aet

SafeSign Identity Client Standard Version 3.8

Release Document for Linux

Table of Contents

Table of Figures

Warning Notice

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). "

Document Information

Document ID: SafeSign IC Standard Version 3.8 Release Document for Linux

Project Information: SafeSign IC Release Documentation

Document revision history:

Version	Date	Author	Changes
1.0	05 August 2022	Drs. C.M. van Houten	First version for SafeSign IC Standard Version 3.8 for Linux; release 3.8.0.0

Document approval:

Version	Date	Name	Function
1.0	05 August 2022	Dr. A. Jeckmans	Chief Technical Officer

WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE

About the Product

This competent all-rounder in terms of strong authentication, integration and compatibility gives you complete freedom and flexibility. Once rolled out, SafeSign Identity Client (IC) serves as the perfect guard for IT security and enables unlimited possibilities for securing your IT infrastructure.

SafeSign IC offers the most comprehensive support available on the market for (card) operating systems, smart cards, USB tokens, languages and functions. This means you have sustainable and permanent freedom of choice when it comes to manufacturer independence.

SafeSign IC enforces two- or multi factor authentication/logon to the network, client PC or application, requiring the end user to have both the USB token or smart card (something you have) and a Personal Identity Number (something you know). USB tokens and smart cards are physically and logically tamper-resistant, ensuring that the end user's digital credentials can not be copied, modified or shared. Authentication based on smart cards or USB tokens provides the highest degree of security.

SafeSign IC is available for both fixed and mobile devices like desktops, servers, laptops, tablets and smart phones. SafeSign IC is also found in Thin Clients, printers or any other devices requiring authentication.

1   About this Document

The aim of this document is to document the status of the release of SafeSign Identity Client Standard version 3.8 for Linux (henceforth referred to as "SafeSign IC Standard version 3.8 for Linux").

This document is part of the release documentation of SafeSign IC and is intended to be a reference to both end users and administrators.

2   Release Information

2.1   Deliverables

SafeSign IC Standard version 3.8 for Linux for is provided in a .deb file or .rpm file.

2.2   Date of Release

The date of the release is 5 August 2022.

2.3   Release Details

SafeSign IC Standard version 3.8 for Linux reflects the SafeSign IC product version numbering scheme, i.e. version number, build number and distribution number, which is reflected in the Version Information dialog of the Token Administration Utility.

> Note that the file versions of the components delivered with the release of SafeSign IC Standard version 3.8.0.0 do not necessarily have the name format '3.8.0.xxxx'.

Release version: Standard Release 3.8.0.0-AET.000		
Description	File Name	File Version
Java Card Handling Library	libaetjcss.so	3.9.5.1
PKCS #11 Cryptoki Library	libaetpkss.so	3.9.9.1
Dialog Library	libaetdlglib.so	3.7.17.1
Common Dialogs	libaetdlss.so	4.2.5.1
Token Administration Utility	tokenadmin	3.8.31.1

> Note that in the distribution number (AET.000), the prefix AET is unique and reserved for AET general releases only.

2.4   Release Documents

SafeSign IC Standard version 3.8 for Linux provides at least the following release documentation:

Document Name	Version
SafeSign Identity Client Standard Version 3.8 Release Document for Linux	1.0

3   Features

The following features are supported by SafeSign IC Standard version 3.8 for Linux:

1   Multiple Token Support
2   Multiple Smart Card Reader Support
3   Multiple Application Support
4   Multiple Language Support
5   Activate QSCD Card Support
6   RSA 4096 Keys Support

These features are described in the following paragraphs.

3.1   Multiple Token Support

SafeSign IC Standard version 3.8 for Linux supports an large number of smart cards and tokens, as listed in section 7.

No new smart card and tokens are supported, but SafeSign IC Standard version 3.8 now includes support for RSA 4096 keys on JCOP 4 QSCD. See section 3.6.

3.2   Multiple Smart Card Reader Support

SafeSign IC Standard version 3.8 for Linux supports the use of PCSC 2.0 Class 1 smart card readers.

Note that a correct operation of a smart card reader depends on correctly working reader drivers.

