USER GUIDE

DEKART LOGON FOR CITRIX ICA CLIENT

Table of Contents

Part I

1 License and trademarks information

COPYRIGHT

DISCLAMER

Dekart SRL makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Dekart SRL 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 SRL makes no representations or warranties with respect to any Dekart Logon for Citrix ICA Client software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Dekart SRL reserved the right to make changes to any and all parts of Dekart Logon for Citrix ICA Client 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.1ST, 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 SRL TRADEMARK ATTRIBUTIONS

Dekart Logon for Citrix ICA Client is a trademark of Dekart SRL
All other registered and unregistered trademarks in this document are the sole property of their respective owners.

DEKART SRL CONTACT INFORMATION

E-mail:

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

Part II

2 Glossary

Dekart Logon for Citrix ICA Client (DLCIC) – name of the product.

ICA-connection (Citrix ICA connection) – personal data required to access a Citrix server (address, domain, password, etc.).

KSD (Key Storage Device) – A device where personal information is stored (data necessary to access and work with a Citrix server). A KSD can be either a smart card or a USB token. The KSD can be secured with a PIN code, or can work without PIN.

PIN (Personal Identification Number) – A personal identification number that is used to access information stored on the KSD. The PIN code length can be from 4 to 8 characters, and should always be memorized, or be in the possession of only the KSD holder.

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 - user authentication based on verification of specific physical characteristics of the user by means of special biometric equipment. Biometric authentication can be based on verification of fingerprints, iris, voice, and other specific characteristics of human body.

Two-Factor Authentication - this is a process controlling the authenticity of the user's identity on the basis of the two following factors: *"Something You Have – for example, the KSD device"* and *"Something You Know — for example, the user name and password, PIN-code"*.

Three-factor authentication - is a process controlling the authenticity of the user's identity on the basis of the three following factors: *"Something You Have – for example, the KSD"*, *"Something You Know — for example, the PIN code"*, *"Something You are – for example, the user's BIO ID"*.

Part III

3 Introducing Dekart Logon for Citrix ICA Client

This chapter contains the information about the purpose and features of **Dekart® Logon for Citrix ICA Client** and defines the basic concepts of enhanced user authentication, provided by the software:

- Identification.
- Authentication.
- Two-factor and three-factor authentication.

Dekart Logon for Citrix ICA Client allows to:

- Identify an authorized user, granting strictly defined access to the resources.
- Identify the third-party user and prohibit access to the resources.

Such recognition is carried out by means of certain procedures: the users must let the system know who they are, i.e. *identify* themselves to the system, and next, they must *authenticate* into the system.

Identification is a control process that examines a unique user ID and determines whether this user is known to the system.

Authentication is a control process that checks the authenticity of the user identity, i.e. this process controls whether the user is the person they say they are. Usually, identification consists in entering a user name, and authentication is based on the user's knowledge of a secret password that must be entered from the personal computer keyboard.

Unfortunately, the standard authentication means are based on the knowledge of two fixed values — the user name and password — and cannot guarantee reliable security if a third party learns these values. Therefore, there is the need to replace the standard *one-factor* authentication with the so-called strong authentication. The *strong authentication* is based on, at least, two of the following three factors:

1. *Something you know*: for example, a user name and ID code.
2. *Something you have*: for example, a device such as a smart card or USB token that enables a system to verify whether it is present or not.
3. *Something you are*: for example, fingerprints, iris, voice, and other specific traits of your body. Conformity to these traits can be verified by the system during authentication.

If two factors are used to authenticate the user to the system, then this authentication is called *two-factor authentication*, if all three factors – *three-factor authentication*. **Dekart Logon for Citrix ICA Client** provides either two or three factor authentication for users of Citrix ICA Client – for successful authentication the user requires a Key Storage Device, a PIN to this device, and, if biometric authentication is enabled, a successful biometric authentication. This type of authentication plays a major role in limiting access of the third-party users to the computer.

How to start work with Dekart Logon for Citrix ICA Client?

3.1 Dekart Logon for Citrix ICA Client purpose and futures

Dekart Logon for Citrix ICA Client is a combined software and hardware solution that provides secure user access to a Citrix server, and its resources, by means of strong (two- and three-factor) authentication.

Security principles of Dekart Logon for Citrix ICA Client

1. Security for Dekart Logon for Citrix ICA Client is provided by a Key Storage Device (PIN code protected) containing the ICA-connections details and user's BIO ID. The user no longer needs to store the connection data on a hard drive, and three-factor authentication reduces the risk of information losses in the event that the KSD is lost or stolen.
2. In order to access a Citrix server and its resources, it is enough to connect the KSD to the computer, enter the correct PIN code and pass biometric verification procedure (voice, fingerprint etc.). When the KSD is removed, the connection to the Citrix server is terminated.
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 appendix).***

Features of Dekart Logon for Citrix ICA Client

1. *Ease of use* – it is no longer necessary to remember or enter the access codes to the Citrix server.
2. *Mobility* – the ICA-connections are stored on the KSD, and therefore access to the Citrix server can be gained from any computer (*). It is enough to connect the KSD and enter the correct PIN code. Moreover, when a Flash disk is used as a KSD, you can store the software on it as well. This eliminates the requirement to install Dekart Logon for Citrix ICA Client on the computer.
3. *Interoperability* – the KSD can be used not only for DLCIC, but also for a variety of additional applications: Dekart Logon and/or Dekart Private Disk, or third party applications too.

(*) It is assumed that both, Citrix ICA Client and Dekart Logon for Citrix ICA Client are installed, and that the latter application is running.

3.2 Dekart Logon for Citrix ICA Client products components

One **Dekart Logon for Citrix ICA Client** package contains the following components:

- the application,
- documentation,
- the Key Storage Device (KSD).

The KSD acts as the unique means of access to a Citrix server.

3.3 Dekart Logon for Citrix ICA Client hardware and software requierments

Hardware requirements

- Personal computer, with at least a single port (COM, or USB) for KSD connection.
- In the event that a smart card is used, the smart card reader must be PC/SC compatible.
- If the user prefers to use three-factor authentication, a biometric device should be used, e.g. BioLink U-Match Mouse.

Software requirements

- Operating System: Windows 98, NT4.0, 2000, ME, XP.
- Citrix ICA Client for Windows 32 bit (Full Program Neighborhood Version 6.xx, 7.xx, 8.0).
- KSD drivers (usually provided with the product, or can be downloaded from the KSD manufacturers' web site.
- Drivers of biometric device.

Note: The Citrix ICA Client must have at least one ICA-connection. While configuring your ICA-Connection via the Properties window, you can select any type of Logon Information (Local user, Smart card or User-specified credentials). When setting the "User-specified credentials" it is necessary to provide the following details: User name, Password, Domain, then enable the Save password checkbox.

Attention!
In order to receive complete information about the Citrix ICA Client (setup, procedures, and other specifics), you should contact Citrix Systems, Inc., or visit their web site www.citrix.com.
Detailed information about biometric devices, used for authentication (features, software etc.) can be obtained from BioAPI Consortium at www.bioapi.org.

3.4 Supported key storage and biometric devices

Dekart Logon for Citrix ICA Client supports the following devices:

Key Storage Devices:

- ACOS1 card;
- ActivCard ActivKey USB token series;
- Aladdin eToken R2 USB token series;
- Aladdin eToken PRO USB token series;
- Algorithmic Research MiniKey USB token series;
- Algorithmic Research PrivateCard smart card series;
- Datakey Model 310 smart card series;
- Datakey Model 330 smart card series;
- Eutron CryptoIdentity ITSEC USB token series;
- Eutron CryptoIdentity 4 USB token series;
- Eutron CryptoIdentity 5 USB token series;

- GemPlus GPK smart card series;
- GemPlus MPCOS EMV smart card series;
- Giesecke & Devrient STARCOS S smart card series;
- Giesecke & Devrient STARCOS SPK smart card series;
- Rainbow iKey 1000 USB token series;
- Rainbow iKey 2000 USB token series;
- Rainbow iKey 3000 USB token series;
- Schlumberger Cryptoflex smart card series;
- Schlumberger Multiflex smart card series;
- Schlumberger Payflex smart card series;
- Siemens CardOS M 4 smart card series
- Dekart USB token series;
- USB flash drives, CD disks, etc.

Smart card readers:
Dekart Logon for Citrix ICA Client uses virtually all PC/CS compatible smart card readers, for example:

- Datakey DKR smart card reader series
- GemPlus GemPC smart card reader series
- OmniKey CardMan smart card reader series
- Schlumberger Reflex smart card reader series
- Towitoko CHIPDRIVE smart card reader series

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. Before you purchase a USB token or smart card, please make sure that it has enough memory to store the required user data (approximate 0.5 kB per ICA-connection). Please, take into account that the part of KSD memory may be allocated to other data, e.g. BIO ID. You can determine the memory usage of the card and read the USB token or smart card using the Dekart Key Manager Utility, as well as delete all unnecessary information using Dekart Key Manager.

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

type of card formatting.

Note 3. Dekart delivers all KSDs without a predefined PIN code.

Part IV

4 Quick Start for Dekart Logon for Citrix ICA Client

Prior Note. The user should have some experience working with Citrix ICA Client – configuring ICA-connections, connecting with Citrix server etc.

Dekart Logon for Citrix ICA Client does not interfere with the security policy of Citrix; it only extends the possibilities of the system. DLCIC allows making the Citrix connections routines easier and safer due to the hardware enhanced authentication. The DLCIC allows storing the information about ICA connections on the KSD. When the user connects to a Citrix server, the information about the required connection is automatically read from the KSD. When Dekart Logon for Citrix ICA Client is used, the user authentication is based on two or three factors (KSD, PIN code to access the KSD, and, optionally, the biometric identifier).

Software installation works like a standard Windows installation. User can install the simple version of DLCIC without KSD administration functions.

DLCIC can work in two modes: *management mode* and *monitoring mode*. In the management mode the application allows setting up the KSD for connection of a specific user to a specific Citrix server, as well as to service the KSD during the normal routines. The monitoring mode offers the user the ease and convenience of connections to Citrix server.

Working with DLCIC can be divided into two separate stages. *First stage*, the preliminary stage, consists of all necessary procedures required to prepare an "empty" KSD to function (the KSD does not contain the information from the DLCIC). To prepare the KSD the application should be started in the management mode.
Note. To store Dekart Logon for Citrix ICA Client data on the smart card or token you will need to format it using a Key Formatting utility or Corporate Key formatting utility. Registered customers can download the Key Formatting utility by providing the registration number for Dekart Logon for Citrix ICA Client at https://www.dekart.com/download/ (please, use Internet Explorer browser to access the restricted download area). The use of USB flash drive enables users to use the strong authentication provided by Dekart Logon for Citrix ICA Client without the need to use any type of card formatting.

Second stage is meant for increasing the security level of user working with Citrix ICA Client (monitoring mode), namely:
• User authentication during Citrix connection.
• Disconnecting user from Citrix server.

First stage.
Preparing the KSD:

1. Save ICA connections from the list of Custom ICA Connections onto the KSD memory;
2. Any of the ICA connections stored on the KSD can be set up to have the "Default connection" status. This connection will then be automatically used to connect to Citrix server once the KSD is inserted;

3. To protect the KSD from unauthorized use and to increase the security level, the KSD should be protected with PIN code. For additional security, it is also advisable to switch to three-factor authentication instead of a two-factor.

Second stage.

After successfully preparing the KSD using the above instructions, the user will have a KSD storing at least one ICA connection. After running DLCIC in the monitoring mode, the user will be able to connect to the Citrix server by connecting the KSD to the computer and using one of the four procedures which allow to connect to the server. To disconnect from Citrix server, it is enough to simply disconnect the KSD from the computer.

Part V

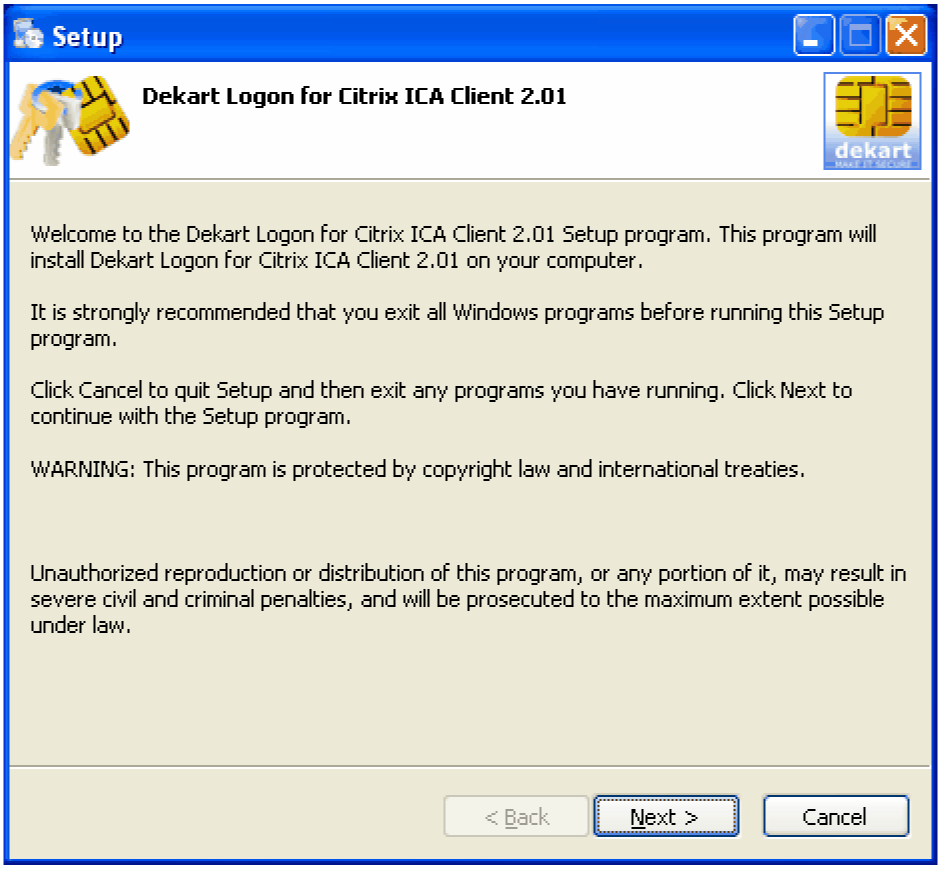
5 Installing, updating and uninstalling Dekart Logon for Citrix ICA Client

- Installing;
- Updating;
- Uninstalling.

