SafeSign Identity Client Standard Version 3.5

Release Document for Linux

Table of Contents

Table of Figures

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 that accompanies each product. Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/ or industrial property rights of or concerning any of A.E.T. Europe B.V. information.

Cryptographic products are subject to export and import restrictions. You are required to obtain the appropriate government licenses prior to shipping this Product.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, A.E.T. Europe B.V. makes no warranty as to the value or accuracy of information contained herein. The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, A.E.T. Europe B.V. reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

A.E.T. EUROPE B.V. HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH REGARD TO THE INFORMATION CONTAINED HEREIN, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL A.E.T. EUROPE B.V. BE LIABLE, WHETHER IN CONTRACT, TORT OR OTHERWISE, FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER INCLUDING BUT NOT LIMITED TO DAMAGES RESULTING FROM LOSS OF USE, DATA, PROFITS, REVENUES, OR CUSTOMERS, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION CONTAINED IN THIS DOCUMENT.

Credit Information:

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

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

Document Information

Document ID: SafeSign IC Standard Version 3.5 Release Document for Linux

Project Information: SafeSign IC Release Documentation

Document revision history:

Version	Date	Author	Changes
1.0	19 March 2019	Drs C.M. van Houten	First edition for SafeSign IC Standard Version 3.5 for Linux, release 3.5.0.0-AET.000
2.0	30 April 2019	Drs C.M. van Houten	First edition for SafeSign IC Standard Version 3.5 for Linux, release 3.5.2.0-AET.000
3.0	31 January 2020	Drs C.M. van Houten	First edition for SafeSign IC Standard Version 3.5 for Linux, release 3.5.6.0-AET.000
3.1	14 April 2020	Drs C.M. van Houten	First edition for SafeSign IC Standard Version 3.5 for Linux, release 3.5.6.1-AET.000

Document approval:

Version	Date	Name	Function
1.0	19 March 2019	B. Smid MBT	Chief Development Officer
2.0	30 April 2019	B. Smid MBT	Chief Development Officer
3.0	31 January 2020	B. Smid MBT	Chief Development Officer
3.1	14 April 2020	B. Smid MBT	Chief Development 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 (IC) Standard version 3.5 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 for Linux is provided in a .deb file or .rpm file.

2.2 Date of Release

The date of the release is 14 April 2020.

2.3 Release Details

SafeSign IC Standard Version 3.5 for Linux reflects the new SafeSign IC version 3.5 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 and which now includes the version number for all components delivered with the release of SafeSign IC version 3.5 for Linux.

Release version: Standard Release 3.5.6.1-AET.000		
Description	**File Name**	**File Version**
Java Card Handling Library	libaetjcss.so	3.5.4381
PKCS #11 Cryptoki Library	libaetpkss.so	3.5.4358
Dialog Library	libaetdlglib.so	3.5.4315
Common Dialogs	libaetdlss.so	3.5.4126
Token Administration Utility	tokenadmin	3.5.4401

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 version 3.5 for Linux provides at least the following release documentation:

Document Name	Version
SafeSign Identity Client Standard Version 3.5 Release Document for Linux	3.1

3 Features

The following features are supported by SafeSign IC version 3.5 for Linux:

1. Multiple Token Support
2. Multiple Smart Card Reader Support
3. Multiple Application Support
4. Multiple Language Support
5. Attribute Certificate Support (≥ release 3.5.2.0)
6. Activate QSCD Card Support (≥ release 3.5.4.0)

These features are described in the following paragraphs.

3.1 Multiple Token Support

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

Newly supported smart card and tokens in SafeSign IC version 3.5 for Linux are:

- Giesecke & Devrient StarSign Crypto USB-Token S
- Infineon Oracle JCOS Ed.1
- Morpho IDealCitiz v2.1
- NXP JCOP 3 SecID P60

3.2 Multiple Smart Card Reader Support

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

3.3 Multiple Application Support

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

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

- Web authentication
- Email signing and encryption
- Document signing

SafeSign IC Standard version 3.5 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 3.5 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 3.5 supports.

