Product Description

SafeSign Identity Client Standard

Version 3.0 for Linux

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

© 2009, A.E.T. Europe B.V., 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 - 2009.

All rights reserved.

8SafeSign 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 (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.

Copyright © 1997 - 2009 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_3.0_Linux_Product_Description**

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

Document revision history

Version	Date	Author	Changes
1.0	20-03-2009	Drs. C.M. van Houten	First edition for SafeSign Identity Client Standard Version 3.0 for Linux

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 Linux Functionality 1

3 Features 2

3.1 Multi-token support 2

4 Tested Configurations 3

4.1 SafeSign Identity Client version 3
4.2 Operating System 3
4.3 Tokens 4
4.4 Smart Card Readers 4
4.5 Applications 4

5 Installation 5

5.1 Installation Process 5
5.2 Verify installation 6

6 Installation of SafeSign Identity Client Security Module 7

6.1 Iceweasel / Firefox 7
6.2 Icedove / Thunderbird 11

7 Known Issues 15

List of Figures

Figure 1: tokenadmin: Version Information 3
Figure 2: Package Installer: safesignidentityclient 5
Figure 3: Package Installer: Installation finished 5
Figure 4: Terminal: tokenadmin 6
Figure 5: Token Administration Utility: SafeSign Token 6
Figure 6: Device Manager: Security Modules and Devices 7
Figure 7: Device Manager: Load PKCS#11 Device 7
Figure 8: Device Manager: Load SafeSign 8
Figure 9: Device Manager: Are you sure you want to install this security module? 8
Figure 10: Device Manager: A new security module has been installed 8
Figure 11: Device Manager: SafeSign Security Module 9
Figure 12: Device Manager: Token inserted 9
Figure 13: Prompt 10
Figure 14: Unable to add module 10
Figure 15: External security module successfully deleted 10
Figure 16: Device Manager: Security Modules and Devices 11
Figure 17: Device Manager: Load PKCS#11 Device 11
Figure 18: Device Manager: Load SafeSign 11
Figure 19: Device Manager: Are you sure you want to install this security module? 12
Figure 20: Device Manager: A new security module has been installed 12
Figure 21: Device Manager: SafeSign Security Module 12
Figure 22: Device Manager: Token inserted 13
Figure 23: Prompt 13
Figure 24: Unable to add module 13
Figure 25: External security module successfully deleted 14

About the Document

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

1 Introduction

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

2 SafeSign Identity Client for Linux Functionality

SafeSign Identity Client for Linux 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.
Token Administration Utility to initialise the token, change PIN, etc.

3 Features

In principle, SafeSign Identity Client Standard Version 3.0 for Linux supports all the features of SafeSign Identity Client version 3.0 for Windows, if such functionality is available for the Linux platform.

3.1 Multi-token support

SafeSign Identity Client version 3.0 for Linux supports multiple tokens.

Newly supported tokens in SafeSign Identity Client Standard Version 3.0 are:

- NXP JCOP21 v2.3.1 (Java Card 2.2.1 smart card)
- NXP JCOP31 v2.3.1 (Java Card 2.2.1 smart card)
- NXP JCOP41 v2.3.1 (Java Card 2.2.1 smart card
- Siemens CardOS 4.3B 32K/64K

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 for Linux was tested with the smart cards, USB tokens, smart card readers, applications and Linux distributions 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 Linux, as part of AET's Quality Assurance procedures.

Note that this does not imply that all tested tokens / readers (combinations) work flawlessly, or 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 Linux, release 3.0, are:

Description	File name	File version
Java Card Handling Library	libaetjcss.so	3.0.1785
PKCS #11 Cryptoki Library	libaetpkss.so	3.0.1785
Token Administration Utility	tokenadmin	3.0.1785

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

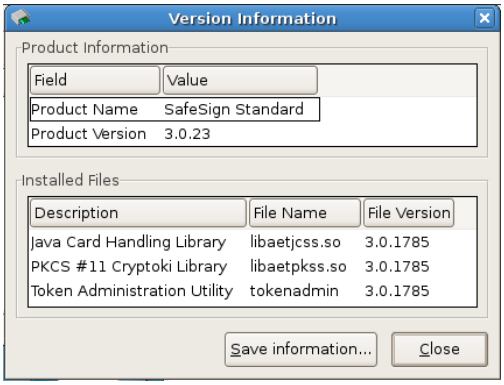

Figure 1: tokenadmin: Version Information

4.2 Operating System

SafeSign Identity Client Standard version 3.0 for Linux comes in (separate) versions for the following Linux distributions:

