



eToken Overview (RTE 3.65)

January 2006



Contact Information

Support

If you have any questions regarding this package, its documentation and content or how to obtain a valid software license you may contact your local reseller or Aladdin's technical support team:

Country / Region	Telephone
USA	1-212-329-6658 1-800-223-3494
EUROPE: Austria, Belgium, France, Germany, Netherlands, Spain, Switzerland, UK	00800-22523346
Ireland	0011800-22523346
Rest of the World	+972-3-6362266 ext 2

If you want to write to the eToken Technical Support department, please go to the following web page:

http://www.Aladdin.com/forms/eToken_question/form.asp

COPYRIGHTS AND TRADEMARKS

The eToken™ system and its documentation are copyrighted © 1985 to present, by Aladdin Knowledge Systems Ltd.

All rights reserved.

eToken™ is a trademark and ALADDIN KNOWLEDGE SYSTEMS LTD is a registered trademark of Aladdin Knowledge Systems Ltd.

All other trademarks, brands, and product names used in this guide are trademarks of their respective owners.

This manual and the information contained herein are confidential and proprietary to Aladdin Knowledge Systems Ltd. (hereinafter "Aladdin"). All intellectual property rights (including, without limitation, copyrights, trade secrets, trademarks, etc.) evidenced by or embodied in and/or attached/connected/related to this manual, information contained herein and the Product, are and shall be owned solely by Aladdin. Aladdin does not convey to you an interest in or to this manual, information contained herein and the Product, but only a limited right of use. Any unauthorized use, disclosure or reproduction is a violation of the licenses and/or Aladdin's proprietary rights and will be prosecuted to the full extent of the Law.

NOTICE

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, libraries, utilities, diskettes, CD-ROM, eToken™ keys and the accompanying technical documentation) (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 (within 7 days from the date you received this package) RETURN THE PRODUCTS WITH THE ORIGINAL PACKAGE AND THE PROOF OF PAYMENT TO ALADDIN, 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 the 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 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 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 technical 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 accompanying technical guide provided by Aladdin ("**Technical 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 Technical 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 than 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 Technical 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 REQUIREMENTS 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 Technical 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 PRODUCT 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 PRODUCT.
10. **Termination.** Your failure to comply with the terms of this Agreement shall terminate your license and this Agreement. Upon termination of this 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, 3, 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 re-export restriction as set forth herein and any update made thereto from time to time.
13. **Third Party Software.** Product contains third party software, as set forth in Exhibit A. Such third party's software is provided "As Is" and use of such software shall be governed by the terms and conditions as set forth in Exhibit A. If the Product contains any software provided by third parties other than the software noted in Exhibit A, 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 AGREEMENT AND AGREE TO BE BOUND BY ALL OF THE TERMS.

Exhibit A**A. Notices.**

- I.** Product has incorporated source code licensed under the Mozilla Public License ("MPL").
- II.** MPL is available at <http://www.mozilla.org/MPL/>

The MPL License, version 1.1, Copyright © 1998-2004 The Mozilla Organization.

- III.** The source code is freely available from:
<http://lxr.mozilla.org/mozilla/source/security/nss/cmd/modutil/modutil.c/>
- IV.** "Covered Code" means: source code governed by the MPL.

B. DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

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	1
Introduction	1
eToken Solutions	2
What is eToken.....	3
eToken Features and Benefits.....	4
eToken Solutions	6
eToken Product Offering.....	8
eToken Security Applications	8
eToken TMS (Token Management System).....	10
eToken Development Tools	10
eToken-Enabled Third-Party Applications	11
eToken Models	12
eToken PRO	14
eToken NG-OTP	18
eToken PRO Smartcard	21
eToken R2	22
FIPS	26
Overview	26
eToken PRO	26
The eToken RTE.....	27
RTE Features.....	28
Chapter 2.....	31
Security Concepts	31
Security Risks and Corporate Vulnerability.....	32
Password Storage and Authentication	35
How Safe is a Password?.....	35
Password Quality.....	36
Rating your eToken Password.....	37
Challenge-response Authentication	38

x

Chapter 1

Introduction

This 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. It also explains some important security-related concepts and standards that administrators and users should take into account.

