eToken™

YOUR KEY TO eSECURITY

Reference Guide

August 2003

Aladdin®

SECURING THE GLOBAL VILLAGE

Contact Information

For technical support and queries, contact:

Tel: **+972 3 636 2266**
Fax: **+972 3 537 5796**
Email: **eToken.techsup@eAladdin.com**
Website: **http://support.eAladdin.com**

To download the latest product updates and documentation, go to:

Website: **http://support.eAladdin.com**

August 2003

eToken™
YOUR KEY TO eSECURITY

COPYRIGHTS AND TRADEMARKS

DISCLAIMER

NEITHER ALADDIN NOR ANY OF ITS WORLDWIDE SUBSIDIARIES AND DISTRIBUTORS SHALL BE OBLIGATED IN ANY MANNER IN RESPECT OF BODILY INJURY AND/OR PROPERTY DAMAGE ARISING FROM THIS PRODUCT OR THE USE THEREOF. EXCEPT AS STATED IN THE eToken DEVELOPER'S LICENSE AGREEMENT, THERE ARE NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, REGARDING ALADDIN'S PRODUCTS, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. The product must be used and maintained in strict compliance with instructions and safety precautions contained herein, in all supplements hereto and according to all terms of its Developer's License Agreement. This product must not be modified or changed without the written permission of the copyright holder.

All attempts have been made to make the information in this document complete and accurate. Aladdin is not responsible for any direct or indirect damages or loss of business resulting from inaccuracies or omissions. The specifications in this document are subject to change without notice.

ALADDIN KNOWLEDGE SYSTEMS LTD.

eToken ENTERPRISE 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, the libraries, utilities, diskettes, CD_ROM, eToken™ keys and User Guides) (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 (as defined hereunder) AND/OR BY INSTALLING THE SOFTWARE ON YOUR COMPUTER AND/OR BY USING THE PRODUCT, YOU ARE ACCEPTING THIS AGREEMENT AND AGREEING TO BE BOUND BY ITS TERMS AND CONDITIONS.

IF YOU DO NOT AGREE TO THIS AGREEMENT DO NOT OPEN THE PACKAGE AND/OR DOWNLOAD AND/OR INSTALL THE SOFTWARE AND PROMPTLY (at least within 7 days from the date you received this package) RETURN THE PRODUCTS TO ALADDIN WITH THE ORIGINAL PACKAGE AND PROOF OF PAYMENT, ERASE THE SOFTWARE, AND ANY PART THEREOF, FROM YOUR COMPUTER AND DO NOT USE IT IN ANY MANNER WHATSOEVER.

1. Title & Ownership.

The object code version of this software component of Aladdin's eToken Enterprise Product, including any revisions, corrections, modifications, enhancements, updates and/or upgrades thereto about to be installed by you, (hereinafter in whole or any part thereof defined as: "**Software**"), and the related documentation, ARE NOT FOR SALE and are and shall remain in Aladdin's sole property. All intellectual property rights (including, without limitation, copyrights, trade secrets, trademarks, etc.) evidenced by or embodied in and/or attached/connected/related to the Product, are and shall be owned solely by Aladdin. This License Agreement does not convey to you an interest in or to the Software, but only a limited right of use revocable in accordance with the terms of this License Agreement. Nothing in this Agreement constitutes a waiver of Aladdin's intellectual property rights under any law.

2. License.

Subject to payment of applicable fees, Aladdin hereby grants to you, and you accept, a personal, nonexclusive and fully revocable limited License to use the Software, in executable form only, as described in the Software accompanying user documentation and only according to the terms of this Agreement: (i) you may install the Software and use it on computers located in your place of business, as described in Aladdin's related documentation; and (ii) you may merge and link the Software into your computer programs for the sole purpose described in the User Guide.

3. Prohibited Uses.

The Product must be used and maintained in strict compliance with the instruction and safety precautions of Aladdin contained herein, in all supplements thereto and in any other written documents of Aladdin. Except as specifically permitted in Sections 1 and 2 above, you agree not to (i) use, modify, merge or sub-license the Software or any other of Aladdin's Products, except as expressly authorized in this Agreement and in the User Guide; and (ii) sell, license (or sub-license), lease, assign, transfer, pledge, or share your rights under this License with/to anyone else; and (iii) modify, disassemble, decompile, reverse engineer, revise or enhance the Software or attempt to discover the Software's source code; and (iv) place the Software onto a server so that it is accessible via a public network; and (v) use any back-up or archival copies of the Software (or allow someone else to use such copies) for any purpose other that to replace an original copy if it is destroyed or becomes defective. If you are a member of the European Union, this agreement does not affect your rights under any legislation implementing the EC Council Directive on the Legal Protection of Computer Programs. If you seek any information within the meaning of that Directive you should initially approach Aladdin.

4. Maintenance and Support.

Aladdin has no obligation to provide support, maintenance, upgrades, modifications, or new releases under this Agreement.

5. Limited Warranty.

Aladdin warrants, for your benefit alone, that (i) the Software, when and as delivered to you, and for a period of three (3) months after the date of delivery to you, will perform in substantial compliance with the User Guide, provided that it is used on the computer hardware and with the operating system for which it was designed; and (ii) that the eToken™ key, for a period of twelve (12) months after the date of delivery to you, will be substantially free from significant defects in materials and workmanship.

6. Warranty Disclaimer.

ALADDIN DOES NOT WARRANT THAT ANY OF ITS PRODUCT(S) WILL MEET YOUR REQUIRMENTS OR THAT ITS OPERATION WILL BE UNINTERRUPTED OR ERROR-FREE. TO THE EXTENT ALLOWED BY LAW, ALADDIN EXPRESSLY DISCLAIMS ALL EXPRESS WARRANTIES NOT STATED HEREIN AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NO ALADDIN'S DEALER, DISTRIBUTOR, RESELLER, AGENT OR EMPLOYEE IS AUTHORIZED TO MAKE ANY MODIFICATIONS, EXTENSIONS, OR ADDITIONS TO THIS WARRANTY. If any modifications are made to the Software or to any other part of the Product by you during the warranty period; if the media and the eToken™ key is subjected to accident, abuse, or improper use; the Product has not been properly installed, operated, repaired or maintained in accordance with the instructions supplied by Aladdin; the Product has been subjected to abnormal physical or electrical stress, negligence or accident; or if you violate any of the terms of this Agreement, then the warranty in Section 5 above, shall immediately be terminated. The warranty shall not apply if the Software is used on or in conjunction with hardware or program other than the unmodified version of hardware and program with which the Software was designed to be used as described in the User Guide.

7. Limitation of Remedies.

In the event of a breach of this warranty, Aladdin's sole obligation shall be, at Aladdin's sole discretion: (i) to replace or repair the Product, or component thereof, that does not meet the foregoing limited warranty, free of charge; (ii) to refund the price paid by you for the Product, or component thereof. Any replacement or repaired component will be warranted for the remainder of the original warranty period or 30 days, whichever is longer. Warranty claims must be made in writing during the warranty period and within seven (7) days of the observation of the defect accompanied by evidence satisfactory to Aladdin. All Products should be returned to the distributor from which they were purchased (if not purchased directly from Aladdin) and shall be shipped by the returning party with freight and insurance paid. The Product or component thereof must be returned with a copy of your receipt.

8. Exclusion Of Consequential Damages.

The parties acknowledge, that Product is inherently complex and may not be completely free of errors. ALADDIN SHALL NOT BE LIABLE (WHETHER UNDER CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE) TO YOU, OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE (INCLUDING INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES), INCLUDING, WITHOUT LIMITATION, ANY LOSS OR DAMAGE TO BUSINESS EARNINGS, LOST PROFITS OR GOODWILL AND LOST OR DAMAGED DATA OR DOCUMENTATION, SUFFERED BY ANY PERSON, ARISING FROM AND/OR RELATED WITH AND/OR CONNECTED TO DELIVERY, INSTALLATION, USE OR PERFORMANCE OF THE SOFTWARE AND/OR ANY COMPONENT OF THE PRODUCT, EVEN IF ALADDIN IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

9. Limitation Of Liability.

IN THE EVENT THAT, NOTWITHSTANDING THE TERMS OF THIS AGREEMENT, ALADDIN IS FOUND LIABLE FOR DAMAGES BASED ON ANY DEFECT OR NONCONFORMITY OF ITS PRODUCT(S), ITS TOTAL LIABILITY FOR EACH DEFECTIVE PRODUCT SHALL NOT EXCEED THE PRICE PAID TO ALADDIN FOR SUCH DEFECTIVE PRODUCT.

10. Termination.

Your failure to comply with the terms of this Agreement shall terminate your license and this Agreement. Upon termination of this License Agreement: (i) the License granted to you in this Agreement shall expire and you, upon termination, shall discontinue all further use of the Software and other licensed Product(s); and (ii) you shall promptly return to Aladdin all tangible property representing Aladdin’s intellectual property rights and all copies thereof and/or shall erase/delete any such information held by it in electronic form. Sections 1, 6-11 shall survive any termination of this Agreement.

11. Governing Law & Jurisdiction.

This Agreement shall be construed and governed in accordance with the laws of Israel (except for conflict of law provisions) and only the courts in Israel shall have jurisdiction in any conflict or dispute arising out of this Agreement. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

12. Government Regulation and Export Control.

You agree that the Product will not be shipped, transferred, or exported into any country or used in any manner prohibited by applicable law. It is stipulated that the Product is subject to certain export control laws, rules, and/or regulations, including, without limiting the foregoing, to the United States and/or Israeli export control laws, rules, and/or regulations. You undertake to comply in all respects with the export and reexport restriction as set forth herein and any update made thereto from time to time.

13. Third Party Software.

If the Product contains any software provided by third parties, such third party's software are provided "As Is" and shall be subject to the terms of the provisions and condition set forth in the agreements contained/attached to such software. In the event such agreements are not available, such third party software shall be provided ”As Is” without any warranty of any kind and Sections 2, 3, 6, 8, 9-12 of this Agreement shall apply to all such third party software providers and third party software as if they were Aladdin and the Product respectively.

14. Miscellaneous.

This Agreement represents the complete agreement concerning this License and may be amended only by a written agreement executed by both parties. If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.

I HAVE READ AND UNDERSTOOD THIS LICENSE AGREEMENT AND AGREE TO BE BOUND BY ALL OF THE TERMS.

FCC Compliance

eToken USB has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

a. Reorient or relocate the receiving antenna.

b. Increase the separation between the equipment and receiver.

c. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

d. Consult the dealer or an experienced radio/TV technician.

FCC Warning

Modifications not expressly approved by the manufacturer could void the user authority to operate the equipment under FCC rules.

All of the above applies also to the eToken USB.

FCC authorities have determined that the rest of the eToken product line does not contain a Class B Computing Device Peripheral and therefore does not require FCC regulation.

CE Compliance

The eToken product line complies with the CE EMC Directive and related standards*. eToken products are marked with the CE logo and an eToken CE conformity card is included in every shipment or upon demand.

*EMC directive 89/336/EEC and related standards EN 55022, EN 50082-1.

UL Certification

The eToken product line successfully completed UL 94 Tests for Flammability of Plastic Materials for Parts in Devices and Appliances. eToken products comply with UL 1950 Safety of Information Technology Equipment regulations.

ISO 9002 Certification

The eToken product line is designed and manufactured by Aladdin Knowledge Systems, an ISO 9002-certified company. Aladdin's quality assurance system is approved by the International Organization for Standardization (ISO), ensuring that Aladdin products and customer service standards consistently meet specifications in order to provide outstanding customer satisfaction.

Certificate of Compliance

Upon request, Aladdin Knowledge Systems will supply a Certificate of Compliance to any software developer who wishes to demonstrate that the eToken product line conforms to the specifications stated. Software developers can distribute this certificate to the end user along with their programs.

Table of Contents

Chapter 1

Introduction

This Reference Guide is intended for those responsible for administering data security and integrity in an organization.

It provides an overview of the benefits and features of Aladdin's eToken™ security key and of the eToken set of ready-to-use security clients, explains some important security-related concepts and standards, and provides installation and administration guidelines for eToken.

The following sections are contained in this chapter:

- "What is eToken?", on page 3, describes the eToken security key and lists the major benefits that eToken offers your organization and its users.
- "eToken Models", on page 6, describes the two models of the eToken that are currently available.
- "eToken Security Solutions", on page 15, lists the major applications that support eToken integration.
- "FIPS", on page 16, explains what is FIPS and how the eToken complies with FIPS standards.

For detailed instructions for specific eToken solutions, please refer: **www.eAladdin.com/etoken**.

eToken Solutions

eToken is a set of ready-to-use security client solutions, based on Aladdin’s eToken security key.

These solutions are specifically tailored to safeguard the integrity of secured data and user access rights throughout an organization, while providing maximum flexibility and control.

Employing state-of-the-art eToken technology, eToken helps your organization protect its digital assets, conveniently and securely.

eToken is particularly interesting for an organization’s system administrators because it makes it easy to improve data security quickly, without having to write new code.

System administrators can integrate eToken easily into an existing IT security framework, providing increased protection for users’ everyday operations.

With eToken, user access is individual, exclusive and secure.

What is eToken?

eToken is a powerful and secure hardware device that enhances the security of data on public and private networks. The size of a normal house key, eToken can be used to generate and provide secure storage for passwords and digital certificates, for secure authentication, digital signing and encryption. eToken is based on smart card technology but requires no special readers.

eToken provides security with portability. It has smart card functionality in the form of a Universal Serial Bus (USB)-based device. The USB's "hot plug" capability allows one or more devices to be connected and disconnected without turning off the system.

eToken can be used to hold secret information, certificates and private keys for use in authentication solutions for LANs, WANs, VPNs, e-commerce and mobile computing. Its USB functionality enables companies to minimize deployment costs, and to maximize user-friendliness without compromising security.

With its advanced technology, eToken enables organizations to trust the identity of individuals requesting access to protected content or applications through corporate networks or websites.

eToken has the flexibility to hold the information required by the most advanced digital security systems, eliminating the added cost of integrating an expensive reader system. A single eToken can store a number of private keys, certificates and passwords concurrently, for use in a wide variety of applications.

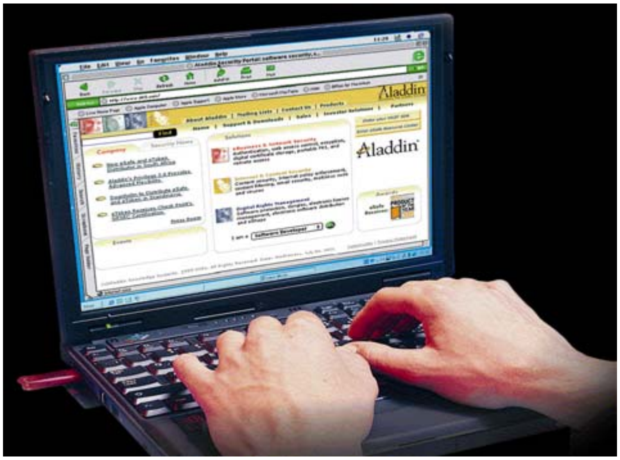
eToken PRO can also generate keys and perform sensitive encryption operations on-chip, ensuring that users' keys are never exposed to the PC environment.

Benefits of eToken

The key benefits of eToken include:

- **Strong authentication:** eToken provides strong two-factor authentication, through the simultaneous use of something the user knows - a specific password or passphrase, and something the user has - the personalized eToken. The authentication method used by eToken employs strong, industry-standard encryption algorithm technology.
- **High security:** Using a hardware key provides a much higher degree of security than software-only solutions. Security credentials are not at risk because they are held in a secure, tamper-evident container. eToken technology is completely resistant to cracking, even with full knowledge of the encryption algorithms and protocols used. The eToken PRO provides full hardware-based protection for essential security information, with on-chip key generation.
- **Cost-effectiveness:** eToken is more cost-effective than any other hardware security system. While providing all the benefits of smart card technology, eToken requires no costly smart card readers.