5.1 Installing Dekart Logon for Citrix ICA Client

Prior Note. Before beginning installation of the Dekart Logon for Citrix ICA Client software, you must install Key Storage Device drivers. **Please, see chapter Supported key storage and biometric devices about KSD and its formatting procedure.**

1. Before beginning installation of the software, you must close all open applications.
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 Logon for Citrix ICA Client you must launch the program: ICALogon.exe.
4. In the appearing window select **Next**.



Welcome to the Dekart Logon for Citrix ICA Client 2.01 Setup program. This program will install Dekart Logon for Citrix ICA Client 2.01 on your computer.

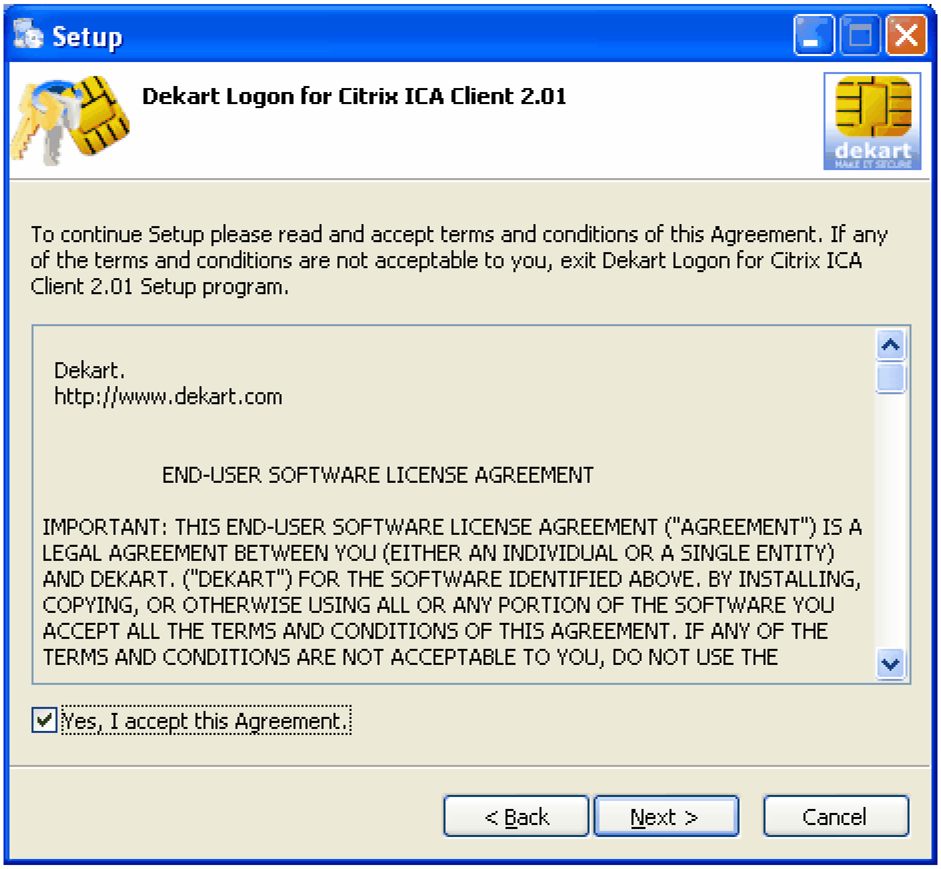
It is strongly recommended that you exit all Windows programs before running this Setup program.

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

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

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

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



Dekart Logon for Citrix ICA Client 2.01

To continue Setup please read and accept terms and conditions of this Agreement. If any of the terms and conditions are not acceptable to you, exit Dekart Logon for Citrix ICA Client 2.01 Setup program.

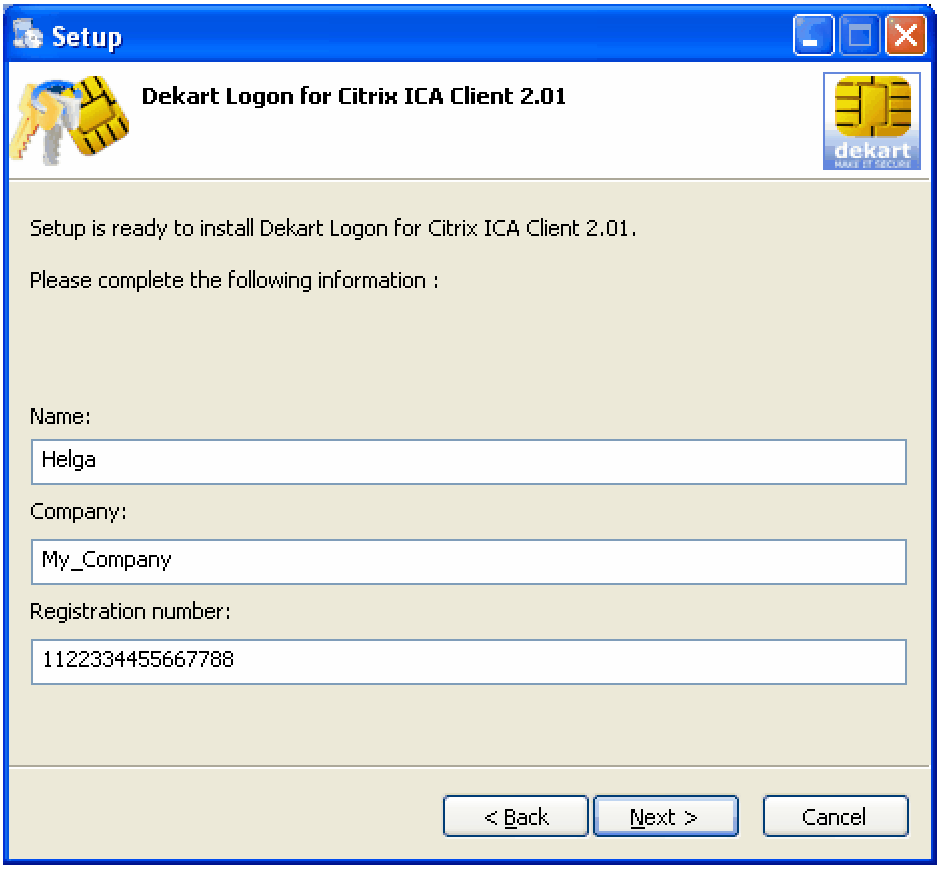
Dekart.
http://www.dekart.com

END-USER SOFTWARE LICENSE AGREEMENT

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

☑ Yes, I accept this Agreement.

6. The next step requires that you enter your personal information, and the serial number of the product.



Dekart Logon for Citrix ICA Client 2.01

Setup is ready to install Dekart Logon for Citrix ICA Client 2.01.

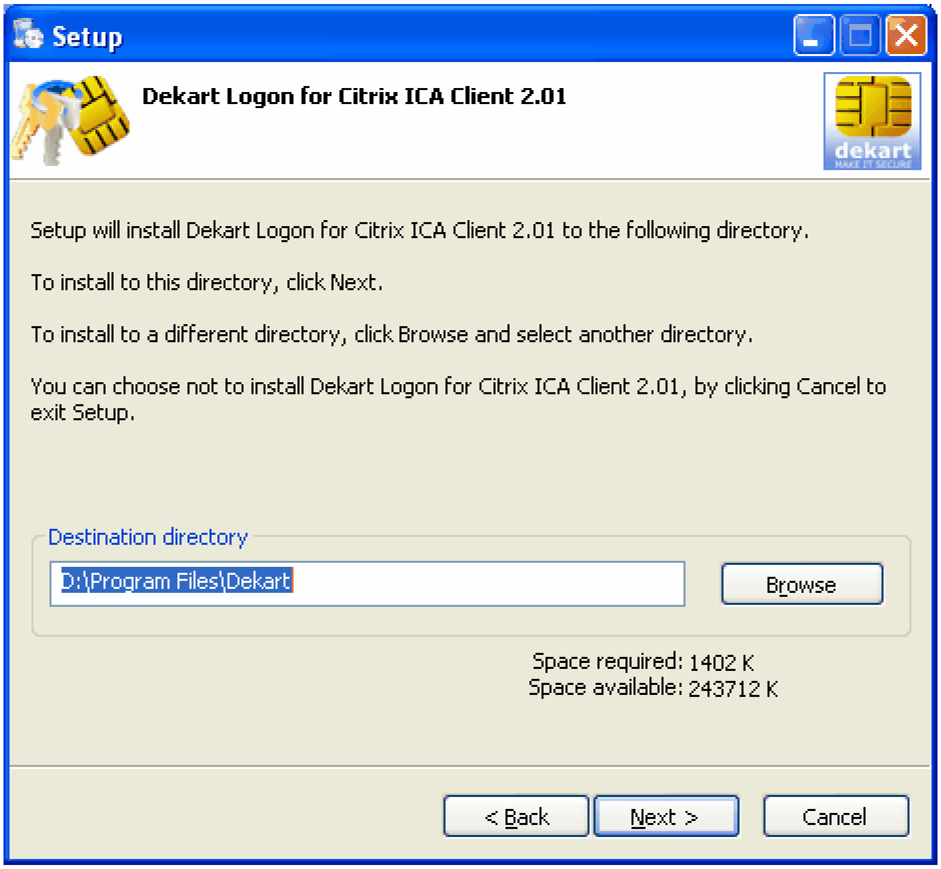
Please complete the following information :

Name: Helga

Company: My_Company

Registration number: 1122334455667788

7. You must then select the folder (**NOT ON THE REMOVABLE DEVICE!**), where the Dekart Logon for Citrix ICA Client software is to be installed.



Dekart Logon for Citrix ICA Client 2.01

Setup will install Dekart Logon for Citrix ICA Client 2.01 to the following directory.

To install to this directory, click Next.

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

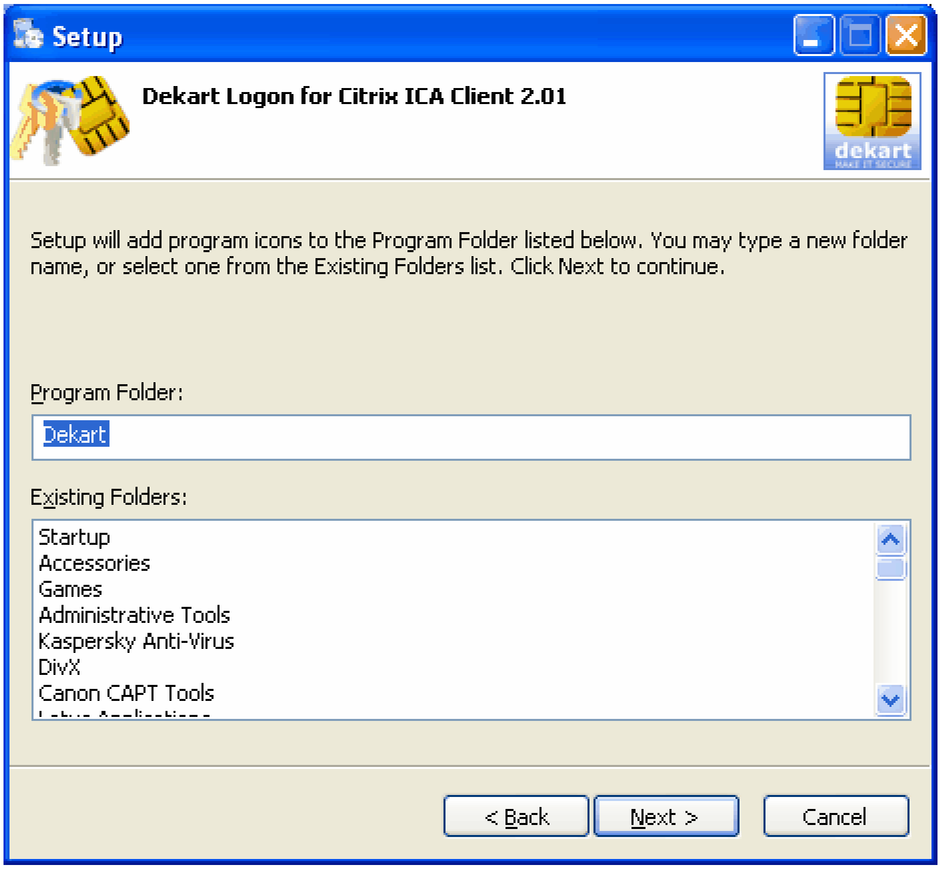
You can choose not to install Dekart Logon for Citrix ICA Client 2.01, by clicking Cancel to exit Setup.

Destination directory

D:\Program Files\Dekart

Space required: 1402 K
Space available: 243712 K

8. You must then select the folder in the **Start Menu**, where the Dekart Logon for Citrix ICA Client software is to be added.



Dekart Logon for Citrix ICA Client 2.01

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

Program Folder:

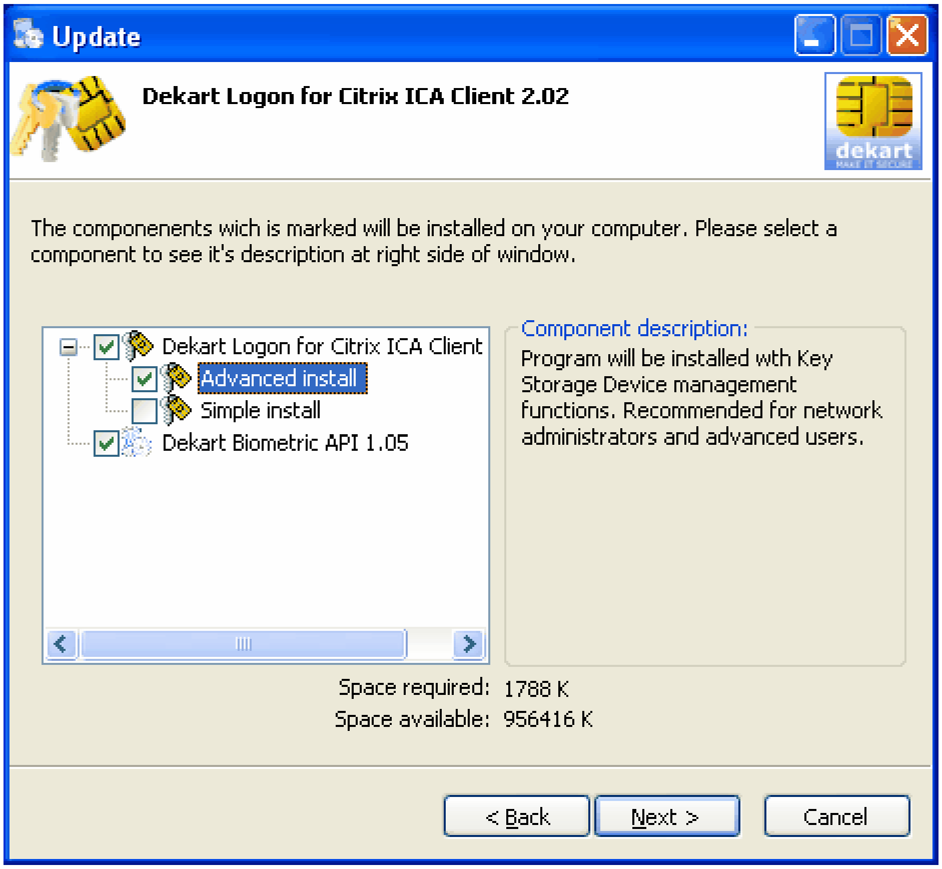
Dekart

Existing Folders:

Startup
Accessories
Games
Administrative Tools
Kaspersky Anti-Virus
DivX
Canon CAPT Tools

9. The next step requires that you set installation mode:

- Advanced install - program will be installed wth Key Storage Device management functions. Recommended for network administrators and advanced users.



