

Product Description

SafeSign Identity Client Standard Version 2.3 for MAC OS X 10.4

This document contains information of a proprietary nature.
No part of this document may be reproduced or transmitted
in any form or by any means electronic, mechanical or
otherwise, including photocopying and recording for any
purpose without written permission of A.E.T. Europe B.V.
Individuals or organisations, which are authorised by A.E.T.
Europe B.V. in writing to receive this information, may
utilise it for the sole purpose of evaluation and guidance.

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.

© Copyright A.E.T. Europe B.V., 1997 - 2006.

All rights reserved.

SafeSign is a trademark of A.E.T. Europe B.V. All A.E.T. Europe B.V. product names are trademarks of A.E.T. Europe B.V. All other product and company names are trademarks or registered trademarks of their respective owners.

Credit information:

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

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

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

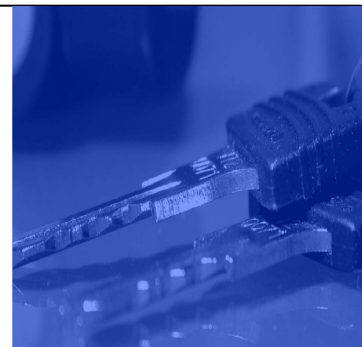
IJsselburcht 3
NL-6825 BS
P.O. Box 5486
NL-6802 EL Arnhem
The Netherlands
Tel. +31-26-365 33 50
Tel. Support +31-26-365 35 43
Fax +31-26-365 33 51



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

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

Copyright © 1997 - 2006 A.E.T. Europe B.V.,
Arnhem, The Netherlands.
All rights reserved.



Document Information

Filename: Product Description
SafeSign Identity Client Standard

Document ID: SafeSign-IC-Standard_2.3_MACOSX_Product_Description

Project Information: SafeSign Identity Client Release Documentation

Document revision history

Version	Date	Author	Changes
1.0	15-08-2006	Drs. C.M. van Houten	First edition for SafeSign Identity Client Standard Version 2.3 for MAC OS X 10.4 (release 2.3.0)
1.1	24-11-2006	Drs. C.M. van Houten	Edited for SafeSign Identity Client Standard Version 2.3 for MAC OS X 10.4 (release 2.3.1)

WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE

Table of contents

Warning Notice	II
Document Information	III
Table of contents	IV
List of Figures	V
About the Document	VI
1 Introduction	1
2 SafeSign Identity Client for MAC OS X 10.4 Functionality	1
3 Features	2
3.1 Multi-token support	2
3.2 Support for PIN / PUK of 15 characters	2
3.3 Support for secure off-line PIN unlock	2
3.4 Multiple language support	3
3.5 Token Administration Utility	3
4 Tested Configurations	4
4.1 SafeSign version	4
4.2 Operating System	4
4.3 Tokens	4
4.4 Smart Card Readers	4
4.5 Applications	5
5 Installation	6
5.1 Installation Process	6
5.2 Verify installation	11
6 Installation of SafeSign Security Module	12
6.1 Firefox	12
6.2 Thunderbird	16
7 Known Issues	20
Appendix 1: How to remove smart card reader drivers	a

List of Figures

Figure 1: Token Utility: Unlock PIN	2
Figure 2: Install SafeSign 2.0: Welcome to the SafeSign 2.0 Installer.....	6
Figure 3: Install SafeSign: Software License Agreement	7
Figure 4: Software License Agreement: Agree to the terms	7
Figure 5: Select a Destination: Destination volume selected	8
Figure 6: Install SafeSign: Easy Install	9
Figure 7: Easy Install: Authenticate	10
Figure 8: Install SafeSign: The software was successfully installed.....	10
Figure 9: Token Administration Utility: CCID Smart Card Reader.....	11
Figure 10: Token Administration Utility: SafeSign Token	11
Figure 11: Firefox Device Manager: Security Modules and Devices.....	12
Figure 12: Firefox Device Manager: Load PKCS#11 Device.....	12
Figure 13: Firefox Device Manager: Load SafeSign	13
Figure 14: Firefox Device Manager: Are you sure you want to install this security module?.....	13
Figure 15: Firefox Device Manager: A new security module has been installed	13
Figure 16: Firefox Device Manager: SafeSign Security Module	14
Figure 17: Firefox Device Manager: Token inserted	14
Figure 18: Firefox: Prompt	15
Figure 19: Firefox: Unable to add module	15
Figure 20: Firefox: External security module successfully deleted.....	15
Figure 21: Thunderbird Device Manager: Security Modules and Devices.....	16
Figure 22: Thunderbird Device Manager: Load PKCS#11 Device.....	16
Figure 23: Thunderbird Device Manager: Load SafeSign	17
Figure 24: Thunderbird Device Manager: Are you sure you want to install this security module?.....	17
Figure 25: Thunderbird Device Manager: A new security module has been installed	17
Figure 26: Thunderbird Device Manager: SafeSign Security Module	18
Figure 27: Thunderbird Device Manager: Token inserted	18
Figure 28: Thunderbird: Prompt	19
Figure 29: Thunderbird: Unable to add module	19
Figure 30: Thunderbird: External security module successfully deleted.....	19

About the Document

This product description defines the features and supported configurations of SafeSign Identity Client Standard for MAC OS X 10.4 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 10.4 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 10.4 that allows the user to generate and store public and private data on a personal token.

2 SafeSign Identity Client for MAC OS X 10.4 Functionality

SafeSign Identity Client for MAC OS X 10.4 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.

PKCS #12 support.