3.5 Attribute Certificate Support

SafeSign IC Standard Version 3.5.2.0 allows you to view (information on) Attribute Certificates on the token and to import / export Attribute Certificates through the Token Administration Utility.

“An attribute certificate (AC) is a structure similar to a Public Key certificate (PKC); the main difference being that the AC contains no public key. An AC may contain attributes that specify group membership, role, security clearance, or other authorization information associated with the AC holder.” (From: https://tools.ietf.org/html/rfc5755).

The Token Administration Utility (TAU) now includes the following information on ACs:

- *PKCS #11 objects* dialog (Show Token Objects): the column ‘Type’ indicates whether the certificate is a (PKC) ‘Certificate’ or an ‘Attribute Certificate’.
- *Certificate* dialog (View certificate): the *Certificate* dialog includes information on ‘Certificate Attributes’ for an Attribute Certificate.
- *Certificate analysis* dialog (Analyse certificate quality): the (new) column ‘Type’ now indicates whether the certificate is a (PKC) ‘Certificate’ or an ‘Attribute Certificate’.
- It is possible to import Attribute Certificates through the Import Certificate feature.
- It is possible to export Attribute Certificates through Save Object / Save to file.
- When making a dump file (Dump Token Contents), the resulting .tkn will include information on the certificate type; an Attribute Certificate will contain ‘CKA_CERTIFICATE_TYPE: CKC_X_509_ATTR_CERT’.

  Note that translations for Attribute Certificates and their attributes / extensions are only available in Dutch, Portuguese and Brazilian Portuguese.

3.6 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.

From SafeSign IC Standard Version 3.5.4.0 onwards, the SafeSign IC Token Administration Utility offers users of a QSCD 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 require the user to authenticate to the card by entering the PIN or it may require the user to change the Transport PIN set for the card.

SafeSign IC Standard version 3.5 for Linux supports the following QSCD cards:

- Defensiepas 3 (≥ SafeSign IC Standard version 3.5.4.0)
- UZI-pas 3 (≥ SafeSign IC Standard version 3.5.6.0)

4 New Features and Fixes

SafeSign IC Standard version 3.5 for Linux has a number of new features and fixes / changes.

Section 4.1 will describe the new features and functionality.

Section 4.2 will describe the improved and fixed features and functionality.

4.1 New

- Added support for Infineon Oracle JCOS Ed.1
- Added support for Morpho IDealCitiz 2.1
- Added support for StarSign Crypto USB-Token S
- Added support for NXP JCOP 3 SecID P60
- Added a number of new ATRs for supported cards.
- The tokenadmin app reflects the new SafeSign IC version 3.5 product version numbering scheme and now includes the version number for all components included.
- In the Token Information dialog, the field ‘Last Update of PIN’ now includes the exact date of the last PIN change in the format YYYY-MM-DD (in accordance with the extended date representation of the ISO 8601 standard). When the last update of the PIN is the same day /today, the field includes the text ‘today’ (not the date in YYYY-MM-DD format).
- As users may want to be able to see the number of PUK retries left when entering the PUK (to prevent the PUK from getting blocked), a PUK retry country counter has been implemented. This should be enabled by the registry setting ‘ShowPUKRetryCounter’. When enabled, any dialog that includes PUK entry (such as Change PUK or Unlock PIN) will display not only that the PUK inserted was wrong (which is existing functionality), but also the remaining tries before the PUK will be blocked.
- A PIN retry counter has been added to the Change PIN dialog of the tokenadmin as well.

4.1.1 Version 3.5.2.0

- Support for Ubuntu 18.04 LTS.
- SafeSign IC Standard Version 3.5.2.0 allows you to view (information on) Attribute Certificates on the token and import / export Attribute Certificates through the Token Administration Utility.
- Added support for Oberthur IDone Cosmo v7.0.2 (ATR).

