ***Change PIN Dialog*** will show up (see Changing the PIN code section). If you do not want to use two-factor authentication press ***Leave PIN empty.***

If the Key Storage Device is already PIN-protected, the following window will show up:

3. Enter your PIN-code and press **OK.**

Note. If the Key Storage Device contains a BIO ID as well, Dekart Password Carrier will ask you to perform the biometric authentication too.

If the authentication is successful, you will notice Dekart Password Carrier's icon in the system tray area.

8.2 "Training" Dekart Password Carrier

No special actions are needed to train the application, i.e. make it memorize the data you enter. The process is fully automated. To "train" the system, you should (at least once) open a web-page or an application that contains forms, fill them in with the right values, then confirm your actions (ex: by pressing **OK**, **Next**, **Send**, etc.). All the typed-in details will be stored on the Key Storage Device. You can see these stored details in the *Collected Favorites* (web-site URLs) and *Managed Passwords and other Edits* (all stored data) windows.

Next time you run the same application or open the same web-page, the fields will be filled automatically (you will notice that the color of the fields changes to turquoise). From that moment on, you can browse the page in a usual manner.

One of the program's additional features is the ability to pre-define values for fields that are frequently used on web-forms (ex: Full Name, Address, email, Phone, etc.). To create a template, follow the steps given in the **User Profile Tuning** section. To fill in a field with one of the pre-defined values:

1. Right-click the icon in the system tray.
2. Choose **Force Form Fill** from the menu**.**

Afterwards, the program will automatically find the fields and fill them in with data from the template (see User Profile Tuning).

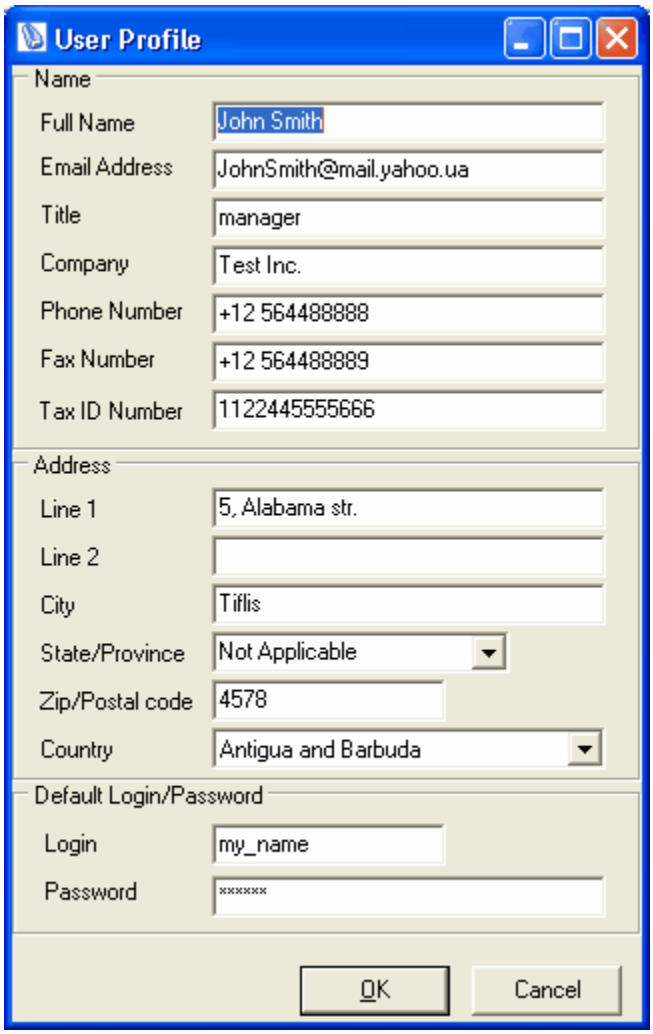
Note. The fields can be edited, even after they were automatically filled by Dekart Password Carrier. If you enter a new value in a certain field, Dekart Password Carrier will update the record on the Key Storage Device, and use it next time you open the same page or use the same application.

8.3 User Profile Tuning

To create or to change a template field from User Profile, follow these steps:

1. Right-click the icon in the system tray.
2. Choose **User Profile Tuning** from the menu**.**

The *User Profile* window will appear on the screen.



3. Fill in the fields of the form and press OK. The profile will be stored on the Key Storage Device and it can be used in the future if necessary.

8.4 Form filling

Filling forms with Dekart Password Carrier is a simple process.

After launching Dekart Password Carrier, the fields of the web-forms and applications you use will be **automatically** filled with appropriate data from the Key Storage Device.

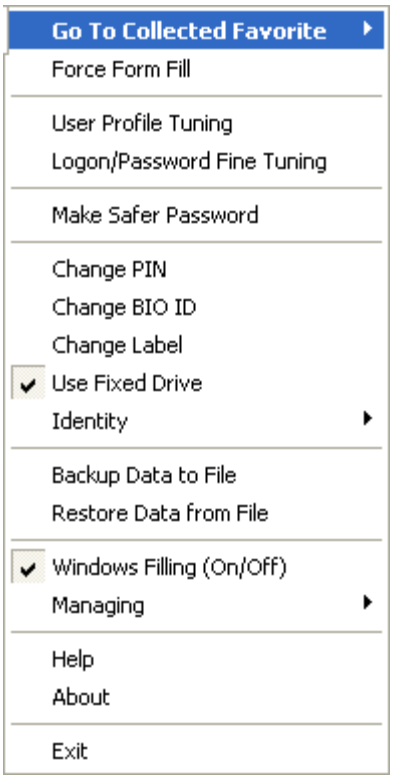
When visiting a web-site or launching an application for the first time, you can fill in the forms manually, or use the previously defined User Profile to do that automatically.

Note. If some input-fields are not filled when you visit a web-site for the first time, Dekart Password Carrier will fill in these forms with data taken from the most appropriate details of your User Profile when you visit the web-site next time.

8.5 Opening a web-page from a Key Storage Device

A web-page can be opened in the default Internet browser directly from Dekart Password Carrier's main menu, if it was previously written to the Key Storage Device:

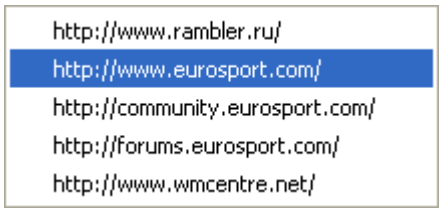
1. Right-click the icon in the system tray.
2. Choose **Go to Collected Favorite** from the menu.



