

Product Description

SafeSign Identity Client Standard Version 2.3 for SuSE 10.0

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.

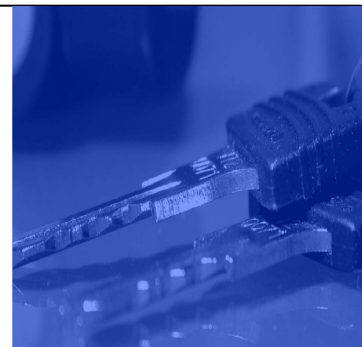
IJsselburcht 3
NL-6825 BS
P.O. Box 5486
NL-6802 EL Arnhem
The Netherlands
Tel. +31-26-365 33 50
Tel. Support +31-26-365 35 43
Fax +31-26-365 33 51



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 version 2.3 for SuSE 10.0

Document ID: SafeSign-IC-Standard_2.3_SuSE-10.0_Product_Description

Project Information: SafeSign Identity Client Release Documentation

Document revision history

Version	Date	Author	Changes
1.0	24-08-2006	Drs. C.M. van Houten	First edition for SafeSign Identity Client Standard Version 2.3 for SuSE 10.0 (release 2.3.0)
1.1	24-11-2006	Drs. C.M. van Houten	Edited for SafeSign Identity Client Standard Version 2.3 for SuSE 10.0 (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 SuSE 10.0 Functionality	1
3 Features	2
3.1 Multi-token support	2
3.2 Support for PIN / PUK of 15 characters	2
3.3 Multiple language support	2
3.4 Token Management Utility / Token Administration Utility	2
4 Tested Configurations	3
4.1 Installation files	3
4.2 PC/SC lite	3
4.3 Operating System	3
4.4 Tokens	4
4.5 Smart Card Readers	4
4.6 Applications	4
5 Installation	5
5.1 Installation Process	5
5.1.1 YaST	5
5.1.2 Terminal	6
5.2 Verify installation	6
6 Installation of SafeSign Security Module	8
6.1 Firefox	8
6.2 Thunderbird	12
7 Known Issues	16

List of Figures

Figure 1: SafeSign Installation: Install Package with YaST.....	5
Figure 2: SafeSign Installation: Install Package with Konsole.....	6
Figure 3: Token Administration Utility: CCID Smart Card Reader.....	6
Figure 4: Token Administration Utility: SafeSign Token	7
Figure 5: Firefox Device Manager: Security Modules and Devices.....	8
Figure 6: Firefox Device Manager: Load PKCS#11 Device.....	8
Figure 7: Firefox Device Manager: Load SafeSign	9
Figure 8: Firefox Device Manager: Are you sure you want to install this security module?	9
Figure 9: Firefox Device Manager: A new security module has been installed	9
Figure 10: Firefox Device Manager: SafeSign Security Module	10
Figure 11: Firefox Device Manager: Token inserted	10
Figure 12: Firefox: Prompt	11
Figure 13: Firefox: Unable to add module	11
Figure 14: Firefox: External security module successfully deleted.....	11
Figure 15: Thunderbird Device Manager: Security Modules and Devices.....	12
Figure 16: Thunderbird Device Manager: Load PKCS#11 Device.....	12
Figure 17: Thunderbird Device Manager: Load SafeSign	13
Figure 18: Thunderbird Device Manager: Are you sure you want to install this security module?.....	13
Figure 19: Thunderbird Device Manager: A new security module has been installed	13
Figure 20: Thunderbird Device Manager: SafeSign Security Module	14
Figure 21: Thunderbird Device Manager: Token inserted	14
Figure 22: Thunderbird: Prompt	15
Figure 23: Thunderbird: Unable to add module	15
Figure 24: Thunderbird: External security module successfully deleted.....	15

About the Document

This product description defines the features and supported configurations of SafeSign Identity Client Standard for SuSE 10.0 and that were tested by its developer A.E.T. Europe B.V. and describes its installation process.

1 Introduction

SafeSign Identity Client for SuSE 10.0 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 SuSE 10.0 that allows the user to generate and store public and private data on a personal token.

2 SafeSign Identity Client for SuSE 10.0 Functionality

SafeSign Identity Client for SuSE 10.0 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.

RPM packages for installation on the SuSE 10.0

Token Management Utility / 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 SuSE 10.0 (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;
- Multiple language support;
- Token Management Utility / Token Administration Utility.

3.1 Multi-token support

SafeSign Identity Client version 2.3 for SuSE 10.0 supports multiple tokens.

