



PKI Client (Mac) Reference Guide

Version 4.55



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.

February 2008

Contacting Aladdin eToken

If you have any questions about Aladdin eToken, contact your local reseller or the Aladdin eToken technical support team:

| Region | Contact |
|---|--|
| USA | 1-212-329-6658 1-866-202-3494 etoken.ts.us@aladdin.com |
| Austria, Belgium, France, Germany, Italy, Netherlands, Spain, Switzerland, UK | 00800-22523346 |
| Ireland | 0011800-22523346 |
| Rest of the World | +972-3-9781299 |

You can submit a question to the Aladdin eToken technical support team at the following web page:

http://www.aladdin.com/forms/etoken_question/form.aspx

Website

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

Additional Documentation

We recommend reading the following Aladdin eToken publication:

- eToken PKI Client (Mac) 4.55 ReadMe



Table of Contents

| | |
|---|-----------|
| 1. Introduction..... | 1 |
| Overview | 1 |
| New Features | 2 |
| Supported APIs | 2 |
| 2. System Requirements | 3 |
| 3. Installation..... | 5 |
| Pre-Installation for PKI 4.55 (Mac) | 5 |
| Uninstalling eToken PKI Client 3.65..... | 5 |
| Uninstalling eToken RTE 3.60..... | 6 |
| Installing PKI 4.55 (Mac) with the Installer | 7 |
| Installing PKI Client 4.55 (Mac) from the Terminal..... | 11 |
| Uninstalling PKI Client 4.55 (Mac)..... | 12 |
| 4. Configurable Settings..... | 15 |
| Configuration Files..... | 15 |
| Automatic Save of Configuration Files..... | 16 |
| eToken.conf Configuration Keys | 17 |
| General..... | 17 |
| CertStore | 17 |
| InitApp | 18 |
| PQ | 18 |
| UI | 20 |
| Init..... | 20 |
| eToken.common.conf Configuration Keys | 20 |
| 5. Administration | 21 |
| Initializing a Token | 21 |
| Setting Up a New User | 22 |
| Replacing a Token..... | 22 |
| Resetting a Token..... | 22 |

| | |
|---|-----------|
| 6. eToken Properties Application | 25 |
| eToken Properties Overview | 25 |
| Quick Functions | 26 |
| Accessing the Quick Functions Menu | 26 |
| Opening eToken Properties | 27 |
| Generating a One Time Password (OTP) | 28 |
| Changing the eToken Password | 29 |
| Selecting the Active eToken | 29 |
| Viewing Product Information | 29 |
| Hiding and Unhiding the Quick Functions menu | 30 |
| Views | 30 |
| Logging On | 30 |
| Simple View | 31 |
| Renaming the eToken | 33 |
| Changing the eToken Password | 34 |
| Unlocking the eToken using Challenge - Response | 35 |
| Viewing eToken Information | 36 |
| Disconnecting eToken Virtual | 37 |
| Advanced View | 38 |
| Tokens & Readers | 39 |
| Managing eTokens | 40 |
| Certificates | 51 |
| Settings | 53 |
| PKI Client Settings | 56 |
| 7. Apple Keychain | 59 |
| Features Supported by Keychain Access | 59 |
| Displaying eToken in Keychain Access | 60 |
| A. Copyrights and Trademarks | 63 |
| B. FCC Compliance | 65 |
| FCC Warning | 65 |
| CE Compliance | 66 |
| UL Certification | 66 |

Introduction

This chapter introduces Aladdin's eToken PKI Client, the software that enables eToken USB operations and the implementation of eToken PKI-based solutions.

- Overview
- New Features
- Supported APIs

Overview

Public Key Infrastructure (PKI) is a framework for creating a secure method for exchanging information based on public key cryptography, providing for trusted third-party vetting of, and vouching for, user identities. It is an arrangement that 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.

Aladdin's eToken PKI Client 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, proprietary eToken applications such as SSO (Single Sign-On), 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.

The 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 PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications offering secure web access, PC and data security, secure email and more. PKI keys and certificates can be securely created, stored, and used from within eToken smart card-based devices.

The eToken PKI Client can be deployed and updated using any standard software distribution system.

The eToken Properties application and the PKI Client Monitor Service are installed with the eToken PKI Client, providing friendly configuration tools for users and administrators.

New Features

- Java Card-based token support.
- FIPS support.
- Accessibility from the desktop via the PKI Client icon.
- Improved performance through high level caching mechanism
- Support for eToken Virtual (enables users to connect to eToken Virtual, but not to create it).
- Support for Cisco ASA 8.0 connector - supports the Mac-Intel Any-connect VPN client.
- Unified installation for Mac - same installation file for PowerPC and Intel-based versions. All components, drivers and APIs are delivered as a universal binary.

Supported APIs

The following APIs are supported in the Mac version of eToken PKI Client 4.55:

- SAPI (provides cross platform compatibility)
- PKCS#11
- PKCS#11 Extensions

Chapter 2

System Requirements

| | |
|-------------------------------|--|
| Supported Operating Systems | PowerPC - Mac OS X 10.4 (Update 11 and higher) (Tiger) |
| | Intel - Mac OS X 10.4 (Update 11 and higher) (Tiger) |
| | Intel - Mac OS X 10.5 (Update 1 and higher) (Leopard) |
| Supported Browser | Firefox 2.0.x |
| Supported eToken Devices | eToken PRO (both Siemens CardOS and Java Card-based) |
| | eToken NG-OTP |
| | eToken NG-FLASH |
| | eToken PRO Smartcard |
| Required Hardware | USB port |
| Recommended Screen Resolution | 1024 x 768 pixels or higher (for eToken Properties) |

Note:

- Low level APIs used in eToken RTE 3.65 and earlier are not supported.
-

PCSC-Lite

PKI Client 4.55 (Mac) uses the default PCSC-Lite that is installed with Mac OS X. PKI Client 4.55 (Mac) installs a plug-in and driver for PCSC-Lite, during the normal installation process.

PCSC-Lite is managed by the Mac OS X Security Manager. When a device is inserted, the service runs automatically.

No further user intervention is required to install and run PCSC-Lite.

Chapter 3

Installation

In this chapter:

- Pre-Installation for PKI 4.55 (Mac)
- Installing PKI 4.55 (Mac) with the Installer
- Uninstalling PKI Client 4.55 (Mac)

Pre-Installation for PKI 4.55 (Mac)

Before installing PKI 4.55 (Mac), uninstall previous versions of PKI (RTE 3.60 and 3.65)

Uninstalling eToken PKI Client 3.65

1. Open the Mac terminal and type:
`cd /usr/local/Uninstall_PKI\ Client/Uninstall\PKI\ Client.app/Contents/MacOS`
2. Press **Enter**.
3. Type `/Uninstall\ PKI\ Client`
4. Press **Enter**.
The Uninstall PKI Client Wizard is displayed.
5. Click the lock to make changes
The *Authenticate* window is displayed.
6. Enter the administrator *User Name* and *Password* in the appropriate fields and click **OK**.

The *Uninstall PKI Client* runs and a progress bar is displayed indicating the status. When the progress bar stops running, the *Uninstall PKI Client* window is displayed.

7. Click **Next**.

The *Uninstall Options* window is displayed.

8. Click **Complete Uninstall** and **Next**.

The files and folders are uninstalled.

9. Click **Next**.

The Uninstall Complete dialog box is displayed.

10. Click **Done**.

The eToken PKI Client is uninstalled.

Uninstalling eToken RTE 3.60

To uninstall eToken RTE 3.6 automatically:

Note:

The user must have root/administrator rights to complete the installation successfully.

1. Open the Finder and locate eToken Middleware-3-60.xx (where xx represents the build number).

Since this file was installed during the installation process, the right pane shows the file needed for the uninstall.

The *eToken Middleware.pkg* and *eToken Middleware Uninstall.pkg* packages are displayed.

2. Double-click eToken Middleware Uninstall.pkg to start the uninstall process.

The *Install eToken - Introduction* window opens and a confirmation pop up opens asks you to confirm that the installation should continue.

3. Click **Continue** to return to the *Install eToken* window.

4. Click **Continue**

The *Select Destination* window opens.

