SafeSign for MAC OS X

Configuration and Installation Guide

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/
http://www.safesign.com

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

Document Information

Filename: **SafeSign for MAC OS X**
Configuration and Installation Guide

Document ID: **SafeSign_Installation_MACOSX_v1.0**

Project Information: **SafeSign User Documentation**

Document revision history

Version	Date	Author	Changes
1.0	08-07-2004	Drs C.M. van Houten	First edition for SafeSign Standard Version 2.0 for MAC OS X

WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE

Table of contents

Table of Figures

About the Product

SafeSign for MAC OS X is a software package that can be used to enhance the security of Internet applications that support PKCS #11 by hardware tokens, on the MAC OS X platform.

The SafeSign package installs the SafeSign PKCS #11 library that allows you to store public and private data on a personal token, i.e. a smart card or an USB token.

For more information, refer to the latest SafeSign Product Description.

About the Manual

This document describes the configuration and installation of SafeSign for MAC OS X.

It describes the requirements before installing SafeSign for MAC OS X, the installation of SafeSign and how you can verify that SafeSign is properly installed and how to use SafeSign in Netscape and/or Mozilla.

1 Requirements

This chapter describes the requirements for installing and using SafeSign for MAC OS X, as tested by A.E.T. Europe B.V.

All tokens, smart card readers and applications SafeSign Standard 2.0 for MAC OS X was tested for, can be find in the SafeSign Standard 2.0 for MAC OS X product description.

1.1 Software Requirements

1.1.1 Operating System

- MAC OS X 10.2
- MAC OS X 10.3

1.1.2 Applications

Note: this only applies if you want to use Netscape and/or Mozilla for e.g. web authentication and secure e-mail. Other applications supporting PKCS #11 may also be used.

- Netscape 7.1
- Mozilla 1.6, 1.7
- Mozilla Firefox 0.9.1
- Mozilla Thunderbird 0.7.1

1.2 Hardware Requirements

Note that though SafeSign 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. This does not imply that other tokens / readers (combinations) do not work.

1.2.1 Smart Card Readers

SafeSign for MAC OS X has been tested with the following smart card readers:

- Omnikey CardMan 2020 USB smart card reader
- Omnikey CardMan 3121 USB smart card reader
- Rainbow iKey 3000 USB Token

Note

Please note that there are some issues (e.g. the IFD handler crashing at unexpected moments), with the CardMan 2020 and the iKey 3000 USB token, which are due to the smart card reader drivers. These issues are currently under investigation by their respective suppliers.

The CardMan 3121 has been found to be the most reliable and stable and is therefore the preferred reader for testing and using SafeSign with MAC OS X.

1.2.2 Smart Cards

No token utilities are delivered for the MAC, so you should use a smart card initialised with SafeSign 1.0.9.04 (or higher)[1] or SafeSign Standard 2.0 for Windows.

The following tokens have been tested:

- G&D STARCOS SPK 2.3 v7.0 smart card
- G&D STARCOS SPK 2.4 v3.0 smart card
- G&D STARCOS SPK 2.4 FIPS v3.3 smart card
- G&D Sm@rtCafé Expert v2.0 smart card
- IBM JCOP 20
- Rainbow iKey 3000 USB token

1.3 Installation files

The installation package *SafeSignInstaller20.tar.gz* will extract in:

- Directory called *meta-installer*
- *SafeSign2.0.mpkg*

Execute the file *SafeSign2.0.mpkg*.

The *SafeSign2.0.mpkg* file will install all packages installed in the *meta-installer* directory.

1.4 User requirements

User needs to have sufficient privileges and basic knowledge of Mac OS X to install SafeSign for MAC OS X.

[1] Either 1.0.9.04 or 1.0.9.04-Update

2 SafeSign Installation for MAC OS X

After extracting the *SafeSignInstaller20.tar.gz* file, locate the *SafeSign2.0.mpkg* file in the directory *meta-installer*, which contains all packages.