- **Compatibility and ease of integration:** eToken can be used with various environments, USB-compatible devices and operating systems, including Windows 95, 98, NT 4.0, Me, 2000 and XP and supports the major cryptographic API standards, such as Microsoft CAPI and PKCS #11, allowing for seamless integration with applications.
- **Convenience and portability:** Easy to carry on a personal key ring, eToken is portable from one computer or site to another.
- **Ease of use:** No additional hardware is required. To obtain true two-factor authentication, users simply insert their personalized eToken into the USB port on a hub, desktop, laptop, keyboard or monitor, and enter their unique password or passphrase.



- **Ease of administration:** eToken provides easy-to-use security client solutions for administrators, simplifying the process of initial deployment and ongoing user and certificate management.
- **Versatility:** A single eToken can be used with different types of applications concurrently, and can contain multiple private keys and digital certificates. eToken is available in a range of memory sizes and colors.

eToken Models

The two eToken models currently available are the eToken R2 and the eToken PRO.

The eToken PRO adds to the functionality and strong security features of the eToken R2, by providing full hardware-based protection for all security information stored on the eToken, together with on-chip key generation and cryptographic processing. The eToken PRO generates the keys on the token itself, and they never leave the secure environment of the eToken.

Both eToken models are identical in their physical casing, size and shape, and are equally robust, tamper-resistant and water-resistant.

eToken PRO

The eToken PRO offers strong authentication and guaranteed non-repudiation for sensitive applications such as eBanking, stock trading, eCommerce and financial transactions.

eToken PRO Features

The eToken PRO:

- Uses advanced smartcard chip technology, with on-chip cryptographic processing using RSA1024, 3xDES and SHA-1.
- Provides full on-chip RSA 1024-bit key generation, authentication & digital signing capabilities.
- Provides highly secure, logical and physical smart card level security which is ITSEC LE4 Certified.
- Uses standard Crypto API connectivity.
- Provides secure storage and a robust file system.
- Private keys never leave the token.
- Supports PKCS #11, CAPI and Application Protocol Data Unit (APDU) APIs.
- Has ITSEC 4 security certification approval.
- Provides multiple color options, security coding and third party branding capabilities.
- Has robust plug-and-play connectivity to mainstream private key and security clients.
- Uses a standard USB interface.

On-board Cryptographic Functionality.

The eToken PRO uses advanced Smartcard Chip technology that provides the following on-chip cryptographic operations:

- Asymmetric encryption/decryption and signing/verification with RSA keys up to 1024 bits long.
- Symmetric DES and 3DES encryption, decryption and MACing with key lengths up to 168 bits long.
- Message digesting using SHA-1 and optionally MD5 (through a downloadable module).

The eToken PRO can perform a dual digest and signing operation on-chip. The rich feature set allows the eToken PRO to be used as a secure signing device and as an encryption/decryption engine to protect information on a PC.

Key Generation

The eToken PRO can generate truly random asymmetric RSA keys up to 1024 bits long. On average, generating a 1024-bit key by the eToken PRO 32k takes 15 seconds.

Hardware Random Number Generation

The eToken PRO has a true hardware random number generator that is used internally for RSA key generation and authentication challenges.

Physically Protected Chip

The eToken PRO is implemented in a secure chipcard that meets the ITSEC 4 standard. All data stored on the eToken PRO is stored internally within this chipcard and is intrinsically secure.

Access Protection

The eToken PRO possesses a comprehensive access control mechanism that protects data and keys stored on the eToken. Access to data can be controlled by a variety of mechanisms, such as challenge-response authentication or PIN entry.

eToken PRO Benefits

The key eToken PRO benefits can be summarized as follows:

- Non-repudiation using advanced digital signing technology; data is signed on the smart card chip inside the eToken.
- On-board private key generation: private keys are never exposed outside the eToken.
- No need for special development or integration work: eToken supports standard security interfaces and a wide range of security clients.
- Flexible development tools for seamless integration with third party applicants.
- Portable USB design: no special reader required.
- Two-factor authentication: requires eToken itself, together with the eToken password.
- Secure storage of users’ credentials, keys and sensitive information.
- Private labelling and color options for brand enhancement.

eToken PRO Specifications

Operating Systems	Windows 95/98/98SE/Me/2000/XP, and Windows NT4.0 SP4 and later
Certification and standards	PKCS#11 v2.01, CAPI (Microsoft Crypto API), Siemens/ Infineon, APDU commands, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE
Models (by memory size)	16k and 32k
On board security algorithms	RSA 1024-bit, DES, 3DES (Triple DES), SHA1, (MD5-optional)
Smartcard Chip security level	ITSEC LE4 smart card security certification (Infineon)
Speed	RSA 1024-bit signature approx. 1 second. RSA 1024-bit key generation approx. 15 seconds (32k)
Dimensions	47 x 16 x 8 mm (1.85 x 0.63 x 0.31 inches)
ISO specification support	Support for ISO 7816-1 to 4 specifications
Weight	5g
Power dissipation	120mW
Operating temperature	0 C to 70 C (32 F to 158 F)
Storage temperature	-40 C to 85 C (-40 F to 185 F)
Humidity rating	0-100% without condensation
Water resistance certification	IP X8 - IEC 529
Connector	USB type A (Universal Serial Bus)
Casing	Hard molded plastic, tamper evident
Memory data retention	At least 10 years
Memory cell rewrites	At least 500,000

eToken R2

The eToken R2 is an authentication device that offers robust and powerful on-board 120-bit DES-X two-factor authentication.

eToken R2 Features

The eToken R2:

- Uses a secure microcontroller (EEPROM), with 16K/32K bytes of secured memory, and a 120-bit DES-X on-chip processor.
- Provides on-board symmetric DES-X challenge response authentication.
- Has a protected chip serial ID (32 bit).
- Uses standard Crypto API connectivity.
- Secure and protected storage of users' private credentials.
- Enables compatible implementation with smartcard applications.
- Supports PKCS#11, CAPI and Application Protocol Data Unit (APDU) APIs.
- Provides multiple color options, security coding and third party branding capabilities.
- Uses a standard USB interface.

On-board Cryptographic Functionality

The eToken R2 supports the DES-X symmetric algorithm with 120-bit keys. eToken R2 uses this algorithm internally to encrypt all sensitive data and to perform the challenge-response user authentication protocol. The eToken R2 can be used as an encryption/decryption engine to protect information on a PC.

RNG-based Challenge-response Logon

The eToken R2 has a pseudo-random number generator based on a truly random seed and the DES-X function, which is believed to be pseudo-random.

In order to verify the password, eToken R2 generates a random challenge and sends it to the PC. The response is verified against the stored password. This enables eToken to securely authenticate the user using two-factor authentication.

Physically Protected Chip

The eToken R2 is implemented as a secure microcontroller and external EEPROM pair. The EEPROM is used to store all eToken data. Sensitive data, such as user data and encryption keys are encrypted on the EEPROM using DESX with keys stored in the microcontroller. These keys cannot be read or accessed in any way.

Access Protection

The eToken R2 differentiates between public, private and secret data. The eToken can be in either a logged-in or logged-out state. Only the eToken R2 user can log in to the token by using the challenge response mechanism as detailed above. Once logged in, the user may read and write public and private data or write and use secret data. In the logged out state, it is only possible to read public data and use one factor secret data.

Secure On-token Memory Storage

An eToken R2, together with the correct password, can be used to store secret data securely. For example, storage of a password for an application can utilize this type of secure memory.

eToken R2 provides a secure means for storing RSA keys. These keys can be used for signing messages and decrypting private information that was sent in a secure manner.

USB Data Traffic Encryption

Once the user is logged in to the eToken R2, sensitive data traffic is always encrypted. eToken R2’s data traffic encryption uses DESX with a session key randomly generated during the login procedure.

The secret information on the eToken is accessible only after the correct password is verified, and cannot be retrieved without it.

eToken R2 Benefits

The key eToken R2 benefits can be summarized as follows:

- No need for special development or integration work.
- Flexible development tools for seamless integration with third party applications.
- Portable USB design: no special reader required.
- Two-factor authentication: requires the eToken itself together with the eToken password.
- Secure storage of users' credentials, digital certificates, private keys and sensitive information for advanced authentication, confidentiality and non-repudiation.
- Private labelling and color options for brand enhancement.

eToken R2 Specifications

Operating Systems	Windows 95/98/98SE/Me/2000/XP, and Windows NT4.0 SP4 and later
Certification and standards	PKCS#11 v2.01, CAPI (Microsoft Crypto API), APDU commands, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE
Models (by memory size)	16k and 32k
On board security algorithms	DES-X 120-bit*
Chip security level	Secured and encrypted EEPROM memory chip
Dimensions	47 x 16 x 8 mm (1.85 x 0.63 x 0.31 inches)
Weight	5g
Power dissipation	120mW
Operating temperature	0 C to 70 C (32 F to 158 F)
Storage temperature	-40 C to 85 C (-40 F to 185 F)
Humidity rating	0-100% without condensation
Water resistance certification	IP X8 - IEC 529
Connector	USB type A (Universal Serial Bus)
Casing	Hard molded plastic, tamper evident
Memory data retention	At least 10 years
Memory cell rewrites	At least 100,000

* DES based algorithm enhanced to offer similar level of security as 3DES (Triple DES). Microsoft also uses this strong and fast algorithm in its EFS system.

eToken Enabled Security Services and Applications

The eToken PRO and the eToken R2 provide access to the following enables security services and applications:

- Online financial services: authentication and transaction signing for eBanking and stock trading applications
- Extranet/Intranet access
- Online government services: citizens' information, vehicle registration, tax returns and health care
- eCommerce B2B & B2C services: authentication and transaction signing for eCommerce applications
- VPN solutions: two-factor authentication
- Remote Access Server (RAS) authentication
- Secured network logon
- Secured email communications, encryption and signing
- PC security: boot protection and file encryption

Key Application Support

Network Security Clients:

Windows 2000 Smartcard and NT network logon, Check Point VPN client, Cisco VPN client, RAS Dialup / RADIUS. The eToken also supports various PC security and file encryption applications.

eMail Clients:

Microsoft Outlook, Outlook Express & Internet Explorer, Netscape Messenger.

eBusiness Security Clients:

Web Browser SSL v3 inter operability: Microsoft Internet Explorer public key authentication. Netscape Navigator public key and signing. WAC authentication. Support for various Solution partners' communication and encryption applications.

For a full list of eToken Partners, go to: **http://www.eAladdin.com/partners/solutions**.

eToken Security Solutions

eToken is a range of ready-to-use security client solutions that can be easily implemented to suit your organization's specific requirements, by integrating eToken with existing applications.

eToken enables you to secure your corporate network and to implement strong eBusiness protection.

Corporate Network Security Solutions

Currently available solutions for corporate network security include:

- Remote access security for VPN systems, with Check Point™ VPN-1™ SecuRemote™.
- Secure smart card logon for Windows 2000 networks.
- Remote Access Server (RAS) dial-up connection management.

eBusiness Security Solutions

eBusiness security solutions include:

- Systems and services, such as:
  - Baltimore Technologies™ UniCERT™ CA.
  - VeriSign® .
  - Entrust® Technologies.
  - Digital Signature Trust (DST).
  - RSA Keon®.
- Web-based security clients, including SSLv3.
- Secure website access using Thin Client Technology (Active-X).

NOTE: In addition to the eToken set of ready-to-use security solutions, the eToken *Software Developer's Kit (SDK)* enables developers to integrate eToken with proprietary and third-party software applications.

For more detailed information about individual eToken solutions, downloads and documentation, and about the eToken SDK, please refer to: **www.eAladdin.com/etoken**.

FIPS

Overview

FIPS is the Federal Information Processing Standards. It is a US government approved set of standards. These standards are created by the National Institute of Standards and Technology (NIST) and are the official standards adopted under the provisions of Section 5131 of the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987. These mandates are designed to improve the utilization and management of computer and related telecommunications systems.

The NIST provides leadership, technical guidance and coordination of government efforts in the development of standards and guidelines in these areas.

eToken PRO

The eToken PRO can be enabled in FIPS mode for organizations that require this mode. The eToken PRO is compliant with the rules and procedures needed in order to meet FIPS #140-1 levels 2 and 3 requirements.

Depending upon your organization’s needs, a single token can be formatted as FIPS or non-FIPS. eTokens need to be formatted as FIPS tokens in order to be FIPS compliant. It is also possible to move between different eToken formats FIPS to non-FIPS or vice-versa.

For specific information on formatting eTokens, please refer to the eToken Utilities Guide.

Chapter 2

Getting Started with eToken

This chapter provides the basic information that you need in order to start using eToken, and gives detailed instructions for installing and personalizing eToken.

The following sections are contained in this chapter:

- "Minimum Requirements", on page 18, lists the hardware, software and operating system requirements for using eToken.
- "Installing the eToken RTE", on page 18, explains how to install the eToken runtime environment and eToken extension cable.
- "Personalizing the eToken", on page 23, explains how to change the eToken password and name.

Minimum Requirements

The following are the minimum requirements for using eToken:

- PC with at least 10 MB disk space.
- Windows 95, Windows 98, Windows NT 4.0 (with Service Pack 4 or later installed), Windows Me, Windows 2000 or Windows XP.
- Microsoft Windows Installer (MSI) 1.1 or later.
- Internet Explorer 5.0 or later.

  MSI 1.1 is included with all installations of Windows 2000 and Windows Me. Please see: www.eAladdin.com/etoken for details.
- At least one USB port, with USB support enabled in the BIOS.

NOTE: Additional software may be required for individual eToken solutions. For more information, please refer to **www.eAladdin.com/etoken**.

Installing the eToken RTE

The eToken runtime environment (RTE) includes all the necessary files and drivers to support eToken integration. It also includes the eToken Properties facility, which enables easy user management of the eToken password and name.

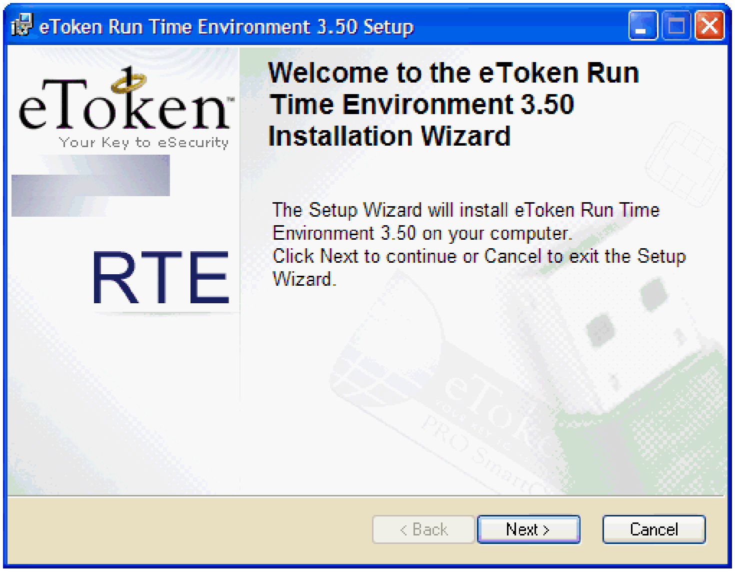
The eToken RTE (version 3.5) must be installed on each computer on which eToken is to be used.

NOTE: In order to benefit from the enhanced features provided by eToken RTE 3.5, it is recommended that any existing installations are upgraded from previous versions.

To install the eToken RTE:

1. Close all currently opened applications.
2. Insert the installation CD ROM which will launch automatically.
3. Click the **Install eToken RTE** link.