5. Select the destination folder and click **Continue**.

6. The *Authenticate* dialog box opens.

7. Enter the *Name* and *Password* and then click **OK**.

The installation process continues until the *Finish Up* window opens with the message "Software was successfully installed".

8. Click **Close** to exit the installation.
 9. Close the Finder
- eToken RTE 3.60 is removed.

To uninstall eToken RTE 3.60 manually:

1. Type `cd /Volumes/eToken\ Middleware-3-60.*/eToken\ Middleware.pkg\Contents/Resources/payload`
2. Change to the root user.
3. Run the command: `/petoken uninstall`

Installing PKI 4.55 (Mac) with the Installer

Installation Packages

The installation packaging for eToken PKI Client 4.55 (Mac) is PackageMaker.

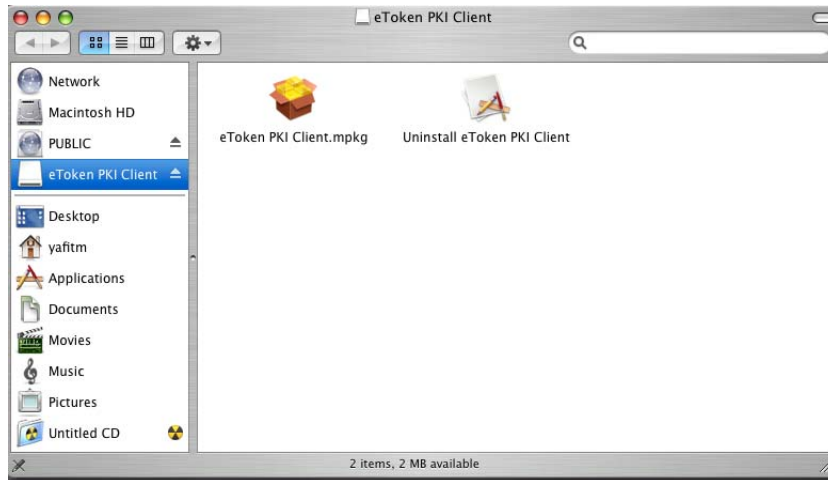
There are three eToken PKI Client 4.55 (Mac) .dmg packages, to support different installation types:

| Installation Type | Description | .dmg Package Name (where [build] = build number) |
|-------------------|---|---|
| Full | Includes eToken Properties with full features | pkiclient.4.55.[build].dmg |
| Limited | Includes eToken Properties with basic features only | pkiclient-limited.4.55.[build].dmg |
| Minimal | Without eToken Properties | pkiclient-minimal.4.55.[build].dmg |

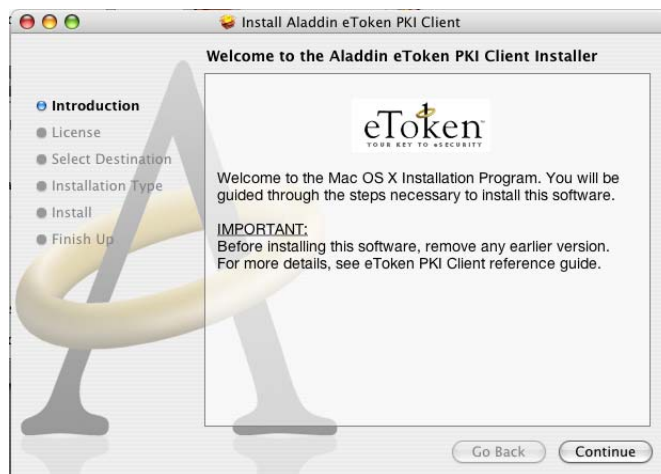
To install PKI Client 4.55 (Mac) with the installer:

1. Double click the .dmg file.

A new disk image file is created in the Finder window, including an mpkg installation file and an uninstall application.

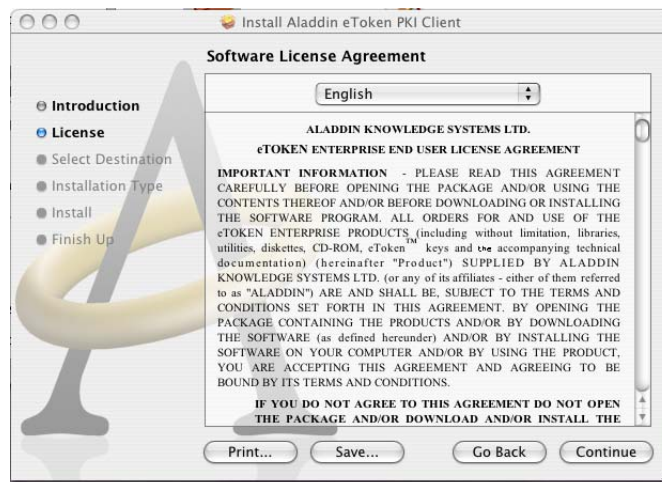


2. To start the installation, double click **eToken PKI Client.mpkg**. The *Welcome to the Aladdin eToken PKI Client installer* window opens



3. Click **Continue**.

The *Software License Agreement* window opens.



4. Click **Continue**.

The agreement window opens.

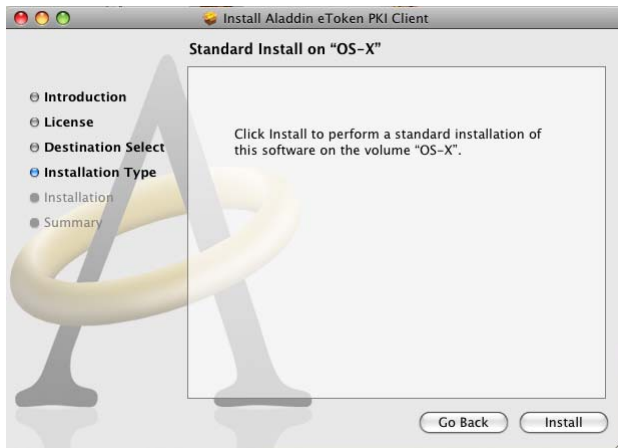


5. Click Agree to accept the software license agreement.

Note:

If a previous version of PKI Client is installed, the installation cannot continue and you are prompted to uninstall the previous version. The uninstallation of earlier versions cannot be performed with the PKI Client 4.55 (Mac) uninstall application. For details of uninstalling earlier versions see *Uninstalling eToken PKI Client 3.65* on page 5 or *Uninstalling eToken RTE 3.60* on page 6.

The *Standard Install* on "OS-X" window opens.



6. Click **Install**.

The *Authenticate* window opens.

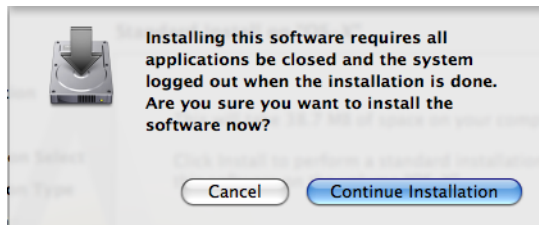


7. Enter *Name* and *Password* and click **OK**.

Note:

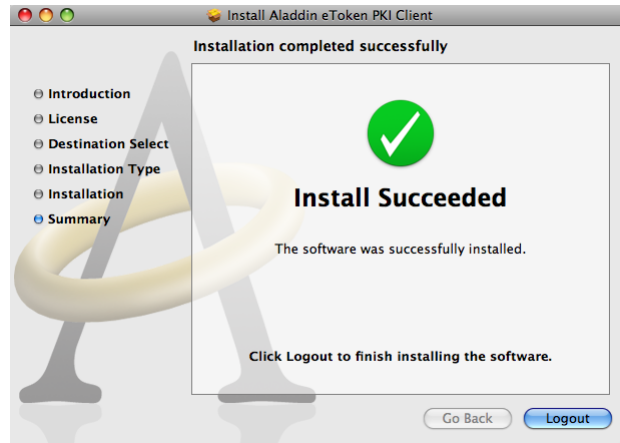
You require Administrator permissions to install eToken PKI Client.

A message warns you that the installation will close all applications and log you out of the system when the process is complete.



8. To continue click **Continue installation**.

PKI Client installs. The *Installation completed successfully* screen opens.