PKCS #15 support.

Product Description with installation instructions for end users (no developer documentation). All documentation is in the English language.

DMG package for installation on the MAC OS X 10.4 platform.

Token Administration Utility to initialise the token, change PIN, etc.

3 Features

The following (new) features are supported by SafeSign Identity Client Standard Version 2.3 for MAC OS X 10.4 (in analogy to the (new) features supported by SafeSign Identity Client version 2.3 for Windows):

- Multiple token support;
- Support for PIN / PUK of 15 characters;
- Support for secure off-line PIN unlock;
- Multiple language support;
- Token Administration Utility.

3.1 Multi-token support

SafeSign Identity Client version 2.3 for MAC OS X 10.4 supports multiple tokens.

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

3.2 Support for PIN / PUK of 15 characters

In combination with the Java Card 2.2 (or up) / GlobalPlatform 2.1.1 compliant Java smart cards supported, it is possible to initialise the token with a PIN and / or PUK of 15 characters.

3.3 Support for secure off-line PIN unlock

Secure off-line PIN unlock allows an end user to unblock the PIN of their card by off-line means, for instance via a telephone conversation with a helpdesk. The benefit of secure off-line PIN unlock is that the PUK code does not have to be disclosed to end users.

SafeSign Identity Client version 2.3 includes the standard SafeSign PKI applet v2 with off-line PIN unlock and built-in support for off-line PIN unlock in the Token Administration Utility as part of the standard middleware (installation) package (thus facilitating an easy roll out to end users without the need to build custom unlock applications):



Figure 1: Token Utility: Unlock PIN

Secure off-line PIN unlock on MAC OS X has been tested with the following cards:

- Giesecke & Devrient Sm@rtCafé Expert 64
- IBM JCOP41

In principle, any token that is not listed but complies with Java Card 2.2 (or up) and Open/Global Platform 2.0.1 (or up) can be supported¹.

For more information on this feature and the requirements for implementation on the server side, please contact AET at support@aeteurope.nl. AET can also provide a sample program, which allows you to experiment with the off-line PIN unlock wizard.

3.4 Multiple language support

SafeSign Identity Client for MAC OS X 10.4 supports multiple languages.

The language of the Token Administration Utility depends on the system language.

3.5 Token Administration Utility

SafeSign Identity Client for MAC OS X 10.4 includes the Token Administration Utility for token management operations.

For general functionality of the Token Administration Utility, please refer to the SafeSign Identity Client Token Administration Utility User Guide for Windows.

¹ For SafeSign identity Client version 2.3 (release 2.3.0), the cards need to have support for logical channels.

4 Tested Configurations

SafeSign Identity Client Standard version 2.3 for MAC OS X 10.4 was tested with the smart cards, USB tokens, smart card readers, applications and Macintosh environments listed below.

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 10.4, as part of AET's Quality Assurance procedures. This does not imply that other tokens / readers (combinations) do not work.

4.1 SafeSign version

The version numbers of the components installed by SafeSign Identity Client Standard version 2.3 for MAC OS X 10.4, release 2.3.1, are:

Description	File name	File version
Java Card Handling Library	libaetjcss.dylib	2.3.0.5
PKCS #11 Cryptoki Library	libaetpkss.dylib	2.3.0.1444
Token Administration Utility	tokenadmin	2.3.0.18

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 2.3 for MAC OS X 10.4 comes in a standard version for the following environments:

- MAC OS X 10.4

4.3 Tokens

SafeSign Identity Client Standard version 2.3 for MAC OS X 10.4 supports the following tokens:

- STARCOS® smart cards developed by Giesecke & Devrient (G&D): SPK2.3 and STARCOS 3.0;
- The G&D StarKey100 (M) USB token with the completed STARCOS SPK 2.3 / 2.4 operating system;
- The G&D StarKey400 and StarKey400 M (with flash memory) USB token with Sm@rtCafé Expert 64k;
- Java Card v2.1.1 / Open Platform 2.0.1 compliant Java smart cards:
G&D Sm@rtCafé Expert 2.0, IBM JCOP20;
- Java Card v2.2+ / GlobalPlatform 2.1.1 compliant Java smart cards:
G&D Sm@rtCafé Expert 64, G&D Sm@rtCafé Expert 3.0, IBM JCOP41.

4.4 Smart Card Readers

SafeSign Identity Client Standard version 2.3 for MAC OS X 10.4 supports the following smart card readers and USB tokens:

- Omnikey CardMan Desktop USB 3121 (using the native CCID MAC OS X driver which is part of the operating system);
- G&D StarKey100 (M), StarKey400 (M) USB tokens (with the driver Driver-StarKey100_400-1.0-ppc.pkg.tar.gz);
- Gemplus GemPC Twin (using the native CCID MAC OS X driver which is part of the operating system).

4.5 Applications

SafeSign Identity Client Standard version 2.3 for MAC OS X 10.4 supports the following applications:

- Mozilla Firefox version 1.0.5.6, 2.0
- Mozilla Thunderbird version 1.0.5.5, 1.5.0.8

5 Installation

5.1 Installation Process

Note that users need to have sufficient privileges and basic knowledge of Mac OS X to install SafeSign for MAC OS X 10.4.



Note

Please note that AET strongly recommends using the native CCID MAC OS X driver which is part of the operating system, both on PowerPCs and Intel based Macintosh PCs.

1

Save the *SafeSign-Identity-Client-2.3.1 installer.dmg* file to a location on your MAC computer and double-click it.