Opens a short list of previously-visited sites that contained forms filled by the user. The number and the order of the displayed sites depends on how frequently the sites are visited, and when they were visited last time.

To view the full list of previously-visited sites, click **Show all collected favorites**.

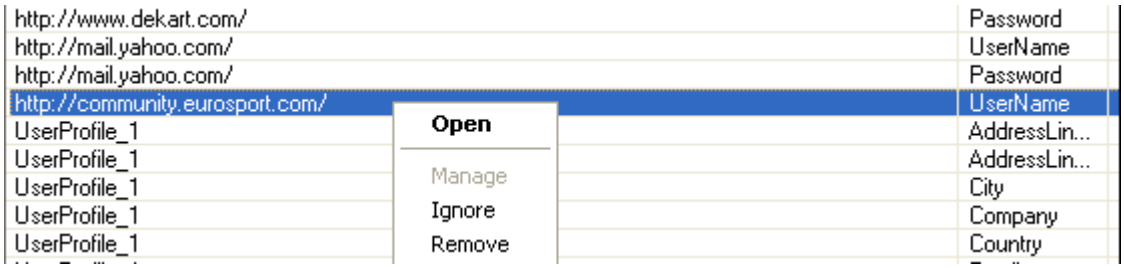
3. Choose an URL from the list and click it.



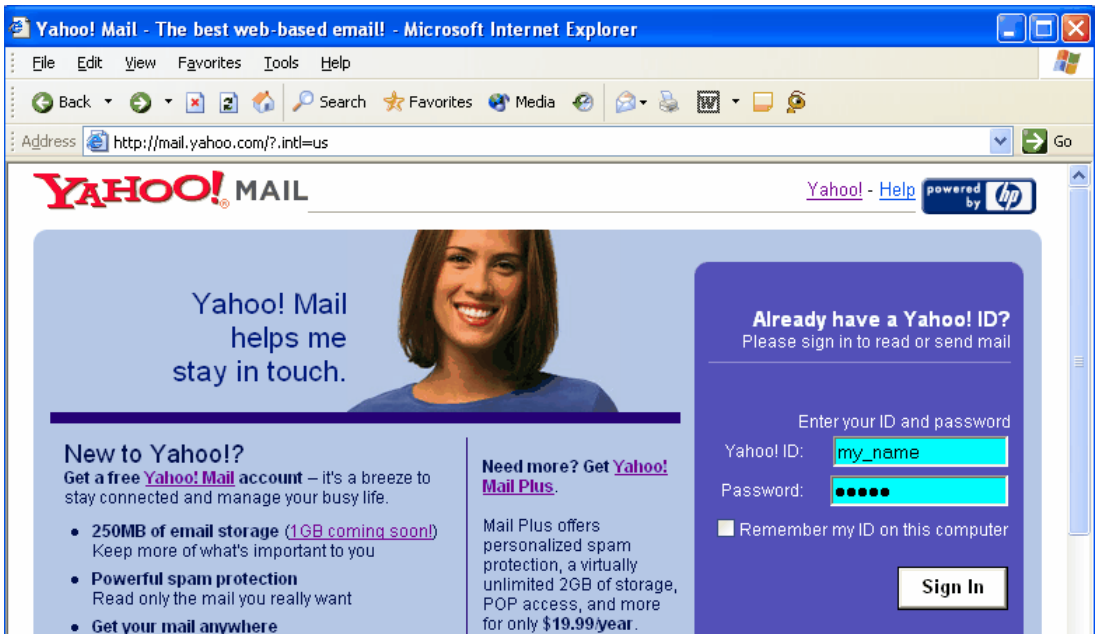
See also Managing Collected Favorites.

A web-page can also be opened in the default Internet browser directly from Dekart Password Carrier's main window, if it was previously written to the Key Storage Device:

1. Right-click the icon in the system tray.
2. Press **Logon/Password Fine Tuning**. A window that displays the contents of the Key Storage Device will show up – *Managed Passwords and other Edits.* (see Dekart Password Carrier Automating setting).
3. Click an item in the list (i.e. a line in the table).
4. Press **Open** in the menu.



The default Internet browser will be launched and directed to the chosen page. All the fields of the page will be filled with their respective values.



8.6 Managing Collected Favorites

The Collected Favorites can be viewed as a single (full) list, or as two lists (short, full). The short list will only include the frequently visited sites, and it is being updated automatically while you change your surfing habits.

You can exclude one or several sites from the short list of favorites:

1. Right-click the icon in the system tray.
2. Choose **Go to Collected Favorite** from the menu.
3. Right-click an address from the list.
4. Press **Hide** (to hide the selected address) or **Hide All** (to hide all addresses).

You can edit the full list of Collected Favorites too – either by deleting a list entry, or by setting the Ignore mode (do not fill forms) for a chosen site.

To delete a site from the list, or change its status:

1. Right-click the icon in the system tray.
2. Choose **Go to Collected Favorite** from the menu.
3. Right-click an address from the list.
4. Click **Delete** (to remove the address) or **Ignore** (to change the status of the site).

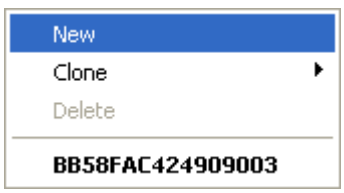
See also Dekart Password Carrier automation settings **and** Removing unused records from a Key Storage Device**.**

8.7 Using identities

You can create multiple identities; each of them will hold a different set of credentials for the forms you fill. Password Carrier creates a default identity, where your personal data are stored as you fill forms on web sites and in Windows applications. If you wish to use a different set of data for a particular form, you can create a new identity; Password Carrier also allows you to clone, rename and delete an identity.

To manage your identities, follow these steps:
1. Right-click the icon in the system tray.
2. Choose **Identity >** from the menu.
3. The identities menu will be shown.

Before adding a new identity, the menu looks like this:



As you switch between identities, the menu will change its appearance:

The top side of the menu lists the actions that can be carried out with an identity (create new, clone, delete). The lower side of the menu lists the existing identities.

Note: The name of the default identity is the serial number of the key storage device that contains your credentials.

Choosing an identity

To choose a different identity, find it in the list and click on it; it will become the first entry in the list and its name will be written in **bold** letters. In addition, you can see the current identity when you hold the mouse over Password Carrier's icon in the system tray, it will be shown as "KSD Label: identityi_name".

The current identity will be activated when Password Carrier is started next time

Creating a new identity

To create a new identity, press **New** in the menu, you will then be asked to enter the name of the new identity.

