



## eToken PKI Client (Linux)

Administrator's Guide  
Version 5.0 Revision B



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.

Date of publication: July 2009

Last update: Sunday, July 12, 2009 2:49 pm

---

## Support

We work closely with our reseller partners to offer the best worldwide technical support services. Your reseller is the first line of support when you have questions about products and services. However, if you require additional assistance you can contact us directly at:

### Telephone

You can call our help-desk 24 hours a day, seven days a week:

*USA:* 1-800-545-6608

*International:* +1-410-931-7520

### Email

You can send a question to the technical support team at the following email address:

[support@safenet-inc.com](mailto:support@safenet-inc.com)

### Website

You can submit a question through the SafeNet Support portal:

<http://c3.safenet-inc.com/secure.asp>

## Additional Documentation

We recommend reading the following Aladdin eToken publication:

- eToken PKI Client (Linux) 5.0 Revision B User's Guide
- eToken PKI Client (Linux) 5.0 ReadMe
- eToken PKI Client (Linux) 5.0 SP1 ReadMe



## Table of Contents

<b>1. Introduction.....</b>	<b>1</b>
Overview .....	2
New Features .....	3
<b>2. System Requirements .....</b>	<b>5</b>
<b>3. Installation .....</b>	<b>7</b>
Pre-Installation .....	8
Upgrading .....	8
Pre-Installation for 32-bit Operating Systems .....	8
Pre-Installation for Ubuntu .....	9
Pre-Installation for 64-bit Operating Systems .....	9
Installing eToken PKI Client.....	10
Installing on Red Hat Enterprise, SUSE, CentOS, or Fedora .....	10
Installing on Ubuntu.....	12
Uninstalling eToken PKI Client .....	13
Uninstalling on Red Hat Enterprise, SUSE, CentOS, or Fedora.....	13
Uninstalling on Ubuntu .....	13
Loading the eToken PKCS#11 Security Module .....	13
<b>4. Configurable Settings.....</b>	<b>17</b>
Configuration Files.....	18
Configuration Files Hierarchy .....	18
eToken.conf Configuration Keys .....	19
General .....	19
CertStore .....	19
InitApp .....	20
PQ .....	21
UI .....	21
Init .....	22
eToken.common.conf Configuration Keys .....	22

---

<b>A. Copyrights and Trademarks .....</b>	<b>23</b>
<b>B. FCC Compliance.....</b>	<b>25</b>
FCC Warning .....	25
CE Compliance .....	26
UL Certification.....	26

# Introduction

---

eToken PKI Client enables eToken operations and the implementation of eToken PKI-based solutions.

---

**Note:**

This document refers to eToken PKI Client 5.0 and eToken PKI Client 5.0 SP1.

eToken PKI Client 5.0 SP1 supports only Ubuntu 8.04 (32-bit) and 9.04 (32-bit).

For details of supported platforms in eToken PKI Client 5.0 and eToken PKI Client 5.0 SP1 see *System Requirements* on page 5.

---

### In this chapter:

- Overview
- New Features

## 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 PKCS#11 or proprietary eToken applications.

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 created, stored, and used securely from within eToken hardware or software devices.

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

The eToken PKI Client Properties application and the eToken PKI Client Monitor process are installed with eToken PKI Client, providing easy-to-use configuration tools for users and administrators.



## New Features

**The following features were introduced in eToken PKI Client (Linux) 5.0:**

- Improved usability and customization options for the eToken PKI Client user interface
- Improved user interface
- Support for administrator and non-administrator privilege levels for screen access and actions performed in the eToken PKI Client user interface
- Simplified supportability by providing option logging as part of the standard shipping release
- Support for the *Clear* function in addition to the *Initialize* option (**Warning:** This feature deletes all eToken content including certificates, RSA Keys and other data)
- A logon retry counter is displayed in the eToken logon window on logon failure
- Enhanced password complexity support - manual password complexity settings and character repeat count
- Support for 64-bit Red Hat Enterprise and CentOS operating systems
- Support for 2048 RSA keys, including Java Cards using Applet 1.1 or later
- Support for the new eToken Virtual
- Support for eToken Pro Anywhere (in PKI mode only)

