SafeNet Authentication Client (Mac)

Version 8.1 Revision A

Administrator's Guide

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

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 SafeNet Token publication:

- SafeNet Authentication Client (Mac) 8.1 User's Guide
- SafeNet Authentication Client (Mac) 8.1 ReadMe

Table of Contents

Chapter 1

Introduction

SafeNet Authentication Client enables Token operations and the implementation of Token based PKI solutions.

In this chapter:

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.

SafeNet's Authentication Client enables integration with various security applications. It enables token security applications and third party applications to communicate with the token. These include PKI solutions using PKCS#11 or proprietary token applications.

SafeNet Authentication 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 token hardware or software devices.

SafeNet Authentication Client can be deployed and updated using any standard software distribution system.

The SafeNet Authentication Client Tools application is installed by the SafeNet Authentication Client, providing easy-to-use configuration tools for users and administrators.

New Features

The following feature was introduced in SafeNet Authentication Client 8.1 (for Mac):

- Support for OS x10.7 (Lion)
- Resume functionality for SAC Tools supported on Lion
- Firefox version 4, 5, and 6 (32 and 64 bit mode) supported
- Support for Centrify integration for Smartcard logon on MAC OS X in an Active Directory Environment

Chapter 2

System Requirements

Supported Operating System	Mac OS X 10.6 (Snow Leopard) - Intel 32-bit and Intel 64-bit Mac OS X 10.7 (Lion) - Intel 64-bit
Supported eToken Authenticators	eToken PRO
	eToken NG-OTP
	eToken NG-FLASH 4.5 and eToken NG-FLASH 5.3
	eToken NG-FLASH Anywhere (PKI mode only)
	eToken PRO Smartcard
	eToken PRO Anywhere (PKI mode only)
	SafeNet eToken Virtual
Required Hardware	USB port (for physical Token devices)
Recommended Screen Resolution	1024 x 768 pixels or higher (for SafeNet Authentication Client Tools)

PCSC-Lite

SafeNet Authentication Client 8.1 uses the default PCSC-Lite that is installed with Mac OS X. SafeNet Authentication Client 8.1 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.

The SafeNet Authentication Client 8.1 installation runs PCSC after reboot even if a token device is not inserted. This is required to support SafeNet eToken Virtual on a flash device.

Chapter 3

Installation

In this chapter:

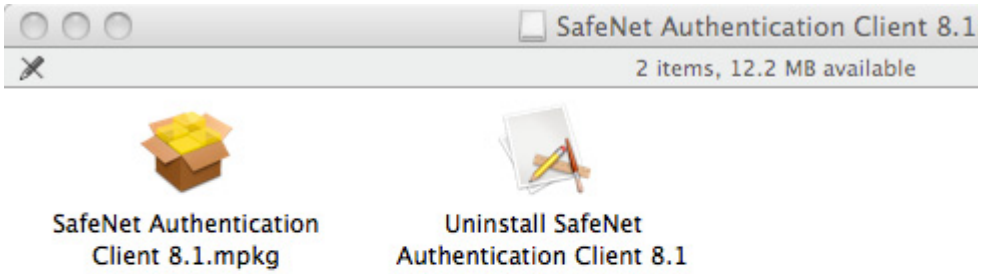
Installing with the Installer

The installation packaging for SafeNet Authentication Client 8.1 (Mac) is PackageMaker.

The installation package is ***SafeNetAuthenticationClient.8.1.0.x.dmg***.

