

APPROVED

DEKART[®] TLogon[™]

User's Guide

Pages: 17

2003

Notice

The present document is a general user guide for DEKART Terminal Logon product, containing all reference material necessary to work with the product.

Contents

1	<i>Technical terms and Acronyms (Glossary of terms)</i>	4
2	<i>Scope</i>	5
3	<i>General description</i>	5
3.1	Security Principles of Dekart TLogon	5
3.2	Features of Dekart TLogon	5
3.3	Product components	5
3.4	System requirements	6
4	<i>Installation routines for Dekart TLogon</i>	7
5	<i>Updating Dekart TLogon</i>	10
6	<i>Uninstalling Dekart TLogon</i>	12
7	<i>Working with Dekart TLogon</i>	12
7.1	Terminal software choice	13
7.2	Logging in to Unix/Linux	13
7.3	Accessing information about Dekart TLogon	15
	<i>Attachment</i>	16
	Device characteristics of KSD (PIN-codes, memory size)	16

1 Technical terms and Acronyms (Glossary of terms)

Dekart Terminal Logon (TLogon) – product name.

KSD (Key Storage Device) – device to securely store important data (personal data to logon and work in UNIX/Linux OS). Both smart card and USB Token are Key Storage Devices. You can either protect your KSD by a PIN code or use it without a PIN code.

PIN (Personal Identification Number) – personal identification number to access KSD. A PIN must be 4 to 8 characters in length and must be kept secret by the KSD owner.

Telnet – the Internet standard protocol for remote login. Runs on top of TCP/IP. Unix BSD networking software includes a program, telnet, which uses the protocol and acts as a terminal emulator for the remote login session.

SSH (secure shell) - the Internet protocol that allows a user to connect to a remote host via an encrypted link. As against Telnet provides authentication of the server and of the user, confidentiality and information integrity.

2 Scope

Dekart TLogon is intended to establish secure connection to remote host (Unix/Linux OS) via SSH protocol

3 General description

Dekart TLogon is a software-hardware solution, allowing remote user to securely access Unix/Linux operating system and its resources, using hardware-enhanced authentication solution and SSH protocol.

3.1 Security Principles of Dekart TLogon

1. Security of Dekart TLogon is provided by use of KSD device (PIN code protected), storing login and password pair to access Unix/Linux operating system. Therefore, user is not required to remember his login/password pair.
2. To access a remote system the user has only to connect the KSD to the computer, enter correct PIN code and choose necessary remote system from the list of available systems.
3. KSD will block upon multiple wrong PIN code entries. *Note. Different KSDs have different error counters, allowing from 3 to 10 attempts to enter the wrong PIN code before blocking the KSD (see attachment).*

3.2 Features of Dekart TLogon

1. Convenient for end-user - no need to remember and re-enter complicated passwords.
2. Mobility – login/password pair is stored on KSD, therefore, to access a network from another workstation the only thing to do is to connect the KSD to the computer and provide correct PIN code.
3. Compatibility – KSD may be used not only with Tlogon, but other applications like Dekart Logon and Dekart Private Disk.

3.3 Product components

The Tlogon package contains the software itself, a KSD enabling you to securely access the Unix/Linux operating system, the present User's Guide and Quick Start Card (QSC).

You can choose one of the following key storage devices offered by different vendors:

- Aladdin eToken PRO;
- Aladdin eToken R2;
- Schlumberger Multiflex;
- Schlumberger Cryptoflex;
- Schlumberger Payflex;
- Rainbow iKey 1000;
- Rainbow iKey 2000;
- Rainbow iKey 2032;
- Rainbow iKey 3000;

- Eutron CryptoIdentity ITSEC;
- Eutron CryptoIdentity 4;
- Eutron CryptoIdentity 5;
- Datakey Model 310;
- Datakey Model 330;
- GemPlus GPK.

Note 1. Device characteristics of some KSDs are described in an attachment to this guide.

Note 2. Dekart delivers KSDs without a PIN Code.

3.4 System requirements

Hardware requirements

- PC with at least one port available to connect KSD (COM, USB, etc.) \
- In the event that a smart card is used as a KSD, a PC/SC compatible smart card reader is required.

Software requirements

- Operating system: Windows 98, NT4.0, 2000, ME, XP.
- Telnet terminal software.
- KSD drivers.

Note. Before you start work, refer to the Administrator's Guide of a corresponding system to create a user account in Unix/Linux OS, allow remote users to establish connections via SSH protocol and generate user keys.