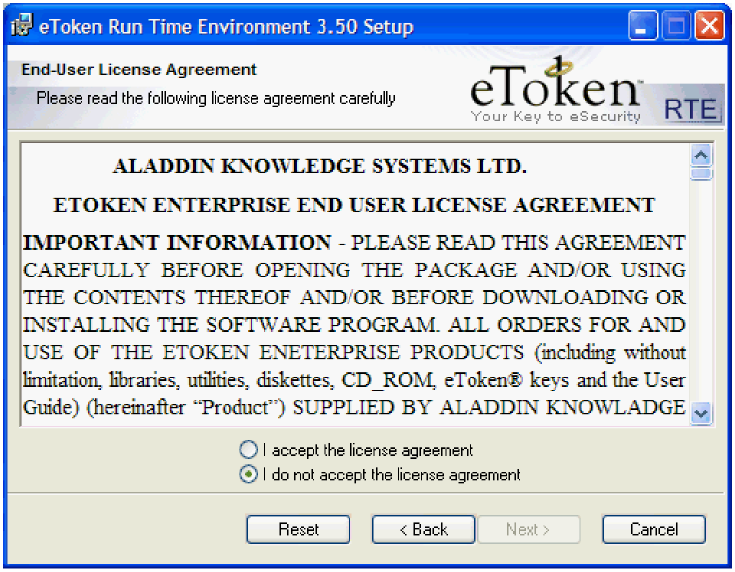
4 The eToken RTE Installation Wizard opens as displayed:



Welcome to the eToken Run Time Environment 3.50 Installation Wizard

The Setup Wizard will install eToken Run Time Environment 3.50 on your computer.
Click Next to continue or Cancel to exit the Setup Wizard.

5 Click **Next** on the eToken RTE installation window. The License Agreement is displayed:



End-User License Agreement

Please read the following license agreement carefully

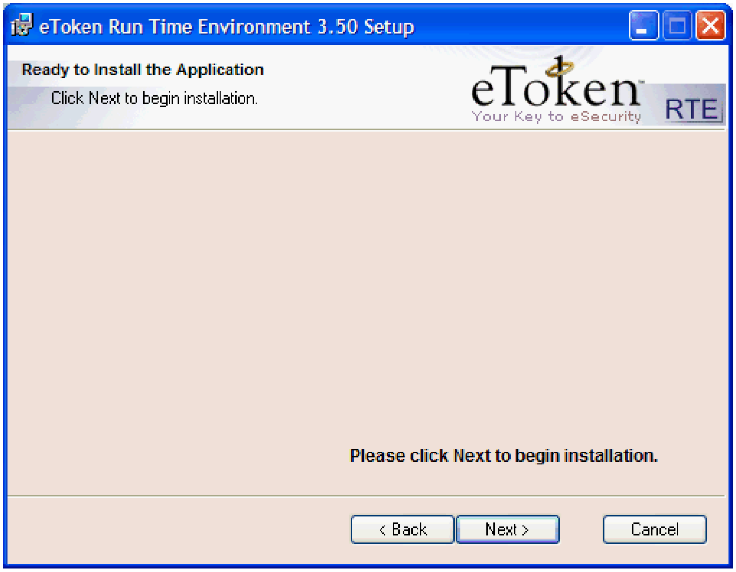
ALADDIN KNOWLEDGE SYSTEMS LTD.

ETOKEN ENTERPRISE 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 ENETERPRISE PRODUCTS (including without limitation, libraries, utilities, diskettes, CD_ROM, eToken® keys and the User Guide) (hereinafter "Product") SUPPLIED BY ALADDIN KNOWLADGE

○ I accept the license agreement
● I do not accept the license agreement

6 Select **I accept** and click **Next. The Ready to Install** window is displayed:



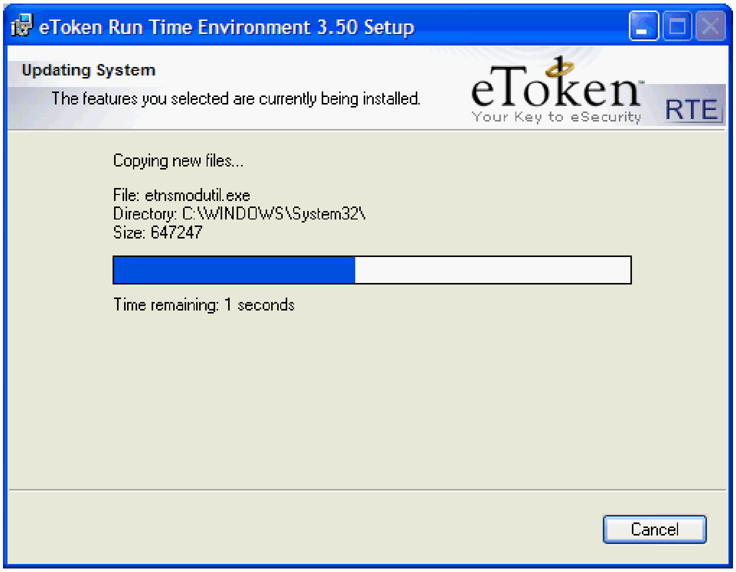
eToken Run Time Environment 3.50 Setup

Ready to Install the Application

Click Next to begin installation.

Please click Next to begin installation.

7 Click **Next** and the eToken RTE installation starts as displayed



eToken Run Time Environment 3.50 Setup

Updating System

The features you selected are currently being installed.

Copying new files...

File: etnsmodutil.exe
Directory: C:\WINDOWS\System32\
Size: 647247

Time remaining: 1 seconds

8 When the installation is complete, click **Finish**.

9 Connect an eToken to the USB port or cable. The new hardware is processed and the eToken lights up. This process may take some time, depending on the operating system and computer. The installation is successful.

If the USB port is not easily accessible, an eToken USB extension cable can be used, as described below. This extension cable enables you to insert and remove the eToken easily without having to access the USB port directly.

Connecting the eToken Extension Cable

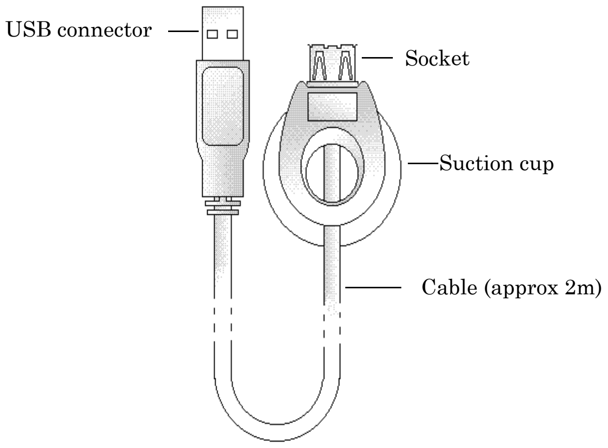
The eToken connects to the computer's USB port. If the USB port is located at the back of the PC, it is probably difficult to reach. The eToken extension cable enables easy access to the USB port for insertion and removal of the eToken. Extension cables are available from your local Aladdin dealer.

If a USB port or hub is located on the keyboard or monitor, you may not need an eToken extension cable. If the port is on the monitor, make sure that the monitor is connected to the USB port of the PC through a standard USB type A to type B cable.

Your eToken extension cable package includes:

- A round, translucent sticker.
- A cable, two meters (approximately six linear feet) long, with USB type A to type B connectors.

At one end of the cable is a socket and a special suction cup. This end should be mounted in a convenient place, so that you can easily insert and remove the eToken. At the other end of the cable is a small plug that connects to the existing USB connector on the PC.



To install the eToken extension cable:

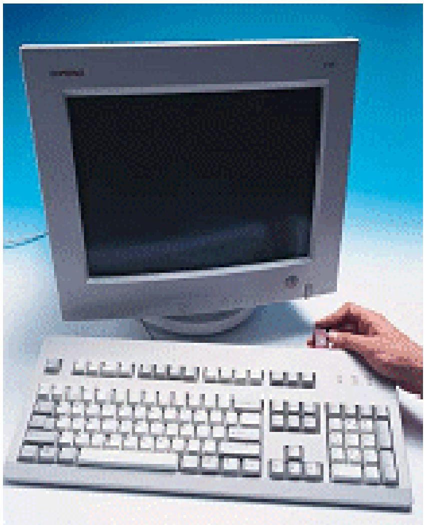
1. Locate the computer's USB port, and insert the small USB connector plug into it.
2. Peel off the sticker and paste it in a convenient place, for example, on the side of the monitor or on the casing of the PC.
3. Affix the suction cup of the eToken extension cable to the smooth surface of the sticker, pressing it firmly in place.
4. Plug the eToken into the cable socket and make sure it lights up.

Personalizing the eToken

All eTokens are configured at manufacture with the factory default password. This password is **1234567890**.

To ensure strong, two-factor security, and to enable full user functionality, it is important that the user changes the factory default password to an eToken password of the user's own choice, as soon as possible after receipt of a new eToken. For additional convenience and ease of identification, the eToken name can also be personalized.

After an eToken password has been changed, the new password must be used with the eToken for all eToken applications. It is the user's responsibility to remember the eToken password - without it, the eToken cannot be used for any purpose.



Password Quality

Your password is an important security measure in safeguarding your company's private information. Choosing an effective password is therefore critical.

The best passwords are at least 8 characters long and include upper and lower case letters, punctuation marks and numbers created in a random order. It is not recommended that you use names or birth dates of family members which can easily be discovered.

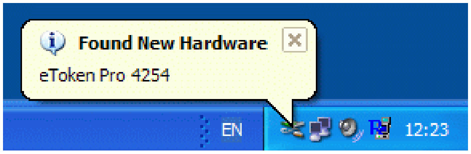
When changing your password, you can use the eToken Password Quality feature to ensure you are using the most secure password. The eToken Password Quality feature assigns a quality rating to your new password and provides you with tips on how to improve the password. For information on using eToken's Password Quality feature, refer to "eToken Password Quality", on page 67.

Enabling your eToken

After installing the RTE, it is necessary to enable the eToken the first time it is inserted into the USB port.

To enable the eToken:

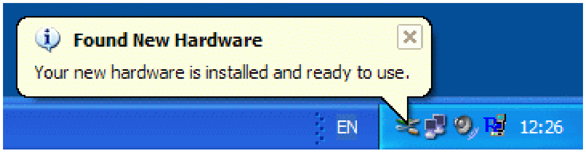
1 Insert your eToken into the USB port or alternatively the USB extension cable for the first time, the eToken lights up and during this process, which may take a few moments, the **Found New Hardware** pop-up on the Start Bar (The images displayed below are from a Windows XP system. The hardware recognition steps and messages may vary on other Operating Systems) is displayed:



Found New Hardware

eToken Pro 4254

2 The hardware installation continues until complete when the following pop-up is displayed:



Found New Hardware

Your new hardware is installed and ready to use.

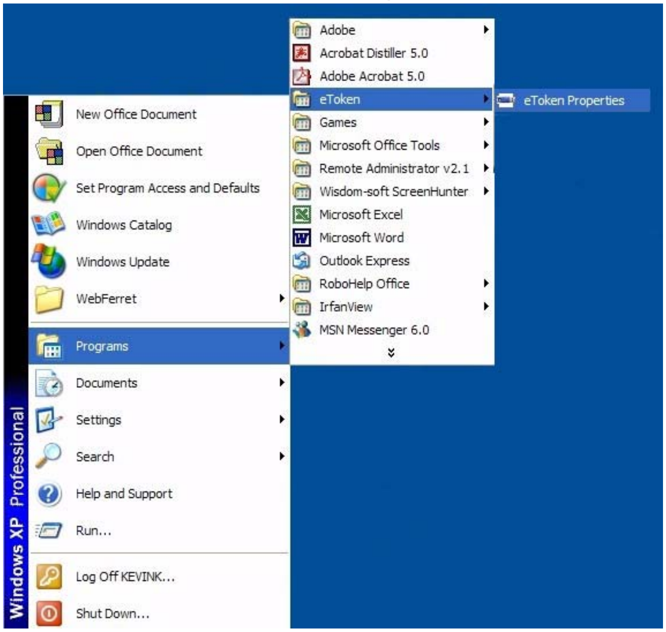
3 On completion, the eToken is now ready to be used.

Using the RTE

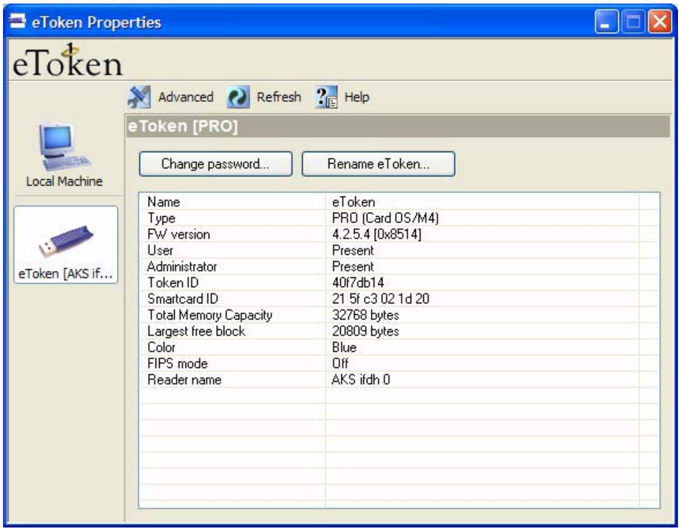
To enable and use your eToken with eToken Properties you must first start eToken Properties.

To use the RTE:

1 From the **Start** menu, select **Programs >eToken >eToken Properties** and the following is displayed:



2 Click **eToken Properties** and with your eToken inserted, the following screen is displayed:



Name	eToken
Type	PRO (Card OS/M4)
FW version	4.2.5.4 (0x8514)
User	Present
Administrator	Present
Token ID	40f7db14
Smartcard ID	21 5f c3 02 1d 20
Total Memory Capacity	32768 bytes
Largest free block	20809 bytes
Color	Blue
FIPS mode	Off
Reader name	AKS ifdh 0

3 You are now ready to work with eToken Properties.

Changing eToken Password and Name

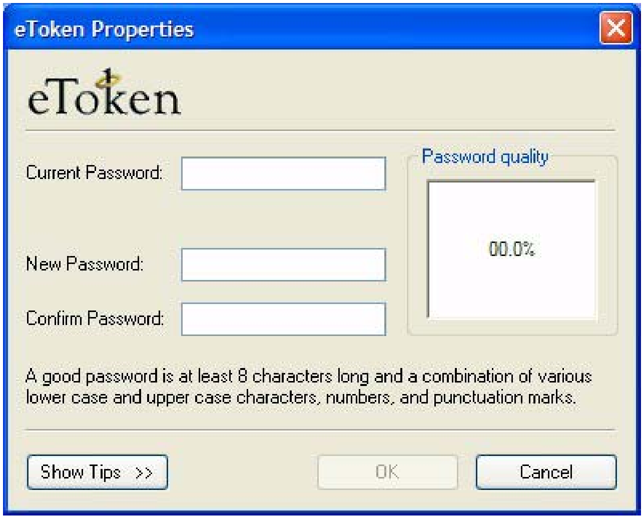
To ensure security you will be required to change the factory default password to a personal eToken password of your choice.

For additional convenience and ease of identification, the eToken name can also be personalized.

eToken Properties provides a simple user interface to the eToken, enabling users to personalize their eToken by setting and changing their own eToken password and name whenever they wish.

To change the eToken Password:

1 Click **Change password..** on the eToken Properties screen and the following eToken Properties dialog is displayed:



A good password is at least 8 characters long and a combination of various lower case and upper case characters, numbers, and punctuation marks.

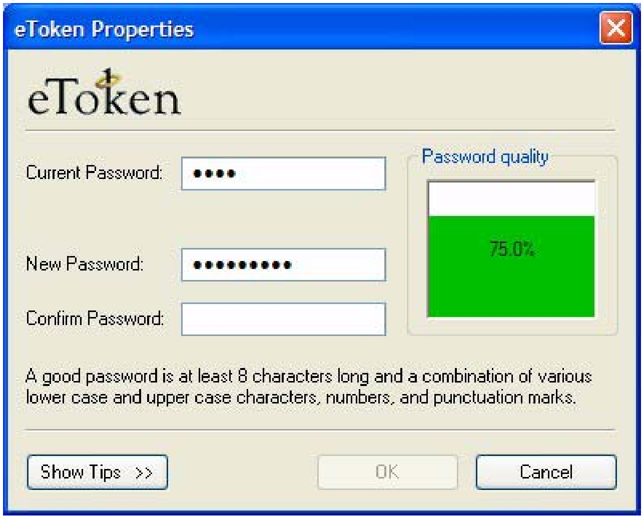
2 Enter your current eToken password in the **Current Password:** field.