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

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 Multiple language support

SafeSign Identity Client for SuSE 10.0 supports multiple languages.

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

3.4 Token Management Utility / Token Administration Utility

SafeSign Identity Client for SuSE 10.0 includes the Token Management Utility and/or Token Administration Utility for token management operations (provided in two separate RPM packages).

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

4 Tested Configurations

SafeSign Identity Client Standard version 2.3 for SuSE 10.0 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 SuSE 10.0, as part of AET's Quality Assurance procedures. This does not imply that other tokens / readers (combinations) do not work.

4.1 Installation files

The complete installation package for SafeSign Identity Client version 2.3 for SuSE 10.0 comprises of:

- **pcsc-lite-1.2.9-7.i586.rpm** or **pcsc-lite-devel-1.2.9-7.i586.rpm**: pcscd is the daemon program for PC/SC Lite. It is a resource manager that coordinates communications with Smart Card readers and Smart Cards that are connected to the system. The purpose of PCSC Lite is to provide a Windows[®] SCard interface in a very small form factor for communicating to smartcards and readers. PCSC Lite uses the same winscard api as used under Windows[®]. This package was tested to work with A.E.T. Europe SafeSign. This package is supported by A.E.T. Europe B.V. when used in combination with SafeSign.
- **safesign-javacard-2.3.1-1.i586.rpm**: Enables the use of Java Card 2.1.1+ smart cards with SafeSign Identity Client cryptographic middleware.
- **safesign-pkcs11-2.3.1-2.i586.rpm**: Enables the use of smart cards in PKCS #11 enabled applications, such as web browsers (Netscape, Mozilla and Firefox), e-mail clients (Thunderbird, Mozilla Mail and Netscape Mail) and various other applications such as VPN clients.
- **safesign-tokenmanager-2.3.1-1.i586.rpm** or **safesign-tokenadmin-2.3.1-1.i586.rpm**: The Token Management Utility / Token Administration Utility allows you to initialise and manage cryptographic tokens supported by the SafeSign Identity Client middleware.

4.2 PC/SC lite

SafeSign Identity Client Standard Version 2.3 for SuSE 10.0 includes an AET enhanced Linux PC/SC daemon, which was especially developed to improve the performance and stability of the Linux PC/SC daemon (as available from the MUSCLE site) and thus the stability of the SafeSign PKCS #11 Library.



Important Note

Use of the AET PC/SC daemon is a requirement to qualify for support of SafeSign Identity Client Version 2.3 for SuSE 10.0.

4.3 Operating System

SafeSign Identity Client Standard version 2.3 for SuSE 10.0 comes in a standard version for the following environments:

- SuSE 10.0

4.4 Tokens

SafeSign Identity Client Standard version 2.3 for SuSE 10.0 has been tested to support the following tokens:

- STARCOS[®] smart cards developed by Giesecke & Devrient (G&D): SPK2.3, STARCOS 3.0;
- 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.

4.5 Smart Card Readers

SafeSign Identity Client Standard version 2.3 for SuSE 10.0 supports the following smart card readers and USB tokens:

- Omnikey CardMan Desktop USB 3121 (using the Linux driver, version 2.6.0, provided by Omnikey);

4.6 Applications

SafeSign Identity Client Standard version 2.3 for SuSE 10.0 supports the following applications:

- Mozilla Firefox version 1.0.5.6
- Mozilla Firefox version 1.0.8
- Mozilla Thunderbird version 1.0.5.5

5 Installation

5.1 Installation Process



Note

Note that users need to have sufficient privileges and basic knowledge of Linux / SuSE 10.0 to install SafeSign for SuSE 10.0.

Note that previous installation of SafeSign (packages) on SuSE 10.0 should be de-installed first, before installing the latest RPM packages.

To prevent problems with discrepancies in the registry, users should execute the following command in their home directory after upgrading SafeSign: `rm -rf ~/.safesign`

The next time a SafeSign component is used, the system registry from `/etc/safeSign/registry` will be automatically copied.

After saving the installation packages to a location on your computer, there are two basic ways of installing them:

1. Using YaST;
2. Using a Terminal.

5.1.1 YaST

When clicking on one of the RPM packages, you will get information on the content of the package.