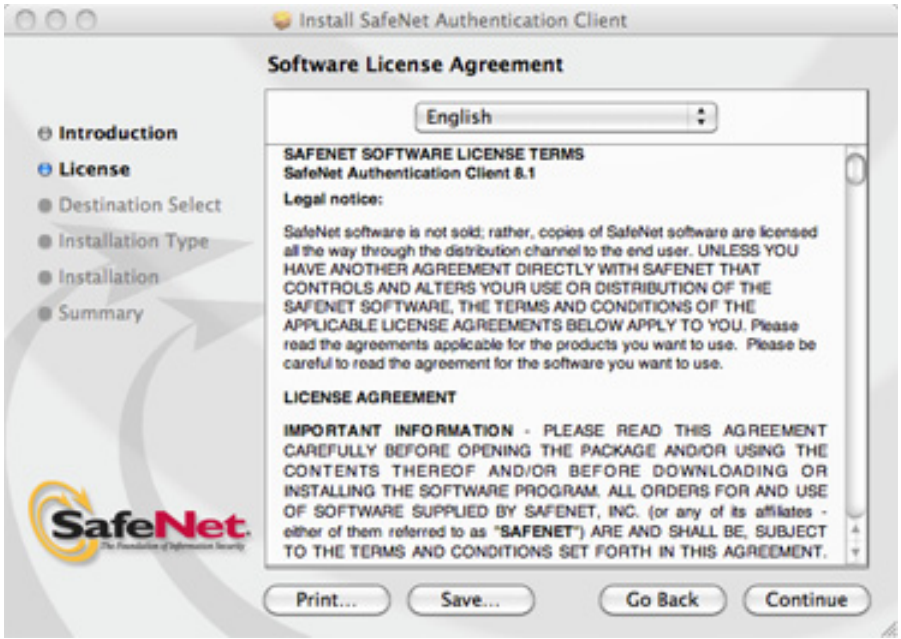
To install with the installer:

1. Double click the ***SafeNetAuthenticationClient.8.1.0.x.dmg*** file.
   A new disk image file is created in the Finder window, including an mpkg installation file and an uninstall application.



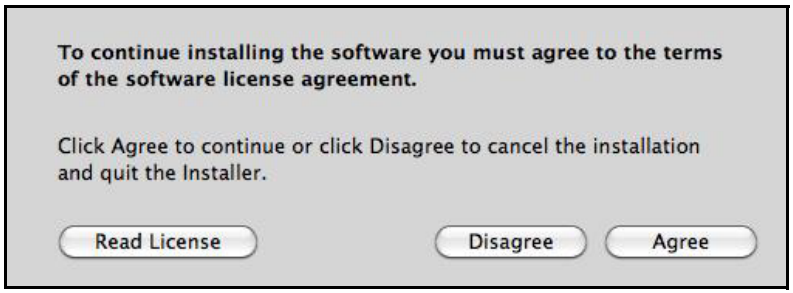
2. To start the installation, double click **SafeNet Authentication Client 8.1.mpkg**.
   The *Welcome to the SafeNet Authentication Client Installer* window opens.