Note: for your convenience, a default name is generated automatically (containing the name of the current identity and a number).
Note. To ensure the security of the new Identity, follow the change_PIN and change_BIO_ID procedures..

Cloning an identity

To create a copy of an identity, press **Clone** in the menu, and choose the identity which you wish to clone. You will be asked to provide a name for the new identity. Press **OK** to complete the operation.

Note. A cloned identity will retain the BIO ID and the PIN of the original identity.

Renaming an identity
An identity can be renamed: make that identity the current one, and then change the label of your Key Storage Device (see Changing the Label of a Key Storage Device).

Deleting an identity
To remove an identity, press **Delete** in the menu, and click on the identity you wish to remove.

8.8 Modifying the parameters of a Key Storage Device

While using Dekart Password Carrier, you might wish to change some parameters of the Key Storage Device:

- Add a BIO ID, or change the current one.
- Add or change the PIN-code.
- Change the label of the Key Storage Device.
- Use a hard disk as a Key Storage Device.

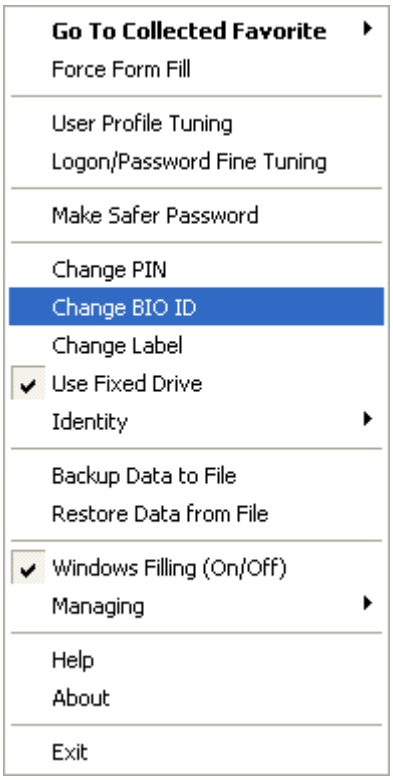
Note. The following operations apply to the current identity: Add or change BIO ID, Add or change PIN-code, Change the Label.

8.9 Adding a BIO ID to a Key Storage Device

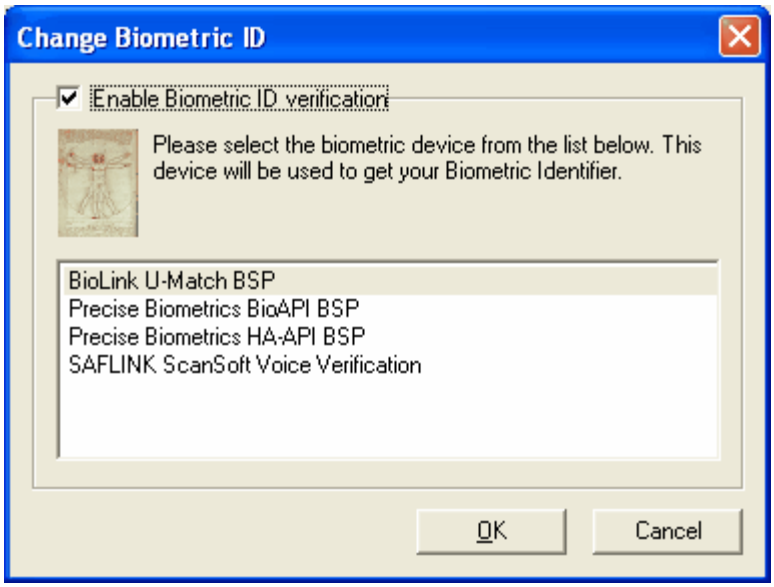
Three-factor authentication requires a BIO ID to be assigned to the Key Storage Device (current identity).

Note. When choosing a biometric device, consider your intrinsic physical traits (ex: certain fingerprint scanners will not work if the skin is too dry). Keep in mind that the environment has a major impact on voice-recognition; therefore the position of your computer is important.

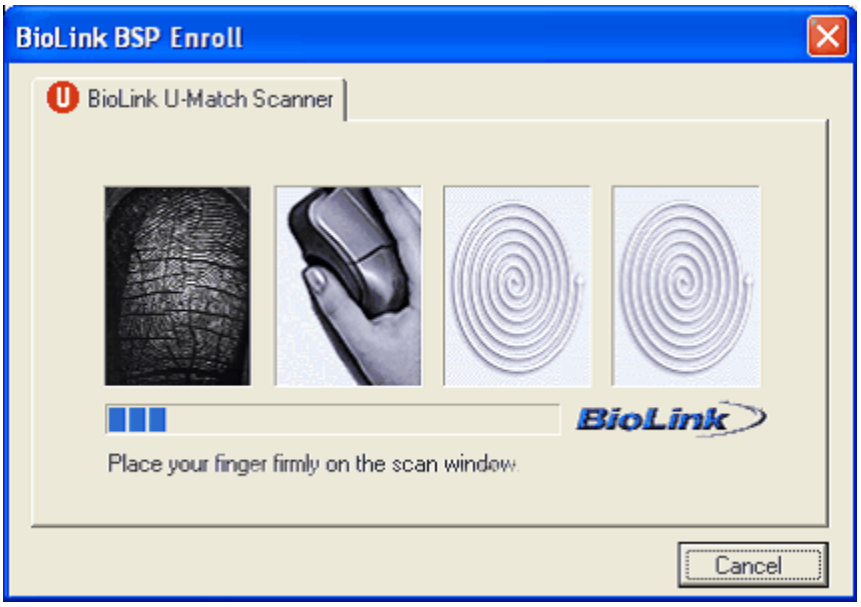
To add a BIO ID, follow these steps.
1. Right-click the icon in the system tray.



2. Choose **Change BIO ID** from the pop-up menu. A list of available biometric devices will appear.



3. Check **Enable Biometric ID verification** and choose the desired device from the list.
4. If a fingerprint scanner is chosen, ex: Bio-Link U-Match, you will be asked to press your finger against the scanner several times (Figure 20). When the necessary information is gathered, it will be saved to the Key Storage Device.



If you choose a voice recognition device, such as SAFLINK Scan-Soft Voice Verification, you will be asked to pronounce a key-phrase. As in the previous case, the biometric ID is stored on the Key Storage Device once it is collected.