3 Enter the new password in the **New Password:** field.

NOTE: As you type the password, the password quality indicator on the right displays how well the new password matches the password quality policy.

If you wish to view more information on why the password quality receives the score shown, click **Show Tips >>**. This expands the window to show a New password tips window. Following these tips will improve the password quality score.

The Password Quality indicator (on the right) provides a percentage score of the quality of the new password. Below the minimum required score, as defined in *etpass.ini*, the password quality indicator remains red. Once the score reaches and passes the minimum required, this color changes to green as displayed:



Current Password: ••••

New Password: •••••••••

Confirm Password:

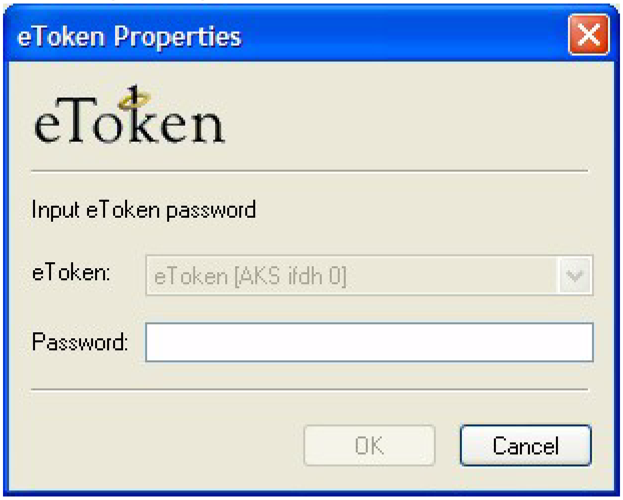
A good password is at least 8 characters long and a combination of various lower case and upper case characters, numbers, and punctuation marks.

4 Re-enter the new password in the **Confirm Password:** field and click **OK**. The eToken password is replaced.

NOTE: The password quality policy can be enforced if desired. For details on how to enforce such a policy, please refer to “eToken Password Quality”, on page 67.

To rename the eToken:

1 Click **Rename password..** on the eToken Properties screen. Since renaming the eToken requires the eToken password, if this is the first time the eToken password is needed, the following dialog is displayed:



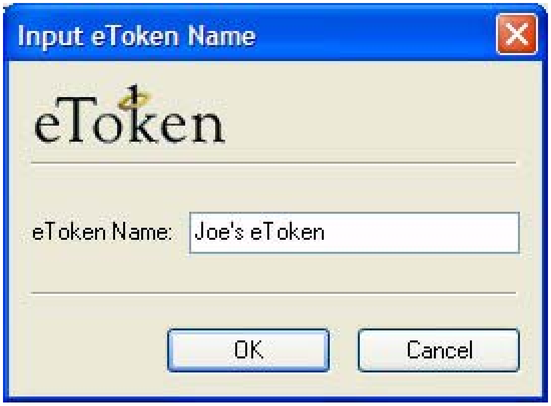
Input eToken password

eToken: eToken [AKS ifdh 0]

Password:

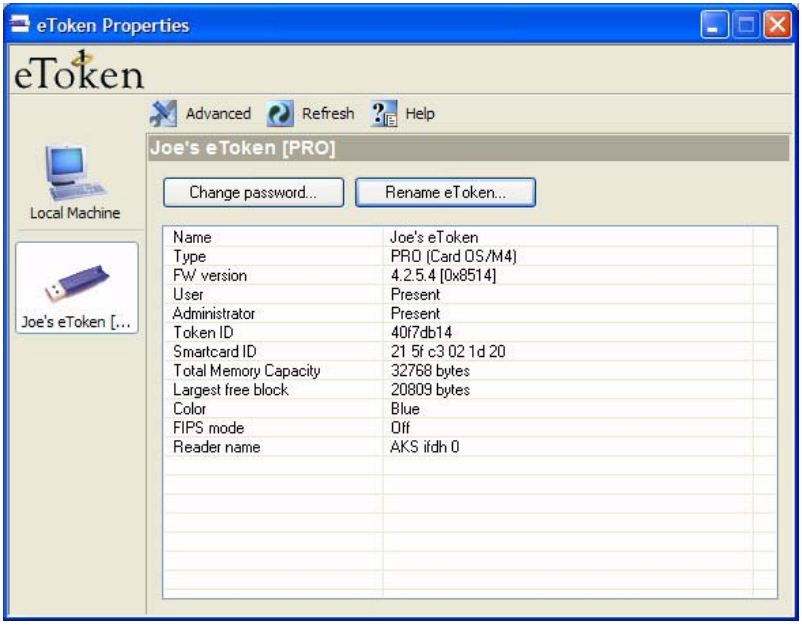
2 Enter the eToken password, click **OK** and the **Input eToken Name** dialog will be displayed.

3 Enter the new eToken name in the **eToken Name:** field, as displayed:



eToken Name: Joe's eToken

4 Click **OK** and in the eToken Properties window the new eToken name is displayed:



Name	Joe's eToken
Type	PRO (Card OS/M4)
FW version	4.2.5.4 (0x8514)
User	Present
Administrator	Present
Token ID	40f7db14
Smartcard ID	21 5f c3 02 1d 20
Total Memory Capacity	32768 bytes
Largest free block	20809 bytes
Color	Blue
FIPS mode	Off
Reader name	AKS ifdh 0

Chapter 3

eToken Properties

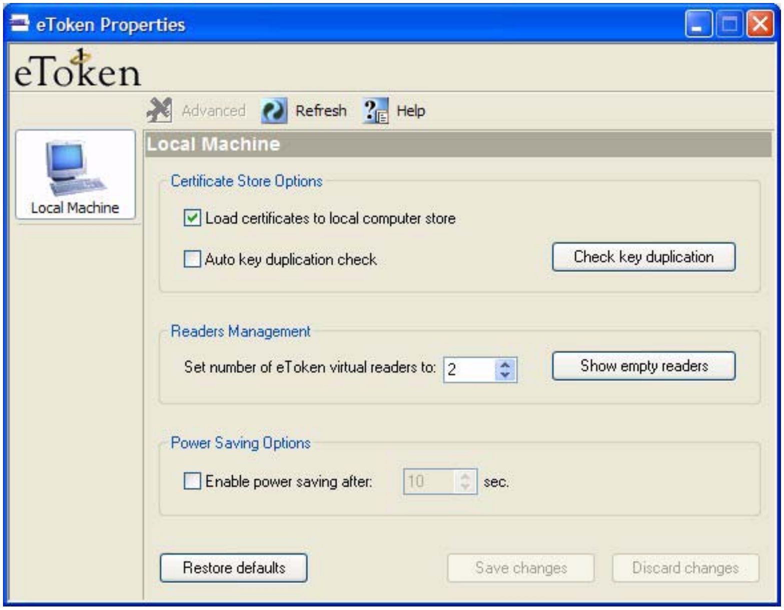
This chapter provides a brief explanation of what eToken Properties is and the various configuration options available to the administrator and user respectively.

The following sections are contained in this chapter:

- "Local Machine Configuration Options", on page 32 details the specific options available on the Local machine at all times.
- "eToken Configuration Options", on page 38 explains all the configuration options available in both Basic and Advanced mode as well as setting of administrator and user passwords.

Local Machine Configuration Options

The Local Machine configuration options enable setting global parameters that affect the eToken operation. These options are displayed when **eToken Properties** is launched (and no eToken is inserted) or when the **Local Machine** button in the left panel is clicked, as shown below:



☑ Load certificates to local computer store

□ Auto key duplication check

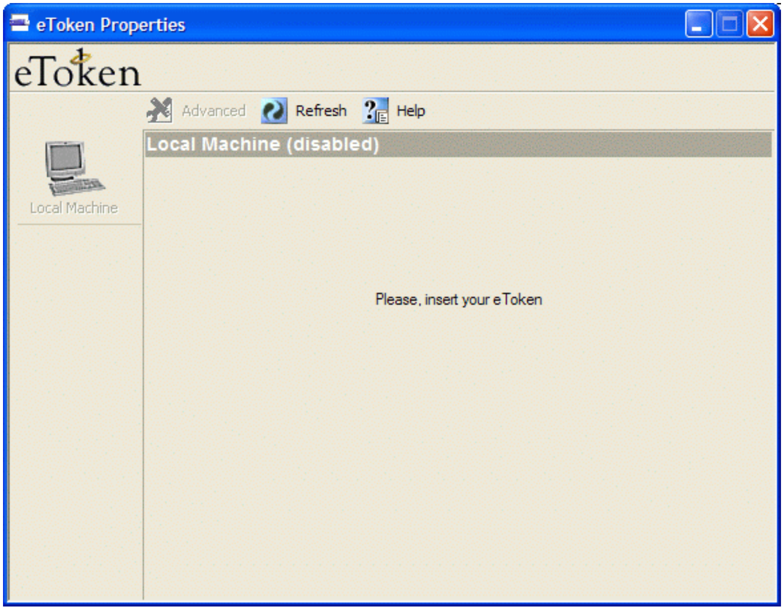
Set number of eToken virtual readers to: 2

□ Enable power saving after: 10 sec.

The window consists of a left vertical panel containing buttons and a right pane that contains information on the currently selected button.

The top button in the left panel is the **Local Machine** button, which is automatically selected when launching **eToken Properties**. The configuration options associated with this button are **not** specific to one eToken, but are general configuration options applicable to any eToken.

Some administrators may choose to disable **Local Machine** and **Advanced** features. In such a case the following is displayed:



Local Machine (disabled)

Please, insert your eToken

In order to use the application in this configuration you will need to insert an eToken.

Certificate Store Options

- **Load certificates to local computer store**

Default - enabled

PKI operations usually require certificates, private and public keys. Private keys should always be securely stored on the eToken. Certificates should also be stored on the eToken as this enables mobility (the certificate will be readily available when using the eToken on a different machine).

Since certificates themselves do not contain private information, checking this box enables pre-loading of certificates from the eToken and caching them on the local machine. This considerably speeds up accessing of these certificates by various applications, and can dramatically shorten response time when several certificates on the eToken need to be enumerated by an application.

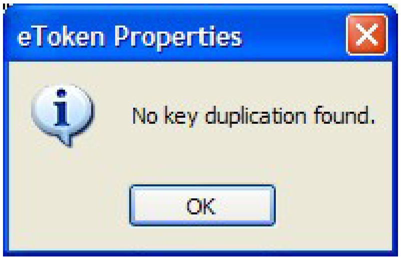
- **Auto key duplication check**

Default - disabled

It is possible that private keys have, in the past, been placed on the computer. This leads to duplication in that there is a key on the computer AND on the eToken. For effective security, only one private key should be allowed. This key should always be kept on the eToken in order to maximize security.

To perform an automatic key duplication check each time an application enumerates the eToken certificates, mark the **Auto key duplication check** checkbox. Note that this might slow down certificate and key operations.

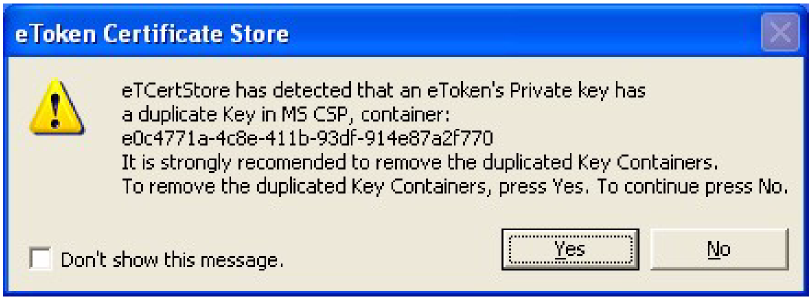
Alternatively, if you want to check whether the Auto Key is duplicated on an ad hoc basis, click **Check key duplication**. If no duplicate keys are found, the following pop-up is displayed:



eToken Properties

No key duplication found.

If duplicate keys are found, the following pop-up is displayed:

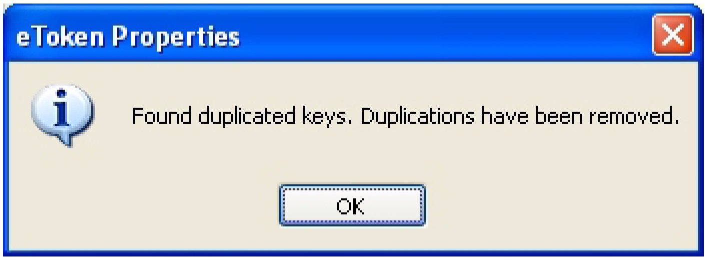


eToken Certificate Store

eTCertStore has detected that an eToken's Private key has a duplicate Key in MS CSP, container: e0c4771a-4c8e-411b-93df-914e87a2f770
It is strongly recomended to remove the duplicated Key Containers.
To remove the duplicated Key Containers, press Yes. To continue press No.

□ Don't show this message.

Click **Yes** to remove the duplicate keys from the computer and the following is displayed:



eToken Properties

Found duplicated keys. Duplications have been removed.

Readers Management

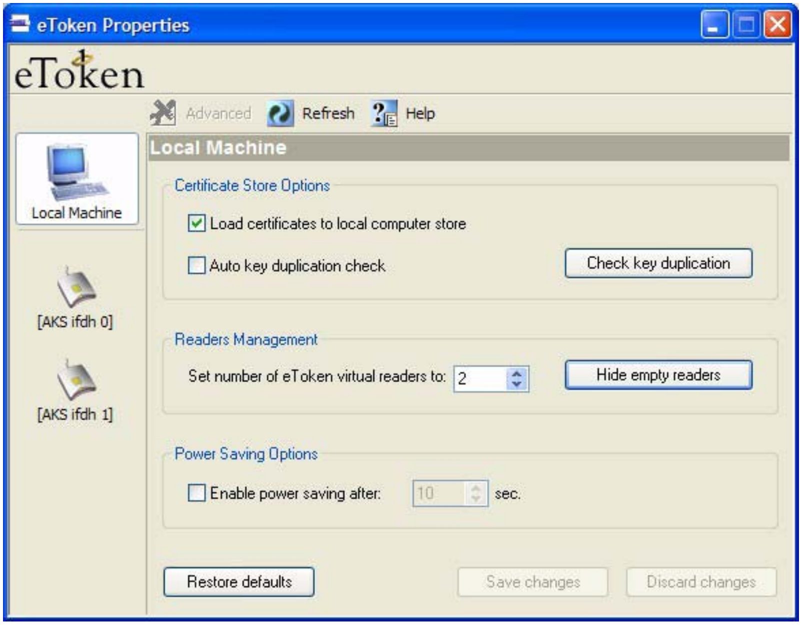
- **Set number of eToken virtual readers to:**

Default - 2 readers

eToken RTE setup installs two virtual readers. This means two eTokens can be recognized at the same time and accessed by applications using them.

You can change the number of installed readers by changing the value of this field and thereby increase or decrease the number of eTokens that can be recognized simultaneously by the system.