> Note that SafeSign IC Standard will install the dependencies it requires when necessary (such as libccid), but we assume that otherwise, the Linux distribution is fully up-to-date, with the latest packages installed.

SafeSign IC Standard version 3.8 for Linux has been tested to support a number of smart card readers, as listed in section 8.

See section 3.6 with regard to smart card readers and extended APDU.

3.3   Multiple Application Support

SafeSign IC Standard version 3.8 for Linux supports applications on Linux that work through PKCS #11.

SafeSign IC Standard version 3.8 for Linux supports a number of applications, that provide the following functionality:

- Web authentication

- Email signing and encryption

- Document signing

SafeSign IC Standard version 3.8 for Linux has been tested to support a number of applications, as listed in section 9.

3.4   Multiple Language Support

SafeSign IC Standard version 3.8 for Linux supports a number of different languages.

Although your Linux distribution is set to the English language by default, you can choose a different language to use.

You can set language options in the appropriate Language Support settings menu of your Linux distribution.

Section 10 lists the languages that SafeSign IC Standard version 3.8 for Linux supports.

3.5   Activate QSCD Card Support

In accordance with the (European) eIDAS Regulation and related standards for cryptographic modules, the legitimate user / signatory of a Qualified Signature Creation Device (QSCD) is reponsible for activating the card (keys), i.e. to change the state of the card (keys) from non-operational to operational.

The SafeSign IC Token Administration Utility offers users of a QSCD the possibility to activate their card. When a QSCD is inserted in the smart card reader, the SafeSign IC middleware will enable the user to activate the card, based on the presence of the Common Criteria (CC) certified SafeSign IC applet and the card specific ATR. If these conditions are met, the Token menu of the SafeSign IC Token Administration Utility will display the option 'Activate Card'.

> Note that the activation process for a particular card may be very specific. It may require the user to:
> - authenticate to the card by entering the PIN (UZI-pas 3, SafeSign QSCD);
> - change the Transport PIN set for the card (Defensiepas 3);

SafeSign IC Minidriver version 3.8 supports the following QSCD cards:

- Defensiepas 3[1]
- UZI-pas 3[2]
- SafeSign Default / Generic QSCD (JCOP 3)
- UZI-pas 4
- QSCD on JCOP 4

---

[1] Defensiepas 3 is supported from SafeSign IC Minidriver version 3.5.4.0 onwards.

[2] UZI-pas 3 is supported from SafeSign IC Minidriver version 3.5.6.1 onwards.

3.5.1　Menu

On Ubuntu as well as on Red Hat, when using an HID OMNIKEY 3121 USB Smart Card Reader, the option 'Activate Card' may not be available. This is caused by the reader name being more than 64 bytes when C_GetSlotInfo is called. The workaround is to modify (shorten) the reader name (string) "HID Global OMNIKEY 3x21 Smart Card Reader" in the *Info.plist* file.

- In Ubuntu, this file is located in: /usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/.
- In Red Hat, this file is located in: /usr/lib64/pcsc/drivers/ifd.ccib.bundel/Contents/.

See also Known Issues section 5.2 and Extended APDU section 8.1.

3.6　RSA 4096 Keys Support

SafeSign IC Standard version 3.8 includes support for RSA 4096 keys.

For this functionality to be available, the following is required:

- A JCOP 4 card with the Common Criteria (CC) certified SafeSign IC applet
- A smart card reader that supports extended APDU

3.6.1　Extended APDU

An extended APDU is an APDU (command) with data and/or response of more than 256 bytes, as defined by ISO/IEC 7816-4.

Because sending extended APDUs can cause issues with readers / drivers that do not support it (such as the reader or drivers crashing), a whitelist is added in the registry with the names of the readers tested and supported, that indicates per reader what the maximum APDU size possible is. When your reader is not in the list, the use of extended APDU (and thus the use of RSA 4096 keys) is not possible.

The registry can be found here: */home/[user name]/.safesign*

The list can be found in the registry under:

HKEY_LOCAL_MACHINE\SOFTWARE\A.E.T. Europe B.V.\SafeSign\2.0\Readers\

⚠ These readers are verified by AET to work on all Operating Systems supported and must not be modified.

See also section 8.1.

4 New Features

SafeSign IC Standard version 3.8 for Linux has a number of new features.

