COPYRIGHT

DISCLAMER

Dekart, Inc. 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, Inc**. 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, Inc**. makes no representations or warranties with respect to any Dekart RSA Cryptographic Provider software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, **Dekart, Inc**. reserved the right to make changes to any and all parts of Dekart RSA Cryptographic Provider 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, INC. TRADEMARK ATTRIBUTIONS

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

DEKART, INC. CONTACT INFORMATION

		Headquarters	**European Regional Office**
Address:		Dekart, Inc. 6 Curlew Place Massapequa, NY 11758 United States	Dekart, B.V. Jan Rebel Straat 44 1069 CC Amsterdam, The Netherlands
Voice:		+1 516 541 5065	+31 20 667 0168
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	

TRADEMARKS

Trademarks of third party

Bull is a registered trademark of Bull Group.

ChipDrive is a trademark of Towitoko Inc.

eToken is a trademark of Aladdin Knowledge Systems.

iKey is a trademark of Rainbow Technologies.

Hewlett-Packard is a registered trademark of Hewlett-Packard, Inc.

Intel and Pentium are registered trademarks of Intel Corporation.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

Multiflex, Payflex and Cryptoflex are trademarks of Schlumberger.

CONTENTS

Preface

Dekart RSA Cryptographic Provider (**CSP**) is a software and hardware system incorporating a cryptographic core designed for integration into the user's applications, and a set of miniature personalized keys — smart cards or **eToken***/**iKey*** USB keys. The cryptographic core implements encryption algorithms using private encryption keys, and is stored in a smart card or a USB key and enables encrypting and decrypting data, as well as generating digital signatures and verifying their authenticity.

Operating Guide Purpose

This *Operating Guide* is designed for **Dekart RSA Cryptographic Provider** users. It describes in detail installing and operating **Dekart RSA Cryptographic Provider**.

User Proficiency Requirements

Dekart RSA Cryptographic Provider expands Windows* PC cryptographic capabilities providing additional encryption tools designed for ready integration with the user's applications to ensure information security. There are two types of product users:

- An administrator who installs **Dekart RSA Cryptographic Provider** and enables it to operate with applications.
- A standard user of Windows applications who wants the product to routinely protect information.

Operating Guide Structure

This Guide consists of the following chapters and an appendix:

- Chapter 1 *Introducing Dekart RSA Cryptographic Provider* describes the purpose and the features of **Dekart RSA Cryptographic Provider** and its integration with the USB keys and smart cards.
- Chapter 2 *Dekart RSA Cryptographic Provider Software and Hardware Requirements* lists and describes PC software and hardware required for **Dekart RSA Cryptographic Provider** to operate properly as well as the product software and hardware requirements.
- Chapter 3 *Hardware Installation, Setup, and Inspection* describes how to setup the hardware product components (smart card reader, USB port, **eToken/iKey** devices, etc.) and check their operability.
- Chapter 4 *Dekart RSA Cryptographic Provider Installation/Update and De-Installation* describes in detail how to install, update, and de-install the product and its auxiliary components.
- Chapter 5 *Operating Dekart RSA Cryptographic Provider* describes in detail product management and operation.
- Chapter 6 *Troubleshooting* is devoted to detecting and eliminating possible problems in product operation. All diagnostic messages and events causing them are listed, and troubleshooting measures are suggested.
- Glossary is an explanatory dictionary containing important terms used in this Guide.

Documentation Conventions

New terms, key concepts, and guides' chapters and sections are *italicized* in this Guide.

In this Guide, the *greater than* (>) symbol is used to separate operations within one action.

Interface elements are ***bold-faced and italicized***.

An asterisk (*) denotes the trademark of a third party.

To distinguish between the user possessing a smart card or the USB key and a common computer user, the former is defined as a *secured user* in this Guide. The *secured user* is the user possessing the smart card or the USB key and utilizing **Dekart RSA Cryptographic Provider**.

Operation of **Dekart RSA Cryptographic Provider** is based upon the use of electronic identifiers, such as USB keys and smart cards, which are functionally analogous to one another. To avoid excessive repetition of a long term *eToken/iKey/smart card*, a short-cut universal term *electronic key* or simply *key* is used in this Guide. When the *eToken* or *iKey* key is specifically mentioned, the *USB key* term is used, when the private cryptographic key for data encoding is specifically mentioned, the *private key* term is used.

Documentation Set

This *Operation Guide* is a part of the following documentation set shipped together with **Dekart RSA Cryptographic Provider**:

- *Quick Start Card (QSC)* designed to help the user to quickly prepare **Dekart RSA Cryptographic Provider** for operation.
- The *Operating Guide* is designed for **Dekart RSA Cryptographic Provider** users.

How to Contact Dekart

To order the products, information on the products, technical support, etc., please contact Dekart.

- **Customer Services**

  To order **Dekart RSA Cryptographic Provider** or request additional information, refer to Dekart:

Telephone:	+1 516 797 0693	+31 20 667 0168
E-mail:	sales@dekart.com	

  address your mail to:

  Dekart, Inc.
  6 Curlew Place
  Massapequa, NY
  11758
  United States

  Dekart, B.V.
  Jan Rebelstraat 44
  1069 CC Amsterdam,
  The Netherlands

- **Technical Support**

  For technical support on **Dekart RSA Cryptographic Provider**, refer to:

Telephone:	+1 516 797 0693	+31 20 667 0168
E-mail:	support@dekart.com	

Comments and Feedback

Please mail your comments and feedback regarding any aspects of using **Dekart RSA Cryptographic Provider**, including your remarks about the hardware, software, or documentation to the following address: info@dekart.com.

Chapter 1. Introducing Dekart RSA Cryptographic Provider

This chapter describes the following:

- **Dekart RSA Cryptographic Provider** purpose and features, principle security concepts in the area of electronic message exchange, using public communications links, and the main aspects of product operation.
- **Dekart RSA Cryptographic Provider** integration with electronic keys — the **eToken***and **iKey*** devices and smart cards; the benefits of this hardware and software system shared use for information access control.

Dekart RSA Cryptographic Provider Purpose and Features

Why Is Information Security Necessary?

Globalization and mobility are the characteristic features of modern business. On the one hand, today's business consolidates more and more sites, branches, and partners all over the world, and on the other hand, more and more employees have to work away from the office. Therefore, the present-day economy is based on the real-time cooperation of people by means of the e-mail systems and other Web services. The Web has expanded globally due to its availability, reliability and openness. But it is this availability and openness that make Web information security a crucial issue. There is no total security from computer viruses spreading through the Web, hackers, or infringement of e-mail privacy – unauthorized viewing or falsifying of electronic messages.

Another important feature of the modern business is its comprehensive transition to paperless technologies encouraged by the use of corporate computing networks and the Web itself. Business intensification contributes to the increase in the flow of important documents between parties. When the paper-based technology was used, the important paper documents were printed on special forms protected like banknotes, signed, and sometimes sealed by the sender. Sealed envelopes and responsible postal officers also contributed to the protection of important documents from being stolen or falsified. The paper itself provided *document integrity control* — it was very difficult to alter the words of a paper document or paste anything into it. The form, the signature and the seal provided the *document authenticity and authorship control*. If a dispute concerning the document's integrity, authenticity, or authorship arose, the unique personal handwriting features could be verified to establish its validity.

Traditional paper, forms, signatures, and seals do not fit into the present-day electronic documents circulation. But such old problems as *document integrity, authenticity, and authorship control* still remain. These problems have to be tackled anew, now by special electronic means. For example, *document integrity control* can be provided by encrypting documents using certain check sums; its *authenticity and authorship control* can be enabled with a unique digital signature.

It is often difficult for an addressee to check whether an e-mail was composed and sent by the person, on whose behalf it was mailed. There is no guarantee that the received file has not been read by a third party during transmission, which is unacceptable for documents containing classified commercial information. Electronic documents are prone to inconspicuous alterations resulting in a conflict between the sender and the addressee of a message.

To solve the above mentioned problems of electronic document circulation, a *special security technology* must be applied. It must ensure that:

- The transmitted data's confidentiality is maintained.
- The sender has a unique identity.
- The message is secure from unauthorized alterations.
- There is a technique to correctly resolve conflicts.

Tasks one, two, and three are accomplished by means of cryptographic data protection capabilities, task four is settled by special electronic messaging exchange regulations between sender and addressee.

In Web transactions authenticity and authorship control, forms, handwriting, signatures, and seals are replaced by digital signatures and digital certificates. The *Digital Signature* is an equivalent of a hand-written signature. This is a special encrypted set of digital data used both to sign documents and uniquely identify the sender of the electronic message. The digital signature is not the inherent property of the person who originated the message. It should be acquired from a Certification Authority that will arbitrate all disputes that may arise concerning the authenticity and authorship of documents.

Certificates and Certification Authorities

To acquire a personal certificate, it is necessary to apply to the *Certification Authority*. Depending on the scale and significance of communication between the sender and the addressee, the following organizations can serve as a Certification Authority:

- A special department-wide, nation-wide, or world-wide organization. In that case, the Certification Authority verifies the identity of an applicant, generates and sends the certificate back to the applicant in the form of a file or a digital document.
- Special corporate network software automatically assigns unique digital certificates to the authenticated users. In that case, the corporate network administrator should resolve all disputes concerning the authenticity and authorship of the documents signed with such certificates.

The acquired certificate will serve to identify you as uniquely as your DNA structure does, but, unlike your DNA structure, your can change this digital code at any moment. In much the same way, as you can use several paper documents to identify yourself — a passport, driver's license, or an authentication card — you can also use several digital certificates for self-identification. One, for example, can be used for communications inside the company, another — for external mail, and the third — for private mail.

The digital certificate must conform to a certain standard: it must contain a *subject public key* and the digital signature of its *issuer*. The certificate also contains its owner's additional identifying information, certificate expiration date, and the terms of use.

Currently, the certificates based on the third version of the International Telecommunication Union ITU-T X.509 standard and the IETF (Internet Engineering Task Force) RFC 2459 recommendations are used most often.This is a basic technology used in Windows 2000 public key infrastructure.

When the user requests a certificate, a *key pair* is generated: the *public key* and the *private key*. The public key is then transmitted to the Certification Authority and entered into the users certificate. The secret private key pairs-up the public key and enables the *asymmetric key* cryptographic information security. The Public Key Infrastructure defines the principles of information security. This infrastructure was developed for the present-day electronic document circulation systems designed for common users.

Encryption and *Digital Signature* are among the most important techniques of cryptographic data protection. Both techniques employ transforming computer files containing the documents.

- **Encryption.** With respect to computer data representation, both keys represent symbol strings used by the corresponding software to encrypt, decrypt, digitally sign the documents, and verify the digital signature. The symbol strings are so generated that only the owner of a pair private key can decrypt the document, encrypted with a corresponding public key. While the public key is distributed among all prospective correspondents, the personal private key should be kept secret. If the e-mail sender encrypts the document with the open key of a certain addressee, only that very addressee will be able to read the encrypted document. Encryption hides the document contents from everyone except the addressee, thus accomplishing the first task: ensuring correspondence confidentiality.
- **Digital signature.** Digital Signature helps to accomplish two other tasks: the signature uniquely verifies the document authorship and protects its contents from distortion. To digitally sign the document, its author's private key is used by the signing software. As a result, the signed document will contain an additional string with information on both the document contents and its author's private key. After receiving this document and obtaining the sender's public key, the addressee can use digital signature analysis software to establish whether the signature actually belongs to the document author (who is the sole owner of the private key) and whether the signed text has been altered after signing (whether the signature itself complies with the signed document).

Certificates provide reliable connection between the public key and the corresponding private key holder. The Certification Authority ensures connection between the subject public key and the subject identification information stored in the certificate. Thereby, the fourth task is accomplished — should a conflict arise, the digitally signed electronic document can be presented as proof ad litem.

The document author should first sign the document (using his/her personal *private key*), encrypt it (with the *public key* of an addressee), and then mail it. The addressee will first decrypt the document (with his/her personal *private key*) and then check the authorship and integrity of a document (using the sender's *public key*).

In Windows, all these operations are performed by the *cryptographic service provider certified by Microsoft** that is used for information protection, excluding information containing state secrets.

Cryptographic Service Providers

In Windows 95 and higher, information protection is based on *Microsoft CryptoAPI* unified cryptographic interface. This interface allows to fully implement data presentation and exchange according to the international recommendations and Public Key Infrastructure. Cryptographic functions are implemented in separately shipped cryptographic modules called *Cryptographic Service Providers* (CSP) that can be accessed via CryptoAPI by any Windows application. Cryptographic Service Providers are required to create and store encryption keys including digital certificate private keys.

Currently, Cryptographic Service Providers are most often used to protect e-mails transmitted in the *S/MIME* format (*Secure Multipurpose Internet Mail Extensions*) recommended for use with such algorithms as SHA-1, RC2, etc.Cryptographic Service Providers can have various capabilities, for example, they can implement highly complex algorithms or support additional hardware.

CryptoAPI supports the following standard Windows applications:

- Microsoft Internet Explorer
- Microsoft Outlook Express
- Microsoft Outlook 2000
- Microsoft Internet Information Server
- Microsoft Office XP

Enhancing Security

Imagine some ill-intentioned third party gaining access to your computer. No doubt, their first wrongdoing could consist of trying to read your encrypted mail and imitating your digital signature thus compromising your good name and passing all of your confidential information to your competitors. This will be possible only if they manage to obtain your private keys. Therefore, remember to take care of your security yourself. While handling the digital certificates for encrypting/decrypting documents, the cryptographic service providers also ensure that the private keys are stored securely, so that a third party could never obtain them. Usually, the certificate private key is protected with a password that has to be entered from the keyboard to authenticate the certificate holder.

Authentication is a control process that checks the authenticity of the users identity, i.e. this process controls whether the user is the person they say they are.

This password is requested every time the user sends a digitally signed message or opens an encrypted e-mail. In theory, using this approach ensures that only the legitimate owner of a certificate is able to operate the corresponding private key. In fact, the key is available to anybody who has gained knowledge of the password by either, spying, intercepting, or cracking it.

More and more companies consider the standard *one-factor* authentication not reliable enough to authorize the use of digital certificates. Therefore, they add more rigorous security requirements and replace the standard *one-factor* authentication with so-called strong authentication. *Strong authentication* is based on two factors:

1. *Something you know*: for example, a symbol string used as a password or a PIN.
2. *Something you have*: for example, a special electronic device that enables a system to verify whether it is present or not while signing or decrypting a digital document. These are electronic keys such as smart cards and USB keys that have these properties.

This type of authentication is also called *two-factor authentication*. The strong two-factor authentication is the type of authentication provided by **Dekart RSA Cryptographic Provider**. It enables you to store the certificate private key in the memory of a smart card or a USB key. To sign or decrypt an electronic document with that certificate, both the smart card or the USB key and the identification PIN are required. This is the feature that ensures your private key safety and, consequently, your right to secure correspondence: a third party will not be able to send a message on your behalf or read your confidential mail even after logging on to the system under your user name.

Integration with Electronic Keys

The main feature of **Dekart RSA Cryptographic Provider** is its close integration with hardware authentication devices – such as the smart cards and USB keys described below.

What is a Smart Card?

A **smart card** is a plastic card with an embedded microchip that implements encryption algorithms — tools for encrypting and decoding of secret information — by means of its hardware. It is a handy, compact, and resilient device that can be stored in your pocket or wallet.

The smart card is equipped with an embedded integrated circuit including its own processor, permanent *Read Only Memory (ROM)*, dynamic *Random Access Memory (RAM)*, and nonvolatile *Electrically Erasable Programmable Read-Only Memory (EEPROM)*. Each card stores its identification number, controller type information, serial number, various access keys, and it also contains encryption algorithm implementation hardware for data encrypting/decoding within the card.

Flexibility, thickness, and the dimensions of a smart card are specially selected to protect it from physical damage and make its storage and application more convenient.

Depending on the application, there are several types of smart cards — memory smart cards, designed mainly for data storage and microprocessor-equipped multifunctional smart cards possessing their own operating and file systems.

A smart card can only be applied if a special device providing information input and output is available — the Smart Card Reader that must be connected to the computer with its driver installed into the operating system. Readers are usually manufactured in two variations: external and internal. An internal reader occupies a vacant 3.5" slot of a computer (a floppy disk drive occupies the same 3.5" slot). Connecting the reader to the computer does not require special skills and does not take more than 3 to 5 minutes. Several port types are used to connect smart card readers to desktop and laptop computers — COM, USB, PS/2, PCMCIA, IRDA, etc.