3. Click **Continue**.
   The *Software License Agreement* window opens.

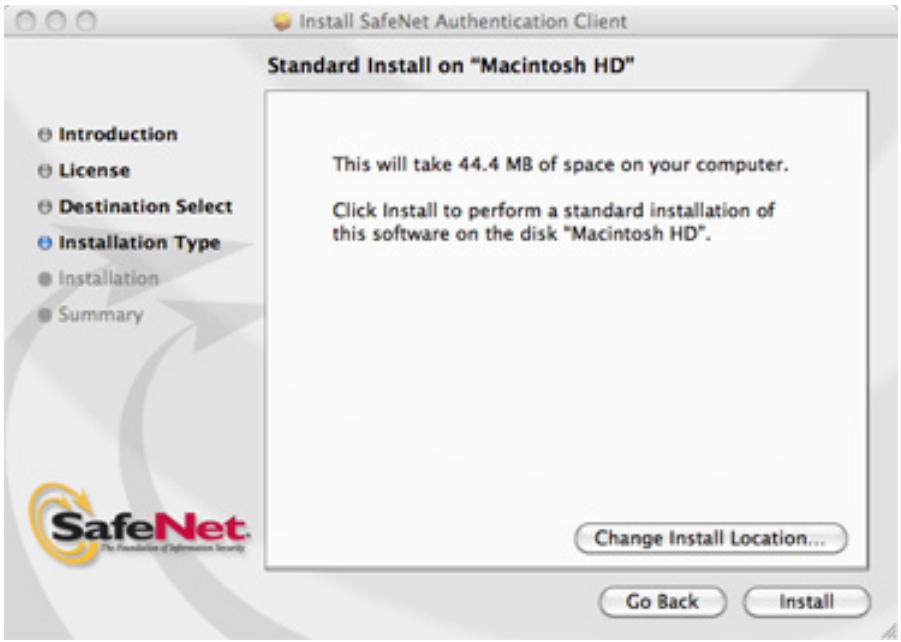


4. Click **Continue**.

The agreement window opens.



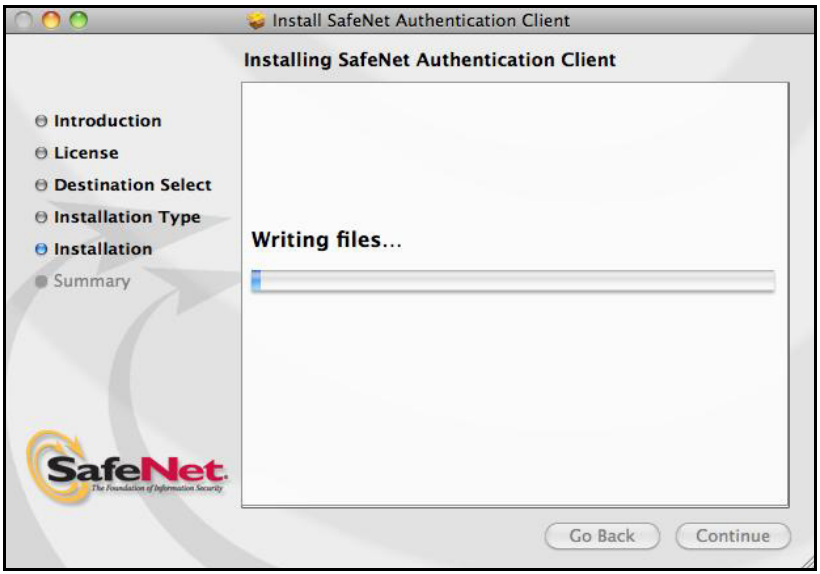
5. Click **Agree** to accept the software license agreement.
The *Standard Install on "OS-X"* window opens.



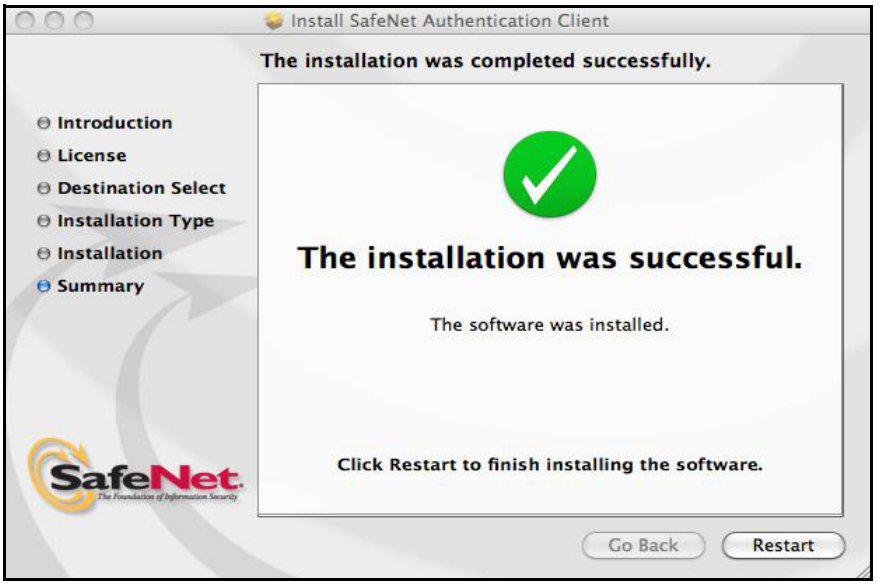
6. Click **Install**.
The *Authenticate* window opens.