1 This will open the *Welcome to the SafeSign 2.0 Installer* window, introducing the package contents:

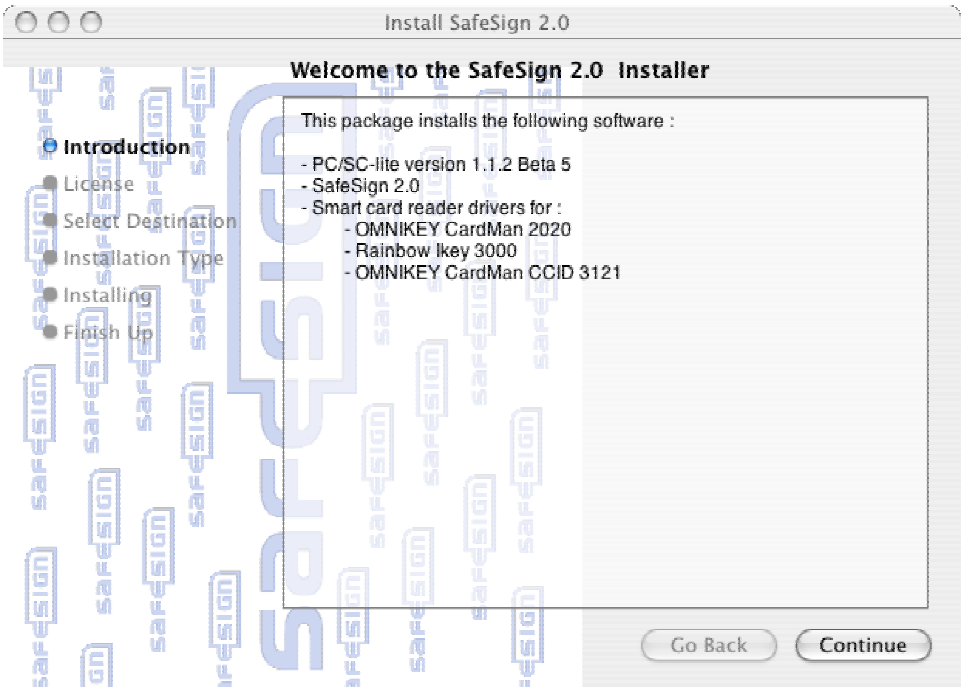

Figure 1: Install SafeSign 2.0: Welcome to the SafeSign 2.0 Installer

This window will list the components installed by SafeSign for MAC OS X, version 2.0.

➔ Click **Continue** to proceed to the next step of the installation process

2 The next window will display the SafeSign License Agreement:

Figure 2: Install SafeSign 2.0: 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.

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

Figure 3: 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.

4 Upon clicking **Agree** to accept the terms of the Software License Agreement, you will be asked to select a destination for SafeSign to be installed in:

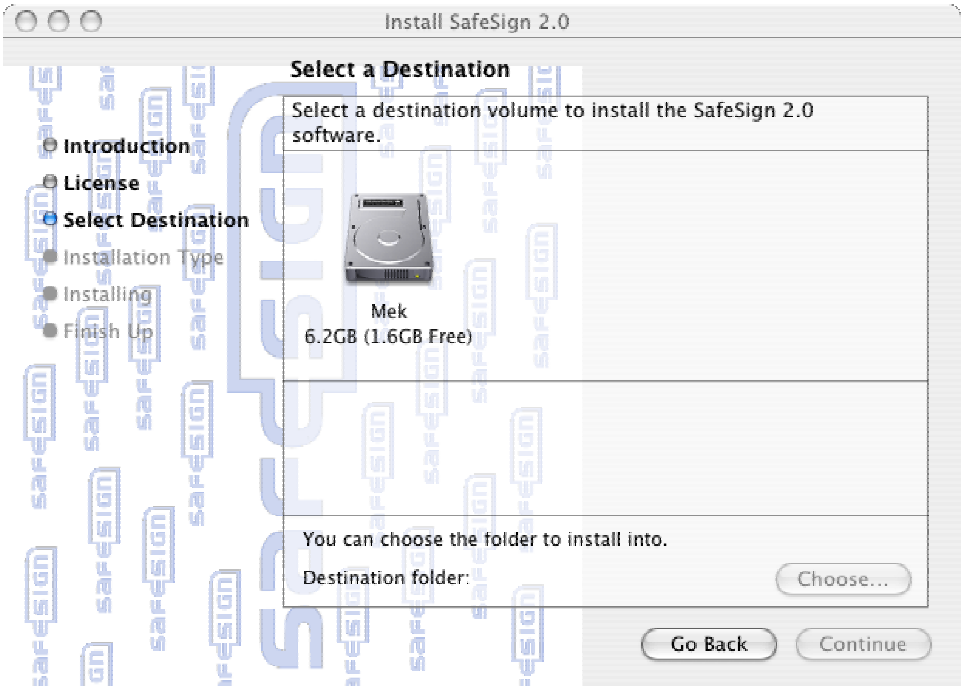

Figure 4: Install SafeSign 2.0: Select a Destination

This will allow you to select a destination volume to install the SafeSign 2.0 software in.

In our example, the destination volume will be the local hard disk (called '*Mek*').

➔ Select the destination volume by clicking on it:

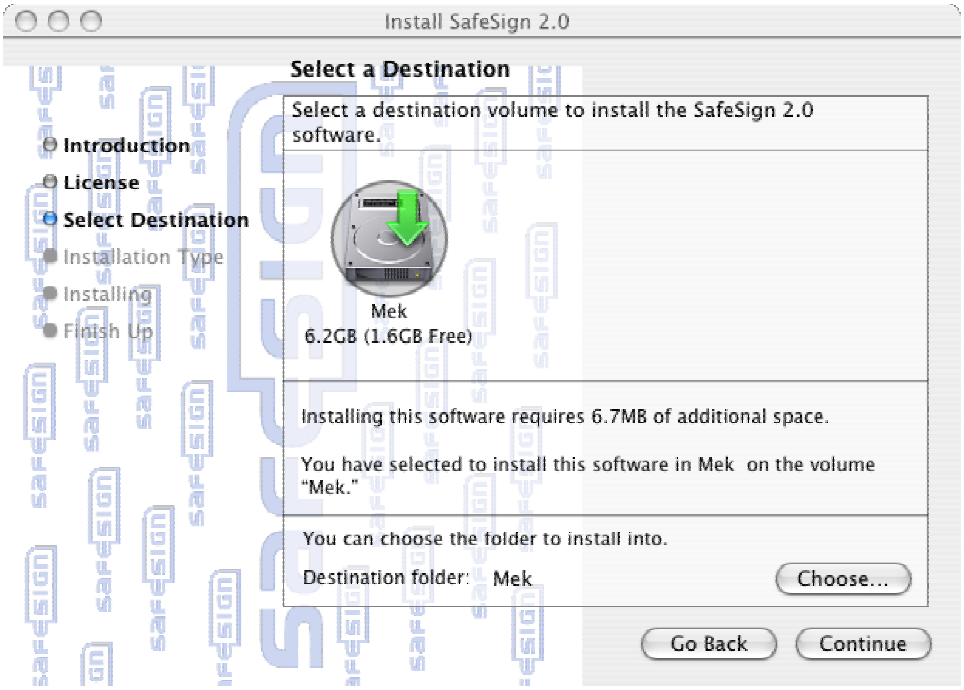

Figure 5: Select a Destination: Destination volume selected

➔ When you have selected the destination to install SafeSign in, click **Continue**

Note

*You can select a specific destination folder by clicking on **Choose**.*

5 Upon clicking **Continue**, you will be allowed to install / upgrade SafeSign:

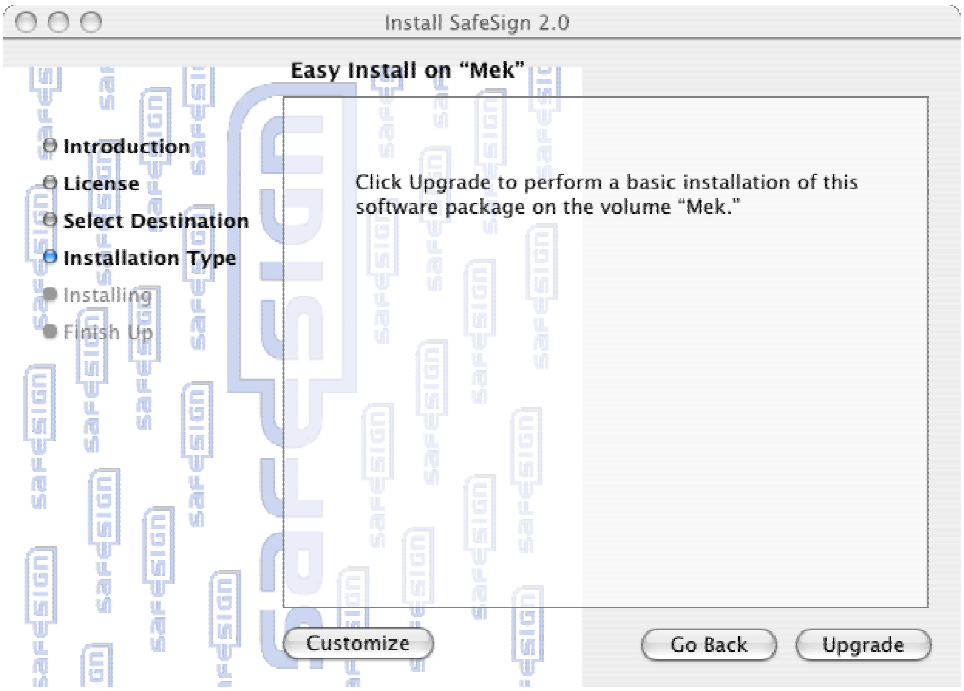

Figure 6: Install SafeSign 2.0: Easy Install on "Mek"

Now you will be able to install SafeSign, either performing a new installation or an upgrade installation.

When SafeSign has already been installed before, you will be allowed to upgrade the installation (as in the picture above, by clicking **Upgrade**). If you are performing a new installation, the button **Install** will be available. In our example, we will upgrade the installation.

➔ Click **Upgrade** to upgrade SafeSign

Custom Installation

You may want to select the components you wish to install, for example if you are using a particular smart card reader. In this case, you may not want to install the drivers for other smart card readers as well.

In order to perform a custom installation, select **Customize** in the *Easy Install on "Mek"* window to open the following window where you can select / deselect packages to be installed:

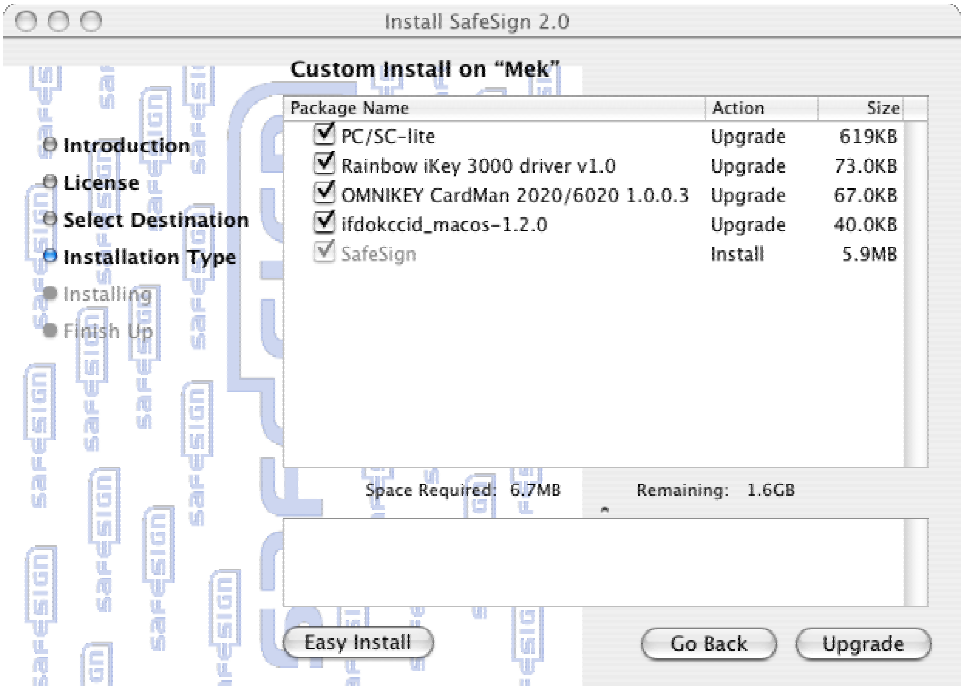

Figure 7: Install SafeSign 2.0: Custom Install on "Mek"

By default, all packages will be installed:

Package Name	Description
PC/SC-lite	This package contains PC/SC-lite version 1.1.2 Beta 5 modified to be used with SafeSign
Rainbow iKey 3000 driver v1.0	This package installs the iKey 3000 device drivers v1.0
OMNIKEY CardMan 2020/6020 1.0.0.3	n/a
OMNIKEY AG CCID device driver v1.1.0	OMNIKEY CardMan 3121 smart card reader
SafeSign	This package contains SafeSign and some test tools

Table 1: Custom Installation: Packages

➔ Deselect the packages you do not wish to install, then click **Upgrade** to upgrade SafeSign

6 Upon clicking **Upgrade**, you may be asked to authenticate:

Figure 8: Easy Install on “Mek”: Authenticate

When you do not have sufficient privileges, you will be asked to authenticate with username and password.

This is because you need administrator / root rights to install the SafeSign software.