9. Click **Logout**.
Mac OS X logs out.
10. Log in again to Mac OS X.

Installing PKI Client 4.55 (Mac) from the Terminal

To install PKI Client 4.55 (Mac) from the terminal:

1. Extract the eToken PKI Client 4.55.mpkg file from the dmg file.
2. At the location in the terminal in which you extracted the file run
`sudo installer -pkg ./eToken\ PKI\ Client\ 4.55.mpkg/ -target /`
3. Enter your root password when prompted.
PKI Client 4.55 (Mac) is installed.
4. Following installation, log out of Mac OS X and log in again.

Uninstalling PKI Client 4.55 (Mac)

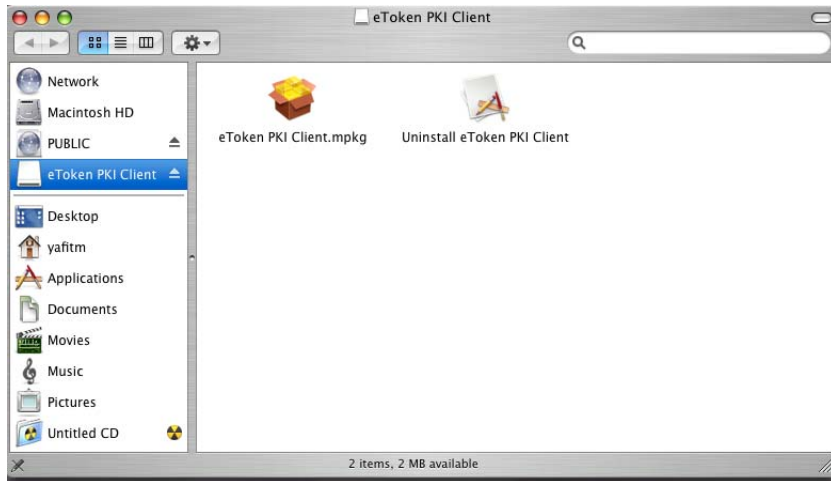
Note:

Before uninstalling PKI Client 4.55 (Mac), make sure that eToken Properties is closed.

To uninstall PKI Client 4.55 (Mac)

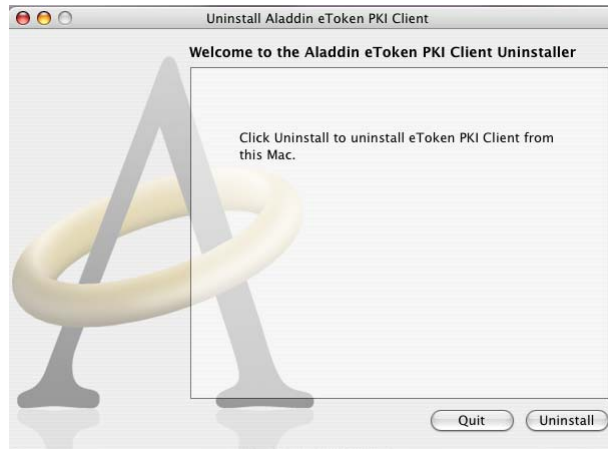
1. Double click the .dmg file.

A new disk image file is created in the Finder window, including an mpkg installation file and an uninstall application.



2. Click **uninstall eToken PKI Client**.

The *Welcome to the Aladdin eToken PKI Client Uninstaller* window opens.



3. Click **Uninstall**.
The *Authenticate* window opens.

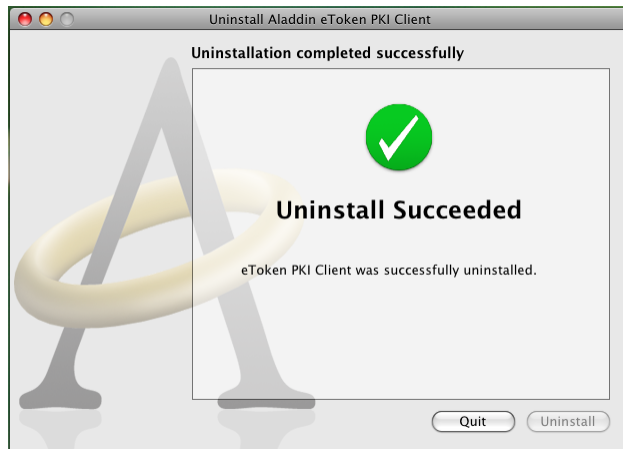


4. Enter *Name* and *Password* and click **OK**.

Note:

You require Administrator permissions to uninstall eToken PKI Client.

PKI Client uninstalls and the *Uninstallation completed successfully* screen opens.



5. Click **Quit**.

Chapter 4

Configurable Settings

This chapter provides administrator guidelines for setting configuration keys.

In this chapter:

- Configuration Files
- eToken.conf Configuration Keys
- eToken.common.conf Configuration Keys

Configuration Files

PKI Client (Mac) 4.55 contains two configuration files:

- eToken.conf
/etc/eToken.conf (-rw-rw-r--)
- eToken.common.conf (eToken Virtual)
/etc/eToken.common.conf (-rw-rw-rw-)

Owner: root\admin

eToken.conf has administrator permissions

eToken.common.conf has user permissions.

Automatic Save of Configuration Files

When PKI Client (Mac) is uninstalled, the configuration files are saved to:

```
/etc/eToken.conf.saved  
/etc/eToken.common.conf.saved
```

The saved files can then be used to copy the settings to a new installation.

eToken.conf Configuration Keys

eToken.conf contains all keys except for eToken Virtual keys, which are located in eToken.common.conf

General

| Key Name | Description | DWord Value | Default |
|---------------|--------------------------|-------------|---|
| PcscSlots | Number of PC/SC slots | 1-16 | 3 Note: to use more than 3 slots concurrently, enter the required number. |
| SoftwareSlots | Number of software slots | 1-10 | 1 |

CertStore

| Key Name | Description | DWord Value | Default |
|-------------------------|---|-------------|---------|
| PropagateCACertificates | Export all CA certificates on the token to the Trusted CA location 0 = disabled 1 = enabled | 0/1 | 1 |

InitApp

| Key Name | Description | DWord Value | Default |
|--------------|---|-------------|---------|
| FIPS | FIPS Support 0 = disabled 1 = enabled | 0/1 | 0 |
| AdvancedView | <i>Advanced</i> button in eToken Properties application 0 = disabled 1 = enabled | 0/1 | 1 |
| showintray | The Quick Functions menu (monitor) is displayed on the desktop 0 = not displayed 1 = displayed 2 = displayed when token inserted (does not disappear when token removed) | 0/1/2 | 1 |

PQ

| Key Name | Description | DWord Value | Default |
|---------------|---|-------------|---------|
| pqModifiable | The password quality can be changed after initialization 0 = cannot be changed 1 = can be changed | 0/1 | 1 |
| pqHistorySize | Number of recent passwords that may not be repeated | >=0 | 10 |
| pqMaxAge | Total number of days password is valid 0 = no expiration | >=0 | 0 |

| Key Name (Continued) | Description (Continued) | DWord Value | Default (Continued) |
|-------------------------|--|----------------|------------------------|
| pqMinAge | Total number of days required before change 0 = none | >=0 | 0 |
| pqMinLen | Minimum password length | >=4 | 6 |
| pqMixChars | Mixed characters required 0 = disabled 1 = enabled | 0/1 | 1 |
| pqWarnPeriod | Total number of days before expiration to display warning 0 = no warning | >=0 | 0 |

UI

| Key Name | Description | DWord Value | Default |
|------------|---|-------------|---------|
| Languageld | UI Language (PKI Client (Mac) 4.55 supports English only) | EN | EN |
| linguist | Path to Linguist application | | |

Init

| Key Name | Description | DWord Value | Default |
|--------------------------------|---|-------------|---------|
| RSASecondaryAuthenticationMode | Can be configured in eToken Properties. For details see <i>Initializing eToken</i> on page 42 | | |
| PrivateDataCaching | Can be configured in eToken Properties. For details see <i>Initializing eToken</i> on page 42 | | |
| RSA-2048 | Can be configured in eToken Properties. For details see <i>Initializing eToken</i> on page 42 | | |
| HMAC-SHA1 | Can be configured in eToken Properties. For details see <i>Initializing eToken</i> on page 42 | | |

eToken.common.conf Configuration Keys

eToken.common.conf contains eToken Virtual keys.

| Key Name | Description | DWord Value | Default |
|-----------------|---------------------------|-------------|---------|
| FileName(slot0) | File name with full path. | | |

Chapter 5

Administration

In this chapter:

- Initializing a Token
- Setting Up a New User
- Replacing a Token
- Resetting a Token

Initializing a Token

The process of initializing a token:

- Erases all data and configurable parameters on the token
- Resets the token to the default password
- Restores a token with corrupted data to a usable state
- Enables the administrator to set an administrator password on the token, thus allowing a token user password to be reset in the future without data being erased from the token
- Enables the administrator to set configurable parameters on the token
- Enables a CardOS 4.01 or 4.2B-based eToken PRO device to be initialized either as a standard eToken PRO or as a FIPS eToken PRO

For detailed information on performing token initialization in eToken Properties, see *Initializing eToken* on page 42.