This will result in an installer package called *SafeSign-Identity-Client-2.3.1*

➔ Click the file to install

2

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



Figure 2: Install SafeSign 2.0: Welcome to the SafeSign 2.0 Installer

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

➔ Note that SafeSign for MAC OS X will only run on MAC OS X 10.4 or up

3 The next window will display the SafeSign License Agreement:

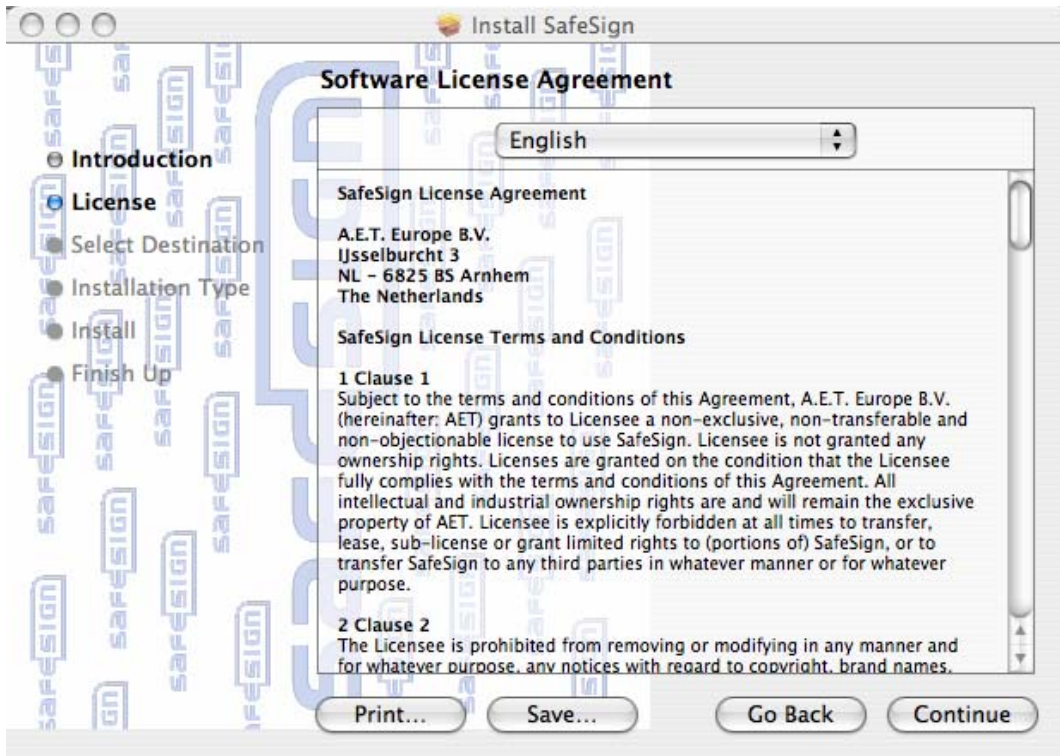


Figure 3: Install SafeSign: Software License Agreement

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.

4 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.

5

Upon clicking **Agree** to accept the terms of the Software License Agreement (in [Figure 4](#)), you will be asked to select a destination for SafeSign to be installed.

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

In our example, the destination volume will be the local hard disk (called 'OS X 10.4').

➔ Select the destination volume by clicking on it (as below):