The **Show empty readers** button is a toggle button that allows you to see what readers are installed on the system. When you click this button, the Local Machine left panel changes as displayed:



Certificate Store Options

☑ Load certificates to local computer store

□ Auto key duplication check

Readers Management

Set number of eToken virtual readers to: 2

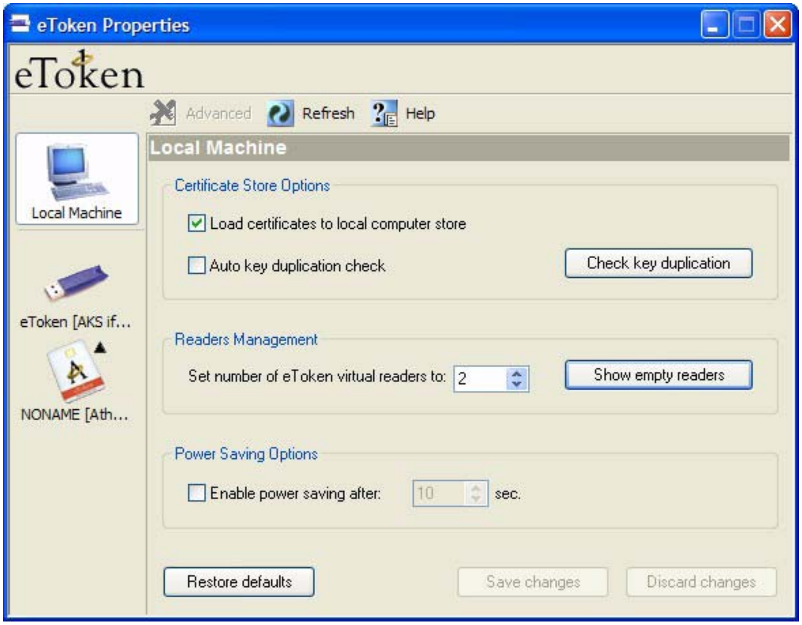
Power Saving Options

□ Enable power saving after: 10 sec.

Below the **Local Machine** button (left panel), are buttons which represent eTokens and/or smart card readers available on the system. When installing the eToken RTE, two virtual SmartCard readers are installed with it. The names of eToken SmartCard readers begin with **AKS ifdh**. This is followed by the reader number.

When an eToken is inserted into the USB port, it has the effect of inserting a SmartCard into one of the readers. The button's icon changes to an eToken icon to reflect this.

Physical SmartCard readers are also displayed if installed. Once a SmartCard is inserted into these readers, the reader icon will change to one with a SmartCard inserted as displayed:



Local Machine

Certificate Store Options

☑ Load certificates to local computer store

□ Auto key duplication check

Readers Management

Set number of eToken virtual readers to: 2

Power Saving Options

□ Enable power saving after: 10 sec.

Power Saving Options

- **Enable power saving after: ----Sec.**

Default - disabled

This enables Windows XP support for the USB "Selective Suspend" feature. This feature stops the USB host controller (HC) from polling if all ports are suspended and allows the processor to go to C3/C4 state. This option is particularly important when using laptops or other portable devices.

C3/C4 states are low power states for the processor in which the processor saves power and under typical use conditions allows for battery life to be extended by~10%.

When the **Enable power saving after...** button is checked, you have the option to change how many seconds before the power saving mode activates.

In order to activate the change made to the power saving configuration, you need to remove the eToken and then reinsert it.

General Control Buttons

Restore defaults

Clicking this button restores the local machine default configuration values.

Save changes

Clicking this button saves any changes that have been made to the local machine configuration values.

Discard changes

Clicking this button discards any changes that have been made to the local machine configuration values

eToken Configuration Options

Several operations which relate to eToken configuration options require entering either the eToken user password or the eToken administrator password. Once the required password has been entered, it is cached and there is no need to re-enter it during that session. The password cache is cleared when **eToken Properties** is closed.

Basic eToken Properties

After an eToken is inserted into the USB slot (or if **eToken Properties** is started with an eToken inserted), an icon indicating the eToken is accessible becomes visible in the left panel below the Local Machine icon.

The table below defines the fields in the basic properties window.

Items marked with (*) apply only to the eToken PRO.

Field Name	Field Description
Name	The name given to the token. This name can be changed by clicking **Rename eToken...**
Type	Product type description
FW version	The version of the eToken firmware.

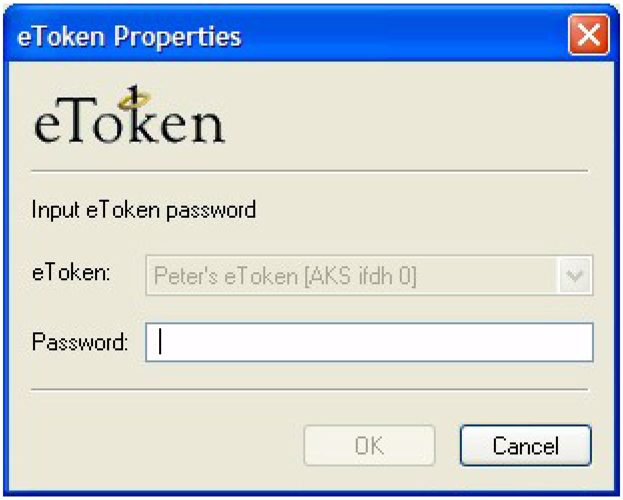
User	For the eToken R2 this value is always **Present**. For the eToken PRO this describes if a User has been defined for this token. Value is either **Present** or **Not Present**. A value of **Not Present** is displayed if the eToken was formatted without defining a user (blank token).
Administrator*	This describes if an Administrator has been defined for this token. Value is either **Present** or **Not Present**. A value of Present is displayed if the eToken was formatted with an administrator password.
Token ID	The unique ID for the currently inserted eToken.
Smartcard ID*	The unique smartcard ID for the currently inserted eToken PRO.
Total Memory Capacity	The total memory size of the eToken.
Largest free block	The size of the largest contiguous block of free memory currently available on the eToken.
Color	This field specifies the color of the eToken. This color is set during the eToken format process.
FIPS Mode*	Value can be either **On** or **Off**. This field specifies if the eToken was formatted as a FIPS token or not.
Reader Name	Describes the name of the reader. For USB eTokens, this will always begin with 'AKS ifdh'.

Advanced eToken Properties

eToken Properties provides additional functionality that enables setting various advanced configuration options for the eToken user and eToken administrator, if one or both have been defined for the eToken.

For more information on the roles of the eToken user and eToken administrator entities, please refer to the eToken Reference Manual.

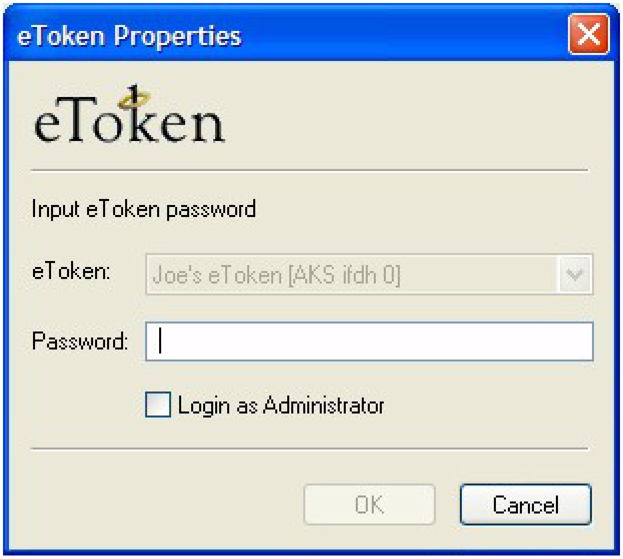
Click **Advanced** Advanced and for the eToken R2 or an eToken PRO formatted **without** an Administrator password the following dialog is displayed:



eToken: Peter's eToken [AKS ifdh 0]

Password:

For an eToken PRO, formatted with an Administrator password, the following dialog is displayed:



eToken: Joe's eToken [AKS ifdh 0]

Password:

☐ Login as Administrator

For the eToken PRO, you may log on as a user or as an administrator.

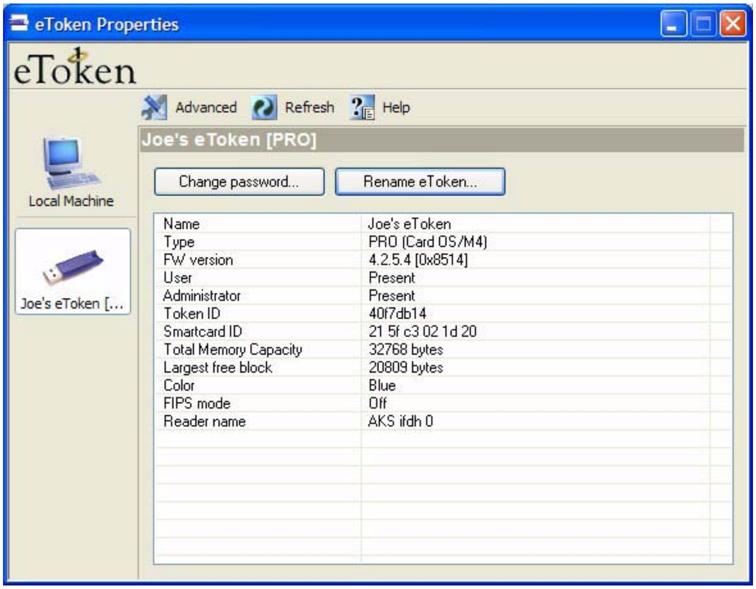
To log in as a user, enter the user password in the **Password** field and click **OK**.

To log in as an administrator, enter the Administrator password in the **Password** field, mark the **Login as Administrator** checkbox and click **OK**.

NOTE: **Administrator login and User functions**

If you log in as an administrator and wish to access functions that require a user password you will be requested to provide the eToken user password. Enter the eToken user password and click **OK**.

The **Advanced Properties** dialog is displayed:



Joe's eToken [PRO]

Name	Joe's eToken
Type	PRO (Card OS/M4)
FW version	4.2.5.4 [0x8514]
User	Present
Administrator	Present
Token ID	40f7db14
Smartcard ID	21 5f c3 02 1d 20
Total Memory Capacity	32768 bytes
Largest free block	20809 bytes
Color	Blue
FIPS mode	Off
Reader name	AKS ifdh 0

Advanced Properties consists of the following four tabs:

Details

Settings

Certificates and Keys

Administrator

NOTE: **Advanced Properties User access**

If you log in as a user, you do not automatically have access rights to the Administrator tab. See "Administrator tab", on page 50 for details.

Details tab

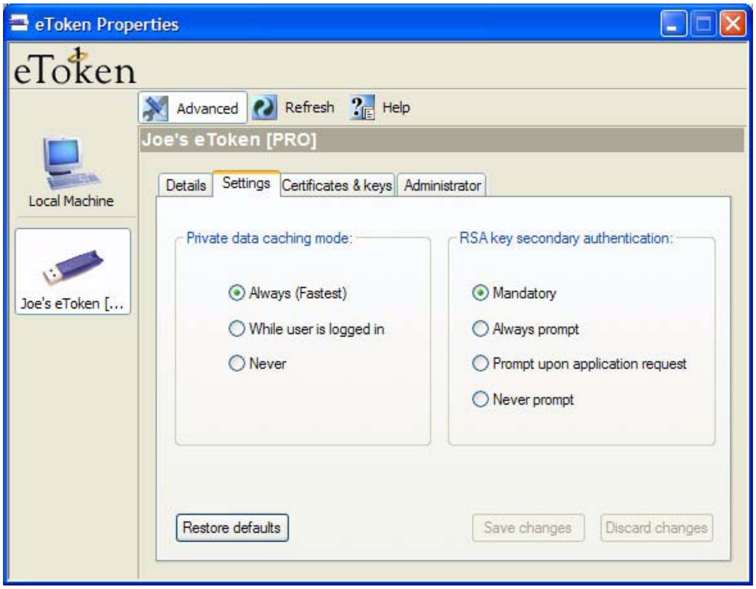
The **Details** tab provides the same information as the **Basic Properties** tab.

See "Basic eToken Properties", on page 38 for details.

Settings tab

This tab enables the configuring of settings relating to cache policies and RSA secondary authentication.

Where no administrator entity exists for the token, the user may set these parameters as displayed:



Private data caching mode:

● Always (Fastest)
○ While user is logged in
○ Never

RSA key secondary authentication:

● Mandatory
○ Always prompt
○ Prompt upon application request
○ Never prompt

Where an administrator entity exists, the administrator has the ability to allow or disallow the user to modify these parameters. This is done by marking one or both of the **Allow user to modify this option** checkboxes on the Administrator tab (Default - Allow):

- **Private data caching mode:**

In RTE 3.500, public information stored on the eToken is cached by the eToken drivers in order to enhance performance. This group defines the way private information (excluding private keys on the eToken PRO) is cached outside the eToken. The following options are available:

  - **Always (Fastest)**

  Always caches private information in the eToken drivers. This enables fast performance as certain information is cached on the host machine but because of this, this option is less secure than if no cache is allowed.

  - **While user is logged in**

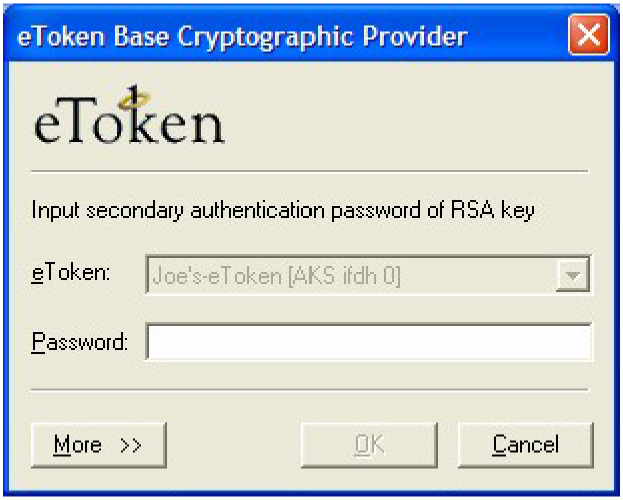
  Caches private data outside the eToken as long as the user is logged into the eToken. Once the user logs out, all the private data in the cache is erased.

  - **Never**

  Does not cache private data in the eToken drivers.

- **RSA key secondary authentication:**

In RTE 3.50, for the eToken PRO an option exists to set an additional authentication password for an RSA key. If this option is used, then in addition to having the eToken and knowing the eToken's password, accessing the RSA key requires knowing the password set for that particular key (as displayed below):



eToken Base Cryptographic Provider

Input secondary authentication password of RSA key

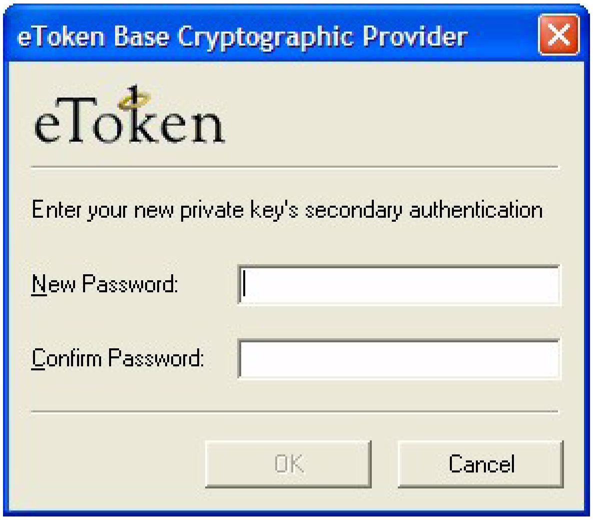
eToken: Joe's-eToken [AKS ifdh 0]

Password:

This group defines the policy for making use of this secondary authentication of RSA keys. Various options can be set for this policy:

- **Mandatory**

Every time an RSA key is generated, a secondary password for accessing this key is required as displayed:



Enter your new private key's secondary authentication

Clicking **Cancel** will cause key generation to fail. Clicking **OK** generates the key and uses the entered password as the secondary RSA password for that key.

- **Always prompt**

Every time an RSA key is generated, a secondary password for accessing this key is requested as above, however the user can choose to dismiss the prompt (by clicking **Cancel**) and key generation will continue without using a secondary password for the generated RSA key.

- **Prompt upon application request**

Enables applications that wish to use secondary authentication to RSA keys to make use of this feature on the eToken (when creating the key in Crypto API with a user protected flag).

- **Never prompt**

Secondary passwords will not be created for any RSA key and the authentication method will only use the eToken password to access the key.

Restore Defaults

Clicking **Restore defaults** restores the settings to their default values (private data is always cached and secondary authentication is never allowed). This is only possible if the eToken administrator has defined that the eToken user can modify these parameters.

Save Changes

Saving changes is only possible if the eToken administrator has defined that the eToken user can modify these parameters.

Clicking **Save changes** saves any setting changes that have been made.