Setting Up a New User

To set up a new user:

1. Install the eToken PKI Client on the user's computer.
2. Initialize a token for the user.
See the *Initializing eToken* on page 42.
3. Issue the token to the user, with instructions to personalize it as soon as possible by renaming it and changing the password.
See the *Renaming the eToken* on page 33 and *Changing the eToken Password* on page 29.

Replacing a Token

When a user's token is lost or damaged, the administrator should initialize another token and issue it to the user, with instructions to personalize it as soon as possible.

Resetting a Token

If a user forgets the token password, the administrator should take the token and do one of the following:

- Re-initialize the token, whereby the token's data and configurable parameters are erased and the default token password is reset.
See *Initializing eToken* on page 42.
- Reset only the user password, whereby all of the token's data and configurable parameters are retained.
See *Setting User Password* on page 50.

This option is available only if the token was initialized with an eToken administrator password.

Note:

eToken TMS 2.0 offers a Virtual eToken solution, specially designed for employee on-the-road situations where the replacement of a lost or missing token is not practical.

Chapter 6

eToken Properties Application

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

In this chapter:

- [eToken Properties Overview](#)
- [Quick Functions](#)
- [Views](#)
- [Logging On](#)
- [Simple View](#)
- [Advanced View](#)

eToken Properties Overview

Administrators use eToken Properties to set token policies. Users use eToken Properties to perform basic token management functions, such as changing passwords and viewing certificates on the tokens. In addition, eToken Properties provides users and administrators with a quick and easy way to transfer digital certificates and keys between a computer and a token.

eToken Properties includes an initialization feature allowing administrators to initialize tokens according to specific organizational requirements or security modes, and a password quality feature which sets parameters to calculate a token password quality rating.

CAUTION:

Do not remove the token from the USB port during an operation. Many operations, such as key generation, certificate enrollment, and certificate removal require multiple actions. If the token is removed during one of these actions, the data structure on the token may be damaged and data lost. The token may need to be re initialized as a result.

eToken Properties provides information about the token, including its identification and capabilities. It has access to information stored on the token such as keys and certificates, and enables management of content, such as password profiles.


Quick Functions

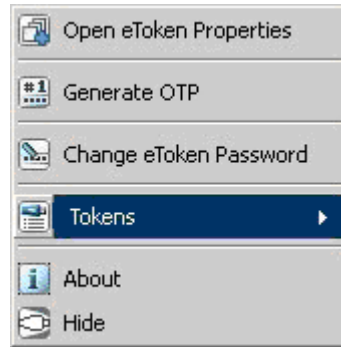
The following functions can be accessed quickly from the tray icon:

- **Open eToken Properties**
- **Generate OTP:** generates OTP for eToken Virtual
- **Change eToken Password**
- **Tokens:** selects the activated token when more than one is inserted
- **About:** displays product information
- **Hide:** hides the icon

Accessing the Quick Functions Menu

To access the quick functions menu:

- Right-click the eToken icon .
The quick functions menu opens.



Opening eToken Properties

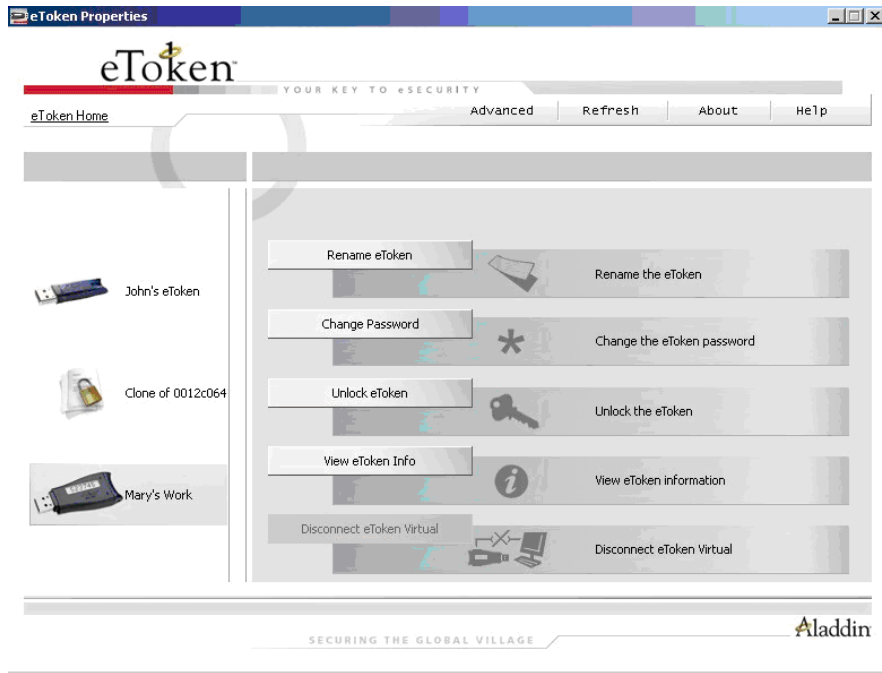
To open eToken Properties:

- From the Quick Functions Menu select **Open eToken Properties**.

Note:

eToken Properties can also be started from
Go>Applications>eToken>eToken Properties.

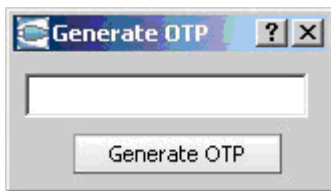
The *eToken Properties* window opens in the Simple view, displaying all tokens that are connected to your computer.



Generating a One Time Password (OTP)

To generate an OTP:

1. Select **Generate OTP**.
The **Generate OTP** dialog box opens.



2. Click **Generate OTP**.
The *Log On to eToken* dialog box opens.
3. Enter the token password.
The generated OTP is displayed in the *Generate OTP* dialog box.

Changing the eToken Password

To change the eToken password:

- Select **Change eToken Password**.
The *Change Password* dialog box opens.
See *Changing the eToken Password* on page 34.

Selecting the Active eToken

To select the active eToken:

1. Select **eTokens**.
A list of inserted eTokens is displayed.



2. Select the required eToken.

Viewing Product Information

To view product information:

- Select **About**.

Hiding and Unhiding the Quick Functions menu

To hide the quick functions menu:

- Select **Hide**.

To unhide the quick functions menu:

Do one of the following

- Remove and re-insert the token
- Re-boot the computer

Views

eToken Properties includes two viewing options:

- **Simple view:** to perform basic and common tasks.
See *Simple View* on page 31.
- **Advanced view:** for complete control over the PKI Client and the inserted tokens.
See *Advanced View* on page 38.

Each view displays two panes:

- The left pane indicates which token (Simple view) or which object (Advanced view) is to be managed.
- The right pane enables the user to perform specific actions to the selected token or object.

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

Logging On

Certain operations which change token configurations require entering either the token user password or the token administrator password.

When the token user password is required, the *Log On to eToken* dialog box is displayed:

To log on to eToken as a user:

- Enter the token password and click **OK**.

You may only log on as an administrator if an administrator password is present on the token.

When the token administrator password is required, the *Administrator Logon to eToken* dialog box is displayed:

To log on to eToken as an administrator:

- Enter the token administrator password and click **OK**.