About This Chapter

This chapter contains the following sections:

- ◆ “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 Product Offering”, on page 8, lists the various usages and integrated applications for eToken.
- ◆ “eToken Models”, on page 12, describes the models of the eToken that are currently available.
- ◆ “FIPS”, on page 26, explains what FIPS is and how the eToken complies with FIPS standards.
- ◆ “The eToken RTE”, on page 27, provides a brief overview of what the RTE is and lists its main features.

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

eToken Solutions

eToken enterprise security 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 technology, eToken helps your organization protect its digital assets, conveniently and securely.

eToken is attractive to system administrators because it makes it easy to enhance IT security quickly, without requiring complex back-end installation and configuration. 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 enables generation and secure storage of passwords and digital certificates, strong authentication, digital signing and encryption, and more.



eToken Smartcard



eToken NG - OTP



eToken PRO



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.

A single eToken can store a number of private keys, certificates and passwords concurrently, for use in a wide variety of applications.

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

eToken Features and Benefits

The key features and benefits of eToken include:

- ◆ **Strong authentication:** eToken provides strong two-factor authentication, by requiring something that the user has – an eToken device, and something the user knows – the eToken password. The authentication method used by eToken employs strong, industry-standard encryption algorithm technology.
- ◆ **High security:** eToken eliminates security issues arising from users writing down their passwords, using easy-to-hack passwords, or using the same password for multiple applications in order to handle all of their passwords. Security credentials are not at risk because they are held in a secure, tamper-evident container. The eToken smartcard is completely resistant to cracking, even with full knowledge of the encryption algorithms and protocols used. eToken provides full hardware-based protection for essential security information, with on-chip key generation.
- ◆ **Reader-less smartcard:** eToken USB devices provide all the benefits of smart card technology but require 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 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. All a user needs to remember is a single eToken password in order to access all personal credentials, PKI certificates, and other secret information stored on the eToken.
- ◆ **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 eToken password.



- ◆ **Ease of administration:** eToken provides easy-to-use management solutions for administrators and does not require complex back-end installation and configuration, simplifying the process of initial deployment and ongoing token life cycle 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.

- ◆ **Cost effectiveness** – eToken significantly reduces password related help-desk calls, meaning significant password management cost savings to your organization.
- ◆ **Increased user productivity** – Users spend less time worrying about remembering and organizing their passwords.

eToken Solutions

Today's IT environment demands that you do more with less. eToken delivers a broad platform of solutions to enable greater standardization, with lower deployment and management costs.

One eToken enables all of these solutions and more — It's your digital identity organizer.

VPN Security (Secure Remote Access)

eToken enables enterprises to strongly authenticate their remote users when accessing the organizational network, offering seamless integration with mainstream VPN systems such as: Cisco, Check Point, Microsoft, SSH and many others.

Web Access

eToken enables strong user authentication when accessing protected web resources and signing sensitive digital transactions. Using standard browser technology and digital certificates, users can also verify that the websites they are accessing are what they claim to be.

Network Log-on

eToken enables organizations to add strong user authentication when logging on to protected network resources supporting Smartcard logon technology using PKI and also the native Microsoft (GINA) logon mechanism by storing users' passwords and access credentials.

Proximity Access (Doors/badges)

eToken enables the integration of a variety of proximity technologies combined with network access for both, with its traditional Smartcard and USB token form factors, depending on organizational needs. Printing of a user's picture and identification details on the Smartcard offers an ideal solution for organizations requiring visual user verification.

File & Data Encryption

eToken offers advanced connectivity to many types of data protection systems, ranging from full hard drive encryption and boot protection, to specific file encryption and signing.

Secure Email

eToken offers seamless connectivity to major email clients using standard security features.

Advanced Password Management

With eToken, a user no longer needs to remember passwords for different accounts – their single eToken password combined with their eToken is all they need. eToken manages the user's credentials and automatically submits them to different log-on applications.