Attention!

For detailed information concerning SSH protocol (settings and features etc.) visit the <http://www.freessh.org/> site.

4 Installation routines for Dekart TLogon

1. Close all open applications before installing Dekart TLogon.
2. Run the setup program TLogon.exe.
3. If all the given conditions are satisfied the Dekart TLogon welcome screen appears. Click the **Next** button on the welcome screen.



Figure 1

4. At this stage you are required to enter your personal information and product serial number.
5. After you have entered all necessary information the Dekart license agreement appears. You must accept the license agreement before you can proceed with installation.



Figure 2

6. Please, choose the folder you want to install Dekart TLogon into.

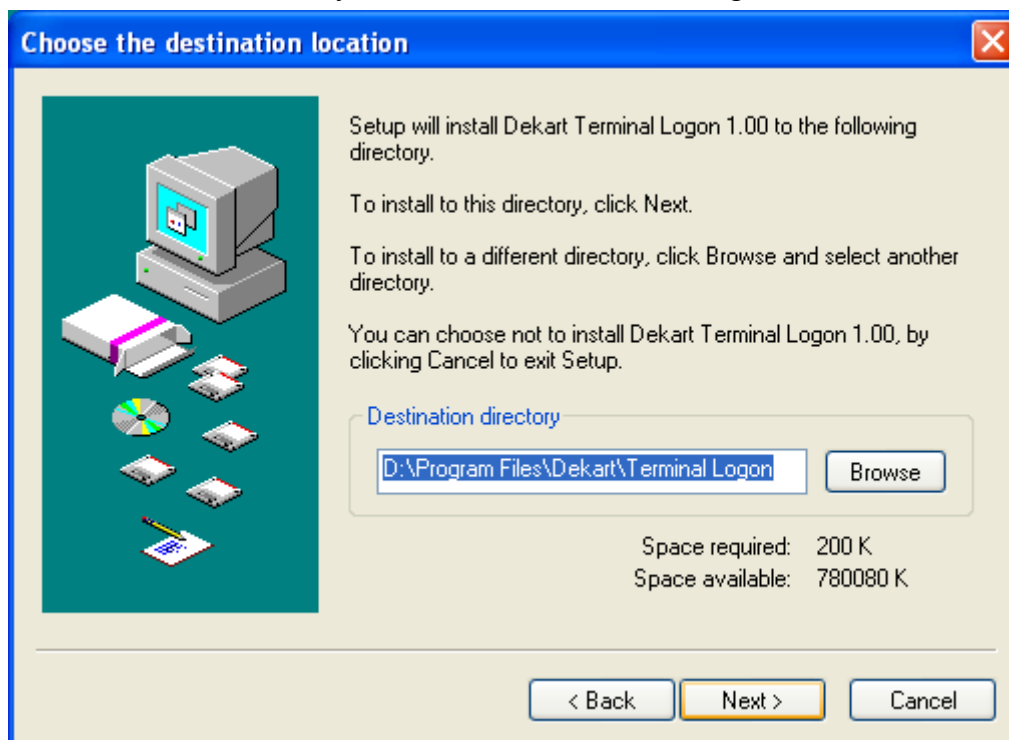


Figure 3

7. Please, select a folder or create a new one in **Start Menu** to install the Dekart TLogon software.

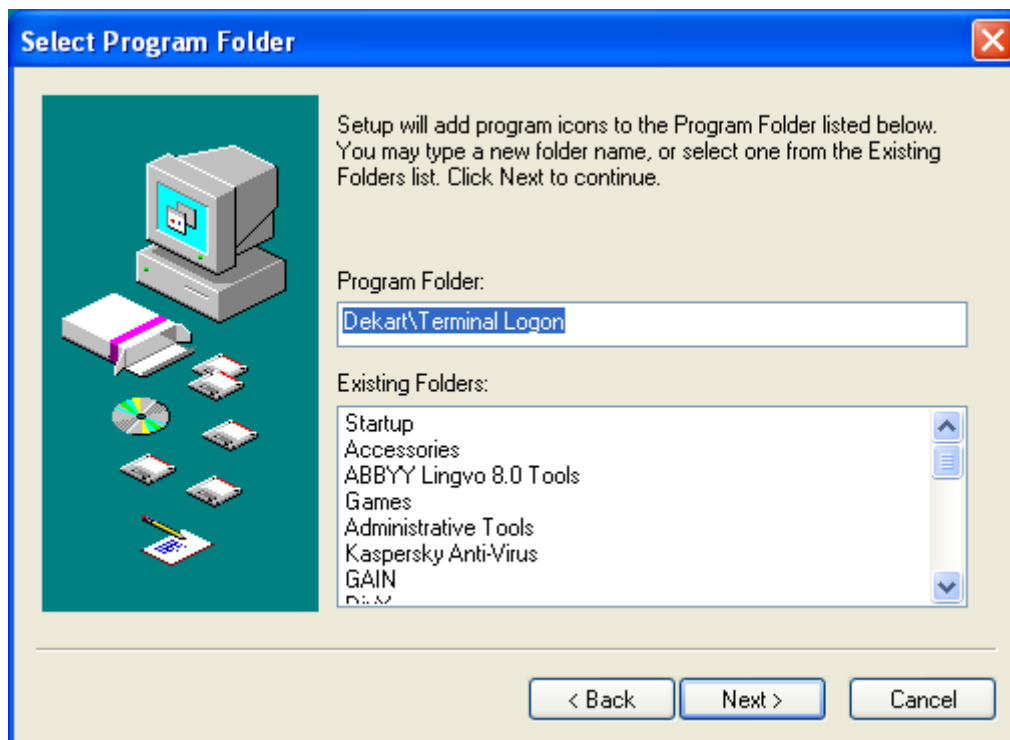


Figure 4

8. Click the **Finish** button to terminate the installation.

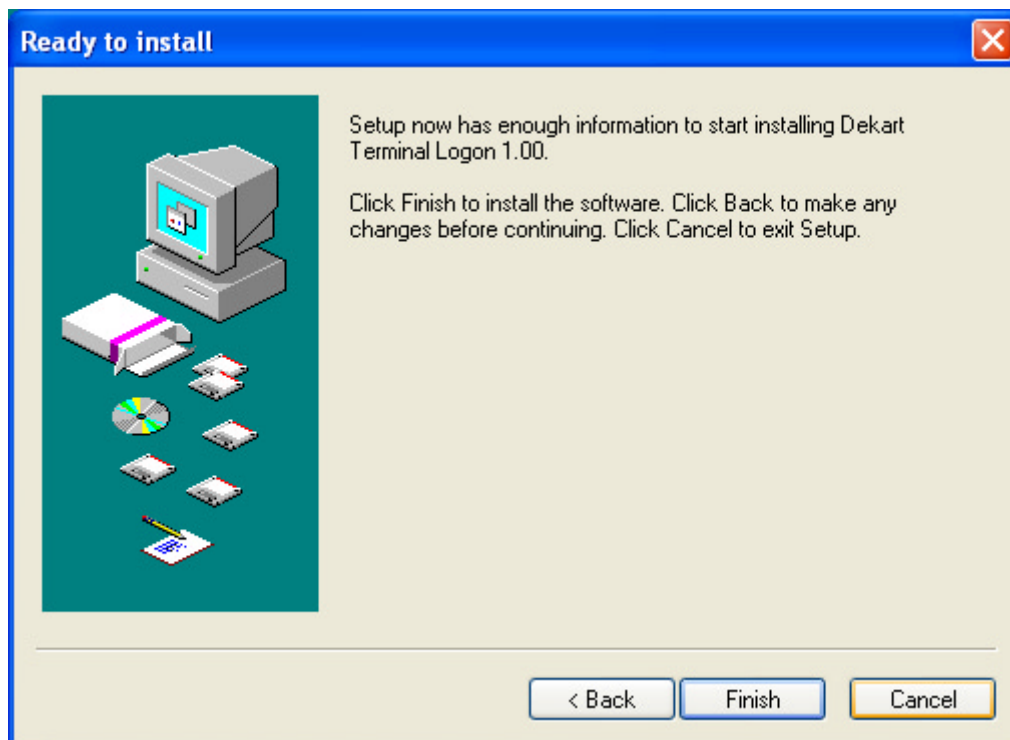


Figure 5

After the program has copied all necessary files into the program directory, the installation is complete.

