



Reference Guide for
eToken PKI Client 4.0

January 2007



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, Italy, Netherlands, Spain, Switzerland, UK	00800-22523346
Ireland	0011800-22523346
Rest of the World	+972-3-9781299

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

Website

<http://www.Aladdin.com/eToken>

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.

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
PKI Client Overview	2
What's New in eToken PKI Client 4.0	4
Supported eTokens	5
PKI Client 4.0 Backward Compatibility	6
Minimum Requirements	7
Chapter 2	8
Main Administrative Activities	8
Installing the eToken PKI Client	9
Setting Up a New eToken User	11
Issuing a Replacement eToken	12
Administrator Password	12
Initializing eToken	13
eToken Password Quality	14
Chapter 3	15
eToken Deployment	15
Deploying eToken PKI Client	16
Properties	23
Command Line Installation	24
Silent Mode Installation	24
All About Certificates	25
Chapter 4	27
eToken Properties Application	27
Overview	28
Starting eToken Properties	29
eToken Properties Views	30
Simple View	31
Logging on to eToken	33

- Renaming the eToken..... 34
- Changing the eToken Password..... 35
- Unlocking the eToken 38
- Viewing eToken Info..... 42
- Advanced View 43**
 - Using the Advanced View 44
 - Logging on in Advanced View..... 45
 - eTokens and Readers..... 45
 - Inserted eToken 48
 - User Certificates..... 64
 - Settings 67
 - PKI Client Settings 73
 - PKI Client Tools 76
- Chapter 5..... 78**
 - Troubleshooting..... 78**
 - Problems and Possible Solutions 79**
 - Technical Support..... 81**

Chapter 1

Introduction

The eToken PKI Client is the software that enables eToken USB operations and the implementation of eToken PKI-based solutions. An introduction to the PKI Client is provided in this chapter.

About This Chapter

This chapter contains the following sections:

- ◆ “PKI Client Overview”, on page 2, presents a short description of the PKI Client and what it does.
- ◆ “What’s New in eToken PKI Client 4.0”, on page 4, provides a brief explanation of new features, additions and changes to PKI Client 4.0 from previous RTE versions.
- ◆ “PKI Client 4.0 Backward Compatibility”, on page 6 details relevant issues regarding the eToken PKI Client 4.0.
- ◆ “Minimum Requirements”, on page 6 lists the hardware, software and operating system requirements for using eToken.

PKI Client Overview

PKI or Public Key Infrastructure is a framework for creating a secure method for exchanging information based on public key cryptography. It is an arrangement that provides for trusted third party vetting of, and vouching for, user identities and consists of a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

The eToken PKI enables integration with various security applications. It enables eToken security applications and third party applications to communicate with the eToken device so that it can work with various security solutions and applications. 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 eToken assignment, deployment and personalization within an organization.

Aladdin's eToken PKI Client enables the implementation of strong two-factor authentication using standard certificates, as well as encryption and digital signing of data. Generic integration with both Microsoft CAPI and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications offering secure web and VPN access, secure network logon, PC and data security, secure email and more. PKI keys and certificates can be securely created, stored and used from within the eToken.

When used with all eToken smart card-based devices: eToken PRO / Smartcard, eToken NG-OTP or eToken NG-FLASH, the PKI private keys are generated and stored on board the secure smart card chip.

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



What's New in eToken PKI Client 4.0

The eToken PKI Client 4.0 is enhanced with new features and additional functionality from previous versions of the eToken RTE.

The new eToken PKI Client 4.0 features include:

- ◆ **Software-based “eToken Virtual”** that is built into the PKI Client and is specially designed as a solution for “employee on the road” difficulties when used with TMS 2.0.
- ◆ **New enhanced and upgraded user interface** that provides an improved user experience, with the advantage of easier eToken management for the user.
- ◆ A new **single logon mode** on the eToken that enables multiple access to the eToken with only one request for the password. This alleviates the need to log on to each application separately.
- ◆ **On-token password** policy is an enhanced security feature that ensures the security level of the password is defined on the eToken itself.
- ◆ **Password quality management** has been simplified to make it easier for setting these policies without reducing in any way the level of password security desired.
- ◆ **One factor authentication** is now possible enabling users to initialize an eToken so that no password is required to work with the eToken (One factor is presence of the eToken itself). **This reduces security but may be essential for particular applications.**

Supported eTokens

The following eToken devices are supported by the eToken PKI Client 4.0:

- ◆ eToken PRO
- ◆ eToken NG-OTP
- ◆ eToken NG-FLASH
- ◆ eToken PRO Smartcard



PKI Client 4.0 Backward Compatibility

- ◆ Password policy mechanisms are not backward compatible.
- ◆ Obsolete low level APIs (not documented in SDK 3.60) are not supported.
- ◆ eToken PKI Client 4.0 no longer supports the eToken R2 device.
- ◆ A user cannot delete certificates from the eToken via Certificate Store.
- ◆ To use eToken SSO profiles created in previous RTE versions, they must be backed up to a separate database while the eToken is reinitialized using PKI Client 4.0. The profiles can then be restored to the eToken and used.

Minimum Requirements

The following are the minimum requirements for using eToken PKI Client 4.0:

- ◆ At least 10 MB disk space.
- ◆ Operating Systems:
 - ◆ Windows 2000 (with Service Pack 4 or later installed).
 - ◆ Windows XP with SP 2.
 - ◆ Windows Server 2003.
 - ◆ Windows Vista.
- ◆ For eToken Properties, the supported screen resolution is 1024 x 768 pixels or higher.
- ◆ USB port

NOTE:

Additional software may be required for individual eToken solutions. For more information, please refer to www.Aladdin.com/eToken.

Chapter 2

Main Administrative Activities

Administering eToken in an organization is simple and straightforward. This chapter details the main administration tasks required for ongoing use of eToken devices within the organization.

About This Chapter

The chapter includes the following sections:

- ◆ “Installing the eToken PKI Client”, on page 9, details the installation process for PKI Client.
- ◆ “Setting Up a New eToken User”, on page 11, outlines what needs to be done to set up a new user with eToken.
- ◆ “Issuing a Replacement eToken”, on page 12, explains what actions to take in the event of damaged, lost or stolen, or forgotten eToken passwords.
- ◆ “Initializing eToken”, on page 13, provides general information on the process of initializing an eToken.
- ◆ “eToken Password Quality”, on page 14, explains the various settings used in amending the Password policy.

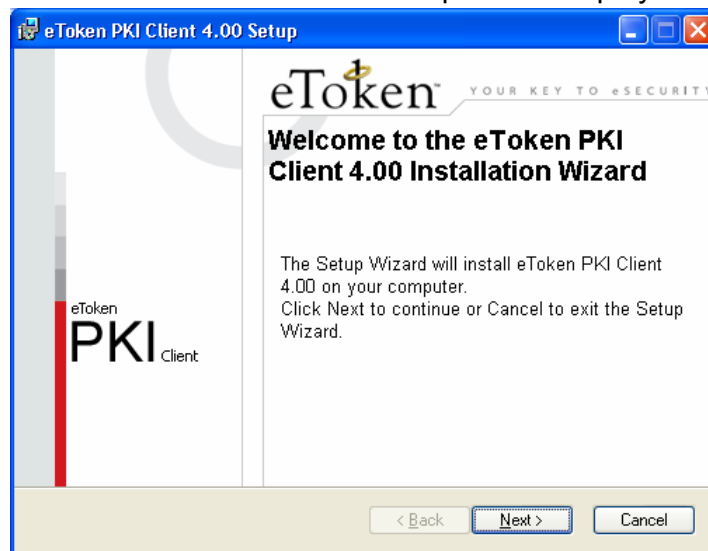
Installing the eToken PKI Client

In addition to the needed drivers, the PKI Client also includes the eToken Properties configuration tool, which enables straightforward user management of the eToken.

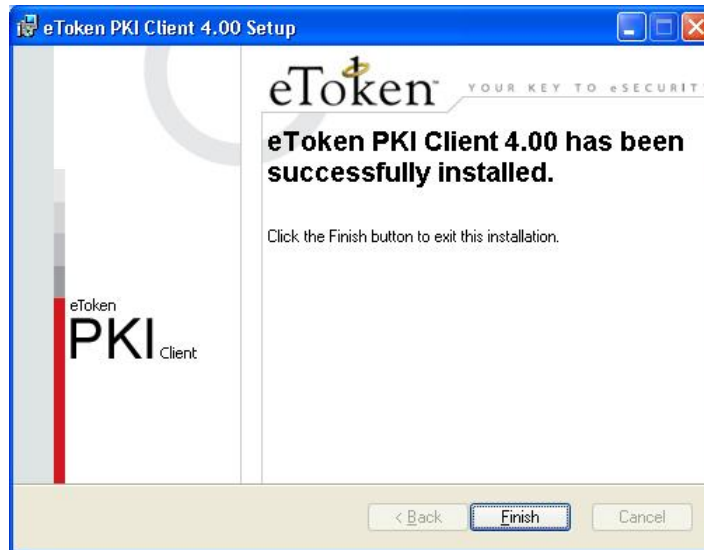
The eToken PKI Client 4.0 must be installed on each computer on which eToken is to be used.

➤ **To install the eToken PKI Client:**

- 1 Close all currently opened applications.
- 2 Double-click the **PKIClient4.00.msi** file. The eToken PKI Client 4.00 Installation Wizard opens as displayed:



- 3 Click **Next** to continue. The License Agreement opens.
- 4 Read the license agreement carefully and then select the **I accept the license agreement** option.
- 5 Click **Next** and the installation begins. During the installation, an **Updating System** window is displayed providing progress on the installation. When the installation is complete, a successfully installed message is displayed.



- 6 Click **Finish**. The eToken PKI Client 4.0 is installed.

Setting Up a New eToken User

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

- ◆ Install the eToken PKI Client 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. This includes "Renaming the eToken" on page 34 and "Changing the eToken Password" on page 35.

Issuing a 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, the administrator should issue the user another eToken, with a requirement to personalize it as soon as possible.

If a user forgets the eToken password, it can either be reinitialized whereby the eToken's details are erased and the eToken is reset to the default password, or the user password can be reset using the eToken administrator password with all of the eToken's details preserved.

Administrator Password

A special Administrator password function is included with the PKI Client. This function enables administrators to reset the eToken user password.

If this functionality is required, the administrator **MUST** first initialize the eToken with this administrator password before distributing the eTokens throughout the organization.

For details on using the Administrator password, refer to Administrator Log On on page 53 and Change Administrator Password on page 55.

Initializing eToken

The eToken Initialization feature erases all data on an eToken and resets the file structure according to various configurable parameters. In addition, the feature can set the Administrator password and other functional parameters.

The eToken PRO can be initialized as a standard eToken PRO or as a FIPS eToken PRO (only eToken PROs with CardOS 4.01). Any eToken device can be initialized as a blank eToken.

For detailed information on the eToken Initialization feature included in the eToken Properties configuration tool, please refer to the Initialize section on page 57.

eToken Password Quality

The eToken Password Quality feature allows administrators to set and edit the password quality parameters according to the organization's password policy. The feature includes a number of configurable parameters.

General password quality settings apply to all eTokens within the organization, but the IT Administrator can set different parameters for a specific eToken with the new on-token password policy feature. This feature manages on a per-token basis the password from data stored on the eToken itself and is not maintained on the computer. The feature is implemented the next time that eToken is inserted into a computer.

Altering the password quality parameters is controlled from within eToken Properties. For detailed information on the eToken Password Quality feature included in the eToken Properties configuration tool, please refer to the eToken Password Quality section on page 67 of this Reference Guide.

Chapter 3

eToken Deployment

Deploying eToken in an organization is simple and straightforward. This chapter provides administration guidelines in respect of the Administrator's role in defining the PKI Client 4.0 features to be used and how to manipulate these features.

About This Chapter

The chapter includes the following sections:

- ◆ "Deploying eToken PKI Client ", on page 16, details how to deploy the eToken PKI Client in the organization and the various deployment options available.

Deploying eToken PKI Client

The eToken PKI Client includes all the necessary files and drivers to support eToken integration. It also includes the eToken Properties configuration tool, which enables easy user management of the eToken password and name.

The eToken PKI Client 4.0 must be installed on each computer on which eToken is to be used depending on the organization's policies and the administrator's settings.