Discard Changes

Clicking Discard changes discards any changes made to the private data cache settings or the secondary authentication policy.

Certificates & Keys tab

This tab shows the various certificates, keys and cryptography parameters available on the selected eToken. The following icons are used to identify the various PKI elements:

📜 " - Represents a certificate

🔑 " - Represents an RSA private key

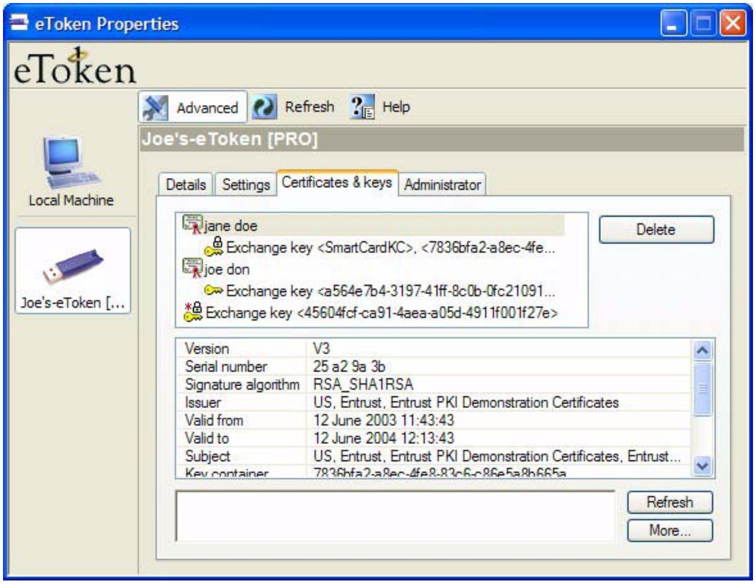
*🔑 " - Represents an RSA private key stored in a default key container

🔒🔑 " - Represents an RSA private key that requires secondary authentication

*🔒🔑 " - Represents an RSA private key that requires secondary authentication stored in a default key container

For more information on secondary authentication for private keys see “RSA key secondary authentication:”, on page 43.

The **Certificate & keys** tab is divided into three windows as displayed:



jane doe
Exchange key <SmartCardKC>, <7836bfa2-a8ec-4fe...
joe don
Exchange key <a564e7b4-3197-41ff-8c0b-0fc21091...
Exchange key <45604fcf-ca91-4aea-a05d-4911f001f27e>

Version	V3
Serial number	25 a2 9a 3b
Signature algorithm	RSA_SHA1RSA
Issuer	US, Entrust, Entrust PKI Demonstration Certificates
Valid from	12 June 2003 11:43:43
Valid to	12 June 2004 12:13:43
Subject	US, Entrust, Entrust PKI Demonstration Certificates, Entrust...
Key container	7836bfa2-a8ec-4fe8-83c6-c86e5a8b665a

The top window contains the list of certificates and keys that are stored on the eToken. The list is organized so that if a key corresponds to a certificate, the key appears directly below and to the right of the certificate it relates to.

The middle window (below the key and certificate list) provides information on a key or certificate selected in the top window. The following tables summarize the available information fields and their meaning for RSA keys and certificates.

Information for RSA Keys

Field Name	Field Description
Algorithm	Defines the cryptographic algorithm used.
Default KC	The key container used when no specific key container name has been specified when trying to acquire a key container handle.
Key Container	The key container is the place on the token where keys are stored. This field is the name of the key container that holds the selected key.
Key Length	The size of the key in bits.
Key Permissions	Specifies what actions are permitted for this key, e.g. if the key is exportable, the permission would be 0x00000001. eToken PRO keys always have permissions 0x00000000. eToken R2 keys may have permissions 0x00000004.
Secondary Authentication	Details whether the RSA key needs another password in order to be used. Valid for eToken PRO **only**.
Public Key	The public part of the RSA private key that enables encryption of messages, e. g. email, that can be decrypted and read only by the eToken owner (who holds the corresponding private key).

Information for RSA Certificates

Field Name	Field Description
Version	The version of the certificate format.
Serial Number	The serial number assigned by the certificate issuer.
Signature Algorithm	The algorithm used for the private key when using it for signing.
Issuer	The name of the organization that issued this certificate.
Valid from	The date the certificate becomes valid. The certificate cannot be used before this date.
Valid to	The date until which the certificate is valid. The certificate cannot be used after this date.
Subject	A combination of the purpose, conditions and name of the certificate owner might be used as the subject.
Key container	The name of the key container that holds the private key belonging to the certificate's public key.
Key spec.	The key specification that defines the purpose of the key.
Public Key	The content of the key that is part of the certificate and is used for encryption.
Certificate Usage	Details for what purposes the certificate is dedicated.
Friendly Name	A combination of the reader name:: and the simple display name of the certificate.

If one of the field names in the middle window is selected, all the field information is displayed in the bottom window. If required, this information can be copied to the clipboard by selecting the text and pressing **Ctrl+C**.

There are three buttons located to the right of the key and certificate list (top window). Clicking these button perform an action on the currently selected RSA key or certificate. The following table describes the key and the action that is performed on the selected RSA key or certificate when clicking that button

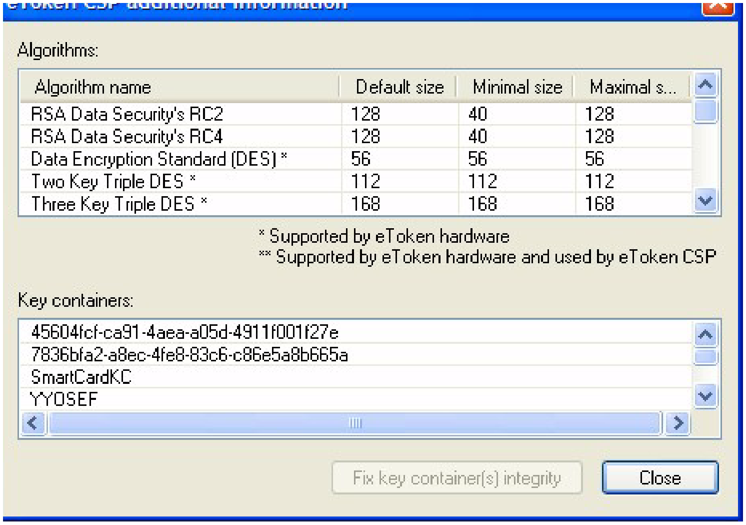
To the right of the certificate and key list window are buttons that perform an action on the currently selected RSA certificate or key as described in the following table:

	Removes the selected RSA key or certificate from the eToken. A confirmation message appears prior to performing this action.
	Sets the current key's key container as the default.
	This key is enabled only when an RSA key created with secondary authentication capability is selected. Key protection… enables setting a new secondary authentication password for the selected key.

To the right of the bottom window are the **Refresh** and **More...** buttons.

Clicking **Refresh** rescans the eToken for RSA keys and certificates.

Clicking **More...** button opens a pop-up window that provides additional information on the eToken CSP as displayed:



eToken CSP additional information

Algorithms:

Algorithm name	Default size	Minimal size	Maximal s...
RSA Data Security's RC2	128	40	128
RSA Data Security's RC4	128	40	128
Data Encryption Standard (DES) *	56	56	56
Two Key Triple DES *	112	112	112
Three Key Triple DES *	168	168	168

* Supported by eToken hardware
** Supported by eToken hardware and used by eToken CSP

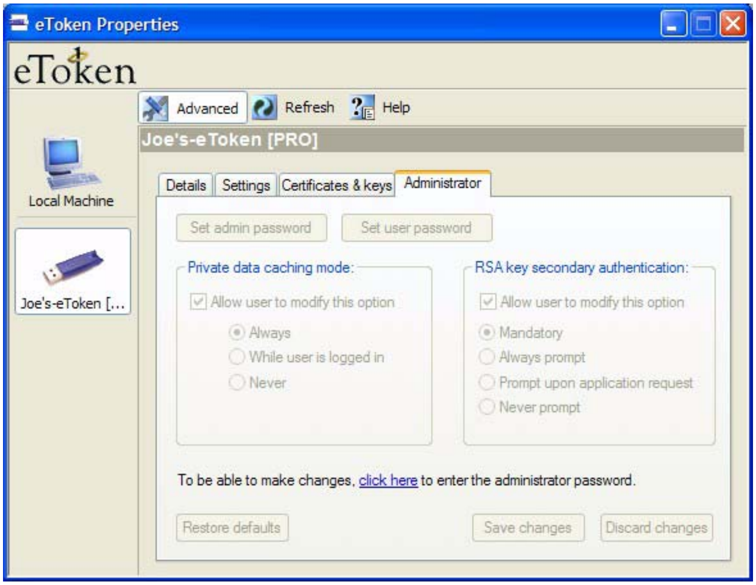
Key containers:

45604fcf-ca91-4aea-a05d-4911f001f27e
7836bfa2-a8ec-4fe8-83c6-c86e5a8b665a
SmartCardKC
YYOSEF

This window contains information on the set of available algorithms and the list of existing key containers.

Administrator tab

If logged on as a user, the administrator tab entries will not be accessible as shown below.



Joe's-eToken [PRO]

Private data caching mode:

☑ Allow user to modify this option

● Always
○ While user is logged in
○ Never

RSA key secondary authentication:

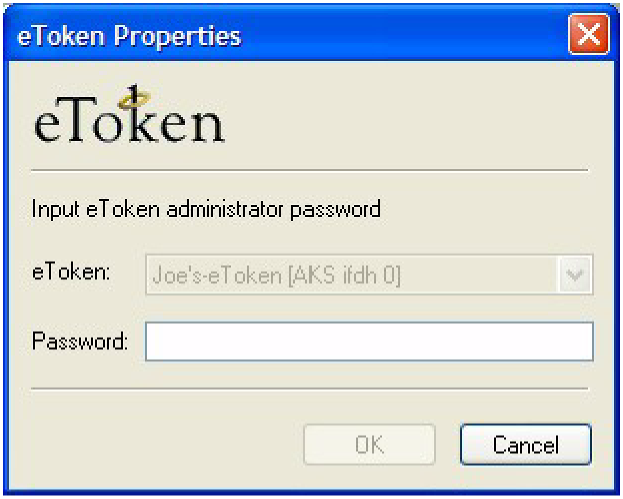
☑ Allow user to modify this option

● Mandatory
○ Always prompt
○ Prompt upon application request
○ Never prompt

To be able to make changes, click here to enter the administrator password.

Enabling them requires logging in as the administrator.

Click the link **click here**. This opens a pop-up window requesting the eToken administrator password as displayed:

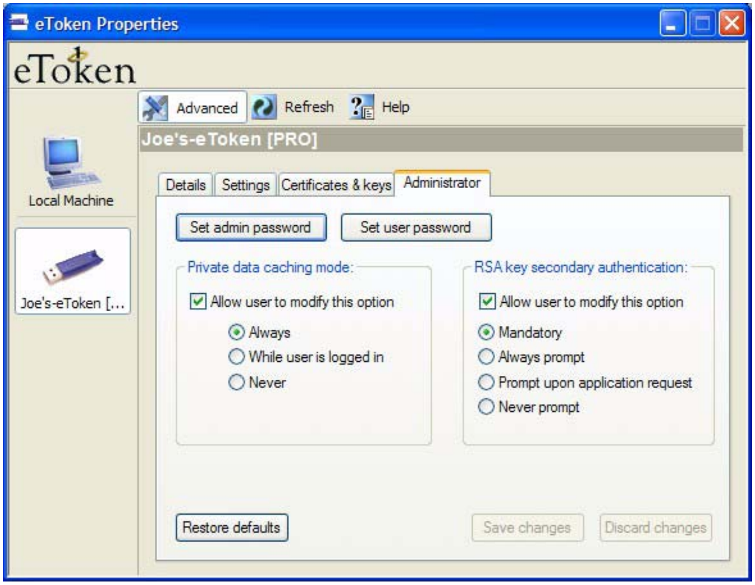


Input eToken administrator password

eToken: Joe's-eToken [AKS ifdh 0]

Password:

Enter the correct administrator password and the Administrator dialog is opened and active as displayed:



Joe's-eToken [PRO]

Private data caching mode:

☑ Allow user to modify this option

● Always

○ While user is logged in

○ Never

RSA key secondary authentication:

☑ Allow user to modify this option

● Mandatory

○ Always prompt

○ Prompt upon application request

○ Never prompt

The Private data caching mode: and RSA key secondary authentication options on the Administrator tab group are exactly the same as on the Settings tab

However, each group has an additional check box **Allow user to modify this option**. If this option is checked, the eToken user can change the settings set by an eToken administrator. If the option is unchecked, the user cannot change the administrator settings for these groups. For more information on these options, refer to the “Settings tab”, on page 42.

Clicking **Restore Defaults** will restore the default configuration for the Administrator settings (private data is cached and user cannot modify private data cache policy, secondary authentication for RSA keys is mandatory and user can modify RSA keys secondary authentication policy).

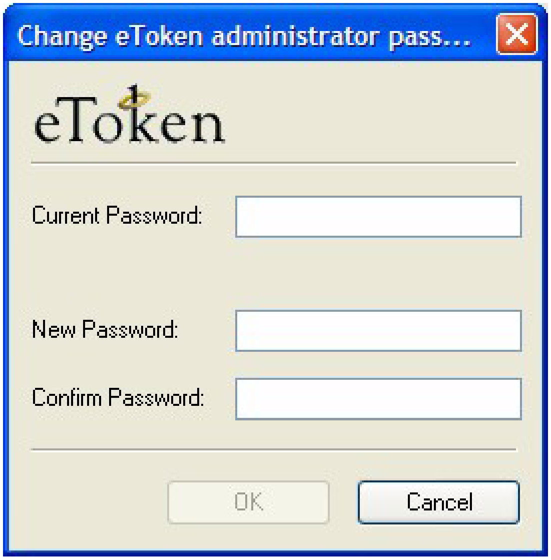
Clicking **Save Changes** will save all changes made to the Administrator settings.

Clicking **Discard Changes** will discard any changes made to the administrator settings.

If logged on as an eToken administrator, you have the option to set the eToken user password and change the eToken administrator password.

Setting the eToken Administrator Password

Click **Set admin password** to change the eToken administrator password and the following dialog is displayed:



Enter the current eToken administrator password in the **Current Password** field.

Enter the new eToken administrator password in the **New Password** field.

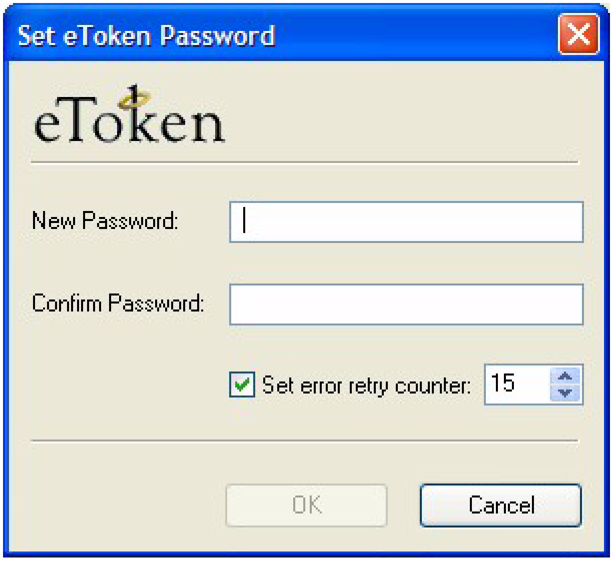
Reenter the new administrator password in the **Confirm Password:** field and click **OK**.

The eToken administrator password is replaced with the new administrator password.

Setting the eToken User Password

When logged in as an eToken administrator, you have the option to reset the eToken user password and error retry counter. This is usually used in cases where the eToken user password has been forgotten.

Click **Set user password** to change the current user password. The following dialog is displayed:



☑ Set error retry counter: 15

Enter the new user password for the eToken in the **New Password** field.

Re-enter the new user password in the **Confirm Password** field

Set the error retry counter if required, (default is 15 retries) and click **OK**.