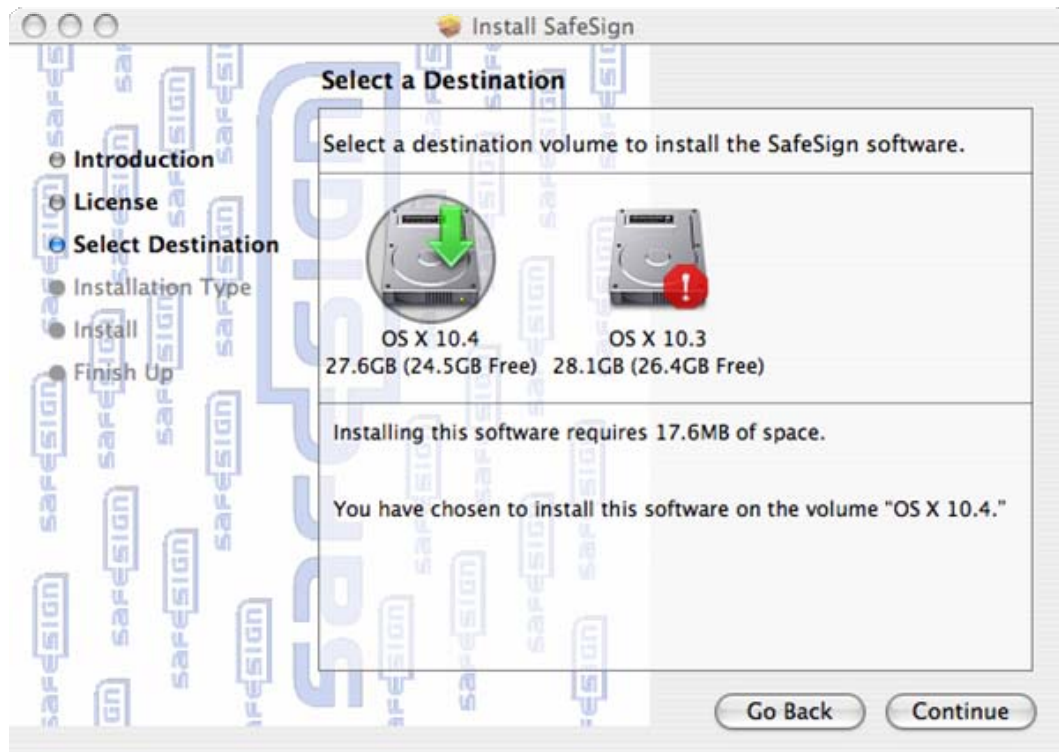


Figure 5: Select a Destination: Destination volume selected

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

6

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

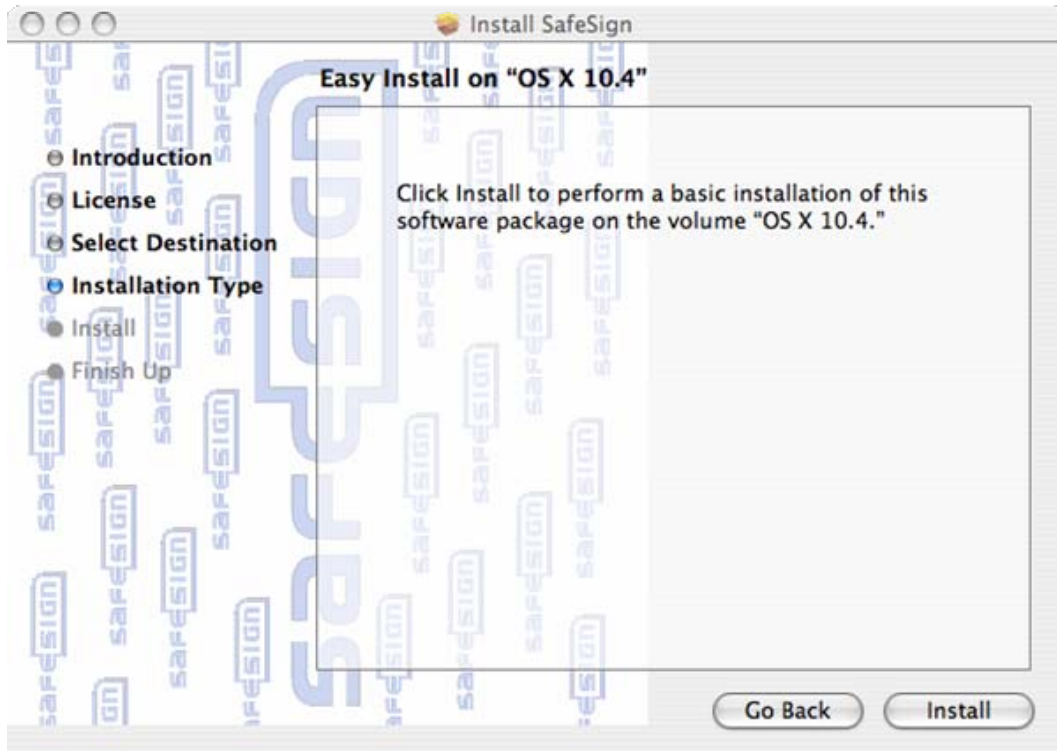


Figure 6: Install SafeSign: Easy Install

➔ Click **Install** to install SafeSign.



Note

*When SafeSign has already been installed before, you will be allowed to upgrade the installation, in which case instead of the button **Install**, there will be a button **Upgrade**.*

7

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



Figure 7: Easy Install: 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 will be installed.

You will be informed when the installation process is completed:

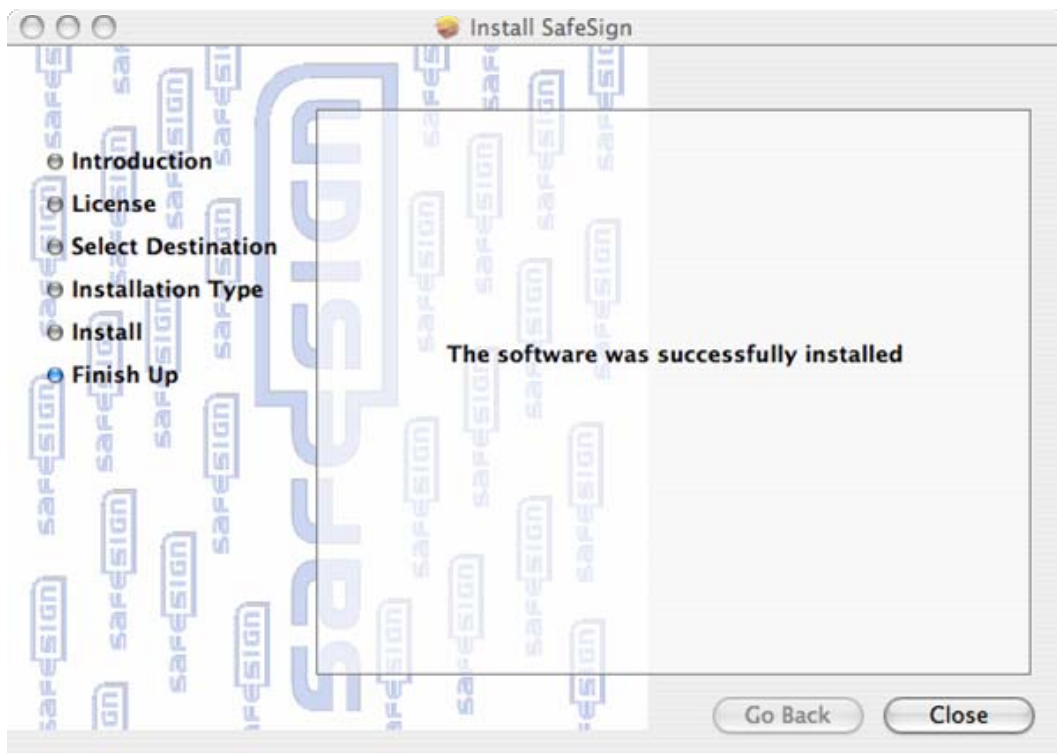


Figure 8: Install SafeSign: The software was successfully installed

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

5.2 Verify installation

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

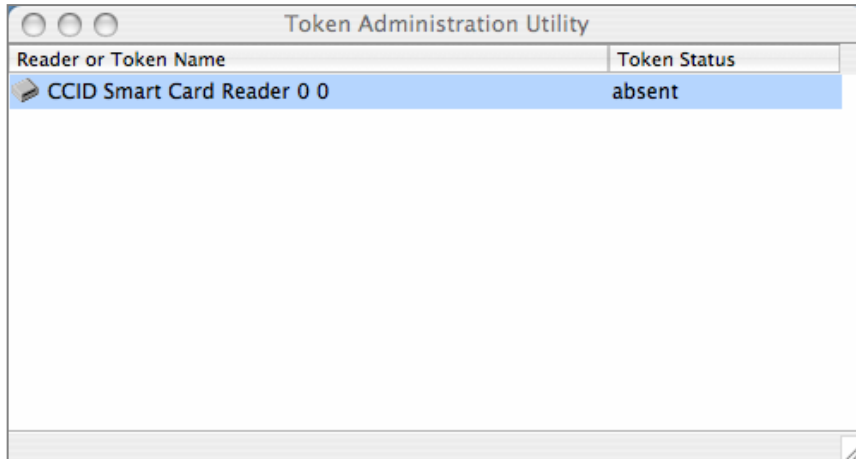


Figure 9: Token Administration Utility: CCID Smart Card Reader

Note that 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):

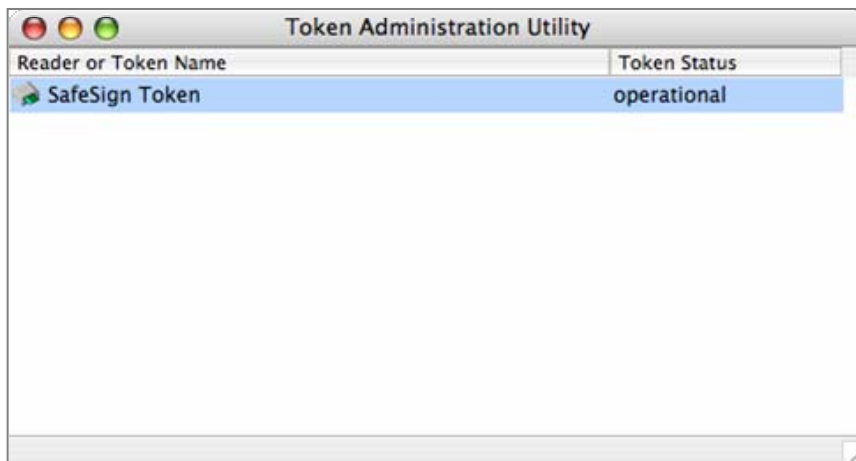


Figure 10: Token Administration Utility: SafeSign Token

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 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.

In order to do so, you should install or "load" the SafeSign Identity Client PKCS #11 library as a security module in these applications¹.

6.1 Firefox

1

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

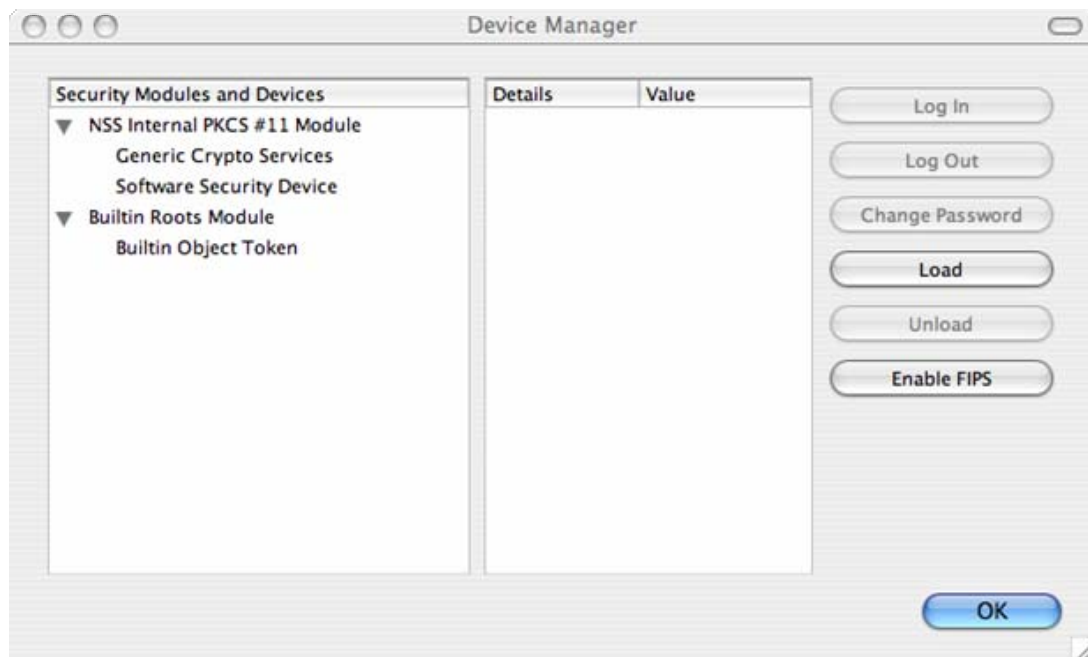


Figure 11: Firefox Device Manager: Security Modules and Devices

The SafeSign 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:

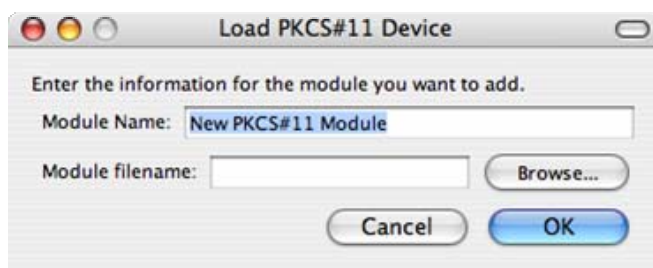


Figure 12: Firefox Device Manager: Load PKCS#11 Device

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 13: Firefox Device Manager: Load SafeSign

→ Click **OK**

4

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

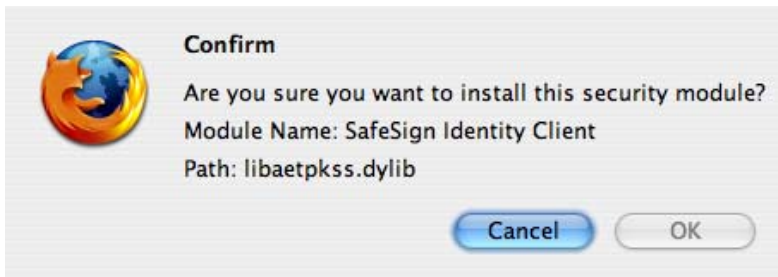


Figure 14: Firefox Device Manager: Are you sure you want to install this security module?

→ Click **OK** to continue installation

5

You will be informed when the module is successfully loaded:



Figure 15: Firefox 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 Firefox:

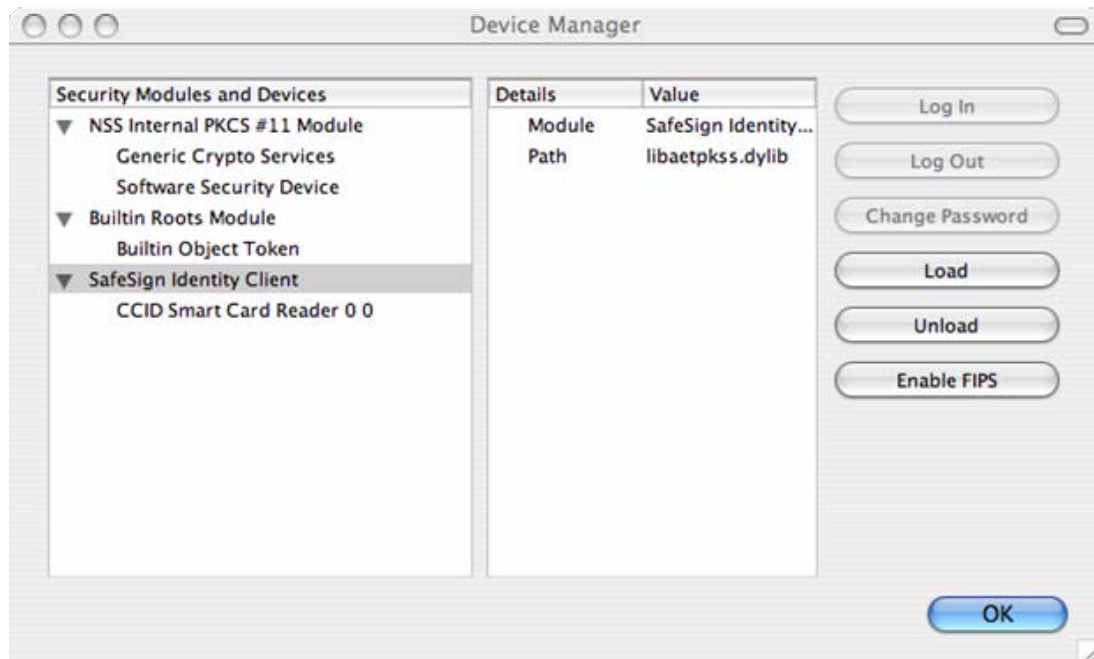


Figure 16: Firefox Device Manager: SafeSign Security Module

Under the name of the security module ('SafeSign Identity Client', as specified in [Figure 13](#)), 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 17: 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 token in Firefox for such operations as web authentication, where you will be asked to select a device and enter the PIN:

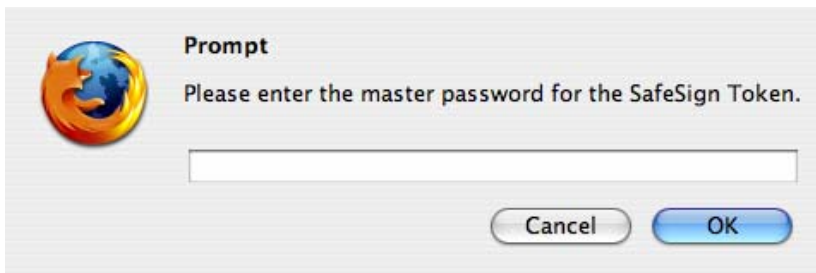


Figure 18: Firefox: Prompt



Installation Fails

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



Figure 19: 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:

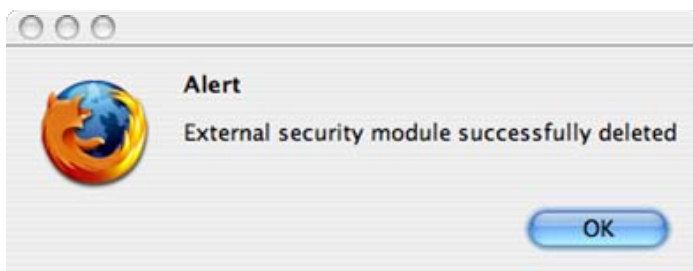


Figure 20: Firefox: External security module successfully deleted

6.2 Thunderbird

1

In Thunderbird, go to **Thunderbird > Preferences > Privacy > Security > Security Devices:**

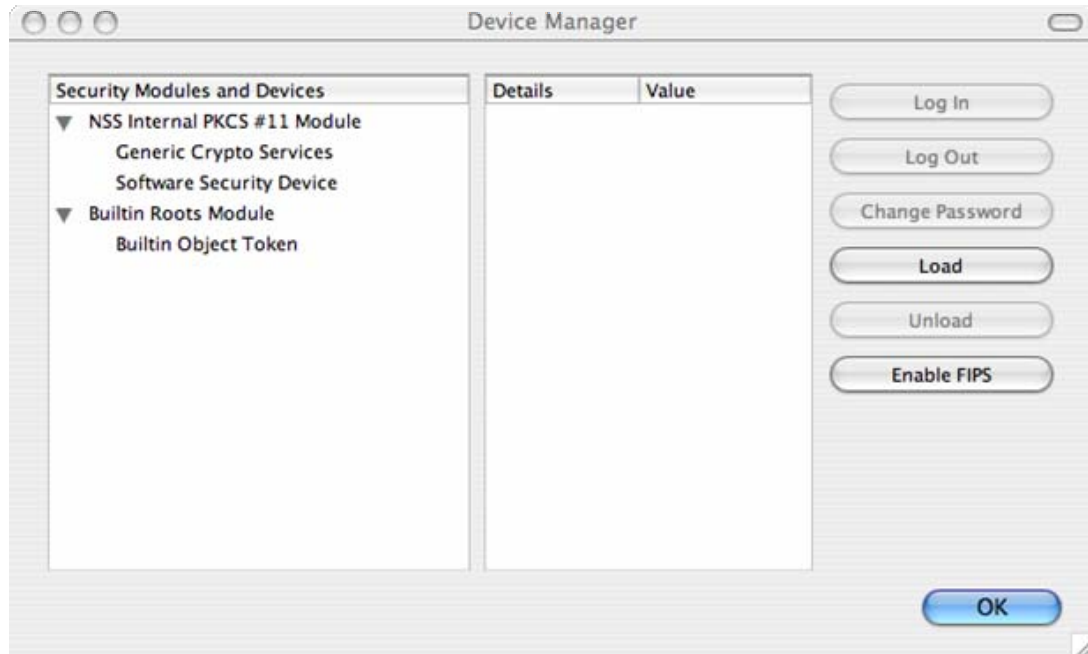


Figure 21: Thunderbird Device Manager: Security Modules and Devices

The SafeSign 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:

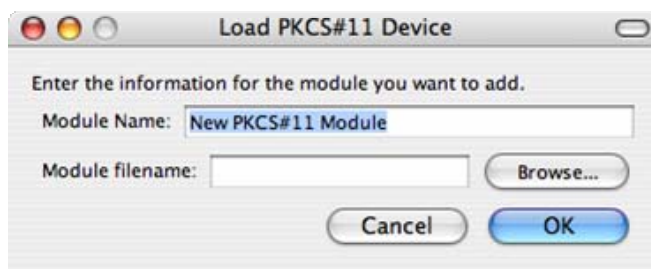


Figure 22: Thunderbird Device Manager: Load PKCS#11 Device

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 23: Thunderbird Device Manager: Load SafeSign

→ Click **OK**

4

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



Figure 24: Thunderbird 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 25: Thunderbird 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 Thunderbird:

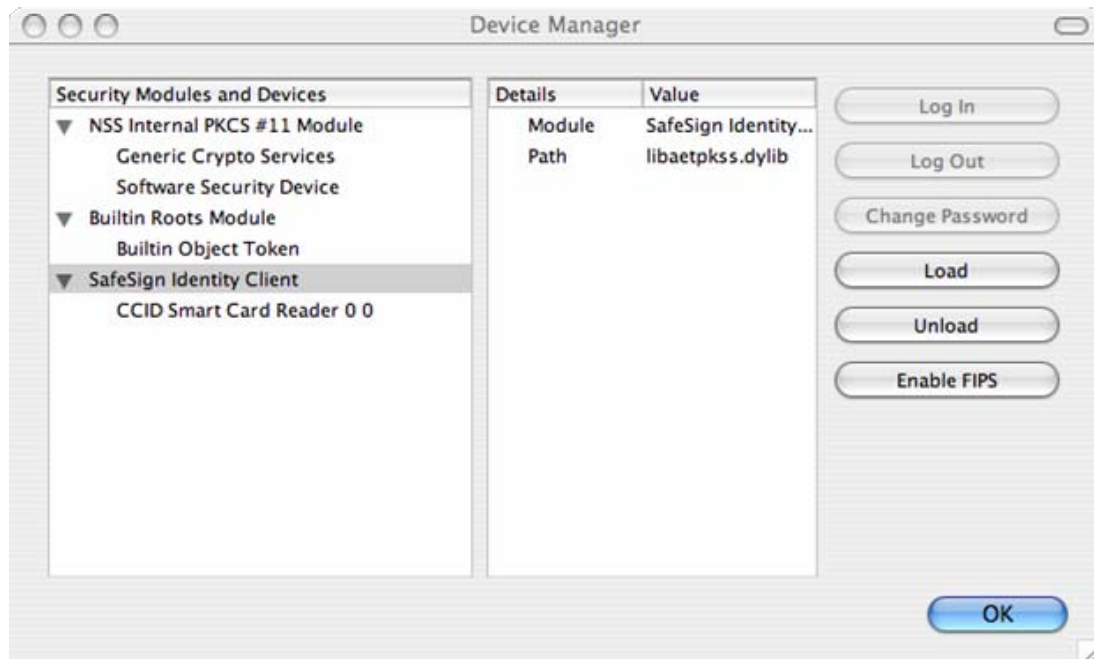


Figure 26: Thunderbird Device Manager: SafeSign Security Module

Under the name of the security module ('SafeSign Identity Client', as specified in [Figure 23](#)), 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 27: Thunderbird 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 token in Thunderbird for such operations as web authentication, where you will be asked to select a device and enter the PIN:

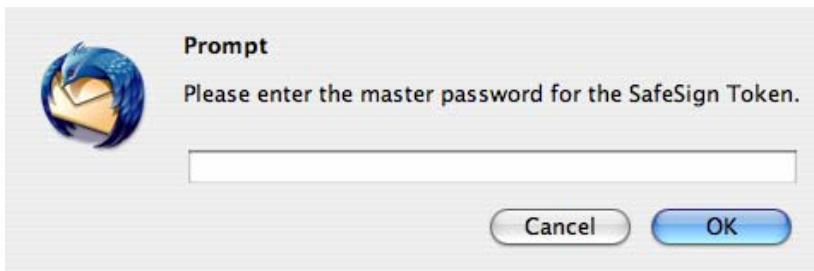


Figure 28: Thunderbird: Prompt



Installation Fails

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

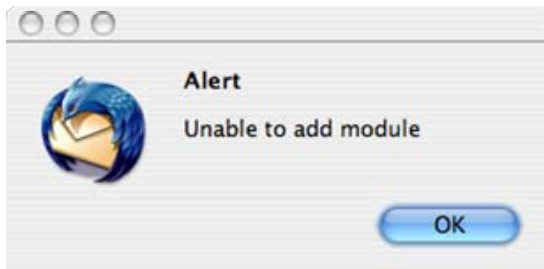


Figure 29: Thunderbird: Unable to add module

➔ 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:

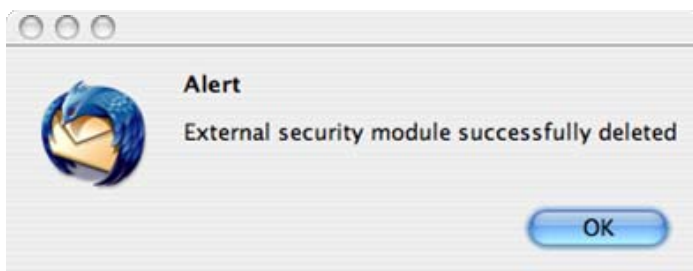


Figure 30: Thunderbird: External security module successfully deleted

7 Known Issues

1. Note that it may not be possible to initialise more than one (blank, i.e. with no SafeSign applet installed) Java Card 2.2+ card at a time. Even though the first card may be initialised without problems, the second card may fail (with a device error or 'Contact AET Support' error). Closing the Token Utility and restarting it, will initialise the same card without problems. This happens with all smart card readers tested and seems to be caused by changes that were made in the CCID / PCSC layer of MAC OS X 10.4.8. This issue has been seen to occur on Power MACs, not on Intel MACs. Note that when the SafeSign PKI applet is installed on the token, this problem does not occur.
2. It is recommended to use the native CCID smart card reader driver included in MAC OS X 10.4, rather than installing the smart card reader drivers provided by the smart card reader supplier.
3. Note that users of Intel based Macintosh computers must not install smart card reader drivers that are not Universal Binaries, as installing these drivers will corrupt the smart card subsystem.
4. Tests have shown that the driver for the StarKey100 and StarKey400 USB token is not very stable and may present problems with token detection and initialisation.
5. SafeSign Identity Client version 2.3 for MAC OS X includes only a Token Administration Utility, no Token Management Utility.
6. Note that SafeSign Identity Client version 2.3 for MAC OS X can be used with / on MAC OS X 10.4 only.
7. In the Token Administration Utility, the Task Manager is not available.

Appendix 1: How to remove smart card reader drivers

AET recommends using the native CCID driver included in MAC OS X 10.4, for reasons of stability. If you have installed smart card reader driver's from your smart card reader manufacturer, you can remove / uninstall these.

CardMan 3121

Select 'Go to Folder' and then `/usr/libexec/SmartCardServices/drivers/` and locate the file 'ifdokcm3121_macos_2.2.0.bundle'.

Move this file to trash and then restart the computer. After restarting the computer, the Token Administration Utility will display 'CCID Smart Card Reader' (instead of 'OMNIKEY CardMan 3121').

StarKey100 / StarKey400

Select 'Go to Folder' and then `/usr/local/pcsc/drivers/` and locate the file 'ifd-ePs2k.bundle'.

Move this file to trash and then restart the computer. After restarting the computer, the Token Administration Utility will no longer display 'FT SCR2000'.