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

7 Upon clicking **OK**, SafeSign will be installed and you will be informed of its progress:

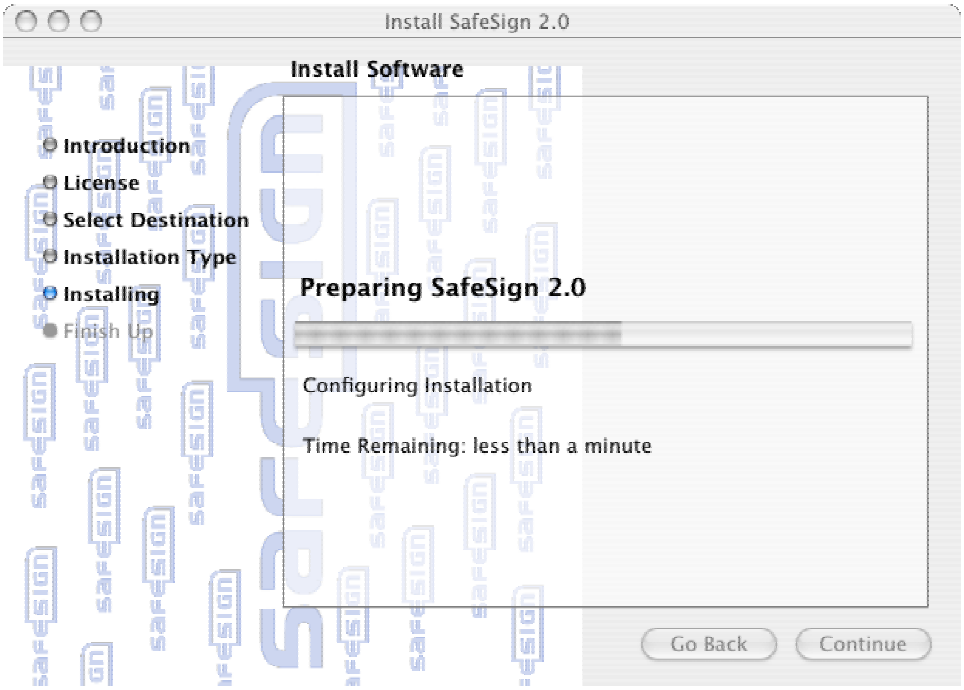

Figure 9: Install SafeSign 2.0: Install Software

➔ Wait until the installation process is completed

8 You will be informed when the installation process is completed:

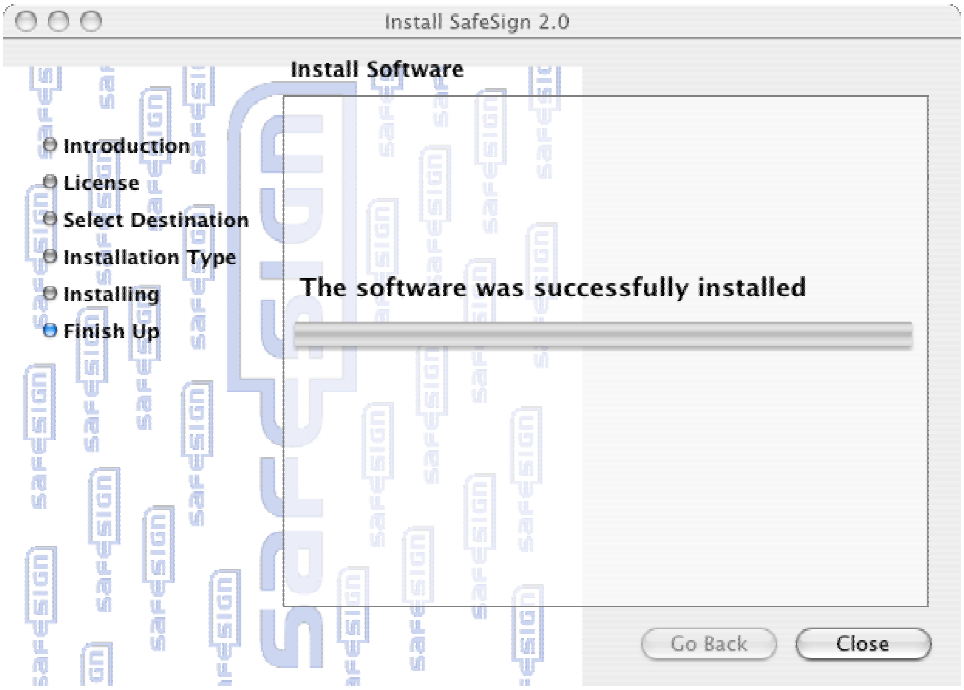

Figure 10: Install Software: The software was successfully installed

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

3 Verify and Test Installation

3.1 SafeSign PKCS #11 Library

In order to verify that the SafeSign PKCS #11 Library has been properly installed, open a Terminal and enter:

ls /usr/lib/libaetpkss.dylib

as in the picture below:

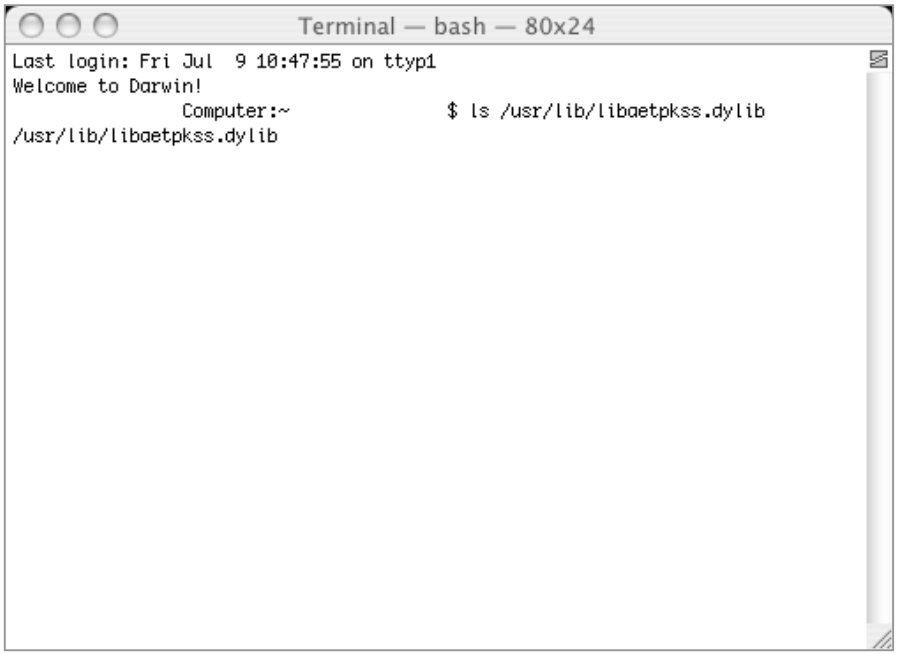

Figure 11: Terminal: /usr/lib/libaetpkss.dylib

The SafeSign PKCS #11 Library is located in /usr/lib/ and is called: *libaetpkss.dylib*

3.2 Sign and Verify test

You can test SafeSign by means of the utility called **SignAndVerifyLinux**, installed by SafeSign. This test program will test several PKCS#11 actions.