**The following features were introduced in eToken PKI Client (Linux) 5.0 SP1:**

- Support for Ubuntu 9.04 (32-bit)
- Support for SSH Agent



## Chapter 2

# System Requirements

---

Supported Operating Systems (eToken PKI Client (Linux) 5.0 GA)	Red Hat Enterprise 5.2 (32-bit and 64-bit)
	CentOS 5.2 (32-bit and 64-bit)
	SUSE Linux Enterprise 10.3 (32-bit)
	Fedora 9 (32-bit)
Supported Operating Systems (eToken PKI Client (Linux) 5.0 SP1)	Ubuntu 8.04 (32-bit) and 9.04 (32-bit)
Supported Browser	Firefox 3.0.1
Supported Mail Client	Thunderbird 2.0
Supported eToken Devices - Both Siemens CardOS and Java Card-based	eToken PRO
	eToken NG-OTP
	eToken NG-FLASH
	eToken PRO Smartcard
	eToken PRO Anywhere
Required Hardware	USB port (for physical eToken devices)
Recommended Screen Resolution	1024 x 768 pixels or higher (for eToken PKI Client Properties)



## Chapter 3

# Installation

---

This chapter describes the installation options for eToken PKI Client.

**In this chapter:**

- Pre-Installation
- Installing eToken PKI Client
- Uninstalling eToken PKI Client
- Loading the eToken PKCS#11 Security Module

---

## Pre-Installation

### Upgrading

If an earlier version of eToken PKI Client is installed, uninstall it before installing eToken PKI Client.

### Pre-Installation for 32-bit Operating Systems

The built-in PCSC-Lite service for 32-bit operating systems must be installed before running the eToken PKI Client installation.

The following table lists the built-in PCSC-Lite service versions for 32-bit operating systems.

Operating System	Required PCSC-Lite Service Version
CentOS 5.2 32-bit	pcsc-lite 1.4.4-0.1.el5.i386
Red Hat Enterprise 5.2 32-bit	pcsc-lite-1.4.4-0.1.el5.i386
SUSE Linux Enterprise 10.3	pcsc-lite-1.4.3-16.i586
Fedora 9	pcsc-lite-1.4.4-3.fc9
Ubuntu 8.04 and 9.04	pcsc-lite - 1.4.99 pcsc-lite - 1.4.102 is required to support the SSH Agent. If SSH Agent support is required in Ubuntu 8.04 then pcsc-lite - 1.4.102 must be installed (it is already included in the installation of Ubuntu 9.04).

---

#### Note:

The PKI driver requires the PCSC-Lite service to be compiled and installed with `libusb` support. Ensure that `pcscd` is compiled with `libusb` support, and not with `libhal` support.

---

## Pre-Installation for Ubuntu

Before installing eToken PKI Client on Ubuntu:

- Ensure that you have Super User permissions.
- Ensure that the following QT library components are installed:
  - ◆ `libqt4-core` version 4.2.3
  - ◆ `libqt4-gui` version 4.2.3
- If the built-in PCSC-Lite service is compiled with `libhal` support, uninstall the service, and install it with `libusb` support.

---

### Note:

The PKI driver requires the PCSC-Lite service to be compiled and installed with `libusb` support.

---

## Pre-Installation for 64-bit Operating Systems

The built-in PCSC-Lite service for 64-bit operating systems is not appropriate for eToken PKI Client. Before installing eToken PKI Client, the built-in PCSC-Lite service must be uninstalled, and PCSC-Lite 1.4.102 or later must be installed.

## Getting the PCSC-Lite Packages

The PCSC-Lite packages can be downloaded from the following website:

<http://pcsc-lite.alioth.debian.org/>

The following is an example for building the PCSC-Lite package:

```
./configure --prefix=/usr --localstatedir=/var --
sysconfdir=/etc --enable-
usbdropdir=/usr/lib64/pcsc/drivers \LDFLAGS="-m32"
PTHREAD_CFLAGS="-pthread" PTHREAD_LIBS="-lpthread"
CFLAGS="-m32" --enable-daemon \--disable-libhal --enable-
libusb
```

Alternatively, any published RPM package compiled with `libusb` support can be used.

