Product Description

SafeSign Identity Client Standard

Version 3.0.45 for MAC OS X 10.6

A.E.T. Europe B.V.

IJsselburcht 3

NL - 6825 BS Arnhem

The Netherlands

Warning Notice

All information herein is either public information or is the property of and owned solely by A.E.T. Europe B.V. who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

This information is subject to change as A.E.T. Europe B.V. reserves the right, without notice, to make changes to its products, as progress in engineering or manufacturing methods or circumstances warrant.

Installation and use of A.E.T. Europe B.V. products are subject to your acceptance of the terms and conditions set out in the license Agreement which accompanies each product. Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/ or industrial property rights of or concerning any of A.E.T. Europe B.V. information.

Cryptographic products are subject to export and import restrictions. You are required to obtain the appropriate government licenses prior to shipping this Product.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, A.E.T. Europe B.V. makes no warranty as to the value or accuracy of information contained herein. The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, A.E.T. Europe B.V. reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

A.E.T. EUROPE B.V. HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH REGARD TO THE INFORMATION CONTAINED HEREIN, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL A.E.T. EUROPE B.V. BE LIABLE, WHETHER IN CONTRACT, TORT OR OTHERWISE, FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER INCLUDING BUT NOT LIMITED TO DAMAGES RESULTING FROM LOSS OF USE, DATA, PROFITS, REVENUES, OR CUSTOMERS, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION CONTAINED IN THIS DOCUMENT.

Credit information:

This product includes cryptographic software written by Eric A. Young (eay@cryptsoft.com)

This product includes software written by Tim J. Hudson (tjh@cryptsoft.com).

Contact Information: A.E.T. Europe B.V.

IJsselburcht 3
NL-6825 BS
P.O. Box 5486
NL-6802 EL Arnhem
The Netherlands
Tel. +31-26-365 33 50
Tel. Support +31-26-365 35 43
Fax +31-26-365 33 51

info@aeteurope.nl / support@aeteurope.nl
http://www.aeteurope.com/

SafeSign Identity Client is a product developed by A.E.T. Europe B.V.

Document Information

Filename: **Product Description**
SafeSign Identity Client Standard

Document ID: **SafeSign-IC-Standard_3.0.45_MACOSX_Product_Description**

Project Information: **SafeSign Identity Client Release Documentation**

Document revision history

Version	Date	Author	Changes
1.0	14-11-2011	Drs. C.M. van Houten	First edition for SafeSign Identity Client Standard Version 3.0.45 for MAC OS X

WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE

Table of contents

List of Figures

About the Document

This product description defines the features and supported configurations of SafeSign Identity Client Standard for MAC OS X and that were tested by its developer A.E.T. Europe B.V. and describes its installation process.

1 Introduction

SafeSign Identity Client for MAC OS X is a software package to enhance the security of applications that support PKCS #11 by hardware tokens, i.e. smart cards, USB tokens or SIM cards.

The SafeSign Identity Client package provides the SafeSign Identity Client PKCS #11 library for MAC OS X that allows the user to generate and store public and private data on a personal token.

2 SafeSign Identity Client for MAC OS X Functionality

SafeSign Identity Client for MAC OS X includes all functionality necessary to use hardware tokens in a variety of Public Key Infrastructures (PKIs). This includes:

PKCS #11 for integration with applications supporting PKCS #11, including Mozilla Firefox and Adobe Reader.
PKCS #12 support.
PKCS #15 support.
Product Description with installation instructions for end users (no developer documentation). All documentation is in the English language.
PKG package for installation on the MAC OS X platform.
Token Administration Utility to change PIN, etc.

3 Features

In principle, SafeSign Identity Client Standard Version 3.0.45 for MAC OS X 10.6 supports all the features of SafeSign Identity Client version 3.0.45 for Windows, if such functionality is available for the MAX OS X 10.6 platform.

3.1 Multi-token support

SafeSign Identity Client version 3.0.45 for MAC OS X 10.6 supports multiple tokens.