NOTE: Uninstalling PKI Client

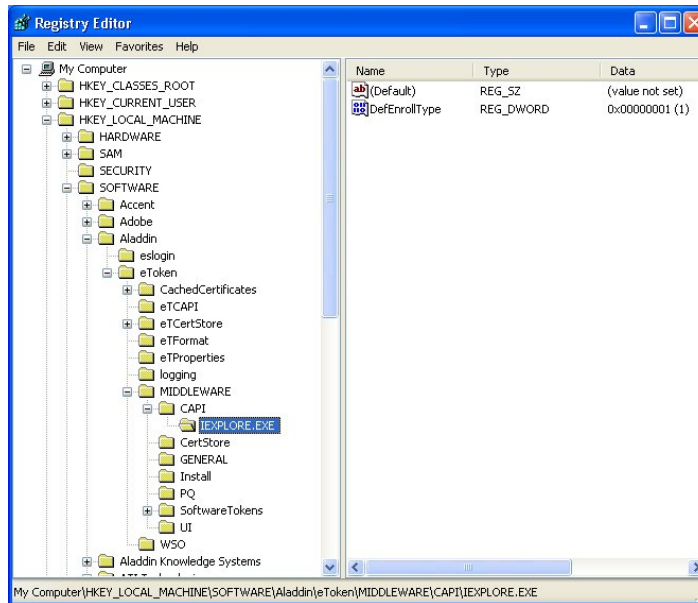
When PKI Client 4.0 is installed, the RTE (previously installed) settings are NOT touched. If you uninstall PKI Client, its registry settings also remain. Another installation will still use them unless overwritten by a command line installation.

If you want to remove any keys after uninstalling, you must do it manually.

All registry keys that are controlled by the installation are stored on a per computer basis.

Registry keys are divided into groups and the type of key is coded in Table 1: eToken PKI Client Registry Keys according to the description provided:

- ◆ M (Machine): These are "per machine" settings. They are located in the HKEY_LOCAL_MACHINE directory. Only the administrator may change these settings.
- ◆ U (User): These settings may be fine-tuned on a per-user basis. PKI Client 4.0 looks for these settings in the HKEY_CURRENT_USER directory. If no entry is found here, eToken PKI Client continues to look for the same key name under the HKEY_LOCAL_MACHINE directory. In this location, settings are originally written during installation.
- ◆ P (Process): In addition to what was said previously (Machine vs. User) these settings may be fine-tuned per process as shown below.



Where appropriate they are cross-referenced with the properties found in Table 2.

Table 1: eToken PKI Client Registry Keys

Key Name	Type	Key Value	Default	Explanation
General				
HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Token\MIDDLEWARE\GENERAL				
SingleLogon	M	0/1	0	Single Logon mode enabled or disabled
SingleLogonTimeout	M	>=0	0	Timeout of single logon in seconds (0 = no timeout)
Software Slots	M	1-10	1	Number of Software Slots
PcscSlots (Integer)	M	1-16	16	Number of PC/SC slots

Key Name	Type	Key Value	Default	Explanation
EnablePubCache	U P M	0/1	1	Enables or disables the public cache. This is persistent in the registry.
EnablePrivCache	U P M	0/1	1	Enables or disables the public cache. This is per process and in memory.
Init				
HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\MIDDLEWARE\Init				
HMAC-SHA1	U P	0/1	N/ A	Determines whether to enable HMAC-SHA1 support
RSA-2048	U P	0/1	N/ A	Determines whether to enforce RSA 2048 support
RSA-KEY-SIZE	U P	>=0	N/ A	Determines which area (number of bytes) on CardOS eTokens to allocate for RSA keys. If the value is 0, no RSA keys on the eToken are allowed.
LEGACY-FORMAT-VERSION	U P	0 or 4	4	Determines whether or not to initialize the eToken to be backward compatible. 0 – Yes, 4 – No
InitApp				
HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\MIDDLEWARE\InitApp				

Key Name	Type	Key Value	Default	Explanation
AdvancedView	M	0/1	1	Enables or disables the Advanced View in eToken Properties. 1 – Enabled, 0 – Disabled
FIPS	M	0/1	0	Determines whether or not to initialize the eToken as FIPS compatible
OneFactor	M	0/1	0	Determines that if a password is not supplied whether to initialize the eToken for One Factor authentication rather than empty
CAPI				
HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Token\MIDDLEWARE\CAPI				
MaxKeySize	M	2048		Maximum key size to be reported in the absence of an eToken
DefKeySize	M	1024		The size of the RSA key to be generated if not passed explicitly. A value lower than 1024 will be ignored.
PasswordTimeout	M	0/1	0	If the password is asked for by CAPI UI determines for how long it is valid in this process.

Key Name	Type	Key Value	Default	Explanation
LogoutMode	M P	0/1	0	Whether to ask for the password for each operation requiring the user to be logged on.
CertStore				
PropagateUserCertificates	U	0/1	1	Whether to keep user certificates in the personal store after eToken removal 1 – keep, 0 – remove
PropagateCACertificates	M	0/1/2	0	Whether to copy CA certificates from the eToken to the user store(s) 0 – No, 1 – Yes, 2 – Ask
Password Policies				
pqMinLen	M	>=4	4	Minimum password length
pqMixChar	M	0/1	0	Whether mixed characters are required in the eToken password 0 – No, 1 – Yes
pqMaxAge	M	>=0	0	Maximum length of time in days before the password expires 0 – no expiry at all
pqMinAge	M	>=0	0	Minimum length of time in days before the password may be changed 0 – No minimum

Key Name	Type	Key Value	Default	Explanation
ppWarnPeriod	M	>=0	0	How many days before password expiry to give a warning 0 – No warning
ppHistorySize	M	>=0	0	How many old passwords should not be repeated
InitApp				
ppProxy	M	0/1		If defined and not zero, a password policy object will not be created on the eToken. The remaining password policy properties are ignored in this case.
ppModifiable	M	0/1		If defined, the password policy on the newly initialized eToken may be modified by the owner afterwards. By default if there is an administrator for the eToken, the administrator is the owner and the object is modifiable. If there is no owner (administrator) then the object is not modifiable.

Key Name	Type	Key Value	Default	Explanation
pqOwner	M	0/1		<p>If defined, it defines who is the owner of the password policy of the newly initialized eToken (i.e. who may change the policy at a later stage)</p> <p>0 – Administrator, 1 – User, By default if there is an administrator for the eToken, the administrator is the owner and the object is modifiable. If there is no owner (administrator) then the object is not modifiable.</p>

Properties

The various settings of eToken PKI Client may be controlled by the installation process when using a command line installation method. Table 2 describes the properties available for a command line installation of eToken PKI Client, and they are cross referenced to the appropriate registry key in Table 1.

Table 2: eToken PKI Client Properties

Name	Command Line	Reference
READER_COUNT	Yes	
Group CertStore		
PROP_PropagateUserCertificates (Y/N) or 1 if not used	Yes	PropagateUserCertificates on page 20
PROP_PropagateCaCertificates (0/1/2) or 1 if not used	Yes	PropagateCACertificates on page 20
Group General		
PROP_SingleLogonTimeout (integer>=0) or 1 if not used	Yes	SingleLogonTimeout on page 17
PROP_SoftwareSlots (integer) default – 1	Yes	Software Slots on page 17
PROP_PCSCSlots (integer) default – 16	Yes	PcscSlots on page 17
PROP_Advanced_View (integer) default – 1 (0 = No Advanced)	Yes	AdvancedView on page 19

Command Line Installation

Command line installation enables full control of registry value settings. This is done by referring to each setting as a “property”.

For details on the complete list of registry key settings, please contact [eToken Product Management](#).

All commands take the format:

```
msiexec /i PKIClient4.00.msi PROPERTY=VALUE
```

Where PROPERTY is the name of the registry key
 VALUE represents the key value

It is possible to install PKI Client without eToken Properties Advanced mode. This is done via a command line installation. To do so use the following command:

```
msiexec /i PKIClient4.00.msi PROP_ADVANCED_VIEW=0
```

Silent Mode Installation

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

```
msiexec /i PKIClient4.00.msi /q
```

NOTE:

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

```
msiexec /x PKIClient4.00.msi /q
```

This command line should uninstall the PKI Client in silent mode.

All About Certificates

A certificate is a document issued by some authority to attest to a truth or to offer certain evidence. A digital certificate is commonly used to offer evidence in electronic form about the holder of the certificate. Its most common use is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

In PKI it comes from a trusted third party, called a certification authority (CA) and it bears the digital signature of that authority. The certificate contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.

The CA is asserting that this unique public key belongs to one individual; that individual is the person who holds the linked private key. Only the person who holds the private key can decrypt something that's encrypted with the public key.

For further information on PKI, Certification Authorities, certificates, public and private keys, please refer to the following books:

Network Security: Private Communication in a Public World, by Charlie Kaufman, Radia Perlman, Mike Speciner

Cryptography and Network Security: Principles and Practices, 4th edition, by Stallings

Additionally, information can be obtained from Microsoft at the following links:

[TechNet](#)

[MSDN](#)

PKI Client 4.0 only supports certificates where the associated key was generated using the RSA algorithm. Other algorithms are not supported (like DSA).

For additional information on certificates, eToken and PKI Client use of certificates, contact [eToken Technical Support](#)

Chapter 4

eToken Properties Application

eToken Properties provide administrators with a configuration tool to administer and set eToken policies. This tool enables users to perform basic eToken management such as password changes, viewing of information, and viewing of certificates on the eToken. In addition, eToken Properties provides users and administrators with a quick and easy way to transfer digital certificates and keys between a computer and an eToken.

eToken Properties also includes an initialization feature allowing administrators to initialize the eToken according to specific organizational requirements or security modes and a password quality feature enabling the manipulation of the parameters which calculate an eToken's password quality rating.

About This Chapter

This chapter provides an explanation of eToken Properties and the various configuration options available to the administrator and user respectively.

The chapter includes the following sections:

- ◆ “Overview”, on page 28, provides a general introduction to and information on starting eToken Properties.
- ◆ “Simple View”, on page 31, explains the available options and commands in this view.
- ◆ “Advanced View”, on page 43, details how to work in this view and all the commands and options.

Overview

eToken Properties is a configuration tool that allows the user to:

- ◆ View contents of the eToken
- ◆ Perform eToken management activities, such as changing the password, renaming the eToken, unlocking locked eTokens, inserting or removing a certificate or setting a default certificate

Many operations, such as key generation, certificate enrollment, certificate removal etc. require multiple actions with the eToken. If the eToken is removed during one of these actions, the data structure on the eToken may be damaged and data lost as a result. In such a case the eToken may need to be reinitialized.

Note:

Do not remove an eToken from the USB port during an operation.

eToken Properties makes possible the management of the eToken (changing passwords, unlocking etc.) and eToken Properties settings as well as integrating the functionality of certain associated Aladdin applications.

eToken Properties provides all possible information about the eToken including it's identification and capabilities. It explores the information stored on the eToken such as keys and certificates and enables management of content only, such as password profiles, which is understood by the user (i.e. not PKCS#11 objects) and by the PKI Client but not by third-parties, either vendor or in-house applications.

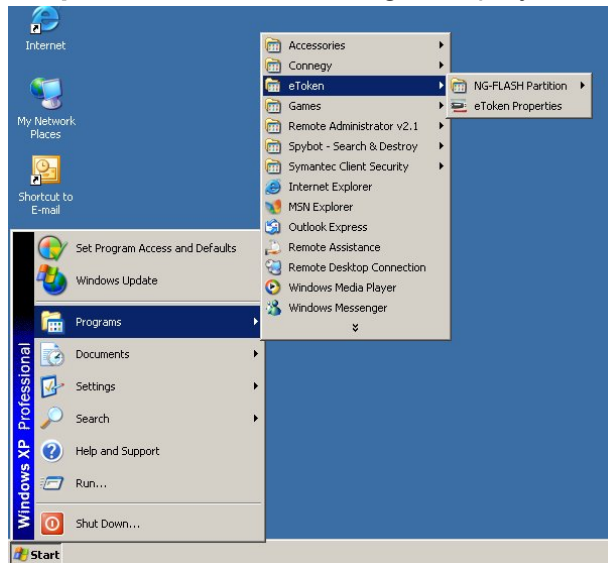
This configuration tool is also used for configuring the initialization parameters of an eToken and for performing the initialization. In addition eToken Properties integrates the functionality of the eToken NG-FLASH partitioning application.