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

Note:
You require Administrator permissions to install SafeNet Authentication Client.



SafeNet Authentication Client installs. The *Installation completed successfully* screen opens.



8. Click **Restart**.
   Mac OS X restarts.
9. Log in again to Mac OS X.

Installing from the Terminal

To install from the terminal:

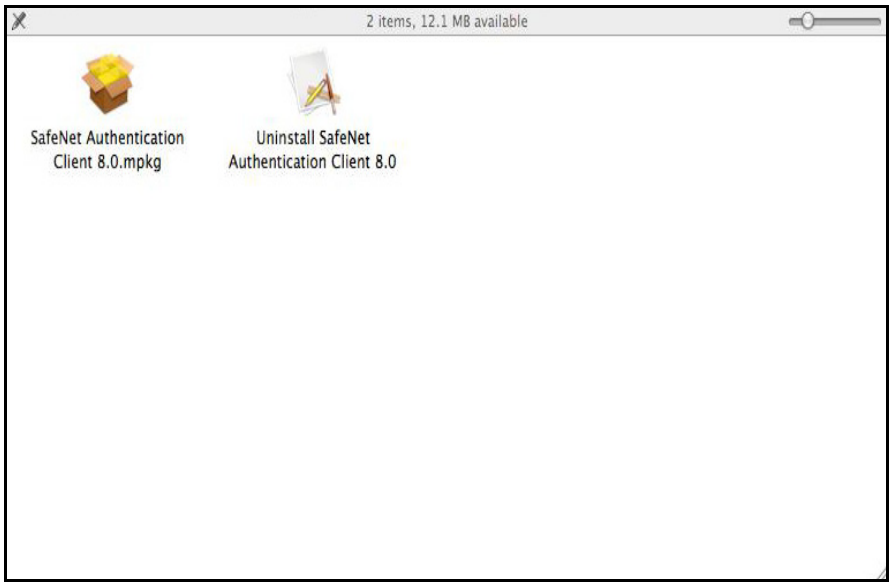
1. Extract the *SafeNet Authentication Client 8.1.mpkg* file from the dmg file.
2. At the location in the terminal in which you extracted the file run
   `sudo installer -pkg ./SafeNet\Authentication\Client\ 8.1.mpkg/ -target /`
3. Enter your root password when prompted.
   SafeNet Authentication Client 8.1 is installed.
4. Following installation, restart Mac OS X.

Uninstalling SafeNet Authentication Client 8.1

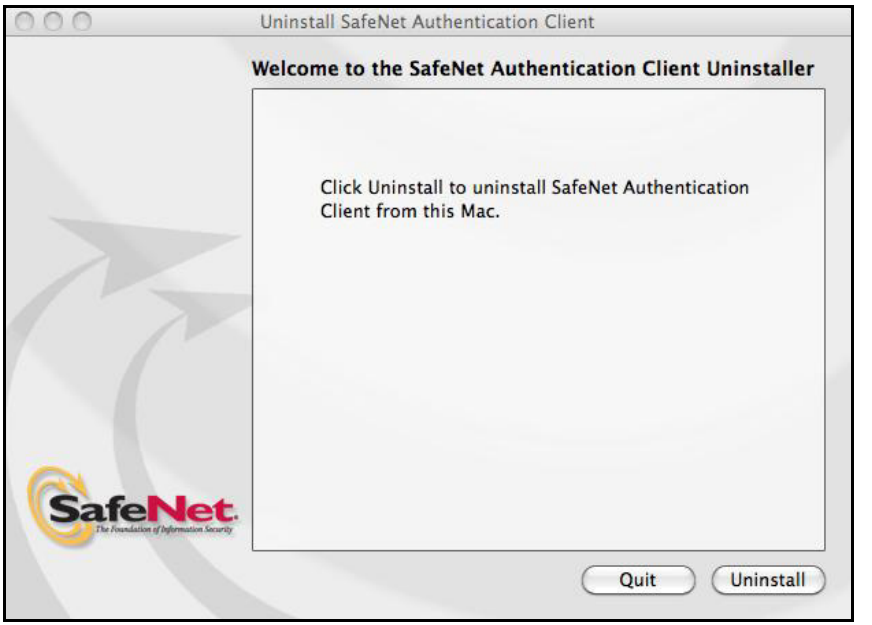
Note:
Before uninstalling SafeNet Authentication Client 8.1, make sure that SafeNet Authentication Client Tools is closed.