The number of smart card and reader manufacturers is big, therefore a standard *ISO 7816* containing the list of requirements to the physical properties of the readers and smart card information exchange protocols was developed by the *International Organization for Standardization (ISO)* to provide compatibility. On its basis, a task group representing a number of companies (Groupe Bull*, Hewlett-Packard*, Microsoft, Schlumberger*, Siemens* Nixdorf, etc.) suggested its own manufacturing standard for smart cards and readers — *Personal Computer/Smart Card (PC/SC)* specifications. These are the smart cards and readers complying with this standard that **Dekart RSA Cryptographic Provider** supports.

One smart card can be used for work with several applications, including those of different vendors. Generally, the application itself finds the required data in the memory of a smart card or starts the corresponding processes within the card. The only limitations are the type of smart card and the capacity of its available random access memory.

Smart cards are inserted into the reader similarly to inserting a floppy disk into the corresponding disk drive, and they do not require any additional installation in Windows. However, the smart card readers do require preliminary installation and reader driver setup in the system. The reader driver is a program module implementing the interaction of a smart card with applications.

The area of application of smart cards is not limited by information access control. Presently, they are prevalent in electronic payment systems and mobile telephony. Most smart cards look similar, but the embedded microchips are not all the same. They can differ in memory capacity, computational ability, the number of implemented encryption algorithms, and, certainly, in their price.

Individual user information and a unique 32-bit serial number (smart card identifier) pre-set at the manufacturing stage are stored in the memory of the smart card. This identifier can be used to authenticate the card owner in various purpose security systems such as client-bank systems, eCommerce systems, etc.

For more information about smart cards and readers, please refer to the Web sites of their respective vendors. For example, for information about Schlumberger* smart cards and readers, please refer to http://www.slb.com/smartcards/.

What is a USB Key?

The **USB key** is the first full-scale analog of a smart card manufactured in the shape that lends itself to being put on a key ring. It is encased in a water-resistant plastic shell and can be connected to the computer by means of the USB port. Several makes of monitors and keyboards are also equipped with this type of port. This device does not require a costly reader, as it incorporates these functions in itself. All secure information is stored in the secured memory of this key.

In addition to the identification information, these electronic devices can store other important confidential information (depending upon the model, the key memory capacity runs up to 64 Kbytes) such as encryption keys, digital certificates, etc.

Dekart RSA Cryptographic Provider supports the USB keys of two vendors:

- The **eToken** key from Aladdin Knowledge Systems.

There are several types of the **eToken** keys designed for different applications and differing in their functionality — **eToken R2**, **eToken PRO**. For more information about the **eToken** key family, please refer to the Web site of Aladdin Knowledge Systems at: http://www.eAladdin.com. Both **eToken R2** and **eToken PRO** can be used with **Dekart RSA Cryptographic Provider**.

- The **iKey** electronic key from Rainbow Technologies.

The **iKey 20xx** series electronic keys from Rainbow Technologies are functionally analogous to the **eToken PRO** keys, but they differ in protected memory capacity — 8 KB for **iKey 2000** and 32 KB for **iKey 2032**.

For more details on the **iKey 20xx** series, refer to http://www.rainbow.com. The **eToken** and **iKey** USB keys comply with most of the present-day standards and *Application Programming Interfaces (API)* including the *PC/SC* specifications. A special extension cord can be used to facilitate inserting the USB key by extending the USB port onto the front panel of the computer.

Individual user information and a unique 32-bit serial number pre-set at the manufacturing stage are stored in the memory of the USB key equipped with a microprocessor module with the special (encrypting) algorithms implemented on-board. This identifier can be used to authenticate the key owner in a variety of security systems, such as client-bank systems, eCommerce systems, etc.

Like a smart card, the USB key can be used for work with several applications, including those of different vendors. Generally, the application itself finds the required data in the eToken memory or starts the corresponding processes. The only limitation is the capacity of its available random access memory.

Therefore, the USB key is a permanent and safe identifier for its owner, because:

- This device has no internal power supply unit, the power being supplied by means of the USB bus.
- It is encased in a water-resistant plastic shell. Secured nonvolatile *Electrically Erasable Programmable Read-Only Memory (EEPROM)* is used in the USB key for data storage. The memory data is destroyed when the USB key shell is unsealed.
- Secured memory data storage time exceeds 10 years.

The **eToken** and **iKey** are USB devices, designed for Windows 95 OSR2.1, Windows 98, Windows Me, Windows NT*/2000/XP. Each of them requires a driver — a program managing input and output and interfacing the applications and operating system on the one part and the key on the other.

The **eToken** driver is supplied as a part of **eToken Runtime Environment** (**RTE**), an execution environment, which must be installed on every computer where there is an **eToken** user. (Windows NT does not support USB devices, therefore, a special **eToken** driver has been developed for this operating system).

For more information about the **eToken** key and the **RTE**, please refer to the Web site of Aladdin Knowledge Systems at http://www.eAladdin.com.

The **iKey** driver is supplied as a part of a separate **Rainbow iKey Driver** installation package, which must be run on every computer where there is an **iKey** user.

For more details on the **iKey** electronic key and its driver, please refer to the Web site of Rainbow Technologies at http://www.rainbow.com.

Initializing the Electronic Keys

All of the electronic keys purchased for use with **Dekart RSA Cryptographic Provider** (smart cards or USB keys) are subject to mandatory formatting with a special utility from **Dekart**. Formatting does not in any way damage the information previously recorded onto this key. Only a number of additional records (special auxiliary files) required for **Dekart** software are written into the memory of the key. Software will use these files to store its data. All previously recorded auxiliary files from **Dekart** are erased and their new versions are created.

Note: Electronic keys purchased directly from **Dekart** are pre-formatted with a special utility.

Note: If an electronic key was not purchased from **Dekart**, please refer to **Dekart** technical support service to format the key with a utility from **Dekart**. Otherwise, the software will not be able to use this key.

Dekart RSA Cryptographic Provider Licensing Management

All software purchased together with **Dekart RSA Cryptographic Provider**, including the product itself, must be registered in the database of **Dekart**. After registering the product, the user is assigned a registration number used for obtaining **Dekart RSA Cryptographic Provider** updates and new versions as well as technical support from **Dekart**.

The registration form is available:

1. in printed form in the product box,
2. in digital form on the product CD,
3. at the Web site of **Dekart** at http://www.dekart.com.

The following means of registration are available:

1. The serial number and the registration form, both printed and in digital form, accompany each product purchased in a box. Software purchased in this fashion has no limitations. All of its functionality is readily available to the user after entering the serial number during the product installation. However, registration with **Dekart** is necessary to have the opportunity to obtain new versions of software and technical support. The software owner must fill out the registration form with the following information: the serial number indicated on the box or on the product CD, their name, country, and e-mail are also required. After the form is completed, the user should mail it to the technical support service either by post, or by e-mail, or from the **Dekart** Web site. The registration number will be e-mailed to the user after the registration is completed.
2. The product user is registered automatically after filling out the payment card if the product is purchased on-line. The registration number is e-mailed to the user. Software obtained from the **Dekart** Web site will not operate without this registration number.
3. In certain cases, the registration number can be found in the product box.

Note: If necessary, the user can be registered by a regional representative by prior arrangement.

Note: The user must provide their registration number every time when contacting **Dekart** technical support service and purchasing new versions of software or other products from **Dekart**.

Electronic Key Compatibility with Dekart RSA Cryptographic Provider and Other Products

Confidential data stored in the memory of an electronic key can be additionally protected with a special password — the Personal Identification Number, (PIN). In addition, every product using the electronic key can allocate their own PIN. The PIN can be altered by the user at their discretion by means of special product functions. The PIN provides a very important additional security means: a third party will be unable to take advantage of acquiring the electronic key without knowing its PIN. Even though its encrypted hash value is stored in the electronic key, it can not be transformed into its initial form.

Smart cards and the **eToken PRO** keys also have a high-level PIN initially pre-set by the key manufacturer to **1234567890**.This code can be employed by the products using electronic keys for confidential data access control and can be altered by means of the **RTE** (if the **eToken PRO** keys are used). Do not change this code needlessly.

The user can select to use or not to use the PIN with **Dekart RSA Cryptographic Provider** and smart cards/**eToken Pro**. **Dekart RSA Cryptographic Provider** sets its own PIN for these keys which is independent of the high level PIN. The electronic keys purchased together with **Dekart RSA Cryptographic Provider** have an empty default PIN.

If the **eToken R2** or **iKey** are used, **Dekart RSA Cryptographic Provider** employs the high level PIN, which is initially pre-set to **1234567890** for **eToken R2** and **12345678** or **PASSWORD** for **iKey**. The **iKey** electronic keys purchased together with **Dekart RSA Cryptographic Provider** initially have an empty PIN. The **eToken R2** key PIN cannot be empty. It is recommended that the initial PIN be changed shortly after product installation and the key owner registration. The PIN must comply with the following requirements:

- It must contain 1 to 8 alphanumeric symbols for smart cards or the **eToken PRO/iKey** electronic keys or 4 to 64 alphanumeric symbols for the **eToken R2** keys. Remember that the PIN is case-sensitive.

- It must be sufficiently complex (to make spying and guessing it more difficult).
- It must be easy to remember. If the user forgets their PIN, they will fail to open the door to the treasury of information, and the electronic key will become worthless.

Dekart RSA Cryptographic Provider supports **Muitiflex***, **Payflex***, and **Cryptoflex*** smart cards from Schlumberger*, readers complying with the *PC/SC* specifications, and the following makes of the USB key: **eToken R2**, **eToken PRO** from Aladdin Knowledge Systems and **iKey 2000**, **iKey 2032** from Rainbow Technologies.

How Does Dekart RSA Cryptographic Provider Protect Information?

To use **Dekart RSA Cryptographic Provider** effectively, take the following preparatory steps:

1. Study this Guide thoroughly.
2. Obtain an electronic key. Every such key (a USB key or a smart card) is unique, therefore, you cannot use your colleague's key. Keep your key safe, do not lose or damage it. Without it, you will not be able to use your certificate to sign or decrypt an electronic document. Do not entrust your key to anyone, always keep it with you in your wallet (good for smart card). You could also, for example, attach it to your key-ring together with the keys to your home or car (good for the USB key).
3. Prepare the computer. The preparation consists of installing the product onto the PC.
4. Select and set up one or more certificates for use with the product. If you do not have a certificate, refer to the Certification Authority or to your company network administrator. For detailed instructions on acquiring a certificate, see Chapter 5, *Operating Dekart RSA Cryptographic Provider.*
5. Set up the applications requiring strong cryptographic protection, for example, the e-mail system, for operation with the selected certificates. With these certificates, the applications will apply the encryption methods supported by the product and authenticate the user when signing and decrypting e-mails.
6. If required, set the electronic key Personal Identification Number (PIN) in the product environment to strengthen authorized access control to the certificate private key. Memorize your key PIN and do not write it down where it can be easily discovered. **Dekart RSA Cryptographic Provider** provides special utilities to change the PIN. For directions on changing the PIN, refer to Chapter 5, *Operating Dekart RSA Cryptographic Provider*. Be sure not to forget the PIN and keep it secret. If a third party finds out your key PIN and has your electronic key, they will be able to access your data.

Thereafter, you can start working with **Dekart RSA Cryptographic Provider**. It is very easy, because the product transparently implements strong protection and does not differ in any way from the cryptographic service providers you are accustomed to.

What Are the Benefits of Dekart RSA Cryptographic Provider & eToken/iKey/Smart Card Integration?

By enabling the user to additionally encrypt the private key and store it (at user's option) in either the Windows system registry or in the protected memory of a smart card/USB key, **Dekart RSA Cryptographic Provider** supplements the functionality of a usual cryptographic service provider.

Storing the private key in the protected memory of a smart card/USB key boosts the security efficiency by removing confidential data from the computer's hard disk, where they can be stolen. In this instance, all sensitive data resides inside a key-ring-style device or a plastic card which can be taken away by its holder when leaving their computer.

First of all, the electronic key is an electronic identifier of its owner. Because the electronic key is a read/write-enabled device (with an encrypted data exchange algorithm), **Dekart RSA Cryptographic Provider** employs it as storage for certain sensitive and unique information used to identify you as the registered certificate holder. There is no need to enter the password from the keyboard to access confidential data, as long as the key is inserted into the reader, and your correspondence will be under your complete control. In this way, the second strong authentication factor is implemented — *Something You Have*, i.e. the electronic key. Sending digitally signed e-mails and opening encrypted e-mails will only be possible with the right key at hand. Unlike the key to your car, this device cannot be duplicated by a locksmith because it is a very complicated electronic device. It can only be stolen from the owner (which can hardly happen inconspicuously, as the key is required for day-to-day routine work)

Even if you lose the key, or if someone steals it from you, it will be of no use because accessing the encrypted data requires entering the PIN that only you know. This is how the first strong authentication factor is implemented — *Something You Know*.

Thus, **Dekart RSA Cryptographic Provider** integration with electronic keys (smart cards or USB keys) allows you to create and easily utilize a very reliable system with a high level of security. And remember that all of the secret information is stored in the protected memory of the electronic key.

Dekart RSA Cryptographic Provider Capabilities

Dekart RSA Cryptographic Provider has the following capabilities:

- Digital signature encryption algorithm:
    - RSA in compliance with RSA Data Security, Inc. PKCS №1 v1.5 with 384 to 16,384 bit key length range
- Data encryption algorithms:
    - DES in compliance with the National Institute of Standards and Technology, USA, NIST FIPS №46 with 56 bit key length
    - Triple DES in compliance with NIST FIPS №46 with 112 and 168 bit key length
    - RC2 in compliance with Internet Engineering Task Force IETF RFC №2268 with 1 to 128 bit key length range
    - AES in compliance with NIST FIPS №197 with 128, 192, and 256 bit key length
- Message authentication (digital signature verification) algorithms:
    - HMAC in compliance with IETF RFC №2104

    - MAC in compliance with NIST FIPS №113
- Hash function value generation algorithms:
    - MD2 in compliance with IETF RFC №1319
    - MD4 in compliance with IETF RFC №1320
    - MD5 in compliance with IETF RFC №1321
    - SHA in compliance with NIST FIPS №180
- Session key encryption algorithms:
    - RSA in compliance with PKCS №1 v1.5 with 384 to 16384 bit supported key length range
- System registry asymmetric key storage with access provided for the current computer user
- Microprocessor card or USB key asymmetric key storage protected by the key owner's personal PIN
- Supported USB key types:
    - **eToken PRO** with PIN containing 0 to 8 alphanumeric symbols
    - **eToken R2** with PIN containing 4 to 64 alphanumeric symbols
    - **iKey 2000** with PIN containing 0 to 8 alphanumeric symbols
    - **iKey 2032** with PIN containing 0 to 8 alphanumeric symbols
- Smart card readers complying with the *PC/SC* specifications are supported
- Smart cards with 0 to 8 alphanumeric symbols PIN are supported

Dekart RSA Cryptographic Provider Components

Dekart RSA Cryptographic Provider package consists of the following mandatory components:

- A CD with the application program components
- One of the following sets of electronic keys (depending upon the delivery option):
    - two smart cards from Schlumberger* **Multiflex*** (either **Cryptoflex*** or **Payflex***)
    - one or two electronic USB keys ((**eToken R2**, **Token PRO**, **iKey 2000**, or **iKey 2032**)
- *Quick Start Card (QSC)*
- An *Operating Guide*

The following optional components can also be shipped with **Dekart RSA Cryptographic Provider** package (depending upon the delivery option):

- Microsoft software for smart card support
- An **RTE** containing drivers and utilities for the **eToken** key support
- The **iKey** electronic key drivers
- Smart card reader drivers
- One of the following smart card readers:
    - Towitoko* ChipDrive* 100

  - Towitoko ChipDrive 120
  - Towitoko ChipDrive 130
  - Towitoko ChipDrive Keyboard 710
  - Towitoko ChipDrive Intern
  - Schlumberger Reflex 72
  - Schlumberger Reflex 20
  - Any other reader complying with the PC/SC specifications
- 25-pin COM port adapter
- PS/2 port adapter
- USB extension cord

Chapter 2. Dekart RSA Cryptographic Provider Hardware and Software Requirements

Dekart RSA Cryptographic Provider is a compact product integrated with the electronic keys hardware produced by third parties. It does not have any significant requirements for the computer on which it operates.

This chapter describes the following:

- **Dekart RSA Cryptographic Provider** personal computer hardware requirements.
- Operating systems (OS) with the corresponding service packs required for the product to run properly.

Personal Computer Hardware Requirements

Dekart RSA Cryptographic Provider does not have any significant additional requirements to the PC hardware. The requirements are mainly subject to the operating system used on the computer.

To install **Dekart RSA Cryptographic Provider**, the PC must be equipped with a CD-ROM drive.