Dekart Logon for Citrix ICA Client 2.02

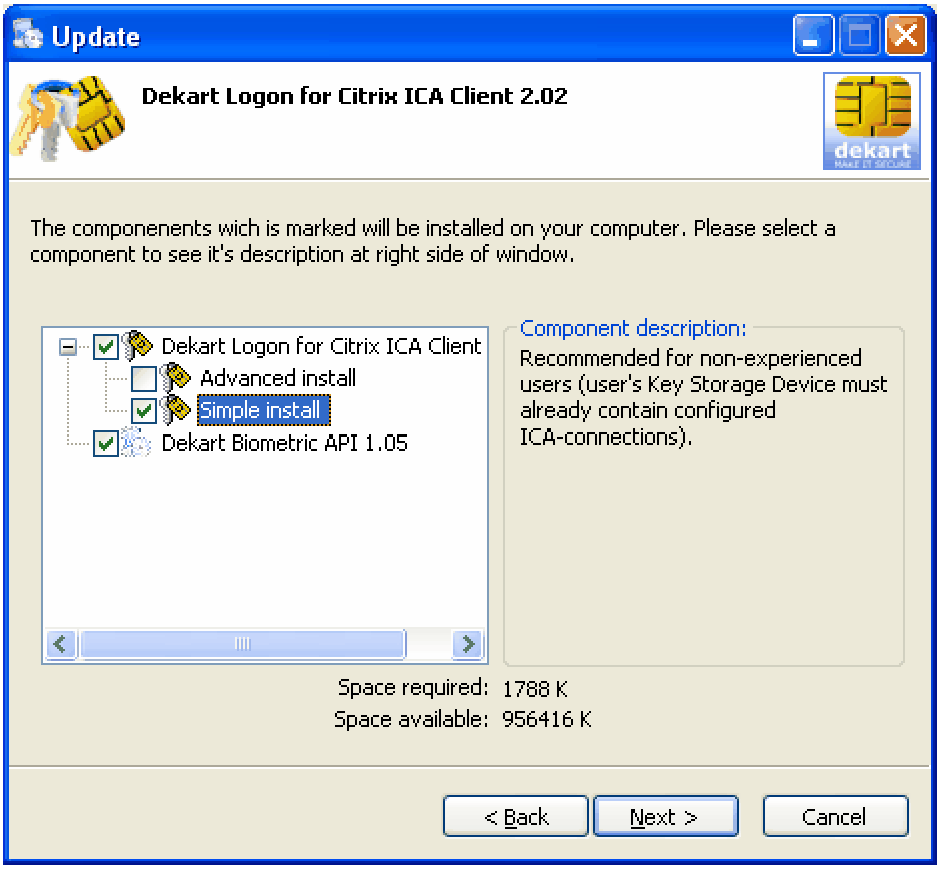
The componenents wich is marked will be installed on your computer. Please select a component to see it's description at right side of window.

- ☑ Dekart Logon for Citrix ICA Client
  - ☑ Advanced install
  - □ Simple install
- ☑ Dekart Biometric API 1.05

Component description:
Program will be installed wth Key Storage Device management functions. Recommended for network administrators and advanced users.

Space required: 1788 K
Space available: 956416 K

- Compact install - recommended for non-experienced users (user's Key Storage Device must already contain configured ICA-connections).



Update

Dekart Logon for Citrix ICA Client 2.02

The componenents wich is marked will be installed on your computer. Please select a component to see it's description at right side of window.

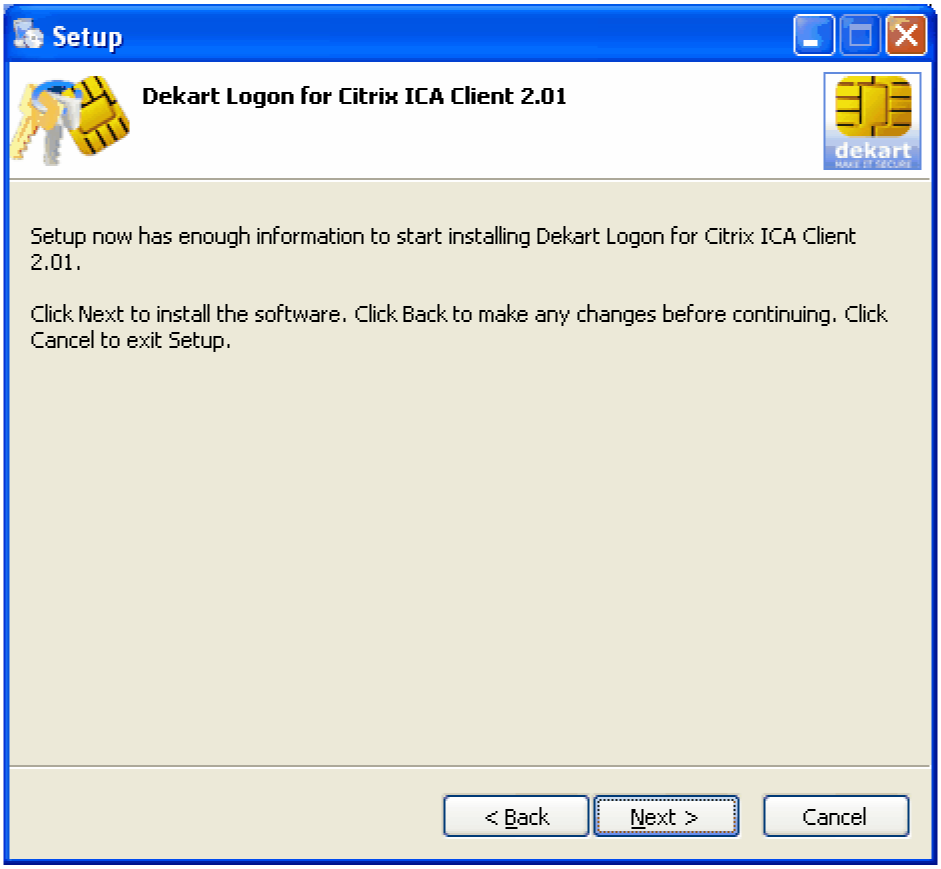
- ☑ Dekart Logon for Citrix ICA Client
  - □ Advanced install
  - ☑ Simple install
- ☑ Dekart Biometric API 1.05

Component description:
Recommended for non-experienced users (user's Key Storage Device must already contain configured ICA-connections).

Space required: 1788 K
Space available: 956416 K

- Additionally, you have to indicate whether you want to install the biometric API in order to use three-factor authentication.

10. The next step in the installation process requires that you press **Next**.

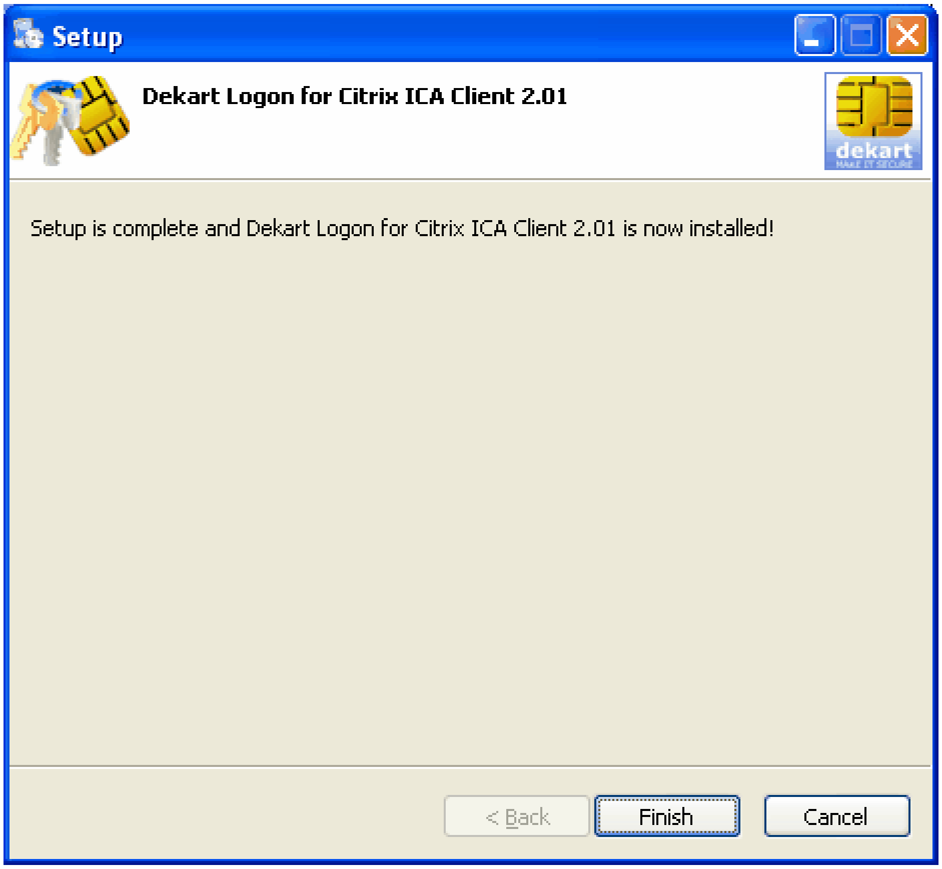


Dekart Logon for Citrix ICA Client 2.01

Setup now has enough information to start installing Dekart Logon for Citrix ICA Client 2.01.

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

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



Setup is complete and Dekart Logon for Citrix ICA Client 2.01 is now installed!

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

The following icon will appear on your desktop.

5.2 Installing Dekart Logon for Citrix ICA Client on a Flash disk

Using a Flash disk as a KSD (Key Storage Device) allows you to exploit another useful feature of the product – its mobility. In this case, the removable disk will not contain only the encrypted profiles of the ICA-connections, but also the application itself. This is how you can connect to a remote Citrix-server from any computer without having to set up Logon for Citrix ICA Client.

To do this, follow these steps:

1. Install Dekart Logon for Citrix ICA Client.
2. Open the **Start** menu, go to: **Programs\Dekart\Logon for Citrix ICA Client**, and

choose **Install to removable device (Advanced mode)** or **Install to removable device (Simple mode)**. Depending on the mode you choose, you will be able to configure more or less settings.

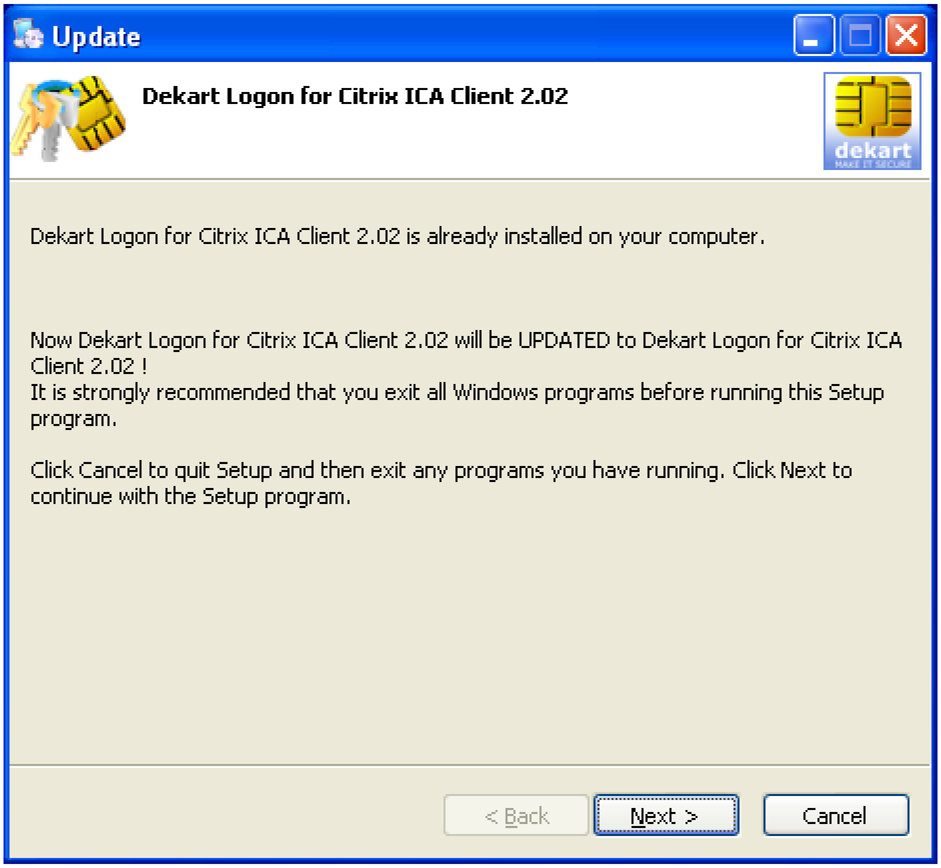
3. In the opened window select removable device (Flash disk) which you will use as KSD and press ***OK***.

Note: If you installed Dekart Logon for Citrix ICA Client on the hard disk in the Simple mode - then you can install it to the flash drive in the Simple mode only.

5.3 Updating Dekart Logon for Citrix ICA Client

To update **Dekart Logon for Citrix ICA Client** 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 necessary information in the picture below.