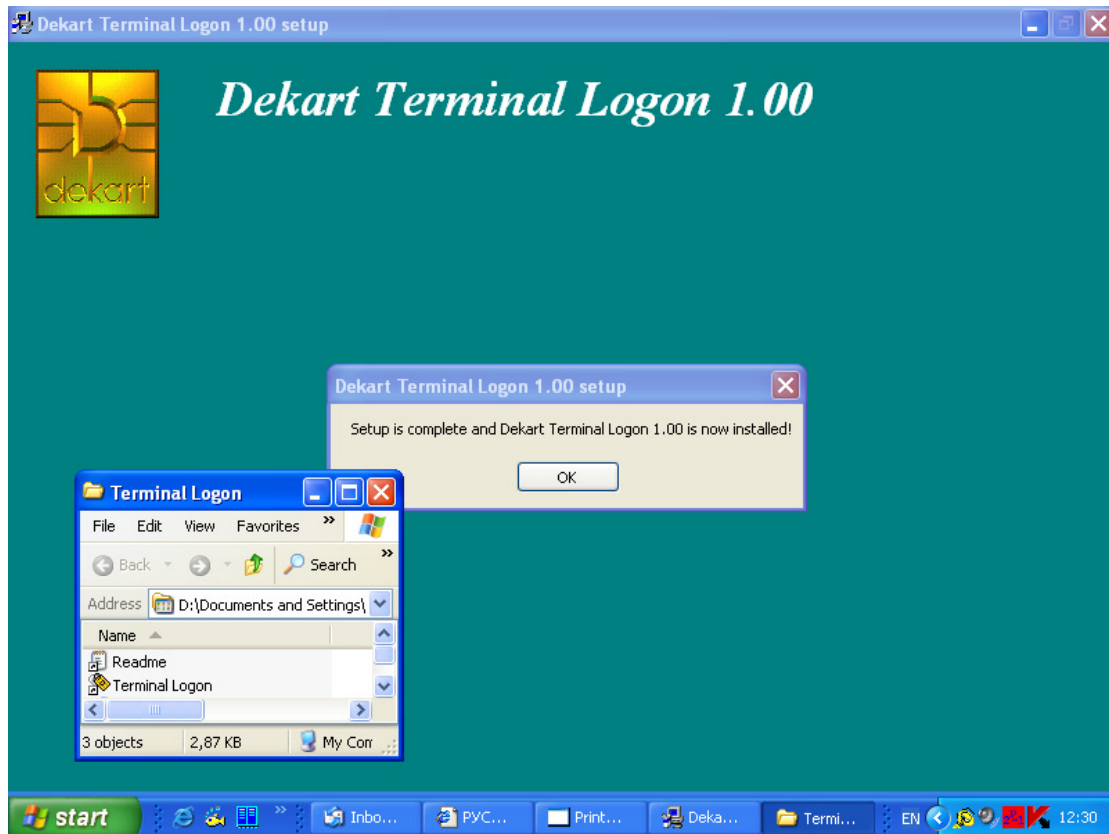


Figure 6

Note. After the installation of Dekart TLogon for Unix/Linux is complete you will have to restart your computer.

5 Updating Dekart TLogon

1. The next time you run the installation program, it automatically determines the version of the Dekart TLogon on your computer and collects all necessary system information.