Starting eToken Properties

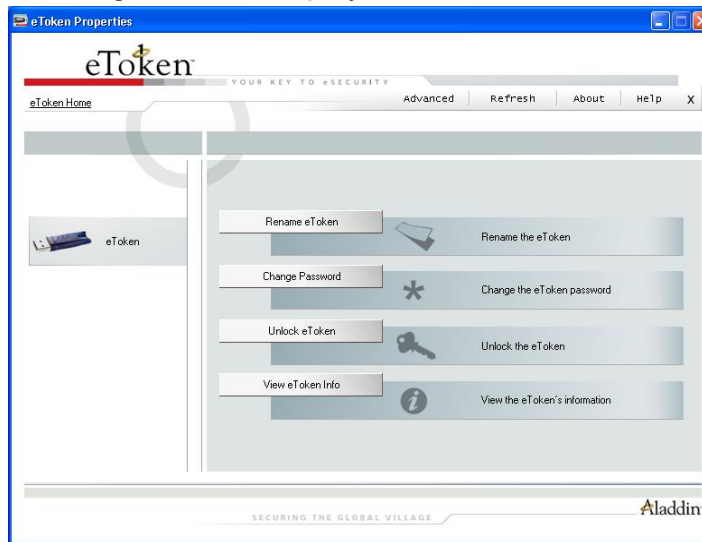
To enable and use the eToken with eToken Properties, first start eToken Properties.

➤ **To start eToken Properties:**

- 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:



- 3 You are now ready to work with eToken Properties.

eToken Properties Views

The eToken Properties configuration tool has 2 different viewing options. These options enable the user to perform certain actions on the eToken. Depending on how complex are the required actions, the user will decide which view to use.

These views are:

- ◆ Simple View – provides the ability to perform basic and common tasks (see Simple View on page 31).
- ◆ Advanced View – provides complete control over the PKI Client and the inserted eToken (see Advanced View on page 43).

Various operations can be performed in the Simple and Advanced Views, the more basic of which are available in both views.

Additionally, in Advanced view many context specific actions can be executed by right-clicking the mouse and selecting the action from a pop-up menu.

Both views show two panes. In each case, the left pane indicates what eToken (Simple View) or what object (Advanced View) is to be managed while the right pane enables the user to perform specified actions to that eToken or object respectively.

A toolbar enables certain actions to be initiated in both views.

eToken Configuration Options

Several operations which relate to eToken configuration options require entering either the eToken user password or the eToken administrator password before attempting to change any configurations.

Simple View

When eToken Properties is launched, the **Simple View** is opened:

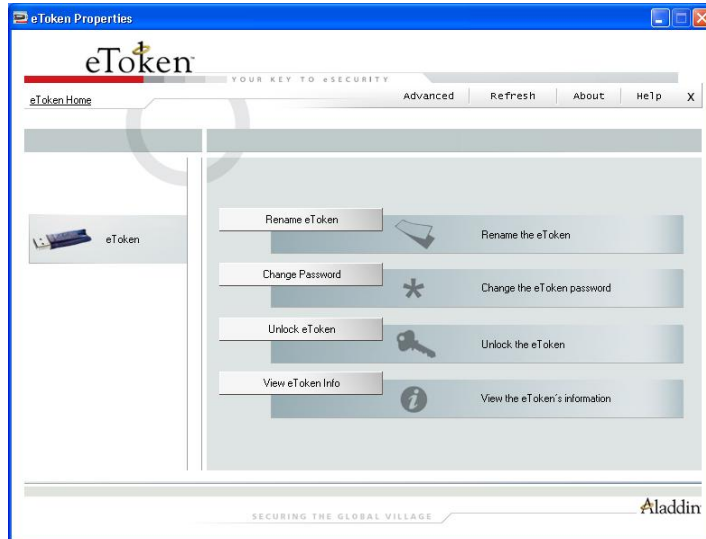


The left pane remains empty if no eTokens are inserted. When one is inserted or an eToken Virtual is added, a device specific icon representing the inserted eToken is displayed. When several eTokens are inserted and the icons extend beyond the length of the screen, a scroll bar enables the viewing of different connected eTokens. The selected eToken in the left pane is marked by shading around the eToken as displayed:



Each eToken has a name to the right of the icon.

If no name has been allocated, a default name – eToken – is used, as displayed:



The right pane allows the user to perform particular actions. These are:

- ◆ **Rename eToken** – sets the eToken name
- ◆ **Change Password** – changes the user password
- ◆ **Unlock eToken** – resets the user's password via challenge response (only enabled when an administrator password is present on the eToken)
- ◆ **View eToken Info** – provides detailed information about the inserted eToken

A tool bar with general control buttons contains these functions:

- ◆ **Advanced** – switches to the Advanced view
- ◆ **Refresh** – refreshes the data for all connected eTokens
- ◆ **About** – provides information about the product version
- ◆ **Help** – launches the online help
- ◆ **X** – exits eToken Properties

A hyperlink to the eToken website – [eToken Home](#) – appears at the top left of the window.

Logging on to eToken

eToken security ensures that when an eToken is inserted, the eToken password is required to enable certain eToken functionality. This functionality includes Renaming, Changing the Password and certain Advanced actions.

➤ **To log on to eToken:**

- 1 Insert the eToken into the USB slot. Select the action to be performed by clicking the appropriate button and the Logon dialog box is displayed:



- 2 Enter the eToken password and click **OK**. The requested action's dialog box opens.

Renaming the eToken

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

➤ **To rename the eToken:**

- 1 Click **Rename eToken** in the right pane of the eToken Properties window and the **Rename eToken** dialog box is displayed.



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



- 3 Click **OK** and on the eToken icon in the eToken Properties window, the new eToken name is displayed:



Changing the eToken Password

All eTokens are configured at manufacture with the factory initial 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 initial password to an eToken password of the user's own choice as soon as the new eToken is received.

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.

Setting an administrator password on all eTokens enables the administrator to unlock the user password if it is forgotten or lost. It is recommended that all eTokens be initialized with an administrator password.

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. This feature enables the administrator to set certain complexity and usage requirements for the password.

For information on using eToken's Password Quality feature, refer to "Password Quality" on page 67.

➤ To change the eToken Password:

- 1 Click **Change Password...** in the right pane of the eToken Properties window and the **Change Password** dialog box is displayed:



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

- 3 Enter the new password in the **New eToken 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 dialog box to show password tips at the bottom of the dialog box. Following these tips will improve the password quality score.

The Password Quality indicator (on the right) provides a percentage score of the password compliance to the password policies regarding “minimum length” and “mix of characters” as displayed:

Change Password: eToken

Change Password eToken

Current eToken Password:

New eToken Password:

Confirm New eToken Password: [] 100%

The best passwords are at least 8 characters long and include upper and lower case letters, punctuation marks and numbers created in random order.

Current Language: EN

Show Tips >> OK Cancel

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

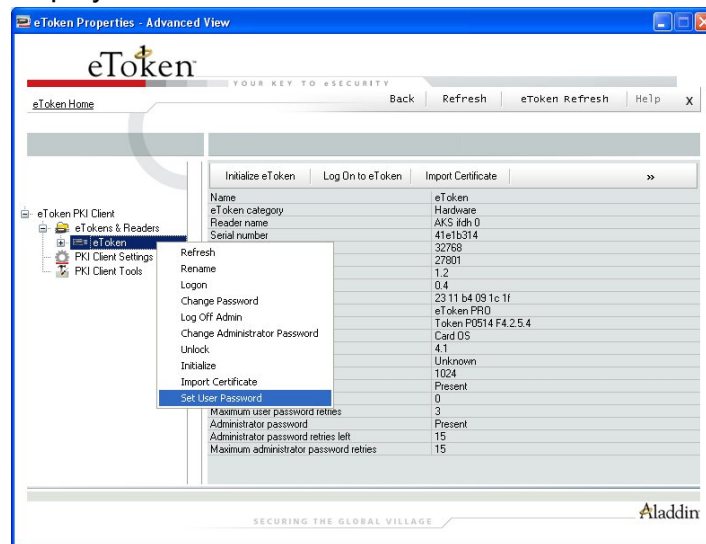
Unlocking the eToken

Where an eToken has been initialized with an Administrator password, eToken Properties provides the ability to unlock a password on the eToken that may have been locked by attempting to enter an incorrect password too many times.

Two methods for unlocking the eToken exist.

If the administrator is present and can enter the administrator password, the Set User Password method can be used.

- **To unlock a locked eToken using Set User Password:**
 - 1 Close the **eToken is locked** message box and open eToken Properties Advanced View.
 - 2 Log on to eToken as an administrator and right click the eToken name.
 - 3 From the dropdown menu select **Set User Password** as displayed:



The Set Password dialog box is displayed:



The dialog box titled "Set Password: eToken" contains the following elements:

- Header: "Set eToken Password" and the eToken logo.
- Fields: "New Password:" (empty text box), "Confirm Password:" (empty text box), and "Set Error Retry Counter:" (spin box with value 0).
- Footer: "Current Language: EN", "OK" button, and "Cancel" button.

- 4 Enter any new password and confirm it as displayed:



The dialog box titled "Set Password: eToken" contains the following elements:

- Fields: "New Password:" (masked with 6 dots), "Confirm Password:" (masked with 6 dots), and "Set Error Retry Counter:" (spin box with value 0).
- Footer: "Current Language: EN", "OK" button, and "Cancel" button.

- 5 Reset the **Set Error Retry Counter** from 0 to the required number as displayed:



The dialog box titled "Set Password: eToken" contains the following elements:

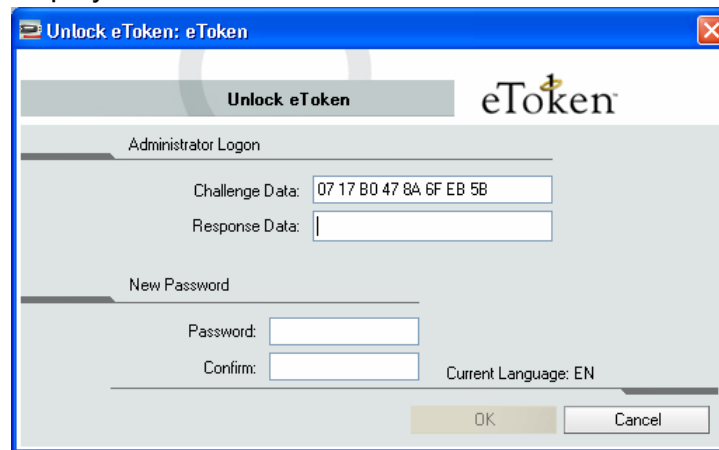
- Fields: "New Password:" (masked with 6 dots), "Confirm Password:" (masked with 6 dots), and "Set Error Retry Counter:" (spin box with value 5).
- Footer: "Current Language: EN", "OK" button, and "Cancel" button.

- 6 Click **OK** and the eToken is unlocked. It is now possible to log on as a user with the new password.

Alternatively, when the administrator can only be located remotely, for example when an employee is out of the office, a Challenge Response authentication method can be employed to unlock the eToken. In this method, the user contacts the administrator with the Challenge data from eToken Properties and enters the Response data provided by the administrator. The user then enters a new password and the eToken is unlocked.

➤ **To unlock a locked eToken using Challenge Response:**

- 1 Click **Unlock eToken** in the right pane of the eToken Properties window and the **Unlock eToken** dialog box is displayed:

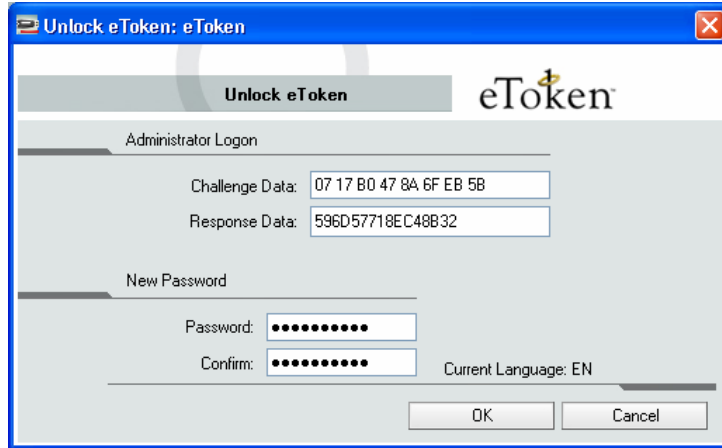


- 2 Contact the administrator and provide him with the **Challenge data** (in the example 07 17 B0 47 8A 6F EB 5B).
- 3 The administrator provides the **Response data** (in the example 596D57718EC48B32).