8.10 Changing the BIO ID

To change the biometric ID assigned to the Key Storage Device (current identity), follow these steps:

1. Right-click the icon in the system tray.
2. Click **Change BIO ID.** The ***Change Biometric ID*** dialog will appear on the screen (see Adding a BIO ID to the Key Storage Device).
3. Choose your biometric device from the list.
4. As in the case of adding a BIO ID, depending on the biometric device you choose, you will be asked to perform a certain action (ex: pronounce a phrase, press your finger against the scanner, etc). When the process is done, the BIO ID is saved to the Key Storage Device.

Note. If you wish to disable biometric authentication, uncheck "Enable Biometric ID verification" in the Change Biometric ID window.

8.11 Changing the PIN Code

In order to change the PIN code of the current identity, do the following:

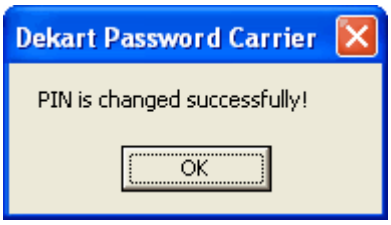
1. Right-click the icon in the system tray.
2. Choose **Change PIN** from the menu**.** The following window will appear on the screen.

3. Enter the new PIN code in the field, or leave it blank if you wish to disable the PIN-code. Then press **OK.**

   Note. The PIN-code can be 4 to 8 characters long.

4. You will then be asked to enter the PIN-code again. Press **OK** when you are done.

5. If the operation is successful, you will see this window:

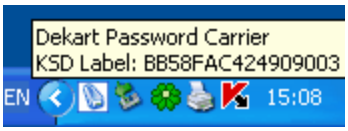


Note. The Key Storage Devices shipped by Dekart are not PIN-protected, you will be prompted to set a PIN when you launch the application for the first time.

8.12 Changing the label of a Key Storage Device

The label of a Key Storage Device can contain various information about itself or its owner. ***Note: this parameter can be used to rename the identity.***
To change it, follow these instructions:
1. Right-click the icon in the system tray.
2. Choose **Change Label.** The following window will appear:

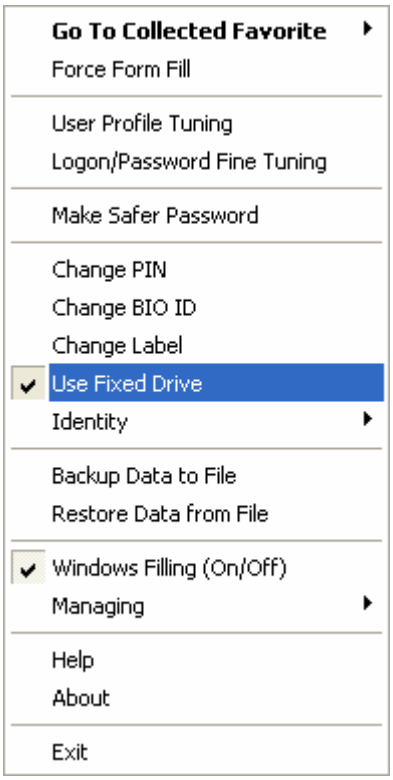
3. Enter the new label and press **OK**. If you wish to remove the label, leave the field blank. In this case the label will be changed to the serial number of the device.



Note. The label of the Key Storage Device cannot be longer than 32 characters.

8.13 Using a hard disk as Key Storage Device

If you want to use an encrypted file on the hard disk as Key Storage Device, do the following:
1. Right-click the icon in the system tray.
2. Choose **Use Fixed Drive** from the menu.



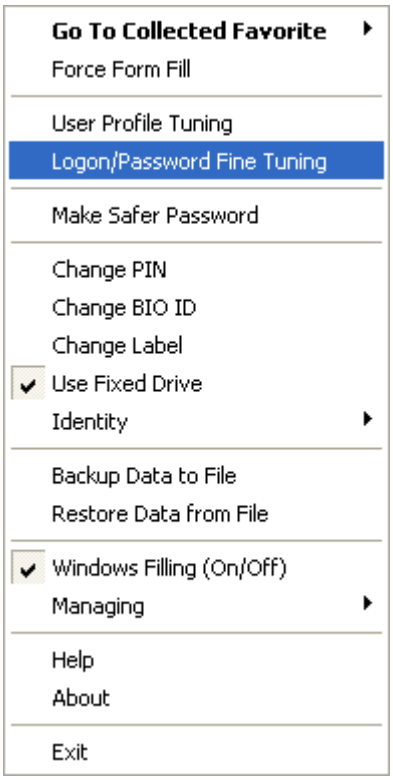
3. If you have previously used Password Carrier with a protected (with two- or three-factor authentication) removable Key Storage Device, you will be asked to go through the authentication procedure.
4. To disable the **Use Fixed Drive** option, uncheck it.

Note. When enabling *Use Fixed Drive*, you will start using a new Key Storage Device, thus Password Carrier will have to be "trained" again.

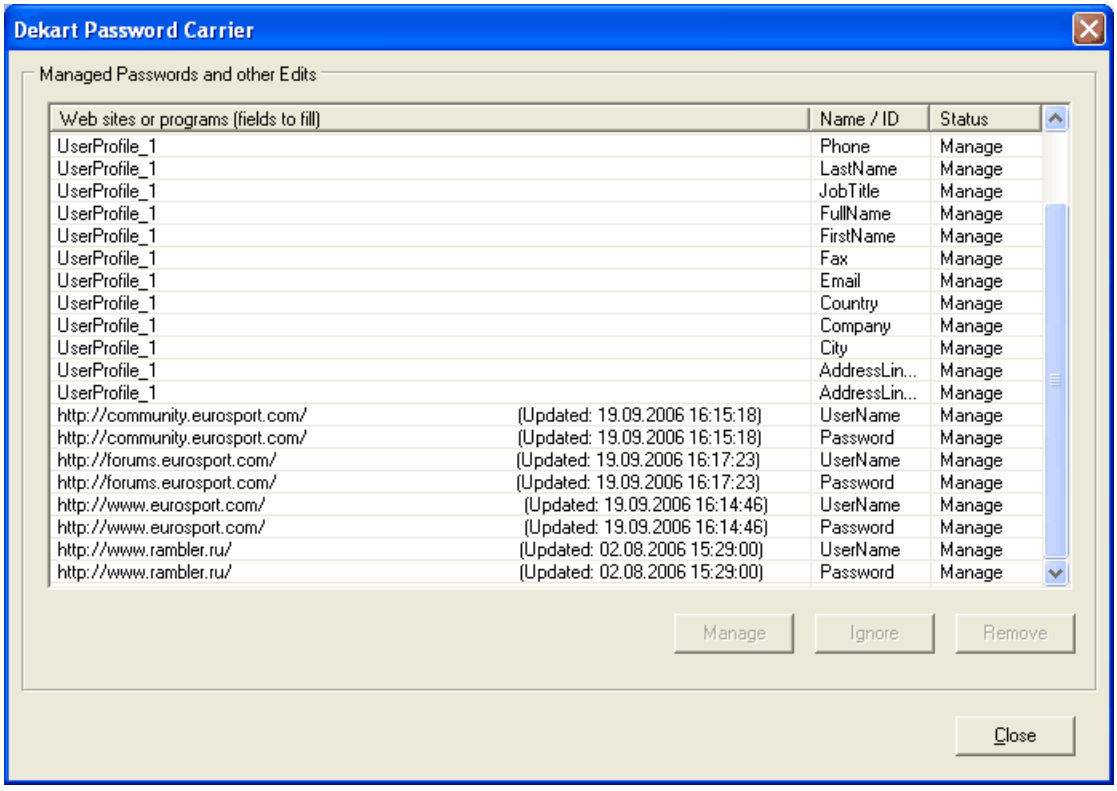
8.14 Dekart Password Carrier automation settings