To uninstall SafeNet Authentication Client 8.1

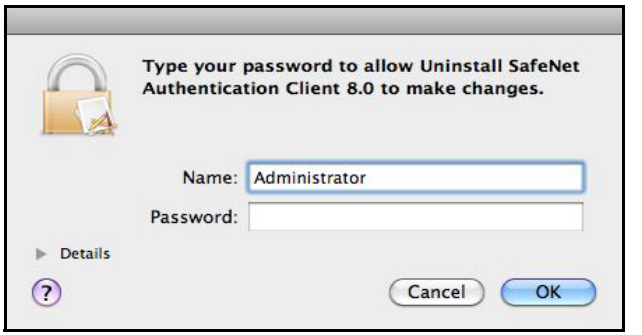
1. Double click *SafeNetAuthenticationClient.8.1.0.x.dmg* file.
   A new disk image file is created in the Finder window, including an mpkg installation file and an uninstall application.



2. Click **Uninstall SafeNet Authentication Client 8.1**.
   The *Welcome to the SafeNet Authentication Client Uninstaller* window opens.



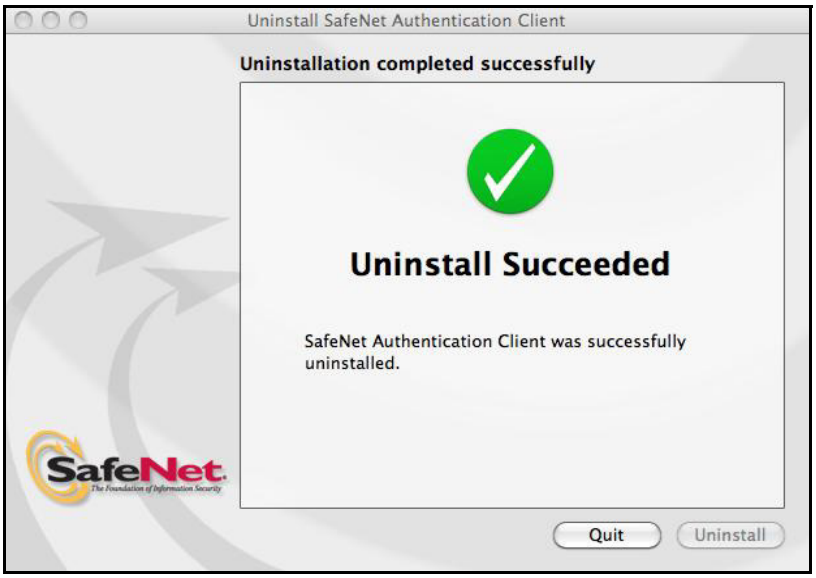
3. Click **Uninstall**.
   The *Authenticate* window opens.



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

Note:
You require Administrator permissions to uninstall SafeNet Authentication Client.

SafeNet Authentication Client uninstalls and the *Uninstallation completed successfully* screen opens.



5. Click **Quit**.

Installing the Firefox Security Module

When SafeNet Authentication Client is installed, it does not install the security module in Firefox. This must be done manually.

To install the security module in Firefox:

1. From the *Firefox* menu, select **Preferences > Advanced**.
2. On the *Encryption* tab click **Security Devices**.
   The *Device Manager* window opens.
3. Click **Load**.
   The *Load PKCS#11 Device* window opens.
4. In the *Module Filename* field enter the following string:
   `/usr/local/lib/libeTPkcs11.dylib`
   The *Confirm* window opens.
5. Click **OK**.
   The new security module is installed.