Transaction and Document Signing (Non-repudiation)

Transactions and documents can be digitally signed with eToken through PKI technology, ensuring the authenticity of electronic transactions.

eToken Product Offering

eToken offers a robust framework for integration with many of today's leading technology companies, providing organizations with a variety of applications to meet their specific needs.

eToken Security Applications

Public Key Infrastructure (PKI)

eToken provides strong 2-factor challenge/response authentication using PKI keys and certificates. It operates with any standard PKI aware application, using either PKCS#11 or Microsoft CAPI. Full support is available for applications such as: Network Logon via Microsoft Smartcard Logon, Novell NMAS or Entrust EntelligenceSecurity; Secure Web Access via standard web browser security using advanced Secure Sockets Layer V3; Remote Access VPN Authentication with Cisco, Check Point, Microsoft, SSH and many other leading systems; Signed and Encrypted Emails using mainstream email systems such as Outlook, Netscape, and Eudora; Document Signing using Adobe Acrobat and other document signing systems.

One-Time Password (OTP)

eToken One-Time Password (OTP) authentication offers secure clientless network logon using one-time passwords, giving you the versatility to securely log onto your network from wherever you are, without the need for any client software installation or a USB connection.

The eToken OTP offering is based on the eToken NG-OTP device, Aladdin's innovative smartcard-based hybrid token that enables full strong authentication and password management capabilities in connected mode (with the USB connection), as well as OTP-based strong authentication in detached mode.

The eToken OTP architecture includes the eToken RADIUS server for back-end OTP authentication, which enables integration with any RADIUS-enabled gateway/application, including leading VPN solutions, web access solutions, and more. The eToken RADIUS server utilizes the Active Directory infrastructure (via Aladdin TMS) for user information.

WSO (Web Sign-On)

eToken's WSO application securely stores and manages a user's web logon credentials, IDs and passwords. It automatically fills in logon details after their eToken password has been entered. No changes need to be made to the web application and only authorized people are granted access to sensitive online information.

SSO (Simple Sign-On)

eToken SSO simplifies the logon process to restricted applications by securely storing and presenting digital identity credentials when required. This greatly simplifies the logon process, reduces password management time and enhances user productivity. The eToken SSO enables the caching of access credentials to any standard Windows logon screen such as Notes, RAS Dialers, VPN Clients, etc. All a user needs to do is present one simple eToken password to access all his login credentials.

eToken for Network Logon

The eToken Network Logon solution provides a low-cost method for implementing hardware-based network authentication. This includes domain name combinations, usernames, and authentication passwords, as well as PKI keys and certificates. A user authentication password can be randomly generated and users will not need to remember it (supporting both Microsoft GINA and Novell Netware).

eToken TMS (Token Management System)


































The Aladdin Token Management System is a complete framework for managing all aspects of token assignment, deployment and personalization within an organization. Built on open standards and Active Directory, TMS allows you to manage your authentication tokens through simple plug-ins, centrally push software updates, and inject and revoke eToken credentials. Linked directly to the existing organizational user management systems, the TMS offers a robust and flexible link between the user, the security application, the authentication device used and the organizational rules. TMS includes a robust SDK for integration and management of third-party security applications.

eToken Development Tools

eToken SDK (Software Developer's Kit) allows software developers to integrate eToken security functionality into their applications. This user-friendly SDK includes a set of industry standard APIs and supporting documentation, enabling seamless integration with third-party applications. The eToken SDK uses standard security interfaces for Windows, Linux, Microsoft CAPI, and PKCS#11 interfaces. Special 16-bit libraries enable integration with boot protection security solutions requiring logon prior to operating system loading.

eToken-Enabled Third-Party Applications

eToken integrates with a variety of third-party applications from leading security companies. The *eToken Enabled* designation given to our partners' applications means that through integration with the eToken, they offer a complete security solution for that specific need.

Partner	Boot Protection & Disk Encryption	Email & Data Protection	CA/ PKI	Single Sign On	VPN & Web Remote Access	Network/ Workstation Logon	Other
Check Point							
Cisco							Router Provisioning
Citrix							
CA							
Control Break							
Entrust							
HID							Proximity
IBM							
Microsoft							
Novell							
PGP							
Pointsec							
RSA							
SAP							
Utimaco							
Verisign							Code Signing

* Partial list. For more details visit:

<http://www.Aladdin.com/etoken/solutions.asp>.

eToken Models

eToken's interchangeable form factors allow organizations complete flexibility to meet their individual needs.