The **SignAndVerifyLinux** utility is installed in: /usr/bin/

You can execute it from any location, by entering 'SignAndVerifyLinux', after which the program will run:

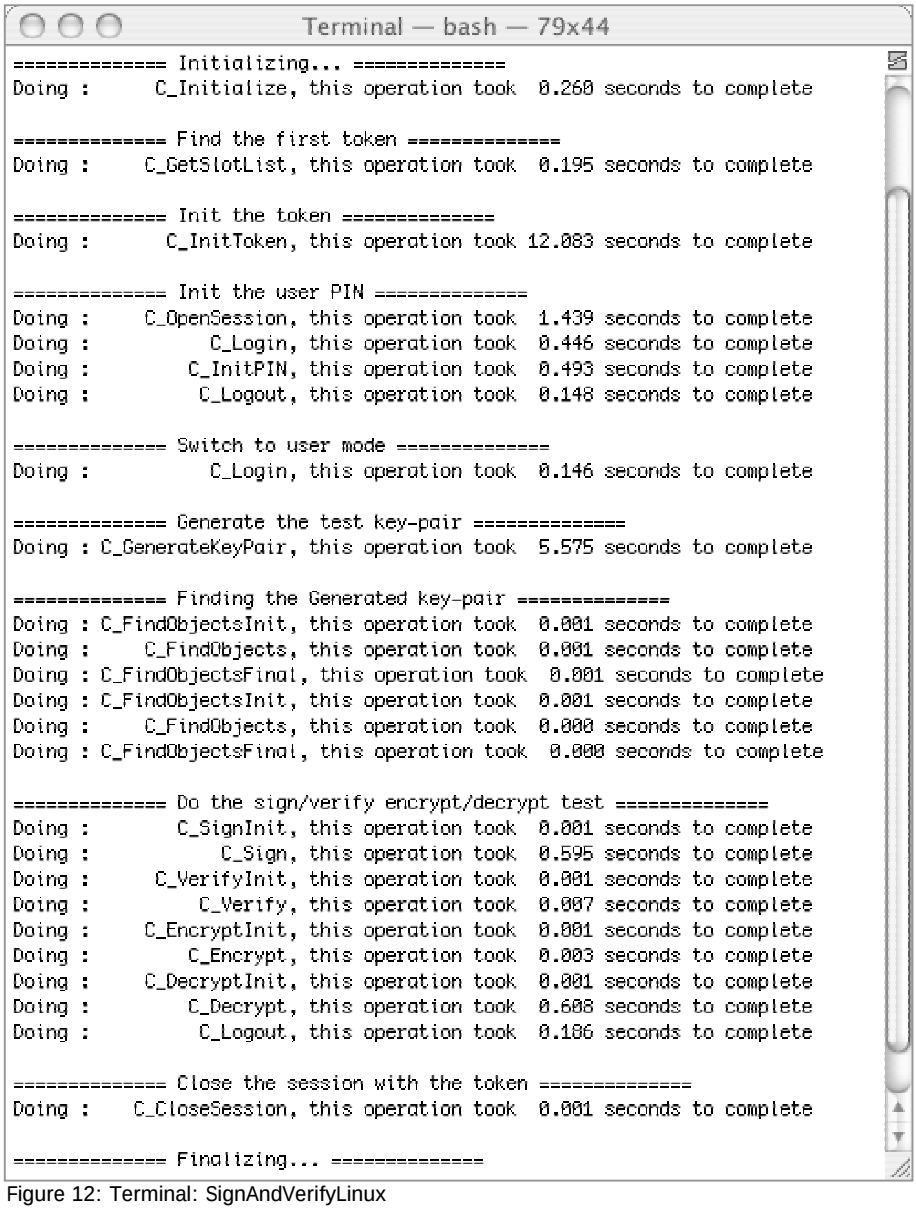

Figure 12: Terminal: SignAndVerifyLinux

4 Set up PKCS#11 library in Netscape and Mozilla

4.1 Netscape

In Netscape, go to **Netscape > Preferences > Privacy & Security > Certificates > Manage Security Devices**:

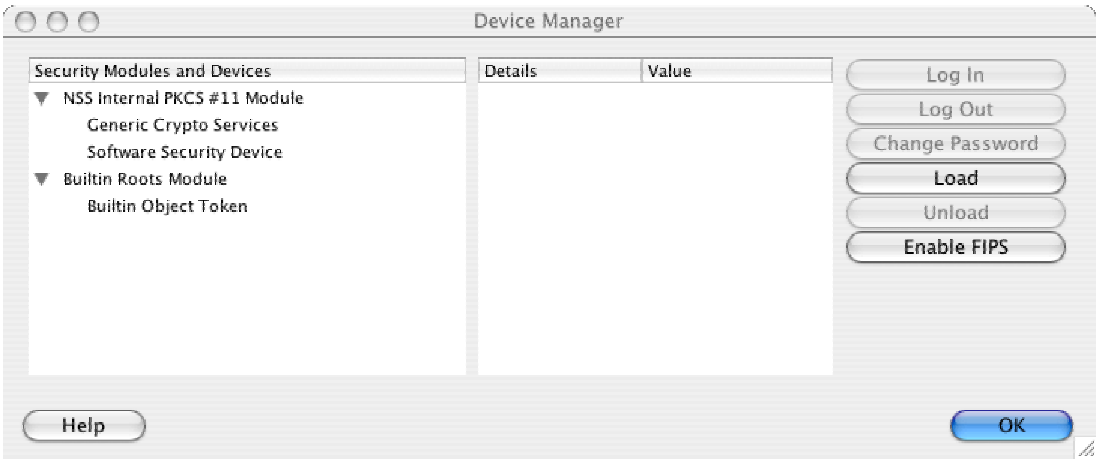

Figure 13: Netscape Device Manager: Security Modules and Devices

The SafeSign PKCS #11 module is not yet installed.