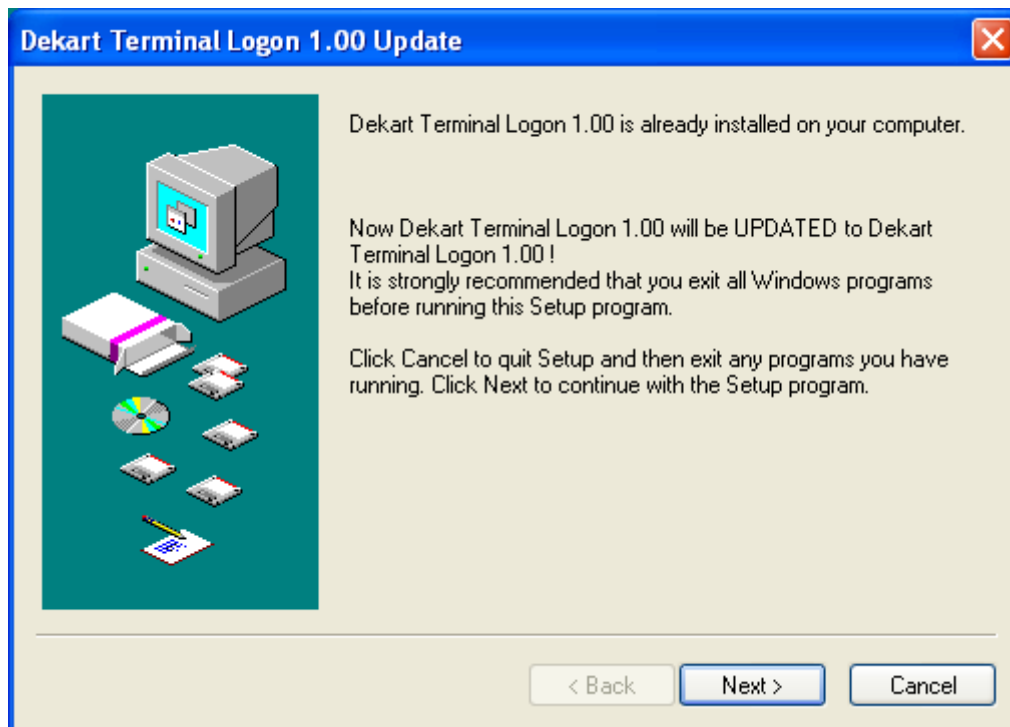


Figure 7

2. Click the **Next** button to view the license agreement. You must accept the license agreement before you can proceed to upgrade.
3. Click the **Finish** button to terminate the update process.

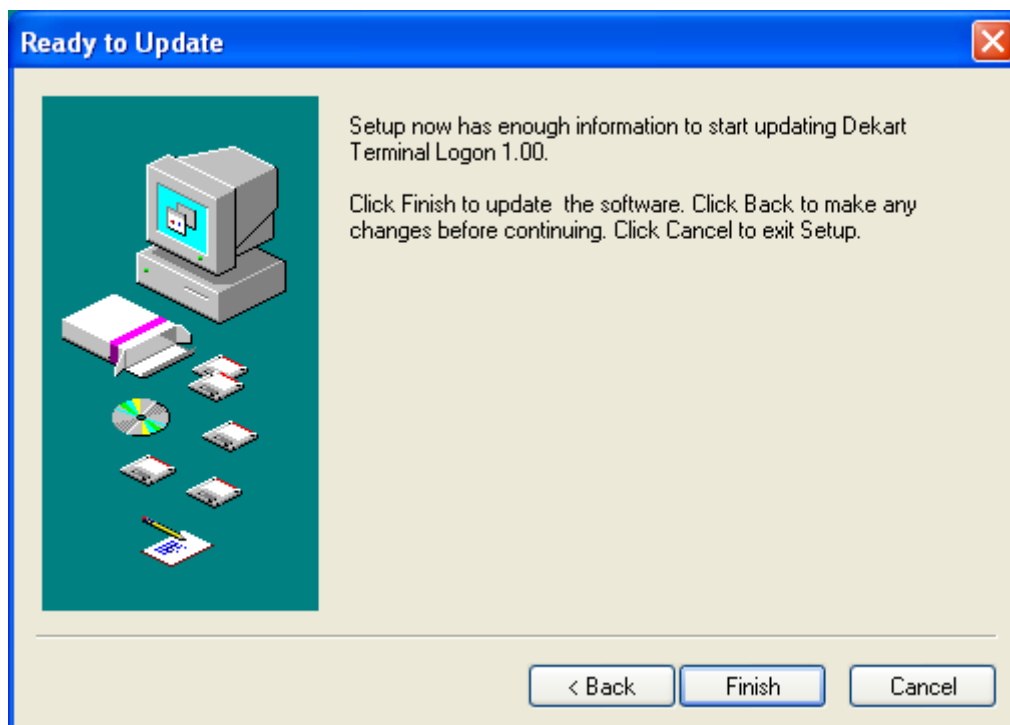


Figure 8

The program overwrites all files, or installs updated files if the newer program version is being installed.

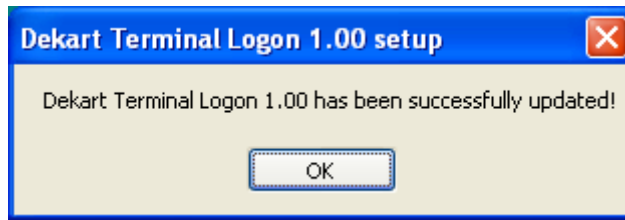


Figure 9

Note. After the update of Dekart TLogon is complete you will have to restart your computer.

6 Uninstalling Dekart TLogon

To uninstall the program, please, follow these steps:

1. Select **Programs** menu in **Start Menu**, locate the folder you have entered in step 7 when installing the program (see p.4), 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).