Note: Creating Response Data

Creating the Response Data depends on the backend application being used by the organization. Please refer to the relevant documentation for details on how to generate the Response Data.

- 4 Enter the **Response Data** in the appropriate text box as displayed:



- 5 Enter a **New Password** in the **Password** and **Confirm** text boxes.
- 6 Click **OK** and the eToken is unlocked. A confirmation message is displayed:

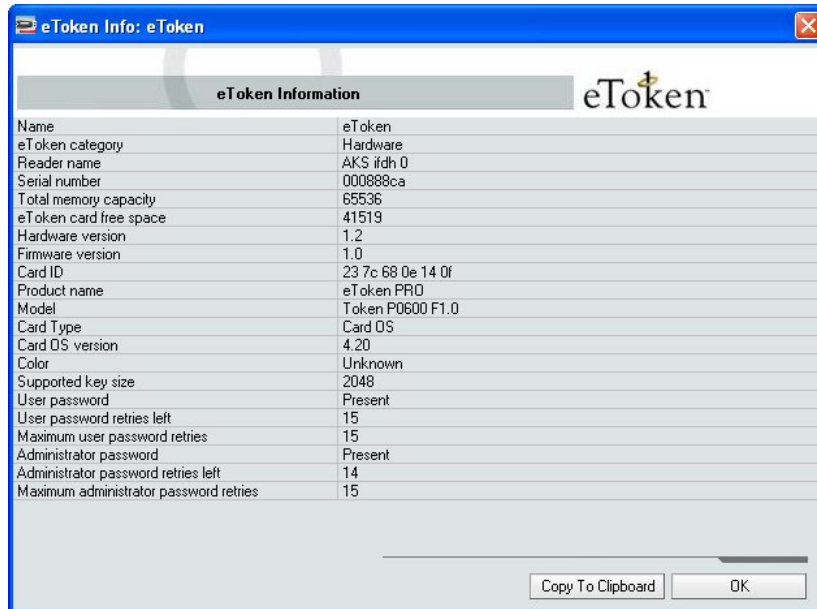
**Note:**

After providing the Challenge data to the administrator, the user **MUST NOT** undertake any activities that use the eToken until after receiving the Response Data and completing the unlocking procedure.

If any other eToken activity occurs during this process, it will affect the context of the Challenge – Response process and invalidate the procedure.

Viewing eToken Info

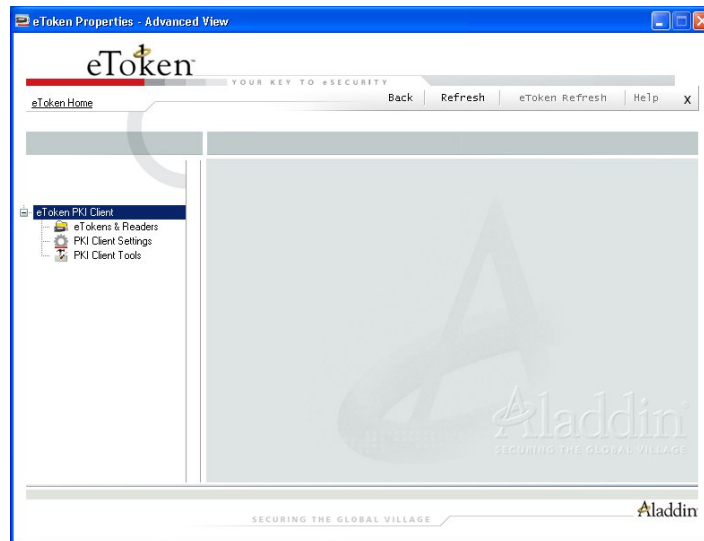
All relevant information relating to a specific eToken can be viewed at any time by pressing the **View eToken Info** button in the right pane of the eToken Properties window. The **eToken Info** dialog box is displayed:



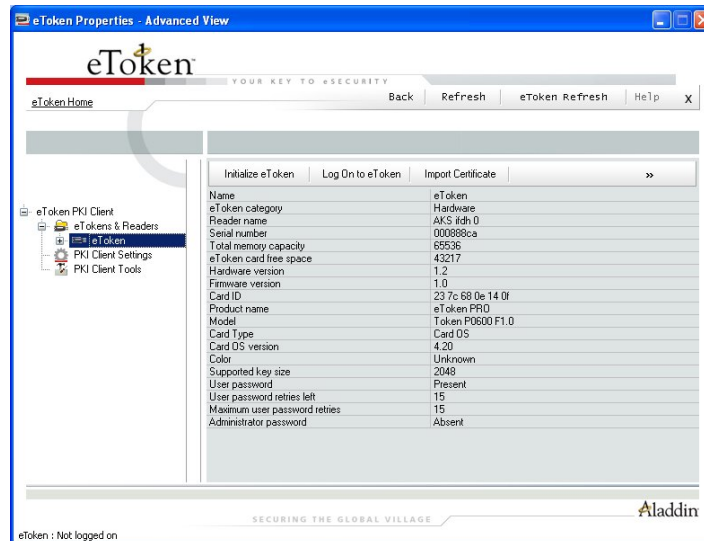
If required for any reason, the information in this dialog box can be copied to the clipboard. Press **Copy to Clipboard** to select all the information. Paste the information to the required application from the clipboard or press **Ctrl + V** or right-click and select **Paste**.

Advanced View

eToken Properties advanced view provides the full functionality of controlling eToken. Click **Advanced** on the menu bar in **Simple View** and the **Advanced View** window is displayed:



The left pane provides a tree view of the various objects to be managed. When an eToken is inserted, this tree is expanded to show objects and details of the inserted eToken as displayed:



Using the Advanced View

Double-click an object in the tree to expand or contract the subtree.

Click the object to open the right pane with details about that object and display a toolbar with key command buttons.

Right click the object to open a shortcut menu of commands specifically for that object.

A tool bar with general control buttons contains these functions:

- ◆ **Back** – switches to the Simple view
- ◆ **Refresh** – refreshes the data for all connected eTokens
- ◆ **eToken Refresh** – refreshes the data for the selected eToken only
- ◆ **Help** – launches the online help
- ◆ **X** – exits the application

A hyperlink to the eToken website – [eToken Home](#) – appears at the top left of the window.

A Status Bar at the bottom of the window displays additional relevant information about the object being highlighted, for example number of connected readers, number of certificates or current logon state depending on which object is being highlighted.

Logging on in Advanced View

For all physical eTokens, you may log on as a user. You may only log on as an administrator if an administrator password is present.

Ensure that the correct logon dialog box (user or administrator) is open. Enter the appropriate password (user or administrator) in the **Password** field and click **OK**.

For more specific information on logging on, refer to the Log On section on page 53 or the Administrator Log On section on page 53.

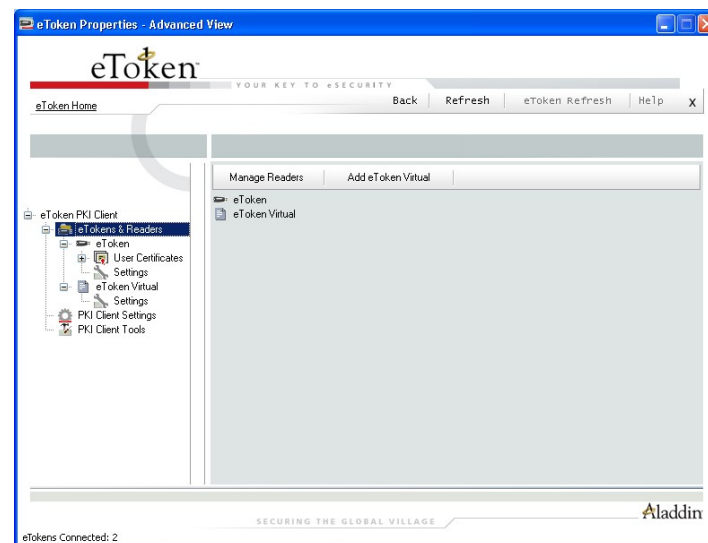
NOTE:

Administrator logon and User functions

If you log on 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.

eTokens and Readers

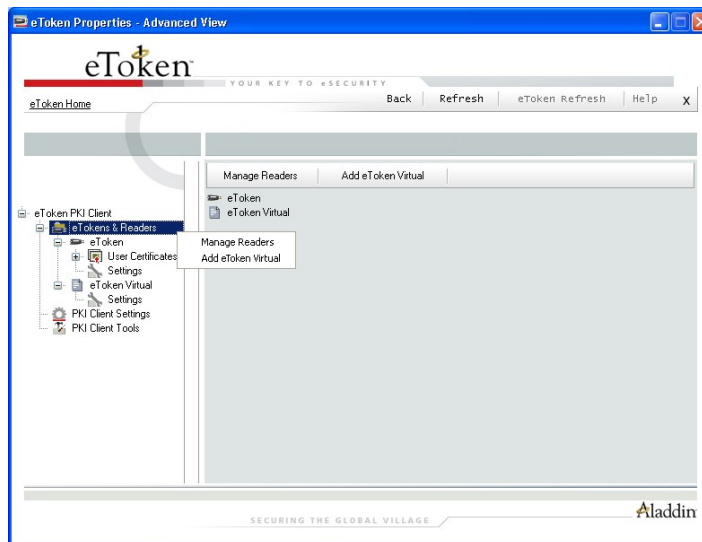
This node deals with all the readers (slots) in the eToken Properties tool that are available on the system.



When selected, the toolbar reflects relevant command options for this object. They are:

- ◆ Manage Readers
- ◆ Add eToken Virtual

When right-clicking the object, the same commands are available as displayed:



Managing Readers

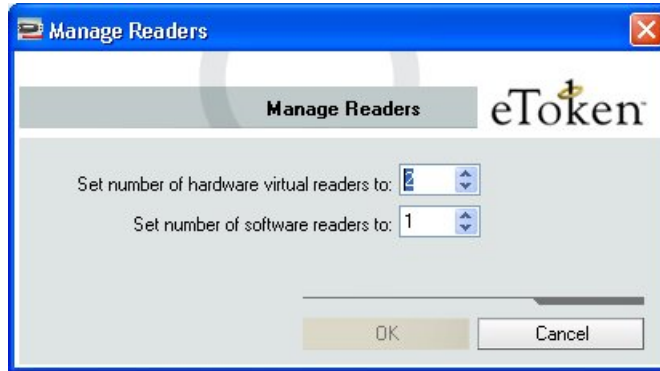
When installing the eToken PKI Client, eToken Properties installs 2 virtual smart card readers and 1 eToken Virtual readers. Physical smart card readers are also displayed if installed.

When an eToken is inserted into the USB port, an eToken Virtual is added or a smart card is inserted into the smart card reader, it has the effect of inserting a smart card into one of the readers.

The number of default readers can be changed if desired. However, this change can only be performed by a user that possesses local administrator rights on that particular computer.

➤ **To change the number of readers:**

- 1 Click **Manage Readers** from the toolbar or by right-clicking the object and selecting the command from the shortcut menu and the **Manage Readers** dialog box is displayed:



- 2 **Set the number of Hardware or Software readers** in the appropriate box to the numbers required.

The default number of available readers is:

- ◆ Hardware Readers 2
- ◆ Software Readers 1

- 3 Click **OK** to close the dialog box. The number of available readers has been changed, but eToken Properties must be restarted to make the changes effective. A message explaining this is displayed:

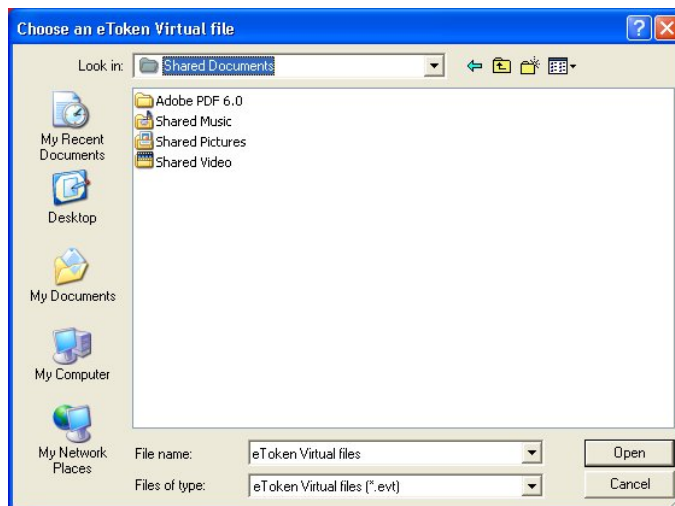


Adding an eToken Virtual

The concept of a software token – eToken Virtual – is built into PKI Client 4.0. It is relevant for use with TMS 2.0. The **eToken Virtual** is stored in a file on the computer itself and is not kept separately.