For **Dekart RSA Cryptographic Provider** to run properly, a PC with the following minimum properties is required (this applies mainly to the computers running Windows 95 OSR2.1):

- Intel Pentium* 166 MHz processor
- 16 MB RAM
- Free hard disk space sufficient for the product installation (200 KB) and the **eToken* RTE** (500 KB) or **iKey*** drivers (2 MB) installation.

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

- A USB port, if a USB key or a smart card reader for the USB port is used.
- A COM port, if a smart card reader for the COM port is used.
- A PS/2 interface, if a smart card reader with the PS/2 interface is used.

One of the following hardware components is required if only the RSA Cryptographic Provider software has been purchased from **Dekart** (without electronic keys and a corresponding reader):

- The **eToken R2**, the **eToken PRO**, the **iKey 2000** or the **iKey 2032** key with sufficient free memory for auxiliary data storage.
- Smart card reader complying with the *PC/SC* specification (*Personal Computer/Smart Card* — developed by Groupe Bull*, Hewlett-Packard*, Microsoft*, Schlumberger*, Siemens Nixdorf*, etc.) connected to the computer.

Personal Computer Software Requirements

One of the following operating systems is required for **Dekart RSA Cryptographic Provider** to run properly on a PC:

- Windows*95 OSR2.1
- Windows 98 SE
- Windows Me
- Windows NT* 4 Workstation, Server with Service Pack 6
- Windows 2000 Professional, Advanced Server with Service Pack 3 or higher
- Windows XP Professional, Home Edition

If the electronic keys have been purchased separately from **Dekart RSA Cryptographic Provider**, for example, as a part of a different product, then one of the following software components must be installed on the PC:

- **eToken** key software — **RTE** (**eToken Run Time Environment**) version 2.65 or higher. The latest version of the **RTE** software can be downloaded from Aladdin Knowledge Systems Web site at http://www.eAladdin.com.
- ***Microsoft Windows Installer*** (*MSI*) is required to install the **RTE** under Windows 95/98/NT. It permits the system to run the MSI files (this is the format of the *RTE* installation module). It can be downloaded from http://support.microsoft.com/downloads/.
- **iKey** software — **Rainbow iKey Driver** set version 3.4.0 or higher.
- The smart card reader software for the corresponding Windows OS (the drivers and utilities set). For more details and new versions of software, refer to the vendor of the reader or to the Web site of the company producing the readers.

Chapter 3. Hardware Installation, Setup, and Inspection

The main goal of this chapter is to explain to the user how to connect the **eToken*** and **iKey*** USB keys and smart card readers to the computer, setup the equipment, inspect it, and use electronic keys with **Dekart RSA Cryptographic Provider**.

This chapter can be omitted if the electronic keys and the corresponding equipment listed in the section *Dekart RSA Cryptographic Provider Components* of chapter 1, *Introducing Dekart RSA Cryptographic Provider*, have already been used with the computer.

Note: To avoid problems during the smart card reader/USB key installation, it is recommended that the electronic key software (drivers, utilities) be installed prior to attaching the reader/USB key to the computer (if this equipment has not been installed previously for some other products). For more details on these software products installation, refer to chapter 4, *Product Installation, Update, and De-Installation*.

This chapter describes the following:

- How to setup the USB port.
- How to setup the USB key and connect it the computer.
- How to setup the smart card reader and connect it to the computer.

USB Port Settings Check

USB Port BIOS Settings Check

The *Universal Serial Bus (USB)* can be used to connect and disconnect peripheral devices without opening the PC case and even without shutting down the computer. The USB automatically detects these devices and configures the corresponding software. Naturally, the OS supporting the USB ports must be installed on the computer for the USB to operate properly.

Up to 127 peripheral devices can be connected to the USB at the same time. USB hubs are used for connecting multiple devices. USB hubs are special devices used to amplify the signal and provide a power supply for peripheral devices.

The standard USB port type A is required to connect the USB key or the smart card reader with the USB interface to the computer. Several makes of monitors and keyboards are equipped with this type of the USB port. A special USB extension cord (shipped separately) can serve to facilitate using the USB port by placing it on the front panel of the computer.

Before using the USB key or the smart card reader with the USB interface, be sure that the ***BIOS*** (*Basic Input/Output System*) settings of this computer allow using the USB functions. The procedure of checking these parameter settings in the *BIOS Setup Utility* can differ depending on the computer manufacturer and the **BIOS** in use. For more details on checking **BIOS** settings, refer to the user manual for this computer. For example, if the *AwardBIOS Setup Utility* is used, do the following after turning the computer on:

1. Press ***Del*** to enter the *BIOS Setup Utility* (for directions on starting this utility, refer to the computer manual).
2. Select ***Advanced*** by pressing the ***Right Arrow*** key. Press ***Enter***.
3. Select ***PCI Configuration*** by pressing the ***Down Arrow*** key and open it with ***Enter***.

4. Find the ***USB Function*** element on the ***PCI Configuration*** menu and make sure that it is ***Enabled***. If it is ***Disabled***, enable it by pressing the ***Enter*** key and the ***Arrow*** keys.
5. Press ***ESC*** to exit the ***Advanced*** menu, select ***Exit***, and press ***Enter***.
6. Press ***Enter*** to save the changes.

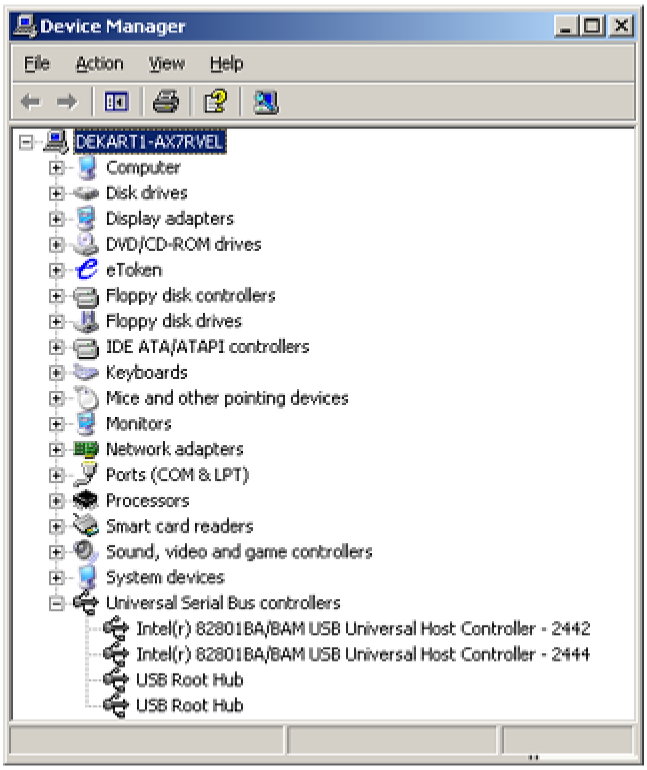
USB Port OS Settings Check

After checking the *BIOS* USB function settings, make sure that the USB support is installed for the Windows* operating system, too.

Note: Windows 95 was not designed to utilize the USB port and it will not work with it, even if the computer is equipped with this port and the *BIOS* settings confirm this. To make USB work, replace Windows 95 with Windows 95 OSR2.1.

Under Windows XP Professional, do the following to check if the USB port is used.

1. Right-click My Computer > Properties > Hardware > Device Manager.
2. The ***Device Manager*** window will appear, as shown in Figure 1, with the list of the system devices. Make sure that the ***Universal Serial Bus Controllers*** section containing the ***USB root Hub*** element is present in this list.



DEKART1-AX7RVEL
- Computer
- Disk drives
- Display adapters
- DVD/CD-ROM drives
- eToken
- Floppy disk controllers
- Floppy disk drives
- IDE ATA/ATAPI controllers
- Keyboards
- Mice and other pointing devices
- Monitors
- Network adapters
- Ports (COM & LPT)
- Processors
- Smart card readers
- Sound, video and game controllers
- System devices
- Universal Serial Bus controllers
  - Intel(r) 82801BA/BAM USB Universal Host Controller - 2442
  - Intel(r) 82801BA/BAM USB Universal Host Controller - 2444
  - USB Root Hub
  - USB Root Hub

Figure 1. The USB is present in the Device Manager

Using the USB Key

Connecting the USB Key

The following types of the USB keys are produced by Aladdin Knowledge Systems, and can be used with **Dekart RSA Cryptographic Provider**:

- **eToken PRO** from Aladdin Knowledge Systems with the embedded *SLE66C Infineon* smart card chip and *Siemens CardOS/M4* operating system
- **eToken R2** from Aladdin Knowledge Systems with the embedded *CY63141* chip emulating a smart card chip
- **iKey 2000** from Rainbow Technologies with the embedded *Philips 858* smart card chip and *Datakey DKCCOS v5* operating system
- **iKey 2032** from Rainbow Technologies with the embedded *Philips 5032* smart card chip and *Datakey DKCCOS v6* operating system

All listed keys can be connected to the USB port of a computer. They have the same functionality in relation to **Dekart RSA Cryptographic Provider**.

Do the following before attaching the USB key to the computer:

- Check the USB port BIOS settings (as described above in *USB Port BIOS Settings Check* section).
- Check the USB port Windows OS settings (as described above in *USB Port OS Settings Check* section).
- Install the **RTE** that contains drivers and utilities to support the **eToken** keys or install the **iKey** drivers. For installation directions, refer to the corresponding section of chapter 4, *Dekart RSA Cryptographic Provider Installation, Update and De-Installation*.

Next, attach the electronic key to the USB port.

Note: The USB port is asymmetric. Therefore, the key should be attached to the USB port only in a certain position and you should not attempt to force it in the upside-down position to avoid damaging the port or the key. Attach the USB key carefully, avoid inserting it at an angle.

If the USB key drivers have been installed on your system, the LED indicator must start glowing after attaching the **eToken** or the **iKey** electronic key to the port, which means that it is ready to work.

Installing the USB Extension Cord for the eToken/iKey

In many cases the USB port is located on the back panel of the computer. Because of this the USB port is difficult to access, which makes using the USB key inconvenient. To solve this problem, using a USB extension cord is recommended. This is a special extension cord shipped by many companies, including **Dekart**. Several types of extension cord are produced with a special suction cup, which facilitates attaching it to the monitor or elsewhere.

If the USB port is located on the keyboard or the monitor, the extension cable may be unnecessary.

If the USB socket is located on the monitor, make sure that it is connected to the USB port of the computer by means of a standard *type A – type B* cord.

Do the following to install the USB extension cord:

1. Attach the USB connector of the cord to the USB port.
2. Place the sticker (shipped with the cord) in a convenient place, for example, on the computer case.
3. Press the cord suction cup to fix it onto the smooth surface of the sticker.

Disconnecting the USB Key

To disconnect the USB key from the USB port, detach it from the socket carefully.

The key is meant for 5000 connection/disconnection cycles, therefore be careful when handling it.

Connecting the Smart Card Reader

One of the following smart card readers can be used with **Dekart RSA Cryptographic Provider**:

- Towitoko* ChipDrive* 100
- Towitoko ChipDrive 120
- Towitoko ChipDrive 130
- Towitoko ChipDrive Keyboard 710
- Towitoko ChipDrive Intern
- Schlumberger* Reflex* 72
- Schlumberger Reflex 20
- any other reader complying with the PC/SC specifications,

Depending upon the model, the reader is attached to the computer by means of one of the following three ports:

- The COM port (if the number of pins of the plug and the socket do not match – 25 or 9 – the adapter is required). The connector and the adapter for the corresponding reader are shown in Figure 2.

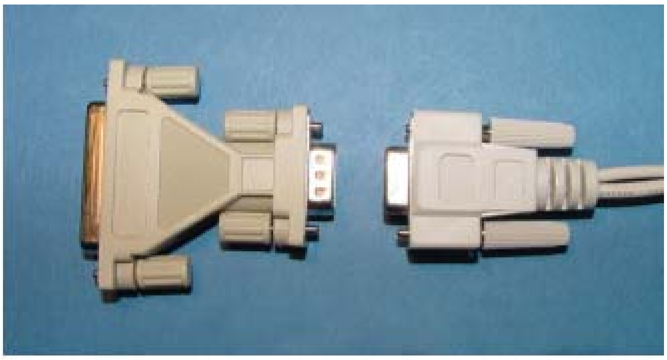


Figure 2. The COM reader interface

- The PS/2 port (the outlet socket can be used to connect the mouse or the keyboard). The connector for the corresponding reader is shown in Figure 3.

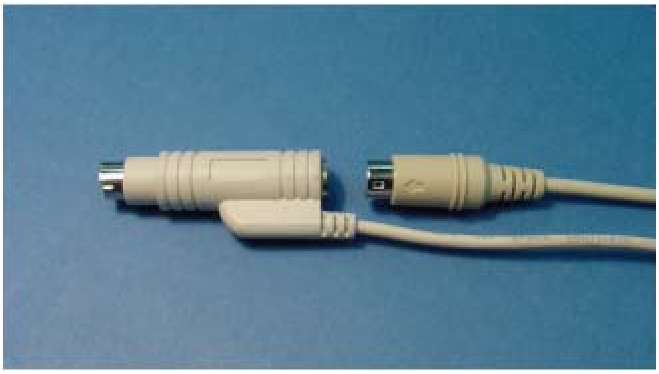


Figure 3. The PS/2 reader interface

- The USB port. The connector for the corresponding reader is shown in Figure 4.

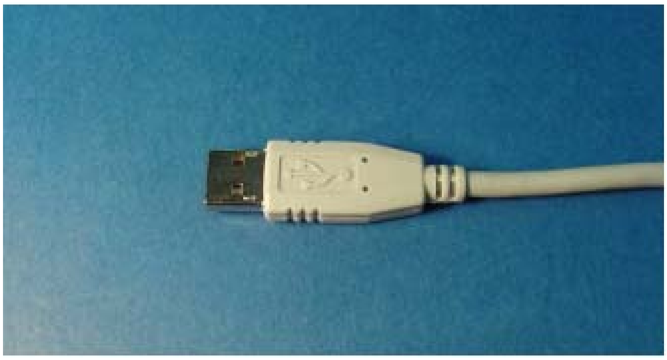


Figure 4. The USB reader interface

Note: For details on connecting and utilizing the reader and smart cards, refer to the manuals shipped with this equipment. Follow the corresponding directions.

Connecting the Reader with the USB Interface

Do the following before connecting the reader to the computer:

- Check the USB port **BIOS** settings (as described above in *USB Port BIOS Settings Check* section).
- Check the USB port Windows OS settings (as described above in *USB Port OS Settings Check* section).
- Install the reader's drivers and utilities. If the smart card reader is shipped together with **Dekart RSA Cryptographic Provider**, then all of the drivers and utilities required for it are located on the product CD. For newer versions of these software products, refer to the Web site of the corresponding reader manufacturer.

For directions on its installation, refer to the corresponding section of chapter 4, *Product Installation, Update and De-Installation*.

Be careful when attaching the smart card to the USB port, avoid inserting at an angle.

Note: The connector should be attached to the USB port only in a certain position and should not be inserted upside-down to avoid damaging the port or the connector.

The OS may have to be rebooted after attaching the reader. Windows OS with *Plug-and-play* functionality (Windows 98, Windows 2000 Professional, Windows XP, Windows Me) will detect and recognize the connected reader automatically.

Note: Windows 2000 can fail to detect the reader with the USB interface after restart; the computer should be restarted again.

Disconnect the reader from the USB port only if the USB configuration is modified. To do so, detach the USB connector of the reader from the port.

For more details on connecting and disconnecting the USB smart card reader, refer to the operating manuals shipped with the reader.

Connecting the Reader with the COM or PS/2 Interface

Connecting the smart card reader with the PS/2 or COM interface is carried out as shown in Figures 2 and 3.

Note: Connect and disconnect the smart card reader with the PS/2 or COM interface only when the computer is shut down.

After connecting the reader, restart the computer and boot the OS. Windows OS with *Plug-and-play* functionality (Windows 95, Windows 98, Windows 2000 Professional, Windows XP, Windows Me) will detect and recognize the connected reader automatically.

Note: Several COM readers are equipped with an autonomous power supply (or utilize the PS/2 interface). Remember to turn the power supply on at the proper time (or connect the reader to the PS/2 interface).

After connecting the reader to the computer, be sure to check whether it works properly. The LED indicator must start glowing after inserting a smart card into the reader, thus indicating that it is ready to work.

For more details on connecting and disconnecting the smart card reader, refer to the operating manuals shipped with the reader.

Operating Smart Cards

The smart card should be inserted into the reader in the same way as a diskette is inserted into a common 3.5" floppy disk drive. For convenience, every card is labeled with an arrow showing what side of the card should be inserted to the reader, the card should be inserted into the slot up to the stop.