Refer to the list of tested configurations which (USB) tokens and readers have been tested (paragraph 4.3).

4 Tested Configurations

SafeSign Identity Client Standard version 3.0.45 for MAC OS X 10.6 was tested with the smart cards, USB tokens, smart card readers, applications and Macintosh environments listed below.

Note that though SafeSign Identity Client is designed to support an extensive range of tokens, only a specific number of tokens / readers (combinations) have been tested with MAC OS X, as part of AET's Quality Assurance procedures.

Note that this does not imply that all tested tokens / readers (combinations) work flawlessly, nor that other tokens / readers (combinations) do not work.

4.1 SafeSign Identity Client version

The version numbers of the components installed by SafeSign Identity Client Standard version 3.0 for MAC OS X, release 3.0.45, are:

Description	File name	File version
Java Card Handling Library	libaetjcss.dylib	3.0.2335
PKCS #11 Cryptoki Library	libaetpkss.dylib	3.0.2311
Token Administration Utility	tokenadmin	3.0.2335

This information can also be found in the *Version Information* dialog of the Token Administration Utility.

4.2 Operating System

SafeSign Identity Client Standard version 3.0.45 for MAC OS X 10.6 comes in a standard version for the following environments:

- MAC OS X 10.6.8

4.3 Tokens

SafeSign Identity Client Standard version 3.0.45 for MAC OS X 10.6 has been tested to support the following tokens:

- Java Card v2.2+ / GlobalPlatform 2.1.1 compliant JCOP cards, including JCOP21, JCOP41, J2A080 and the CrypToken MX2048-JCOP USB Token (with JCOP21 v2.3.1);
- CardOS smart cards developed by Siemens: CardOS 43B.

4.4 Smart Card Readers

Only PCSC 2.0 Class 1 readers are supported. For certain supported readers it is of essential importance which smartcard reader driver is installed and used.

The following reader drivers in combination with the default PCSC-lite and CCID version within Mac OS X 10.6.8 were tested:

- SCM SCR 3311
- ACS ACR 38

The following reader drivers in combination with the default PCSC-lite version within Mac OS X 10.6.8 and proprietary HID Global Omnikey reader drivers version 3.0.2 for Mac OS X 10.6 i386 were tested:

- OmniKey CardMan 3121
- Cherry SmartTerminal-1044U
- Marx CrypToken JCOP21 v2.3.1

4.5 Applications

SafeSign Identity Client Standard version 3.0.45 for MAC OS X 10.6 supports the following applications.

4.5.1 LocalSigner

Application version tested is 2.5.3.

LocalSigner takes only the first reader into account, i.e. the reader connected to the first Slot from the PKCS #11 Slot_ID_list.

Should it be necessary to enumerate all of the user certificates from a smartcard placed in the first reader attached to the Mac, this would need to be additionally configured by marking the appropriate checkbox in the LocalSigner signature dialog.

4.5.2 Adobe Reader

Application version tested is 10.1.0.

In order to use Adobe Reader with qualified signatures, the PKCS #11 access to the smartcard must be used, because the latest AET TokenLounge (minimal) implementation cannot display a PIN from that context (due to the limitations imposed by the OS). This implies that web authentication based on a qualified certificate with tokend-aware apps (such as Adobe Reader) cannot work at all regardless of whether the qualified certificate is suitable for web authentication, unless such a tokend-aware web authentication app offers a direct PKCS#11 card access (like Adobe Reader).

The direct PKCS#11 access to the smartcard has to be configured through Edit->Protection->Security settings. Expand the "Digital IDs" tree node and select "PKCS#11 Modules and Tokens" sub-tree node and click on the "Attach Module". The file path to the SafeSign IC's PKCS#11 is by default "/usr/local/lib/libaetpkss.dylib".