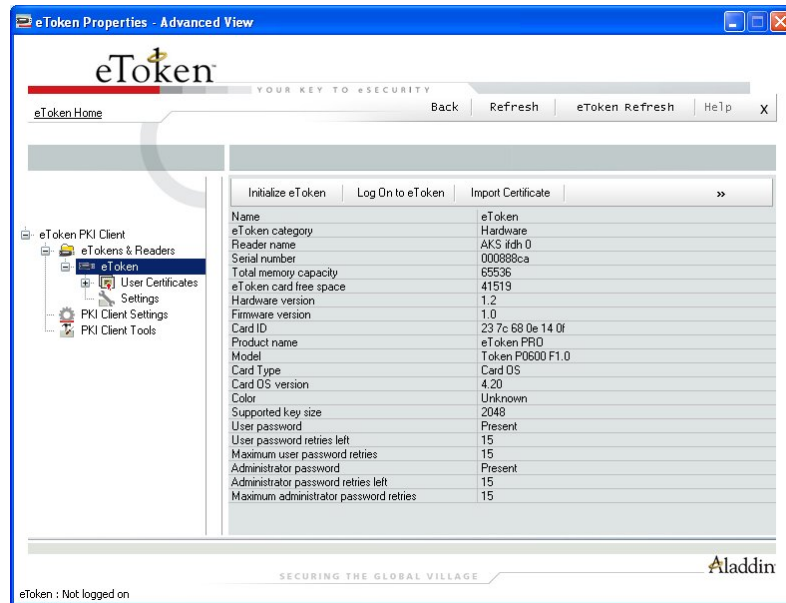
The eToken Virtual is specially designed as a solution for employee on-the-road issues, where the replacement of a lost or missing eToken is not practical.

To add an eToken Virtual, click **Add eToken Virtual** from the toolbar or right-click the object and select the command from the shortcut menu. The **Choose an eToken Virtual** dialog box is displayed:



Inserted eToken

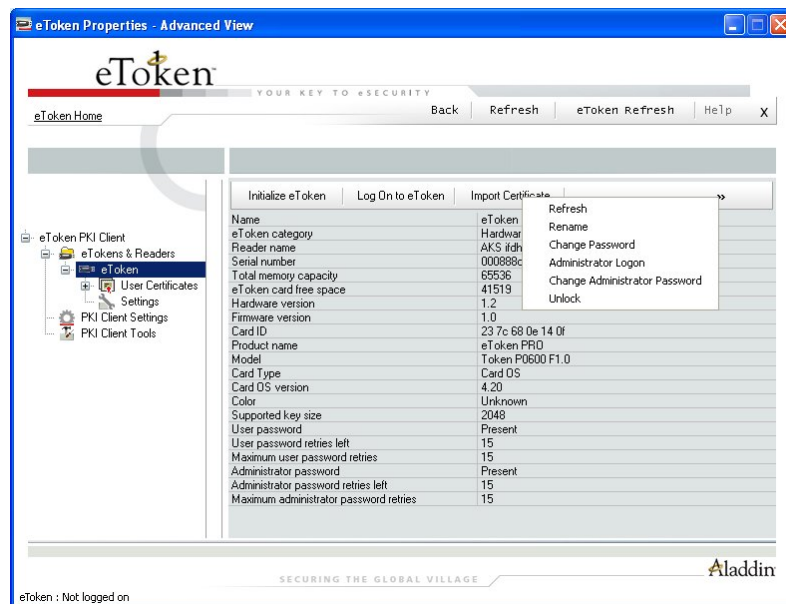
When the eTokens and Readers node is expanded, the names of all inserted eTokens, (hardware and software) are displayed. Standing on one of these eTokens displays all information about this object in the right pane.



This information is the same as in the Viewing eToken Info section on page 42.

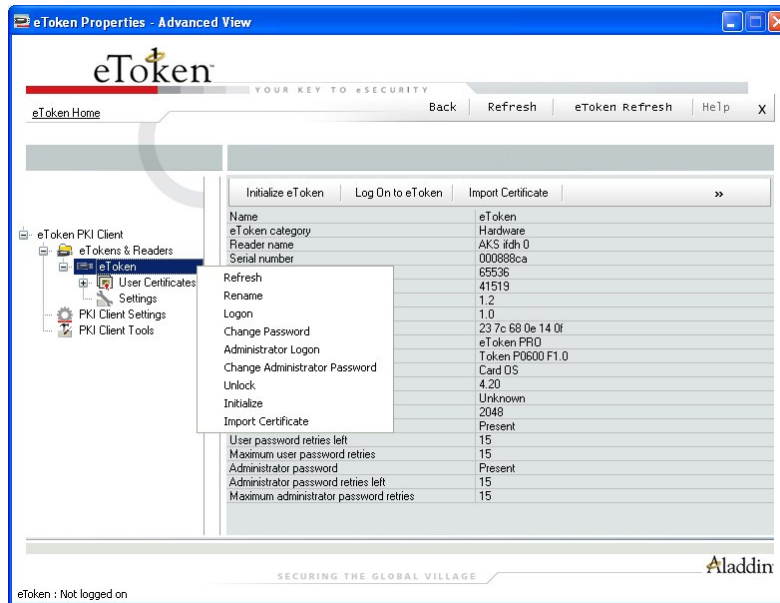
The toolbar displays key commands that can be performed with or about this object such as logging on and importing certificates.

In addition, the expand arrow on the right of the toolbar shows all other commands available with this object as displayed:



All these possible commands are available by right-clicking the shortcut menu on the object itself.

The shortcut menu is displayed:



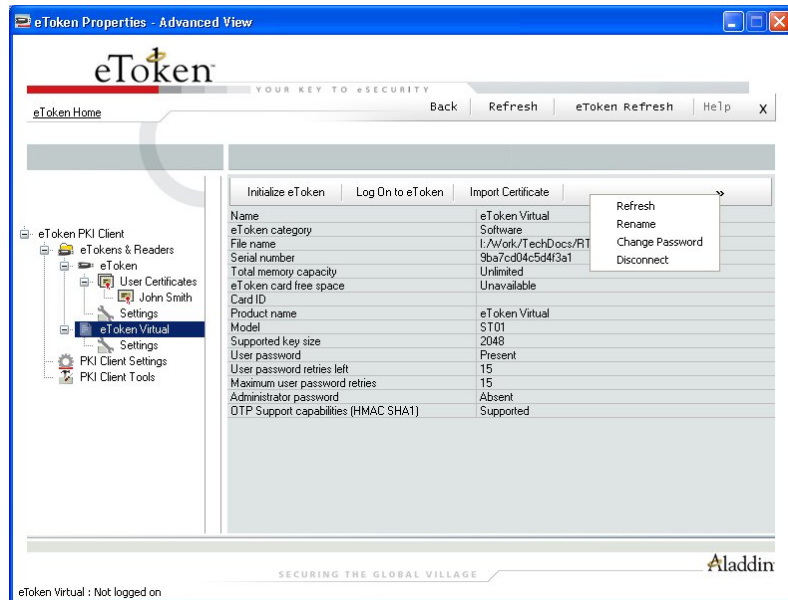
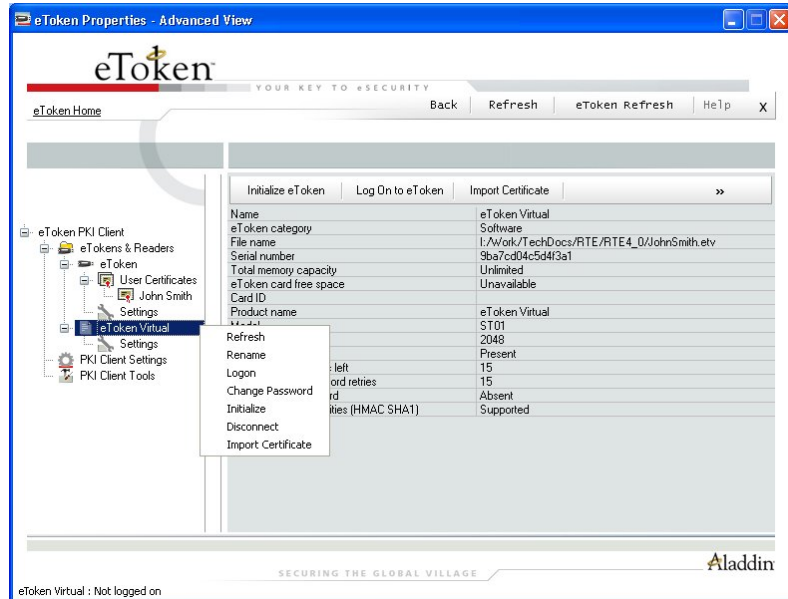
An enlarged version of the shortcut menu is displayed:



By selecting and clicking the command, the selected operation is performed.

Certain commands are disabled if not applicable, for example in the case of an **eToken Virtual**, the administrator functions are disabled.

Therefore, these two menu options – **Administrator Logon** and **Change Administrator Password** – are not available as displayed:



An enlarged version of the shortcut menu is displayed:



All other options are fully functional as described.

Refresh

Selecting this command refreshes the eToken Properties screen to show the relevant information related to that object or eToken.

It is generally used when a new eToken is inserted or a configuration option has been changed.

Rename

To rename an eToken, select **Rename** from the shortcut menu and the **Rename eToken** dialog box is displayed.

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



Click **OK** and the eToken name is changed. On the eToken icon in the eToken Properties window, the new eToken name is displayed.

Log On

This command refers to users logging on to the specific object.

To log on, select **Log On** from the shortcut menu and the **Log On** dialog box is displayed:



Enter the eToken user password in the **Password** field and click **OK**. The user is logged on.

Administrator Log On

To log on as an administrator, select **Administrator Log On** from the shortcut menu and the **Administrator Log On** dialog box is displayed:



Enter the Administrator password in the **Password** field and click **OK**. The user is logged on as the Administrator.

Logging on as an administrator provides limited permissions for the administrator. No changes to any user information can be made, nor can the user's security be affected. The administrator's functions are restricted to Change Administrator Password, Set User Password and Change Password Quality Settings that are stored on the eToken itself.

Change Password

To change the password, either click **Change Password** on the toolbar or select it from the shortcut menu and the **Change Password** dialog box is displayed:



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

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

Re-enter the new password in the Confirm New eToken Password field and click OK. The eToken password is replaced and a success message is displayed:



Change Administrator Password

To change the Administrator password, select **Change Administrator Password** from the shortcut menu and the **Change Administrator Password** dialog box is displayed



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

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

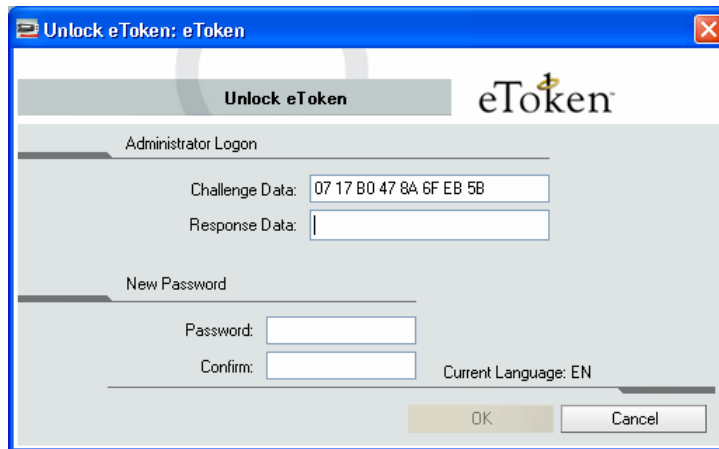
Re-enter the new password in the **Confirm New eToken Password** field and click **OK**. The eToken Administrator password is replaced.

Unlock

Unlocking the eToken can only be done if an Administrator password has been set during initialization.

A challenge response authentication system is used to unlock a locked eToken.