The eToken user password is changed to the newly entered password and the retry counter is set accordingly.

If the error retry counter box is not checked, the eToken will not lock after any number of successive failed login attempts. As this can enable brute force attacks on the password, it is strongly recommended that you always set an error retry counter number.

Chapter 4

Security Concepts

This chapter provides a brief explanation of some of the major concepts relevant to the issue of corporate and eBusiness security.

The following sections are contained in this chapter:

- ”Security Risks and Corporate Vulnerability”, on page 56, outlines the security risks and concerns that are relevant to all commercial and public organizations.
- ”Password Storage and Authentication”, on page 59, explains the risks inherent in dependence on user passwords, how to improve the quality of your password, and highlights the use of eToken for secure password storage.
- ”Challenge-response Authentication”, on page 62, summarizes the use of the challenge-response mechanism for secure authentication.

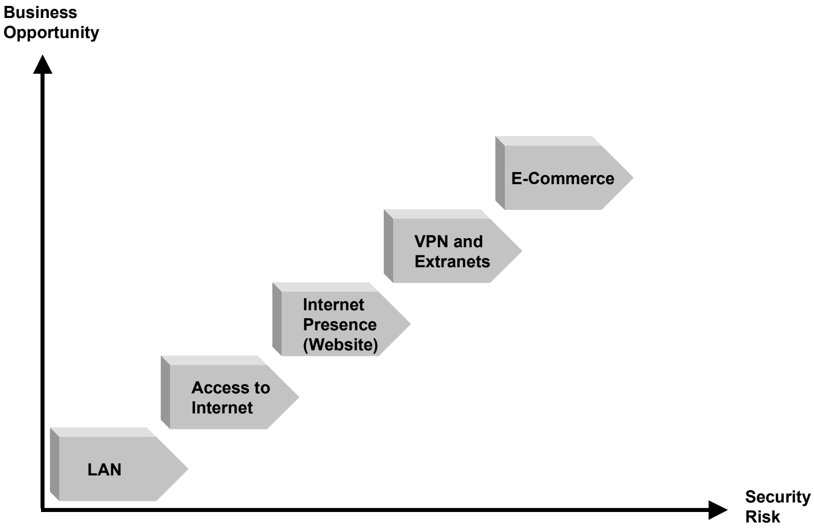
Security Risks and Corporate Vulnerability

In today's ever-changing e-commerce world, security is an essential requirement for any organization. Corporations are caught between the need for remote, convenient Internet and network access, and the need for protection from vandalism, espionage and theft.

The growth of the Internet and e-commerce, together with the opportunities they bring, have increased the need for secure communication between company networks, individual users, and the outside world.

As communication and commerce through the Internet increase, security risks for company networks also increase. Security issues have now become a crucial factor in determining an organization's accessibility to the Internet.

The diagram below illustrates how security risks increase as an organization opens itself up to Internet activity.



According to a survey recently conducted by the FBI, concerns over these security risks are not unfounded. In the *2000 CSI/FBI Computer Crime and Security Survey*, in which over 600 companies were polled, losses were reported totalling some $265 million.

These losses are due to saboteurs, viruses, laptop theft, financial fraud, telecommunications fraud and stolen proprietary information.

Organizations are installing intranets and extranets, in order to connect an increasingly mobile workforce in need of remote access to corporate information systems.

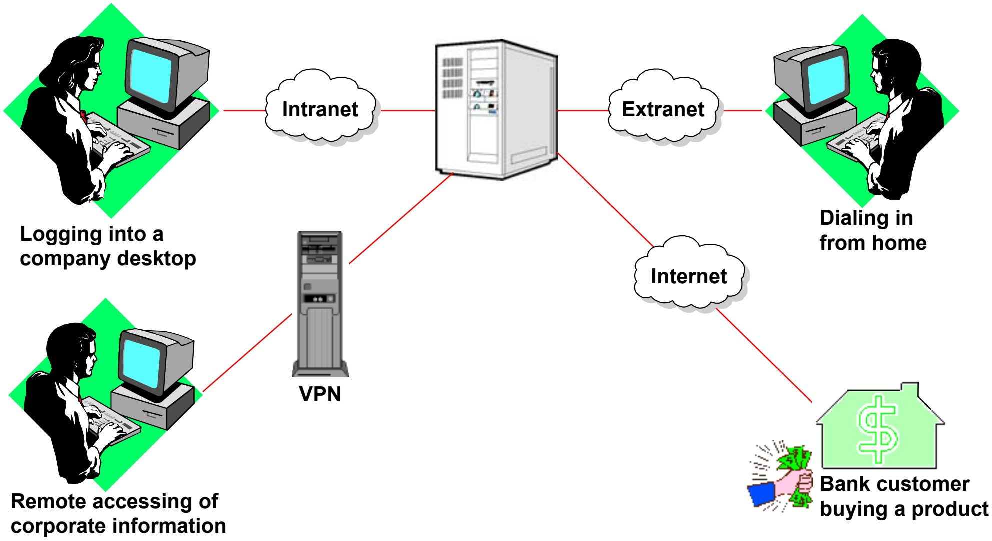
Corporations are creating direct sales sites for their business customers, making these companies more open to illegal access and computer crime.

Every commercial enterprise should be aware of the following:

- Computer security breaches have risen 16% in the last year, according to the *2000 CSI/FBI Computer Crime and Security Survey*. The same survey also revealed that 74% of respondents acknowledged financial losses due to computer security breaches.
- Another recent survey, this time from KPMG Peat Marwick in New York, revealed that some 41% of respondents found security concerns the most significant barrier to their ability to perform web-based e-commerce.
- Password files are regularly stolen by hackers using applications freely available on the Internet. These applications are easy enough for complete novices to master.
- Firewalls, the current popular security solution, do not provide complete security. Recent surveys have indicated that 80% of saboteurs are disgruntled employees.

As Ehud Tenenbaum, the 18-year-old hacker known internationally as the Analyzer, said: "I would move around the Internet asking myself: 'Who should die today?' And by 'die', I mean cut off from the Internet."

The following diagram illustrates the vulnerability of communications networks to the risks of unauthorized access:


Intranet
Extranet
Logging into a company desktop
Dialing in from home
Internet
VPN
Remote accessing of corporate information
Bank customer buying a product

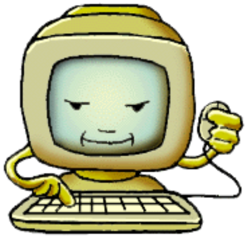
Password Storage and Authentication

eToken helps reduce these inherent security risks by providing secure storage for user passwords.

How Safe is a Password?

Relying on one-factor authentication - a memorized password alone - seriously weakens the security of any system.

Passwords that are typed in to the keyboard of a PC or laptop can be easily copied and can also be hacked. Users often have difficulty remembering several passwords for different applications, so they use the same password for all their access needs.



They often select a short password that is easy to remember (and easy to guess), such as the name of one of their children or their birthday.

In spite of all advice, passwords are seldom changed and are often written down and left in easily accessible places, such as in a desk drawer or on a sticky note on the monitor.

Storing a user's access details and authentication passwords on an eToken significantly enhances access security. eToken provides strong password protection, as well as portability and convenience.

eToken provides full two-factor authentication - the user must both connect the eToken and enter the individual eToken password in order to gain authorized access.

Copying or hacking the eToken password is of no value without the physical eToken. Users do not need to remember different passwords for access to different applications and accounts, only the password for their personal eToken. They can take all their authorization details with them, on their key chain or in their pocket or purse.

For details of eToken integration for password storage for Virtual Private Network (VPN) access, see: **www.eAladdin.com/ eToken**.

Password Quality

Your password is an important security measure in safeguarding your company's private information. Effective password security consists of the following main tenants:

- Do not tell anyone your password.
- Do not write down your password anywhere.
- When deciding upon a password, make sure that someone cannot guess it.
- If there is even a slight chance that someone else may know your password, change it.

A good password should contain at least three of the following four elements:

- It should be more than 8 characters in length
- It should contain upper and lower case letters
- It should contain numbers
- It should contain special characters

What not to do:

- Do not send your password via email. Email is not secure.
- Do not store your password in a file on your computer.
- Do not use the dictionary or foreign words, names, doubled names, first/last names and initials.
- Stay away from simple transformations of words (e.g., 7eleven etc.) or any alphabet or keyboard sequence (backwards or forwards).

- Do not use short words, single characters, phone numbers, birthdays, or numbers substituted for letters (e.g., zero instead of the letter O).
- Be wary of programs that unnecessarily require your password. Once you are logged in to a given computer system, it should not need to know your password again.

The following are three strategies for choosing a good password:

1. Use lines from a childhood verse:

   Verse Line: Yankee Doodle went to town

   Password: YDwto#town

2. Expressions inspired by the name of a city:

   City expression: Chicago is my kind of town

   Password: CimYkot

3. Transformation techniques:

   Illustrative Expression: photographic

   Password: foTOgrafik

Rating your eToken Password

When changing your password, you can use the eToken Password Quality feature to ensure you are using the most secure password. The eToken Password Quality feature assigns a quality rating to your new password and provides you with specific tips on how to improve your password. For more information on using eToken's Password Quality feature, refer to ”Changing eToken Password and Name”, on page 26.

Challenge-response Authentication

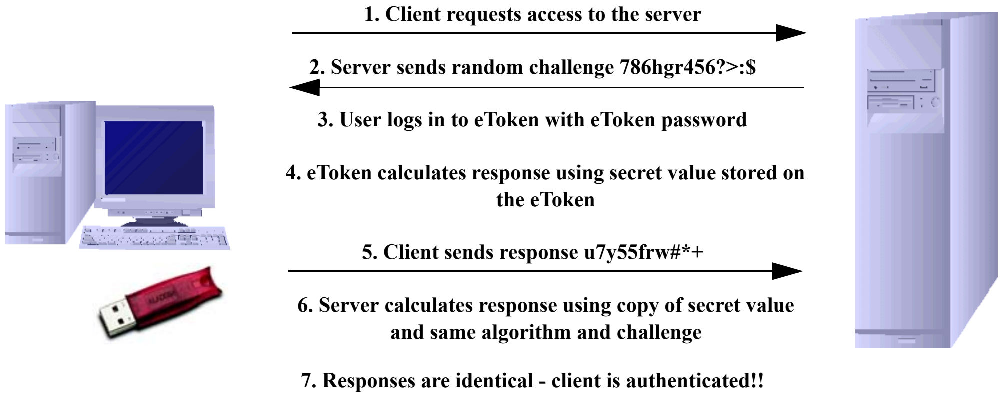
A challenge is a value sent by an authenticating party, such as a company's server, to a party or device requesting to be authenticated. Since the connection between the two parties is usually not secure, the authentication process is vulnerable if the challenge and response are always the same. A secure challenge has a different value each time it is issued, and requires a different response each time.

The challenge is usually chosen as a purely random message. As a result, the challenge value is always unpredictable.

The party being authenticated uses an algorithm and its own copy of a secret value to compute a response to the challenge. The server holds its copy of the same secret value, and computes a response using the same algorithm. If the returned response is identical to the server's computed response, the challenged party is considered genuine.

With eToken, the secret value is held on the eToken and is never revealed or transmitted between the two parties. The response that is sent across the Internet or network is the computed result, produced entirely within the secure environment of the eToken.

The following diagram illustrates a simple challenge-response mechanism for client authentication:



1. Client requests access to the server

2. Server sends random challenge 786hgr456?>:$

3. User logs in to eToken with eToken password

4. eToken calculates response using secret value stored on the eToken

5. Client sends response u7y55frw#*+

6. Server calculates response using copy of secret value and same algorithm and challenge

7. Responses are identical - client is authenticated!!

This mechanism can be used in more complex authentication protocols. For example, SSLv3 combines challenge-response with the use of digital certificates and signatures, to achieve a highly secure method of authentication.

For information about eToken integration with SSL v3 for secure web access, see the **www.eAladdin.com/eToken.**

Chapter 5

eToken Administration

Administering eToken in an organization is simple and straightforward. This chapter provides administration guidelines in respect of the Administrator's role in defining the RTE 3.50 features to be used and how to manipulate these features.

The chapter covers the following sections:

- "Setting Up a New eToken User", on page 66, outlines what needs to be done to set up a new user with eToken.
- "Issuing Replacement eToken", on page 66, explains what actions to take in the event of damaged, lost or stolen, or forgotten eToken passwords.
- "Recovering eTokens from Employees", on page 67, explains what to do when eToken users leave the organization.
- "Formatting eToken", on page 67 provides general information on the process of formatting an eToken.
- "eToken Password Quality", on page 67 explains the various settings used in amending the Password policy.
- "Registry Settings for eToken Properties", on page 72 explains how to manipulate certain registry keys.

For detailed instructions for installing, integrating and using specific eToken solutions, please refer to **www.eAladdin.com/etoken**.

Setting Up a New eToken User

When a new employee joins the organization, do the following:

- Install the eToken RTE on the employee's computer.
- If required, install any additional installation for the relevant eToken solution.
- Issue the employee a new eToken, with the instructions for personalizing it. See "Personalizing the eToken", on page 23.

In eToken RTE 3.00 and prior versions, the Administrator password functionality was limited to opening a blocked user password and enabling the formatting of FIPS tokens.

In eToken RTE 3.50 the Administrator password is also used to protect certain configuration files.

NOTE: The first time an administrator uses the token (e.g. login/change password), a few of the password attributes are changed according to the new RTE functionality. Among these changes is that the Error Retry counter is automatically set to 15 times, regardless of the actual Format setting.

Issuing Replacement eToken

A user's eToken may need to be replaced if the eToken is lost or damaged. When a user reports a lost or damaged eToken, you should discard the eToken and issue the user another eToken, with a requirement to personalize it as soon as possible.

If the user forgets the eToken password there are two different solutions depending on whether the eToken R2 or eToken PRO is being employed.

In the eToken R2, if a user forgets the password for his or her personal eToken, it cannot be used for any eToken-based operation. The eToken password is stored securely on the eToken, and it is not possible to reset it or replace it.

In this case the procedure for dealing with a forgotten eToken password is exactly the same as for a lost or damaged eToken.

In the eToken PRO, if a user forgets the eToken password, the eToken can either be reformatted whereby the token’s details are erased and the token is reset to the default password, or the user password can be reset using the system administrator password with all of the token’s details preserved.

Recovering eTokens from Employees

When an employee leaves the organization, in addition to taking the standard actions, such as revoking any current certificates and closing network accounts, you should recover his or her eToken and its password. You can then choose to discard the eToken, or to change the current password and reuse the eToken.

If you are unable to recover the eToken password from the employee, the eToken is unusable, and you should discard it. An eToken can be used only on computers that have been set up for use with specific eToken Enterprise security applications.

Formatting eToken

The eToken Format Utility erases all data on an eToken PRO and resets the file structure according to various configurable parameters. In addition the utility can set the Administrator password and other functional parameters.

The eToken can be formatted as a standard eToken PRO, as a FIPS eToken PRO and as a blank eToken.

For detailed information on the eToken Format utility, please refer to the Utilities v2.0 Reference Guide.

eToken Password Quality

Altering the password changing policy is controlled by the *etpass.ini* file in the OS system directory. The eToken RTE installation installs an *etpass.ini* file if not already present. If such a file is present, the existing file remains intact and is not changed.

However an IT administrator can define different settings for this file and replace the existing *etpass.ini* file on any user's machine.

The *etpass.ini* file controls the password changing policy when using an eToken application. When using other (i.e. non eToken) application mechanisms to change the eToken password (e.g. changing the password via Netscape) these settings are not relevant.

The eToken Password Quality Tool enables the creation of a password quality policy for the eToken. The Password Quality tool uses definitions from the et*pass.ini* file, located in the system folder, to define the quality of a given password. The Password is rated based on different parameters that have been assigned penalties, which are used to calculated the password rating.

NOTE: The *etpass.ini* file can be edited and distributed over the network to all user stations using a logon script.