Section 4.1 will describe the new features and functionality.

4.1 New

- Added support for RSA 4096 keys.
- Added support for extended APDU.
- Support for Ubuntu 22.04.

5   Known Issues

5.1   General

- The version of Firefox tested cannot handle a certificate that does not have a label. As a workaround, you can set a label on the keys and certificate in the Token Administration Utility's Show Token Objects dialog. Note that the 'EditLabelAction' is disabled by default in the registry.

- It is strongly advised not to use non-ASCII characters on Linux, which may or may not work on different Linux distributions.

- Adobe discontinued support for Adobe Reader for Linux, therefore, it is no longer available for download from the Adobe web site.

- On Ubuntu 22.04, the PC/SC daemon ('pcscd') is not started automatically. You need to start it manually.

- There is an issue with Firefox, that the SafeSign PKCS #11 module cannot be loaded in Firefox (through the FireFox Installer or manually) on Ubuntu 22.04. This is a known bug in the Snap version of Firefox: https://bugzilla.mozilla.org/show_bug.cgi?id=1734371 and https://bugs.launchpad.net/ubuntu/+source/firefox/+bug/1967632. As stated in the first link, "a satisfactory workaround does not exist" and Ubuntu / Mozilla should solve this. Uninstalling Firefox from Snap, downloading it manually and running it from there, seems to work.

5.2   SafeSign IC

- When you export a certificate from the token in the Token Administration Utility and then import it again to the same token, SafeSign IC will not recognise that the certificate already exists on the card, resulting in a duplicate certificate (with maybe a different name).

- It is not possible to set a PIN Timeout for the RIC Card, as this is not supported by the applet for the RIC Card.

- It is not possible to enrol a 1024 bit key pair on the RIC Card, as this is not supported (it is possible to generate a 2048 bits key pair).

- The PUK is not encrypted / protected by secure messaging during initialization, as by design. When the PUK is changed or used to authenticate, it will be encrypted.

- In languages other than English, some items in the Version Information dialog are not translated (e.g. Build number, Distribution number and the names of the Secure Messaging libraries).

- On Ubuntu as well as on Red Hat, the applet version and/or information on secure messaging being enabled, as well as the option to activate a card is not shown in the *Token Information* dialog for a G&D StarSign Crypto USB-Token (with ICP-Brazil certified applet) and a HID OMNIKEY 3121 USB Smart Card Reader. This is caused by the reader name being more than 64 bytes when C_GetSlotInfo is called. The workaround is to modify (shorten) the reader name (string) in the 'Info.plist' file, from from 'Giesecke & Devrient GmbH StarSign Crypto USB Token S' to e.g. 'G & D GmbH StarSign CUT S'

  o In Ubuntu, this file is located in /usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/.

  o In Red Hat, this file is located in /usr/lib64/pcsc/drivers/ifd.ccib.bundel/Contents/.

6 Supported Operating Systems

SafeSign IC Standard version 3.8 for Linux has been tested to support the following Linux Operating System(s):

Operating System	Version	Version 3.8.0.0
Red Hat x64	8.6	√
Ubuntu LTS x64	20.04.4	√
	22.04	√

Note that SafeSign IC Standard version 3.8 for Linux supports 64-bit Linux distributions only.

Note that only support requests for issues reproduced on the supported Operating System(s) will be taken into consideration. Note that SafeSign IC Standard version 3.8 for Linux is not tested to work on beta versions of the mentioned Operating Systems.

SafeSign IC can be made available on other Linux distributions and platforms as well, such as Linux running on ARM and Raspberry Pi, provided against payment of a fee and subject to a separate support agreement.

7   Supported Tokens

SafeSign IC Standard version 3.8 for Linux supports a number of smart cards and tokens, as listed below.

These tokens have been tested to work as part of the release testing for SafeSign IC Standard version 3.8 for Linux.

The number of cards supported in SafeSign IC for Linux has been decreased, to support only those cards that are non-proprietary and are compliant with at least Java Card 2.2.2 and higher.

The SafeSign IC PKI applet enables end users to utilise Java Card 2.2.2 and higher compliant cards with the SafeSign Identity Client middleware. A Java card or token must contain an installed SafeSign Identity Client applet before it can be used with SafeSign Identity Client.