From USB tokens for PCs and remote environments, to Smartcards for access control and identity badges – eToken's accessibility, efficiency and portability mean it's the smart choice for organizations looking to stay ahead in today's ever changing, digitalized world. All devices support the same security interfaces and work seamlessly with both Enterprise and SDK security applications.

eToken PRO is a USB, readerless Smartcard. It is a low cost device that enables strong, 2-factor authentication and is easy to deploy. eToken PRO's secure, on-board RSA 1024-bit and 2048-bit key operations enable seamless integration into any PKI or other security architectures.



eToken NG-OTP is a hybrid USB and One Time Password (OTP) token, offering all of the functionality of eToken PRO USB with the addition of OTP technology for connection-less strong authentication. eToken NG-OTP integrates multiple strong authentication methods and enables a wide variety of security related solutions, all in one device.



<p>eToken PRO Smartcard offers the same functionality as eToken PRO USB, but its shape is that of a traditional credit card form factor. It is operable with a standard Smartcard reader and is ideal for combining secure logical access with ID badging and physical access (proximity) solutions.</p>	 A white smartcard with a gold-colored chip in the upper right corner. The bottom left corner features a red and white logo with the text "eToken" and "PRO SmartCard" below it.
<p>eToken R2 is a USB device that is ideal for secure storage of users' private keys and access credentials. Featuring onboard 120-bit DESX encryption, the R2 combines high security with ease of use. (Sales discontinued).</p>	 A red, elongated USB device with a silver USB connector at one end. The word "ALADDIN" is embossed on the red plastic body.
<p>Proximity (Physical) Access: eToken can integrate with proximity access solutions, combining both physical access and logical access in one device. Proximity technology can be integrated with both USB and smartcard eToken form factors.</p>	 A collection of eToken devices including a white smartcard with a photo of a woman, a red eToken R2 USB device, and a blue eToken R2 USB device with the number "455237" and the "ALADDIN" logo.

eToken PRO

The eToken PRO offers strong authentication and a wide variety of security solutions, including PKI key generation, digital signing and encryption, caching of user credentials, and more.

eToken PRO 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 PRO Features

The eToken PRO:

- ◆ Uses advanced smartcard chip technology, with on-chip cryptographic processing using RSA1024/2048, 3xDES and SHA-1.
- ◆ Provides full on-chip RSA 1024-bit and 2048-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 and CAPI APIs.
- ◆ Has ITSEC LE4 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 2048 bits long.
- ◆ Symmetric DES and 3DES encryption, decryption and MACing with key lengths up to 168 bits long.
- ◆ Message digesting using SHA-1.

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 2048 bits long.

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 LE4 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 labeling and color options for brand enhancement.

eToken PRO Specifications

Operating Systems	Windows 98/98SE/Me/2000/XP and Windows NT4.0 SP6 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)	32K, 64K
On board security algorithms	RSA 1024-bit / 2048-bit*, DES, 3DES (Triple DES), SHA1 (*) with 64K model
Security level	ITSEC LE4 (Infineon and Siemens); FIPS 140-1 level 2 & 3 (32K model)
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 consumption	120mW
Operating temperature	0 C to 70C (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 NG-OTP

The Aladdin eToken NG-OTP hybrid token is a 2-in-1 device, incorporating state-of-the-art smartcard and one-time-password (OTP) technologies. eToken NG-OTP provides the full functionality of the smartcard-based eToken PRO USB - including strong user authentication, PKI encryption and digital signing, secure credential storage, and more - combined with OTP technology for strong user authentication to network resources in connection-less mode.

eToken NG-OTP is highly flexible and versatile, enabling a variety of strong authentication methods and security related solutions, all in one device. eToken NG-OTP is the ultimate solution for enterprise security in a diverse environment, with a wide range of networks, applications, and customer needs.