The data exchange between the reader and the card proceeds through the metallic plate protecting the microchip embedded into the plastic wafer so that it does not protrude from the flat surface and does not obstruct the card placement. This is why the plastic cards have a very long service life. The reader wears out more quickly due to its having many moveable parts and the functions it performs when working with smart cards. The number of insertion/withdrawal cycles is limited to several thousands. Follow the rules below to make the reader last longer:

- Avoid rough movements when inserting and withdrawing the card.
- Wipe the smart card with a slightly damp napkin in order to minimize the accumulation of dust inside the reader.
- Do not remove the card from the reader when the LED indicator is flashing.

Note: For more details on working with the reader and smart cards, refer to the manuals shipped with this equipment. Follow the corresponding directions.

Chapter 4. Dekart RSA Cryptographic Provider Installation, Update, and De-Installation

Dekart RSA Cryptographic Provider should be installed onto a personal computer (PC) by an experienced Windows user (See the *User Proficiency Requirements* section in the *Preface* of this guide). Before installing, make sure that the PC meets the product hardware and software requirements indicated in chapter 2 of this guide, *Dekart RSA Cryptographic Provider Hardware and Software Requirements.*

This chapter thoroughly describes the user actions during **Dekart RSA Cryptographic Provider** components installation:

- First, the auxiliary product components are installed onto the system — the smart card reader and the USB key.
- Next, the main product components are installed.

This chapter also describes the user actions during **Dekart RSA Cryptographic Provider** update and de-installation.

Auxiliary Components Installation

This section, *Auxiliary Components Installation,* describes the installation process of auxiliary program components — the USB key (**eToken*** and **iKey***) and smart card reader drivers and utilities, that will operate on your computer.

Note: Refer directly to the section *Dekart RSA Cryptographic Provider Installation* if the electronic keys (such as **eToken**, **iKey**, or smart cards) are already used with your computer and the required software has been installed previously.

Smart Card Reader Installation

The smart card reader can operate only with the drivers for the corresponding Windows OS installed. These drivers serve as a program interface between the reader and the applications.

If the reader has been purchased independently from the product, refer to the directions and software shipped with this equipment to install the corresponding drivers. The latest version of the drivers can be obtained from the Web site of the reader manufacturer.

Note: If a smart card reader with the USB interface is used, it is recommended to check the USB functionality *BIOS* and Windows OS settings before installing the drivers (See the sections *USB Port BIOS Settings Check* and *USB Port OS Settings Check* in chapter 3 of this *Guide*).

Reader drivers shipped together with **Dekart RSA Cryptographic Provider** are installed as follows:

1. Insert the **Dekart RSA Cryptographic Provider** CD into the CD-ROM drive. The product installation module will run automatically. The installation menu will appear on the screen. If this menu does not appear, the function of automatic application running is probably disabled in your system. Enable this function and re-insert the CD or launch the SETUP.EXE module from the CD manually.
2. Select ***Install reader driver***.
3. Follow the software directions.

4. If prompted to restart the computer upon the completion of the installation, restart it and attach the reader following the directions indicated in chapter 3, *Hardware Installation, Setup, and Inspection*.
5. Check if the reader works properly. The reader LED indicator should start glowing, when the smart card is inserted, it should also flash during the data exchange.

   Note: To avoid errors, do not withdraw the card from the reader while the indicator is flashing.

   If the reader is good and properly installed, its name will appear on the computer hardware list. For example, in Windows XP Professional you can check this in the Device Manager window by taking the actions listed in the *USB Port OS Settings Check* section. If the name of the reader does not appear in the hardware list, try re-installing the driver or refer to the technical support service of the reader's manufacturer.

Go on to the main product components installation described in the *Dekart Logon Installation* section.

eToken Key Installation

The **eToken** key installation consists of two stages:

1. The **eToken** key driver installation (which is a part of the **eToken Runtime Environment**)
2. The **eToken** device attachment

eToken Runtime Environment (**RTE**) contains all tools and drivers required for the **eToken** device to work properly. Therefore, remember to install it on the **Dekart RSA Cryptographic Provider** user's computer before installing the **eToken** key.

Note: To avoid problems, do not attach the **eToken** device to the computer before installing the **RTE**. If you have unintentionally attached it to the USB port *prior to the installation* of the **RTE**, the new hardware search wizard will start in Windows OS if the new hardware automatic search function is enabled (Windows 95 OSR2.1, Windows 98/2000/XP, Windows Me). In this case, it is recommended that you terminate the new hardware search wizard, detach the **eToken** device, install the **RTE** (see above), and then re-attach the **eToken** to the USB port of the computer.

Note: It is recommended to check the USB functionality BIOS and Windows OS settings before installing the **RTE** (See the sections *USB Port BIOS Settings Check* and *USB Port OS Settings Check* in chapter 3 of this *Guide*).

The **eToken RTE** is a multipurpose software interface between the **eToken**-enabled software and the **eToken** device. This execution environment is stored as the RTExxx.MSI file (MSI Installer Database, where xxx is a version number, for instance, RTE260.MSI — version 2.60) on the product CD.

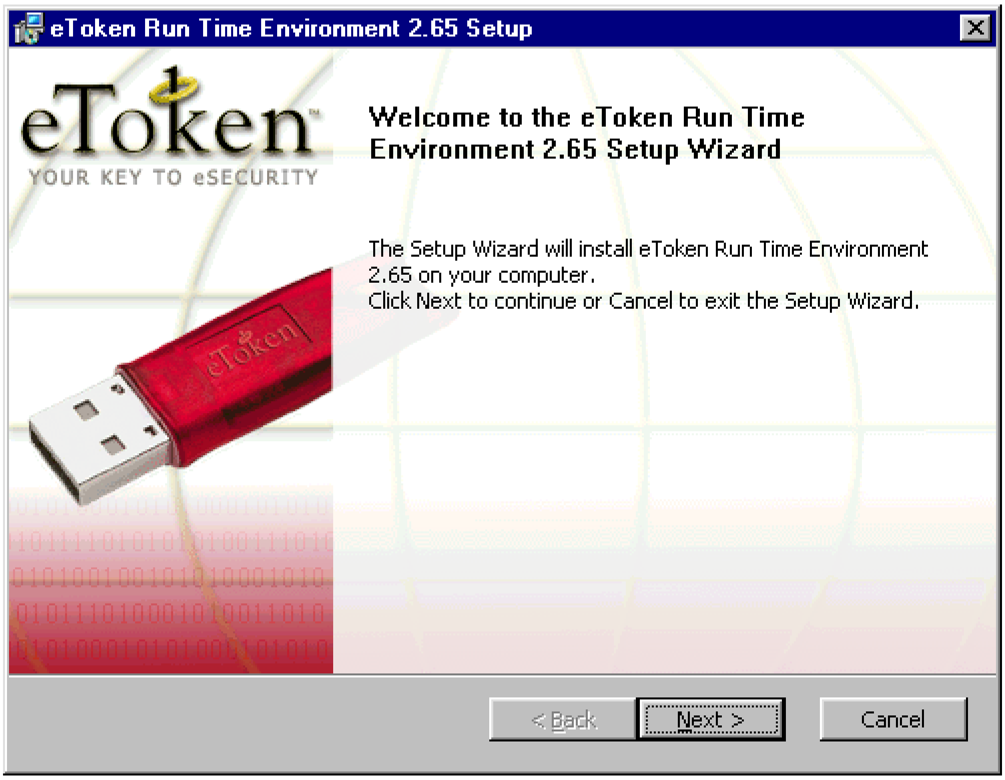
The **RTE** is installed from the MSI file supported by the *Windows Microsoft* Installer* (MSI) program. For Windows 2000/XP and Windows Me, this is a built-in tool. For Windows 95/98 and Windows NT* 4.0, it can be obtained from http://support.microsoft.com/downloads/. Under Windows 95/98 and NT 4.0, install MSI in this system prior to installing the **RTE**.

Do the following to install the **RTE** on the computer:

1. Insert the **Dekart RSA Cryptographic Provider** CD into the CD-ROM drive. The product installation module will run automatically. The installation menu will appear on the screen. If this menu does not appear, the function of automatic application running is probably disabled

in your system. Enable this function and re-insert the CD or launch the SETUP.EXE module from the CD manually.

2. Select ***Install RTE***. A welcome screen of the **RTE** installation program will appear, as shown in Figure 5.

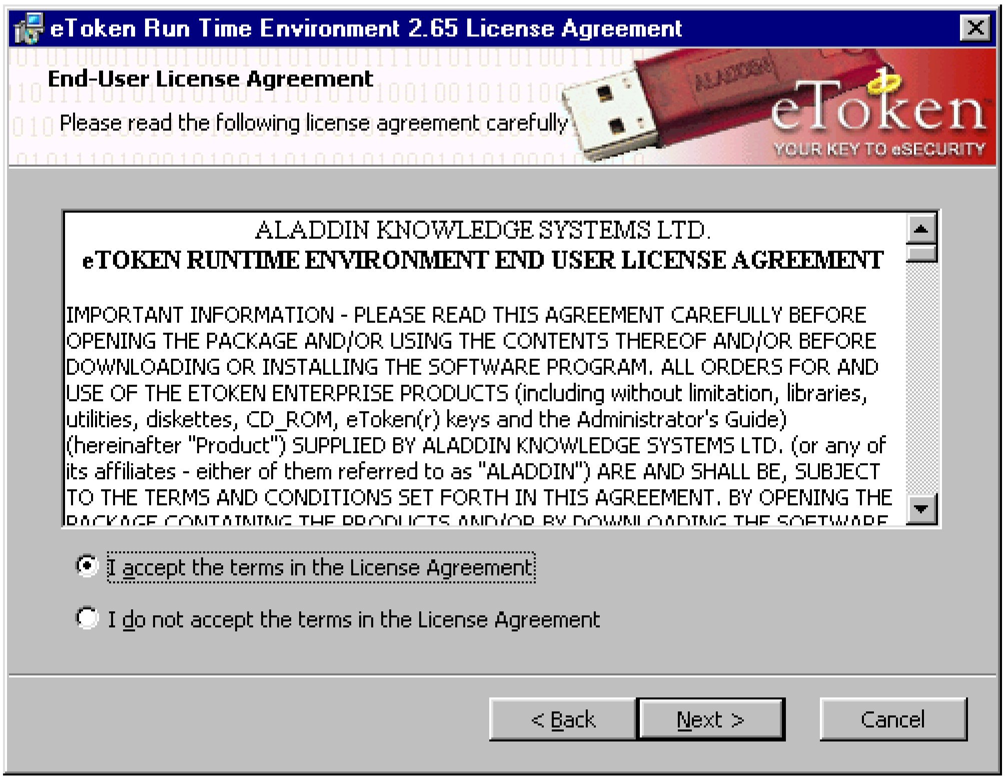


Welcome to the eToken Run Time Environment 2.65 Setup Wizard

The Setup Wizard will install eToken Run Time Environment 2.65 on your computer.
Click Next to continue or Cancel to exit the Setup Wizard.

Figure 5. Welcome screen of the **RTE** installation program

3. Click ***Next*** on the welcome screen. The License Agreement window will appear, as shown in Figure 6.



End-User License Agreement

Please read the following license agreement carefully

ALADDIN KNOWLEDGE SYSTEMS LTD.
eTOKEN RUNTIME ENVIRONMENT END USER LICENSE AGREEMENT

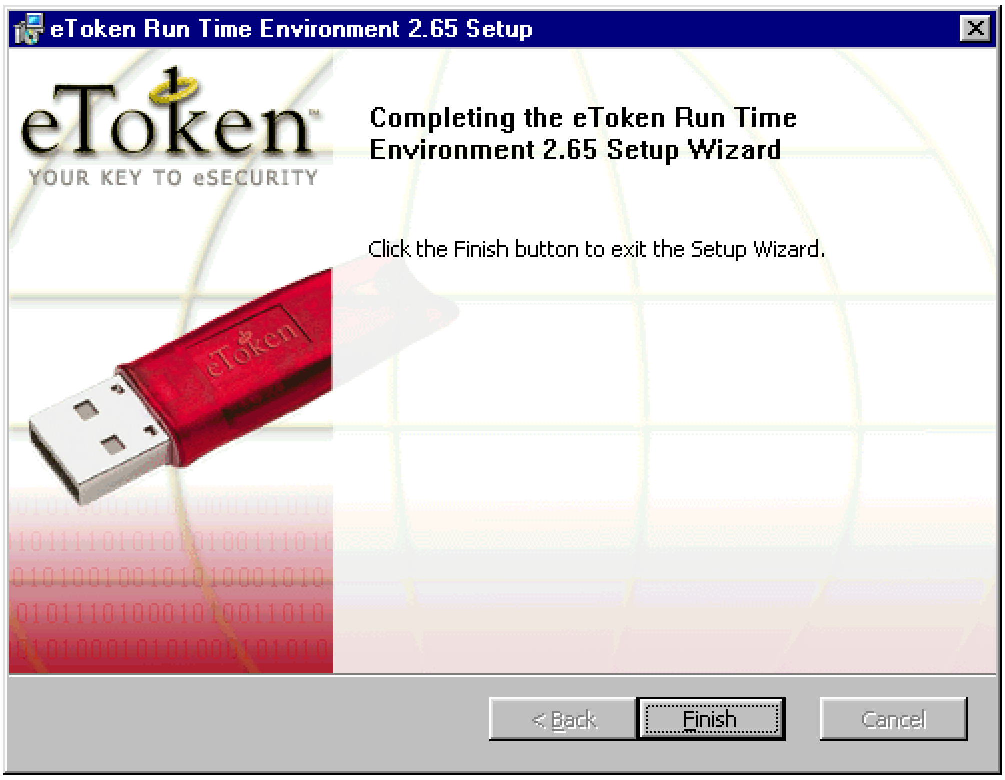
IMPORTANT INFORMATION - PLEASE READ THIS AGREEMENT CAREFULLY BEFORE OPENING THE PACKAGE AND/OR USING THE CONTENTS THEREOF AND/OR BEFORE DOWNLOADING OR INSTALLING THE SOFTWARE PROGRAM. ALL ORDERS FOR AND USE OF THE ETOKEN ENTERPRISE PRODUCTS (including without limitation, libraries, utilities, diskettes, CD_ROM, eToken(r) keys and the Administrator's Guide) (hereinafter "Product") SUPPLIED BY ALADDIN KNOWLEDGE SYSTEMS LTD. (or any of its affiliates - either of them referred to as "ALADDIN") ARE AND SHALL BE, SUBJECT TO THE TERMS AND CONDITIONS SET FORTH IN THIS AGREEMENT. BY OPENING THE PACKAGE CONTAINING THE PRODUCTS AND/OR BY DOWNLOADING THE SOFTWARE

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

Figure 6. The **RTE** ***License Agreement*** window

4. Read the text of the license agreement with Aladdin Knowledge System in the ***License Agreement*** window carefully. Select the check box ***I accept the terms in the License Agreement*** if you agree with the terms of the agreement. Click ***Next*** to proceed the installation. If you do not agree with the terms of the agreement, select ***I do not accept the terms in the License Agreement*** check box and click ***Cancel***. In this case, the **RTE** will not be installed.
5. When a ready-to-install window appears, detach all of the **eToken** devices from the USB ports and click ***Install***.
6. Wait until the installation completion window appears, as shown in Figure 7.



eToken Run Time Environment 2.65 Setup

Completing the eToken Run Time Environment 2.65 Setup Wizard

Click the Finish button to exit the Setup Wizard.

Figure 7. The **RTE** installation completion window

7. Under Windows NT, restart your computer after installing the **RTE**.
8. When the **RTE** installation is completed, attach the **eToken** device to the USB port of the computer. Windows NT requires no additional actions to install the **eToken** key. Under Windows 95/98/2000/XP OS, the attached **eToken** key will be recognized as a new device. The system device installation process will start. It will take several more minutes.
9. Check if the **eToken** key and its drivers have been installed correctly. Right-click ***My Computer*** > ***Properties*** > ***Hardware*** > ***Device Manager***.
10. Make sure that the list of hardware supported by your system contains one or more **Aladdin IFD Handler** drivers and the name of the attached **eToken** device.

    Note: An incorrectly attached or out of order **eToken** is not on the list. If the list does not contain the **Aladdin IFD Handler** driver, the installation has been unsuccessful. In this case, repeat the installation, or refer to the technical support service of **Dekart**.

The LED indicator of the **eToken** starts glowing after the installation is successfully completed. The flashing indicator means that the data exchange between the key and the computer is in progress.

Note: To avoid errors, do not withdraw the **eToken** from the port while the indicator is flashing.

Go on to the main product components installation described in the *Dekart Logon Installation* section.

iKey Installation

The **iKey** installation consists of two stages:

1. The **iKey** driver installation
2. The **iKey** device attachment

The **iKey** driver should be installed on the **Dekart RSA Cryptographic Provider** user's computer before installing the **iKey** device itself.