4.1.2 Version 3.5.4.0

- Support for Defensiepas 3 (ATR) on NXP JCOP 3 SecID P60.

4.1.3 Version 3.5.6.0

- Support for UZI-pas 3 (ATR) on NXP JCOP 3 SecID P60.

4.1.4 Version 3.5.6.1

- Some features of the Token Administration Utility, which were enabled by default, have now been disabled by default:
  - Delete Digital ID (button in *Digital IDs* dialog)
  - Transfer ID to token (button in *Digital IDs* dialog)
  - Import Digital ID (option in **Digital IDs** menu)

4.2 Fixed

- In SafeSign IC Standard Version 3.5, a number of cards (and related data, including ATRs and CPLC data) have been removed. Basically, SafeSign IC will only support Java Card v2.2.2 and higher cards. See section 7 for more details.
- Applet loading functionality has been disabled. This functionality was included for evaluation and demonstration purposes only (working only for cards with a default Global Platform keyset) and use of the included applet has been deprecated.
- As a consequence of the above, the Token Administration Utility option 'QueryUnknownToken' has been removed.
- Applied a consistent name convention for Giesecke & Devrient cards, i.e. 'G&D Sm@rtCafe Expert'.
- The Firefox Installer has been renamed to 'SafeSign IC for Firefox Installer'.
- There was an issue in SafeSign IC Standard Version 3.0.112, when installing the SafeSign IC PKCS #11 Library through the Firefox Installer in Firefox 58.0, due to changes Firefox made in the method for registering a PKCS #11 Library. This has been fixed in SafeSign IC Standard version 3.5.

4.2.1 Version 3.5.2.0

- With the Token Administration Utility open, entering an incorrect PIN in another (external) application (e.g. when doing secure web authentication) will not update the PIN retry counter. This issue has been fixed.
- It is now possible to upgrade from SafeSign IC Standard Version 3.5.0.0 to SafeSign IC Standard Version 3.5.2.0. This also means that the registry file in the user's home directory does not have to be manually deleted to create a new one, but will be overwritten upon an upgrade.
- In SafeSign IC Standard Version 3.0.112 and 3.5.0.0, you could resize the Token Administration Utility window to a very small size. The resize has been limited, to a size where the text of the menu items remains visible.
- When installing SafeSign IC Standard on Ubuntu, the documentation in folder /usr/share/doc/safesignidentityclient contains gz files (instead of txt files) for license.txt and SafeSign_License_Agreement_PT_BR.txt. This has been fixed.

4.2.2 Version 3.5.6.1

- There was an issue in the SafeSign IC for Firefox Installer, which did not install the PKCS #11 Library as a security module in Firefox 68 or higher, although it reports that it is succesful. This is caused by the fact that Mozilla Firefox moved to a “profile per install architecture”. This has been fixed in SafeSign IC Standard version 3.5.6.1. SafeSign IC will now be installed in each Firefox profile available at the time of installation.

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.
- PCSCD is not enabled / running by default in SLED 11 and 12. You have to enable the service, otherwise SafeSign IC will crash.
- Thunderbird is not available in the SLED 11 repositories, therefore it is not tested with signing and encryption on SLED 11.
- The option *LimitPintoascii* does not work in Ubuntu / SLE. This problem has been identified as a Wxwidgets problem.
- Adobe discontinued support for Adobe Reader for Linux, therefore, it is no longer available for download from the Adobe web site.
- The StarSign Crypto USB-Token S is not supported by the default libccid drivers in Ubuntu 14.04 and 16.04. In Ubuntu 16.04, after adding the reader information to the Info.plist file, the reader is available, so it can work with SafeSign IC. Please contact G&D for the appropriate PID and VID of the token and how to add it. This workaround does not work in Ubuntu 14.04, hence the token is not supported in 14.04.
- The support for the non-standard <keygen> HTML element and HTMLKeygenElement DOM interface has been removed with Firefox 69. This means that any enrolment that uses the browser to generate the key pair will cease to work with Firefox 69 onwards. Please refer to: https://developer.mozilla.org/en-US/docs/Web/HTML/Element/keygen.