> *As the correct functioning of SafeSign IC is depending on a properly produced smart card or USB Token, AET requires that smart cards and / or USB tokens are produced for use with SafeSign Identity Client in accordance with our QA policies (which require i.a. the correct applet to be pre-installed in a secure environment and a custom keyset). This is a condition to be eligible for support by AET in case of problems, in addition to the purchase / existence of a valid SafeSign Identity Client Maintenance and Support Agreement.*

If you have any questions, please contact AET (safesignsupport@aeteurope.com).

Card Type
Defensiepas 2
Defensiepas 3 (QSCD)
G&D Sm@rtCafé Expert 3.2
G&D Sm@rtCafé Expert 4.0
G&D Sm@rtCafé Expert 5.0
G&D Sm@rtCafé Expert 6.0
G&D Sm@rtCafé Expert 7.0
Gemalto IDCore 30
Infineon Oracle JCOS Ed.1
JCOP21 v2.3
NXP J2A080 / J2A081 (JCOP 2.4.1 R3)
NXP J2D081 (JCOP 2.4.2 R2)
NXP J3A080 (JCOP 2.4.1 R3)
NXP JCOP 2.4.2 R3
NXP JCOP 3 SecID P60
NXP JCOP 4 P71

Card Type
Oberthur IDone Cosmo v7.0
RDW ABR kaart
Rijkspas
Rijkspas 2
StarSign Crypto USB Token S
UZI-pas 2
UZI-pas 3 (QSCD)
UZI-pas 4 (QSCD)

Note that although some USB tokens may be supported by the libccid drivers on Linux, the specific reader information (PID/VID) may not be included by default in the Info.plist file. Please contact the card manufacturer for the appropriate PID and VID of your token. Of course, this USB token has to be supported by SafeSign IC in the first place.

8 Supported Smart Card Readers

SafeSign IC Standard version 3.8 for Linux provides support for PCSC 2.0 Class 1 readers.

In principle, SafeSign Identity Client supports PCSC v1.0 compliant smart card readers that supply a current of at least 60mA.

AET recommends that customers make a careful selection of the smart card reader to use, as there are many smart card readers on the market, with such restrictions as 'buggy' PC/SC drivers (especially older smart card reader models), not enough power supply for cryptographic cards (which require a minimum of 60mA) and faulty T=0 or T=1 protocol implementation. These reader problems are beyond the control of smart cards and SafeSign Identity Client.

> AET strongly recommends using the native / generic Linux CCID driver which is part of the Linux distribution.

The following table lists the specific readers that have been tested with SafeSign IC Standard version 3.8 for Linux:

Smart Card Reader Manufacturer and Model	Class
HID® OMNIKEY® 3121 USB Smart Card Reader Revision D/2019	1

> Note that smart card readers that have been tested or have been working at a given time with a previous SafeSign IC Standard version for Linux, may not (still) work or be supported in any or all versions of SafeSign IC Standard version 3.8 for Linux.

8.1 Extended APDU

In order to be able to generate RSA 4096 keys on a JCOP 4 card, the smart card reader should support extended APDU.

The ISO 7816-4:2013 specification defines an extended APDU as any APDU whose payload data, response data or expected data length exceeds the 256 byte limit.

The following readers have been tested with RSA4K and extended APDU:

- HID OMNIKEY 3121 USB (Part No. R31210320-01, revision B/2016 and revision D/2019)
- Gemalto IDbridge CT30
- ACS ACR38 (P/N ACR38U-N1)

These card readers have been tested using the OS CCID driver, i.e. the native CCID driver on Linux.

Depending on the Operating System, the reader name may be different. This explains the different names in the registry.

> Note that when using an OMNIKEY 3121 smart Card Reader and you need to shorten the reader name (to be able to activate the card), it is advised to modify the reader name in the 'Info.plist' file to that whitelisted in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\A.E.T. Europe B.V.\SafeSign\2.0\Readers\.

9 Supported Applications

SafeSign IC Standard version 3.8 for Linux has been tested in accordance with AET's Quality Assurance procedures and the SafeSign IC Standard for Linux test plan. This includes testing of a number of defined and representative applications to verify a correct functioning of the SafeSign IC components and Libraries.