Password Quality Parameters

The various parameters all have a variable assigned value determined by the Administrator in accordance with the organization's password quality policy. The value of the parameter will be determined in accordance with the importance that each parameter has in the determination of that policy.

A brief description and explanation of each parameter listed in the *etpass.ini* file follows:

- **ABCOrder** **Consecutive letters penalty**

Use of consecutive letters in the new password.

- **ABCOrderBase** **Consecutive letters base**

The minimum number of consecutive letters in the new password that will create a penalty. Each additional consecutive letter used will add a further penalty.

- **CheckCurrPass** **Current password penalty**

Use of the current password as the new password.

- **CheckDictionary** **Dictionary password penalty**

Use of a word from the dictionary file as the new password.

- **CheckOldPasses Old password penalty**

Use of a password that was previously used as the new password.

- **DefaultPassChange Changepassword policy**

The policy for using the eToken default password at login time allows for 3 modes:

- **None** - No action if default kept.
- **Warning** - A warning message will be displayed.
- **Enforce** - User cannot use default and must change it.

- **Dictionary Dictionary file name**

The name of the dictionary file which contains a list of poor passwords as determined by you.

Each line in the file represents one password. Different passwords need to be on different lines.

See CheckDictionary for penalty details.

- **DigitsOnly Digits only penalty**

Use of digits only as the new password.

- **Duplicates Duplicates penalty**

Use of duplicate characters in the new password.

- **Expiry Password expiry warning**

The specified number of days to use the password before it is recommended to be changed.

- **ExpiryEnforce Password expiry (days)**

The current password is valid only for the specified number of days and will expire at the end of this period.

- **KeyboardProximity Keyboard proximity penalty**

Use of keyboard letters next to each other in the new password.

- **KeyboardProximityBase**
Keyboard proximity base

The minimum number of letters next to each other on the keyboard in the new password that will create a penalty. Each addition will add a further penalty.

- **LikeDictionary** **Dictionary like password penalty**

Use of a word that is like a word from the dictionary file (e.g. one character different from a dictionary word) as the new password.

- **MinChangePeriod** **Minimum change period**

The minimum number of days **before** the password can be changed.

- **MinimalLength** **Minimal password length**

The minimal password character length is as specified. Less than this length is not allowed.

- **MinimalQuality** **Minimal password quality**

The minimum percent password quality that is allowed.

- **NoDigits** **No digits penalty**

Use of no digits in the new password.

- **NoLowerCase** **No lower case penalty**

Use of no lower case characters in the new password.

- **NoPunctuation** **No punctuation penalty**

Use of no punctuation marks in the new password.

- **NoUpperCase** **No upper case penalty**

Use of no upper case characters in the new password.

- **OptimalLength** **Optimal password length**

The optimal password character length is as specified. Use of less than optimal character password length determines the basis of the penalty calculation (e.g. using an 8 character password in a 10 character optimal length password will result in an 80% quality level, before other penalties).

- **PhonesandSerialNumbers** **Phones and serial numbers penalty**

Use of telephone, social security, serial, license numbers etc. in the new password.

- **Repeating** **Repeating penalty**

Use of repeating characters in the new password.

- **SaveOldPasses** **Save old passwords**

The number of previously used passwords that will be encoded and stored on the eToken and not available for reuse.

- **SmallPassword** **Small password penalty**

The penalty in the quality score for each character below the length of WarningLength.

- **WarningLength** **Warning password length**

The length of the password below which a warning is issued in the quality check.

- **WhiteSpaces** **White spaces penalty**

Use of white spaces instead of characters in the new password.

A sample Password INI file with appropriate settings is detailed below:

```
[Password Quality]

MinimalLength = 4
WarningLength = 6
OptimalLength = 12
SmallPassword = -5%

Duplicates = -20%              ; for each duplicate symbol
Repeating = -20%               ; for each symbol in chain

NoLowerCase = -5%
NoUpperCase = -5%
NoPunctuation = -5%
NoDigits = -5%
DigitsOnly = -5%
```

```
PhonesAndSerialNumbers = -5%
WhiteSpaces = -100%
NonPrintable = -100%            ; denied

KeyboardProximity = -10%
KeyboardProximityBase = 3        ; characters

ABCOrder = -10%
ABCOrderBase = 3                 ; characters

Dictionary =                     ; file name
CheckDictionary = -100%          ; denied
LikeDictionary = -80%

Expiry = 360                     ; days
ExpiryEnforce = 0                ; days
MinChangePeriod = 0              ; days

SaveOldPasses = 3                ; history length
CheckOldPasses = 0%
CheckCurrPass = -100%            ; denied
DefaultPassChange = enforce      ; enforce/warning/none

MinimalQuality = 30%
```

Registry Settings for eToken Properties

An IT administrator can control the behavior of some of the RTE features installed on a user machine by manipulating Registry Keys. Some of these keys can be set via the installation process (see “RTE Installation - Command Line Options”, on page 75).

NOTE: It is up to the IT administrator to set the security attributes of these registry keys - so that a user will not be able to change them.

eToken CertStore Settings

- **eTCertStore - Load Local**

Load Local Option, of eToken Certificate Store, automatically loads the eToken certificates to the registry the first time an application enumerates the certificates. The Load Local option has some effect on Certificate's related operations. This option is controlled by a registry key.

Registry Key:

HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTCertStore

Value:

DWORD LoadLocal:

If set to 1 the Load Local is activated. This option can be set during command line installation of the RTE (See “RTE Installation - Command Line Options”, on page 75).

- **eTCertStore Key Duplication Test**

In different situations, keys that are being imported to the token might be found on the Host machine (managed by MS CSP). For security reasons, eToken keys should not be stored on the local machine as well. **eToken CertStore** can perform an automatic duplication key test during Certificate Enumeration. This test has an overhead that affects performance - and could be significant if there are many keys in the registry. The Automatic Key Duplication Test is controlled by a registry key.

Registry Key:

HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTCertStore

Value:

DWORD DuplicateKeyTest.

If value is set to 0 - **No** automatic test will be performed. This registry key is also controlled by **eTProperties** under Local Machine section. In addition, the key can be set during command line installation of the RTE (See “RTE Installation - Command Line Options”, on page 75).

- **eTCertStore Load Local Ignore**

In some applications (e.g. eTProperties) where we need to manipulate the certificates on the token, the **LoadLocal** option is not wanted. To turn the **LoadLocal** option off for a specific process enter the name of the process under the following key in the registry. The name of the process must be without the .exe extension and must be closed by a " **;** ".
Example: **eTProps;**

Registry Key:

HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTCertStore\
Value:

STRING ProcLoadLocalIgnore. eTProps;

By adding a process to the list, eToken Certificate Store will not look for eToken certificates in the registry during certificate enumerations.

- **eToken Certificate Store Friendly Name version**

eToken Certificate Store (eTCertStore) sets the Friendly Name of a certificate in two possible formats:

1 The reader is at the beginning followed by the Certificate's subject.
Example: AKS ifdh 0:: john brown…

OR

2 The certificate subject, followed by its usage, followed by the reader name.
Example: john brown: Server Authentication, Client Authentication, Code Signing, Secure Email, Time Stamping... reader::AKS ifdh 0.

The flavor of the Friendly Name is controlled by the registry key.

Registry Key:

HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTCertStore
Value:

DWORD FriendlyNameVer.

By setting FriendlyNameVer to 2 the format of the Friendly Name will be as described in 2 above. This option can be set during command line installation of the RTE (See “RTE Installation - Command Line Options”, on page 75).

eTProperties Settings

Advanced Mode

An administrator is able to disable the Advanced mode of the **eTProperties** application. When Advanced mode is disabled, both the **Local Machine** and **Advanced** buttons are disabled.

The Advanced mode is controlled by a registry key.

Registry Key:

HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTProperties

Value:

DWORD Advanced

If Advanced is set to 0 - Advanced mode is disabled.

This option can be set during command line installation of the RTE (See “RTE Installation - Command Line Options”, on page 75).

eTProperty Additional Logos

An administrator can define a right side image for eTProperties. This option is set by a registry key.

Registry Key:

HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTProperties

Value:

STRING Logo

Should have the path to a BMP file.

Value:

DWORD LogoTransparency

When you want to use PIXEL(0,0) of the bitmap as a transparent color set the LogoTransparency value to a non-zero value e.g. 1.

RTE Installation - Command Line Options

An IT Administrator can set some of the RTE characteristics during the installation process on the user's machine.

The following settings are available during Installation:

```
ETPROPS_MODE: 0 basic mode, 1 advanced mode (default).
LOAD_LOCAL: 0 Load local false, 1 Load Local true
        (default).
```

```
AUTO_DUPLICATION_CHECK: 0 Disable (default), 1 Auto Check
                        Enabled.
FRIENDLY_NAME_VER: 1 default or 2.
```

For more details please see “Registry Settings for eToken Properties”, on page 72.

Installation Command Line samples

msiexec /i d:\RTE3.50.msi /qb ETPROPS_MODE=
0 AUTO_DUPLICATION_CHECK=1

This command will install the RTE with a basic Installation User Interface (only a progress bar is shown: /qb) and with eTProperties Advanced mode disabled, and with automatic key duplication test on. All other settings are set to their default values.

msiexec /i d:\RTE3.50.msi /q

This command will install the RTE in a silent mode with all installation properties set to their defaults.

NOTE: If reboot is needed in a silent mode it will be activated automatically.

msiexec /x {8A94A108-8329-4265-ABFD-619D8F075DB9} /q

This command line should uninstall the RTE in a silent mode.

Appendix A

Troubleshooting

This appendix offers advice and proposes solutions to problems that you may encounter when installing or using eToken.

The following sections are contained in this appendix:

- “Problems and Possible Solutions”, on page 78, lists the problems that might arise, and suggests their causes and solutions.
- “Checking USB Support”, on page 80, explains how to check whether USB support is enabled in the BIOS for your system.
- “Technical Support”, on page 82, provides contact information for technical assistance.

Problems and Possible Solutions

The following table lists the possible causes of each problem, and suggests the appropriate solutions.

Table A.1: Problems, Diagnoses and Solutions

	Problem	**Possible Diagnosis**	**Solution**
1	Operating system identifies new hardware, but fails to recognize it as a USB device.	The eToken was inserted into the USB port before installation was finished.	Remove the eToken from the port and reinsert.
		Installation was not successful, or the driver was not installed correctly.	Remove the eToken RTE installation, if necessary, and reinstall.
2	LED on *eToken* does not light up.	The USB is not enabled in the BIOS. See "Checking USB Support", on page 80, for details.	Enable the USB in the BIOS. If necessary, consult your technical support services supplier.
		The operating system does not support USB.	Ensure that one of the following operating systems is installed: • Windows 98 • Windows NT 4.0 • Windows ME • Windows 2000
		The eToken is defective.	Obtain a new eToken. Contact your local Aladdin office.
		The eToken was inserted during installation	Remove the eToken and reinsert it in the USB port.

Table A.1: Problems, Diagnoses and Solutions (Continued)

	Problem	Possible Diagnosis	Solution
3	Application does not recognize the eToken.	Errors in the application.	Check the application for errors.
		The eToken is defective.	Obtain a new eToken.
4	Operating system displays the “New Hardware” message when a different USB port is used.	Windows automatically recognizes a new port when it is used for the first time, including ports connected via a hub.	This is normal operating system behavior and needs no further action. The current eToken installation is valid for all USB ports.
5	RTE installation failure on Windows NT 4.0	The USB port is not enabled in the BIOS.	Make sure the USB interrupt is enabled in the BIOS settings.

Checking USB Support

In order for your system to recognize the USB port and your eToken, USB support must be enabled in the BIOS. Your technical support services supplier may need to make the necessary changes to your system setup.

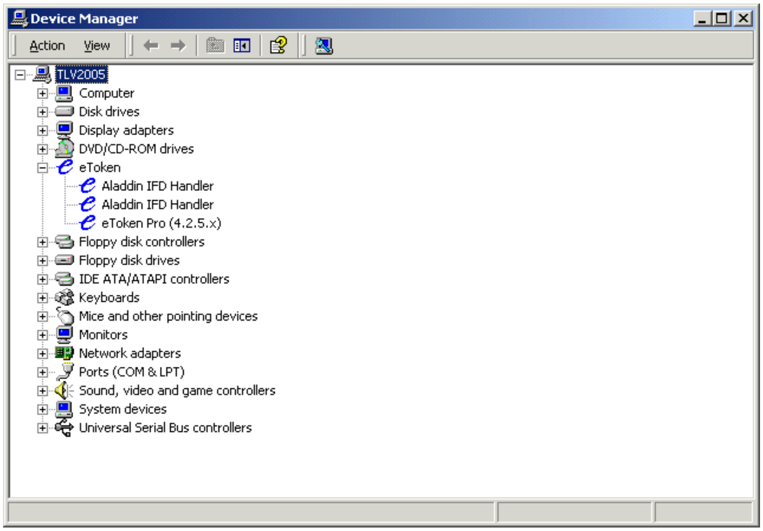
To check whether USB support is enabled for your Windows 98 or Windows 2000 system:

1 Open the Windows **Control Panel**.

2 Select **System (Properties)**.

3 Select **Device Manager**. (In Windows 2000, the **Device Manager** button is located on the **Hardware** tab). A list is displayed of the devices currently enabled in your system.

USB support is enabled if the list of devices includes one or more **IFD Handler** entries, and one or more eTokens, as shown in the example below:



- TLV2005
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - eToken
    - Aladdin IFD Handler
    - Aladdin IFD Handler
    - eToken Pro (4.2.5.x)
  - Floppy disk controllers
  - Floppy disk drives
  - IDE ATA/ATAPI controllers
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
  - Ports (COM & LPT)
  - Sound, video and game controllers
  - System devices
  - Universal Serial Bus controllers

If the displayed list does not include an entry for an eToken, the **eToken** is not correctly inserted or may be defective. If the list does not include an entry for **IFD Handler**, the installation failed. Reinstall or contact Technical Support.

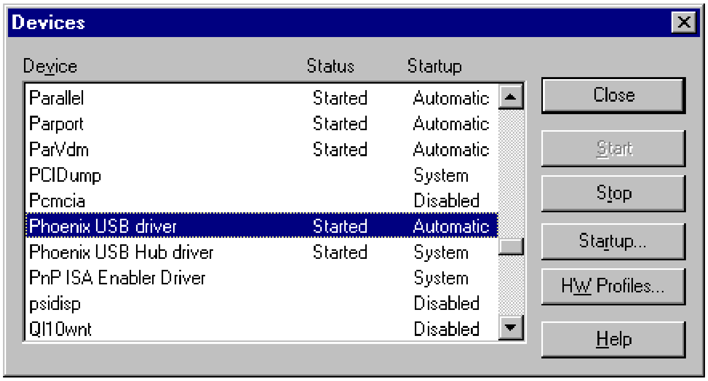
To check whether USB support is enabled for your Windows NT 4.0 system:

1 Open the Windows **Programs Menu**.

2 Select **Settings**.

3 Select **Devices**. A list is displayed of the devices currently enabled in your system

USB support is enabled if the status of the **Phoenix USB driver** and **Phoenix USB Hub driver** is shown as Started, as shown in the example below:,.



Devices

Device	Status	Startup
Parallel	Started	Automatic
Parport	Started	Automatic
ParVdm	Started	Automatic
PCIDump		System
Pcmcia		Disabled
Phoenix USB driver	Started	Automatic
Phoenix USB Hub driver	Started	System
PnP ISA Enabler Driver		System
psidisp		Disabled
QI10wnt		Disabled

If the Device list does not include entries for the **Phoenix USB driver** and **Phoenix USB Hub driver**, the installation failed. Reinstall or contact Technical Support.

Technical Support

If you are unable to solve the problems that you are experiencing and require technical support and assistance, please contact Aladdin by telephone, fax or email, as follows:

Tel:	**+972 3 636 2266**
Fax:	**+972 3 537 5796**
Email:	**etoken.techsup@eAladdin.com**
Website:	**http://ealaddin.com/support/etoken/index.asp**

Index