The `pcsc-lite` and the `pcsc-lite-libs (i386, x64)` packages are required. For development, the `pcsc-lite-devel` package is also required.

## Replacing PCSC-Lite

Remove the unsupported version of PCSC-Lite, and install a supported version.

**To replace the 64-bit version of PCSC-Lite with the appropriate version:**

1. Uninstall PCSC-Lite:
  - ◆ `yum remove pcsc-lite pcsc-lite-devel.i386 pcsc-lite-devel.x86_64 pcsc-lite-libs.i386 pcsc-lite-libs.x86_64`
2. Install the RPM packages:
  - ◆ `rpm -ivh <name>-pcsc-lite-1.4.102-1.x86_64.rpm <name>-pcsc-lite-libs-1.4.102-1.i386.rpm <name>-pcsc-lite-libs-1.4.102-1.x86_64.rpm`  
     where `<name>` is the prefix of your PSCS-Lite filename
3. Start `pcscd`:
  - ◆ `/etc/init.d/pcscd start`

## Installing eToken PKI Client

### Installing on Red Hat Enterprise, SUSE, CentOS, or Fedora

The installation package for eToken PKI Client running on RedHat, SUSE, CentOS, or Fedora is the RPM Package Manager. RPM is a command line package management system that can install, uninstall, and update software packages.

The eToken PKI Client RPM packages:

- RPM Package Name:  
`pkiclient-5.00.nn-0.i386.rpm`
- RPM Installation Script Name:  
`signed-install_pkiclient-5.00.nn-0.i386.rpm.sh`



where `nn` is the build number

**To install with authentication on RedHat, SUSE, or CentOS:**

1. On the terminal, log on as a root user.
2. Run the following:  

```
rpm --import RPM-GPG-KEY-pkiclient
```
3. Run one of the following:
  - ◆ On a 32-bit OS:  

```
rpm -hi pkiclient-5.00.nn-0.i386.rpm
```
  - ◆ On a 64-bit OS:  

```
rpm -hi pkiclient-5.00.nn-0.x86_64.rpm
```

where:

- ◆ `-hi` is the parameter for installation
- ◆ `nn` is the build number

**To install with a script on RedHat, SUSE, or CentOS:**

1. Log on as a root user.
2. Run one of the following installation scripts:
  - ◆ On a 32-bit OS:  

```
./signed-install_pkiclient-5.00.nn-0.i386.rpm.sh
```
  - ◆ On a 64-bit OS:  

```
./signed-install_pkiclient-5.00.nn-0.x86_64.rpm.sh
```

---

**Note:**

When installing with a script, ensure that the following are all in the same folder:

- the key
  - the script
  - the RPM package
- 

**To install on Fedora:**

1. Log on as a non-root user.
2. Double-click the RPM file:  

```
pkiclient-5.00.nn-0.i386.rpm
```

where `nn` is the build number.

A root password prompt appears.

3. Enter the root password.

## Installing on Ubuntu

The installation packaging for eToken PKI Client running on Ubuntu is the Debian software package (.deb).

The following is the eToken PKI Client deb package:

- .deb Package Name:  
pkiclient-5.00.nn-0\_i386.deb  
where nn is the build number

### To install from the package installer:

1. Double-click the required .deb file.  
The package installer opens.
2. Click **Install Package**.  
A password prompt appears.
3. Enter the Super User or root password.  
The installation process runs.
4. To run the eToken PKI Client Quick Menu, go to **Applications > eToken > Start eToken PKI Client**.