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.

5.2.1 Version 3.5.0.0

- 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).

5.2.2 Version 3.5.2.0

- In Firefox version 65.0 and higher, the reader name is displayed in the Security Devices column, not the token label (even when the token is inserted).
- On Ubuntu 18.04 and CentOS 7, the applet version and information on secure messaging being enabled is not shown in the *Token Information* dialog for a G&D StarSign Crypto USB-Token with ICP-Brazil certified applet. This is caused by the reader name being more than 64 bytes when C_GetSlotInfo is called. The workaround is to modify the reader name (string) in the Info.plist file, from 'Giesecke & Devrient GmbH StarSign CUT S' to 'G & D GmbH StarSign CUT S'.
    - In Ubuntu, this file is located in /usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist).
    - In centOS, this file is located in /usr/lib64/pcsc/drivers/ifd.ccib.bundel/Contents/Info.plist.
- On Ubuntu 16.04, horizontal and vertical scrollbars are not usable in the Token Administration Utility's *Certificate* dialog for Attribute Certificates. To view all information available (attributes and extensions), the dialog can be enlarged.

6 Supported Operating Systems

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

Operating System	3.5.0.0	3.5.2.0	3.5.4.0	3.5.6.0	3.5.6.1
CentOS 7 x64	√	√			
SUSE Linux Enterprise 11 Desktop / Server x64 SP4	√				
SUSE Linux Enterprise 12 Desktop / Server x64 SP2	√				
Ubuntu 14.04.5 LTS x64	√				
Ubuntu 16.04.6 LTS x64	√	√			
Ubuntu 18.04.4 LTS x64		√	√	√	√

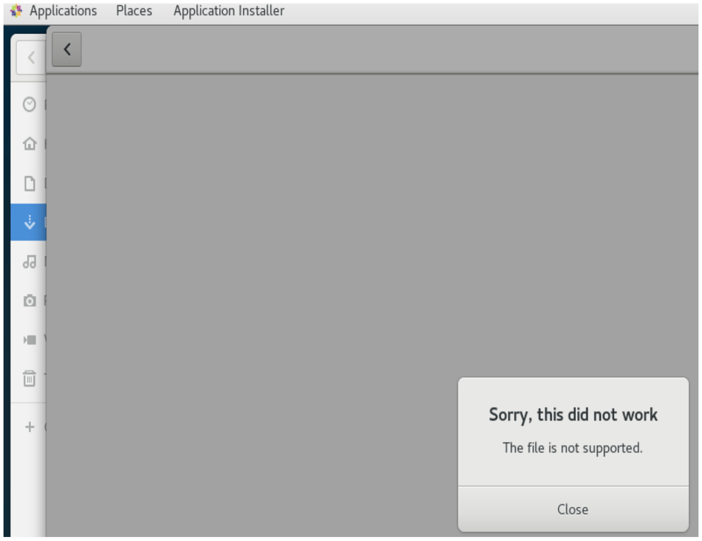
Note that SafeSign IC Standard Version 3.5 for Linux supports 64-bit Linux distributions only.

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 3.5 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 license and support agreement.

6.1 CentOS 7

It is not possible to install SafeSign IC Standard version 3.5 for Linux using the Nautilus File Manager on CentOS 7. Opening the .rpm file via Nautilus leads to an error:



Sorry, this did not work

The file is not supported.