Sometimes you might want to manually edit certain fields of a specific form, rather than let Dekart Password Carrier fill them in automatically. In these cases you can use Dekart Password Carrier's ability to change the status of a specific record: automatic – *Managed,* manual – *Ignored.*

To do that, follow these steps:
1. Right-click the icon in the system tray.



2. Click on **Logon/Password Fine Tuning**. A list of records stored on the Key Storage Device will appear – *Managed Passwords and other Edits.*



Each line contains the description of each record. The first column (*Web sites or programs*) holds the URL of a web-page, or the full path and the name of an application. The second column (*Type*) – the type of the field (Edit, text, password); the third one (*Name/ID*) – the identifier of the field. The last column *(Status)* contains the status of the field (*Managed, Ignored*).

3. Click a line from the table.
4. Press either **Ignore** (if you want to edit the field manually) or **Manage** (if you want it to be filled automatically),

Note 1. By default, all the records stored on the Key Storage Device have the Managed status.

Note 2. Dekart Password Carrier allows you to apply a setting to a group of records. Choose the needed entries by holding Shift (if you wish to choose multiple consecutive items), or Control (if you wish to choose individual items).

Note 3. The UserName field contains the user ID (name, login, SSN, card holder number, etc.).

See also Managing Collected Favorites.

8.15 Working with the contents of a Key Storage Device

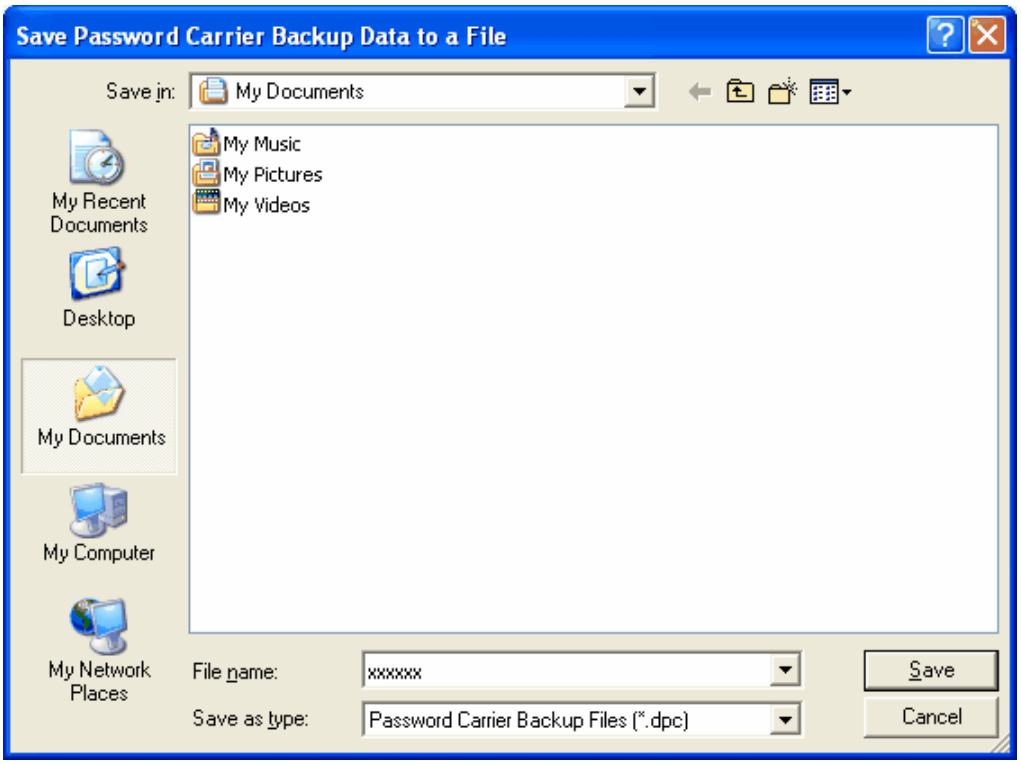
The following operations can be performed with the contents of the Key Storage Device:

1. Create a backup copy of the Key Storage Device (see Creating a backup-copy of a Key Storage Device).
2. Restore the data from a backup copy (see Restoring the data from a backup-copy).
3. Sort the records stored on the Key Storage Device.
4. Erase the unused records.
5. Editing the Login and Password values

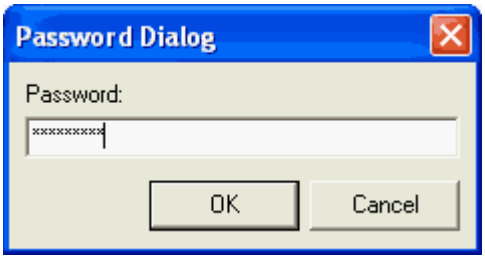
8.16 Creating a backup-copy of a Key Storage Device

To avoid accidental data loss, we recommend you to create backup copies of your Key Storage Device at regular time intervals:

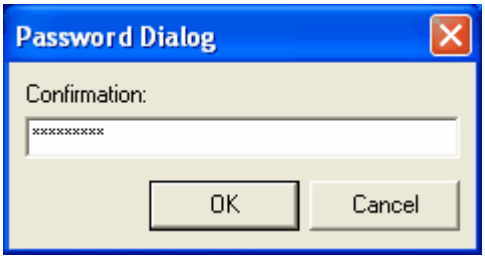
1. Right-click the icon in the system tray.
2. Choose **Backup Data to File** from the menu**.** You will be asked to choose the location and the name of the backup file via the ***Save Password Carrier Backup Data to file*** dialog.