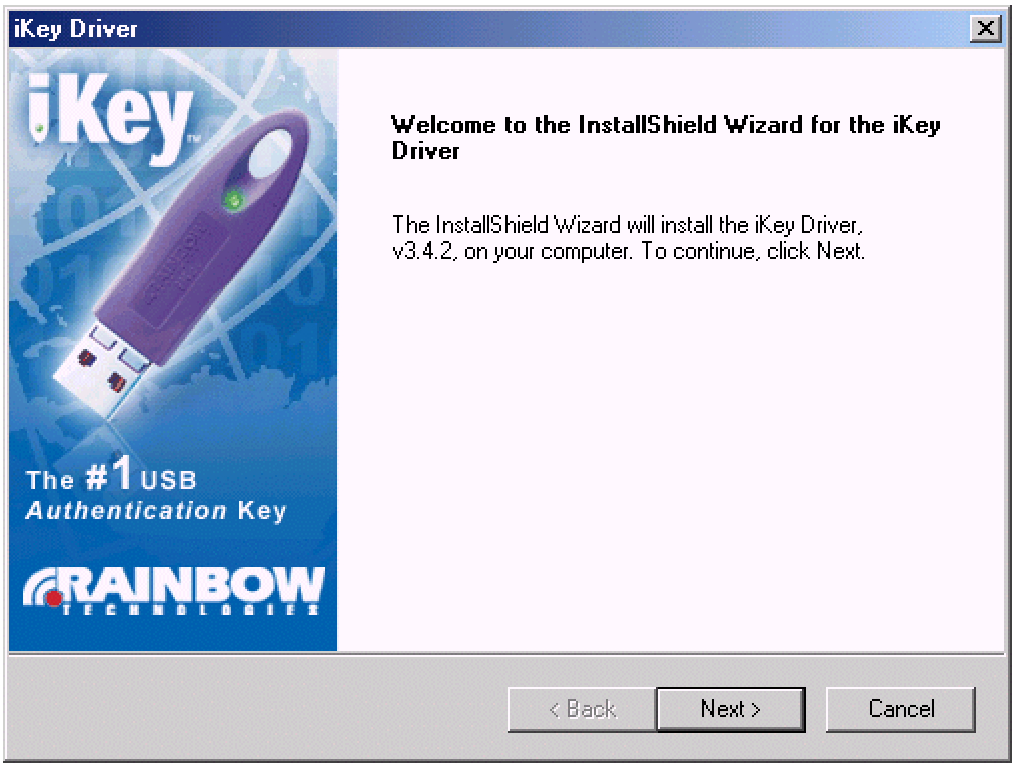
Note: To avoid problems, do not attach the **iKey** device to the computer before installing its driver. If you have unintentionally attached it to the USB port *prior to the installation* of its driver, the new hardware search wizard will start in Windows OS if the new hardware automatic search function is enabled (Windows 95 OSR2.1, Windows 98/2000/XP, Windows Me). In this case, it is recommended that you terminate the new hardware search wizard, detach the **iKey** device, install the driver (see above), and then re-attach the **iKey** to the USB port of the computer.

Note: It is recommended to check the USB functionality BIOS and Windows OS settings before installing the **iKey** driver (See the sections *USB Port BIOS Settings Check* and *USB Port OS Settings Check* in chapter 3 of this *Guide*).

The **iKey** driver is stored as the IKEYDRVR.EXE file on the product CD.

Do the following to install the **iKey** driver on the computer:

1. Insert the **Dekart RSA Cryptographic Provider** CD into the CD-ROM drive. The product installation module will run automatically. The installation menu will appear on the screen. If this menu does not appear, the function of automatic application running is probably disabled in your system. Enable this function and re-insert the CD or launch the SETUP.EXE module from the CD manually.
2. Select ***Install iKey driver***. A welcome screen of the **iKey** driver installation program will appear, as shown in Figure 8.

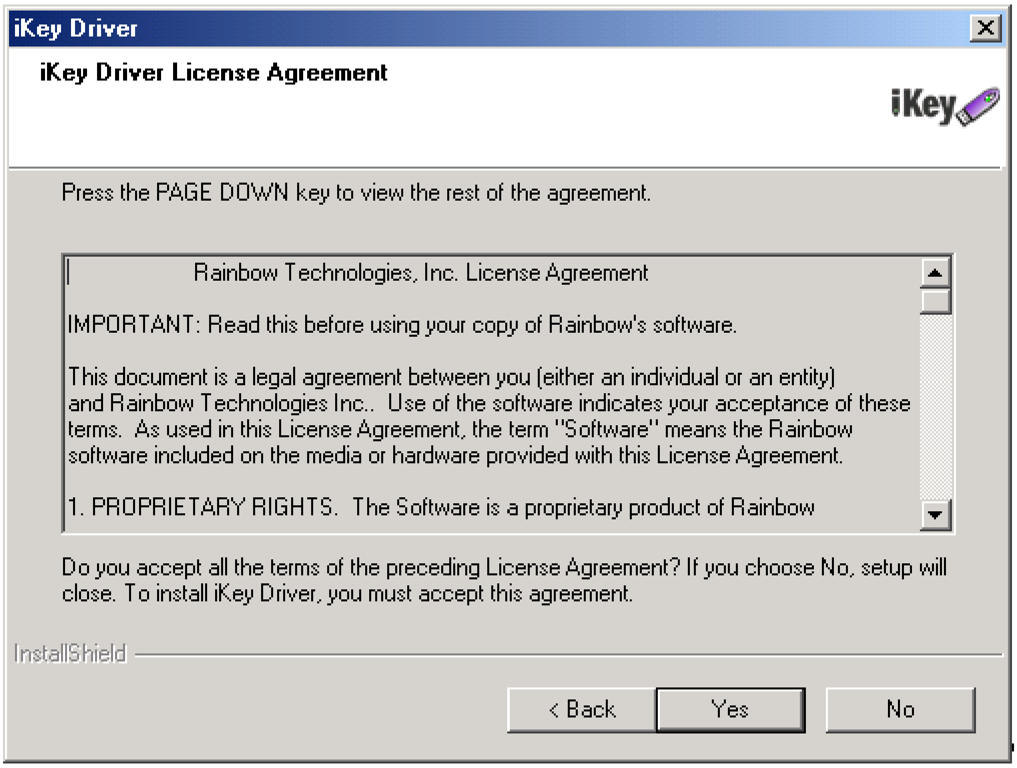


Welcome to the InstallShield Wizard for the iKey Driver

The InstallShield Wizard will install the iKey Driver, v3.4.2, on your computer. To continue, click Next.

Figure 8. Welcome screen of the **iKey** driver installation program

3. Click ***Next*** on the welcome screen. Read the information in the ***iKey Driver ReadMe*** dialog box, click ***Next***. The License Agreement window will appear, as shown in Figure 9.



iKey Driver License Agreement

Press the PAGE DOWN key to view the rest of the agreement.

Rainbow Technologies, Inc. License Agreement

IMPORTANT: Read this before using your copy of Rainbow's software.

This document is a legal agreement between you (either an individual or an entity) and Rainbow Technologies Inc.. Use of the software indicates your acceptance of these terms. As used in this License Agreement, the term "Software" means the Rainbow software included on the media or hardware provided with this License Agreement.

1. PROPRIETARY RIGHTS. The Software is a proprietary product of Rainbow

Do you accept all the terms of the preceding License Agreement? If you choose No, setup will close. To install iKey Driver, you must accept this agreement.

Figure 9. The ***iKey Driver License Agreement*** window

4. Read the text of the license agreement with Aladdin Knowledge System in the ***License Agreement*** window carefully. Click ***Yes*** if you agree with the terms of the agreement. If you do not agree, click ***No***. In this case, the **iKey** driver will not be installed.

5. Wait until the installation program prompts you to attach the **iKey** device and attach it to the USB port of a computer. Windows NT requires no additional actions to install the **iKey**. Under Windows 95/98/2000/XP, the attached **iKey** will be recognized as a new device. The system device installation process will start. It will take several more minutes.
6. Wait until the installation completion window appears and click ***Finish***.
7. Under Windows NT, restart your computer after installing the **iKey** driver.
8. Check if the **iKey** and its driver have been installed correctly: Right-click ***My Computer*** > ***Properties*** > ***Hardware*** > ***Device Manager***.
9. Make sure that the list of hardware supported by your system contains one or more **Rainbow iKey Virtual Reader** drivers and the name of the attached **iKey** device in the ***Smart card readers*** section.

   Note: An incorrectly attached or out of order **iKey** is not on the list. If there is no **Rainbow iKey Virtual Reader** on the list, the installation has been completed incorrectly. In this case, repeat the installation, or refer to the technical support service of **Dekart**.

The LED indicator of the **iKey** device starts glowing after the installation is successfully completed. The flashing indicator means that the data exchange between the key and the computer is in progress.

Note: To avoid errors, do not withdraw the **iKey** from the port while the indicator is flashing.

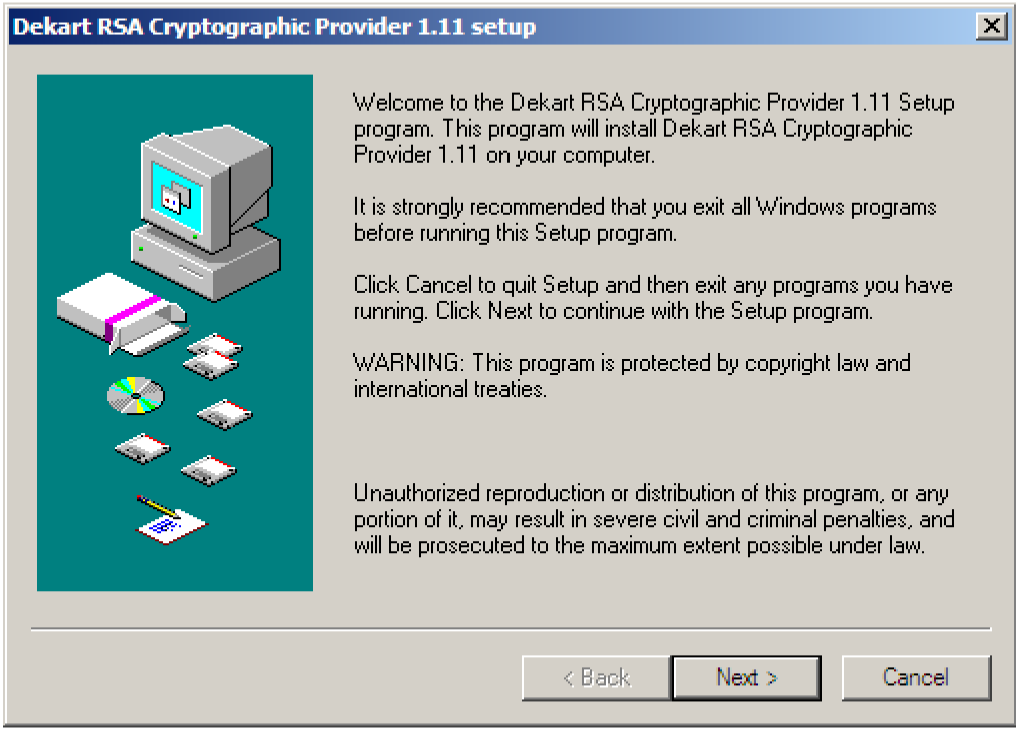
Go on to the main product components installation described in the *Dekart Logon Installation* section.

Dekart RSA Cryptographic Provider Installation

Dekart RSA Cryptographic Provider should be installed onto a personal computer (PC) by an experienced Windows user (See the *User Proficiency Requirements* section in the *Preface* of this *Guide*) only after performing the actions indicated in the *Auxiliary Components Installation* section of this chapter.

To install the product, do the following:

1. Exit all active Windows application.
2. Insert the **Dekart RSA Cryptographic Provider** CD into the CD-ROM drive. The product installation module will run automatically. The installation menu will appear on the screen. If this menu does not appear, the function of automatic application running is probably disabled in your system. Enable this function and re-insert the CD or launch the SETUP.EXE module from the CD manually.
3. Select ***Install Dekart RSA Cryptographic Service Provider***
4. The welcome screen of the installation program will appear, as shown on Figure 10.



Dekart RSA Cryptographic Provider 1.11 setup

Welcome to the Dekart RSA Cryptographic Provider 1.11 Setup program. This program will install Dekart RSA Cryptographic Provider 1.11 on your computer.

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

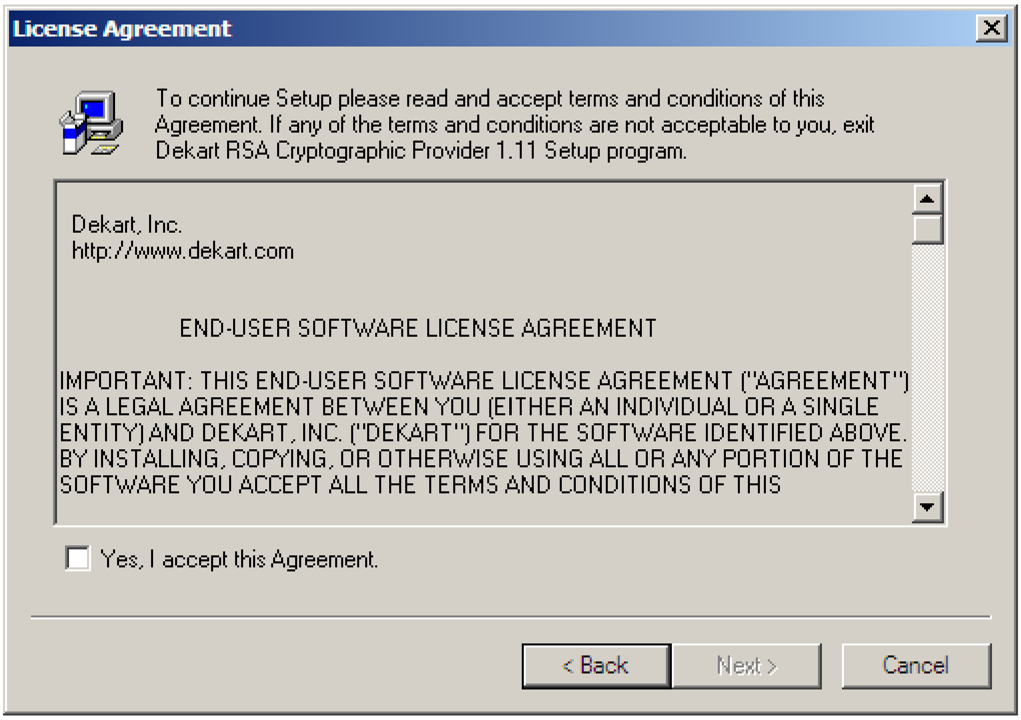
Click Cancel to quit Setup and then exit any programs you have running. Click Next to continue with the Setup program.

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.

Figure 10. Welcome screen of the installation program

5. Click ***Next***. The License Agreement text window will appear, as shown in Figure 11.



License Agreement

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 RSA Cryptographic Provider 1.11 Setup program.

Dekart, Inc.
http://www.dekart.com

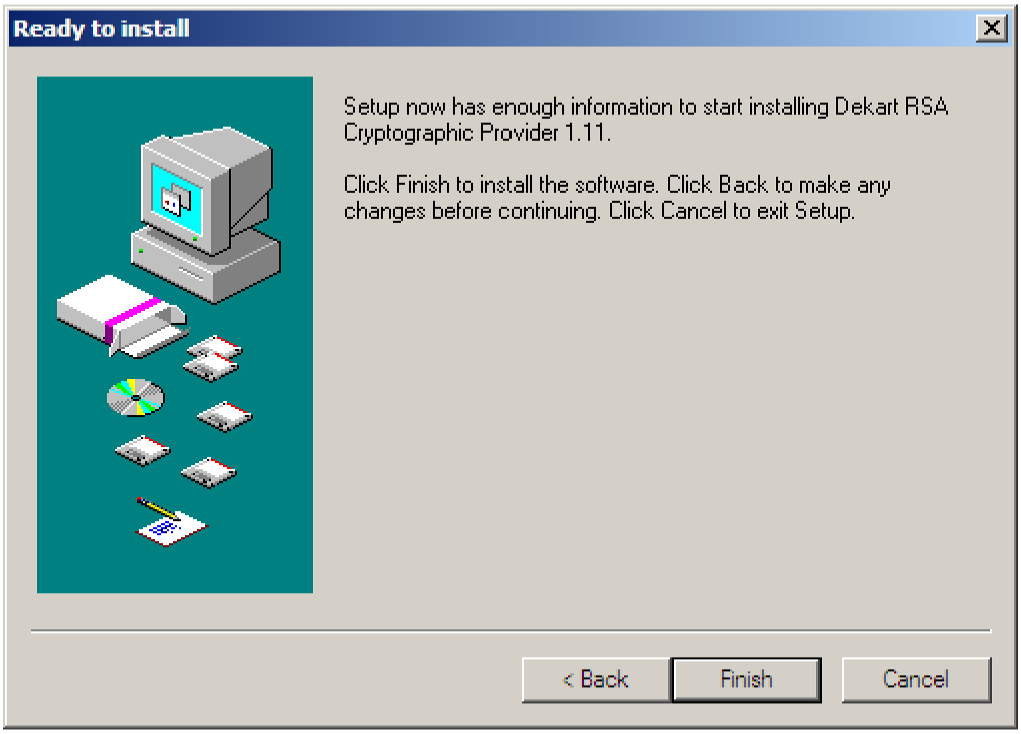
END-USER SOFTWARE LICENSE AGREEMENT

IMPORTANT: THIS END-USER SOFTWARE LICENSE AGREEMENT ("AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AND DEKART, INC. ("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

☐ Yes, I accept this Agreement.