Figure 1: Nautilus File Manager

This is a known error / bug, for which a bug report exists:
https://bugzilla.redhat.com/show_bug.cgi?id=1434477

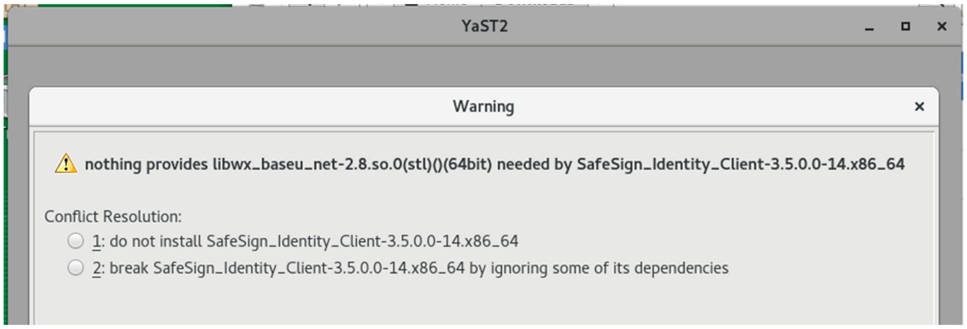
Workaround is to open a terminal and to navigate to the place where the SafeSign IC Standard version 3.5 .rpm file for CentOS is stored, then do a manual install via yum:
sudo yum install "./SafeSign IC Standard Linux 3.5.0.0-AET.000 centos7 x86_64.rpm"

- Note that in order to uninstall SafeSign IC Standard version 3.5 for centOS 7, you should use the following command: sudo yum remove "SafeSign_Identity_Client.x86_64", where "SafeSign_Identity_Client.x86_64" is the name of the installed application.

6.2 SUSE Linux Enterprise 12

There is a specific distribution-related issue with the installation of SafeSign IC Standard version 3.5 for Linux on SUSE Linux Enterprise 12 (both 64-bit Server and Desktop).

Even when the system is fully up-to-date, SafeSign IC Standard version 3.5 for Linux cannot be installed because of package dependency issues related to WxWidgets:

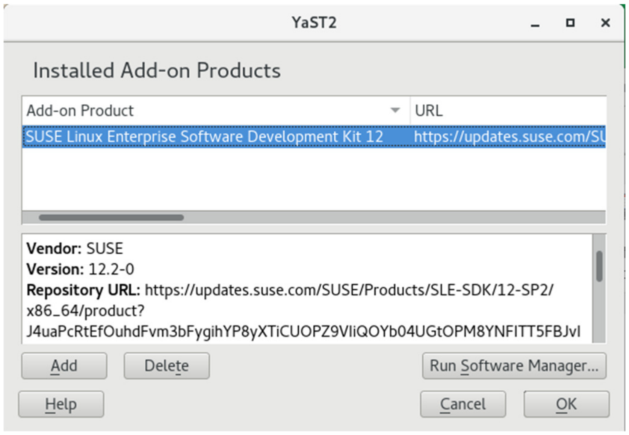


⚠ nothing provides libwx_baseu_net-2.8.so.0(stl)()(64bit) needed by SafeSign_Identity_Client-3.5.0.0-14.x86_64

Conflict Resolution:
○ 1: do not install SafeSign_Identity_Client-3.5.0.0-14.x86_64
○ 2: break SafeSign_Identity_Client-3.5.0.0-14.x86_64 by ignoring some of its dependencies

Figure 2: YaST: Warning

Because SLE 12 does not provide an update or a special package(s) to install the required WxWidgets packages, you need to install the SUSE Linux Enterprise Software Development Kit 12 before installing SafeSign IC Standard version 3.5:



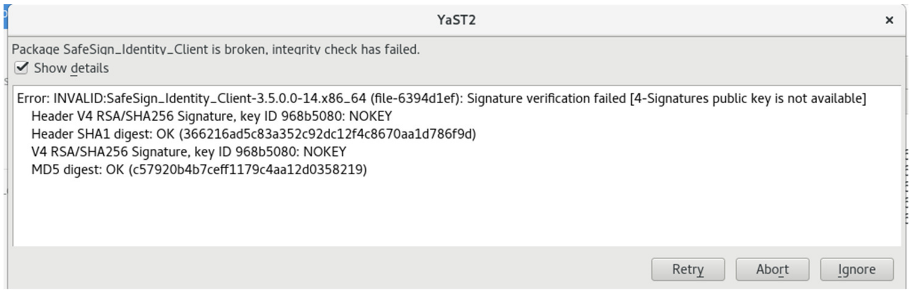
Add-on Product	URL
SUSE Linux Enterprise Software Development Kit 12	https://updates.suse.com/SU