- Debian 4.0
- Ubuntu 8.04
- Fedora 9
- FreeBSD 6.1
- OpenSuSE 11.0
- SuSe Desktop Enterprise Edition 10 sp2

4.3 Tokens

SafeSign Identity Client Standard version 3.0 for Linux supports the following tokens:

- STARCOS® smart cards and USB tokens developed by Giesecke & Devrient (G&D), including STARCOS 3.0;
- Sm@rtCafé smart cards and USB tokens developed by Giesecke & Devrient (G&D), including Sm@rtCafé Expert 64k;
- Java Card v2.1.1 / Open Platform 2.0.1 compliant Java smart cards;
- Java Card v2.2+ / GlobalPlatform 2.1.1 compliant Java smart cards, including JCOP21, JCOP41 and the CrypToken MX2048-JCOP USB Token;
- CardOS smart cards developed by Siemens: CardOS 43B.

4.4 Smart Card Readers

SafeSign Identity Client Standard version 3.0 for Linux supports the following smart card readers and USB tokens:

- CrypToken MX2048-JCOP USB token (using the native Linux CCID driver which is part of the operating system);
- Gemplus GemPC Twin (using the native CCID MAC OS X driver which is part of the operating system);
- Omnikey CardMan Desktop USB 3121 (using the native Linux CCID driver which is part of the operating system).

4.5 Applications

SafeSign Identity Client Standard version 3.0 for Linux supports the following applications:

- Mozilla Firefox version 3.0.5
- Mozilla Thunderbird version 2.0.0.19
- Iceweasel Web Browser version 3.0.5 (Debian only)
- Icedove Mail Client version 2.0.0.19 (Debian only)

5 Installation

5.1 Installation Process

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

Note

Please note that AET strongly recommends using the native Linux CCID driver which is part of the operating system.

1 Save the installation file to a location on your computer and select to have your Package Installer install it.

In our example below, we will use the Debian Package Installer ("GDebi Package Installer"):

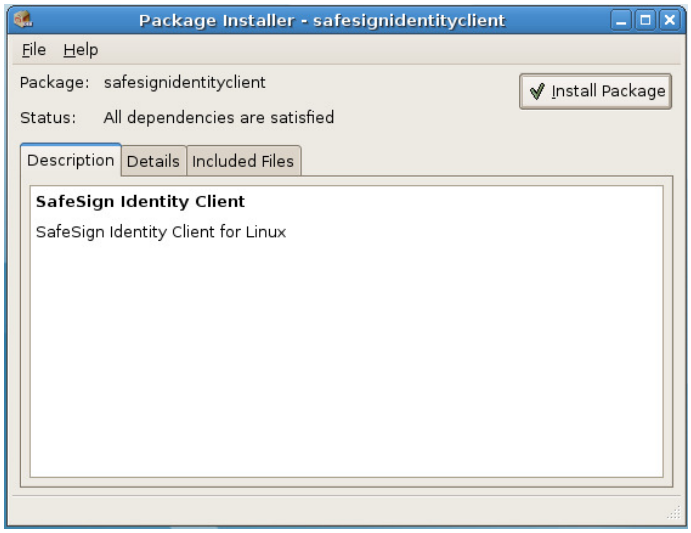

Figure 2: Package Installer: safesignidentityclient

➔ Click **Install Package**

2 When the installation is finished, you will be informed of this:

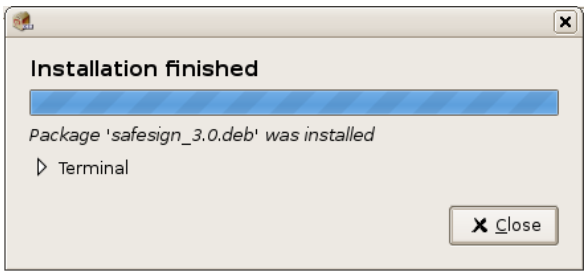

Figure 3: Package Installer: Installation finished

➔ Click **Close** to close the installer and finish the installation

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.