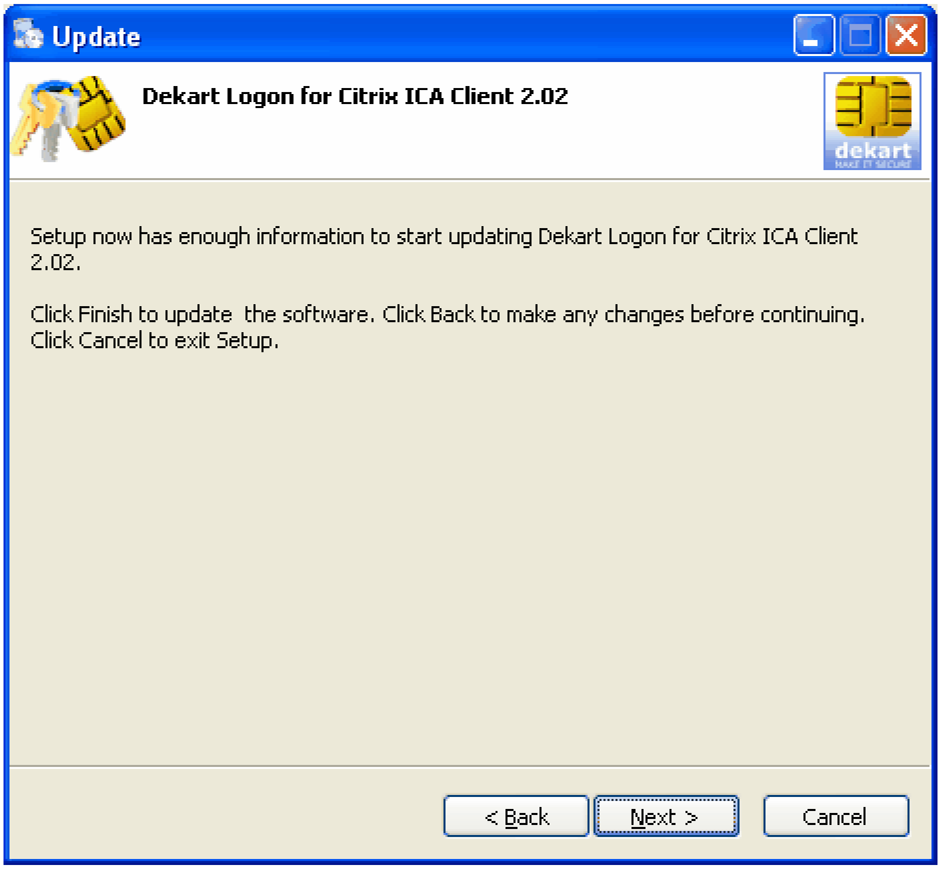


Dekart Logon for Citrix ICA Client 2.02 is already installed on your computer.

Now Dekart Logon for Citrix ICA Client 2.02 will be UPDATED to Dekart Logon for Citrix ICA Client 2.02 !
It is strongly recommended that you exit all Windows programs before running this Setup program.

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

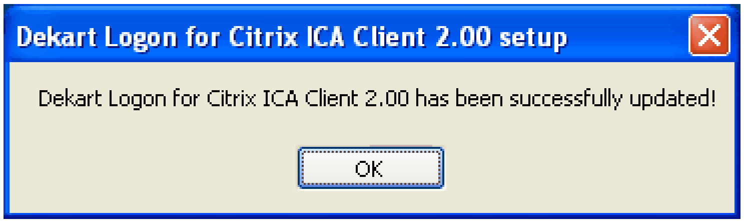
2. In order to continue the process, you must press **Next**. You must accept the license agreement before you can proceed to upgrade.
3. The next step requires that you set installation mode and press **Next**.
4. Click the **Finish** button to terminate the update process.



Setup now has enough information to start updating Dekart Logon for Citrix ICA Client 2.02.

Click Finish to update the software. Click Back to make any changes before continuing. Click Cancel to exit Setup.

Upon 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.



Dekart Logon for Citrix ICA Client 2.00 has been successfully updated!

Note: After updating Dekart Logon for Citrix ICA Client, it is necessary to restart your computer.

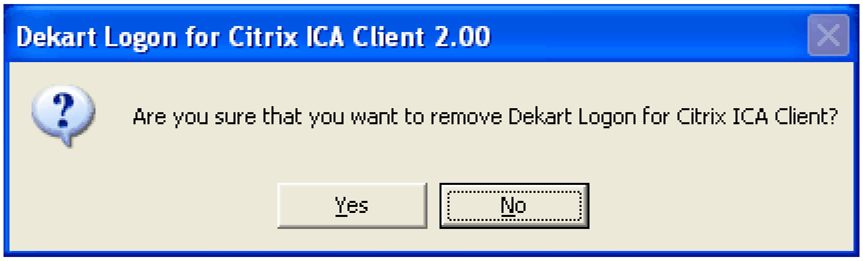
Note: To update the software located on a Flash disk, you have to repeat the steps described in the "Installing Dekart Logon for Citrix ICA Client on a Flash disk" chapter once the update is complete.

5.4 Deleting Dekart Logon for Citrix ICA Client

In order to remove the software, follow these steps:

1. Select **Programs** menu in **Start Menu**, locate the folder you have entered in step 7 when installing the program, select **Uninstall** (alternatively, you can go to **Control Panel**, select

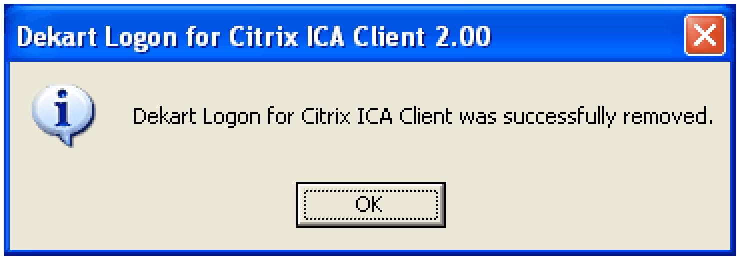
Add or Remove Programs, select the program name in the list and press the **Uninstall** button). The following message will appear:



Are you sure that you want to remove Dekart Logon for Citrix ICA Client?

In order to confirm your intention to remove Dekart Logon for Citrix ICA Client press **Yes**.

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



Dekart Logon for Citrix ICA Client was successfully removed.

Note: If you have a "mobile" version of the product (i.e. it is installed on a Flash disk), you will have to delete the following folder from your removable drive: Dekart\Logon for Citrix ICA Client.

Part VI

6 Working with Dekart Logon for Citrix ICA Client

The DLCIC application can function in two modes – management mode and monitoring mode. The first mode (management) allows you to setup the KSD for user access to a Citrix server, and to manage the KSD. The second mode (monitoring) enables the user to easily connect to a Citrix server.

Management mode options:

Change PIN	Change the PIN code
Change Label	Change KSD label
Change BIO ID	Change biometric identifier
Unblock PIN	Unblock the PIN code
Clear KSD	Clear KSD

Add/Edit	Add or edit the ICA-connection parameters
Remove	Remove the ICA-connection from the list
Store to KSD	Store the ICA-connection on the KSD (without removing from the list)
Move to KSD	Store the ICA-connection on the KSD with simultaneous removal from the list
Restore from KSD	Restore the ICA-connection from the KSD to the list.
Delete	Delete the ICA-connection from the KSD
Make Default	Set up the ICA-connection to have "Default connection" status
Connect to…	Connect to the Citrix-server in compliance with the ICA-connection stored on the KSD
Minimize	Close the window and transfer from management mode to monitoring mode.
Exit	Close the application
F1	Open About Dekart Logon for Citrix ICA Client window

Monitoring Mode options:

Connect	Connect to Citrix server, using the ICA connection details stored on the KSD
Auto Connect	Automatically connect to Citrix server on KSD insertion event (using "Default" ICA-connection).
Restore	Change from monitoring mode to management mode (the operation can be performed only in case of advanced product installation – administrator's version).
Auto Log Off /Disconnect	Automatically log off from Citrix server on KSD removal event
Enable monitoring	Enable/disable monitoring mode
Disable monitoring	Enable/disable monitoring mode
Exit	Close application

About	Information about the application

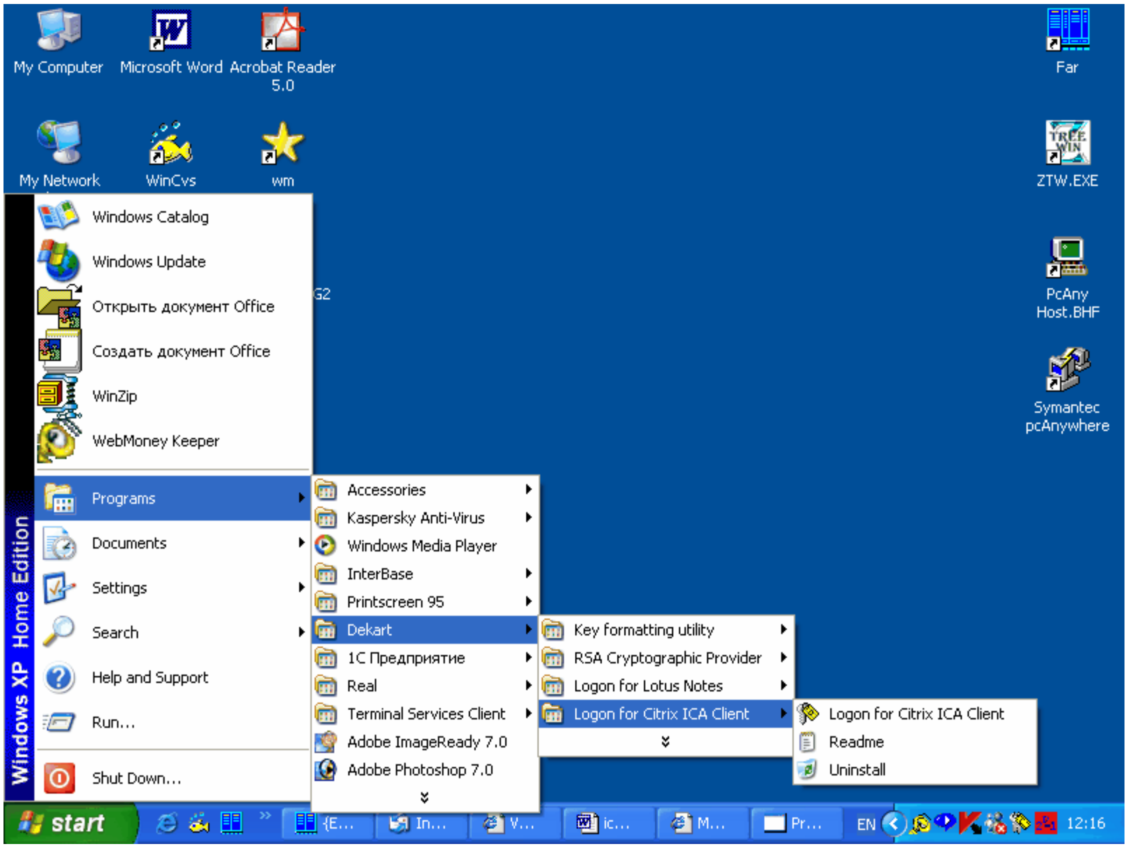
Note: When running the application from a Flash disk, it operates in the monitoring mode.

6.1 Working with Dekart Logon for Citrix ICA Client in management mode

The first mode (management) allows you to setup the KSD for user access to a Citrix server, and to manage the KSD.

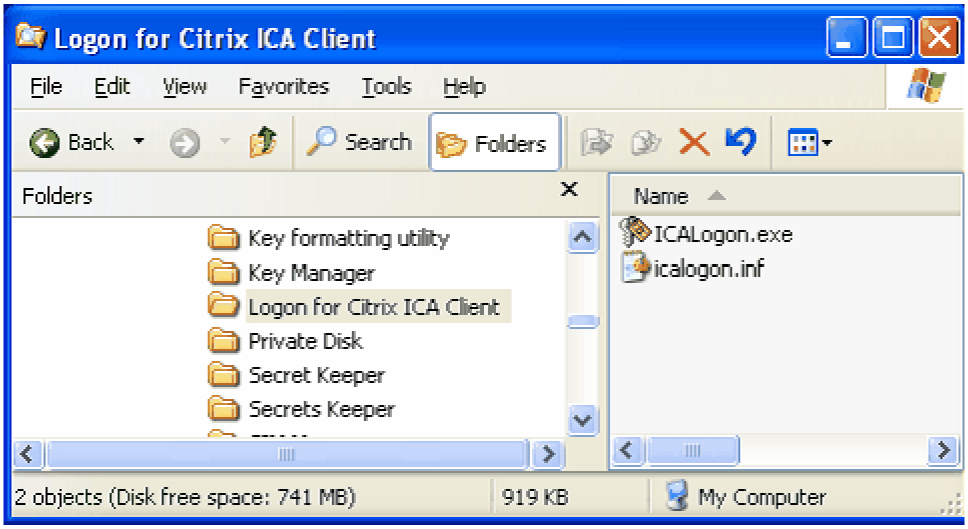
6.1.1 Launch the application in management mode

1. Connect the KSD to the computer.
2. Use one of the following alternatives to launch the application:
   - In the **Start Menu** select **Programs**, and then select the folder where the application is stored (see step 7 in Installing Dekart Logon for Citrix ICA Client).

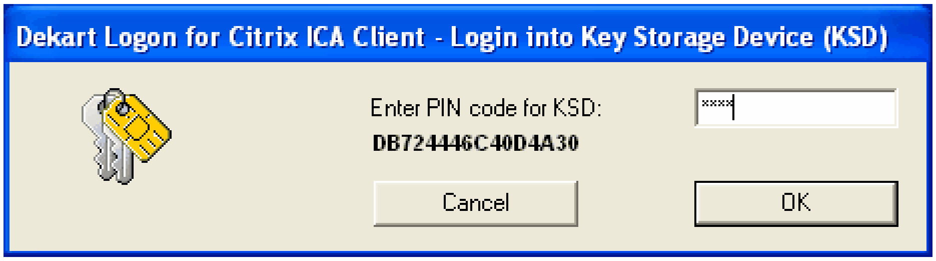


   - Or, in Windows Explorer, open the folder indicated in par. 6 during the installation procedure.

     Note: if you use a USB flash-disk as a KSD, the program has to be executed directly from the disk: <Flash-drive>\Dekart\Logon for Citrix ICA Client\ICALogon.exe.



If the KSD is PIN code protected, you will see a window requesting for the PIN code before allowing you to access the system.