Vendor: SUSE
Version: 12.2-0
Repository URL: https://updates.suse.com/SUSE/Products/SLE-SDK/12-SP2/x86_64/product?J4uaPcRtEfOuhdFvm3bFygihYP8yXTiCUOPZ9VliQOYb04UGtOPM8YNFITT5FBJvl

Figure 3: YaST: Installed Add-on Products

6.2.1 GPG Check Handling

During the final stages of the installation, you will get the following prompt:



Package SafeSign_Identity_Client is broken, integrity check has failed.

☑ Show details

```
Error: INVALID:SafeSign_Identity_Client-3.5.0.0-14.x86_64 (file-6394d1ef): Signature verification failed [4-Signatures public key is not available]
   Header V4 RSA/SHA256 Signature, key ID 968b5080: NOKEY
   Header SHA1 digest: OK (366216ad5c83a352c92dc12f4c8670aa1d786f9d)
   V4 RSA/SHA256 Signature, key ID 968b5080: NOKEY
   MD5 digest: OK (c57920b4b7ceff1179c4aa12d0358219)
```

Figure 4: YaST2: Integrity check has failed

This is caused by the fact that although the SafeSign IC Standard version 3.5 for Linux installer is signed, its public key is not included in the RPM database (see section 3.2.2 in the Release Notes for SUSE Linux Enterprise Server 12: https://www.suse.com/releasenotes/x86_64/SUSE-SLES/12/).

You can click Ignore to finish installation and use your SafeSign IC token in SUSE Linux Enterprise 12.

7 Supported Tokens

SafeSign IC 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 version 3.5 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.

From SafeSign IC version 3.5, applet loading functionality has been disabled. In previous versions, an old and deprecated version of the SafeSign IC applet was included, which could be installed on Java cards (during initialisation through the Token Utility) for demonstration and evaluation purposes, if such a card contained a default GlobalPlatform keyset. Obviously, this is not desirable in production (use), where the proper applet should not only be pre-installed, but the default keyset changed to a custom(er) keyset, in a secure production facility / environment.

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
Defensiepas 2
Defensiepas 3 (QSCD)
G&D Convego Join 4.01 40k/80k
G&D SkySIM Hercules
G&D SkySIM Scorpius
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
G&D Sm@rtCafé Expert 64
Gemalto Desineo ICP D72 FXR1 Java

Card Type
Gemalto IDCore 30
Gemalto MultiApp ID v2.1
Gemalto Optelio D72 FR1
Gemalto TOP DL v2
Infineon Oracle JCOS Ed.1
JCOP21 v2.3
Morpho IDealCitiz v2.1
Morpho JMV ProCL V3.0
NXP J2A080 / J2A081 (JCOP 2.4.1 R3)
NXP JD081 (JCOP 2.4.1 R3)
NXP J3A080 (JCOP 2.4.1 R3)
NXP JCOP 2.4.2 R3
NXP JCOP 3 SecID P60
Oberthur IDOne Cosmo v7.0
RDW ABR kaart
Rijkspas
Rijkspas 2
Sagem YpsID s2
Sagem YpsID s3
StarSign Crypto USB-Token S
Swissbit PS-100u SE
UZI-pas
UZI-pas 2
UZI-pas 3 (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.
- For example, the G&D StarSign Crypto USB-Token S is not by default supported by the default CCID drivers included in Ubuntu 16.04 (as opposed to Ubuntu 18.04).

8 Supported Smart Card Readers

SafeSign IC Standard 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.

We recommend 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 3.5 for Linux:

Smart Card Reader Manufacturer and Model	Class
HID Global CardMan 3x21	1

- Note that smart card readers that have been tested or have been working at a given time with a previous SafeSign IC version for Linux, may not (still) work or be supported in any or all versions of SafeSign IC version 3.5 for Linux.