After the previously described configuration steps are executed, Adobe Reader will show every time two instances of all user certificates which are placed on a smartcard. This further means that a user will have to choose the right instance that originates from the PKCS#11 source and not from the tokend in order to successfully sign a PDF document. The only token of recognition of a user certificate that originates from the PKCS#11 source is an extra PIN entry box which is going to be placed directly under the selected user certificate, provided that the user is not already authenticated with his/her PIN to the smartcard. If the latter is the case, there will be no extra PIN entry box, but the previously chosen qualified user certificates is going to be at the first place in the certificates list.

4.5.3 OpenOffice

Application version tested is 3.3.0.

According to the following article: http://wiki.services.openoffice.org/wiki/How_to_use_digital_Signatures, OpenOffice.org is looking for a certificate in the mentioned profiles according to the following search order:

1. The environment variable MOZILLA_CERTIFICATE_FOLDER
2. The Thunderbird profile
3. The Mozilla suite profile
4. The Firefox profile

and that further implies that the trust chain for a certain user certificate has to be properly imported and configured in that certificates store which is (configured to be) used on a particular system.

4.5.4 Certificates - CA/user

All CA (root and intermediate) certificates have to be imported to the appropriate certificate stores prior to any smartcard based use-case is executed.

4.5.5 KeyChain Access

All CA (root and intermediate) certificates have to imported to work with keyChainApp. The appropriate store/keychain under the KeyChainAccess app is the "System" keychain for these certificates.

4.5.6 Thunderbird cert store

All CA (root and intermediate) certificates have to imported to the appropriate CA Thunderbird certificate store.

4.5.7 Firefox cert. store

All CA (root and intermediate) certificates have to imported to the appropriate CA Firefox certificate store.

5 Installation

5.1 Installation Process

Note that users need to have sufficient privileges and basic knowledge of Mac OS X to install SafeSign IC 3.0.45 for MAC OS X 10.6.

1 Save the installation file (.pkg.zip) to a location on your MAC computer and double-click it.

This will result in an installer package that can be installed.

➔ Click the file to install

2 This will open the *Welcome to the SafeSign Installer* window, introducing the package contents:

Figure 1: Install SafeSign Identity Client: Welcome to the SafeSign Identity Client Installer

➔ Carefully read the introduction and click **Continue** to proceed to the next step of the installation process

➔ Note that SafeSign Identity Client for MAC OS X will only run on MAC OS X 10.6.8 or up