Click **Unlock eToken** on the shortcut menu and the **Unlock eToken** dialog box is displayed:



Unlock eToken: eToken

Unlock eToken eToken

Administrator Logon

Challenge Data: 07 17 B0 47 8A 6F EB 5B

Response Data:

New Password

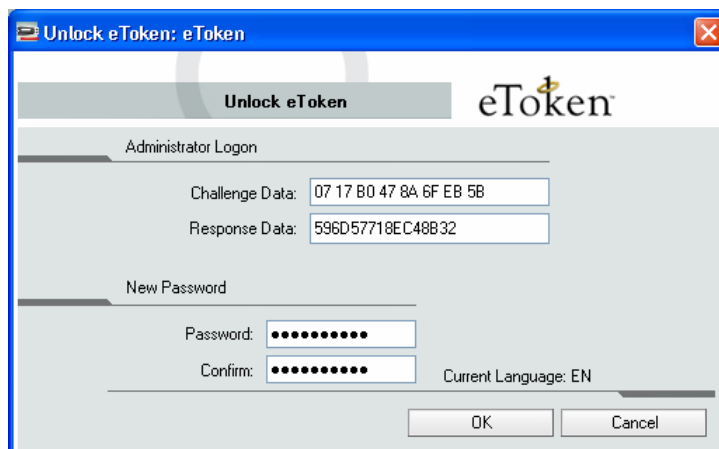
Password:

Confirm:

Current Language: EN

OK Cancel

Contact the administrator and provide him with the **Challenge Data** (in the example 07 17 B0 47 8A 6F EB 5B).



Unlock eToken: eToken

Unlock eToken eToken

Administrator Logon

Challenge Data: 07 17 B0 47 8A 6F EB 5B

Response Data: 596D57718EC48B32

New Password

Password: ●●●●●●●●

Confirm: ●●●●●●●●

Current Language: EN

OK Cancel

The administrator provides the **Response Data** (in the example 596D57718EC48B32).

Note: Creating Response Data

Creating the Response Data depends on the backend application being used by the organization. Please refer to the relevant documentation for details on how to generate the Response Data.

The eToken is unlocked and a success message is displayed:



Initialize

The eToken Initialization option restores an eToken to its initial state. It removes all objects stored on the eToken since manufacture, frees up available memory, and resets the eToken password, allowing administrators to initialize the eToken according to specific organizational requirements or security modes.

Initializing an eToken is useful, for example, after an employee has left a company. It completely removes the employee's individual certificates and other personal data from the eToken, leaving it ready to be set up and used by another employee.

It includes:

- ◆ eToken Name
- ◆ User Password
- ◆ Administrator password (optional)
- ◆ Maximum number of Logon Failures (for user and administrator passwords)
- ◆ Requirement to change the password on the first log on
- ◆ Initialization key

The initialization process loads the Aladdin file system on the eToken.

In addition FIPS support for certain eTokens is possible.

Note:

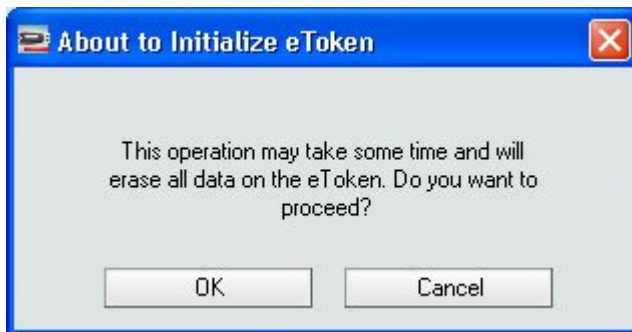
FIPS stands for Federal Information Processing Standards and is a US government approved set of standards designed to improve the utilization and management of computer and related telecommunication systems.

The eToken PRO (version 4.x.5.4) can also be configured in FIPS mode. To do so, certain registry keys must be set. To enable backward compatibility set the LEGACY-FORMAT-VERSION key and to enable FIPS set the FIPS key. After initializing the eToken PRO in this mode, it will be FIPS compliant.

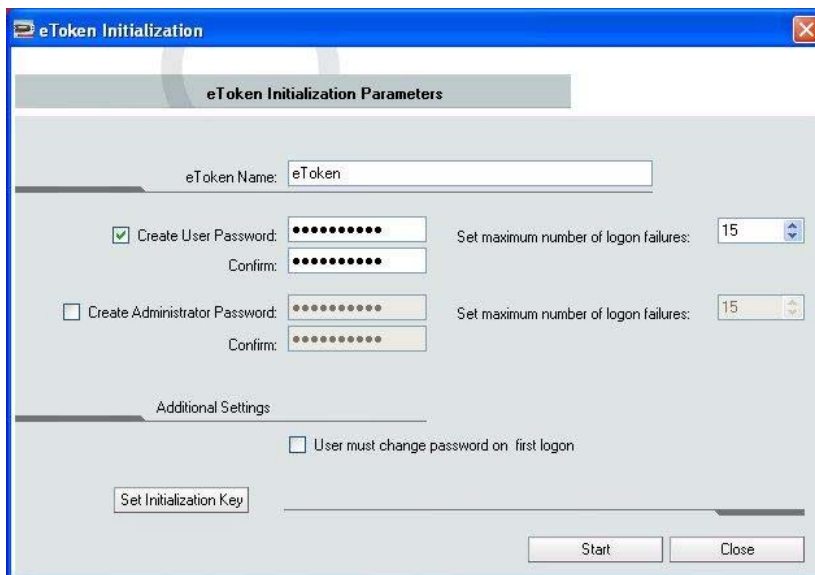
Using customizable parameters, you can select specific parameters that will apply to certain eTokens. These parameters may be necessary if you wish to use the eToken for specific applications or if you require a specific user or administrator password on all the eTokens in the organization.

➤ **To initialize an eToken:**

Click **Initialize eToken** on the shortcut menu and the **About to initialize eToken** message box is displayed:



Click **OK** and the **eToken Initialization** dialog box is displayed:



Enter a name for the eToken in the **eToken Name** field. (If no name is entered, the default name will remain **eToken**).

Enter the new eToken User Password in the **Create User Password** field (the default factory eToken password is **1234567890**) and re-enter it in the **Confirm** field.

If you wish to set an **Administrator Password**, select the **Create Administrator Password** option. Enter the password in the **Create Administrator Password** field (minimum password length must be 4 characters) and re-enter it in the **Confirm** field.

To the right of the password fields are two **Maximum Number of Logon Failure** counters. The **User Password** counter is always enabled while the **Administrator Password** counter is enabled only if an Administrator password is selected. Enter a value between 1 and 15 in the **Maximum Number of Logon Failures** scroll box for the User Password (and if enabled) the Administrator Password.

The counter specifies the number of times the user / administrator can attempt to log on to the eToken with an incorrect password before the eToken is locked.

When the counter is not specified, the default setting for the maximum number of incorrect logon attempts is **15**.

Under **Additional Settings**, decide whether the user must change the password on first logon. If so, select this option.

Set Initialization Key

When attempting to initialize an eToken, an extra security feature is the ability to **Set an Initialization Key**. This key protects against accidental initialization and requires a separate secret to be entered before initialization can occur.

Click **Set Initialization Key** and the **eToken Initialization Key** dialog box is displayed:



Click **OK** to return to the **eToken Initialization** dialog box.

Once all parameters have been set, click **Start** for the eToken to be initialized. When the process is completed, a confirmation message is displayed:



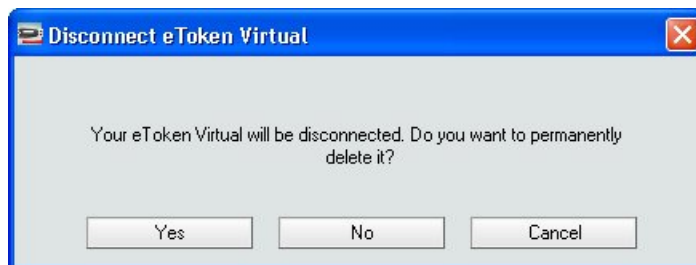
Note:

The Initialization process resets the password to the initial password unless this is changed in the Create User Password field.

Disconnect

Only an eToken Virtual can be disconnected. This means the eToken Virtual is unplugged from its attached reader.

To disconnect an eToken Virtual, select **Disconnect** from the shortcut menu and a message is displayed:



If you want to keep the eToken Virtual file on the computer, click **No** and only the eToken Virtual connection to eToken Properties is disconnected as displayed in the success message:



Disconnecting the eToken Virtual, as opposed to removing the eToken Virtual completely, may be applicable when the user is out of the office and may need to use the eToken at a later stage on the road.

Once back in the office and the lost eToken is replaced, the eToken Virtual should be completely removed from the computer.

Click **Yes** and the eToken Virtual file is removed from the computer. A success message is displayed:



Import Certificate

To import a certificate, either click **Import Certificate** on the toolbar or select it from the shortcut menu and the **Import Certificate** dialog box is displayed:



Select whether to import the certificate from either your personal store on the computer or a file.

If you select the personal certificate store, a list of available certificates to choose from is displayed:

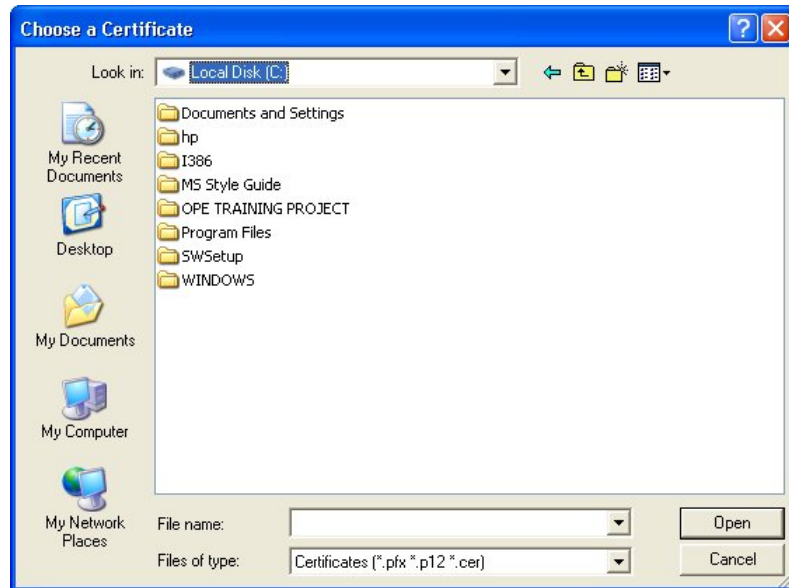


Not all certificates in the store may be listed. Only certificates that can be imported on to the eToken will be listed. These are:

- ◆ Certificates with a private key already on the eToken
- ◆ Certificates that we might import from the computer together with its private key.

Select which certificate to import and click **Import**. A confirmation message is displayed if the import is successful.

If you want to import from a file, you can import either a PFX, P12 or CER file.



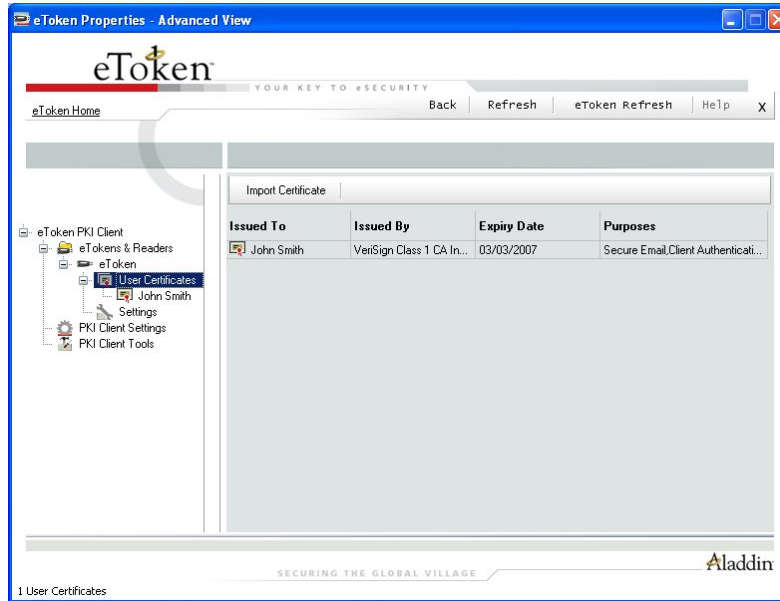
If a PFX file is selected, the private key, corresponding certificate and (optionally) CA certificate(s) will be imported to the eToken. You will be asked to enter the password (if it exists) protecting the PFX file.

In the case of a CER file (which only contains X.509 certificates), the program checks if a private key exists on the eToken. If the private key is found on the eToken, the certificate is stored with it. If no private key is found, then you are asked if you want to store the certificate as a CA certificate. If you indicate yes, the certificate is stored.