Chapter 4

Configurable Settings

This chapter provides administrator guidelines for setting configuration keys.

In this chapter:

Configuration Files

SafeNet Authentication Client installs two configuration files:

- `/etc/eToken.conf`
  Requires administrator permissions `(-rw-rw-r--)`
- `/etc/eToken.common.conf`
  Does not require administrator permissions `(-rw-rw-rw-)`

Owner: root\admin

Note:
`eToken.common.conf` contains settings for SafeNet 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 SafeNet Authentication Client (Windows) registry logic.

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

Automatic Save of Configuration Files

When SafeNet Authentication Client 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

All keys that are not related to SafeNet eToken Virtual are located in **`/etc/eToken.conf`**.

All SafeNet eToken Virtual keys are located in **`/etc/eToken.common.conf`**.

General

Key Name	Description	Value	Default
PcscSlots	Number of PC/SC slots	1-16	3
SoftwareSlots	Number of software slots	1-10	2

Note:
In Mac OS, the number of slots is determined by the **`PcscSlots`** and **`SoftwareSlots`** configuration keys described here. The *Reader Settings* window in Tools displays the number of slots that have been configured, but does not allow the user to change the settings.

CertStore

Key Name	Description	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	Value	Default
FIPS	FIPS Support 0 = disabled 1= enabled	0/1	0
AdvancedView	*Advanced* button in Tools 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	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	Value	Default
LanguageId	UI Language (supports English only)	EN	EN
linguist	Path to Linguist application		

Init

Key Name	Description	Value	Default
RSASecondaryAuthenicationMode	Can be configured in SafeNet Authentication Client Tools.		
PrivateDataCaching	Can be configured in SafeNet Authentication Client Tools.		
RSA-2048	Can be configured in SafeNet Authentication Client Tools.		
HMAC-SHA1	Can be configured in SafeNet Authentication Client Tools.		

eToken.common.conf Configuration Keys

eToken.common.conf contains SafeNet eToken Virtual keys.

Key Name	Description	Value	Default
FileName(slot0)	File name with full path		

Chapter 5

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.

SafeNet Authentication Client provides a plug-in to support integration with Mac OS X Keychain Access. The plug-in is installed during SafeNet Authentication Client installation.

In this chapter:

Features Supported by Keychain Access

The SafeNet Authentication Client Keychain Access integration supports the following features:

- SmartCard Logon. To enable SmartCard log on with Mac OS X refer to the following link:

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

  In Mac OS X 10.6, 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).
- 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.

Keychain Access Limitations

The following limitations apply when working with Keychain Access and SafeNet tokens.

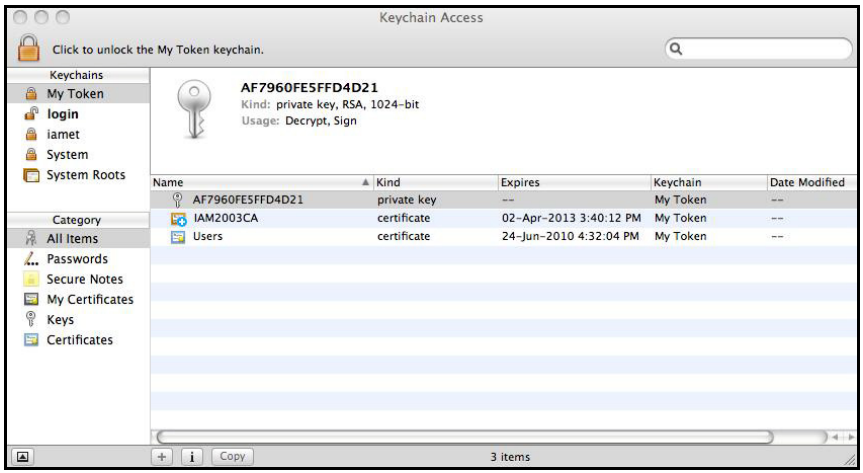
- Keychain cannot be used to create new certificates. It can only upload certificates already located on the token.
- Change token password is not supported (however, it can be changed using SafeNet Authentication Client).
- The following functions are not enabled (These are known Mac issues when using Keychain Access and Smartcards):
  - Keychain settings
  - Change Keychain password
  - New secure note
  - Delete Keychain
  - Unlock Keychain -This option is disabled in the File menu but works by clicking the lock icon.
- It is not possible to import a certificate from a file to a token (however, certificates can be imported using Tools).
- The Keychain does not support RSA key generation from a token.