3. Once the location of the file and its name are set (the default file extension is *.DPM, but you can use other extensions too) press **Save.** You will then be asked to enter a password.



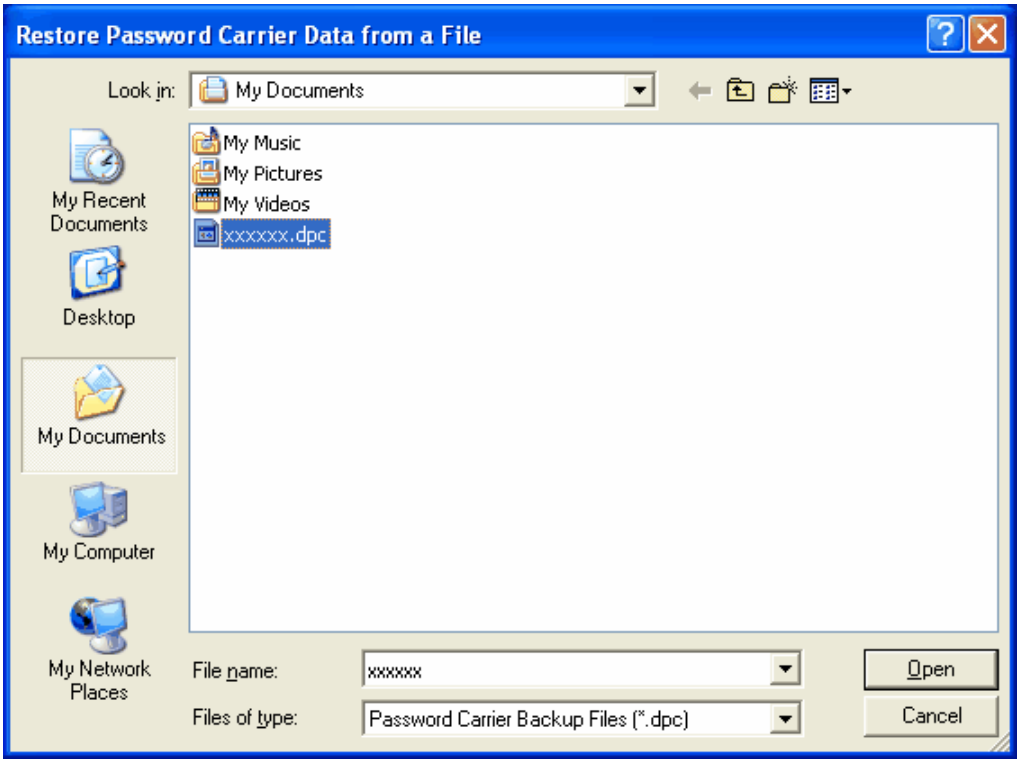
4. A password confirmation dialog will appear.



After the confirmation is complete, the data will be copied to the chosen file.

8.17 Restoring the data from a backup-copy

Follow these steps if you wish to restore your records from a backup copy:
1. Right-click the icon in the system tray.
2. Press **Restore Data from file.** The ***Restore Password Carrier Data from file*** window will appear.



3. Choose the backup file and press **Open**. The program will warn you that the contents of the Key Storage Device (current identity) will be replaced with the data from the backup file.
4. After confirming the operation (by pressing **OK**), you will be asked to enter the password that protects the backup file.

Note: This operation will overwrite the contents of the Key Storage Device (current identity) with the data from the file.

Note: When restoring data from a backup, the name of the backup file will be the Label of the Key Storage Device.

8.18 Removing unused records from a Key Storage Device

If you want to remove unused or old records from your Key Storage Device, follow these steps:
1. Right-click the icon in the system tray.
2. Press **Logon/Password Fine Tuning**. A window that displays the contents of the Key Storage Device will show up – *Managed Passwords and other Edits.* (see Dekart Password Carrier automating setting).
3. Click on the record in the list (i.e. a line in the table).
4. Press the **Remove** button.
5. You can also right-click an entry, and press **Remove** in the context menu.

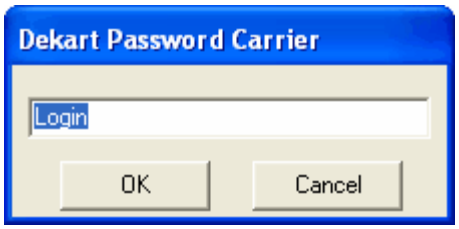
See also Managing Collected Favorites.

8.19 Sorting the list

The records contained within the Key Storage Device can be sorted in several ways:
1. Right-click the icon in the system tray.
1. Press **Logon/Password Fine Tuning**. A window that displays the contents of the Key Storage Device will show up – *Managed Passwords and other Edits.* (see Dekart Password Carrier Automating setting).
2. Click on one of the table's column headers (*Web sites or programs, Name/ID, Status*), to choose the criterion by which the records will be sorted in alphabetical order. If you click on the header again, the order will switch to reversed-alphabetical.

8.20 Editing the Login and Password values

The records (Name and Password) contained within the Key Storage Device can be edited in several ways:
1. Right-click the icon in the system tray.
2. Press **Logon/Password Fine Tuning**. A window that displays the contents of the Key Storage Device will show up – *Managed Passwords and other Edits.* (see Dekart Password Carrier Automating setting).
3. Select a *UserName* or a *Password* entry.
4. You can right-click an entry, and press **Edit** in the context menu.
5. A window which displays the password (or UserName) in plain-text will show up. You can update the password and press **OK** to confirm the change, while pressing **Cancel** will discard the changes you made.



Note 1. The UserName field contains the user ID (name, login, SSN, card holder number, etc.).

Note 2. Be careful when changing a UserName or a Password, otherwise you may be unable to access the resources that used your old credentials.

8.21 Setting the Managing mode

Password Carrier provides three modes of operation: Managing on – in this case the program will collect new passwords and fill them in web-forms and Windows applications; new data that are entered in a field will overwrite the older data assigned to that field. Managing off – this will disable form filling and new data will not be collected. Fill only – Password Carrier will fill the forms with data, but it will not collect new data.

To choose one of the modes:
1. Right-click the icon in the system tray.
2. Press **Managing**.