Dekart Logon for Citrix ICA Client - Login into Key Storage Device (KSD)
Cancel
OK

Enter PIN code for KSD: ****

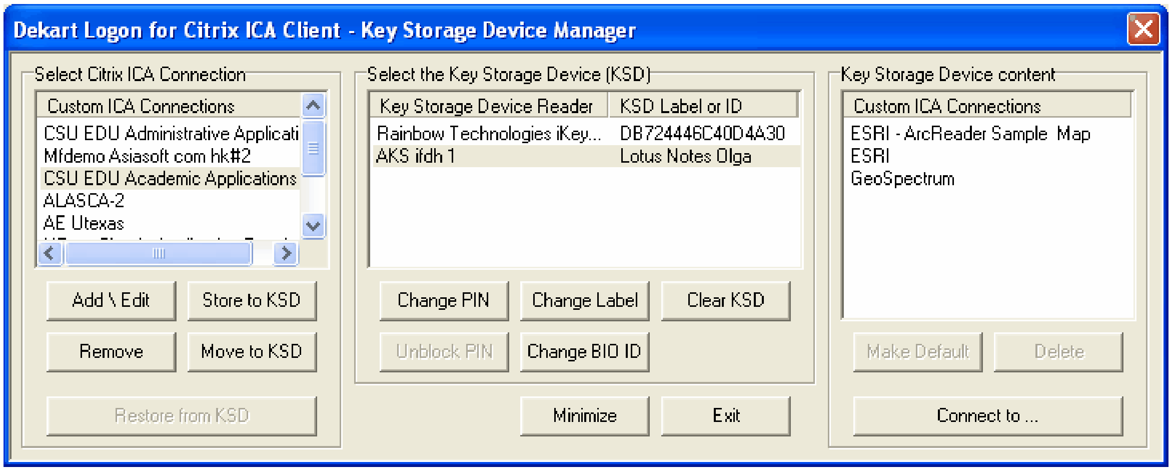
DB724446C40D4A30

3. The user must enter the PIN code and press **OK.**

Attention! KSD will block upon multiple wrong PIN code entries. Please, be careful. The number of allowable incorrect entries varies according to the KSD manufacturer, and the application.

Note: If the BIO ID is stored on the KSD, the software will automatically detect it and will attempt to start biometric authentication.

After successful authentication you will see the main application window.



Custom ICA Connections

CSU EDU Administrative Applicati
Mfdemo Asiasoft com hk#2
CSU EDU Academic Applications
ALASCA-2
AE Utexas

Key Storage Device Reader	KSD Label or ID
Rainbow Technologies iKey...	DB724446C40D4A30
AKS ifdh 1	Lotus Notes Olga

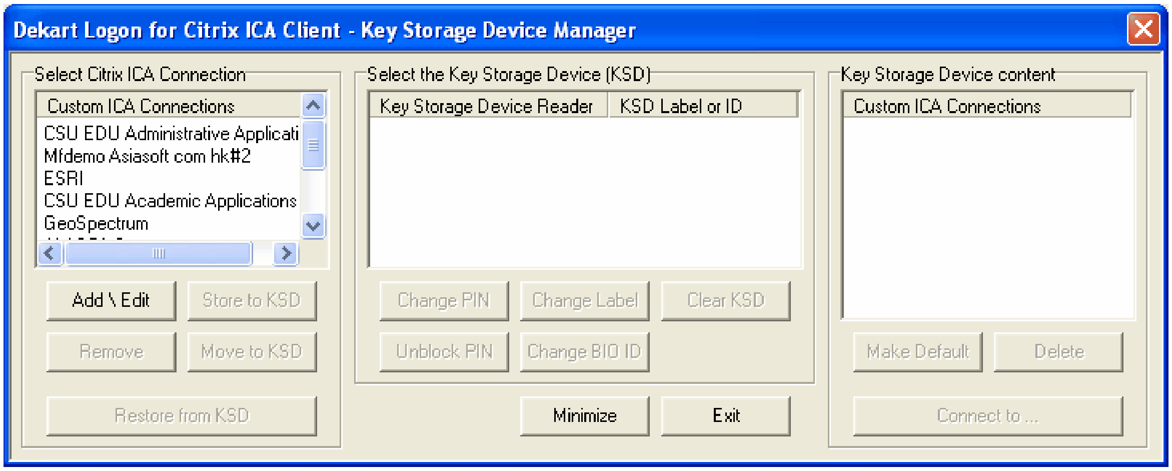
Custom ICA Connections

ESRI - ArcReader Sample Map
ESRI
GeoSpectrum

The left-hand side of the window (*Citrix ICA Connection*) contains all configured ICA-connections. The central part of the window displays the information about KSDs connected to the computer. The first column (*Key Storage Device reader*) contains KSD readers (smart card readers and USB tokens). The second column (*KSD Label or ID*) contains the label of the KSD or identifier. The right-hand side of the window displays the list of ICA-connections, stored on the currently used KSD (*Key Storage Device Content*).

Note: if the KSD is new, then you will see the serial number of the device in the KSD Label or ID field. The user can change this parameter later.

If the application is launched without the KSD, then the main application window will appear:



Custom ICA Connections

CSU EDU Administrative Applicati
Mfdemo Asiasoft com hk#2
ESRI
CSU EDU Academic Applications
GeoSpectrum

Key Storage Device Reader	KSD Label or ID

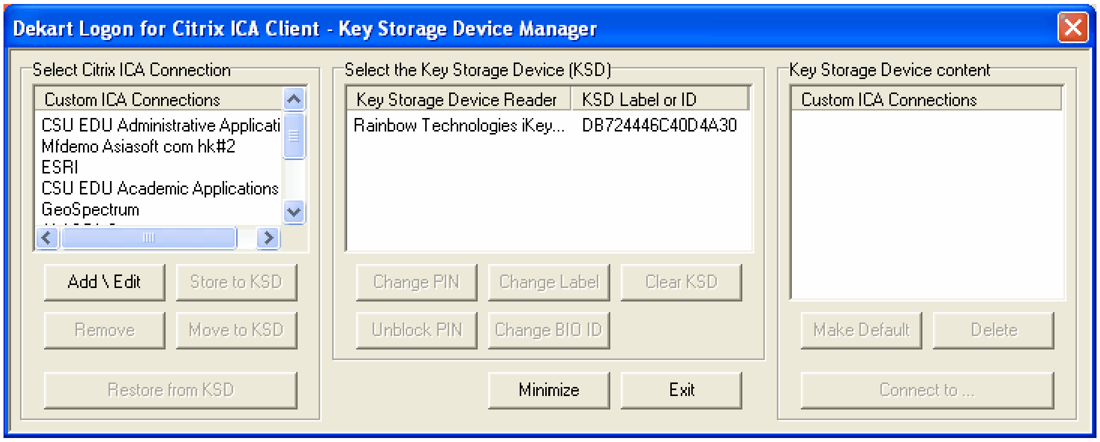
Custom ICA Connections

In this case, the user must connect the KSD to the computer, and enter the PIN code, if necessary.

6.1.2 Preparing the KSD for use with the application

To preparing KSD (i.e. store Dekart Logon for Citrix ICA Client data on the device) such as <u>smart_card_or_token</u> you will need to format it using a Key Formatting utility or Corporate Key formatting utility. Registered customers can download the Key Formatting utility by providing the registration number for Dekart Logon for Citrix ICA Client at https://www.dekart.com/download/ (please, use Internet Explorer browser to access the restricted download area).

After launching the software, and connecting a new KSD, and if required, successful PIN code verification the following window will appear:

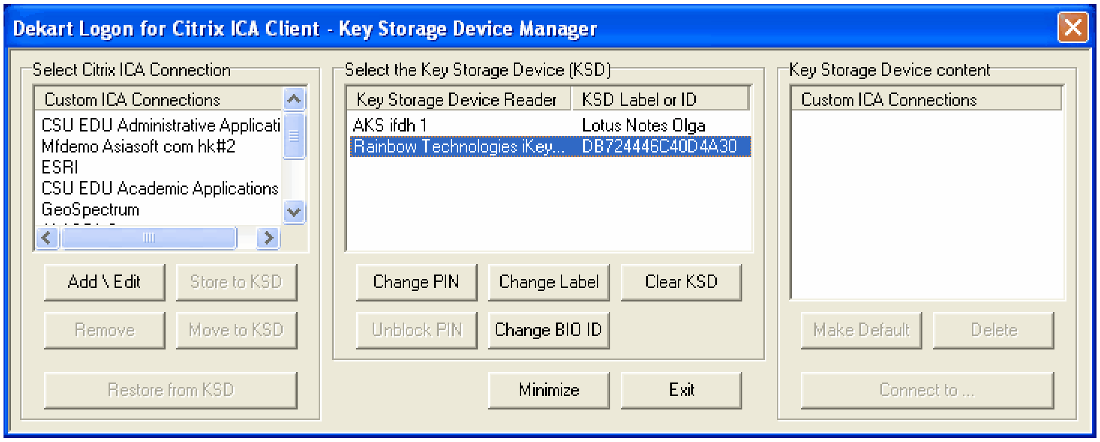


Custom ICA Connections
CSU EDU Administrative Applicati
Mfdemo Asiasoft com hk#2
ESRI
CSU EDU Academic Applications
GeoSpectrum

Key Storage Device Reader	KSD Label or ID
Rainbow Technologies iKey...	DB724446C40D4A30

Note: if you use a USB flash-disk as a KSD, you should re-connect it (disconnect then connect) after starting the application.

1. Left-click the KSD name to select the KSD in the *Key Storage Device Reader*.

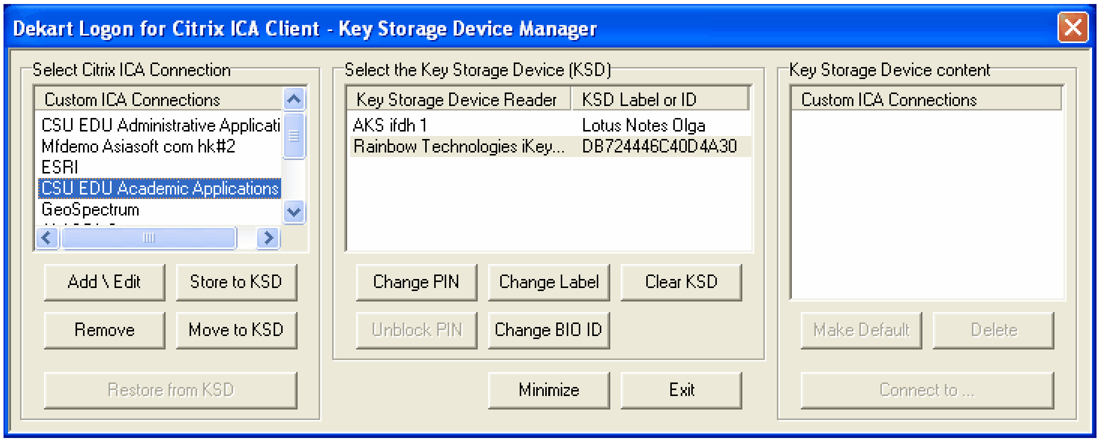


Custom ICA Connections
CSU EDU Administrative Applicati
Mfdemo Asiasoft com hk#2
ESRI
CSU EDU Academic Applications
GeoSpectrum

Key Storage Device Reader	KSD Label or ID
AKS ifdh 1	Lotus Notes Olga
Rainbow Technologies iKey...	DB724446C40D4A30

After this, the C**hange PIN, Change Label, Change BIO ID, Clear KSD** buttons will be activated**.**

2. Select the *ICA-connection* in the *Citrix ICA Connection field.* At this point the **Store to KSD, Move to KSD, Remove** buttons are activated.

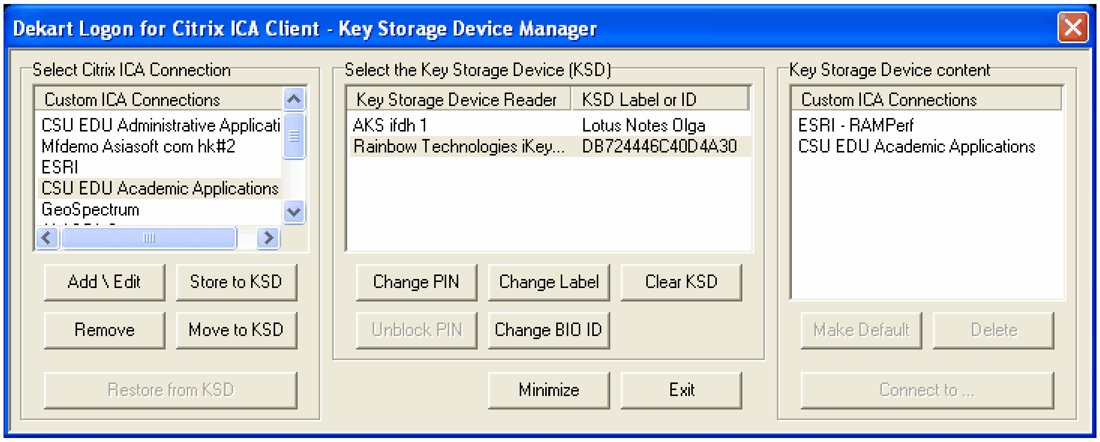


Custom ICA Connections
CSU EDU Administrative Applicati
Mfdemo Asiasoft com hk#2
ESRI
CSU EDU Academic Applications
GeoSpectrum

Key Storage Device Reader	KSD Label or ID
AKS ifdh 1	Lotus Notes Olga
Rainbow Technologies iKey...	DB724446C40D4A30

Custom ICA Connections

3. In order to store the ICA-connection on the KSD, press either the **Store to KSD,** or **Move to KSD** buttons. In first case, the ICA-connection will be listed as an active ICA-connection, in second case, the ICA connection will be deleted from the list. After this procedure, the **Restore from KSD** button is activated.



Custom ICA Connections
CSU EDU Administrative Applicati
Mfdemo Asiasoft com hk#2
ESRI
CSU EDU Academic Applications
GeoSpectrum

Key Storage Device Reader	KSD Label or ID
AKS ifdh 1	Lotus Notes Olga
Rainbow Technologies iKey...	DB724446C40D4A30

Custom ICA Connections
ESRI - RAMPerf
CSU EDU Academic Applications

At this point, all preliminary procedures to make the KSD ready for work are completed.

Note 1. Steps 2 and 3 can be successfully repeated depending on the number of connections to be stored on KSD and the size of KSD memory.

Note 2. In order to increase the security level, it is highly recommended that you assign a PIN code to the KSD using the "Change PIN" feature.

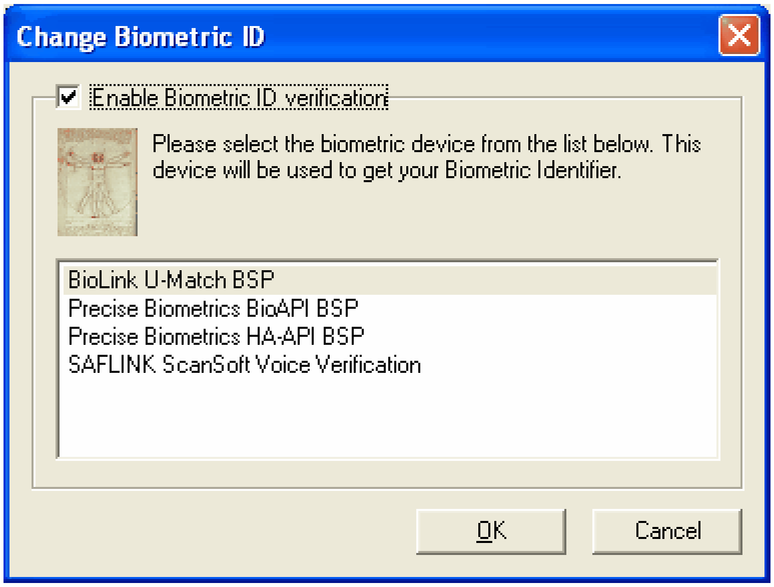
6.1.3 Adding BIO ID to the KSD

In order to enable three-factor authentication, the KSD should store user's biometric identifiers.