### To install from the terminal:

1. Enter the following:  

```
sudo dpkg -i pkiclient-5.00.nn-0_i386.deb
```

  
where nn is the build number.  
A password prompt appears.
2. Enter the password.  
The installation process runs.
3. If the installation fails due to a lack of dependencies, enter the following:  

```
sudo apt-get install -f
```

  
The dependencies are installed and the installation continues.
4. The message *Please run PKI Monitor* is displayed.

5. To run the eToken PKI Client Quick Menu, go to **Applications > eToken > Start eToken PKI Client**.

## Uninstalling eToken PKI Client

When eToken PKI Client is uninstalled, user configuration and policy files are deleted. For information regarding the files, see Chapter 4 *Configurable Settings* on page 17.

## Uninstalling on Red Hat Enterprise, SUSE, CentOS, or Fedora

**To uninstall:**

- Enter the following:  

```
rpm -e pkiclient
```

where `-e` is the parameter for uninstall

## Uninstalling on Ubuntu

**To uninstall:**

- In the console, enter the following:  

```
sudo dpkg -r pkiclient
```

where `-r` is the parameter for uninstall

## Loading the eToken PKCS#11 Security Module

To run eToken PKI Client, the eToken PKCS#11 security module (`libeTPkcs11.so`) must be loaded.

When working with Firefox, the eToken PKCS#11 security module may have been loaded automatically during the eToken PKI Client installation.

When working with Thunderbird, load the eToken PKCS#11 security module manually.

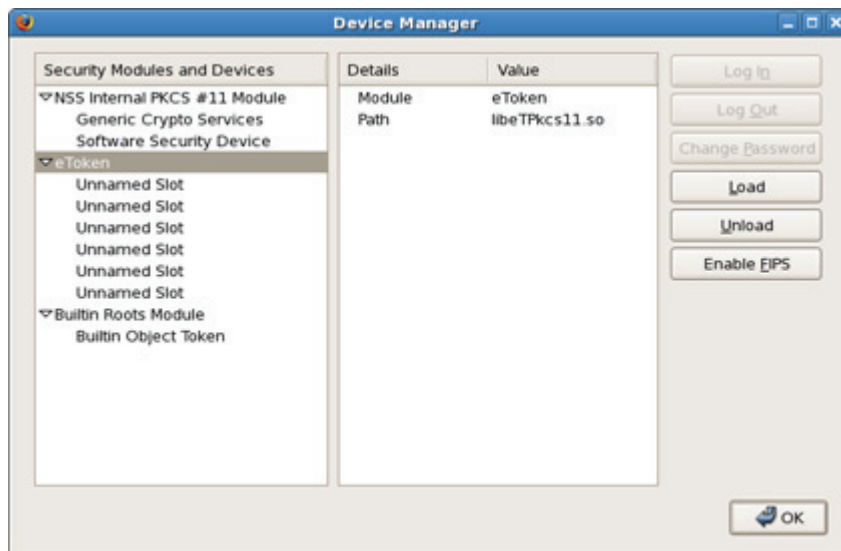
**Note:**

Ensure that there is only one loaded security module having a path with the value **libeTPkcs11.so**.

To ensure that the eToken PKCS#11 module is loaded:

1. Do one of the following:
  - ◆ When working with Firefox, go to **Edit > Preferences > Advanced > Encryption > Security Devices**.
  - ◆ When working with Thunderbird, go to **Edit > Preferences > Advanced > Certificates > Security Devices**.

The *Device Manager* dialog box opens.



2. If **eToken** is listed in the *Security Modules and Devices* column, click **OK** to exit the *Device Manager*.
3. If **eToken** is not listed in the *Security Modules and Devices* column, click **Load**.

The *Load PKCS#11 Device* dialog box opens.