Figure 11. License Agreement text window

6. Carefully read the text of the license agreement between you, the end-user of **Dekart RSA Cryptographic Provider**, and **Dekart**. Select ***Yes, I accept this agreement*** check box if you agree with the terms, and click ***Next***. (If you do not agree with the terms of License Agreement, *do not select* this check box. In this case, the product installation will be discontinued.) A ***Ready to Install*** window will appear, as shown in Figure 12.

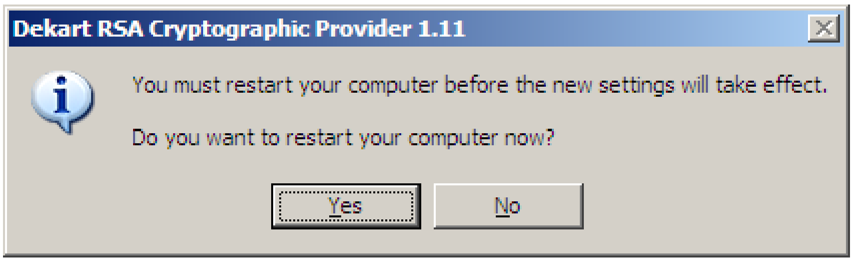


Setup now has enough information to start installing Dekart RSA Cryptographic Provider 1.11.

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

Figure 12. Starting the installation

7. Click ***Finish*** to copy all of the files required for the product to operate properly to the system folder.
8. When the window shown in Figure 13 appears, click ***Yes***. The product will be ready to use after rebooting the computer.



You must restart your computer before the new settings will take effect.

Do you want to restart your computer now?

Figure 13. Rebooting the computer

Re-Installing Dekart RSA Cryptographic Provider

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

- The operating system has been re-installed
- The product functionality has been lost for some reason

If required, the auxiliary components (smart card reader/USB key) can be re-installed according to the directions of the *Auxiliary Components Installation* section.

To re-install the product, start the SETUP.EXE file from the **Dekart RSA Cryptographic Provider** product CD and select ***Install Dekart RSA Cryptographic Provider*** from the main menu. Further actions are similar to those described in the *Product Installation* section of this chapter.

Updating Dekart RSA Cryptographic Provider

Dekart RSA Cryptographic Provider can be updated on acquiring a newer version of the product.

To update the product, start the SETUP.EXE file from the **Dekart RSA Cryptographic Provider** product CD and select ***Install Dekart RSA Cryptographic Provider*** from the main menu. The installation utility will find the current version of the product and will suggest that it be updated. Further actions are similar to those described in the *Product Installation* section of this chapter.

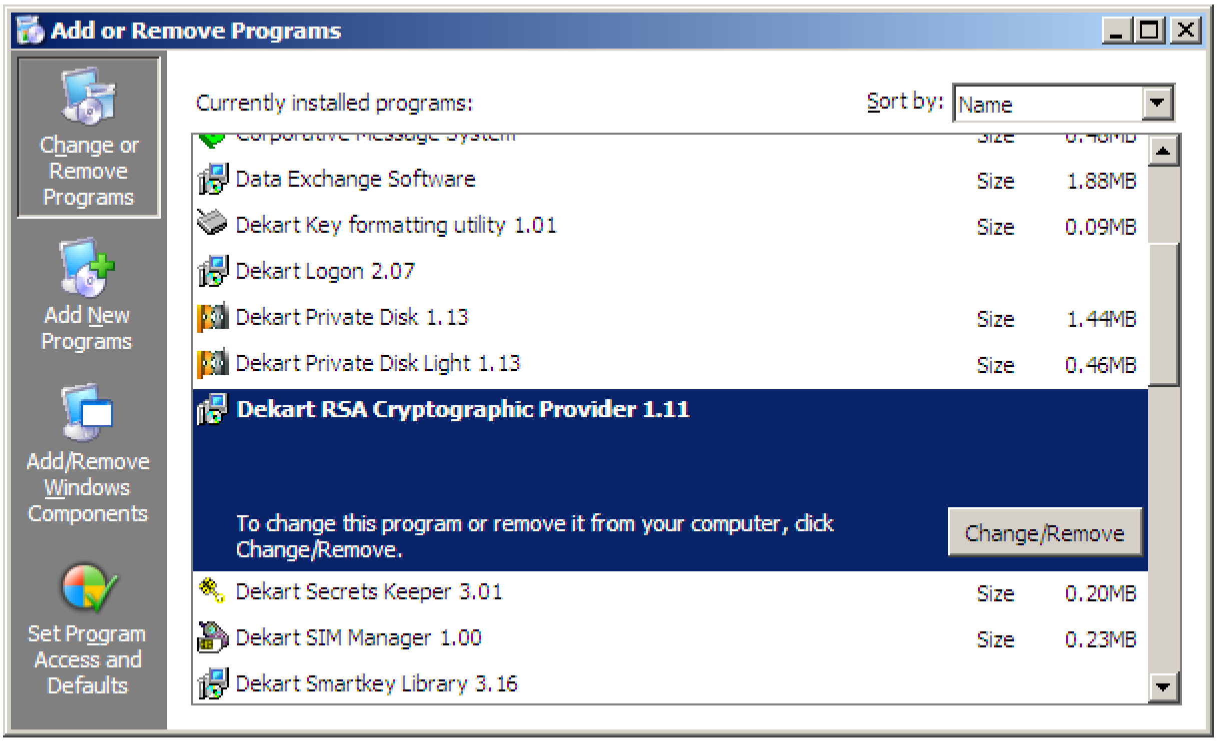
De-Installing Dekart RSA Cryptographic Provider

Under certain conditions, you may need to de-install **Dekart RSA Cryptographic Provider**.

Note: If any of your certificates were adjusted to operate with **Dekart RSA Cryptographic Provider**, you will no longer be able to use them after de-installing the product.

To de-install the product with Windows tools, do the following:

1. Select ***Settings*** > ***Control Panel*** from the ***Start*** menu.
2. Double click ***Add/Remove Programs***. In the window that appears, as shown in Figure 14 the programs installed into the operating system will be listed.


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
Sort by:
Name
Change/Remove

Currently installed programs:

Data Exchange Software	Size	1.88MB
Dekart Key formatting utility 1.01	Size	0.09MB
Dekart Logon 2.07		
Dekart Private Disk 1.13	Size	1.44MB
Dekart Private Disk Light 1.13	Size	0.46MB
Dekart RSA Cryptographic Provider 1.11		
Dekart Secrets Keeper 3.01	Size	0.20MB
Dekart SIM Manager 1.00	Size	0.23MB
Dekart Smartkey Library 3.16		

To change this program or remove it from your computer, click Change/Remove.

Figure 14. Adding or removing programs

3. Select **Dekart RSA Cryptographic Provider** from this list (for example, **Dekart RSA Cryptographic Provider 1.11**) and click ***Add/Remove…***.
4. Confirm removal of the program in the dialog box that appears.
5. Restart the computer.

Dekart Smartkey Library can be de-installed in the same fashion.

Note: If your computer is equipped with other products based on the software and hardware technology from **Dekart**, do not de-install **Dekart Smartkey Library**. Otherwise, those products' operability can be affected.

The smart card reader or the USB key can be de-installed in the same fashion. To do this, activate the ***Add/Remove Programs*** utility, find the reader to be deleted, the **iKey** driver (for example, **Rainbow iKey Driver v3.4.2**), or the **eToken RTE** (for example, **eToken Run Time Environment 2.65**) in the list and click ***Add/Remove…***.

Chapter 5. Operating Dekart RSA Cryptographic Provider

Using CryptoAPI, **Dekart RSA Cryptographic Provider** implements data encryption algorithms based on digital certificates and Public Key Infrastructure (PKI).

In this technology, it is assumed that a cryptographic public key stored in the certificate is associated with the cryptographic service provider storing the pair private key. Confidential information protection in user applications is based on the use of cryptographic algorithms and some personal user information. This information can be, for example, the public and private keys of a user certificate. Cryptographic algorithms are implemented by the corresponding cryptographic service providers. While performing cryptographic operations, an application refers to a certain certificate and employs the cryptographic service provider associated with this certificate.

This chapter describes the following stages of product operation:

- Product pre-service preparation, including selecting a digital certificate and adjusting it to work with the product.
- The **Outlook Express** e-mails and **Microsoft Office XP** documents cryptographic protection using the product and the certificates
- Electronic key management — PIN setting and changing

Dekart RSA Cryptographic Provider Pre-Service Preparation

Dekart RSA Cryptographic Provider is designed to operate with ITU-T X.509 certificates.

If you prefer to use an already existing certificate with this product, make sure that you have no electronic documents encrypted with this certificate and another cryptographic service provider, and then go on to the section *Adjusting Your Certificate to Product Operation*. After changing the cryptographic service provider, you will not be able to decrypt previously encrypted documents. If you have any previously encrypted documents, it is recommended that you acquire a new certificate. For more details, see the section *Acquiring a Certificate*.

Acquiring a Certificate

In accordance with your company corporate policies, obtain a certificate from one of the following organizations:

- Your company certification department. This type of certificate will serve to identify you in e-mail exchange within your organization.
- An independent Certification Authority recommended by your corporate network administrator. This type of certificate will identify you in e-mail exchange outside your organization.

The Certification Authority will generate a certificate in the form of a file storing both the certificate itself and an associated private key. You will be able to export it to any available resource, such as, for example, your PC hard disk. Before exporting the certificate, you will have to set a password to protect access to the private key during its installation in the PC operating system. When attached, or imported, the new certificate is automatically associated with some existing basic cryptographic service provider.

You can use **Outlook Express** to install the certificate into the operating system as follows:

1. Run Outlook Express.
2. In the ***Tools*** menu, click ***Parameters…***, select the ***Security*** tag and click ***Digital IDs…***. In the appearing window, select the ***Personal*** tag and click ***Import…***.
3. Click ***Next*** > ***Browse***; in the appearing dialog box, indicate the path of the file storing your certificate; click ***Open*** > ***Next*** .
4. In the ***Password*** field, enter your certificate access password, select the check box ***Mark the private key as exportable***, and click ***Next*** > ***Next*** > ***Finish***.

Note: The file from which you are importing your certificate and the private key is only protected with a password (security based on one factor authentication). Therefore, it is recommended that it be removed from the PC hard disk or any other resource from which it can be stolen. However, you might need this file if you lose your certificate private key (when a smart card or a USB key goes out of order). To be able to restore your private key in future, save the certificate file to a portable data medium, for example, a 3.5" floppy disk, and store it in a safe.

Adjusting Your Certificate to Product Operation

Using the key pair, the basic cryptographic service provider (to which a new certificate is adjusted) implements encryption algorithms. It also allows you to set an access password to the private key. However, the private key is stored in the Windows system registry, virtually unprotected from theft. Generally, users set short words as their passwords to memorize them easily. Thus, using up-to-date cracking techniques, an "interested party" will guess such a password shortly after accessing your PC. By gaining the private key, the third party will compromise your certificate and cancel the security of all documents protected with it.

Dekart RSA Cryptographic Provider reduces the theft risk to zero by storing the adjusted certificate private key in the memory of a smart card/USB key and using two-factor user authentication for private key access.

To adjust the certificate to **Dekart RSA Cryptographic Provider**, it is enough to modify the private key with the ***Cryptographic Key Migration Tool*** shipped with the product as follows:

1. Select the ***Settings*** option from the ***Start*** menu and click the ***Control Panel*** folder. The ***Control Panel*** window will appear as shown in Figure 15.

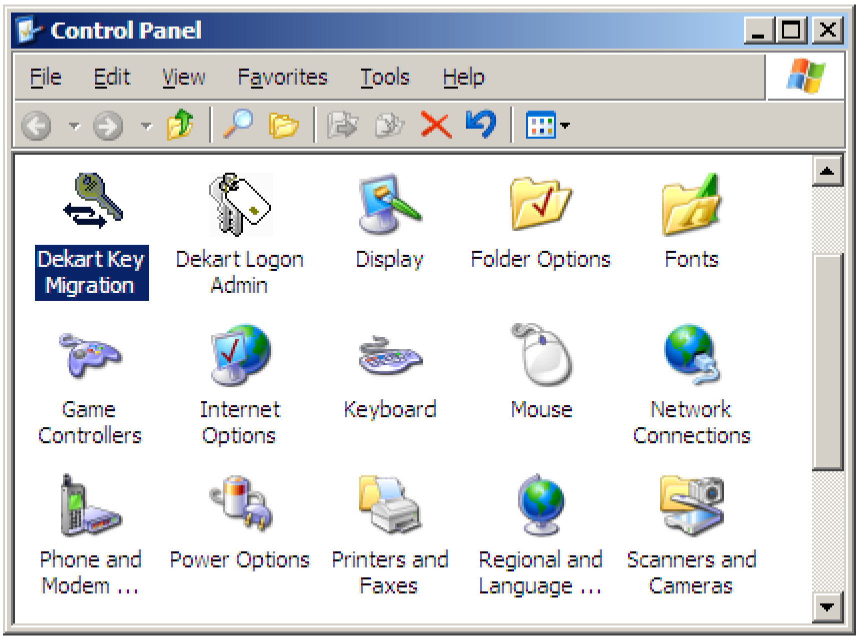
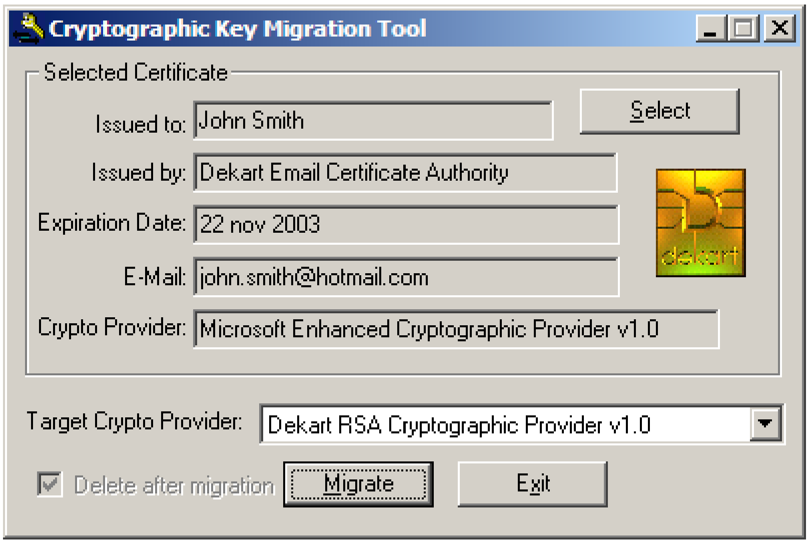


Figure 15. The key migration tool

2. To start the migration tool, double click the ***Dekart Key Migration*** icon. The ***Cryptographic Key Migration Tool*** window will appear, as shown in Figure 16.



Selected Certificate

Issued to: John Smith

Issued by: Dekart Email Certificate Authority

Expiration Date: 22 nov 2003

E-Mail: john.smith@hotmail.com

Crypto Provider: Microsoft Enhanced Cryptographic Provider v1.0

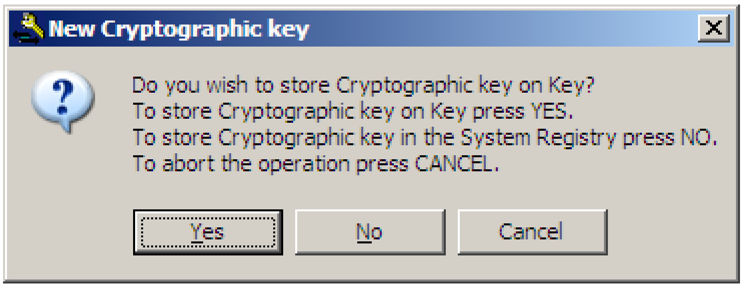
Target Crypto Provider: Dekart RSA Cryptographic Provider v1.0

☑ Delete after migration

Figure 16. Selecting the cryptographic service provider

3. Click ***Select*** and indicate the certificate to be adjusted for **Dekart RSA Cryptographic Provider** in the appearing list. The window will show the certificate description. The title of the cryptographic service provider associated with that certificate will appear in the ***Crypto Provider*** field.