Note:

If you are logged on as an administrator and wish to access functions that require a user password, the *Log On to eToken* dialog box is displayed, requesting the token user password.

Simple View

When eToken Properties is launched, the *eToken Properties* window opens in the Simple view.

When a token is inserted or an eToken Virtual is present, a device specific icon representing the inserted token is displayed in the left pane.

Each token has a name to the right of the icon. *eToken* is the default name if no name has been assigned to the token.

The token that is selected is marked by a shaded rectangle in the left pane.

eToken icons

| | |
|---|----------------------------------|
|  | eToken PRO |
|  | eToken Virtual |
|  | eToken NG-OTP |
|  | eToken NG-FLASH |
|  | Smart Card Reader – with no card |
|  | Smart Card Reader – with card |
|  | eToken with corrupted data |
|  | Unknown token |

In the right pane, the user may select any of the following actions that are enabled:

- **Rename eToken** – sets the token name
- **Change Password** – changes the eToken user password

- **Unlock eToken** – resets the user password via a challenge response mechanism (Only enabled when an administrator password has been initialized on the token)
- **View eToken Info** – provides detailed information about the token
- **Disconnect eToken Virtual** – disconnects the eToken Virtual, with an option for deleting it

The toolbar along the top contains these functions:

- **Advanced** – switches to the Advanced view
- **Refresh** – refreshes the data for all connected tokens
- **About** – displays information about the product version
- **Help** – launches the online help

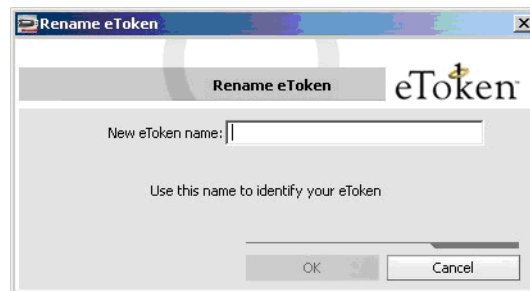
A hyperlink to the eToken website, *eToken Home*, appears at the top left of the window.

Renaming the eToken

The token name can be personalized.

To rename a token:

1. In the left pane of the *eToken Properties* window, select the token to be renamed.
2. Click **Rename eToken** in the right pane
The *Rename eToken* dialog box is displayed.



3. Enter the new name in the *New eToken* name field.
4. Click **OK**.

The new token name is displayed in the *eToken Properties* window.

Changing the eToken Password

All eToken devices are configured with the factory initial password, 1234567890. To ensure strong, two factor security, it is important for the user to change the eToken password to a private user password as soon as the new eToken is received.

When an eToken password has been changed, the new password is used for all eToken applications involving the token. It is the user's responsibility to remember the eToken password. Without it, the user cannot use the token.

Setting an administrator password on the token enables the administrator to unlock a locked token by resetting a new user password if it is forgotten. We recommend initializing all tokens with an administrator password.

eToken's Password Quality feature enables the administrator to set certain complexity and usage requirements for the password.

See *Password Quality* on page 54.

Note:

The eToken user password is an important security measure in safeguarding your company's private information. The best passwords are at least eight characters long and include upper and lower case letters, punctuation marks and numbers created in a random order. We recommend against using passwords that can be easily discovered, such as names or birth dates of family members.

To change the eToken Password:

1. In the left pane of the *eToken Properties* window, select the token to which the new password will be assigned.
2. Click Change Password in the right pane.
The *Change Password* dialog box is displayed.
3. Enter the current eToken password in the *Current eToken Password* field.

4. Enter the new eToken password in the *New eToken Password* and *Confirm* fields.

Note:

As you type a new password, the password quality indicator on the right displays a percentage score of how well the new password matches the password quality policy.

5. Click **OK**.
The eToken password is changed.

Unlocking the eToken using Challenge - Response

A token becomes locked if the eToken password is entered too many times incorrectly.

If the token had been initialized with an administrator password, and the administrator is present, the token may be unlocked using the eToken Properties Advanced view.

See *Setting User Password* on page 50.

When the administrator is located remotely, for example when an employee is out of the office, a Challenge – Response authentication method can be employed to unlock the token. With this method, the user sends the administrator the Challenge Data supplied by eToken Properties, and then enters the Response Data provided by the administrator. The user then enters a new password and the token is unlocked.

To unlock a token using Challenge – Response:

1. In the left pane of the *eToken Properties* window, select the token to be unlocked.
2. Click **Unlock eToken** in the right pane.
The Unlock eToken dialog box is displayed.

3. Contact the administrator and provide him with the Challenge Data.

CAUTION:

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

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

4. The administrator provides the Response Data to be entered.
5. Enter a new token password in the Password and Confirm fields.
6. Select **Change password on first logon** if the new password is known to others and must be changed.
7. Click **OK**.

The token is unlocked and a confirmation message is displayed.

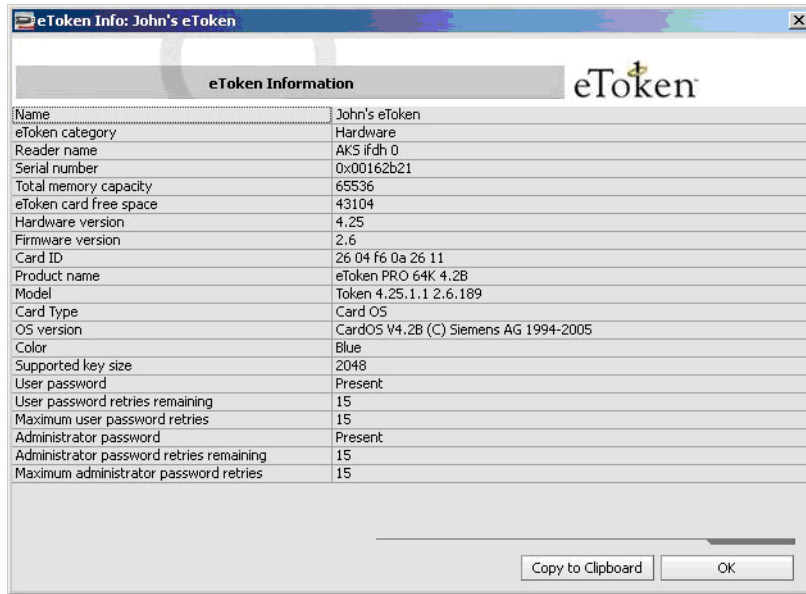
Note:

Response Data creation 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.

Viewing eToken Information

Information relating to a specific token can be viewed by selecting the token in the left pane of the *eToken Properties* window, and clicking **View eToken Info** in the right pane.

The *eToken Information* dialog box is displayed.



The information in this dialog box can be copied to the clipboard.

To paste the information into an application:

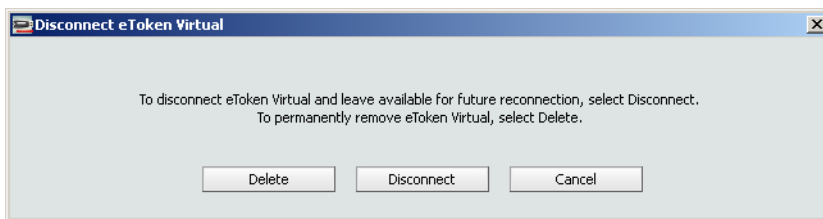
1. Click **Copy to Clipboard**.
2. Place the cursor in the target application and paste the information.

Disconnecting eToken Virtual

When the eToken Virtual is no longer necessary, disconnect it from its attached reader.

To disconnect an eToken Virtual:

1. In the left pane of the *eToken Properties* window, select the eToken Virtual to be disconnected.
2. Click Disconnect in the right pane.
Disconnect eToken Virtual message is displayed.



3. Do one of the following:
- ◆ To keep the eToken Virtual file on the computer, click **Disconnect**; only the connection from the eToken Virtual to eToken Properties is disconnected.
 - ◆ To remove the eToken Virtual file from the computer, click **Delete**.

Note:

Disconnecting the eToken Virtual without removing it completely is applicable when the user is out of the office and may need to use the eToken Virtual on the road later. When the lost eToken is replaced, the eToken Virtual should be completely removed from the computer.