Open a Shell / Terminal and enter tokenadmin:

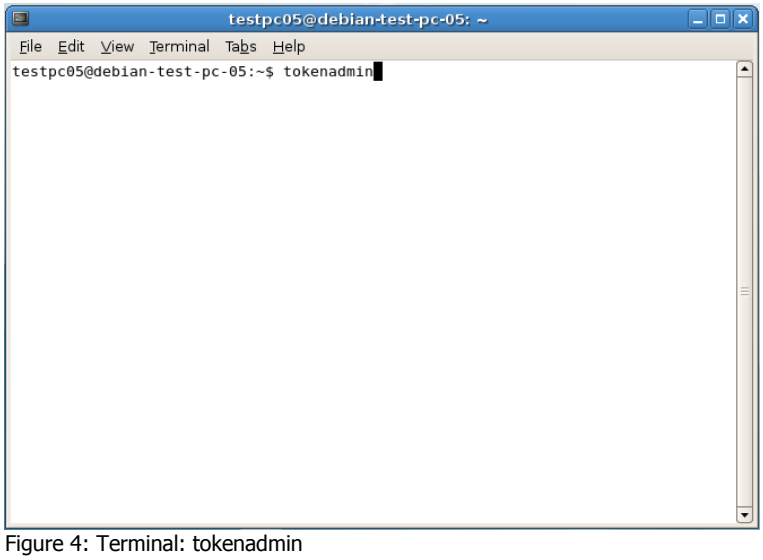

Figure 4: Terminal: tokenadmin

The Token Administration Utility will open.

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):

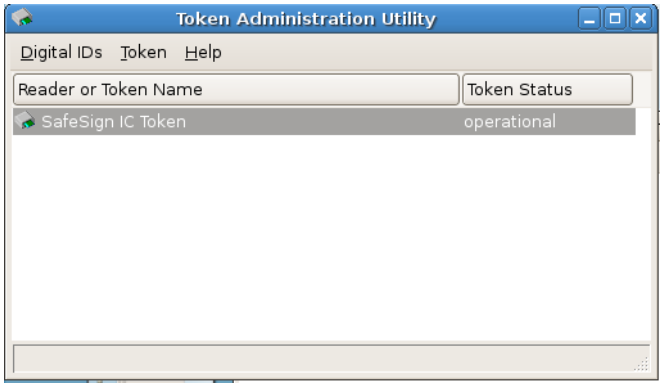

Figure 5: Token Administration Utility: SafeSign Token

Please note that the native Linux CCID smart card reader driver should be installed and that a CCID compliant smart card reader is attached.

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.

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].

In our example, we will install the SafeSign PKCS#11 Library as a security module in Iceweasel (Debian Only) / Firefox and in Icedove (Debian only) / Thunderbird.

6.1 Iceweasel / Firefox

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

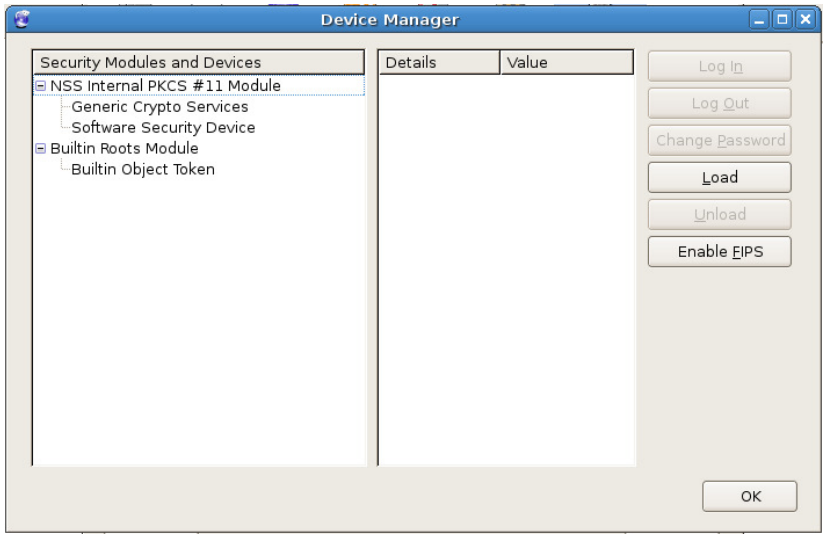

Figure 6: Device Manager: Security Modules and Devices

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:

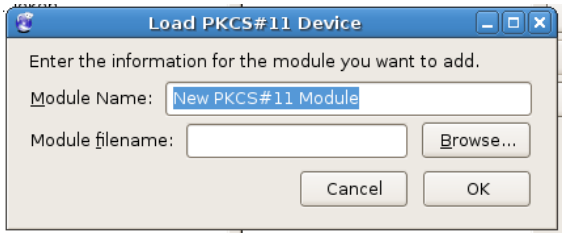

Figure 7: Device Manager: Load PKCS#11 Device

[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 8: Device Manager: Load SafeSign

➔ Click **OK**

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

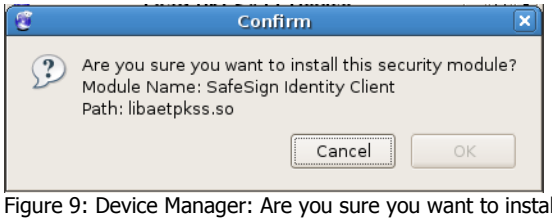

Figure 9: Device Manager: Are you sure you want to install this security module?

➔ Click **OK** to continue installation

5 You will be informed when the module is successfully installed:

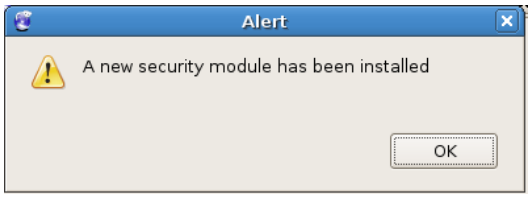

Figure 10: Device Manager: A new security module has been installed

➔ Click **OK**

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

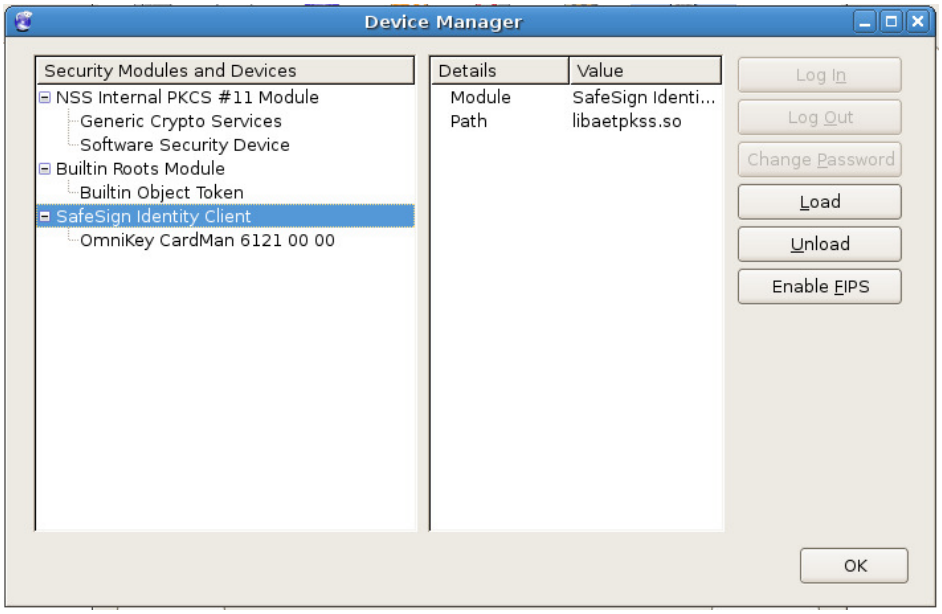

Figure 11: Device Manager: SafeSign Security Module

Under the name of the security module ('SafeSign Identity Client', as specified in Figure 8), the available devices are displayed.

In this case, there is only one device installed, a smart card reader identified by the label 'Omnikey CardMan 6121 00 00'. The token is not inserted in the reader.