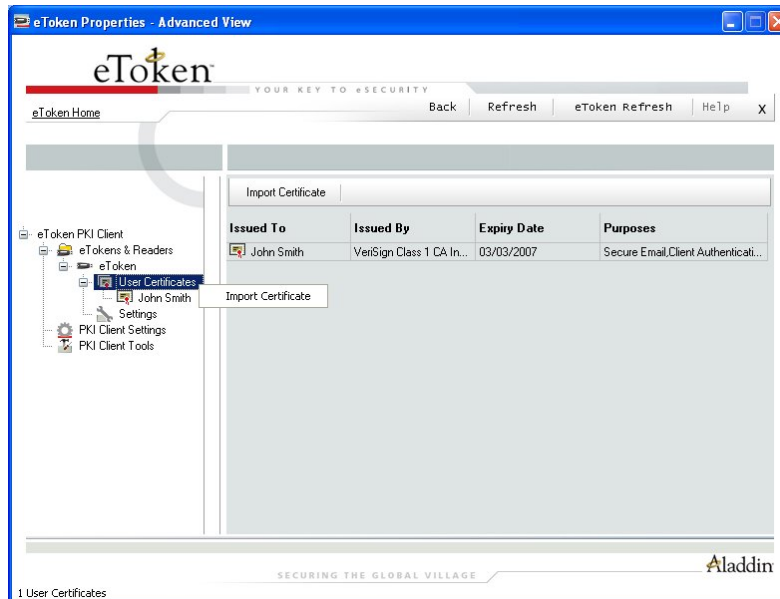
When downloading a certificate to the computer and then importing the certificate to the eToken, the certificate should be removed from the local store and the eToken reinserted before using the certificate to sign and encrypt mail. This ensures you are using the certificate and keys stored on the eToken.

User Certificates

When the specific eToken node is expanded, the object's user certificates are displayed:

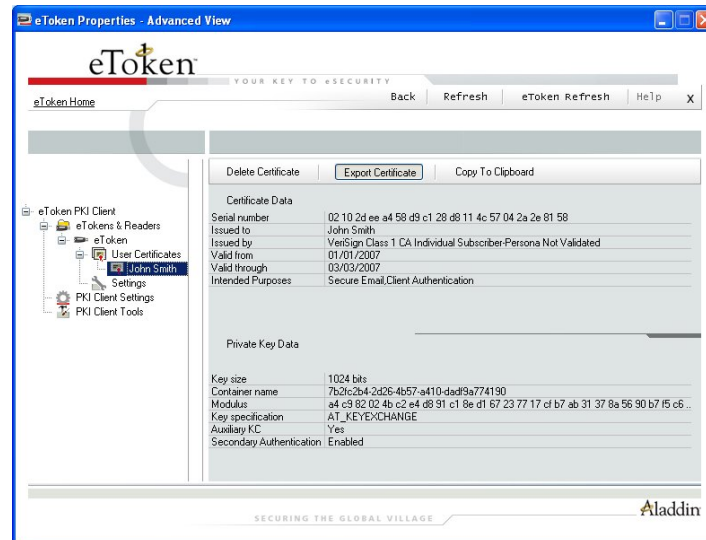


The Import Certificate option is available from the toolbar or the shortcut menu as displayed:

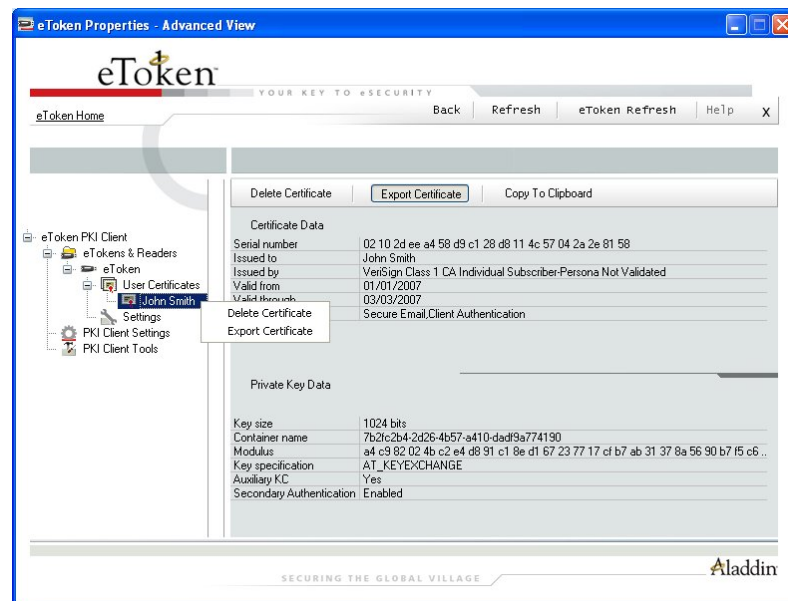


To import a certificate, follow the procedure as described in the Import Certificate section on page 61

The User Certificate(s) on the eToken are itemized in the right pane.



A number of commands regarding a User Certificate are all available by right-clicking the shortcut menu on the certificate itself. The shortcut menu is displayed:

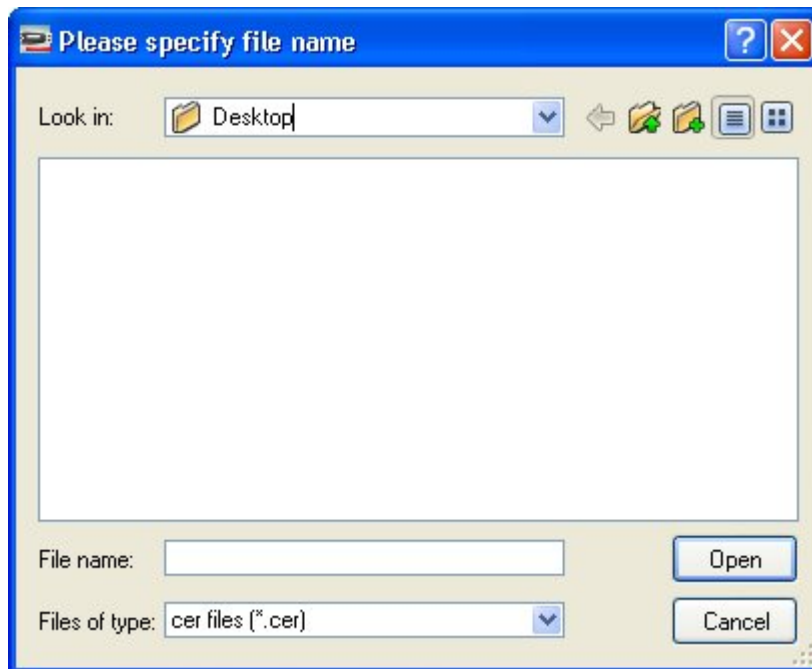


An enlarged version of the shortcut menu is displayed:



A physical eToken only exports the certificate while an eToken Virtual exports the certificate with its key.

Click **Export** Certificate to export the certificate and the following dialog box is displayed:



Select the location to store the certificate and click **OK**.

The user can select a specific certificate to be set as:

- ◆ Default
- ◆ Enrollment Agent
- ◆ Auxiliary

The options are only enabled if the action required can be performed on that particular certificate or key.

Certain applications that use CAPI do not say explicitly which key should be used for their operations (e.g. Microsoft VPN). The PKI Client logic is such that if there is a default key (used for Smartcard Logon) on the eToken, this key will be used for such applications. If no default key exists the PKI Client arbitrarily chooses a key to use.

Most users do not have multiple keys on their eToken so this mechanism works suitably. However in the case where a user needs to explicitly set a key to be used in such an application, the Auxiliary Key serves this purpose.

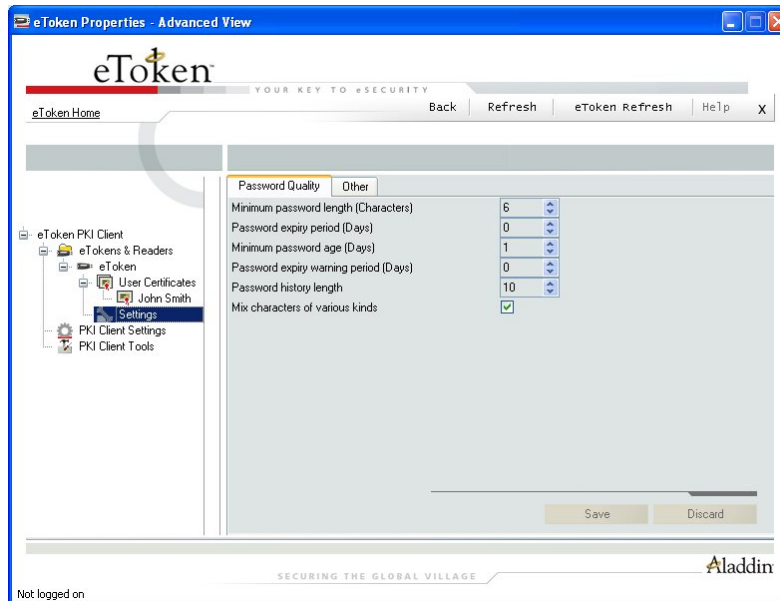
Settings

The settings node under the specific object refers **ONLY** to settings for that object. There are 2 categories of settings:

- ◆ Password Quality – enables configurations relating to password policy for the inserted eToken.
- ◆ Other - enables the configuring of settings relating to cache policies and RSA secondary authentication.

Password Quality

Once the quality parameters have been set, any future passwords are automatically checked against these parameters to determine the password's level of acceptability.



If on your eToken, no password policy is stored on-token you will not see this page e.g. if the eToken was initialized in previous RTE versions.

The various parameters are:

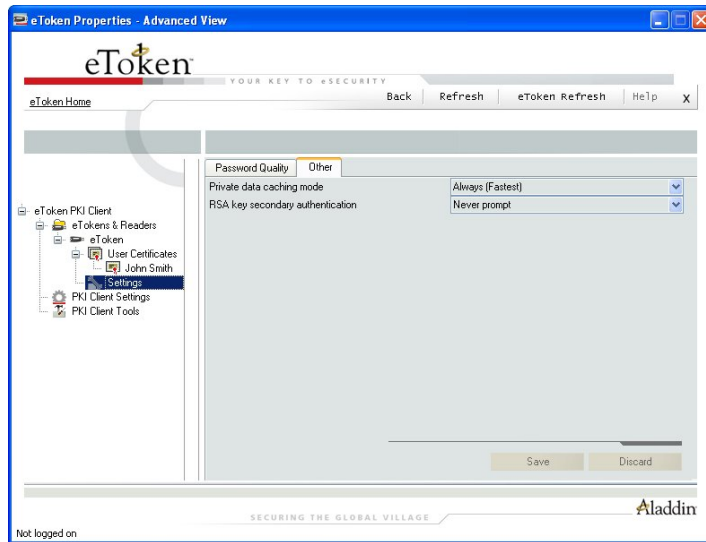
- ◆ **Minimum Password Length** – Defines the minimum password length – Default 6
- ◆ **Password Expiry Period** – Defines the maximum length of time in days before the password expires – Default 0
- ◆ **Minimum Password Age** – Defines the minimum length of time in days before the password can be changed– Default 0
- ◆ **Password Expiry Warning Period** – Defines how many days before password expiry to give a warning– Default 0
- ◆ **Password History Length** – Defines how many old passwords should not be repeated – Default 10
- ◆ **Mix characters of various kinds** – Defines whether mixed characters are required in the eToken password– Default True

Other

These settings refer to options concerning:

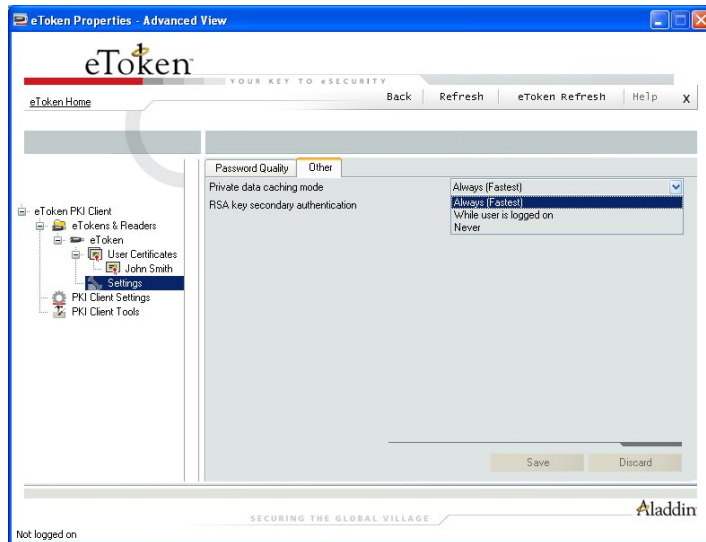
- ◆ **Private data caching mode**

◆ **RSA key secondary authentication**



An explanation of each option is provided:

◆ **Private Data Caching Mode:**



In RTE 3.65 and PKI Client 4.0, public information stored on the eToken is cached in order to enhance performance. This option defines the way private information (excluding private keys on the eToken PRO/NG-OTP / Smartcard) can be cached outside the eToken. The following options are available:

Always (Fastest) – Default Setting

Always caches private information in the application memory. 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.