- Smart card logon requires the user to enter the PIN 3 times to login. This is a known issue with Snow Leopard. Refer to http://smartcardservices.macosforge.org/trac/ticket/17.

Displaying Token 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 a token, the device is displayed in the *Keychains* list.



To display token contents:

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

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

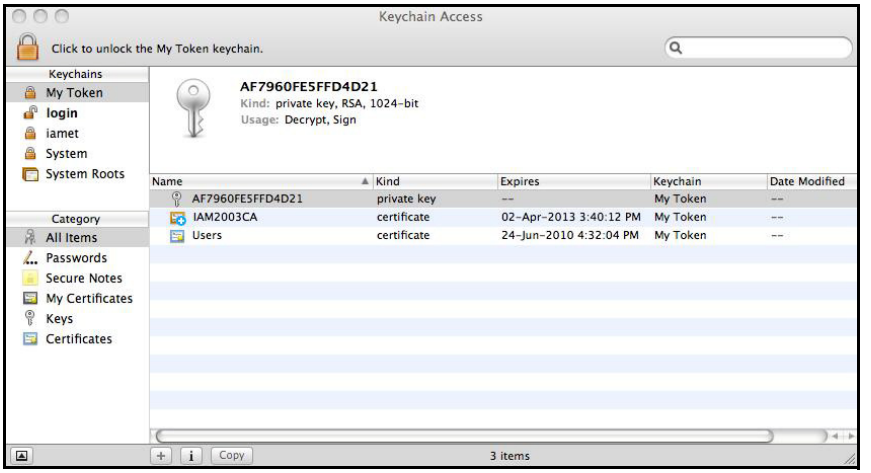
Tip:
For details about performing additional functions with Keychain Access, refer to Mac OS X documentation.

Configuring Mac Keychain to Work with SSL and Secure Mail (S/MIME)

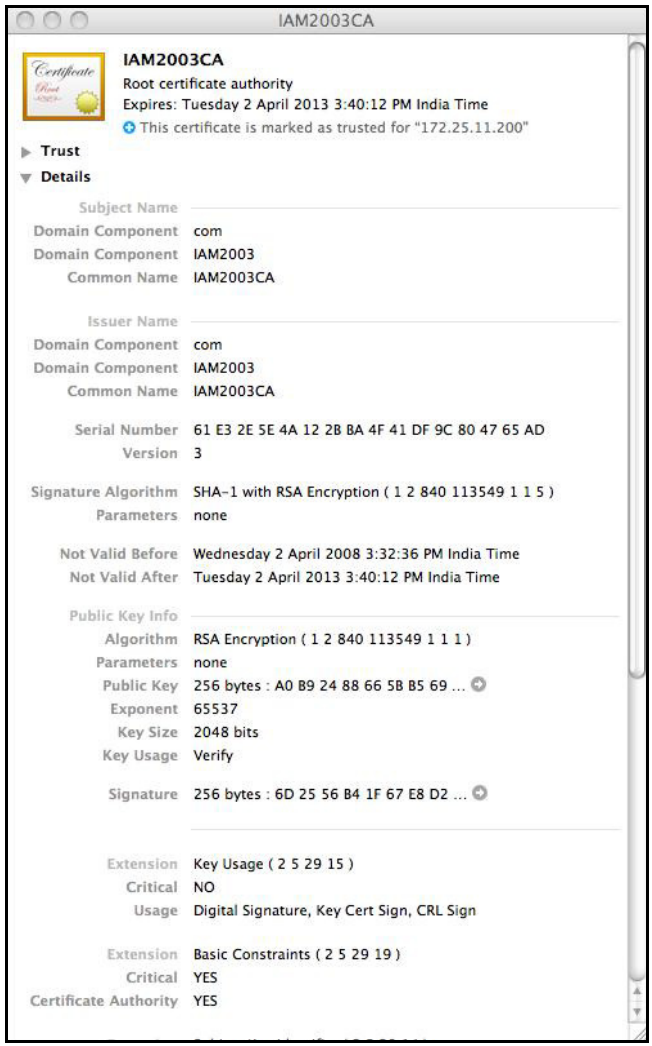
Mac Keychain must be configured to enable Safari to work with an SSL Connection and to enable encryption and decryption of emails.