eToken NG-OTP Features

- ◆ USB token with OTP function (LCD display, battery, and OTP generation button)
- ◆ Smartcard support for RSA 1024 bit, Triple DES, SHA1
- ◆ Standard PKI Support for CAPI, PKCS11 and RADIUS OTP
- ◆ Fully compatible with eToken PRO technology
- ◆ Highly secure implementation using smartcard chip for both PKI and OTP operations
- ◆ Robust plug-and-play USB connectivity
- ◆ Modular OTP algorithm support
- ◆ Strong two-factor authentication: requires both the token itself and the token password
- ◆ Non-repudiation using advanced on-board PKI digital signing technology

eToken NG-OTP Benefits

The key eToken NG-OTP benefits can be summarized as follows:

- ◆ Flexible and versatile solution; PKI, OTP, Secure credential storage.
- ◆ Highly secure smart card technology.
- ◆ Zero footprint authentication
- ◆ Easy back-end configuration
- ◆ Fully compatible with eToken solutions.
- ◆ Improved and cost effective password management.

eToken NG-OTP Specifications

Operating Systems	Windows 98/98SE/Me/2000/XP, and Windows NT4.0 SP6 and later
API & standards support	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)	32K, 64K
On board security algorithms	RSA 1024-bit, DES, 3DES (Triple DES), SHA1
OTP security algorithm	OATH compliant (based on HMAC/SHA1)
Dimensions	70.5 x 28.0 x 10.5 mm (2.75 x 1.09 x 0.41 inches); LCD view area 29.9 x 8.0 mm (1.17 x 0.31 inches)
ISO specification support	Support for ISO 7816-1 to 4 specifications
Weight	17g
Power consumption	120mW

Operating temperature	0 C to 65 C (32 F to 149 F)
Storage temperature	-20 C to 65 C (-4 F to 149 F)
Humidity rating	0-95% without condensation
Connector	USB type A (Universal Serial Bus)
Casing	Hard molded plastic
Battery lifetime	7000 OTP generations
Memory data retention	At least 10 years
Memory cell rewrites	At least 500,000

eToken PRO Smartcard

The eToken PRO Smartcard offers the same functionality as eToken PRO USB, but its shape is that of a traditional credit card. The eToken Smartcard is operable with a standard Smartcard reader.

Just like the eToken PRO, the eToken PRO Smartcard offers strong authentication and a wide variety of security solutions, including PKI key generation, digital signing and encryption, caching of user credentials, and more.

The eToken PRO Smartcard is ideal for combining secure logical access with ID badging and physical access (proximity) solutions.

eToken PRO Smartcard Specifications

Operating Systems	Windows 98/98SE/Me/2000/XP, and Windows NT4.0 SP6 and later
API & standards support	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)	32K, 64K
On board security algorithms	RSA 1024-bit / 2048-bit, DES, 3DES (Triple DES), SHA1
Security level	ITSEC LE4 Smartcard security certification (Infineon and Siemens) (32K model)
ISO specification support	Support for ISO 7816-1 to 4 specifications
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.

PLEASE NOTE: With effect from January 1, 2006 this model is no longer being sold. However, support for eToken R2 devices will continue until December 2006.

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 98/98SE/Me/2000/XP and Windows NT4.0 SP6 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	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 70C (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.

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 (with firmware version 4.x.5.4) 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.

The eToken RTE

The eToken Run Time Environment (RTE) installs all the necessary files and eToken drivers to support eToken integration with various security applications. It enables Windows operating systems and third party applications to access the eToken. Installing the RTE allows communication with all available eToken devices and forms the basis for Aladdin's various security solutions. These include eToken PKI solutions using either PKCS#11 or CAPI, proprietary eToken applications such as WSO (Web Sign ON), SSO (Simple Sign ON), eToken for Network Logon and management solutions like eToken TMS – a Token Management System that is a complete framework for managing all aspects of token assignment, deployment and personalization within an organization.

Aladdin's eToken PKI Solutions enable the implementation of strong two-factor authentication using standard certificates. Generic integration with both Microsoft CAPI and PKCS#11 security interfaces enables interoperability with a variety of security application such As Web Access, VPN Access, Network Logon, PC Protection and Secure eMail. PKI keys and certificates can be securely created, stored and used from within the eToken.