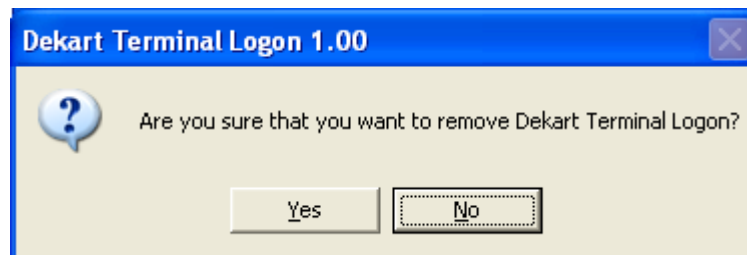


Figure 10

Please, confirm the uninstall of Dekart TLogon by clicking the **Yes** button.

2. After successful execution of the uninstall process the following message will appear:

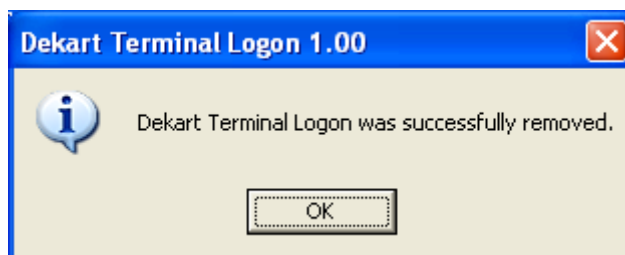


Figure 11

7 Working with Dekart TLogon

The work with **Dekart TLogon** can be divided in two stages. During the first stage (preliminary stage) the KSD should be set up to work as well as serviced and maintained during operation (see. documentation for Dekart KeyManager). During the second stage the Dekart Tlogon provides user authentication in Unix/Linux operating system, thus ensuring all necessary security and reliability.

7.1 Terminal software choice

Once the Dekart TLogon for Unix/Linux is successfully installed, a string in tlogon.ini configuration file should be modified to contain a complete path to the terminal program. E.g.: telnet=c:\program files\netterm\netterm.exe, in the event that you use the Netterm program.

7.2 Logging in to Unix/Linux

Dekart TLogon interacts with standard authentication system of the operating system, using SSH protocol to transmit user login/password pair stored in KSD when starting a session.

- Run the program as following: select **Programs** in the **Start Menu** and locate the program directory (see step 7, p.4).