3 Upon clicking **Continue**, a dialog with some important information is displayed:

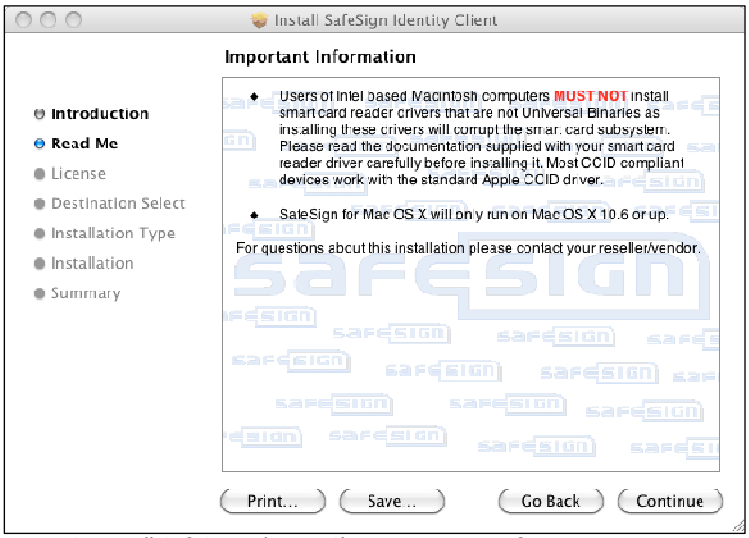

Figure 2: Install SafeSign Identity Client: Important Information Agreement

➔ Click **Continue** to go to the next step

4 The next window will display the SafeSign License Agreement:

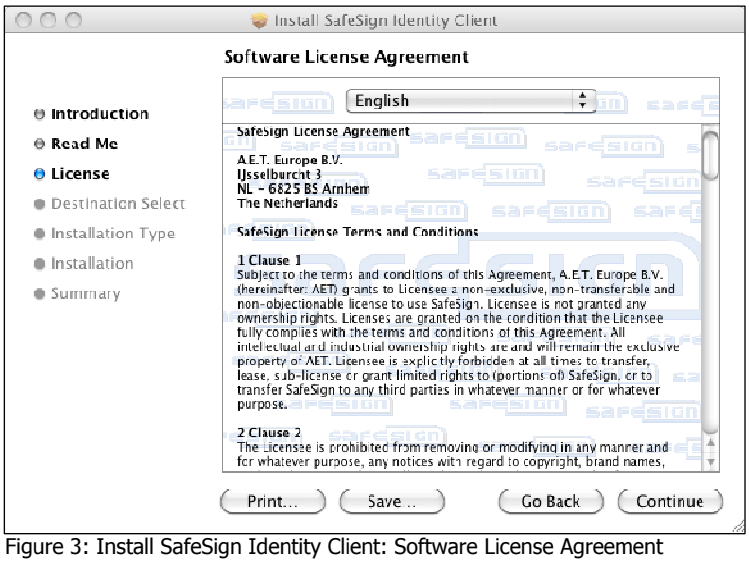

Figure 3: Install SafeSign Identity Client: Software License Agreement

Please read the License Agreement carefully and scroll down to read the whole text.

➔ Click **Continue** when you have read and understood the License Agreement

Note

*In order to go back to the previous step in the installation process, click **Go Back***

In order to quit the installation process, click the red button in the top left corner of the dialog.

5 Upon clicking **Continue**, you will be asked to agree to terms of the software license agreement to continue installation:

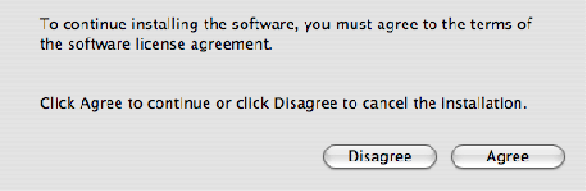

Figure 4: Software License Agreement: Agree to the terms

➔ Click **Agree** when you agree to the terms of the Software License Agreement and wish to continue installing SafeSign.

If you click **Disagree**, you will return to the *Software License Agreement* window.

6 Upon clicking **Agree** to accept the terms of the Software License Agreement (in Figure 4), SafeSign IC will be ready to perform a standard installation for all users on the computer:

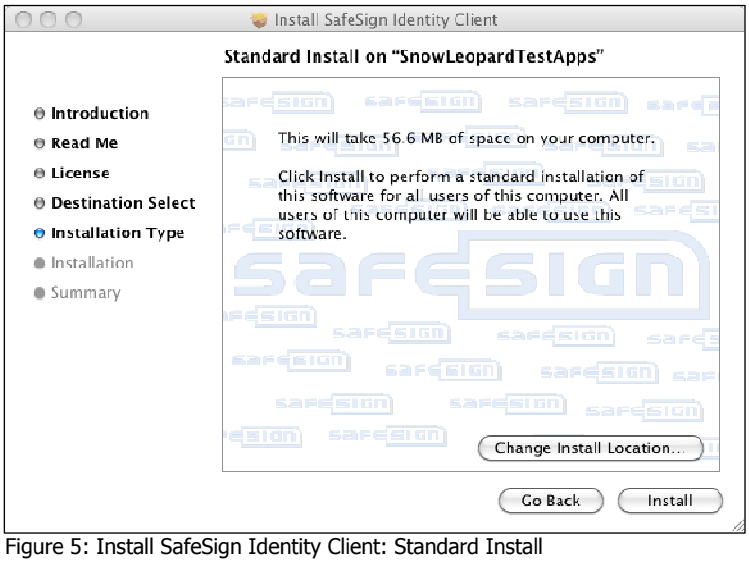

Figure 5: Install SafeSign Identity Client: Standard Install

➔ When you have selected the destination to install SafeSign Identity Client in, click **Install**

Note

*You can change the installation location by clicking **Change Install Location.***

7 Upon clicking **Install**, you may be asked to authenticate with username and password:

Figure 6: Install SafeSign Identity Client: Authenticate

This may happen if you do not have sufficient privileges (because you need sufficient rights to install the SafeSign software).