Advanced View

The eToken Properties Advanced view provides additional token management functions.

Click **Advanced** on the Simple view toolbar. The *eToken Properties* window opens in the Advanced view.

The toolbar along the top offers these functions:

- **Back:** switches to the Simple view
- **Refresh:** refreshes the data for all connected tokens
- **Help:** launches the online help

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 information about the highlighted object, such as the number of connected readers, or the current logon state.

The left pane provides a tree view of the various objects to be managed. The tree expands to show objects of inserted tokens.

- Left-click an object in the tree. Information about that object appears in the right pane.
- Right-click an object in the tree. A shortcut menu of commands for that object appears.

Tokens & Readers

This node manages the readers (slots) that are available on the system.

When the *Tokens & Readers* node is selected, the toolbar displays the following:

- Add eToken Virtual

The same command is available when you right-click the eTokens & Readers node.

Adding an eToken Virtual

PKI Client (Mac) 4.55 supports eToken Virtual, a software token. The eToken Virtual is stored in a file on the computer.

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:

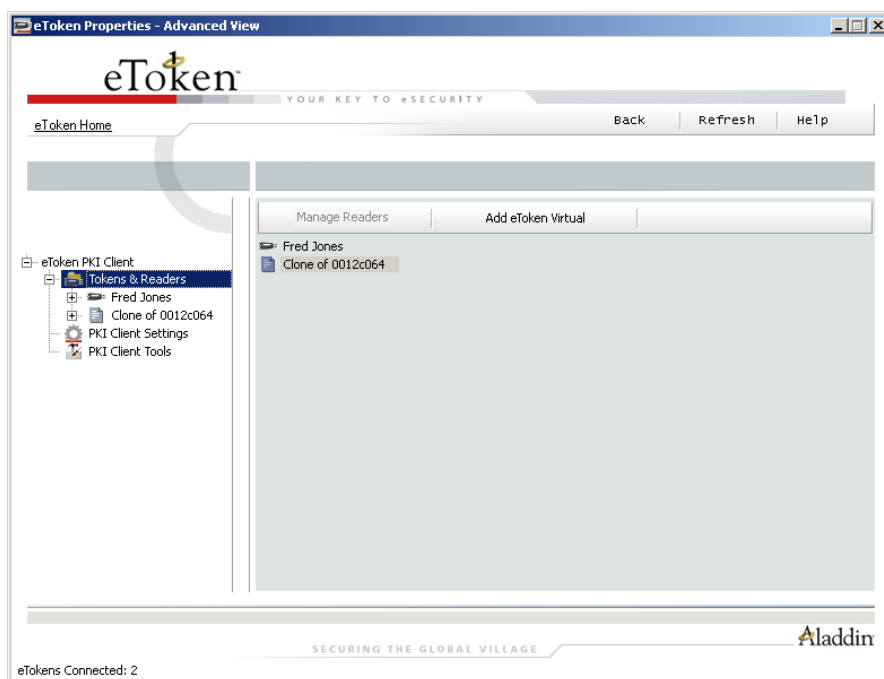
1. Click **Add eToken Virtual** on the toolbar, or right-click **eTokens & Readers** and select **Add eToken Virtual** from the shortcut menu.
 2. Navigate to the eToken Virtual file (*.etv) and double-click it.
- The *eToken Virtual* is added and a confirmation message opens.



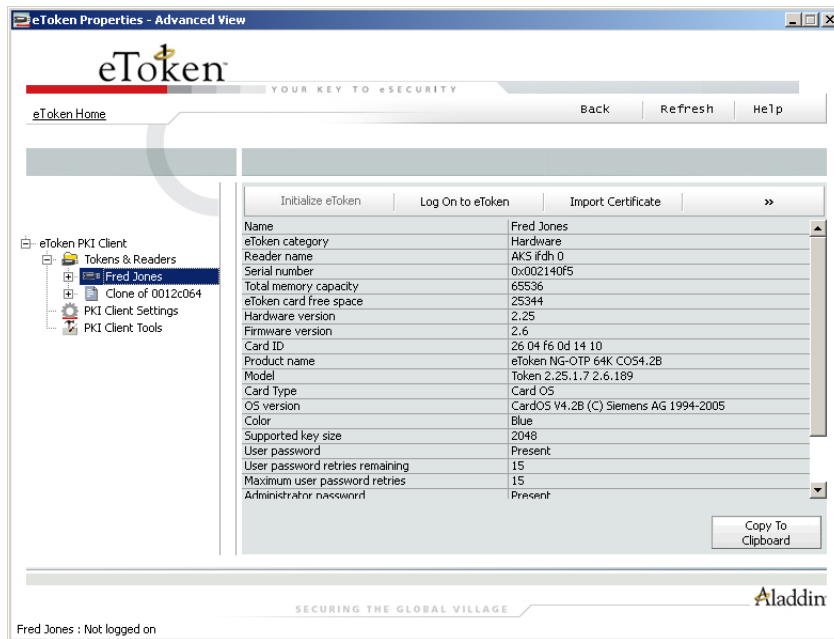
3. Click **OK**.

Managing eTokens

When the Tokens & Readers node is expanded, the names of all inserted tokens, physical and virtual, are displayed.



To display all information about a token in the right pane, select it in the left pane.



This is the same information that is displayed in *Viewing eToken Info* in the Simple view.

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

The expand arrow to the right of the toolbar shows all other commands available with this object.

These commands are also available by right-clicking the object in the left pane.

Certain commands are disabled if not applicable. For example, administrator functions are disabled for an eToken Virtual.

Some Advanced view commands are identical to those in the Simple view:

- Rename
- Change Password
- Unlock
- Disconnect

Initializing eToken

The eToken initialization option restores an eToken to its initial state. It removes all objects stored on the eToken since manufacture, frees up 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, preparing it to be used by another employee.

The following data is initialized:

- 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 logon
- Initialization key

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

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

To initialize an eToken:

1. Click **Initialize eToken** on the toolbar, or right-click the token name in the left pane and select **Initialize** from the shortcut menu. The *eToken Initialization Parameters* dialog box opens.
2. Enter a name for the eToken in the eToken Name field. If no name is entered, the default name, "eToken", is applied.
3. Select **Create User Password** to initialize the token with an eToken user password. Otherwise, the token is initialized without an eToken password, and it will not be usable for eToken applications.

4. If **Create User Password** is selected, enter a new eToken user password in the *Create User Password* and *Confirm* fields.

Note:

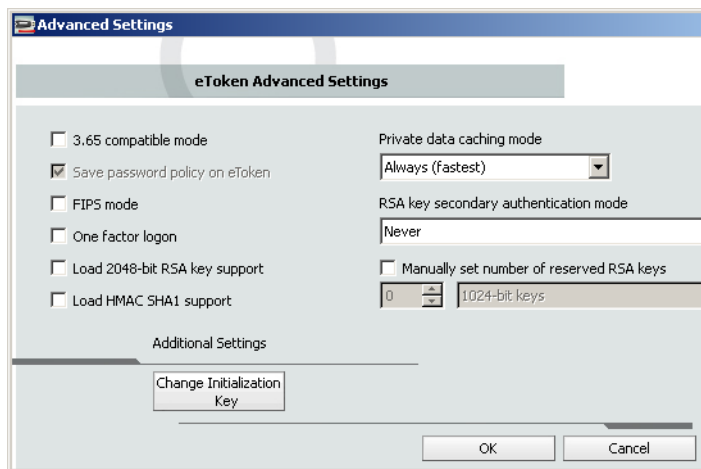
The default password for a new token is 0123456789. If the default password is not changed during initialization, the *Password must be changed at first logon* field must be selected (default setting). If this is not done, the initialization will fail, as the default password will not meet default password quality requirements (See *Password Quality* on page 54). If the *Password must be changed at first logon* field is selected, the initialization will succeed and the user will be prompted to create a new password when next logging on with the token. The user will then be required to enter a password meeting password quality requirements, as configured in the settings window (See *Settings* on page 53).

5. To initialize an administrator password, select **Create Administrator Password** and enter a password in the *Create Administrator Password* and *Confirm* fields. (Minimum password length is 4 characters.)