When used with eToken PRO / Smartcard or eToken NG-OTP the PKI Private keys can be generated and operated on board the secure chip.

eToken RTE supports the various types of eToken devices in both form factors. This means that only a single RTE installation is required to enable operations of either a traditional Smartcard or a USB Token (PRO/ NG-OTP or R2), and results in easy deployment and cost effective installation in use of eToken products and solutions.

eToken RTE can be deployed and updated using any standard software distribution system such as SMS. In addition, the eToken Management System (TMS) supports software distribution using the Microsoft GPO system.

RTE Features

The eToken RTE provides an extensive range of features to enable effective use of the eToken within proprietary and third party security applications. These features include:

- ◆ Support for eToken R2, eToken PRO (USB token and smartcard form factor) and eToken NG-OTP.
- ◆ Support for the generation and use of RSA keys on eToken (for eToken PRO and eToken NG-OTP). Depending on the specific token, the maximal supported key size may be either 1024 bit or 2048 bit.
- ◆ Support for an administrator password (eToken PRO and eToken NG-OTP) that can be used to unblock user password.
- ◆ Advanced settings within the RTE application enabling the definition of a secondary password over the user's private key (for eToken PRO and NG-OTP).
- ◆ Storage of user and CA certificates on the eToken.
- ◆ The ability to import keys and certificates from a computer to the eToken.
- ◆ The possibility of FIPS-compliant initialization of eToken PRO.
- ◆ Incorporates eToken Properties, a complete token configuration tool.
- ◆ Token initialization options that allow for individual token and multi-token initialization.

- ◆ A Password Quality Check feature to determine if the password meets designated criteria.
- ◆ A customizable installation that facilitate installation and deployment in an efficient manner
- ◆ Great level of flexibility (such as data caching, choosing certificates for particular tasks, power management etc.).
- ◆ Support for Terminal Services.

The features detailed cover the main elements of the RTE's functionality, but are by no means exhaustive.

For more information on the RTE, please see the eToken RTE Administrator Guide and the eToken website at:

www.Aladdin.com/etoken .

Chapter 2

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 32, outlines the security risks and concerns that are relevant to all commercial and public organizations.
- ◆ “Password Storage and Authentication” , on page 35, 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 38, summarizes the use of the challenge-response mechanism for secure authentication.

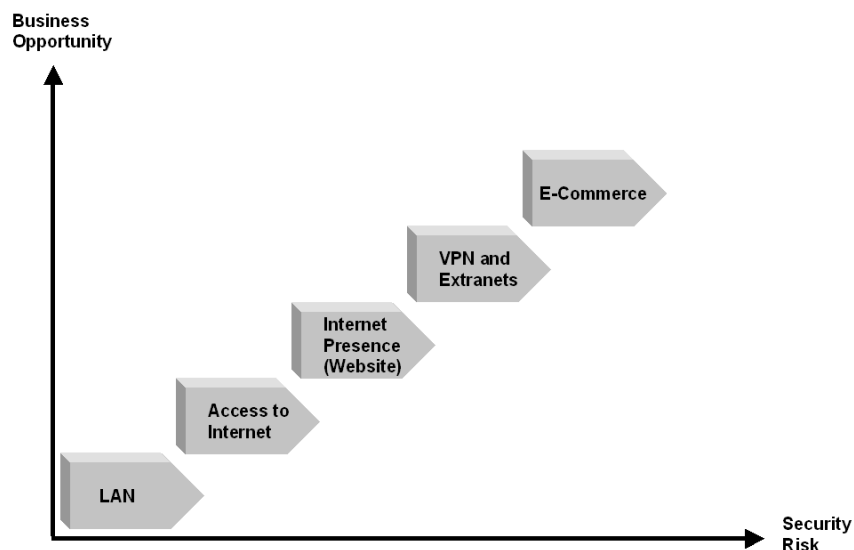
Security Risks and Corporate Vulnerability

In today's ever-changing 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, together with the opportunities it brings, has 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 the latest annual survey conducted by the FBI, concerns over these security risks are not unfounded. In the *2004 CSI/FBI Computer Crime and Security Survey*, in which 500 companies responded, losses were reported of over \$140 million from computer security incidents throughout the year.