➔ Enter the name and password of the root (administrator) and click **OK** to continue

8 Upon clicking **OK**, SafeSign Identity Client will be installed.

You will be informed when the installation process is completed:

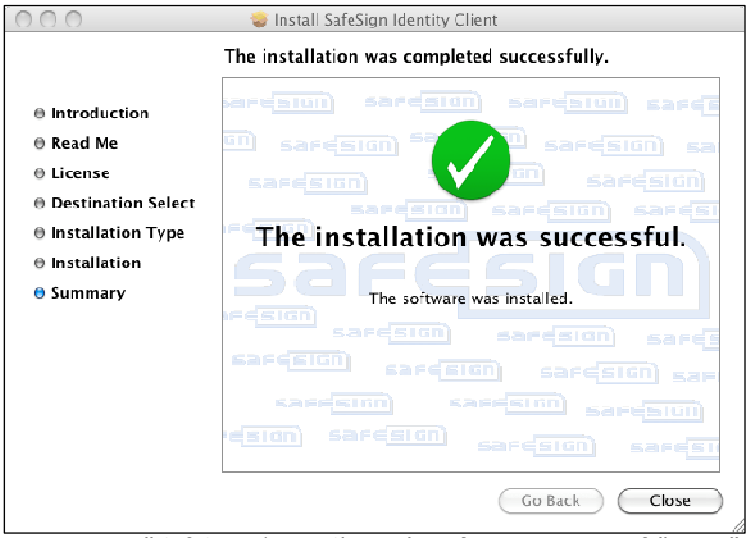

Figure 7: Install SafeSign Identity Client: The software was successfully installed

➔ Click **Close** to close the SafeSign Identity Client Installer.

5.2 Verify installation

When SafeSign Identity Client is installed, you can verify that installation is successful by checking for the presence of the Token Administration Utility (*tokenadmin.app* in the *Applications* folder):

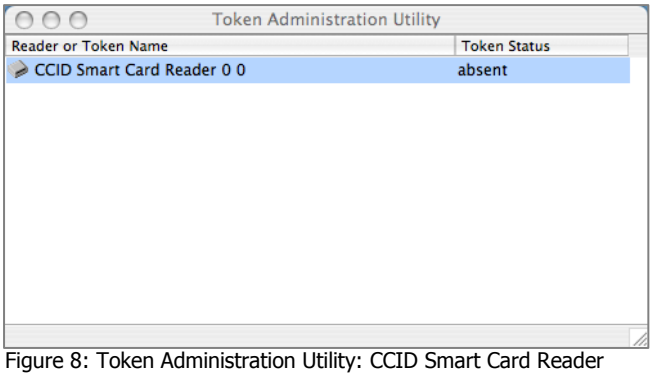

Figure 8: Token Administration Utility: CCID Smart Card Reader

Note that in the example above, the native MAC OS X CCID smart card reader driver is installed and that a CCID compliant smart card reader is attached (in our case, the CardMan 3121 USB smart card reader).