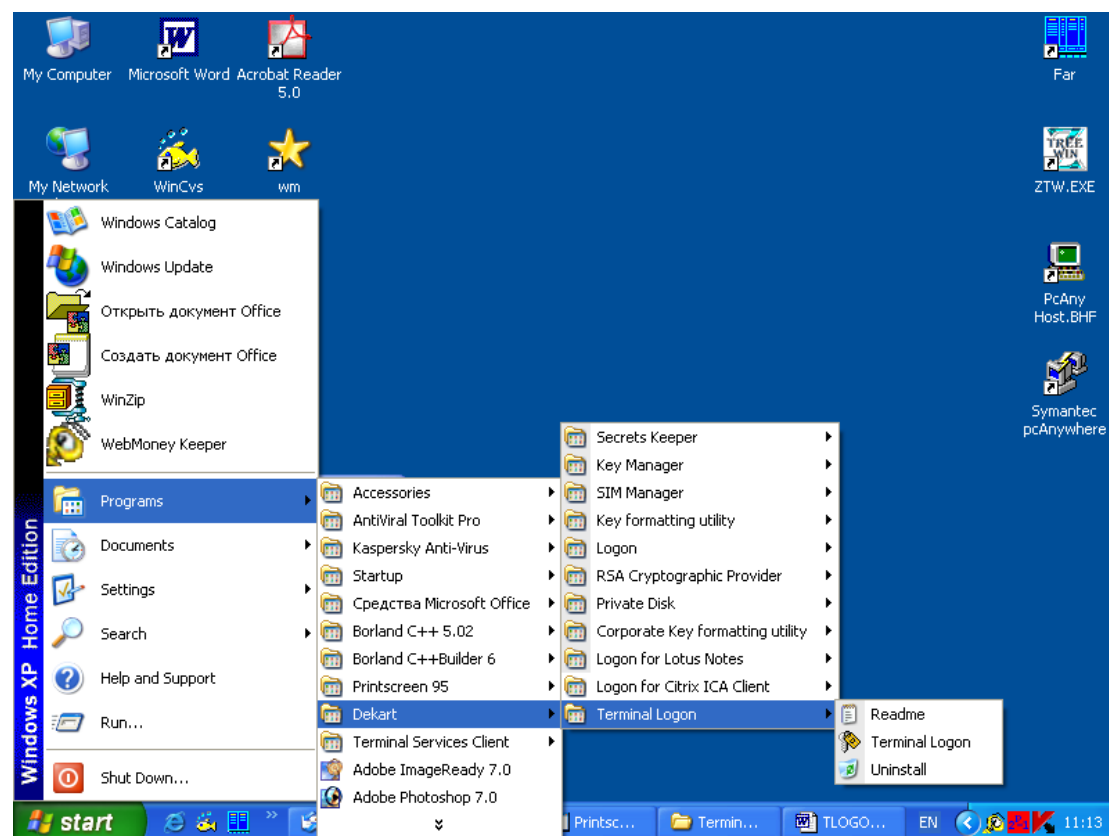


Figure 12

- After TLogon has been launched (provided that KSD is already connected to the computer) a dialog window will appear.

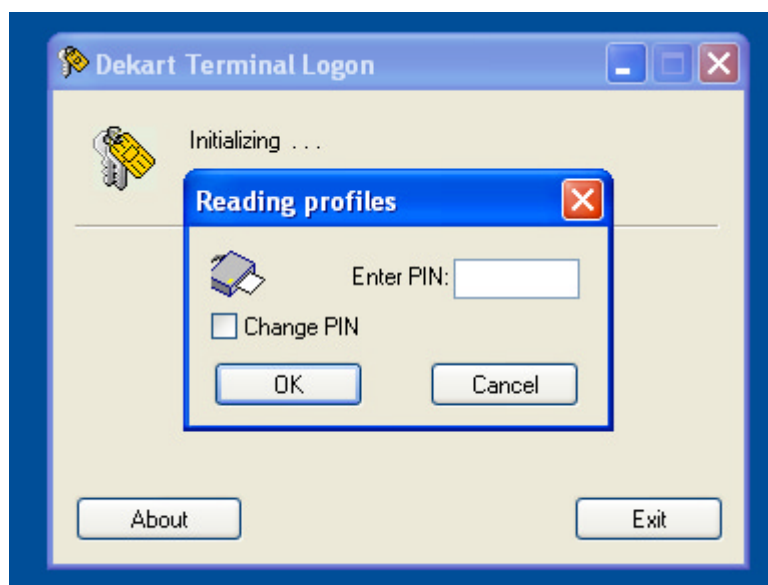


Figure 13

- Enter the PIN code (if requested) and press the **OK** button.

Attention! KSD will block upon multiple wrong PIN code entries. Please, be careful.

- After the PIN code has been successfully verified, select the remote system and press the **Connect** button.

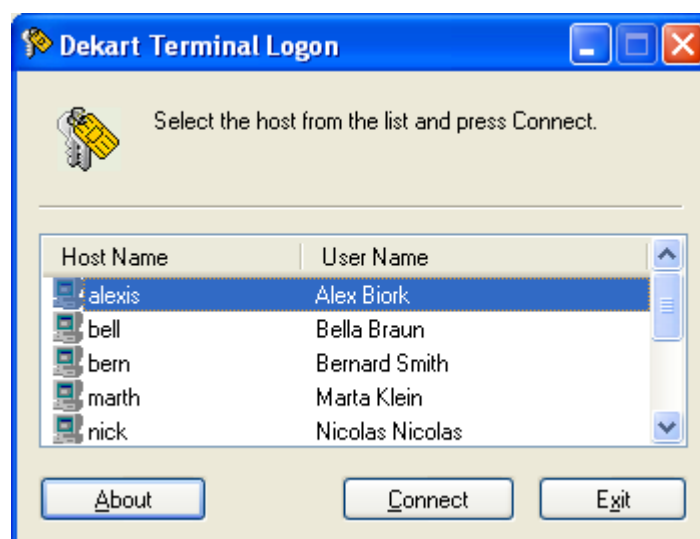


Figure 14

- After establishing SSH connection with a remote host, the login/password pair stored in the KSD is transmitted, and terminal window appears.