4. Do the following:
  - ◆ Replace the contents of the *Module Name* field with **eToken**.
  - ◆ In the *Module filename* field, enter the following:  
**/usr/lib/libeTPkcs11.so**

---

**Note:**

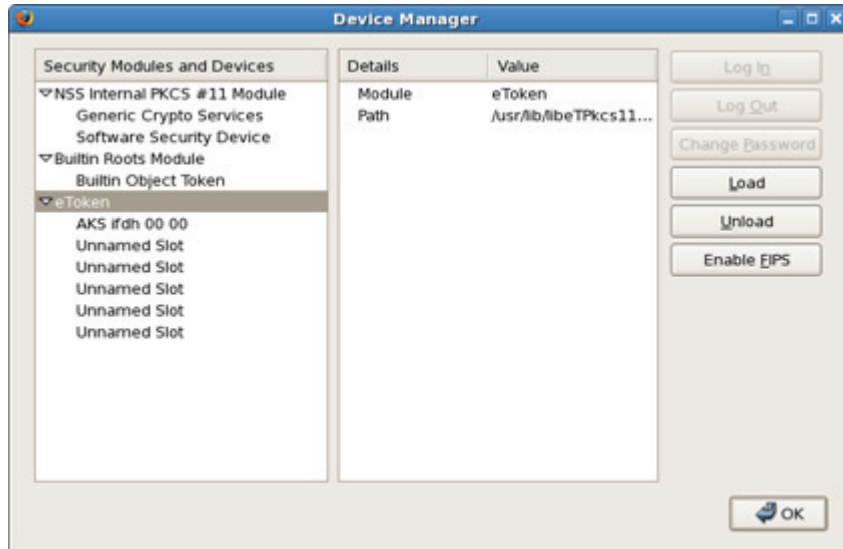
The *Module* fields are case sensitive.

---



5. Click **OK**.  
The *Confirm* dialog box opens.
6. Click **OK**.  
The *Alert* dialog box opens.
7. Click **OK**.

**eToken** is listed in the *Security Modules and Devices* column of the *Device Manager* dialog box.



8. Click **OK** to exit the *Device Manager*.

## 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

eToken PKI Client installs two configuration files:

- `eToken.conf`: requires administrator permissions
- `eToken.common.conf`: does not require administrator permissions

**Note:**  
`eToken.common.conf` contains settings for eToken Virtual use only.

## Configuration Files Hierarchy

To enable hierarchical priorities, up to three different versions of the `eToken.conf` configuration file can be created. For each key, the setting found in the file with highest priority determines the application’s behavior.

This design simulates the eToken PKI Client (Windows) registry logic.

Windows Registry	Linux Installer	Linux File Name	Priority	File Permissions
LM/Policies	Not provided	/etc/eToken.policy.conf	1(High)	Root
CU	Automatically created by GUI	~/.eToken.conf (located in user's home directory)	2	User
LM	Provided	/etc/eToken.conf	3	Root
LM	Provided	/etc/eToken.common.conf for eToken Virtual connections		All

**Note:**  
`/etc/eToken.policy.conf` can be created manually by the system administrator.



## eToken.conf Configuration Keys

`eToken.conf` contains all keys not relating to eToken Virtual. All eToken Virtual keys are located in `eToken.common.conf`.

### General

Key Name	Description	DWord Value	Default
PcscSlots	Number of PC/SC slots	1-16	4 <b>Note:</b> to use more than 4 slots concurrently, enter the required number
SoftwareSlots	Number of software slots	1-10	2

### 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 is displayed on the desktop 0 = not displayed 1 = displayed 2= displayed when token is inserted (does not disappear when token is disconnected)	0/1/2	1

## PQ

Key Name	Description	DWord Value	Default
pqModifiable	Password quality can be changed after initialization 0 = cannot be changed 1 = can be changed	0/1	1
pqHistorySize	Number of recent passwords that cannot be repeated	>=0	10
pqMaxAge	Total number of days a password is valid 0 = no expiration	>=0	0
pqMinAge	Total number of days required before a password 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 (supports English only)	EN	EN
linguist	Path to Linguist application		

## Init

Key Name	Description	DWord Value	Default
RSASecondaryAuthenticationMode	Can be configured in eToken Properties.		
PrivateDataCaching	Can be configured in eToken Properties.		
RSA-2048	Can be configured in eToken Properties.		
HMAC-SHA1	Can be configured in eToken Properties.		

## 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		

# 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