Note: The choice of biometric device is determined by the physiological characteristics of user and the location of his computer.

In order to add BIO ID do the following:

1. Click the **"Change BIO ID"** button in program window. The window with the list of installed drivers for biometric devices will appear.



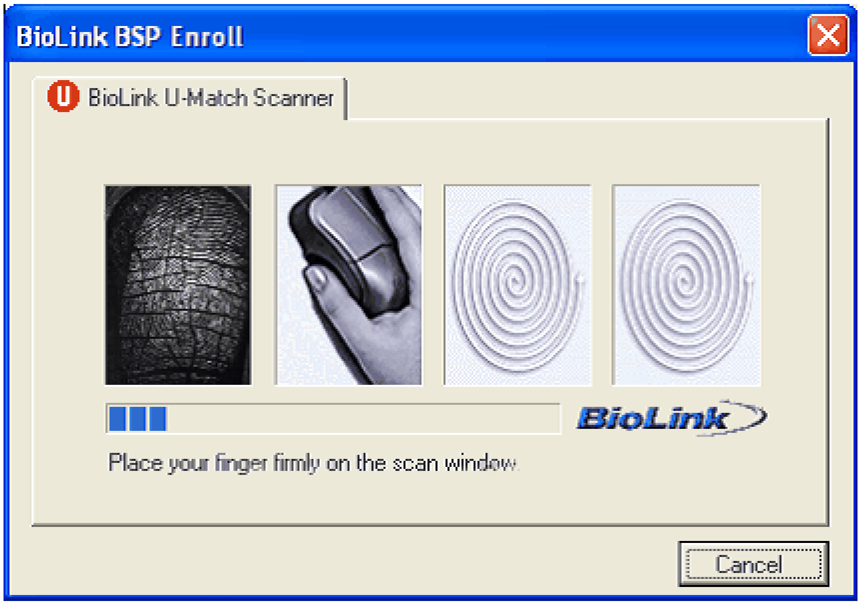
Change Biometric ID

☑ Enable Biometric ID verification

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

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

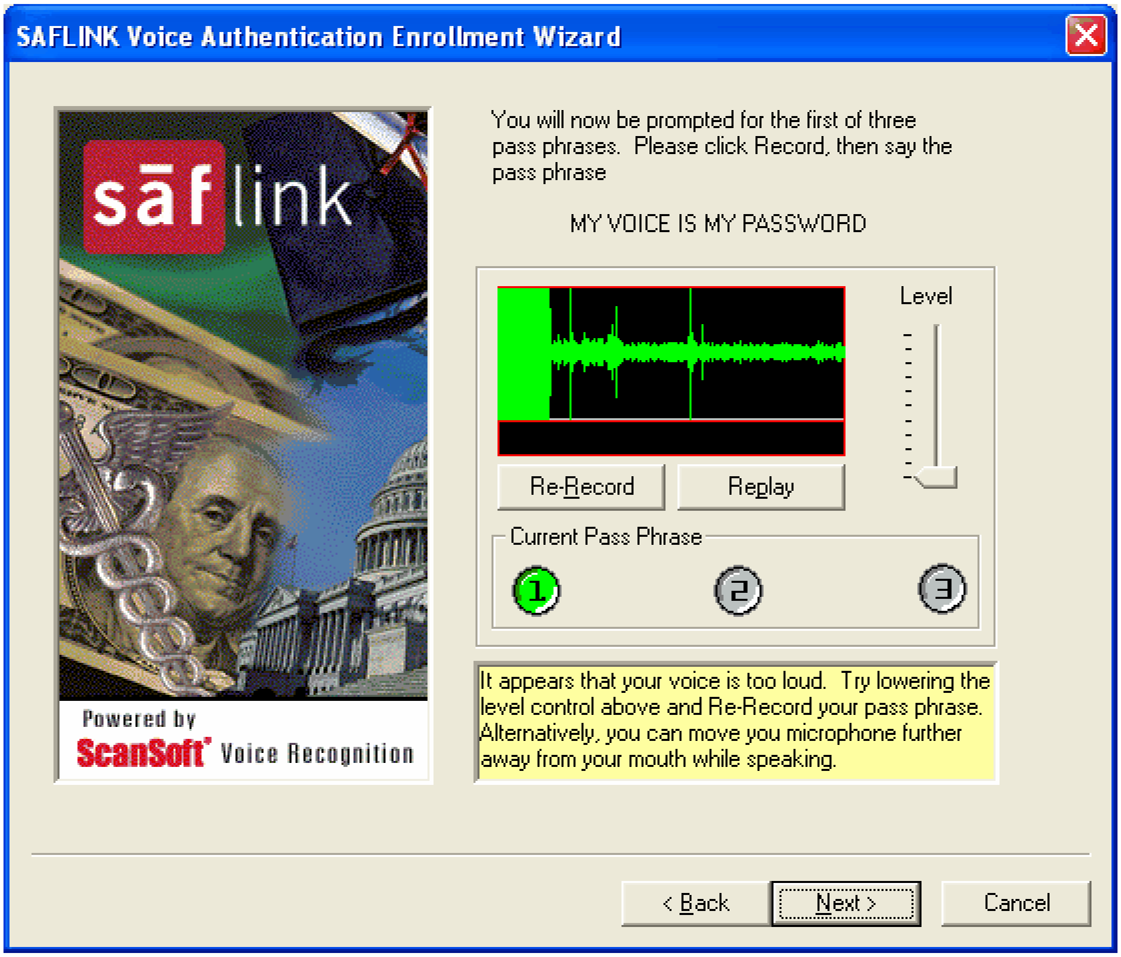
2. Check the **"Enable Biometric ID verification"** checkbox and select the biometric device from the list.
3. If the fingerprint scanner is used, e.g. BioLink U-Match, the user will be required to provide his fingerprints for scanning for several times. As soon as the scanning procedure is complete, the user's BIO ID is stored on the KSD.



BioLink BSP Enroll

Place your finger firmly on the scan window.

If the voice recognition device is used, e.g. SAFLINK Scansoft Voice Verification, the user will be required to speak the key phrase into a microphone to create his voice template. After the voice template is created, it is then stored on the KSD.



SAFLINK Voice Authentication Enrollment Wizard

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

MY VOICE IS MY PASSWORD

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

6.1.4 Managing the KSD

In order to change parameters for the KSD and the information stored therein, it is necessary to do the following:

1. Launch the application, and connect the KSD, then enter the PIN code.
2. Select currently used KSD in *Key Storage Device Reader*.

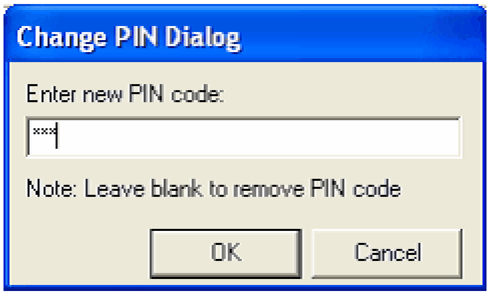
At this point the user can do the following with the KSD:

- Change the PIN code;
- Change the label for the KSD;
- Change BIO ID;
- Clear the KSD;
- Un-block the PIN-code;
- Edit the list of ICA-connections*;*
- Change KSD contents.

6.1.5 Changing the PIN Code

In order to change the PIN code, do the following:

1. Launch the application.
2. Select the KSD from the *Key Storage Device Reader*.
3. Then press **Change PIN.** The following dialog box will appear.



Enter new PIN code:

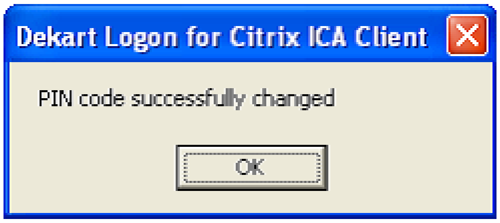
***

Note: Leave blank to remove PIN code

4. In the field *new PIN code*, enter the new PIN code, or leave it blank (in order to work without a PIN code) then press **OK**.

Note: The PIN code length varies from 4 to 8 symbols.

5. Confirm new PIN code and press **OK.**

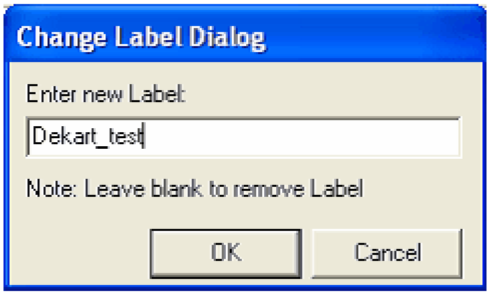


PIN code successfully changed

6.1.6 Changing the label for the KSD

The label for the KSD contains the information about the owner of the device. The field can contain the name of the user, or any other pertinent information you wish to enter into the field. In order to change the label of the KSD, it is necessary to:

1. Launch the application.
2. Using your mouse, select the appropriate KSD in *Key Storage Device Reader*.
3. Then press the **Change Label** button. The following dialog box will appear.



Change Label Dialog

Enter new Label: Dekart_test

Note: Leave blank to remove Label

3. In the field *new Label*, you must select the new label for the KSD and press **OK**. In order to clear the label *new Label*, you should leave the field blank and then press **OK** (in this case, in the field KSD Label or ID, the serial number will be stored).

Note: The KSD label cannot be more than 32 characters long.

6.1.7 Changing BIO ID

In order to change the BIO ID (if it has been previously stored on the KSD) do the following:

1. Launch the program.
2. Select the KSD from the *Key Storage Device Reader*.
3. Click the **"Change BIO ID"** button in the program window. The ***Change Biometric ID*** window with the list of installed drivers of biometric devices will appear.
4. Select the biometric device from the list.
5. Depending on the type of the selected device enter the required biometric information (fingerprint, voice). After the succession of biometric scans, the template will be stored on the KSD.

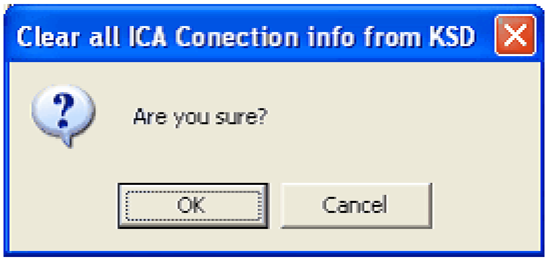
Note: In order to stop using biometric authentication, the user should uncheck the Enable Biometric ID verification checkbox in the Change Biometric ID window.

6.1.8 Clearing the KSD

Attention! Performing this operation will erase all DLCIC data from the device, including all ICA connections!

In order to perform this action, do the following:

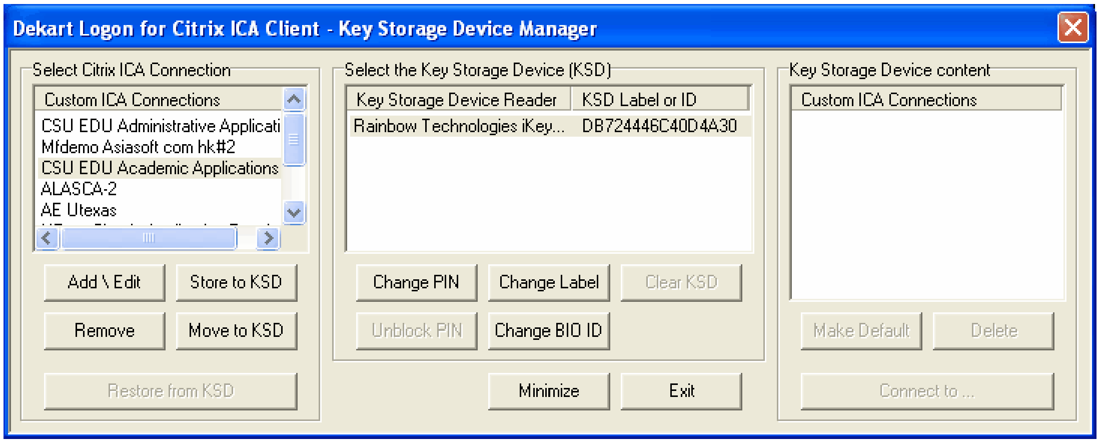
1. Launch the application .
2. Using your mouse, select the KSD being used in *Key Storage Device Reader*.
3. Then select **Clear KSD.** The application will ask you to confirm the action.



Clear all ICA Conection info from KSD

Are you sure?

3. Press **OK** to complete the action. The following window will appear


Dekart Logon for Citrix ICA Client - Key Storage Device Manager

Select Citrix ICA Connection

Custom ICA Connections
CSU EDU Administrative Applicati
Mfdemo Asiasoft com hk#2
CSU EDU Academic Applications
ALASCA-2
AE Utexas

Select the Key Storage Device (KSD)

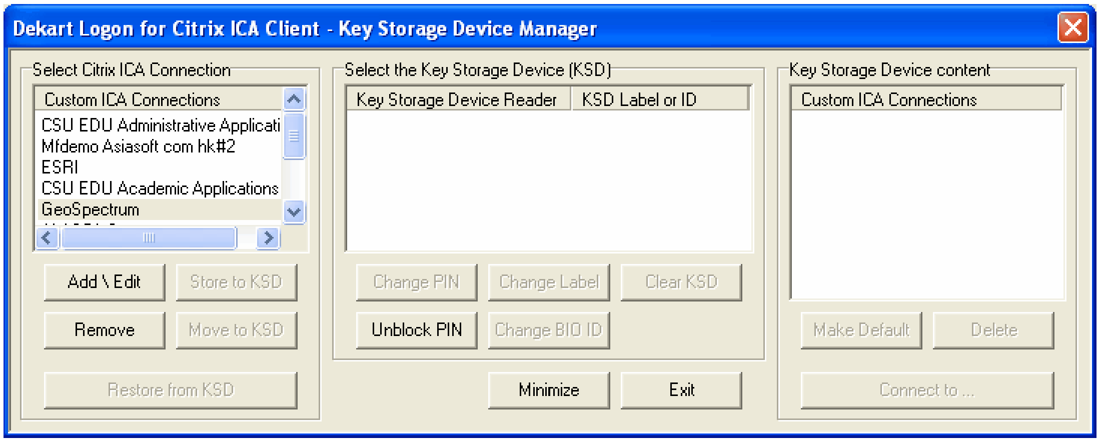
Key Storage Device Reader	KSD Label or ID
Rainbow Technologies iKey...	DB724446C40D4A30

Key Storage Device content

Custom ICA Connections

6.1.9 Unblocking the KSD

After several incorrect PIN code entries, the KSD will be blocked. In order to unblock the KSD, you should launch the application, and in the main window select **Unblock PIN.**


Dekart Logon for Citrix ICA Client - Key Storage Device Manager

Select Citrix ICA Connection

Custom ICA Connections
CSU EDU Administrative Applicati
Mfdemo Asiasoft com hk#2
ESRI
CSU EDU Academic Applications
GeoSpectrum

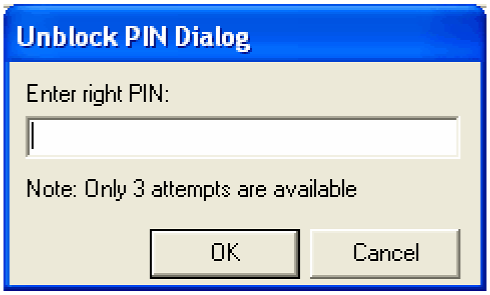
Select the Key Storage Device (KSD)

Key Storage Device Reader	KSD Label or ID

Key Storage Device content

Custom ICA Connections

You will then be prompted to enter the PIN code.