Note:

Creating an administrator password enables certain functions to be performed on the token, such as resetting a user password on a locked token.

6. In the *Set maximum number of logon failures* field, enter a value between 1 and 15. This counter specifies the number of times the user or administrator can attempt to log on to the token with an incorrect password before the token is locked. The default setting for the maximum number of incorrect logon attempts is 15.
7. If required, select **Password must be changed on first logon**. This is selected by default.
8. To configure advanced settings, click **Advanced**. The *eToken Advanced Settings* dialog box opens.



9. Complete the fields as follows:

| Field | Description |
|--------------------------------|---|
| 3.65 compatible mode | Select to maintain compatibility with eToken RTE 3.65. |
| Save password policy on eToken | Select to keep password policy on the eToken device. |
| FIPS mode | Select to enable FIPS support. FIPS (Federal Information Processing Standards) is a US government approved set of standards designed to improve the utilization and management of computer and related telecommunication systems. The eToken PRO can be configured in FIPS mode. |
| One factor logon | Default: disabled. When one factor logon is enabled, only the presence of the eToken is required to log on to applications. A password is not required. Note: For security reasons, single factor logon is not applied to eToken Properties. |
| Load 2048-bit RSA key support | Select to enable 2048-bit RSA key support (on compatible token). |
| Load HMAC SHA1 support | Select to enable HMAC SHA1 support (on compatible token). |

| Field (Continued) | Description (Continued) |
|---------------------------|--|
| Private data caching mode | <p>In PKI Client 4.55, public information stored on the eToken is cached to enhance performance. This option defines when private information (excluding private keys on the eToken PRO / NG OTP / Smartcard) can be cached outside the eToken.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none">■ Always (fastest): always caches private information in the application memory. This enables fast performance, as certain information is cached on the host machine. However, 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 on to the eToken. Once the user logs out, all the private data in the cache is erased.■ Never: does not cache private data. |

| Field (Continued) | Description (Continued) |
|--|---|
| RSA key secondary authentication mode | <p>An authentication password may be set 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.</p> <p>This option defines the policy for using this secondary authentication of RSA keys.</p> <ul style="list-style-type: none"> ■ Always: every time an RSA key is generated, you are prompted to enter a secondary password for accessing this key. Clicking OK generates the key and uses the entered password as the secondary RSA password for that key. Clicking Cancel causes key generation to fail. ■ Always prompt user: every time an RSA key is generated, a secondary password for accessing this key is requested. 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 on application request: this enables applications that 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: secondary passwords are not created for any RSA key and the authentication method uses only the eToken password to access the key. |
| Manually set number of reserved RSA keys | Set the number of reserved RSA keys to reserve space in the token memory. This ensures that there will always be memory available for the keys. |
| Change Initialization Key | The initialization key protects against accidental initialization and requires a separate password to be entered before initialization can occur. |

10. If required, click Change Initialization Key.
The *eToken Initialization Key* dialog box opens.



11. Complete the fields as follows:

| Field | Description |
|----------------------------------|--|
| Use Default Initialization Key | Select to use factory-set default. |
| Use Specified Initialization Key | Enter the password previously configured in the This Value field below. |
| Change Initialization Key to: | <ul style="list-style-type: none"> ■ Default: Revert to default. ■ Random: If selected, it will never be possible to re-initialize the token. ■ This Value: Select and confirm a password. |

12. Click **OK** to return to the *eToken Advanced Settings* dialog box, then click **OK** again to return to the *eToken Initialization Parameters* dialog box.

13. Click **Start**.

When the initialization process is complete, a confirmation message is displayed.

Logging On as a User

To log on as a user:

1. Click **Log On to eToken** on the toolbar, or right-click the token name in the left pane and select **Log On** from the shortcut menu.
The *Log On to eToken* dialog box opens.
2. Enter the eToken user password in the *Password* field and click **OK**.
The user is logged on.

Logging On as an Administrator

An administrator has limited permissions on a token. No changes to any user information may be made, nor may 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 token.

To log on as an administrator:

1. Click **Administrator Logon** on the toolbar, or right-click the token name in the left pane and select **Administrator Logon** from the shortcut menu.
The *Administrator Logon to eToken* dialog box opens.
2. Enter the administrator password in the *Password* field and click **OK**.
The user is logged on as the Administrator.

Importing a Certificate

The following certificate types are supported:

- .pfx
- .p12
- .cer

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

In the case of a CER file (which contains only X.509 certificates), the program checks if a private key exists on the eToken. If the private key is found, 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.

To import a certificate:

1. Click **Import Certificate** on the toolbar, or right-click the token name in the left pane and select **Import Certificate** from the shortcut menu.

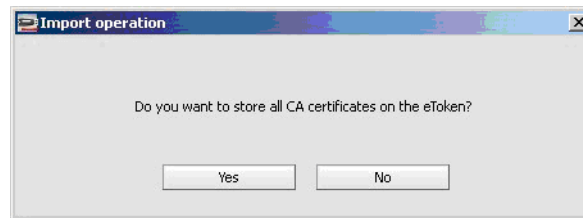
The *Import Certificate* dialog box opens.

2. Select the certificate to import and click **Open**.

If the certificate requires a password, the *Password* dialog box opens.

3. Enter the certificate password.

A dialog box opens asking if you want to store the CA certificates on the eToken.



4. Select **Yes** or **No**.

All requested certificates are imported, and a confirmation message opens.

Changing the Administrator Password

To change the Administrator password:

1. Click **Change Administrator Password** on the toolbar, or right-click the token name in the left pane and select **Change Administrator Password** from the shortcut menu.
The *Change Administrator Password* dialog box opens.
2. Enter the current administrator password in the *Current Password* field.
3. Enter the new administrator password in the *New Password* and *Retype* fields.
4. Click **OK**.
The administrator password is changed.

Setting User Password

Setting a user password to unlock an eToken can be performed only if an administrator password has been set during initialization.

A challenge-response authentication system can also be used to unlock a locked eToken.

See *Unlocking the eToken using Challenge - Response* on page 35.

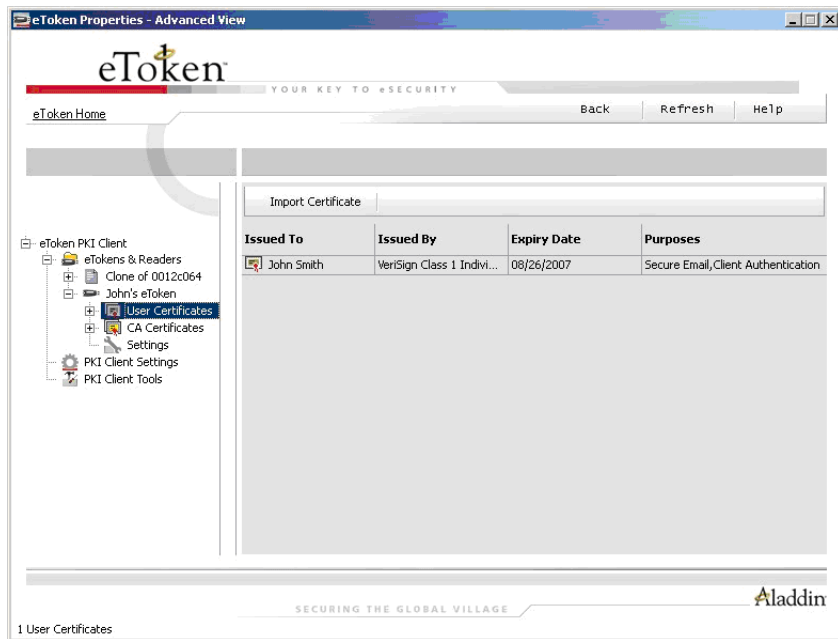
To unlock a token using Set User Password:

1. Log on to the selected token as the administrator.
See *Logging On as an Administrator* on page 48.
2. Click **Set User Password** on the toolbar, or right-click the token name in the left pane and select **Set User Password** from the shortcut menu.
The *Set eToken Password* dialog box opens.
3. Enter a new password in the *New Password* and *Confirm* fields.
4. Set the *Set Error Retry Counter* from 0 to 15.
5. Click **OK**.
The eToken is unlocked.
You can now log on as a user with the new password.