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

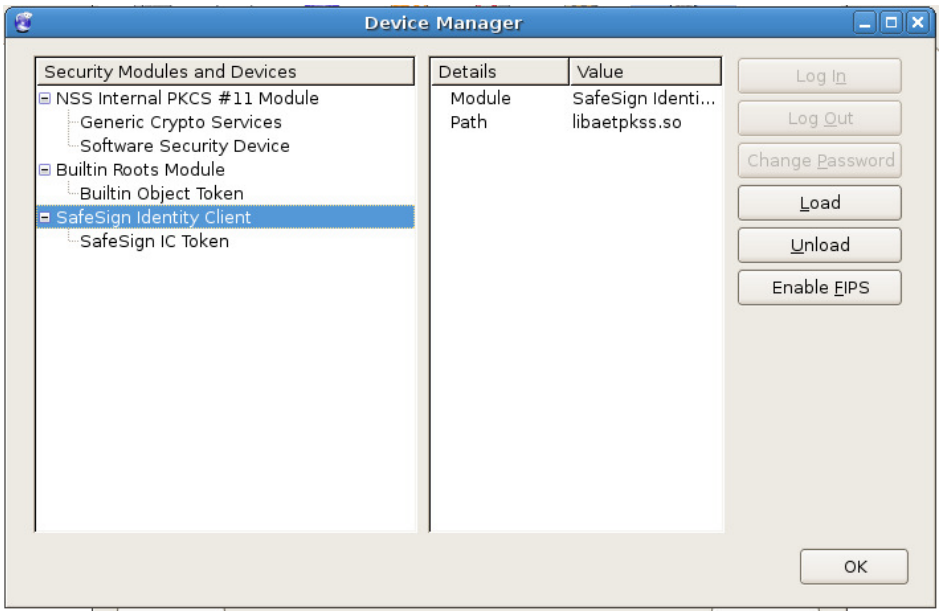

Figure 12: Device Manager: Token inserted

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 for such operations as web authentication, where you will be asked to select a device and enter the PIN:

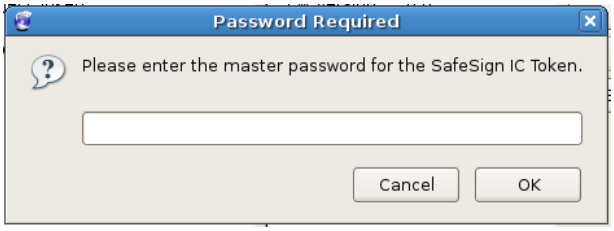

Figure 13: Prompt

Installation Fails

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

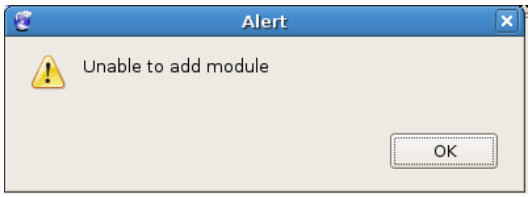

Figure 14: Unable to add module

➔ Verify that you have provided the correct name, i.e. *libaetpkss.so*

Delete Module

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

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

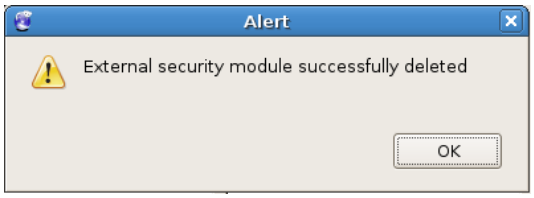

Figure 15: External security module successfully deleted

6.2 Icedove / Thunderbird

1 In Icedove, go to **Edit > Preferences > Security > Security Devices**:

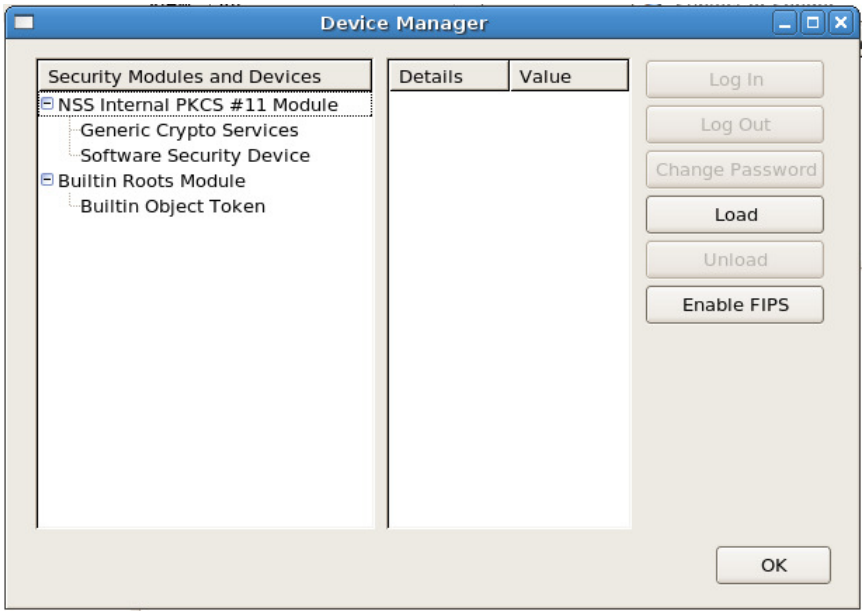

Figure 16: Device Manager: Security Modules and Devices

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:

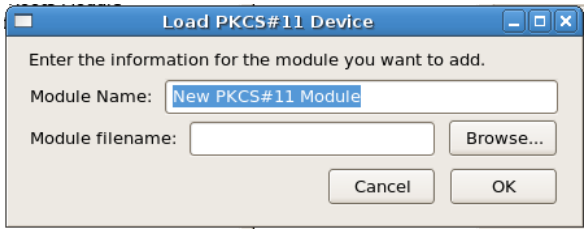

Figure 17: Device Manager: Load PKCS#11 Device

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):

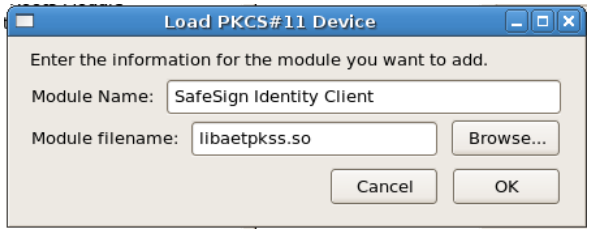

Figure 18: Device Manager: Load SafeSign

➔ Click **OK**

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

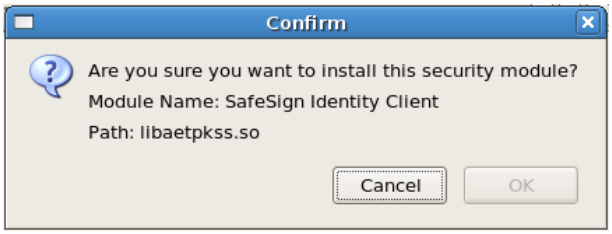

Figure 19: Device Manager: Are you sure you want to install this security module?

➔ Click **OK** to continue installation

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

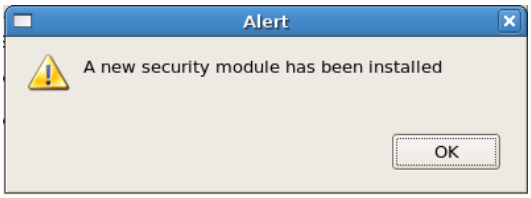

Figure 20: Device Manager: A new security module has been installed

➔ Click **OK**

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

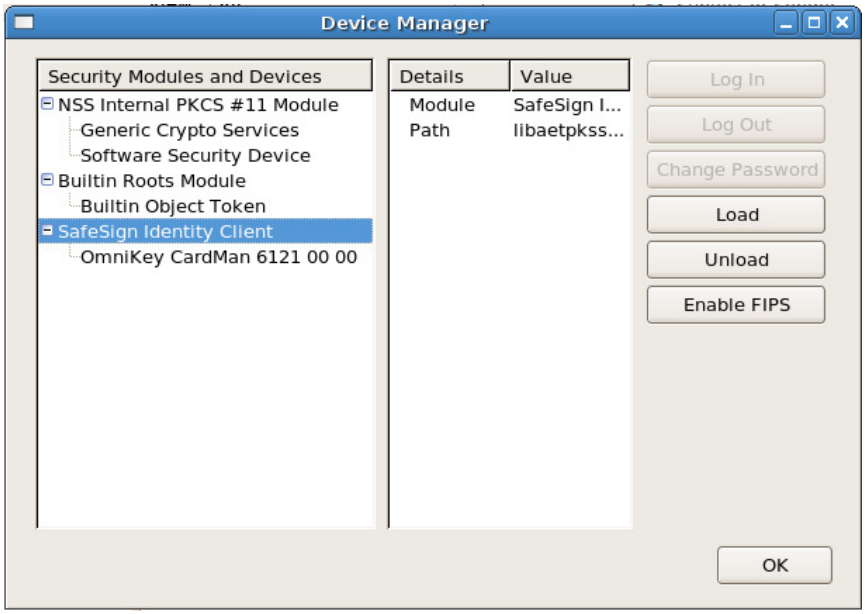

Figure 21: Device Manager: SafeSign Security Module

Under the name of the security module ('SafeSign Identity Client', as specified in Figure 18), the available devices are displayed.