You can then choose to use YaST to install the package, by clicking on **Install Package with YaST**:

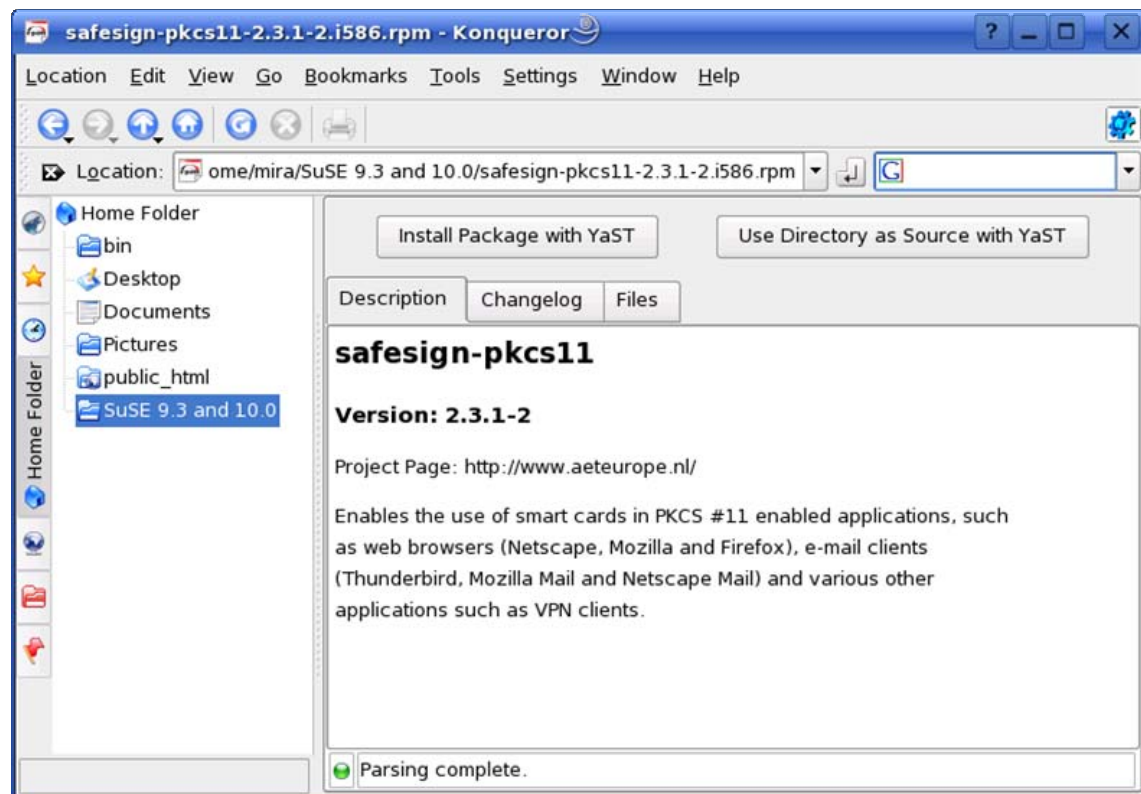


Figure 1: SafeSign Installation: Install Package with YaST

Follow the instructions given to install the package (the SafeSign PKCS #11 Library, in this case) and repeat the same steps for the other SafeSign installation packages (paragraph 4.1).

5.1.2 Terminal

You can install the SafeSign installation packages with a terminal (Konsole in our example), using the following commands:

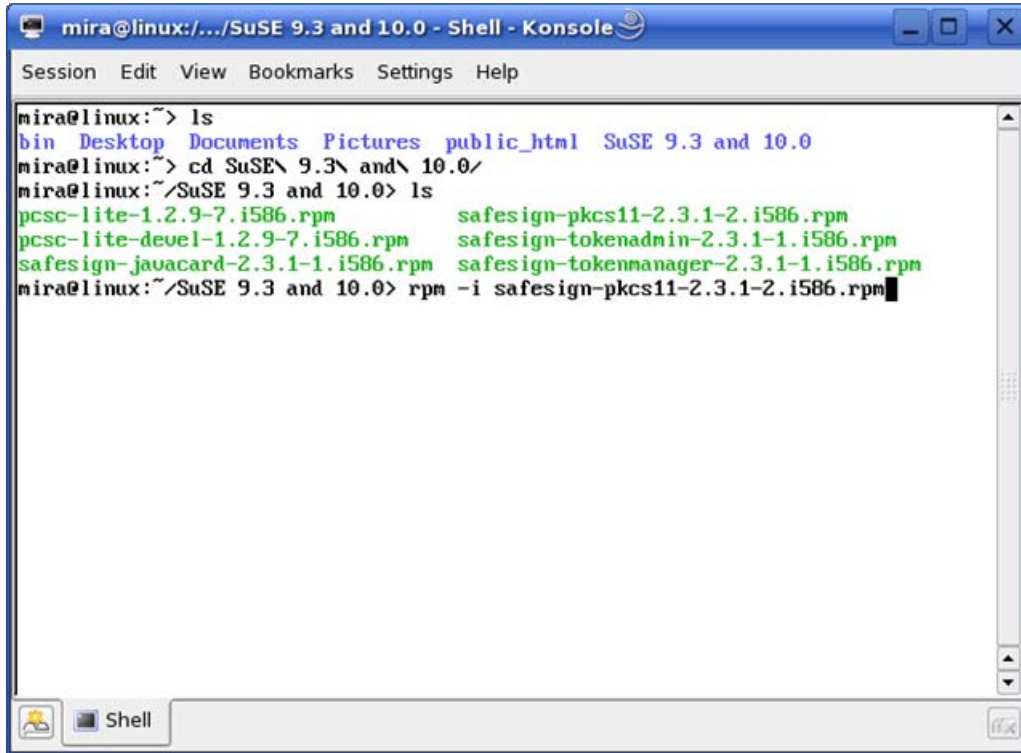


Figure 2: SafeSign Installation: Install Package with Konsole

Repeat the same steps for the other SafeSign installation packages (paragraph [4.1](#)).

5.2 Verify installation

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

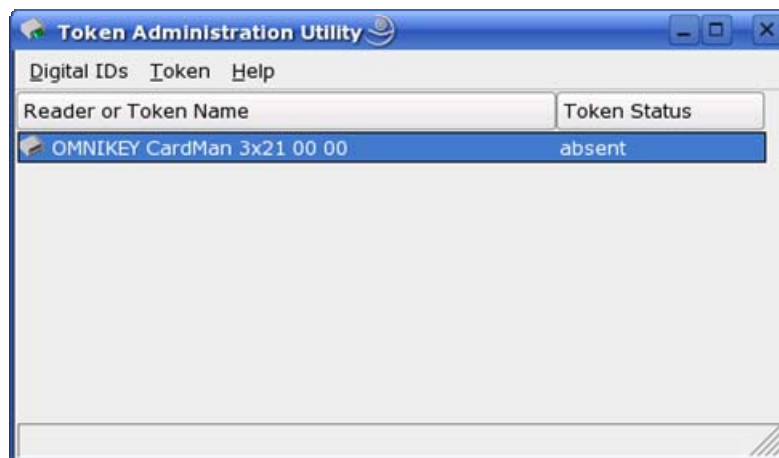


Figure 3: Token Administration Utility: CCID Smart Card Reader

Note that the Omnikey CardMan 3121 USB reader (drivers) have been installed.

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):

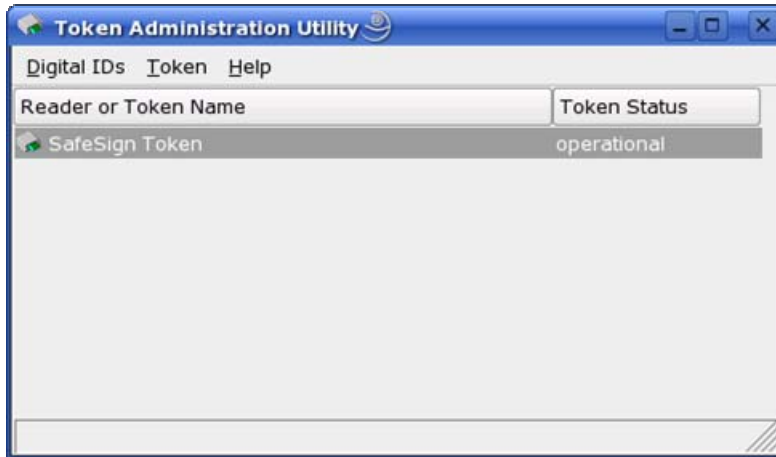


Figure 4: Token Administration Utility: SafeSign Token

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**:

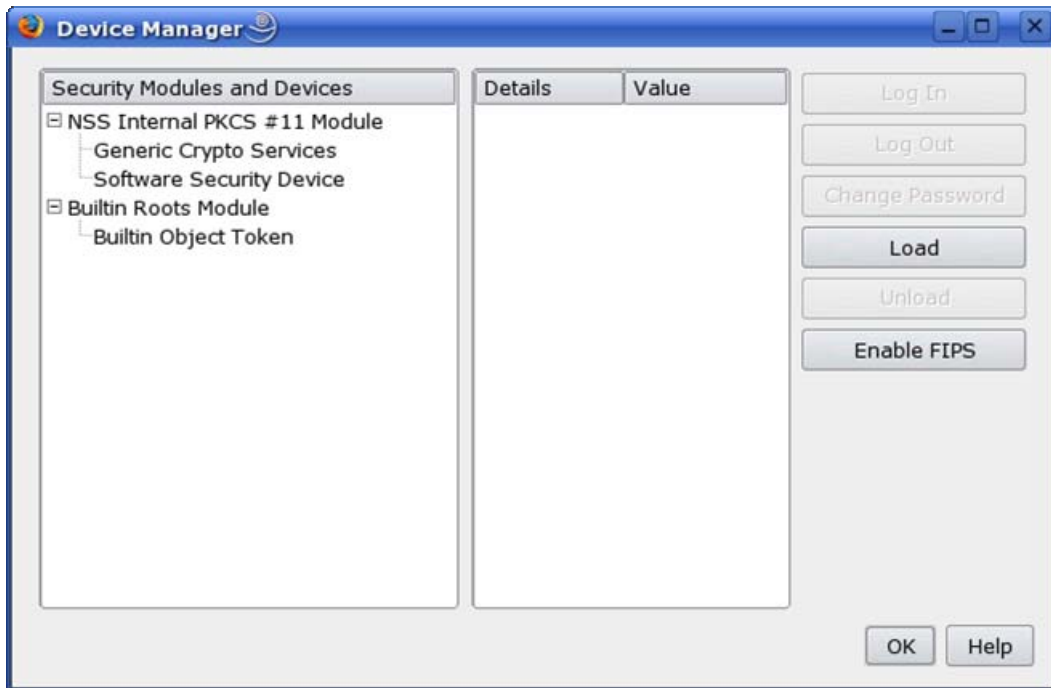


Figure 5: Firefox Device Manager: Security Modules and Devices

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:

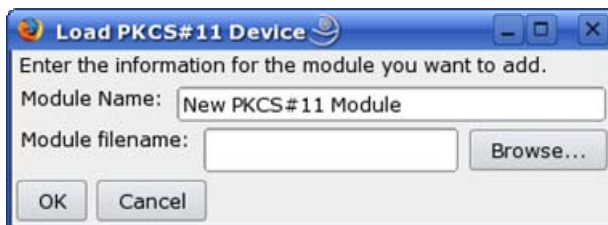


Figure 6: Firefox Device Manager: Load PKCS#11 Device

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.so*):



Figure 7: Firefox Device Manager: Load SafeSign

- Click **OK**

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



Figure 8: 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 9: 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:

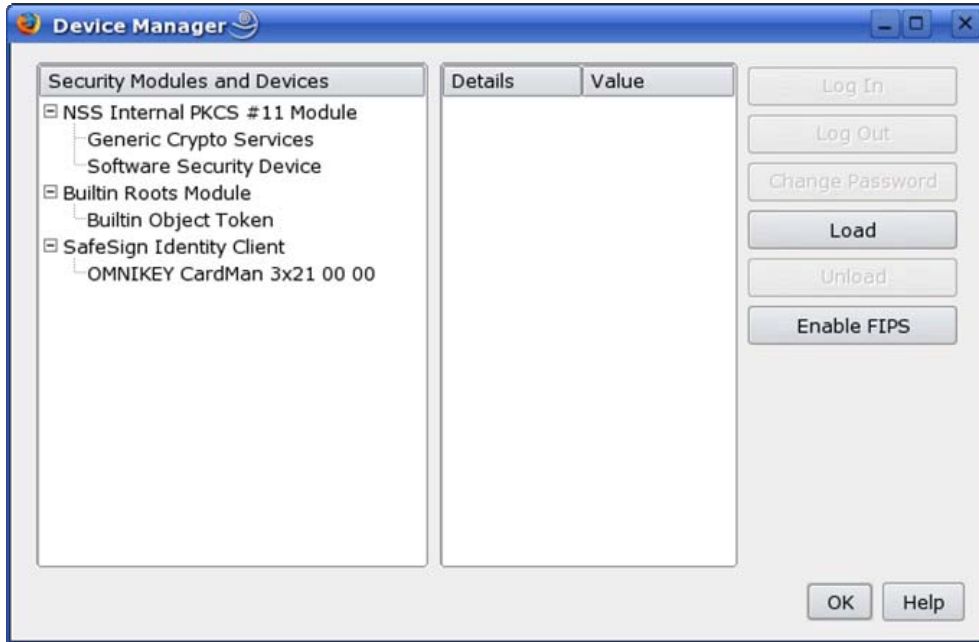


Figure 10: Firefox Device Manager: SafeSign Security Module

Under the name of the security module ('SafeSign Identity Client', as specified in [Figure 7](#)), 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:

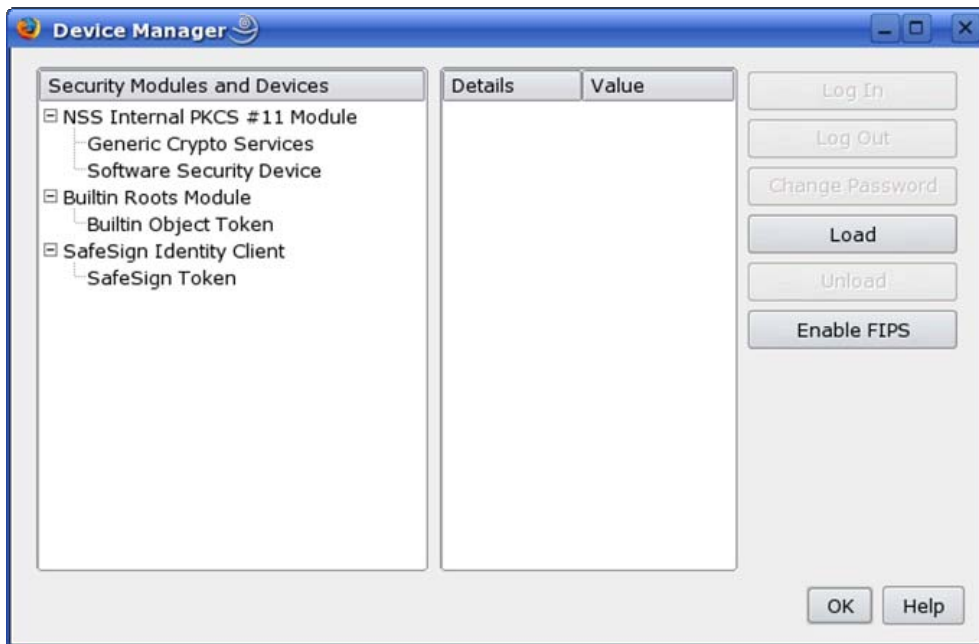


Figure 11: Firefox Device Manager: Token inserted

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 12: 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:

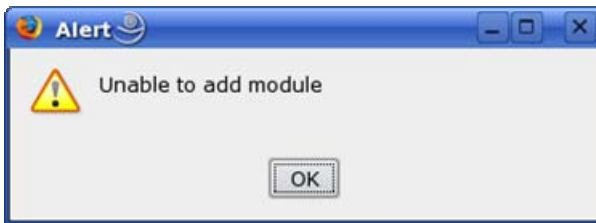


Figure 13: Firefox: Unable to add module

➔ Verify that you have provided the correct name, i.e. *libaetpkss.so* (located in */usr/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:

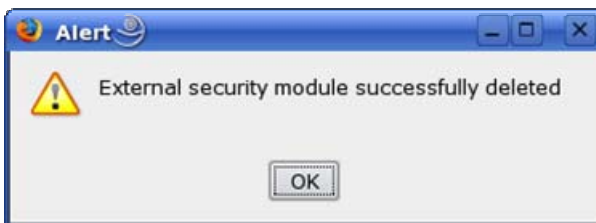


Figure 14: Firefox: External security module successfully deleted

6.2 Thunderbird

1

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

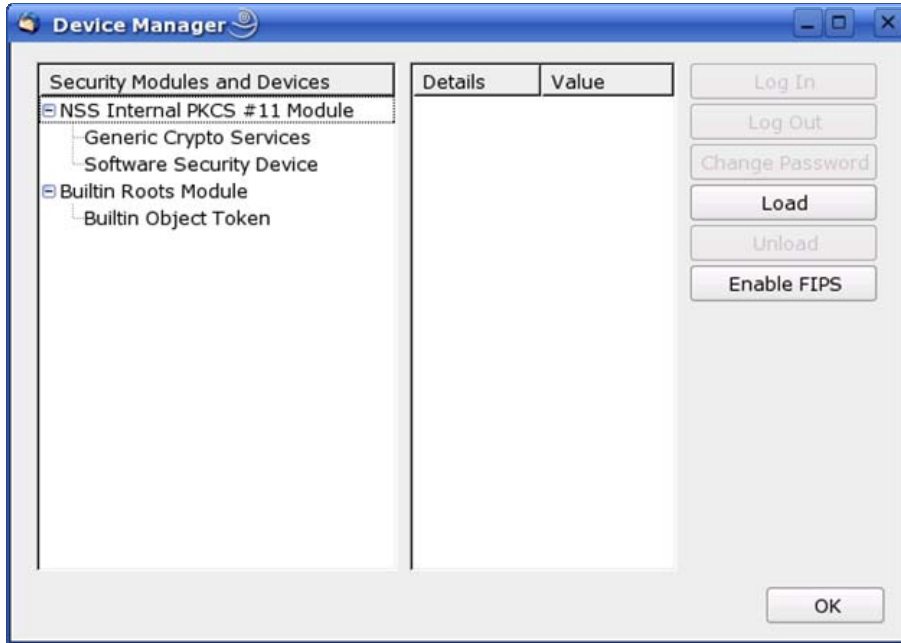


Figure 15: Thunderbird Device Manager: Security Modules and Devices

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 16: 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.so*):



Figure 17: Thunderbird Device Manager: Load SafeSign

- Click **OK**

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

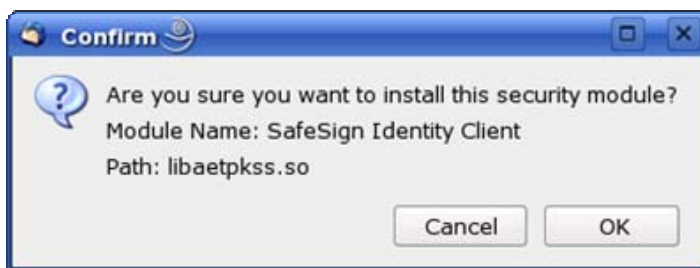


Figure 18: Thunderbird Device Manager: Are you sure you want to install this security module?

- Click **OK** to continue installation

- 5** You will be informed when the module is successfully loaded:

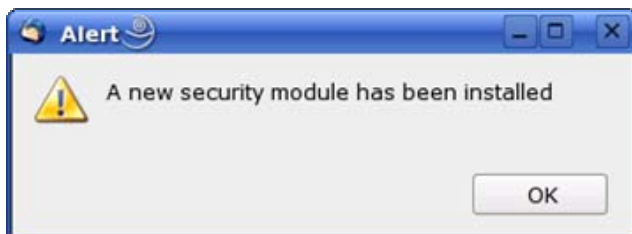


Figure 19: Thunderbird Device Manager: A new security module has been installed

- Click **OK**

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

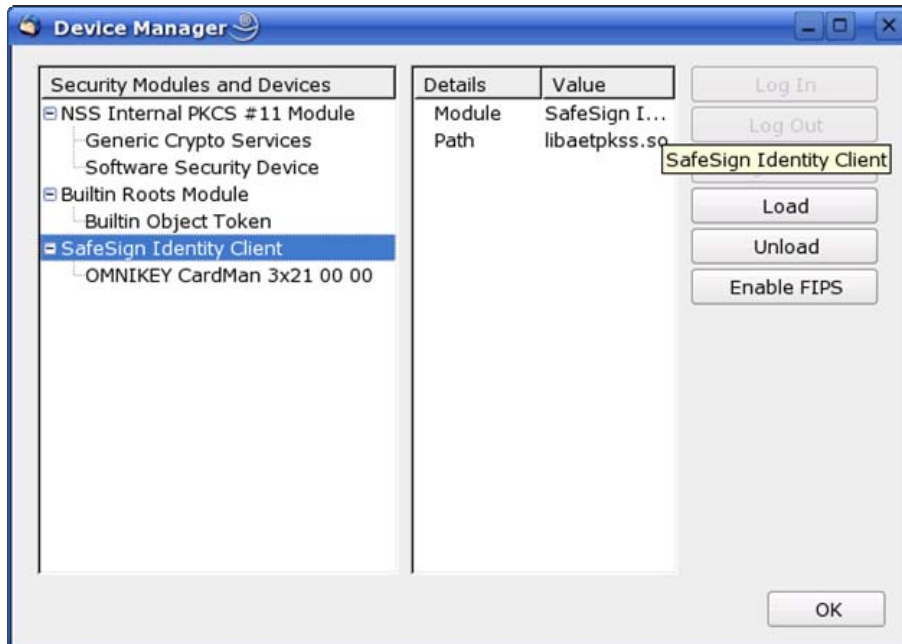


Figure 20: Thunderbird Device Manager: SafeSign Security Module

Under the name of the security module ('SafeSign Identity Client', as specified in [Figure 17](#)), 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:

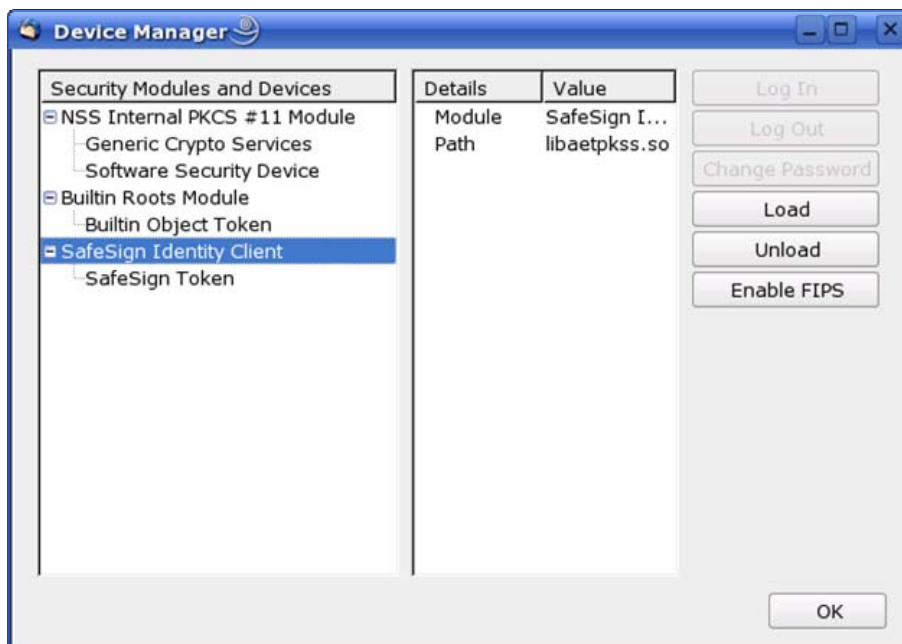


Figure 21: Thunderbird Device Manager: Token inserted

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 22: 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:

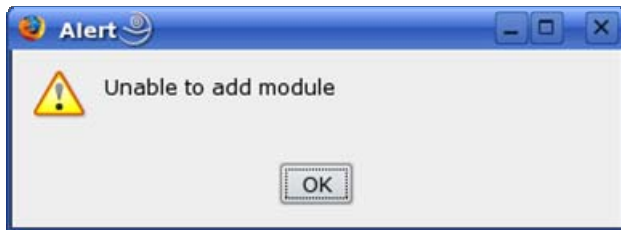


Figure 23: Thunderbird: Unable to add module

➔ Verify that you have provided the correct name, i.e. *libaetpkss.so* (located in */usr/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:

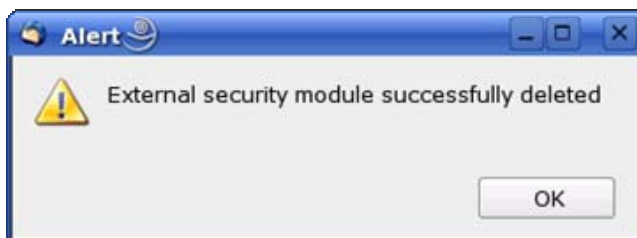


Figure 24: Thunderbird: External security module successfully deleted

7 Known Issues

1. You should use the driver package(s) supplied by Omnikey for the CardMan 3121 instead of the native CCID smart card reader driver. Note that driver version 2.6.0 should be used, as driver version 3.0.0 does not work.
2. Omnikey drivers are installed in the `/usr/local/pcsc/drivers` directory, however, SafeSign expects drivers to be available in `/usr/lib/pcsc/drivers`. Drivers should be installed / available in the last-mentioned directory to be able to work with SafeSign.
3. When using the GNOME desktop, in the *Show Token Objects* dialog, the option *Show Private Objects* is missing. This is not the case when using the KDE Desktop, therefore we recommend using the KDE Desktop.
4. In the Token Administration Utility, the Task Manager is not available.