Unblock PIN Dialog

Enter right PIN:

Note: Only 3 attempts are available

If the PIN code is incorrectly entered, the KSD will be <u>permanently</u> blocked!

Note: The number of allowable attempts for de-blocking the KSD varies depending on the application, and type of KSD.

6.1.10 Possible actions with the Citrix ICA Connection list of ICA-connections

After launching the application the user may edit the ICA connection list:

- Add or edit the parameters for a specific ICA connection within the list;
- Delete an ICA connection from the list;
- Store an ICA connection on the KSD;
- Transfer an ICA connection to the KSD;
- Reinstate an ICA connection from the KSD to the list.

6.1.11 Additions/edits to ICA connections

In order to add or edit the parameters for a specific ICA connection in a list (**Add/Edit** button is active after launching the application, even if the KSD is not attached).
In order to perform this operation it is necessary to:

1. Launch the application.
2. Press **Add/Edit.** At this time the Citrix ICA Client application will be launched (Citrix Program Neighborhood – Custom ICA Connections), which will allow the user to make the desired changes. After the application Citrix Program Neighborhood – Custom ICA Connections is closed, the DLCIC window will appear.

Note: During ICA-connection addition or editing, it is necessary to specify: User name, Password, Domain, and set flag: Save password.

6.1.12 Deleting ICA-connections from the list

In order to delete a specific ICA-connection from the list it is necessary to:

1. Launch the application.
2. Using the mouse, select the ICA-connection from the list: *Custom ICA Connections* and press **Remove**.
3. In order to continue working with the ICA-connection list, you must click on an empty field in the *Key Storage Device (KSD)* table, and then once again select the KSD.

6.1.13 Storing an ICA-connection on the KSD

In order to store a specific ICA-connection from the list on the KSD it is necessary to:

1. Launch the application.
2. Using the mouse, select the active KSD in *Key Storage Device (KSD).*
3. In the *Custom ICA Connections* list select the required ICA-connection and press **Store to KSD**. The selected ICA-connection will appear in the *Custom ICA Connection field of* the Key Storage Device (KSD) table.

6.1.14 Transferring the ICA connection from the list to the KSD

In order to transfer a specific ICA connection from the list to the KSD, it is necessary to:

1. Launch the application.
2. Using your mouse, select the active KSD in *Key Storage Device (KSD)*.

In the list *Custom ICA Connections*, select the required ICA connection, and press **Move to KSD**. The selected ICA-connection will appear in the *Custom ICA Connection field of* the Key Storage Device (KSD) table, and will disappear from the list of *Custom ICA Connections.*

6.1.15 Retrieving the ICA connection in the list, from the KSD

In order to retrieve the ICA connection from the KSD it is necessary to:

1. Launch the application.
2. Using your mouse, select the active KSD in *Key Storage Device (KSD)*.
3. Press **Restore from KSD**.

6.1.16 Working with KSD contents

The following actions can be performed with the KSD contents:

1. Delete ICA-connection.
2. Set the "Make default" status for the ICA-connection.
3. Establish connection with Citrix-server.

6.1.17 Deleting ICA-connection from the KSD

To delete ICA-connection from the KSD do the following:

1. Launch the application.
2. Select current KSD from the *Key Storage Device Reader*.
3. In the appearing list of ICA-connections in the *Key Storage Device content* select the ICA-connections and click the **Delete** button**.**

6.1.18 Setting up the "Make default" status for the ICA connection

To set up the "Make default" status for the ICA connection, do the following:

1. Launch the application.
2. Select current KSD from the *Key Storage Device Reader*.
3. Use the appearing list of ICA-connections in the *Key Storage Device content* to select the ICA-connection (not first in the list) and press the **Make default** button**.** The selected connection will move to the top of the list.

6.1.19 Connecting to a Citrix server

In order to connect to a Citrix server do the following:

1. Launch the application.
2. Select active KSD from the *Key Storage Device Reader.*
3. Press **Connect to…**button**.** The ICA-connection having the "Default connection" status

will be used.

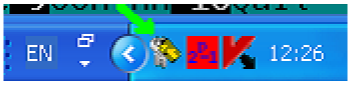
4. To connect to any other Citrix server, select the ICA connection from the *Key Storage Device content* and press the **Connect to…**button**.**

After you perform all mentioned above actions, the connection with the Citrix server will start (using the ICA-connection details stored on the KSD).

Note: After successful connection to the Citrix server, the connection stored on the KSD will not be deleted automatially from the list of ICA connections (Custom ICA Connections).

6.1.20 Switching between management mode and monitoring mode

To switch the application from management to monitoring mode, press **Minimize** in the main window**.** After this, the application icon will appear in the system tray**.**



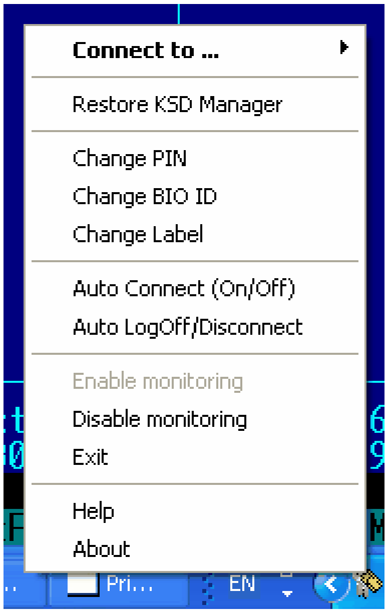
6.2 Working with Dekart Logon for Citrix ICA Client in monitoring mode

6.2.1 Launch the application in monitoring mode

- After installation of DLCIC the application appears in the Startup Menu. Therefore, upon starting your computer, the application will automatically launch in monitoring mode.
- The user may also launch the application in monitoring mode by double-clicking the mouse button on the desktop icon.
- If you installed the program on a Flash disk, you can run it by accessing this folder:

<Flash-drive>\Dekart\Logon for Citrix ICA Client\ICALogon.exe.

Upon successfully launching the application in monitoring mode, the user will be prompted to enter the PIN code (if required), after successful verification of the PIN code, the program icon will appear in the system tray. If you right-click the mouse button on the icon, you will then see the list of allowed actions.

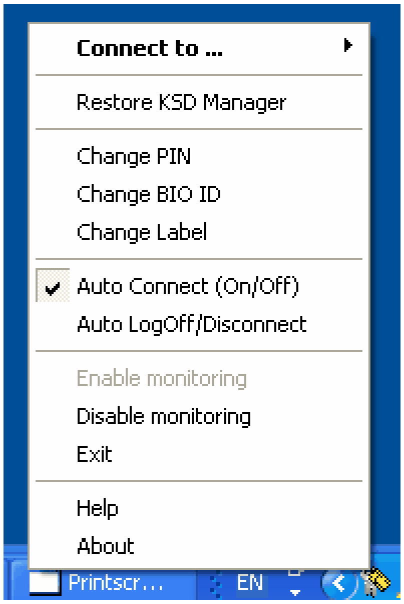


Note. In the simple mode of DLCIC "Restore KSD Manager" is disabled.

6.2.2 Setting the automatic connection mode

When the software detects the insertion of the KSD it can be set up to provide automatic connection with Citrix server using the ICA-connection having the "Default" status:

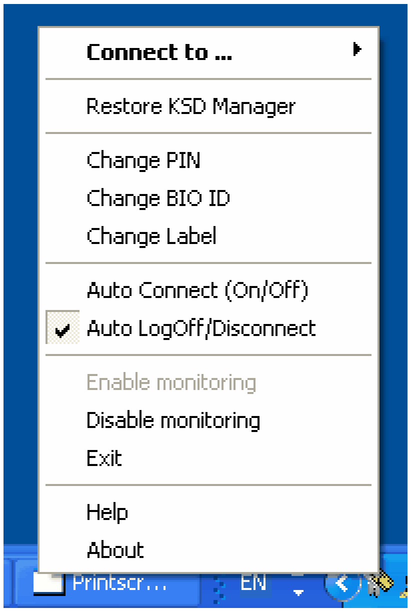
1. Right click the program icon in the system tray on your taskbar.
2. Left-click the **Auto Connect** field in the appearing pop-up window. The **Connect** field will now be deactivated.



6.2.3 Configuring the disconnection from Citrix-server behavior

To configure the application to LogOff from Citrix server on the KSD removal event (you will need to finish all tasks and close open applications on the server before logging off) do the following:

1. Right click on the icon in the system tray.
2. In the appearing popup window with the list of available actions select the **Auto LogOff** field**.**
   Note: Before performing the LogOff procedure, please, close all open application windows to eliminate potential data loss.



If the **Auto LogOff** option is not enabled, the KSD removal will trigger a disconnection from Metaframe (**Disconnect**). If the Citrix server is configured to continue session even if the connection is lost, the session will last until the next connection or server reboot.

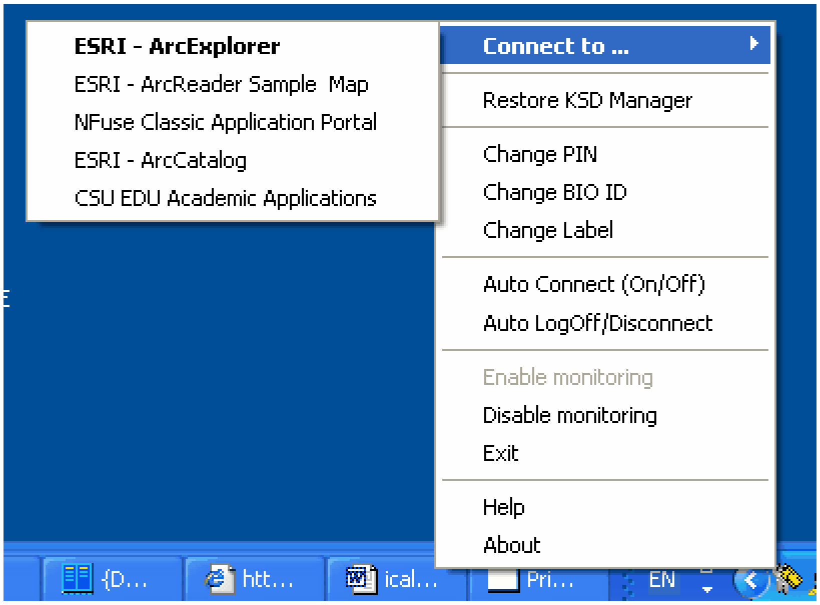
Note. This option will be available only if the Citrix server is preconfigured to continue session on disconnection.

6.2.4 Connecting to Citrix Server

After launching the application in monitoring mode, do the following to connect to the Citrix server:

First method

- Right click the application icon in system tray.
- Select **Connect to…**in the appearing pop-up menu.



- Select the desired ICA-connection in the appearing list of connections.

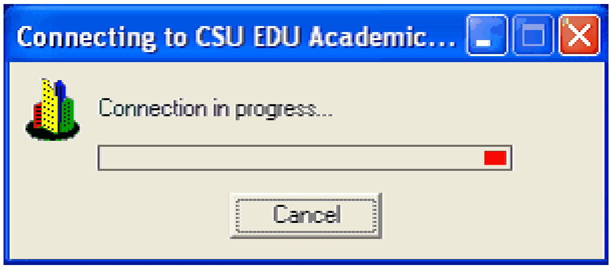
<u>Second method</u>
Left click twice to select the application icon on the desktop.

<u>Third method</u>
Left click twice to select the application icon in system tray.

<u>Fourth method</u>
If the user has set up the automatic connection mode, then the connection is established immediately after the KSD is connected to the computer and the user gets successfully authenticated (two-factor or three-factor authentication).

Note: all methods except the first one use the ICA-connection having the "Default" status

After these actions, the Citrix connection progress window will appear.


Connecting to CSU EDU Academic...

Connection in progress...

Note1: Several connections with Citrix servers can be simultaneously established if there are several ICA connection details stored on the KSD.
Note 2: After successfully connecting to Citrix server(s) the ICA connections stored on the KSD will be deleted from the Citrix ICA Connection list, if this has not been previously

done.

6.2.5 Disconnecting from Citrix-server

In order to disconnect from the Citrix-server, the user needs only to disconnect the KSD from the computer. The type of disconnection (LogOff or Disconnect) is determined by the Citrix server configuration and the selected DLCIC mode.

Note: Before performing the LogOff procedure, please, close all open application windows to eliminate potential data loss.

6.2.6 Switching from monitoring mode to management mode

When DLCIC runs in monitoring mode, the user may require changing the parameters of the ICA-connection, which requires that he switches the application to management mode. To switch to the management mode, do the following:

- Right click the application icon in system tray.
- In the menu that appears, select **Restore.**

After these actions, the application window will appear.

6.2.7 Changing PIN code

To change the PIN code in the monitoring mode, do the following:

- Right click the program icon in the system tray.
- Select Change PIN in the appearing popup menu. Follow the istructions as described Changing the PIN code (Working with Dekart Logon for Citrix ICA Client in management mode).

6.2.8 Changing the KSD Label

To change the the KSD label in the monitoring mode, do the following:

- Right click the program icon in the system tray.
- Select **Change Label** in the appearing popup menu. Follow the istructions as described Changing the label for KSD (Working with Dekart Logon for Citrix ICA Client in management mode).