4. In the ***Target Crypto Provider*** drop-down list, select a **Dekart** cryptographic service provider, for example, **Dekart RSA Cryptographic Provider v1.0**, and click ***Migrate***.



New Cryptographic key

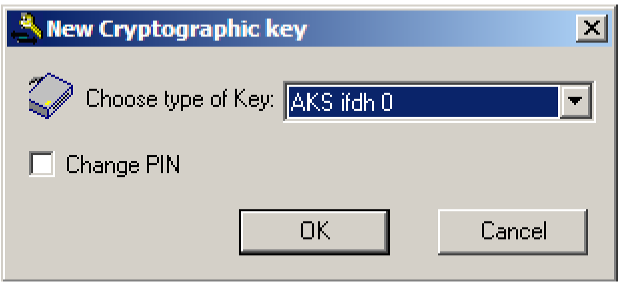
Do you wish to store Cryptographic key on Key?
To store Cryptographic key on Key press YES.
To store Cryptographic key in the System Registry press NO.
To abort the operation press CANCEL.

Figure 17. Selecting the private key storage method

5. The appearing window, shown in Figure 17, will prompt the user to save the private key onto an electronic key — a smart card or a USB key.
   - If you have an electronic key and wish to use it to strengthen your certificate security, click ***Yes***. The certificate private key will be written into the protected memory of a microchip, making its access possible only with an electronic key.
   - Otherwise, click ***No*** to store the certificate private key in the system registry.
6. On selecting strong security, you will be prompted to select a smart card and a corresponding reader or a USB key identifier that you will use from the ***Destination Reader*** list shown below.

   Note: By selecting the ***Change PIN*** check box, you can protect the electronic key data with a PIN. For more details, see the section *Modifying the PIN*.

   Attach a smart card or a USB key and click ***OK***.



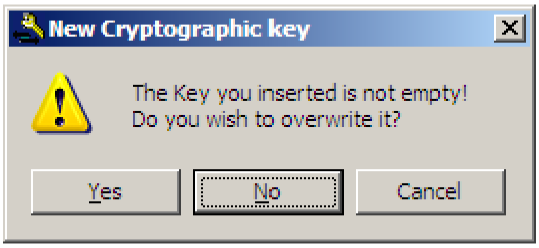
New Cryptographic key

Choose type of Key: AKS ifdh 0

□ Change PIN

Figure 18. Selecting the key medium

7. If a previously recorded private key associated with **Dekart RSA Cryptographic Provider** is detected on a smart card or a USB key during migration, the migration tool will recognize it and prompt replacing it, as shown in Figure 19.



New Cryptographic key

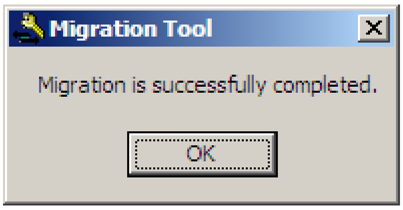
The Key you inserted is not empty!
Do you wish to overwrite it?

Figure 19. Replacing the key data

Note: Dekart RSA Cryptographic Provider retains no private key duplicates required to authenticate its certificate holder. Therefore, deleting the private key makes it impossible to use the corresponding certificate.

  - To delete the old key and replace it with a new one, click ***Yes***.
  - To save the private key to a different key medium, click ***No***. This will bring back the window shown in Figure 18.

8. The window shown in Figure 20 indicates that the private key has been written to the smart card/USB key or to the system registry. The applications associated with the corresponding certificate have been adjusted to use the functionality of **Dekart RSA Cryptographic Provider**.



Migration is successfully completed.

Figure 20. Successful migration completion message

Note: An electronic key can store only one private key. Therefore, to strengthen the protection of several certificates, a corresponding number of electronic keys is required.

Dekart RSA Cryptographic Provider Functionality

Besides implementing the encryption algorithms, **Dekart RSA Cryptographic Provider** also enables you to control whether the digital certificates are used legitimately. The product boosts the security efficiency with the strong two-factor certificate holder authentication protecting the certificate from unauthorized use.

With the certificate adjusted for product operation, you will be able to securely generate the digital signature. This signature ensures that all documents and messages containing it were authored by the owner of the signature and were not altered or substituted after sending or saving. Even if someone gains access to your computer, for example, enters the OS with your username, they will not be able to misuse your certificate, because its private key is safely stored in the memory of a microchip, thus securing your exclusive right to send mail and modify sensitive documents on your behalf.

You can be sure that none of the messages encrypted with your public key were read before you receive them, because you are the exclusive holder of your certificate's private key, allowing you to decrypt them. Even if a third party gains access to your mail box, they will not be able to read your confidential mail, because the private key required to decrypt it is stored on your electronic key (smart card/**eToken**/**iKey**) that you always keep with you, rather than on your possibly unattended computer.

In this way, the product has the standard cryptographic functionality allowing you to:

- Ensure the security of your electronic correspondence
  - Sign the outgoing messages to strongly authenticate the certificate holder
  - Encrypt the outgoing mail
  - Decrypt the incoming messages using the certificate holder strong authentication
  - Verify the digital signatures of the incoming messages
- Ensure that electronic documents are circulated securely
  - Digitally sign **Microsoft Office XP** documents

    - Encrypt **Microsoft Office XP** documents

- Provide access security and authentication for Web pages

Protecting Your Electronic Correspondence

Dekart RSA Cryptographic Provider allows you to protect electronic messages complying with the *Secure Multi-Purpose Internet Mail Extensions* (*S/MIME*) specifications. These specifications are supported by many popular e-mail applications also supporting CryptoAPI. To illustrate the products operation, we will use **Outlook Express**, which is one of these applications.

Dekart RSA Cryptographic Provider has the standard cryptographic functionality recommended for e-mail protection. First of all, it allows you to generate digital signatures.

To generate a digital signature, **Outlook Express** employs a cryptographic service provider associated with a certain user certificate, installed into the OS. If there are several certificates associated with your account in the OS, then select the certificate adjusted for the product to be used by default as follows:

1. Run **Outlook Express**.
2. Click ***Tools*** > ***Parameters…*** > ***Security*** in the ***Options*** > ***Digital IDs…*** window and select the ***Personal*** tag.
3. Select the string with the certificate to be used by default and click ***OK***.

For more details on generating digital signatures, see the section, *Generating a Digital Signature*.

To encrypt an outgoing message, you should obtain the certificate of your addressee containing a public key used for encryption. This certificate is written into your OS registry when you first open a signed message from your prospective addressee. You can check whether you have the certificate in the ***Other Users*** tag list in the ***Options*** window. To encrypt an outgoing message, **Outlook Express** employs one of the cryptographic service providers (including **Dekart RSA Cryptographic Provider**) installed into your OS and supporting the encryption algorithm indicated in the certificate.

In much the same manner, the cryptographic algorithms can be used to decrypt the digital signature of an incoming message, to check its integrity, and verify the identity of the sender's certificates contained in the digital signature and the OS registry. The digital signature is checked automatically when the message is opened. An error message appears if any inconsistency is detected.

Outlook Express can be adjusted to automatically sign and encrypt all outgoing messages. To enable, select the check boxes ***Encrypt contents and attachments for all outgoing messages*** and ***Digitally sign all outgoing messages*** on the ***Personal*** tag of the ***Options*** window.

If an incoming message was encrypted with the public key of the certificate adjusted for the product operation, **Outlook Express** will use this certificate and **Dekart RSA Cryptographic Provider** to decrypt this message even if this certificate is not currently used by default. For more details, see the section *Reading an Encrypted Message*.

Generating a Digital Signature

In **Outlook Express**, you can digitally sign a message as follows:

1. Run **Outlook Express**. Create a new message by clicking ***New*** > ***Message***. Compose a message in the ***New Message*** window, enter an addressee in the ***To*** field and the message topic in the ***Topic*** field.
2. In the ***Tools*** menu, click ***Digitally Sign***. A digital signature icon will appear on the right side of the window.
3. To send a message, click ***Send***. **Outlook Express** generates the digital signature when the message is being sent by employing the cryptographic functionality of the product and the private key. If the certificate is adjusted for the product operation in such a way, that the private key is stored on an electronic key (two-factor security), the strong security system will show the user authentication dialog box prompting you to attach the electronic key.

   Note: To change the electronic key PIN, select the ***Change PIN*** check box in the window shown in Figure 21 and attach the electronic key to the computer. For more details, see the section *Modifying the PIN*.

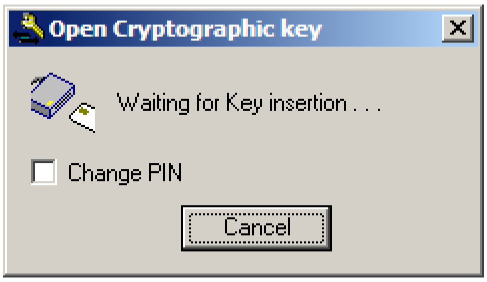


Figure 21. User authentication

4. Attach the electronic medium of your private key. If the attached electronic key is PIN-protected, the strong authentication system will prompt you to enter the PIN.

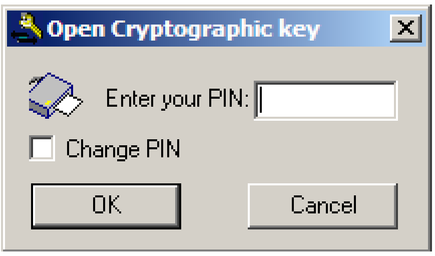


Figure 22. Entering the PIN

5. Enter your PIN in the ***Enter your PIN*** field of the window shown in Figure 22 and click ***OK***. After granting access to the key, the strong security system will continue performing all required safety procedures.

   Note: Be careful — if a smart card/**eToken PRO** is used, the electronic key is blocked after three consecutive wrong PIN entries, and all of its data become temporarily unavailable; if **iKey** is used, the electronic key is blocked after ten consecutive wrong PIN entries, and all of its data become permanently unavailable. For information about unblocking the key, refer to **Dekart** technical support service.
6. Remember to detach your electronic key.

Reading Encrypted Messages

To open an encrypted message, do the following:

1. Run **Outlook Express**. Click the incoming mail folder. All encrypted messages will be marked with an encryption sign. Select and double click a message from the list. The application will activate **Dekart RSA Cryptographic Provider** and you will be prompted to identify yourself — with a smart card/USB key containing the private key.
2. Attach the electronic key and, if prompted, enter the key PIN. To change the key PIN, select the ***Change PIN*** check box in the window shown in Figures 21 and 22. For more details, see the section *Generating a Digital Signature*.
3. Enter the PIN, if prompted, and click ***OK***. The system will decrypt the message and open it. You can read it now.

   Note: Be careful — if a smart card/**eToken PRO** is used, the electronic key is blocked after three consecutive wrong PIN entries, and all of its data become temporarily unavailable; if **iKey** is used, the electronic key is blocked after ten consecutive wrong PIN entries, and all of its data become permanently unavailable. For information about unblocking the key, refer to **Dekart** technical support service.
4. Remember to detach your electronic key from the computer.

When you close the message, it becomes unavailable for any third party. To read it in the future, you will have to pass strong authentication again.

Secure Circulation of Microsoft Office XP Documents

Dekart RSA Cryptographic Provider enables you to control authorship and authenticity of documents stored in a company-wide repository accessed by all employees.

The **Microsoft Office XP** suite of products allows you to use the digital certificates to sign documents that you create. **Dekart RSA Cryptographic Provider** provides the two-factor author authentication to secure the created documents from unauthorized alteration. The certificate imbedded in the digital signature of a document ensures that the document has not been altered since it was digitally signed and saved by the certificate holder. For more details, see the section *Generating and Verifying the Microsoft Office XP Document Digital Signature***.**

In addition, the **Microsoft Office XP** applications enable you to e-mail the generated documents. Immediately before sending, the document can be encrypted with **Dekart RSA Cryptographic Provider** so that the two-factor authentication of an addressee will be required to decrypt it. For more details, see the section *Encryting and Decrypting the Microsoft Office XP Documents*.

Generating and Verifying the Microsoft Office XP Document Digital Signature

Microsoft Office XP enables you to digitally sign a message as follows:

1. Run a **Microsoft Office XP** application, for example, **Microsoft Word XP**. Open the document to be signed by clicking ***File > Open***. If necessary, modify the document and save it by clicking ***File > Save*** or ***File > Save As…***.
2. Click ***Tools > Properties***. In the appearing window, select the ***Security*** tag and click ***Digital IDs***. In the ***Digital ID*** window click ***Add…***.
3. Select a certificate from the list to sign the document, and click ***OK***. If the certificate is adjusted to operate with **Dekart RSA Cryptographic Provider** operation in such a way, that

the private key is stored on an electronic key (two-factor security), the strong security system will show the user authentication dialog box prompting you to attach an electronic key.

Note: To change the electronic key PIN, select the ***Change PIN*** check box in the window shown in Figure 21 and attach an electronic key. For more details, see the section *Modifying the PIN.*

4. Attach the USB key or smart card where your private key is stored. If the attached key is PIN-protected, the strong authentication system will prompt you to enter the PIN.
5. Enter your PIN in the ***Enter your PIN*** field of the window shown in Figure 22 and click ***OK***. After granting access to the key, the strong security system will continue performing all required safety procedures.

   Note: Be careful — if a smart card/**eToken PRO** is used, the electronic key is blocked after three consecutive wrong PIN entries, and all of its data become temporarily unavailable; if **iKey** is used, the electronic key is blocked after ten consecutive wrong PIN entries, and all of its data become permanently unavailable. For information about unblocking the key, refer to **Dekart** technical support service.
6. Remember to detach your electronic key from the computer.
7. Click ***OK*** in the ***Digital ID*** window and in the ***Properties*** window. From this point, the document will contain the digital signature with your certificate.
8. Close the document.

Note: The digital signature will be automatically removed if you modify and save the document after signing it. To restore the digital signature, sign the document once more.

To verify the **Microsoft Office XP** document digital signature, do the following:

1. Run a **Microsoft Office XP** application, for example, **Microsoft Word**. Open a digitally signed document by clicking ***File*** > ***Open***.
2. Click ***Tools*** > ***Properties***. In the appearing window, select the ***Security*** tag and click ***Digital IDs***. In the ***Digital ID*** window, you will see a list of certificates with which this document has been signed.

   Note: If you expected but failed to find any certificates for the document that should have been signed, the document has been modified after signing.
3. Close the ***Digital ID*** and ***Properties*** dialog boxes.
4. Read the document or close it.

Encryting and Decrypting the Microsoft Office XP Documents

To encrypt the **Microsoft Office XP** document, do the following:

1. Run a **Microsoft Office XP** application, for example, **Microsoft Word**. Open a digitally signed document by clicking ***File*** > ***Open***.
2. Click ***File*** > ***Send*** > ***Mail recipient (as attachment)***. A default OS e-mail application will run, for example, **Outlook Express**. A new message window will appear. The icon of the document to be mailed will appear in the ***Attach*** field of this window.
3. Enter an addressee and the topic of the message. If necessary, enter the message text. Encrypt the message with the certificate of the addressee and send it. For more details, see the section *Protecting Your Electronic Correspondence.*

To open the encrypted document with **Outlook Express**, decrypt it, read the message, by double clicking the icon of an attached document. If the certificate used to encrypt the message is adjusted to operate with **Dekart RSA Cryptographic Provider**, and the private key is stored in the memory of a smart card/USB key, the user will have to pass two-factor authentication to decrypt the message. For more details, see the section *Protecting Your Electronic Correspondence*.

Note: To save the encrypted document to a hard disk, you will have to decrypt it first. This will cancel the protection of a document.