To enable Mac Keychain to work with SSL and Secure Mail (S/MIME):

1. Open the *Keychain Access* window.



2. Double click on the root CA.
   The window with the certificate details opens.

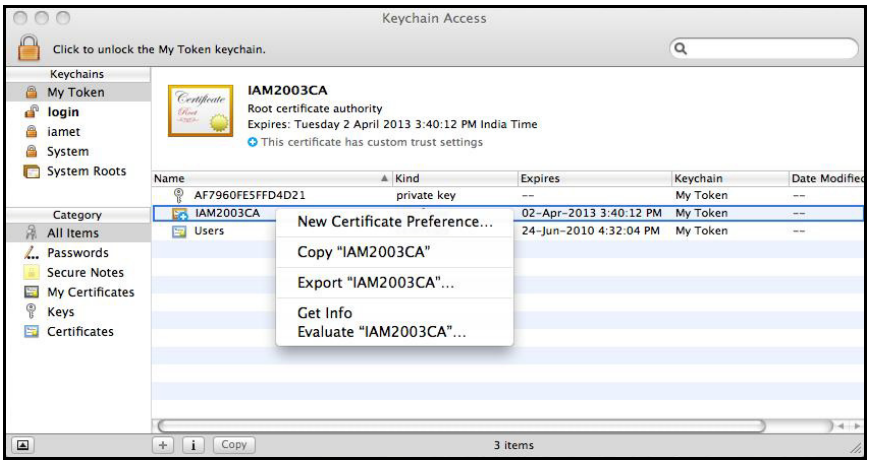


3. Click on **Trust** to expand the section.
4. Set **Secure Socket Layer (SSL)** and/or **Secure Mail (S/MIME)** to *Always Trust*
5. Close the window.

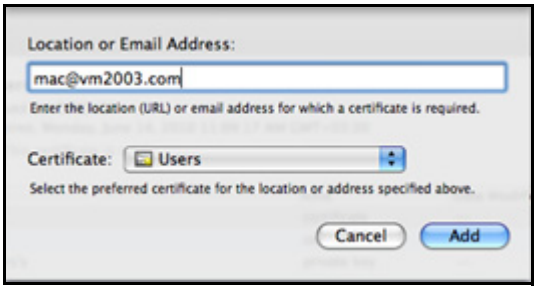
   You are returned to the Keychain Access window.

   The root CA certificate is now trusted for SSL and S/MIME operations.

6. Right click on the Users Certificate and select **New Certificate Preferences**.



The *Location or Email Address* window opens.



7. In the Certificate field, select the required certificate.
8. Do one of the following and click **Add**:
   - For S/MIME, enter the email address of your mail account
   - For SSL, enter the URL of your secured site.

The item is added to the *login* Keychain.

Note:
You must configure SSL for each required secured website.

If you configured Secure email (S/MIME), you will now be prompted to enter the token password when signing and sending an email or when decrypting an encrypted email.

If you configured SSL for your secured sites, when logging on with Safari you will be prompted for the token password.