3. Choose one of these - On, Off, Fill only

8.22 Enabling/Disabling Windows applications form filling

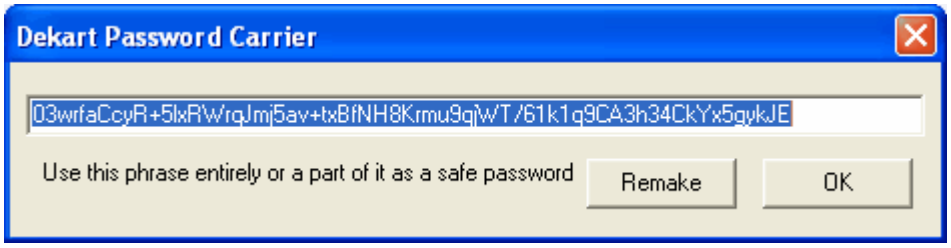
If you decide to temporarily disable the Managing mode only for Windows applications (i.e. you don't want Dekart Password Carrier to collect data and passwords automatically), follow these steps:

1. Right-click the icon in the system tray.
2. Press **Windows Filling (On/Off).**
3. To revert to the previous setting, press **Windows Filling (On/Off)** again**.**

8.23 Generating a strong password

The built-in password generation tool is an efficient way to enhance your privacy. The generated passwords can be used during various registration procedures, or in applications that require authentication.

1. Right-click the icon in the system tray.
2. Click **Make Safer Password.** A window such as this one will appear on the screen.

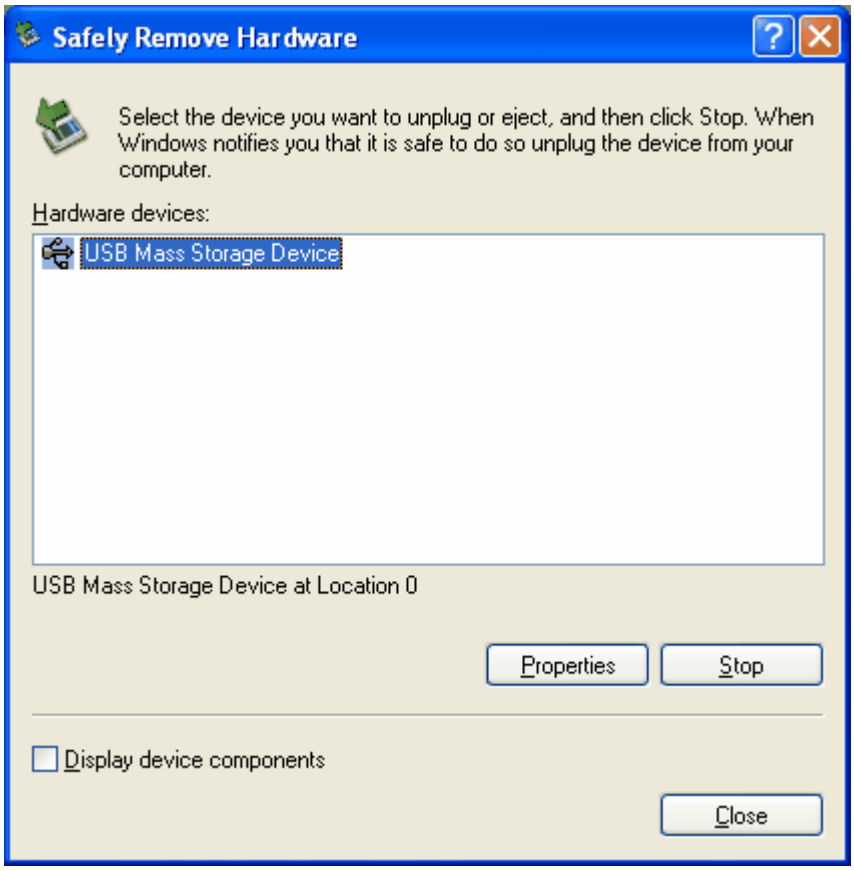


3. If you press the **Remake** button again, a new password will be generated.
4. Afterwards, you can copy the new password (or a part of it) to the clipboard and paste it into the needed field.

8.24 Exiting Dekart Password Carrier

To quit **Dekart Password Carrier**:

- Right-click the icon in the system tray.
- Press **Exit and eject**, if you wish to safely remove the flash disk after quitting **Dekart Password Carrier.** The **Safely Remove Hardware** dialog will be shown.



- Press **Exit**, if you wish to use the flash disk after quitting **Dekart Password Carrier.**

Note. If Password Carrier was started from a removable Key Storage Device, or uses one to store your personal data, you can close the program in two different ways – **Exit**, and **Exit and eject**.
If Password Carrier was started from the hard disk and uses one to store your personal data, only one option will be available – **Exit**.

9 Best practices

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

Tip#1. Enable PIN-code protection for your Key Storage Device. This will solve two problems: others won't be able to use your credentials without knowing the PIN; in addition, Password Carrier will automatically deactivate itself if the computer is left unattended, the PIN is required to continue using the program.

Tip#2. Create backup copies of the data located on the Key Storage Device at a regular interval. This will allow you to restore your data in case the Key Storage Device is lost or corrupted (see Creating a backup-copy of a Key Storage Device and Restoring the data from a backup-copy).

10 Additional information

10.1 Biometric authentication in Dekart Password Carrier

If three-factor authentication is enabled (**Enable Biometric ID verification** is checked in the **Change Biometric ID** window), the biometric authentication will be initiated after you launch **Dekart Password Carrier** (and provide a valid PIN for the **Key Storage Device,** if you have enabled the PIN protection) **.** The software will ask you to provide your biometric data (scan the fingerprints, pronounce the authentication phrase etc.). In case the provided BIO ID does not match the one stored on the Key Storage Device, you will be asked to repeat the biometric authentication. The authentication routine is successful only when the data you provide are identical to the biometric ID stored on the Key Storage Device. Biometric authentication guarantees that even if the Key Storage Device is lost or stolen, an unauthorized user will not get access to your data.