When you insert a token, the Token Administration Utility will either display that a blank token is inserted (that can be initialised) or that a token with a token label has been inserted (as below):

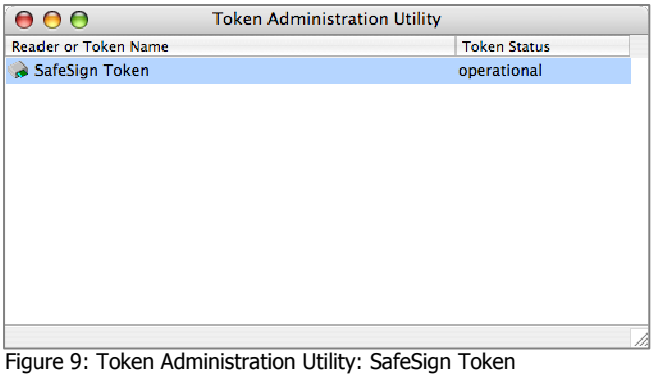

Figure 9: Token Administration Utility: SafeSign Token

All features of the Token Administration Utility are available to you (apart from the Task Manager). Refer to the SafeSign Identity Client Token Administration Utility User Guide for Windows.

6 Installation of SafeSign Identity Client Security Module

When you have installed SafeSign Identity Client, you may want to use SafeSign Identity Client with such applications as Firefox and/or Thunderbird or other (PKCS #11) applications that support the use of tokens, such as Adobe Reader.

In order to do so, you should install or "load" the SafeSign Identity Client PKCS #11 library as a security module in these applications[1].

As an example, the installation of the SafeSign PKCS #11 Library in Firefox is described.

6.1 Firefox

1 In Firefox, go to **Firefox > Preferences > Advanced > Encryption > Security Devices**:

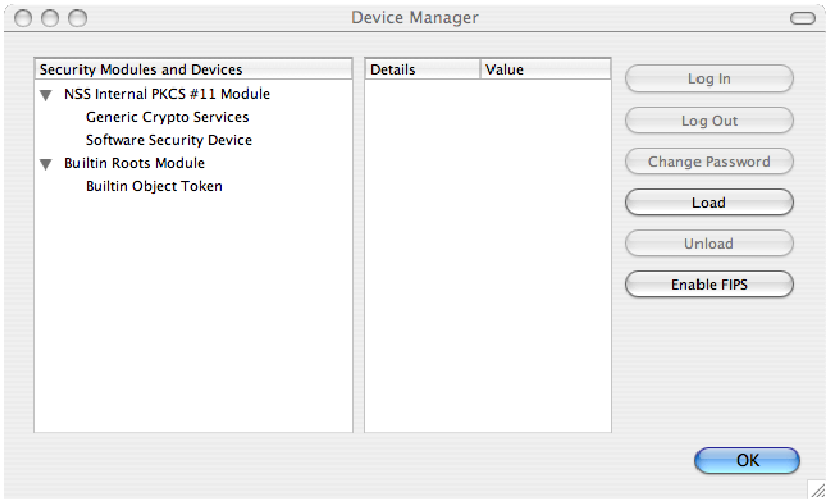

Figure 10: Firefox Device Manager: Security Modules and Devices

The SafeSign Identity Client PKCS #11 module is not yet installed.

➔ Click on **Load** to load a new module

2 Upon clicking on **Load**, you can enter the information for the module you want to add:

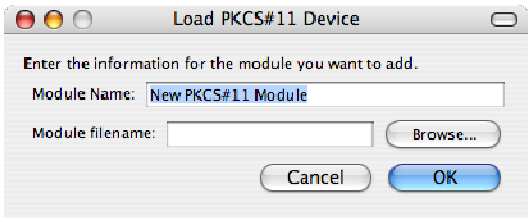

Figure 11: Firefox Device Manager: Load PKCS#11 Device

[1] This is customary for PKCS #11 applications, where you need to load the cryptographic library or make reference to the library to be used for cryptographic / token support.