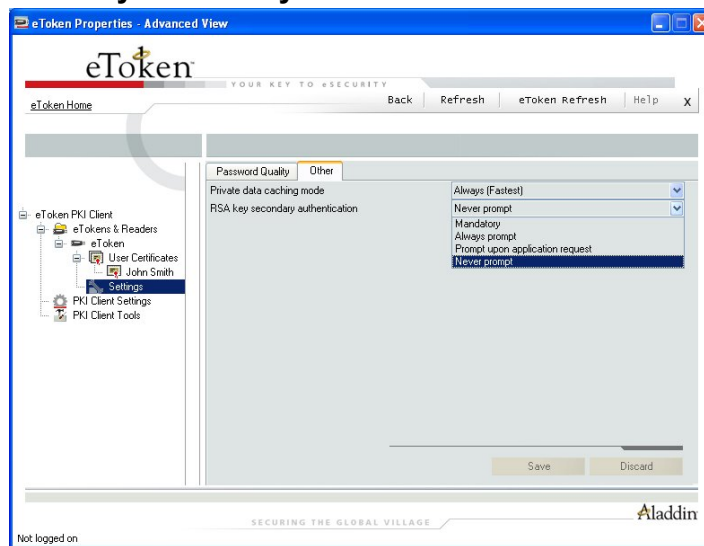
While user is logged on

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.

◆ RSA key secondary authentication:



In PKI Client 4.0 for the eToken PRO and NG-OTP 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):



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:



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

This enables applications that wish to use secondary authentication for 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 – Default Setting

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

- ◆ **Default settings**

The settings default values are:

Private data is **always** cached

Secondary authentication is **never** allowed

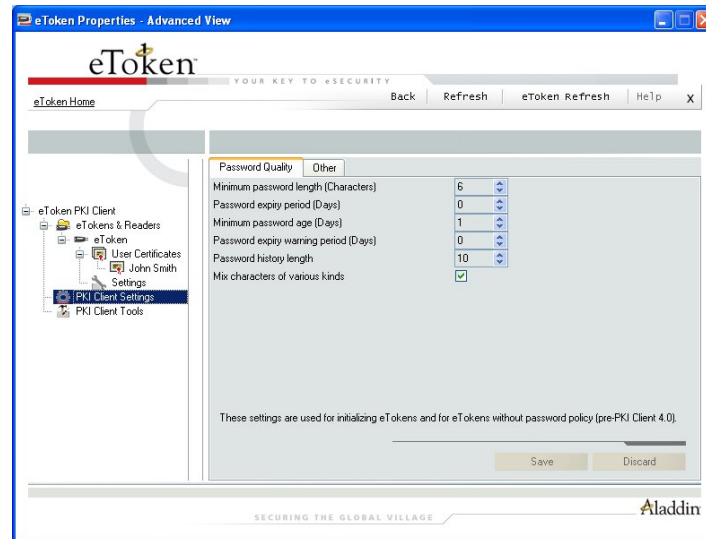
PKI Client Settings

This node refers to generic eToken settings unless superseded by a change to a specific object as detailed above. There are 2 categories of settings:

- ◆ **Password Quality** – enables configurations relating to password policy on eTokens.
- ◆ **Other** - enables the configuring of settings relating to certificate storage, certificate management, logon modes and administrator privileges.

Password Quality

These settings operate globally with the same parameters as the settings for the inserted eToken. For details refer to Password Quality on page 67.

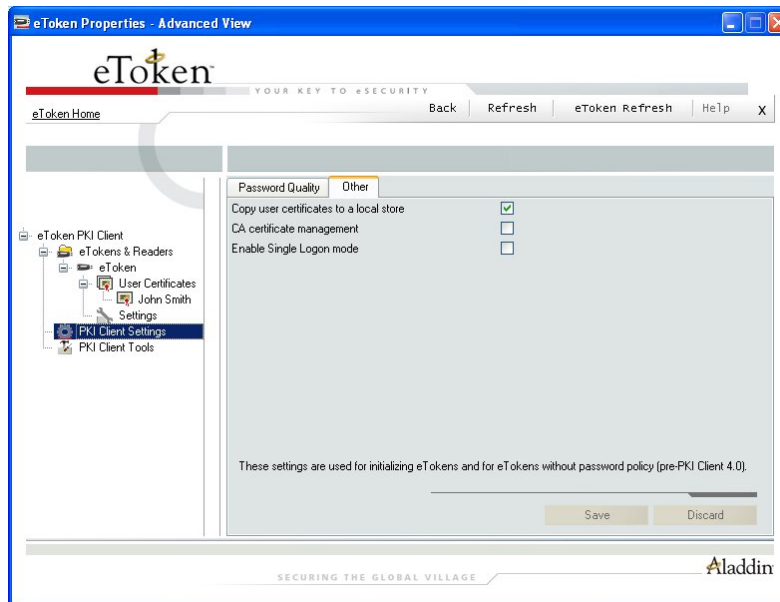


Other

These settings are different from individual eToken "Other Settings" and are:

- ◆ **Copy certificates to a local store**
- ◆ **CA certificate management**
- ◆ **Enable Single Logon mode**

These settings are either enabled or disabled.



Copy user certificates to a local 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 computer).

Upon insertion of an eToken, all certificates are copied to the Certificate Store where Windows applications typically look for them. On eToken removal, these certificates can either be automatically deleted or left in the store. Since certain applications only search the Certificate Store once when they are launched, the default configuration is to leave the certificates in the store on eToken removal.

Since eToken PKI Client propagates all certificates to the Registry store, it never gets any requests for certificate deletion. The certificate is deleted from the Registry store but remains on the eToken. As a result, on the next eToken insertion the certificate is copied again. You may use the eToken Properties configuration tool to remove certificates from the eToken.

CA certificate management

Default – disabled

CA certificates can be downloaded onto the eToken. When this eToken is inserted into the computer, one or more of these CA certificates may not be on the computer. In such a case, an option exists to load the CA certificate if desired.

Note:

Despite the settings chosen, it is possible that another dialog box from Microsoft opens asking if you wish to continue this action. This is standard Microsoft operating procedure because the action to be undertaken may affect security matters on the computer. If you want to copy the CA certificate, click **Yes** in this case.

Enable Single Logon mode

Default – disabled

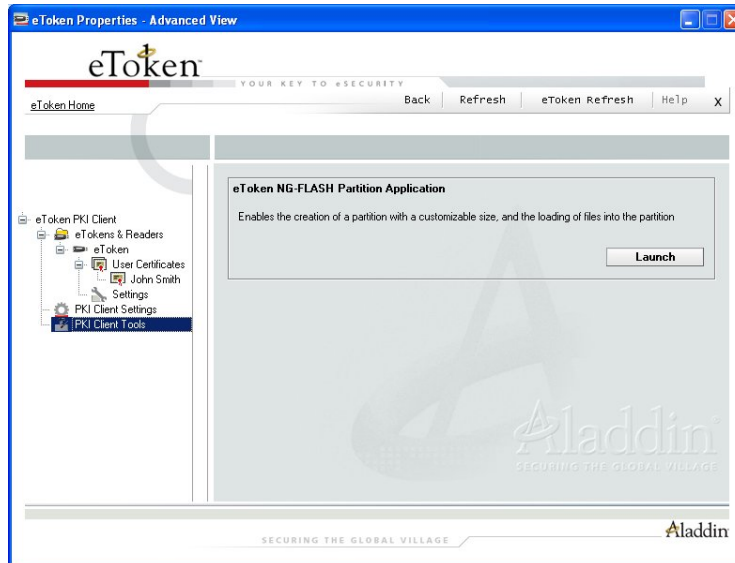
When starting an application with the eToken inserted, the eToken password is needed to proceed. This occurs for each application even if it is during the same computer session. This new option enables users multiple access to the eToken with only one request for the password. This alleviates the need to log on each application separately.

Note

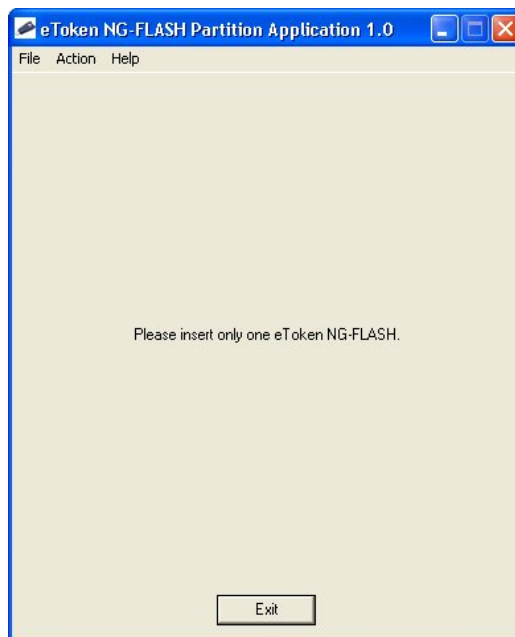
For security reasons, the single logon mode is not utilized by eToken Properties.

PKI Client Tools

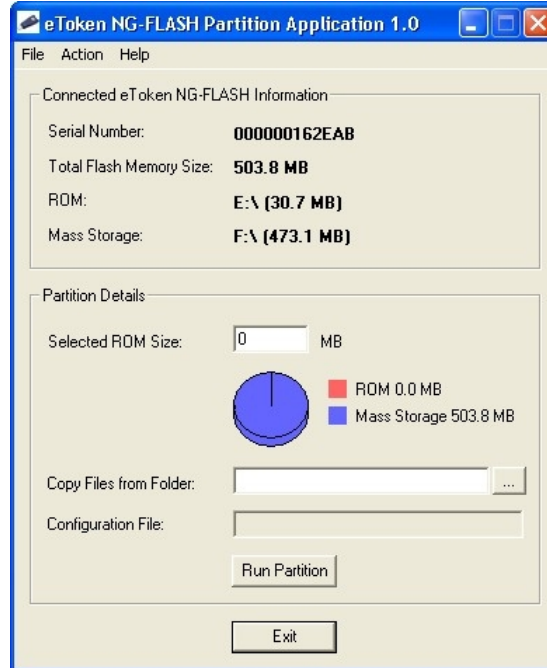
This section provides a link to additional tools that may be applicable to different kinds of eTokens. Currently the only option available is **Launch Mass Storage Application**.



Click **Launch** and the **eToken NG-FLASH Partition Application** is launched as displayed:



Insert an eToken-Flash and the application displays information about the inserted eToken NG-FLASH.



Set the eToken parameters as desired and click **Run Partition**. The eToken NG-Flash is reconfigured.

Chapter 5

Troubleshooting

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

About This Chapter

This chapter includes the following sections:

- ◆ “Problems and Possible Solutions”, on page 79, lists the problems that might arise, and suggests their causes and solutions.
- ◆ “Technical Support”, on page 81, 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 3: Problems, Diagnoses and Solutions

Problem	Possible Diagnosis	Solution
1 Operating system identifies new hardware, but fails to recognize it as 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 PKI Client installation, if necessary, and reinstall.
2 LED on eToken does not light up.	The USB is not enabled in the BIOS.	Enable the USB in the BIOS. If necessary, consult your technical support services supplier.
	The eToken was inserted during installation.	Remove the eToken and reinsert it in the USB port.
	The eToken is defective.	Obtain a new eToken. Contact your local Aladdin office.
3 Application does not recognize the eToken.	Errors in the application.	Check the application for errors.

Problem	Possible Diagnosis	Solution
	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.

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 3 978 1299

Fax: +972 3 978 1010

Email: etoken.techsup@Aladdin.com

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