10.2 How to copy the secret data from one Key Storage Device to another

To migrate your personal data from one Key Storage Device to another, follow these steps:

1. Backup your Key Storage Device.
2. Close the program.
3. Choose your next step from the table below.

Where is Password Carrier located?	Where are your data stored?	Actions
On a removable drive	On a removable drive	1. Install Password Carrier to a new Key Storage Device. 2. Start Password Carrier. 3. Restore the personal data from a backup.
On a removable drive	On the hard disk	1. Install Password Carrier to a new Key Storage Device. ***Note.*** If the program is already installed on a Key Storage Device, you can skip this step. 2. Start Password Carrier. 3. Enable Use Fixed Drive. 4. Restore the personal data from a backup.
On the hard disk	On a removable drive	1. Start Password Carrier from the hard disk. 2. Disable Use Fixed Drive. 3. Restore the personal data from a backup.
On the hard disk	On the hard disk	1. Start Password Carrier from the hard disk. 2. Enable Use Fixed Drive. 3. Restore the personal data from a backup.

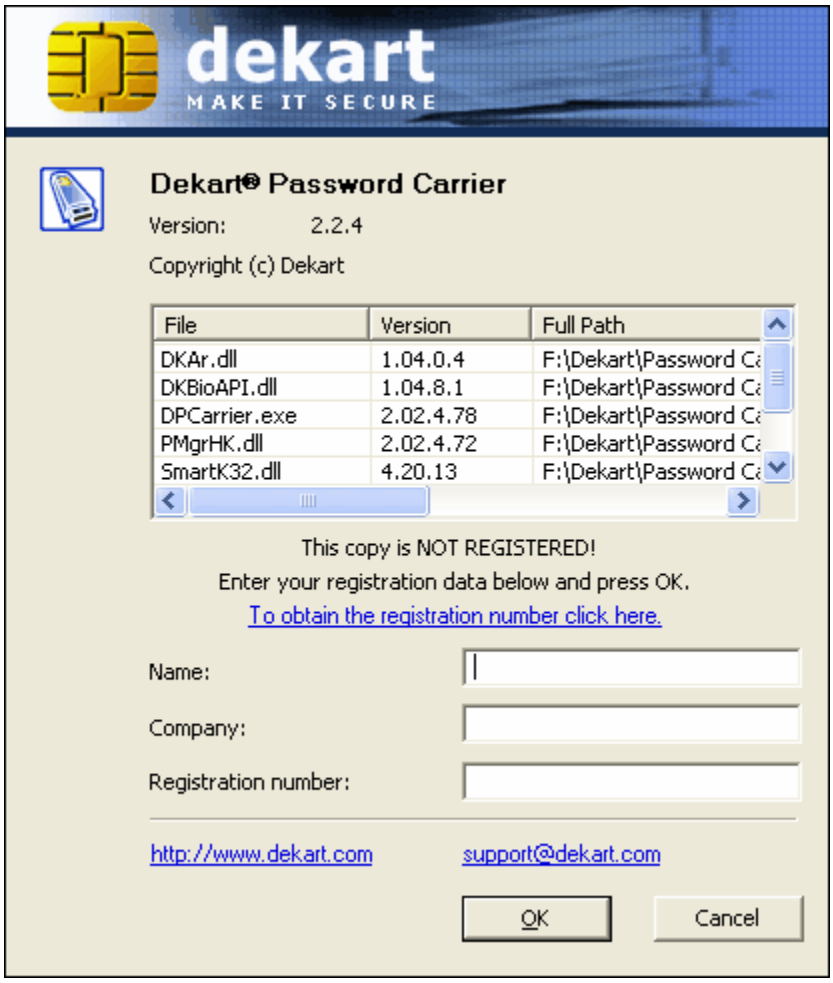
Note. If you previously enabled (and configured) multifactor authentication, you will be asked to go through the two- or three-factor authentication process.

10.3 Viewing information about Dekart Password Carrier

In order to view information about the application, click **About** in the pop-up menu**.** A new window will appear on the screen (*About Dekart Password Carrier*).
Note. If your copy of Dekart Password Carrier is not registered, then the window will look like the one in Registering Dekart Password Carrier.

10.4 Registering Dekart Password Carrier

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



If you use a trial version of the program, please, use the Dekart *Buy on-line* page to purchase a registration number. After your transaction is processed, you will receive an email with the registration number.
If you use a licensed version of the program, you can obtain a registration number at the *Software Registration (Register)* page at **www.dekart.com**.

10.5 Troubleshooting

10.5.1 Form filling troubleshooting

Some problems might be encountered during the process of automatic form-filling, in the following cases:

1. If IFRAME elements were used during the development of the page. Internet Explorer prohibits the processing of such elements' content due to security reasons, therefore Dekart Password Carrier cannot handle such forms.

2. Some web-designers choose to fill in the fields of the forms with default values. When you visit such a site, Dekart Password Carrier will memorize the default values and will use them in the future. There are two ways to avoid that: you can either update the value of the field (by entering a new one, or clearing the old one) and press the **Apply** (**Next**, **Submit**, etc.) button; or you can change the status of

a specific field from Managed to Ignored.

10.5.2 Error messages

Message	Cause	Solution
ATTENTION! Bad a PIN code was entered!	An incorrect PIN-code was entered.	Enter the PIN-code again.
Confirm PIN mismatch	When changing the PIN-code, the original code did not match the one you entered in the confirmation dialog.	Repeat the procedure, make sure that the original PIN-code is identical to the one you enter the second time.
The PIN should be at least 4 symbols long	The length of the PIN-code is below 4 characters.	Repeat the procedure, entering a code which is 4 to 8 characters long.
An error occurred while working with the KSD	An error occurred when the program tried to read\write from\to the Key Storage Device	Try the procedure again. If it still fails, try reconnecting the Key Storage Device. If this fails too, contact support.
Error writing data to Key Storage Device (Not enough free space on KSD)	An error occurred while writing data to the Key Storage Device. Usually this is caused by the lack of free space on the device.	Free up some space on the Key Storage Device.
Biometric verification failed!	The provided BIO ID did not match the one stored on the Key Storage Device.	Perform the biometric authentication again.
Error when opening the Backup file	An error occurred while opening the backup file. Perhaps it is corrupt, or it is being used by another application.	Make sure that the file is not used by a different application. If you have reasons to believe it is corrupt, try to repair it with specialized software (ex: Windows CheckDisk etc.)
Error: Backup file not found	The backup file was not found.	Make sure the path to the file is correct, and that its name is written right.
Removable device not found. Enable at list one and try again.	No removable devices were found in your system.	Connect the Key Storage Device to your computer and retry the operation.

Note. If you encounter other error messages, contact support@dekart.com
Please read this page first http://www.dekart.com/support/howto/howto-contact-us/.

Index

- A -

- B -

- C -

- D -

- E -

- F -

- G -

- I -

- K -

- L -

- M -

- O -

- P -

- R -

- S -

- T -

- U -

- W -