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

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

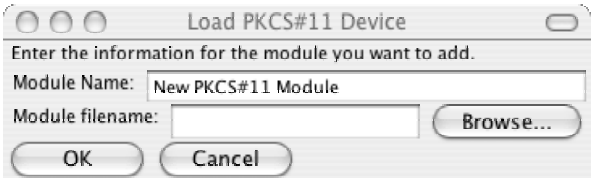

Figure 14: Netscape Device Manager: Load PKCS#11 Device

➔ Enter a name for the security module, e.g. *SafeSign* and type in the path to the location where the PKCS#11 Library is located (/usr/lib/libaetpkss.dylib, as described in paragraph 3.1), as below:

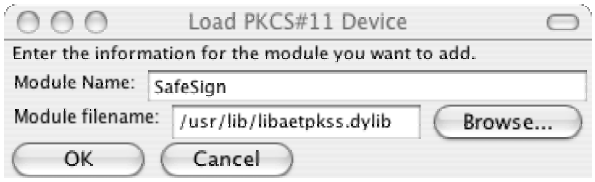

Figure 15: Netscape Device Manager: Load SafeSign

➔ Click **OK**

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

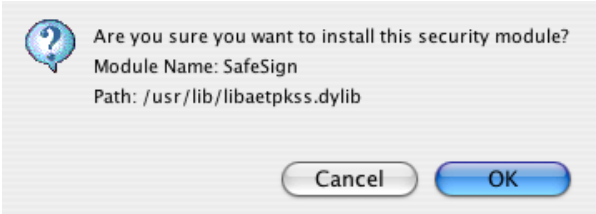

Figure 16: Netscape Device Manager: Are you sure you want to install this security module?

➔ Click **OK** to continue installation

You will be informed when the module is successfully loaded:

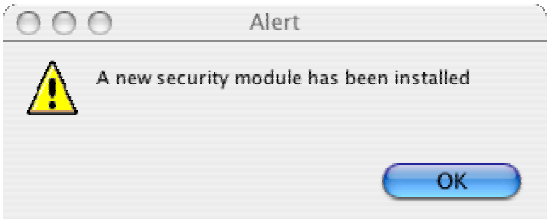

Figure 17: Netscape Device Manager: A new security module has been installed

➔ Click **OK**

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

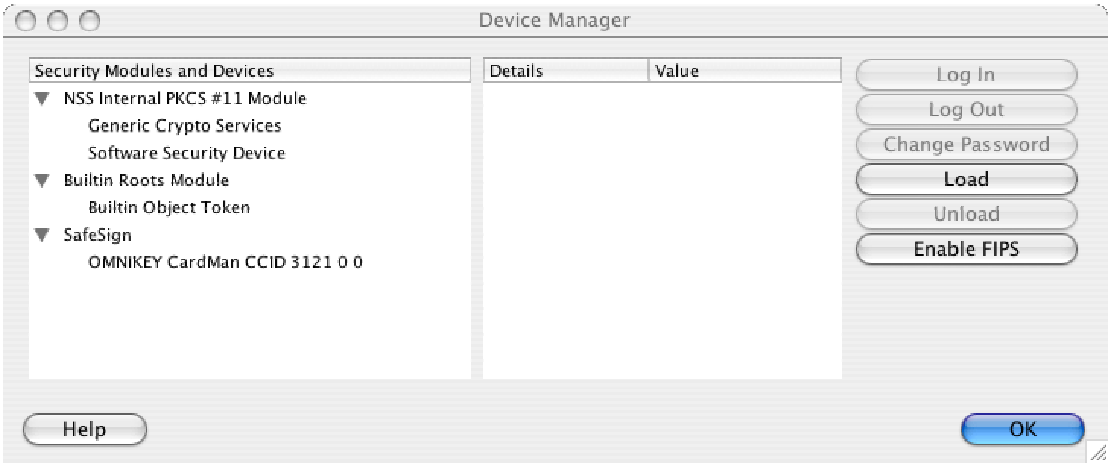

Figure 18: Netscape Device Manager: SafeSign Security Module

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

Figure 19: Netscape: Master Password Prompt

4.2 Mozilla

In Netscape, go to **Mozilla > Preferences > Privacy & Security > Certificates > Manage Security Devices**:

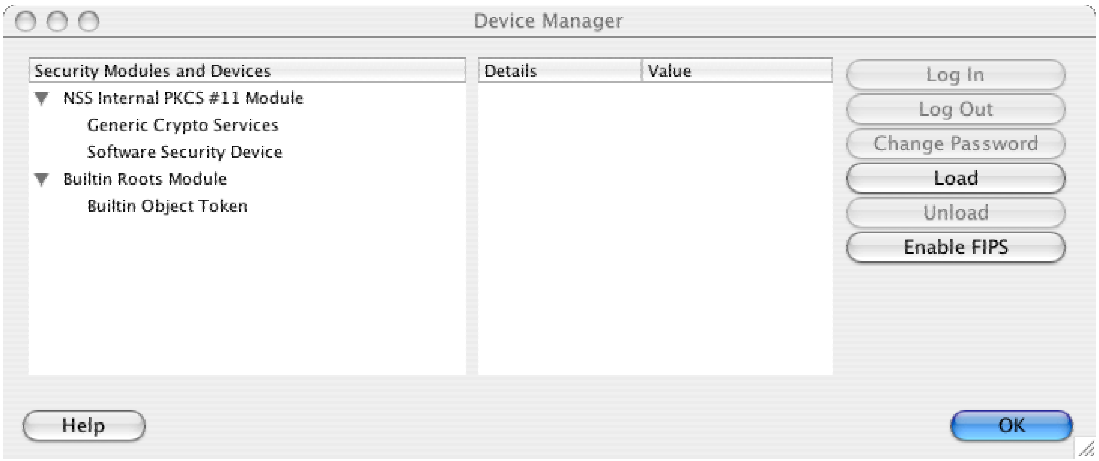

Figure 20: Mozilla Device Manager: Security Modules and Devices

The SafeSign PKCS #11 module is not yet installed.

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

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

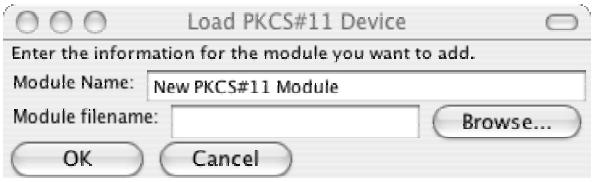

Figure 21: Mozilla Device Manager: Load PKCS#11 Device

➔ Enter a name for the security module, e.g. *SafeSign* and type in the path to the location where the PKCS#11 Library is located (/usr/lib/libaetpkss.dylib, as described in paragraph 3.1), as below:

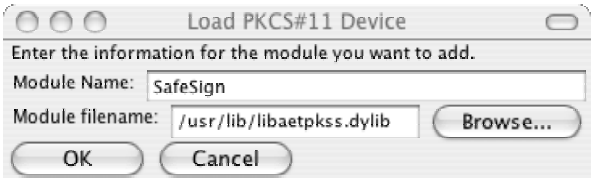

Figure 22: Mozilla Device Manager: Load SafeSign

➔ Click **OK**

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

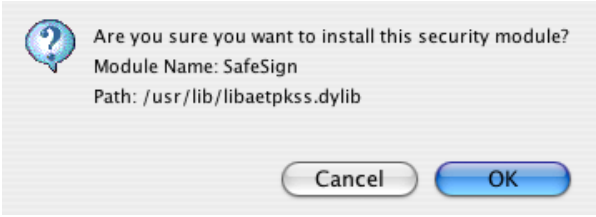

Figure 23: Mozilla Device Manager: Are you sure you want to install this security module?

➔ Click **OK** to continue installation

You will be informed when the module is successfully loaded:

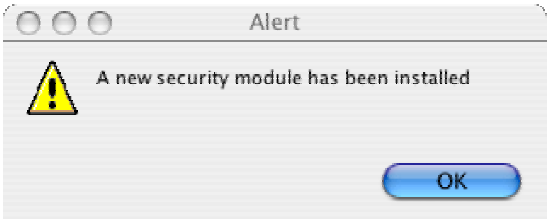

Figure 24: Mozilla Device Manager: A new security module has been installed

➔ Click **OK**

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

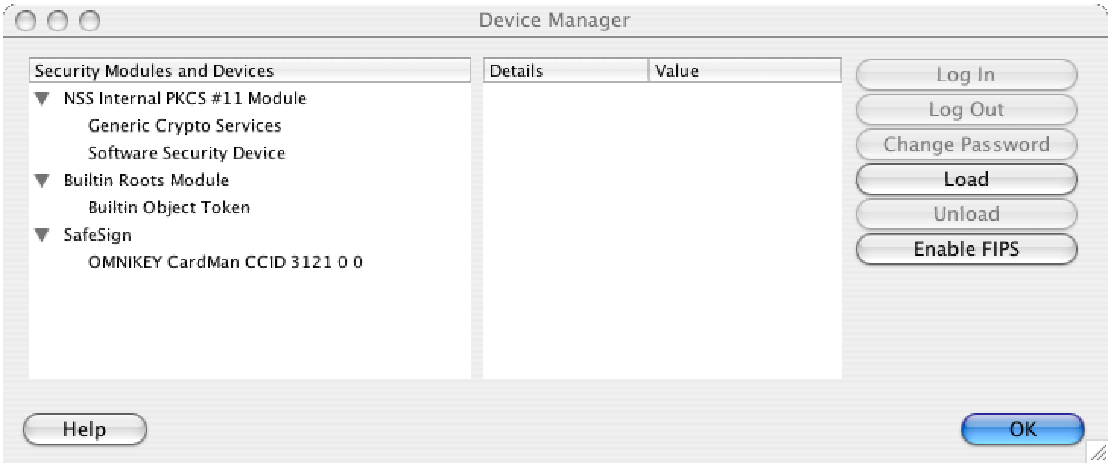

Figure 25: Mozilla Device Manager: SafeSign Security Module

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

Figure 26: Mozilla: Master Password Prompt

Notes