The following applications have been tested with SafeSign IC Standard version 3.8 for Linux:

Application	Version	Functionality
Token Administration Utility	3.8.31.1	PKCS #11 token management functions
Mozilla Firefox	103.0	Authentication to a secure web site
Mozilla Thunderbird	91.11.0	Signing and decrypting e-mail messages
LibreOffice	7.3.4.1	Digitally signing a document

Note that PKCS #11 applications (such as Firefox) need the PKCS #11 Library to be loaded / installed as a security module. The SafeSign IC PKCS #11 Library (called 'libaetpkss.so') can be found in: /usr/lib/.

Firefox can no longer be used to do certificate enrollment with key pair generation.

9.1 Token Administration Utility

With the SafeSign IC Token Administration Utility, you can perform (local) smart card related operations, such as changing the PIN for your smart card or token.

The features available in the Token Administration Utility, can be modified in the file called "registry" in the folder /home/[user name]/.safesign. The features to be enabled (1) or disabled (0) are located under 'Actions'.

In all supported distributions, you can open a terminal and enter 'tokenadmin'.

9.2 Mozilla Firefox

With the SafeSign PKCS #11 Library installed as a security module in Firefox (as described in section 11.1), you can perform secure web authentication with a SafeSign IC token.

To verify whether the SafeSign PKCS #11 Library is installed as a security module in Firefox, go to Preferences -> Advanced -> Encryption (tab) -> Security Devices (button).

9.3   Mozilla Thunderbird

With the SafeSign PKCS #11 Library installed as a security module in Thunderbird, you can send and receive signed and/or encrypted message with a SafeSign IC token.

To verify whether the SafeSign PKCS #11 Library is installed as a security module in Thunderbird, go to Preferences -> Advanced -> Certificates (tab) -> Security Devices (button).

9.4   LibreOffice

It is possible to digitally sign documents in LibreOffice with a SafeSign IC Token.

See: https://help.libreoffice.org/Common/Applying_Digital_Signatures

With the SafeSign PKCS #11 Library installed as a security module in Firefox (as described in section 11.1), you can sign documents with a SafeSign IC token.

> Note that you may have to indicate the path to the PKCS #11 Library in Tools > Options > Security: Certificate Path

10   Supported Languages

The following languages are supported in SafeSign IC Standard version 3.8 for Linux:

- Basque (Basque);
- Catalan (Catalan);
- Chinese (Simplified, China);
- Chinese (Traditional, Hong Kong SAR; Traditional, Taiwan);
- Croatian (Croatia);
- Czech (Czechia);
- Dutch (Netherlands);
- English (United States);
- Finnish (Finland);
- French (France);
- German (Germany);
- Hungarian (Hungary);
- Italian (Italy);
- Italian (Switzerland);
- Japanese (Japan);
- Korean (Korea);
- Lithuanian (Lituania);
- Portuguese (Portugal);
- Portuguese (Brazil);
- Russian (Russia);
- Serbian (Cyrillic, Serbia)
- Serbian (Latin, Serbia);
- Spanish (Spain);
- Thai (Thailand);
- Turkish (Turkey);
- Ukrainian (Ukraine).

11 SafeSign IC Installation

Note that users need to have sufficient privileges and basic knowledge of Linux to install SafeSign IC Standard version 3.8 for Linux.

Save the installation file (.deb or .rpm) to a location on your Linux computer and double-click to install it. Note that each Linux distribution may have its own appropriate means to install and uninstall software.

If any previous version of SafeSign IC Standard for Linux is installed, it should be uninstalled first. Make sure to restart your computer after uninstallation.

11.1 Installation of Security Module

When you have installed SafeSign IC Standard version 3.8 for Linux, you may want to use SafeSign IC 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 .

For Firefox, this functionality is included in the Token Administration Utility. Please refer to section 11.1.1.

For other applications such as Thunderbird, you will need to do so manually. As an example of a manual installation, the manual installation of the SafeSign PKCS #11 Library in Firefox is described. Please refer to section 11.1.2.

> Note that you should not have more than one instance of the SafeSign PKCS #11 Library installed as a security module, under different names (this will cause Firefox to hang).