Certificates

When a token node is expanded, certificate nodes are displayed if the token contains certificates.

Click on the **User Certificates** node or the **CA Certificates** node to itemize the certificates in the right pane, or to import another certificate.



Expand the Certificates node to select individual certificates.



Select a certificate to enable the following commands:

- Delete Certificate
- Export Certificate
- Copy to Clipboard

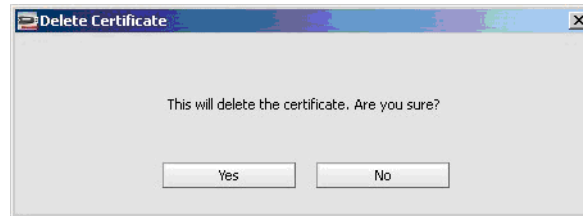
To initiate certificate activity, do one of the following:

- Select the certificate in the left pane and click the appropriate action on the toolbar
- Right-click the certificate name in the left pane and select the required action from the shortcut menu.

Deleting a Certificate

To delete a certificate:

1. Select Delete Certificate.
The *Delete Certificate* dialog box opens.



2. Click **Yes**.

Exporting a Certificate

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

To export a certificate:

1. Select Export Certificate.
The *Export Certificate* dialog box opens.
2. Select the location to store the certificate and click **OK**.

Settings

The settings node under a specific object refers to settings for that object only. There are two types of settings:

- **Password Quality:** configures password policy on the token
- **Other:** configures settings relating to cache policies and RSA secondary authentication

Password Quality

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

If the eToken was initialized in early RTE versions, no password policy is stored on the token.

The password quality parameters are:

- **Minimum password length:** default is 6 characters
- **Maximum usage period:** in days; default is 0 = none
- **Minimum usage period:** default is 0 days
- **Password expiry warning period:** defines the number of days before the password expires that a warning message is shown; default is 0 = none
- **Password history size:** defines how many old passwords should not be repeated (default is 10)
- **Password must meet complexity requirements:** defines whether mixed characters are required in the token password; default = yes

Other

These settings are:

- **Private data caching mode**
- **RSA key secondary authentication mode**

Private data caching mode

In PKI Client (Mac) 4.55, public information stored on the token is cached to enhance performance. This option defines when private information (excluding private keys on the eToken PRO / NG OTP / Smartcard) can be cached outside the eToken.

Select one of the following options:

- **Always** (fastest): always caches private information in the application memory. This enables fast performance, as certain information is cached on the host machine. However, 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 on to 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 mode

An authentication password may be set 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.

This option defines the policy for using this secondary authentication of RSA keys.

Select one of the following options:

- **Always:** every time an RSA key is generated, you are prompted to enter a secondary password for accessing this key. Clicking OK generates the key and uses the entered password as the secondary RSA password for that key. Clicking Cancel causes key generation to fail.
- **Always prompt user:** every time an RSA key is generated, a secondary password for accessing this key is requested. 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 on application request:** this enables applications that 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:** secondary passwords are not created for any RSA key and the authentication method uses only the eToken password to access the key.

PKI Client Settings

This node refers to generic eToken settings unless overridden by a change to a specific object. There are two types of settings:

- **Password Quality:** configures password policy on eTokens
- **Other:** configures settings relating to logon modes

Password Quality

These PKI Client settings share the same parameters as the settings for individual eTokens. They are used to set a global password policy for eTokens with no password quality parameters, such as those in use with versions of eToken RTE 3.65 and earlier.

The password quality parameters are:

- **Minimum password length:** default is 6 characters
- **Maximum usage period:** in days; default is 0 = none
- **Minimum usage period:** default is 0 days
- **Password expiry warning period:** defines the number of days before the password expires that a warning message is shown; default is 0 = none
- **Password history size:** defines how many old passwords should not be repeated (default is 10)
- **Password must meet complexity requirements:** defines whether mixed characters are required in the eToken password; default = yes

In addition to the above password quality parameters that may also be set per token, two global parameters are set:

- **Configurable after initialization:** defines whether the password quality parameters may be changed after initialization; default = yes
- **Configurable by Administrator (uncheck for user):** defines whether the password quality parameters may be changed after initialization by the administrator, or, if unchecked, by the user; default = yes

Note:

If the Configurable after initialization parameter is disabled, the Configurable by Administrator (uncheck for user) parameter is not relevant.

Other

- CA certificate management

| | |
|---------------------------|---|
| CA certificate management | <p>Default: enabled</p> <p>CA certificates can be downloaded onto an eToken. When the eToken is inserted into the computer, one or more of these CA certificates may not be on the computer. In such a case, the CA certificate may be loaded onto the computer.</p> |
|---------------------------|---|



Chapter 7

Apple Keychain

Apple Keychain is Apple Computer's password management system in Mac OS X. Keychain Access is a Mac OS X application that allows the user to access the Apple Keychain and configure its contents.

PKI Client 4.55 (Mac) provides a plug-in to support integration with Mac OS X Keychain Access. The plug-in is installed during eToken PKI Client Installation.

In this chapter:

- Features Supported by Keychain Access
- Displaying eToken in Keychain Access

Features Supported by Keychain Access

The eToken PKI Client Keychain Access integration supports the following features:

- SmartCard Log on.

PKI Client 4.55 (Mac) supports smart card log on.

To enable SmartCard log on with Mac OS X 10.4, refer to the following link:

<http://docs.info.apple.com/article.html?artnum=304035>

In Mac OS X 10.5 Leopard, you are not required to enable the system, as SmartCard log on is built in. However, you must run `sc_auth accept` with the relevant public key hash (see section *Smart cards and Directory Services* in the above link).

- Change of token password.

- Upload of certificates from the token to Keychain Access.
- Encryption and Decryption - By uploading certificates from a token to Keychain, they become available for applications, such as Mail, that can use the certificates to encrypt and decrypt mail messages.

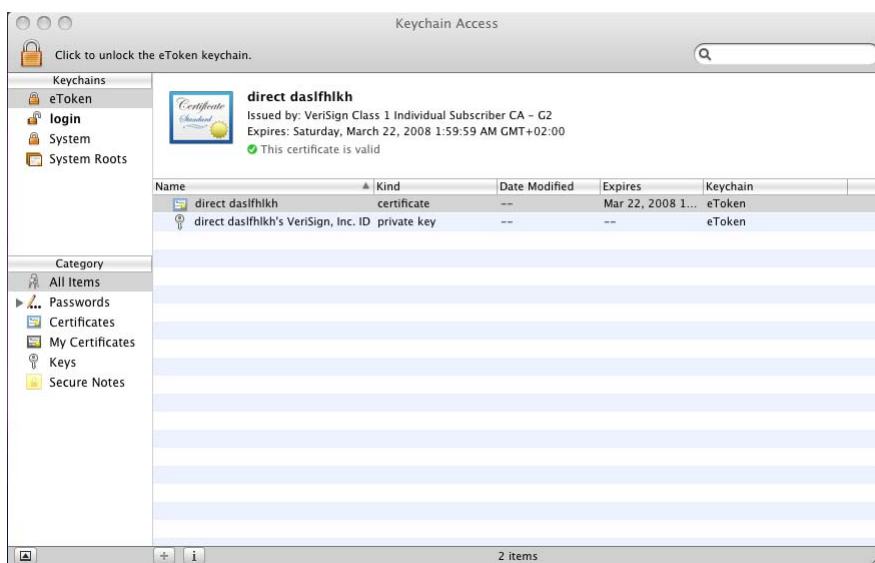
Note:

For details about limitations when working with Key Chain Access, see the *PKI Client 4.55 (Mac) ReadMe*.

Displaying eToken in Keychain Access

When you launch Keychain Access, you see a list of all the items in your Keychain, including information about each item's name, kind, creation date, and modification date.

When you insert an eToken, the device is displayed in the *Keychains* list.



To display eToken items:

- In the *Keychains* list on the left of the window, select eToken, then select an item from the *Category* list.

The details are displayed in the right section of the screen.

Tip:

For details about performing additional functions with Keychain Access, refer to Mac OS X documentation.



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 Manual 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