These losses are due to saboteurs, system penetration and unauthorized access, viruses, laptop theft, financial fraud, telecommunications fraud, abuse of wireless networks 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.

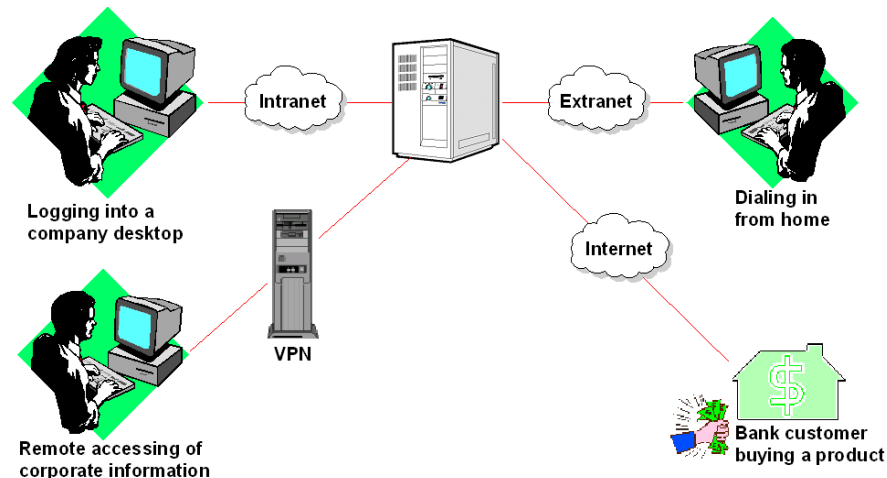
Every commercial enterprise should be aware of the following:

- ◆ According to the *2004 CSI/FBI Computer Crime and Security Survey*, 53% of all respondents experienced unauthorized use of computer systems in the last 12 months and over 60% acknowledged financial losses due to computer security breaches.
- ◆ Another 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.

- ◆ An increasing number of organizations are focusing on the use of Public Key Infrastructure systems (30% of respondents in the 2004 CSI/FBI survey), Smartcards/other one-time password tokens (35%), and reusable account/login passwords (56%) as part of the security technologies used to protect their organizations and prevent intrusions.

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:



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.

“Not only are passwords insecure... Gartner Group and Forrester Research put the cost of resetting a password at about \$50, while a survey from software giant Computer Associates estimated 70% of help desk calls concern password replacements.”
(Financial Post, 2004)

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 additional details, see:

www.Aladdin.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, you should not be required to enter your password again.

Following are three strategies for choosing a good password:

- ◆ Use lines from a childhood verse:
 - Verse Line: Yankee Doodle went to town
 - Password: YDwto#town
- ◆ Expressions inspired by the name of a city:
 - City expression: Chicago is my kind of town
 - Password: CimYkot
- ◆ 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.

Challenge-response Authentication

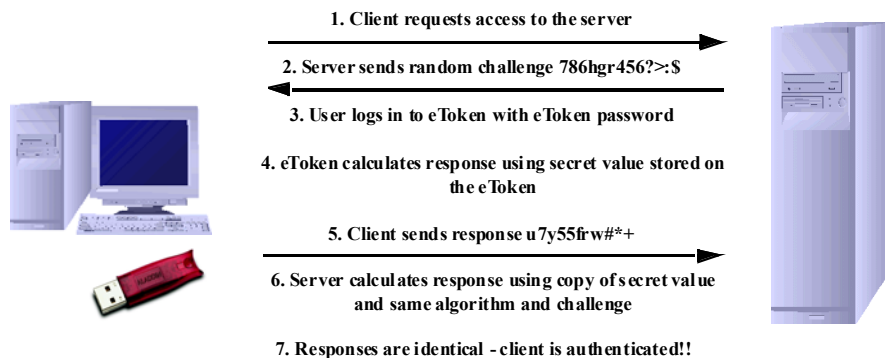
A challenge is a value sent by an authenticating party, such as a company's server, to a party or device requesting to be authenticated. Since the connection between the two parties is usually not secure, the authentication process is vulnerable if the challenge and response are always the same. A secure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



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 www.Aladdin.com/eToken.