11.1.1 SafeSign IC for Firefox Installer

With Firefox installed, in order to install the SafeSign PKCS #11 Library as a security module in Firefox, open the Token Administration Utility and select Install SafeSign in Firefox. This will open the SafeSign IC for Firefox Installer:
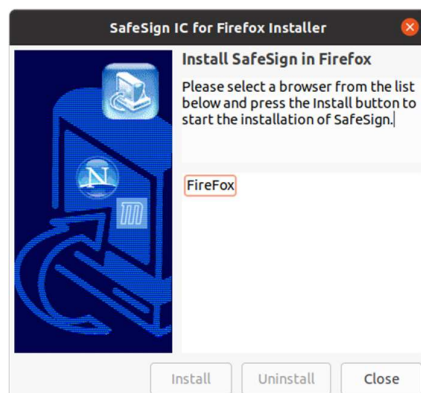

Figure 1: SafeSign IC for Firefox Installer: Install SafeSign in Firefox
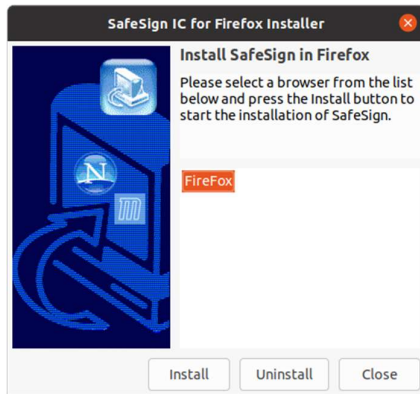
Select Firefox as in the picture below:

Figure 2: SafeSign IC for Firefox Installer: FireFox

➡ Click **Install**

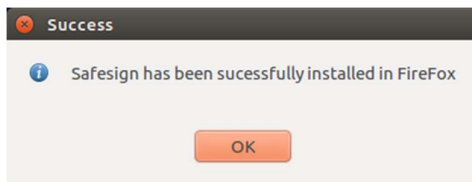When SafeSign is successfully installed in Firefox, you will be notified that:

Figure 3: SafeSign for Firefox Installer: Success

➡ Click **OK**

11.1.2   Manual install in Firefox

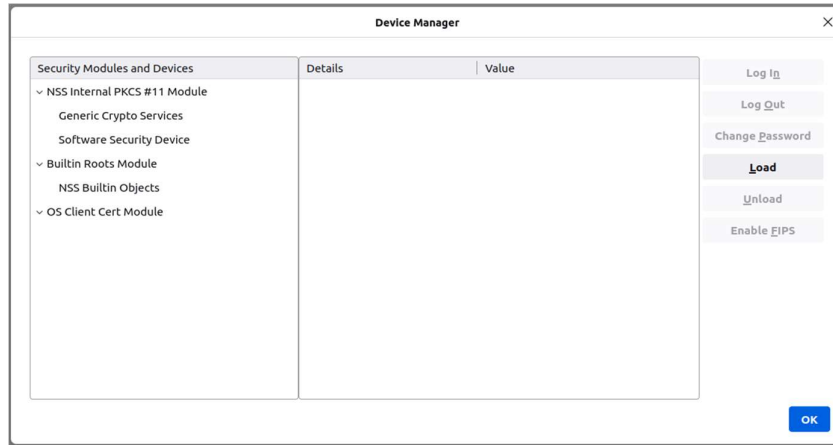In Firefox, go to (Firefox >) Preferences > Privacy & Security > Security Devices (button):

Figure 4: Firefox Device Manager: Security Modules and Devices

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

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

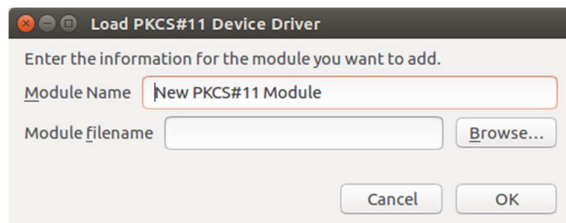Upon clicking on Load, you can enter the information for the module you want to add:

Figure 5: Firefox Device Manager: Load PKCS#11 Device

Enter the name for the security module, i.e. 'SafeSign PKCS #11 Library' and type in the location and name of the SafeSign Identity Client PKCS #11 library, i.e. /usr/lib.
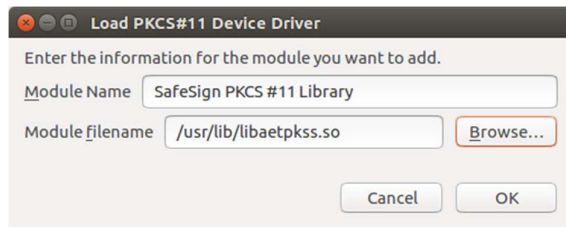
The dialog will now look like this:

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

➡ Click **OK**

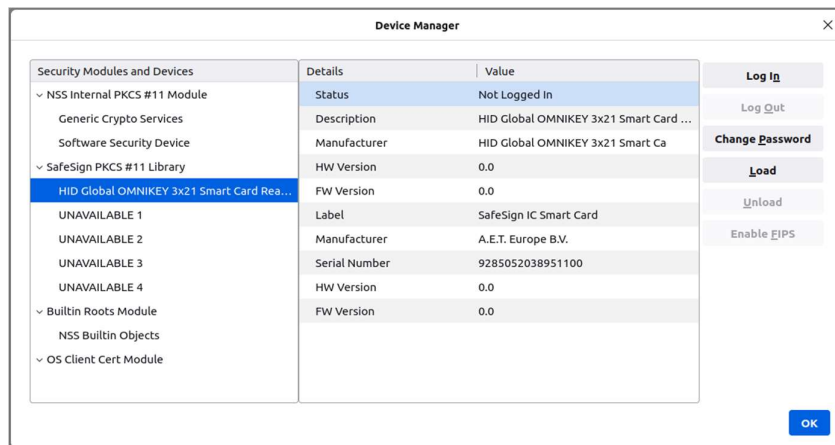The SafeSign Identity Client PKCS #11 Library will now be available as a security module in Firefox:

Figure 7: Firefox Device Manager: SafeSign PKCS #11 Module

Under the name of the security module ('SafeSign PKCS #11 Library'), the available devices are displayed. In this case, there is only one device installed, a smart card reader identified by the label 'HID Global OMNIKEY 3x21 Smart Card Reader'.

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

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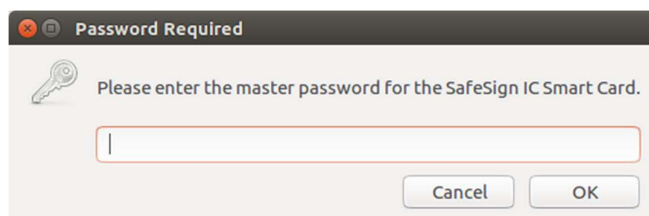

Figure 8: Firefox: Prompt

11.1.3   Unable to add module

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

Figure 9: Firefox: Unable to add module

 Verify that you have provided the correct path and name, i.e. /usr/lib/libaetpkss.so.

11.1.4   Unload

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

Upon clicking Unload, you will be asked to confirm deletion of the security module, after which the module will be deleted:
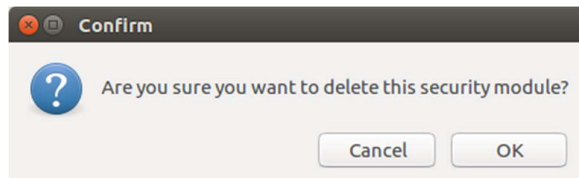

Figure 10: Firefox: Confirm

11.2   Uninstallation

It is possible to uninstall SafeSign IC Standard version 3.8 for Linux from your Linux computer, however, there is no uninstaller for SafeSign IC for Linux. You should uninstall SafeSign IC Standard version 3.8 for Linux through the appropriate means of your Linux distribution.

- Note that in all supported distributions, you can uninstall SafeSign IC through a terminal.
- Note that uninstalling SafeSign IC Standard version 3.8 for Linux does not uninstall the SafeSign PKCS #11 Library from Firefox. It is recommended to use the Firefox Installer to uninstall SafeSign from Firefox, before uninstalling SafeSign. See section 11.1.1.