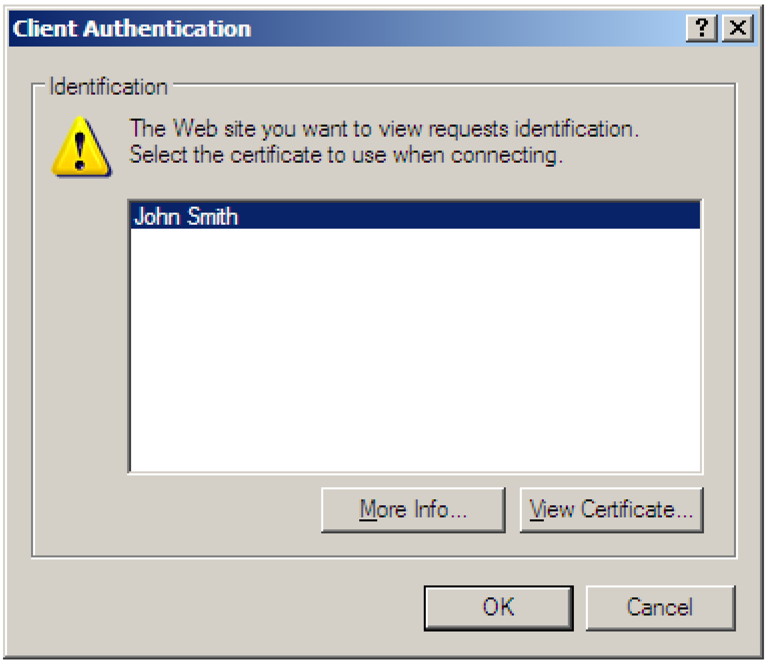
Protecting Web Site Access

Dekart RSA Cryptographic Provider allows you to enforce Web access security for protected Web sites, such as internal corporate sites or any other types of sites, where user authentication is required.

The protected Web site may contain confidential information (internal orders, instructions, employee telephone numbers and home addresses, project information, etc.), assigned for a limited number of users. Access to the Web site is granted on the basis of the digital certificates with the public keys stored on the Web server. The user must provide the private key during authentication. If the private key is stored in the protected memory of a smart card/USB key, both the user and the webmaster can be sure that no third party will use this certificate to access the Web site.

To access the protected Web site using the two-factor authentication, do the following:

1. Run a Web browser, for example, **Internet Explorer**. In the ***Address*** field, enter the address of the protected Web site and press the ***Enter*** key.
2. Before granting access to the protected Web site, a dialog box shown in Figure 23 will appear with the list of certificates available to you for authentication into that Web site. Select a required certificate and click ***OK***.



Client Authentication

Identification

The Web site you want to view requests identification. Select the certificate to use when connecting.

John Smith

Figure 23. Web site client authentication

3. If the certificate is adjusted to operate with **Dekart RSA Cryptographic Provider** in such a way, that the private key is stored on an electronic key (two-factor security), the strong

security system will show the user authentication dialog box prompting you to attach an electronic key.

Note: To change the electronic key PIN, select the ***Change PIN*** check box in the window shown in Figure 21 and attach an electronic key. For more details, see the section *Modifying the PIN*.

4. Attach the USB key or smart card where your private key is stored. If the attached electronic key is PIN-protected, the strong authentication system will prompt you to enter the PIN.
5. Enter your PIN in the field of the window shown in Figure 22 and click ***OK***. After granting access to the key, the strong security system will continue performing all required safety procedures.

   Note: Be careful — if a smart card/**eToken PRO** is used, the electronic key is blocked after three consecutive wrong PIN entries, and all of its data become temporarily unavailable; if **iKey** is used, the electronic key is blocked after ten consecutive wrong PIN entries, and all of its data become permanently unavailable. For information about unblocking the key, refer to **Dekart** technical support service.
6. If your certificate is valid for accessing that Web site, and you have passed the two-factor authentication using a smart card or a USB key, you will be granted a *Secure Sockets Layer* (*SSL*) access to that Web site. The lock sign will appear in the right lower corner of **Internet Explorer**.
7. Detach the electronic key from the computer.

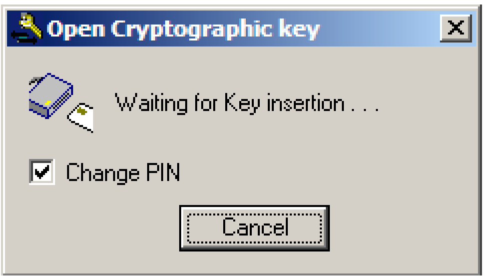
Modifying the PIN

Dekart RSA Cryptographic Provider sets and maintains a special PIN in an electronic key (smart card, **iKey**, or **eToken**) used only to access the private key. The PIN-protected electronic key is a strong authentication means ensuring that it can be used only by its owner who knows the right PIN. There are three reasons for modifying the PIN:

- The default PIN value is empty and it must be changed to maintain security.
- The PIN can be modified periodically, depending on corporate policies.
- The PIN can be modified, if a third party has somehow learned your PIN number, for example, by spying.

Dekart RSA Cryptographic Provider allows you to modify the electronic key PIN whenever the key is attached to the computer, the digital signature is generated, or a new private key is written to the electronic medium. You can modify the PIN as follows:

1. In the dialog box shown in Figure 24, select the ***Change PIN*** check box, attach the electronic key to the computer and click ***OK***.



Open Cryptographic key

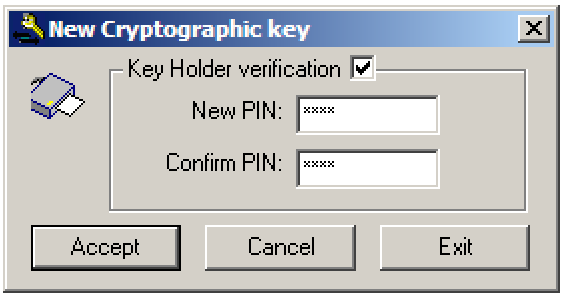
Waiting for Key insertion . . .

☑ Change PIN

Figure 24. Modifying the PIN

2. If the key has already been protected with a PIN, enter the current PIN in the ***Enter your PIN*** field of the window shown in Figure 20 and click ***OK***.

   Note: Be careful — if a smart card/**eToken PRO** is used, the electronic key is blocked after three consecutive wrong PIN entries, and all of its data become temporarily unavailable; if **iKey** is used, the electronic key is blocked after ten consecutive wrong PIN entries, and all of its data become permanently unavailable. For information about unblocking the key, refer to **Dekart** technical support service.



New Cryptographic key

Key Holder verification ☑

New PIN: ****

Confirm PIN: ****

Figure 25. Setting a new PIN

3. Fill out the fields in the appearing dialog box shown in Figure 25. To set the new PIN, select the ***Key Holder verification*** check box, enter the PIN value into the ***New PIN*** field, and retype it in the ***Confirm PIN*** field. The PIN cannot be shorter than eight symbols and it is case-sensitive. With ***Key Holder verification*** check box unselected, the electronic key data will further be accessed without entering the PIN.

4. Click ***Accept***. Next, all changes are recorded into the key memory.

Chapter 6. Troubleshooting

This chapter contains:

- **Diagnostic Messages List**. These messages result from wrong user actions or **Dekart RSA Cryptographic Provider** hardware or software errors.
- **Message Numbers**. These numbers are used for error identification when addressing **Dekart** technical support service.
- **Message Explanation List**. These descriptions are given in the *Explanation* column of the diagnostic messages table.
- **On-Message Actions List**. The actions to be carried out upon receiving a certain message are given in the *Action* column of the diagnostic messages table.

On receiving a diagnostic message, while operating **Dekart RSA Cryptographic Provider**, the user can consult the diagnostic messages table in order to find out what action to take in response:

- The *Message* column, corresponding to this source, contains the message line received by the administrator.
- The *Explanation* cell of the same row contains a reason description for the error message.
- The *Action* cell contains the recommended actions to be taken.
- The ## cell contains the unique message number required only when addressing the technical support service.

The *Diagnostic Messages Table* is given below.

Diagnostic Messages Table. Dekart Key Migration Messages

##	Message	Explanation	Action
01-01	An error occured while exporting Cryptographic key. Please check if your Cryptographic key is exportable and not corrupted	The certificate has not been installed correctly or the private key has been damaged after certificate installation.	Re-install the certificate with the check box ***Mark the private key as exportable*** selected.
01-02	An error occured while importing Cryptographic key.	The target cryptographic service provider functionality is damaged.	Repeat the action. If unsuccessful, re-install the target cryptographic service provider. If the error reoccurs, consult the technical support service.
01-03	An error occured while changing Certificate properties.	The certificate, the source or the target cryptographic service provider functionality is damaged.	Repeat the action. If unsuccessful, re-install the certificate, the source, and the target cryptographic service providers or consult the system administrator.
01-04	An error occured while initializing TARGET Cryptoprovider.	The target cryptographic service provider functionality is damaged.	Re-install the target cryptographic service provider. If the error reoccurs, consult the technical support service.
01-05	An error occured while initializing SOURCE Cryptoprovider.	The source cryptographic service provider functionality is damaged.	Re-install the source cryptographic service provider. If the error reoccurs, consult the technical support service.
01-06	Could not find Cryptographic key.	The certificate private key is missing or damaged. If the private key is stored on an electronic key (smart card/USB key), an error has probably occurred while reading the key data.	Withdraw and re-attach the key. Replace it with another key, if necessary. Re-install the certificate, if necessary. Repeat the action. If the error reoccurs, consult the technical support service.
01-07	An error occurred while loading crypt32.dll.	The crypt32.dll library is missing or obsolete.	Consult the system administrator.
01-08	An error occurred while getting Certificate properties.	The certificate is damaged.	Repeat the action. Re-install the certificate, if necessary.
01-09	An error occurred while migrating.	An unknown error occurred.	Exit and restart the application. Repeat the action that caused this error. If the error reoccurs, consult the technical support service.

Diagnostic Messages Table. Dekart RSA Cryptographic Provider Messages

##	Message	Explanation	Action
02-01	The Key is blocked! To unblock the Key contact Dekart Technical Support.	You have used the maximum allowed number of wrong PIN entries, which resulted in blocking the key.	Attach another key or consult the technical support service for the key unblocking utility and additional information.
02-02	The PIN you entered is incorrect! 2 attempts remaining.	The entered PIN does not match the PIN stored in the key. A wrong key has probably been attached to the PC. The electronic key will be blocked after two more wrong PIN entries.	Re-enter the PIN. Check if the right key has been attached to the computer. Replace it with the right key, if necessary. Withdraw and re-attach the key. If the message appears again, consult the technical support service.
02-03	The PIN you entered is incorrect!	The entered PIN does not match the PIN stored in the key. A wrong key has probably been attached to the PC.	Re-enter the PIN. Check if the right key has been attached to the computer. Replace it with the right key, if necessary. Withdraw and re-attach the key. If the message appears again, consult the technical support service.
02-04	An error occurred while changing the PIN! Do you wish to try again?	The entered PIN length is not supported by the electronic key. A hardware error has probably occurred (the USB key, the smart card, or the reader error)	Repeat the action or enter a longer PIN. Withdraw and re-attach the electronic key. If the message appears again, consult the technical support service.

Glossary

Term	**Description**
Application Programming Interface (API)	This is a software interface used for interaction between the OS and an application.
Basic Input/Output System	See BIOS
BIOS	The Basic Input/Output System is OS-independent software designed for hardware operation support.
BIOS Setup Utility	This utility is used to change BIOS settings.
COM port	PC serial communication port
Electrically Erasable Programmable Read-Only Memory EEPROM	Nonvolatile Electrically Erasable Programmable Read-Only Memory
*eToken**	This is a special device, also called the **eToken** key, produced by Aladdin Knowledge Systems as a key-ring style hardware device and employed by **Dekart RSA Cryptographic Provider**. This is a full-scale analog of a smart card that can be attached to the USB port and used as a means for identifying a user.
eToken Run Time Environment	**eToken Run Time Environment** is a multi-purpose software interface between the eToken-enabled software and the eToken device. On its basis, a variety of eToken-enabled products can be created without knowing the operating features of the device. Aladdin Knowledge Systems is its developer and vendor.
*iKey**	This is a special device, also called the **iKey** electronic key, produced by Rainbow Technologies as a key-ring style hardware device and employed by **Dekart RSA Cryptographic Provider**. This is a full-scale analog of a smart card that can be attached to the USB port and used as a means for identifying a user.
ISO	International Organization for Standardization
IRDA port	Standard port for infrared data transmission and printing developed by the Infrared Data Association.
ISO 7816	List of requirements to the readers' physical properties and smart card data exchange protocols.

Microsoft Windows Installer (MSI)	The Microsoft Windows Installer (MSI) enables the users to install and adjust the applications more quickly and efficiently. For example, this utility can restore the initial computer status if any errors occur during the software installation. This utility is distributed as a part of Windows 2000, Windows Millennium, and Windows XP. It is also available for the Windows 95/98 and NT 4.0 users in the form of a freeware file.
MSI	See Microsoft Windows Installer
PCMCIA port	The port conforming with the PCMCIA specifications (Personal Computer Memory Card International Association)
Personal Computer/Smart Card (PC/SC)	Smart card readers' specifications supported by **Dekart RSA Cryptographic Provider**.
Personal Identification Number	See PIN
PIN	The *Personal Identification Number* is used to confirm the authorization to access the data stored in the memory of a USB key or a smart card. The electronic key PIN should be set independently by the key user or with a special utility (for example, by means of the RTE).
Plug-and-play	This is a standard designed by Microsoft, Intel, etc. in order to simplify connection of additional devices to the computer. The operating system (Windows 95, Windows 98, Windows 2000 Professional, Windows XP, Windows Me) identifies and sets up the recently attached device without any or with minimal user interference.
PS/2 port	The port used to connect the keyboard and the mouse to the PC.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. This system uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.
RAM	Random Access Memory
Read-Only Memory (ROM)	Permanent read-only memory storing the data recorded by its manufacturer.
RTE	See eToken Run Time Environment

Universal Serial Bus	The Universal Serial Bus can be used to connect and disconnect peripheral devices without opening the PC case and even without shutting down the computer. The USB automatically detects these devices and configures the corresponding software.
USB	See Universal Serial Bus
USB key	This is a special device serving as a secure container for the cryptographic keys that can be attached to the USB port of a computer. **Dekart RSA Cryptographic Provider** supports the eToken PRO and eToken R2 keys from Aladdin eToken and the iKey 2000 and iKey 2032 keys from Rainbow Technologies.
Authentication	This is a control process checking the authenticity of the user's identity, i.e. this process checks whether the user is the person they claim to be.
Biometric Authentication	This is the user authentication based on examining specific physical traits of the user by means of special biometric equipment. Biometric authentication can be based on examining fingerprints, iris, voice, and other specific traits of the user's body.
Two-Factor Authentication	This is a process controlling the authenticity of the users identity on the basis of the two following factors: Something You Know — for example, the user name and password. Something You Have – for example, a smart card or the **eToken** device.
Driver	This is software designed to control data input/output and interface the applications/OS and the device connected to the PC.
Secured User	This is user of **Dekart RSA Cryptographic Provider** strong authentication who owns a personal electronic key.
Identification	This is a control process using a unique identifier to determine whether the specific user is known to the system.
Certificate Issuer	See Certification Authority
eToken key	See eToken
iKey electronic key	See iKey
Product License	This is the user registration number stored in the database of **Dekart, Inc**. confirming the right to use the product.

One-Factor or Standard Authentication	This is a process controlling the authenticity of the user identity by standard means of the OS on the basis of a single factor:
Private Key	This is a secret cryptographic key generated as a part of a digital certificate. Paired with the *public key*, it ensures strong cryptographic information security on the basis of the Public Key Infrastructure.
Public Key	This is a cryptographic key generated as a part of a digital certificate and freely distributed. Paired with the *private key*, it enables strong cryptographic information security based on the Public Key Infrastructure.
Digital Certificate	This is a digital document confirming the accordance of the public key with the key holder identification information. The digital certificate includes the *public key*, the digital signature of the *issuer*, the key holder identification information, expiration date, and some other information.
Smart Card	This is a plastic card with an embedded microchip including the secured memory block with special hardware implementing the encryption algorithms — techniques for secret information encrypting/decoding. Smart card is connected to the computer by means of a special device — the smart card reader.
Smart Card Reader	This is a device used to operate smart cards. The reader can be both internal (connected as a standard 3,5' floppy disk drive) and external (connected by means of one of the following ports: *COM, PS/2, USB, PCMCIA, IRDA,* etc.)
Strong Authentication	This is a process controlling the authenticity of the users identity on the basis of, at least, two of the three following factors: Something You Know — for example, the user name and password. Something You Have – for example, a smart card or the **eToken** device. Something You Are – for example, fingerprints or specific physical traits.
Certification Authority	A special organization having the authority to issue the digital certificates and guaranteeing the observance of rights of its certificate holders if any conflicts arise.
Digital signature	This is an encrypted set of digital data that can be used to uniquely identify the electronic message sender or the document signature author.
Electronic Key	This can be either a smart card or the USB token.
Electronic Medium	See Electronic Key