3

➔ Enter a name for the security module, e.g. *SafeSign Identity Client* and type in the name of the SafeSign Identity Client PKCS #11 library (i.e. libaetpkss.dylib):

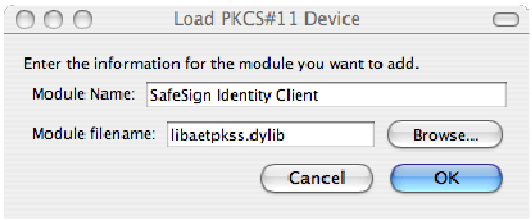

Figure 12: Firefox Device Manager: Load SafeSign

➔ Click **OK**

4

You will be asked to confirm installation of the security module:

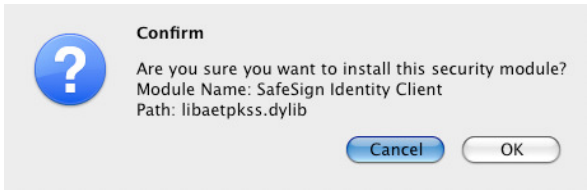

Figure 13: Firefox Device Manager: Are you sure you want to install this security module?

➔ Click **OK** to continue installation

5

You will be informed when the module is successfully loaded:

Figure 14: Firefox Device Manager: A new security module has been installed

➔ Click **OK**

The SafeSign Identity Client PKCS #11 Library will now be available as a security module in Firefox:

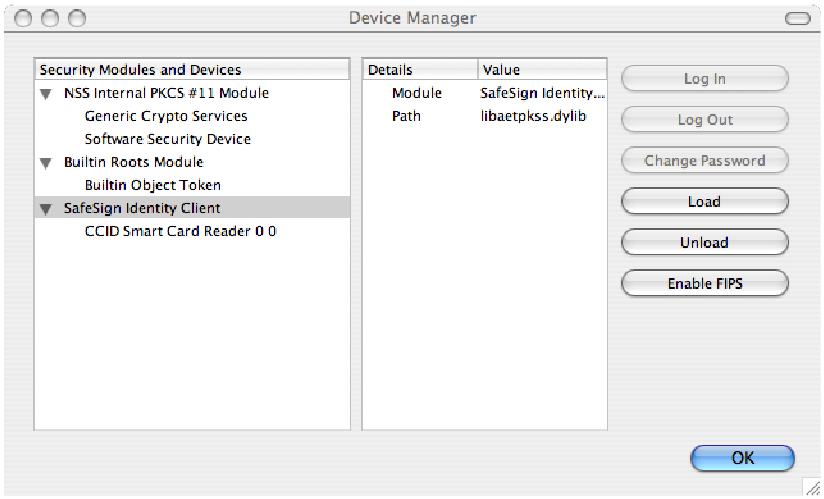

Figure 15: Firefox Device Manager: SafeSign Security Module

Under the name of the security module ('SafeSign Identity Client', as specified in Figure 12), the available devices are displayed.

In this case, there is only one device installed, a smart card reader identified by the label 'CCID Smart Card Reader'. No token is inserted in the reader.

When the token is inserted, the label of the token will be displayed:

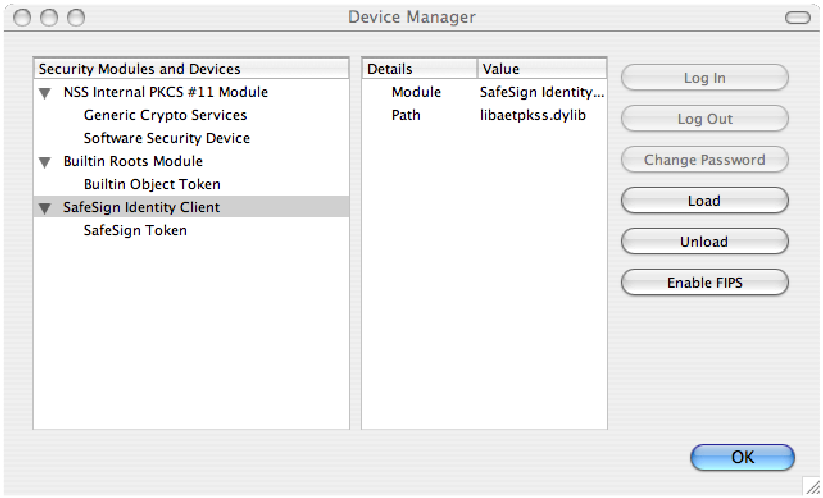

Figure 16: Firefox Device Manager: Token inserted

Note that there may be different reader and token combinations (so-called "slots"), for example, a smart card in a smart card reader or a USB token.