In this case, there is only one device installed, a smart card reader identified by the label 'OmniKey CardMan 6121 00 00'. No token is inserted in the reader.

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

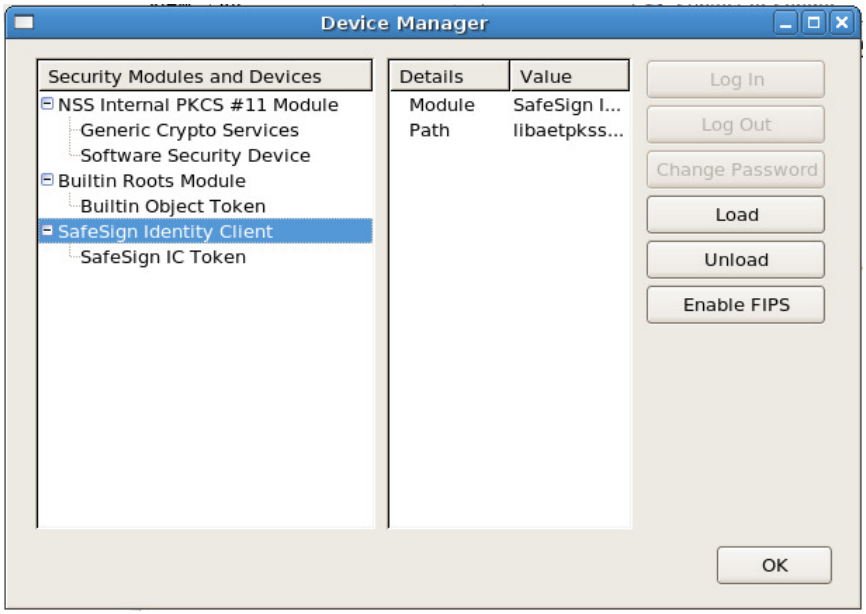

Figure 22: Device Manager: Token inserted

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 Icedove for such operations as web authentication, where you will be asked to select a device and enter the PIN:

Figure 23: Prompt

Installation Fails

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

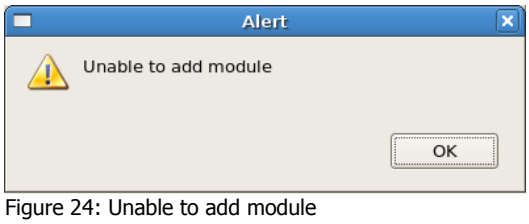

Figure 24: Unable to add module

➔ Verify that you have provided the correct name, i.e. *libaetpkss.so*

Delete Module

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

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

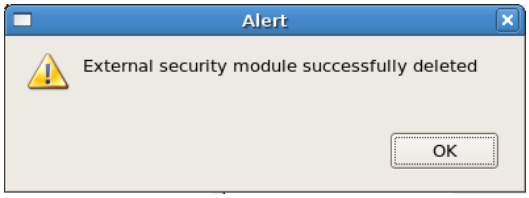

Figure 25: External security module successfully deleted

7 Known Issues

1. In general, it is recommended to use the native CCID smart card reader driver included in Linux, rather than installing the smart card reader drivers provided by the smart card reader supplier. Refer to the list of smart card readers tested for more information.
2. SafeSign Identity Client version 3.0 for Linux includes only a Token Administration Utility, no Token Management Utility.
3. In the Token Administration Utility, the Task Manager is not available.
4. Note that removal and re-insertion events are not detected (for example in the Token Administration Utility or in Mozilla applications), when the USB token and/or smart card reader is inserted or removed after the application is started. It is not possible from a PKCS#11 perspective to have readers and/or tokens appearing and disappearing on the fly (even if this is detected on PC/SC level).