6.2.9 Changing Biometric Identifier

To add and/or change user's biometric identifier on the KSD in the monitoring mode, do the following:

- Right click the program icon in the system tray.
- Select Change BIO ID in the appearing window. Follow the istructions as described in Adding BIO ID to the KSD to add the BIO ID to the KSD, and Changing BIO ID to

change the biometric identifier of the user (Working with Dekart Logon for Citrix ICA Client in management mode).

6.2.10 Changing work modes (temporary disabling of the monitoring mode

In order to temporarily disable the monitoring mode behavior, namely the connect/disconnect behavior on KSD insertion/removal event, the user will require to switch the monitoring mode off. To disable the monitoring mode, do the following:

- Right click the application icon in system tray.
- In the menu that appears, select **Disable monitoring.** The **Enable monitoring** field of the menu will become active (now the **Disable monitoring** field is inactive).

To enable the monitoring mode again select the **Enable monitoring** field in the pop-up menu. The **Disable monitoring** field of the menu will become active (now the **Enable monitoring** field is inactive).

Part VII

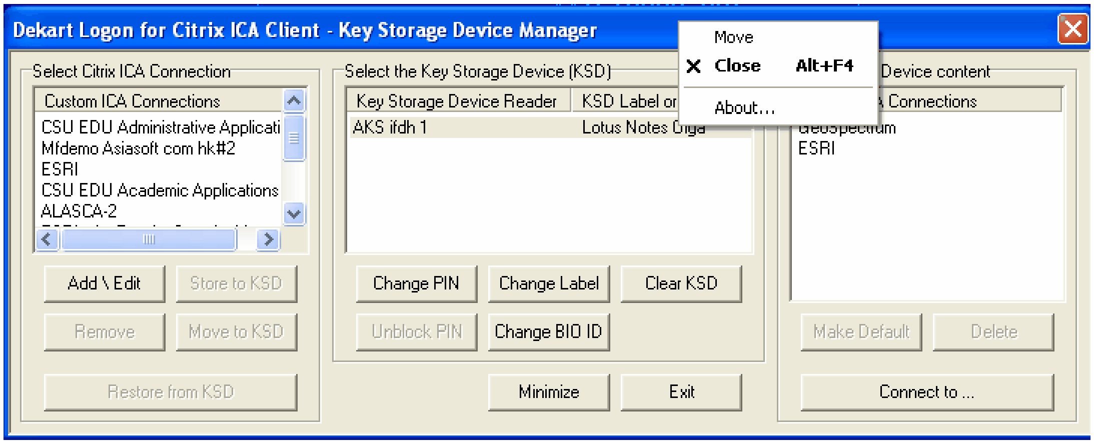
7 Additional information

7.1 Biometric authentication in Dekart Logon for Citrix ICA Client

If the three-factor authentication is enabled (the **Enable Biometric ID verification** checkbox checked in the **Change Biometric ID** window), the biometric authentication will be required after the user launches **DLCIC,** and the PIN for the **KSD** is successfully verified (if the user has set the PIN protection for the KSD)**.** The software will automatically read the biometric templates stored on the KSD and will offer the user to provide his biometric data (scan the fingerprints, speak the authentication phrase etc.). In case the BIO ID provided by the user is not identical with the templates stored on the KSD, the user will be required to repeat the biometric authentication. Authentication routine will be finished only when the data provided by the user will be identical to the biometric templates stored on the KSD. The biometric approach ensures that only authorized user can get access to Citrix-server. Thus, even if the KSD is lost or stolen, no unauthorized user will get access to Citrix server.

7.2 Viewing information about Dekart Logon for Citrix ICA Client

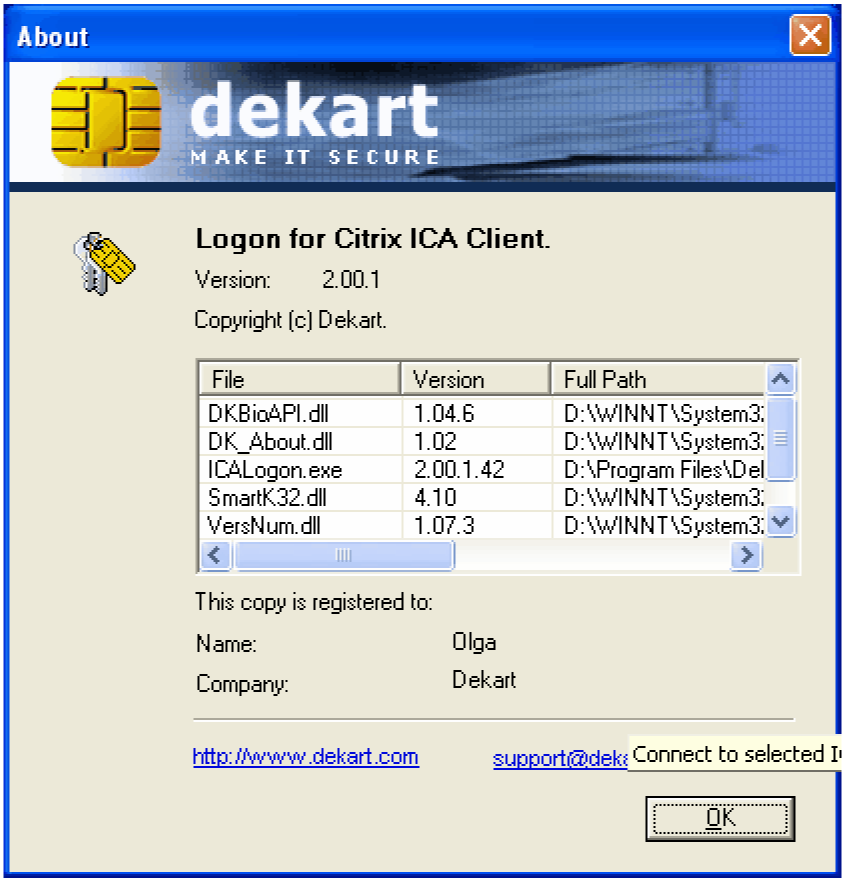
Management mode
In order to view information about the application press **F2** or right-click the mouse in the active window heading.



A menu will appear, in which you should select **About,** *About Dekart Logon for Citrix ICA Client* will appear on your screen. If the user is using an un-registered version of the application then the window *About Dekart Logon for Citrix ICA Client* will appear as it does in Registering Dekart Logon for Citrix ICA Client.

Monitoring mode
In order to view information about the application, select **About.** The *About Dekart Logon for Citrix ICA Client* window will then appear.
Note: If the user is using an unregistered copy of the application, then the window About Dekart Logon for Citrix ICA Client will appear as shown in Registering Dekart Logon for

Citrix ICA Client.



Logon for Citrix ICA Client.

Version: 2.00.1

Copyright (c) Dekart.

File	Version	Full Path
DKBioAPI.dll	1.04.6	D:\WINNT\System3
DK_About.dll	1.02	D:\WINNT\System3
ICALogon.exe	2.00.1.42	D:\Program Files\Del
SmartK32.dll	4.10	D:\WINNT\System3
VersNum.dll	1.07.3	D:\WINNT\System3

This copy is registered to:

Name: Olga

Company: Dekart

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

7.3 Using context Help

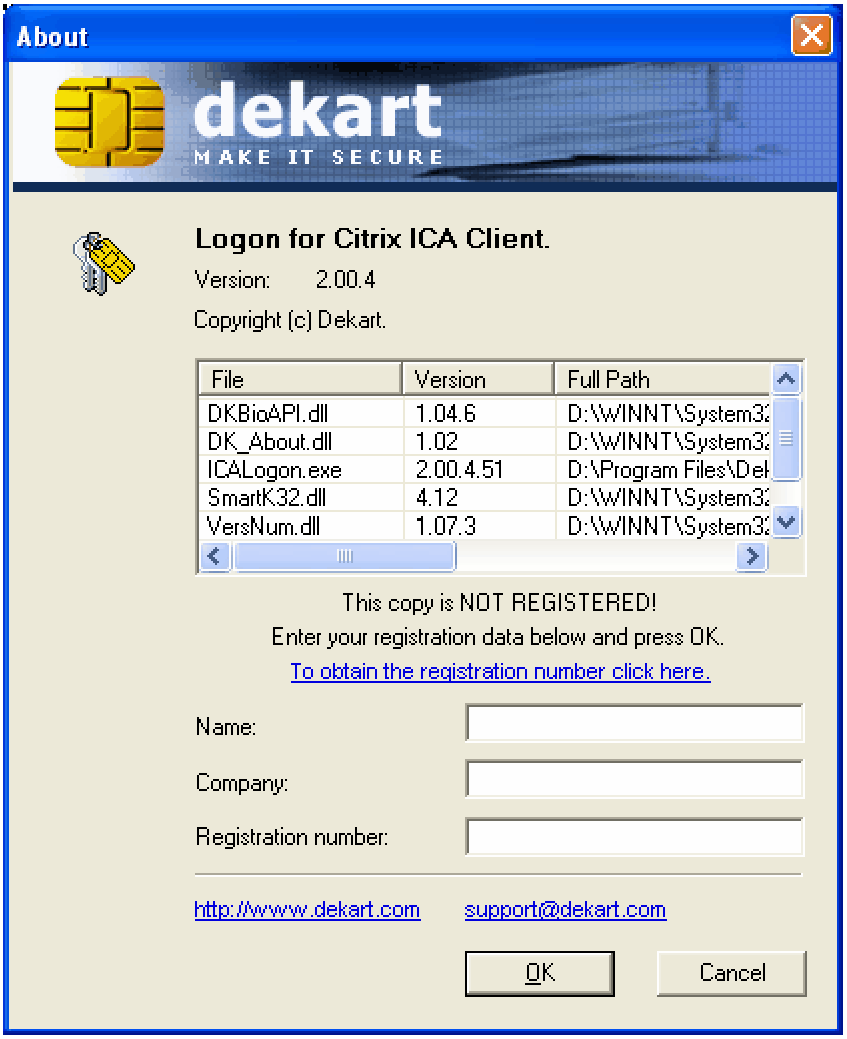
To view the help articles with the information about software functions, do the following:

- Click the **?** icon in the window header (BorderIcon).
- Drag the cursor with the question mark to the required element in the Key Storage Device Manager window and click to view the context help of DLCIC.

Or drag the cursor to the required element in the popup menu and press **F1**.

7.4 Registering Dekart Logon for Citrix ICA Client

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



Logon for Citrix ICA Client.

Version: 2.00.4

Copyright (c) Dekart.

File	Version	Full Path
DKBioAPI.dll	1.04.6	D:\WINNT\System32
DK_About.dll	1.02	D:\WINNT\System32
ICALogon.exe	2.00.4.51	D:\Program Files\Del
SmartK32.dll	4.12	D:\WINNT\System32
VersNum.dll	1.07.3	D:\WINNT\System32

This copy is NOT REGISTERED!

Enter your registration data below and press OK.

To obtain the registration number click here.

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

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 to your 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.

7.5 Running application from command line

The application can be started using the following commands:

Running management mode: <path>\ICALogon.exe
Running monitoring mode: <path>\ICALogon.exe/M

<path> - full path to the directory (folder), specified during the step 7, when installing Dekart Logon for Citrix ICA Client.

7.6 Troubleshooting

Error message	**Possible reason**	**User action**
Key Storage Device is not formatted for Citrix ICA Client Logon	KSD (smart-card or USB Token) not formatted for DLCIC.	It is necessary to use a KSD formatted for DLCIC. ***Registered customers can download the Key Formatting utility by providing the registration number for Dekart Logon for Citrix ICA Client at*** Download ***(please, use Internet Explorer browser to access the restricted download area).***
ATTENTION! Bad PIN code was entered!	Wrong PIN code was entered.	It is necessary to repeat the operation, and enter the correct PIN code. **Attention! Multiple incorrect PIN code entries will result in blocking of the KSD!**
Key Storage Device is blocked	The KSD is blocked after the maximum of allowed attempts has been exceeded.	In order to un-block the KSD it is necessary to follow un-blocking instructions. «Un-blocking the KSD» (key **Unblock PIN**) or contact your administrator. **Attention! If during the un-blocking operation, the incorrect PIN code is entered, the KSD will be permanently blocked!**
KSD is not blocked yet	User presses **Unblock PIN** button but KSD is not blocked yet.	No actions are required. «Un-block KSD» (key **Unblock PIN**) since KSD is not blocked.
Confirm PIN does not match	During PIN code change, the entries did not match.	It is necessary to repeat the operation, and ensure that both PIN code entries match.
PIN length must be at least 4 symbols	The entered PIN code is less than four characters.	It is necessary to repeat the operation, and enter the proper length PIN code.

Citrix ICA Client is not installed.	The computer does not have Citrix ICA client installed.	It is necessary to install Citrix ICA Client
Error working with Key Storage Device	An error has occurred while working with the KSD	It is necessary to repeat the operation. In the event the problem persists, please contact the administrator.
Error writing data to the KSD (Not enough free space on KSD)	An error has occurred while writing data KSD. Most likely cause is not enough free space on the KSD.	The user should use Dekart Key Manager (or similar utility) to free space on the KSD.
ICA Connection is not selected	The operation cannot be completed because not ICA connection has been selected.	Using the mouse, select a valid ICA connection, and repeat the process.
Biometric verification failed!	The BIO ID provided by the user is not identical with the one stored on the KSD.	Repeat biometric verification procedure.
Error copy of file ...	An error has occurred while installation product to KSD. Most likely cause is not enough free space on the KSD.	The user should check the KSD
Removable device is not found. Enable at least one and try again	An error has occurred while installation product to KSD.	It is necessary to insert Flash disk and try again

ICA Client and iKey driver interaction problem

When iKey is installed on an existing ICA client device, the following error message appears when attempting a connection to the MetaFrame server: "ICA Client Error 1043: Invalid Parameter"

Cause

Rainbows' interaction with Citrix and its' USB support, is outlined in USB Support in MetaFrame Products. Installing the Rainbow SmartCard driver creates four virtual USB ports.

Resolution

Modify the iKey driver installation to have only one virtual reader.

Note: Only one iKey can be used on the system at any one time.

1. Uninstall the iKey driver using Add/Remove Programs.

2. Restart your system.

3. Install the iKey driver from the command prompt using the parameters shown below:
Ikeydrvr -a VR=ON READERS=1

4. Restart your system.

More Information
For additional information, visit the Rainbow Web Site at Rainbow Technologies.

7.7 Exiting Dekart Logon for Citrix ICA Client

In order to exit from DLCIC and to remove the application from memory it is necessary to:

- Right-click the application icon in the system tray.
- In the menu that appears, select **Exit.**

Index