You can now use your SafeSign Identity Client token in Firefox for such operations as web authentication, where you will be asked to select a device and enter the PIN:

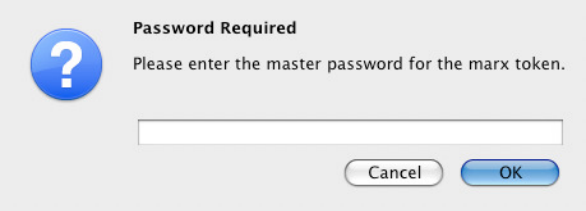

Figure 17: Firefox: Prompt

Installation Fails

When installation of the SafeSign Identity Client PKCS #11 library as a security module in Firefox fails, the following prompt will be shown:

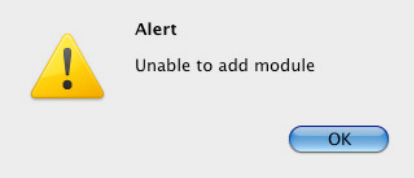

Figure 18: Firefox: Unable to add module

➔ Verify that you have provided the correct name, i.e. *libaetpkss.dylib* (located in /usr/local/lib)

Delete Module

It is possible to delete the SafeSign Identity Client security module, by clicking **Unload**.

Upon clicking **Unload**, the module will be deleted:

Figure 19: Firefox: External security module successfully deleted

7 Known Issues

7.1 Token Administration Utility

7.1.1 Wipe token

The function Wipe token is applicable to series completion tokens (production tokens). It allows you to wipe the contents of a series-completed token.

This function does not work in SafeSign IC version 3.0.45 for MAC OS X 10.6.

7.1.2 Initialize token

The function Initialise token is applicable to non-series completion tokens (test tokens). It allows you to re-initialise a token with a new PUK and PIN.

This function does not work in SafeSign IC version 3.0.45 for MAC OS X 10.6.

It is not possible to initialize test-completed tokens. Initialisation should take place on a Windows Operating System or in a personalization facility.

7.1.3 Show Digital IDs

The function Show Digital IDs enumerates all Digital IDs from a token.

In SafeSign IC version 3.0.45 for MAC OS X 10.6, it enumerates correctly all the certificates from the smartcard, until the inserted smartcard is removed (Show Digital IDs window has to stay opened to reproduce this incorrect behaviour).

If the same or any other smartcard is then inserted, the already opened window "Show Digital IDs" is not going to enumerate and show any certificates from the newly inserted smartcard. The working functionality can be re-established by closing the Token Administration Utility and opening it again.

7.1.4 Show Token Info

CardOS 4.3b smartcards are recognized/called under the Token model section as "Belgian eID".

StarCos 3.4c smartcards are recognized/called under the Token model section as "G&D StarToken 350".

7.1.5 Localization

The Token Administration Utility with its associated PIN and qualified PIN entry dialogs is always going to be loaded in the English language.

7.1.6 Help: Versions info

For the component "Java Card Handling Library" under the column "File versions" displays "unknown".

For the component "PKCS #11 Cryptoki Library" under the column "File versions" displays "unknown".

When you click to save the version info, the version numbers in the resulting file are unknown as well.

7.2 SafeSign Uninstaller

After "SafeSign Uninstaller" is run for the first time, it is going to do a graceful de-installation of both "tokenadmin.app" and itself. In other words, SafeSign IC is going to be gracefully de-installed.

If after this operation, SafeSign IC is again installed to the same system, "SafeSign Uninstaller" is not going to be installed.