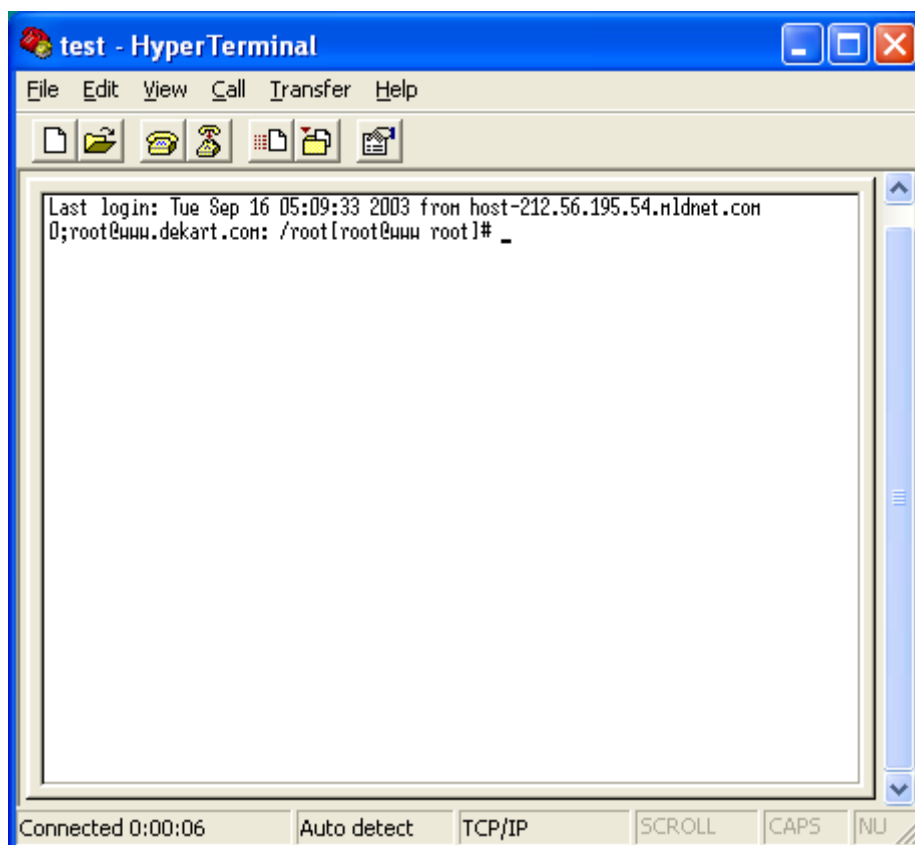


Рисунок 15

7.3 Accessing information about Dekart TLogon

Click the **About** button to get the information about the product. The *About Dekart TLogon* window will appear.



Figure 16

Attachment

Device characteristics of KSD (PIN-codes, memory size)

Table 1

KSD name	PIN-code for applications/ device	Allowed wrong PIN code entries	Allowed attempts to unblock KSD	Memory size (kB)
Aladdin eToken PRO	PIN-code for applications	3	3	16, 32, 64
Aladdin eToken R2	PIN-code for device	∞	-	16, 32, 64
Schlumberger Multiflex	PIN-code for applications	3	3	4, 8
Schlumberger Cryptoflex	PIN-code for applications	3	3	8, 16
Schlumberger Payflex	PIN-code for applications	3	3	4
Rainbow iKey 1000	PIN-code for device	3	3	8, 32
Rainbow iKey 2000	PIN-code for device	10	0	8, 32
Rainbow iKey 2032	PIN-code for device	10	0	8, 32
Rainbow iKey 3000	PIN-code for applications	3	3	32
Eutron CryptoIdentity ITSEC	PIN-code for applications	3	3	32
Eutron CryptoIdentity 4	PIN-code for applications	3	3	8
Eutron CryptoIdentity 5	PIN-code for applications	3	3	32, 64
Datakey Model 310	PIN-code for device	10	0	8, 32
Datakey Model 330	PIN-code for device	10	0	8, 32
GemPlus GPK	PIN-code for applications	3	3	2, 4, 8, 16
ruToken	PIN-code for device	3	12	8, 16, 128

Note 1. Key storage device can have one PIN-code for all Dekart applications, and another PIN code for other applications, or a single PIN code for the device.

Note 2. Most KSDs allow a limited number of consecutive wrong PIN code entries. When this number is reached the KSD blocks. A correct PIN code should be entered while unblocking the KSD, and then the KSD will function properly. In the event that a wrong PIN code is entered while unblocking the KSD, the KSD will automatically block permanently.