9 Supported Applications

SafeSign IC version 3.5 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 for Linux:

Application	Version	Functionality
Token Administration Utility	3.5.4401	PKCS #11 token management functions
Mozilla Firefox	74.0.1	Authentication to a secure web site
Mozilla Thunderbird	68.4.1	Signing and decrypting e-mail messages

- 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).

10 Supported Languages

The following languages are supported in SafeSign IC:

- Basque;
- Catalan;
- Chinese (Simplified);
- Chinese (Traditional);
- Croatian;
- Czech;
- Dutch;
- English;
- Finnish;
- French (France);
- German;
- Hungarian;
- Italian;
- Italian (Swiss);
- Japanese;
- Korean;
- Lithuanian;
- Portuguese (Portugal);
- Portuguese (Brazil);
- Russian;
- Serbian (Cyrillic);
- Serbian (Latin);
- Spanish;
- Thai;
- Turkish;
- Ukrainian.

11 SafeSign IC Installation

Note that users need to have sufficient privileges and basic knowledge of Linux to install SafeSign IC version 3.5 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 (such as YaST and Synaptic Package Manager).

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

Note that from SafeSign IC for Linux release 3.5.2.0 onwards, it is possible to upgrade an existing installation of SafeSign IC version 3.5.

11.1 Installation of 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 .

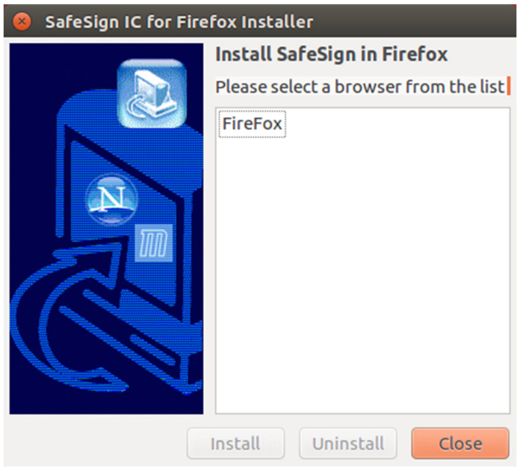
For Firefox, this functionality is included in the Token Administration Utility. Please refer to section 11.1.1.

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:



SafeSign IC for Firefox Installer

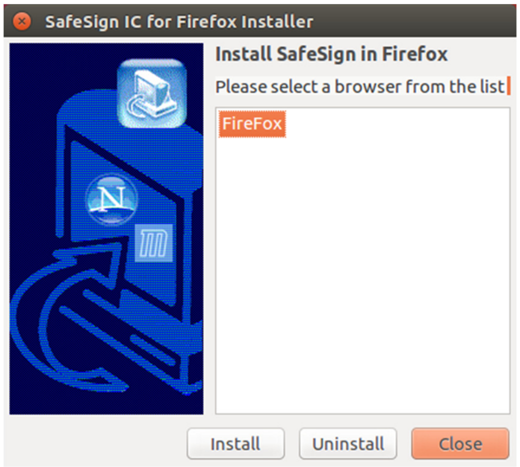
Install SafeSign in Firefox

Please select a browser from the list

FireFox

Figure 5: SafeSign IC for Firefox Installer: Install SafeSign in Firefox

Select Firefox as in the picture below:



SafeSign IC for Firefox Installer

Install SafeSign in Firefox

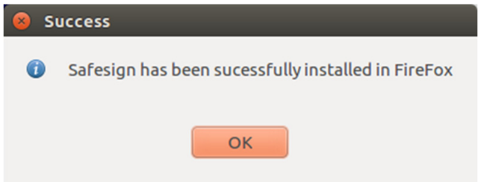
Please select a browser from the list

FireFox

Figure 6: SafeSign IC for Firefox Installer: FireFox

- Click **Install**

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



Success

Safesign has been sucessfully installed in FireFox

Figure 7: 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):

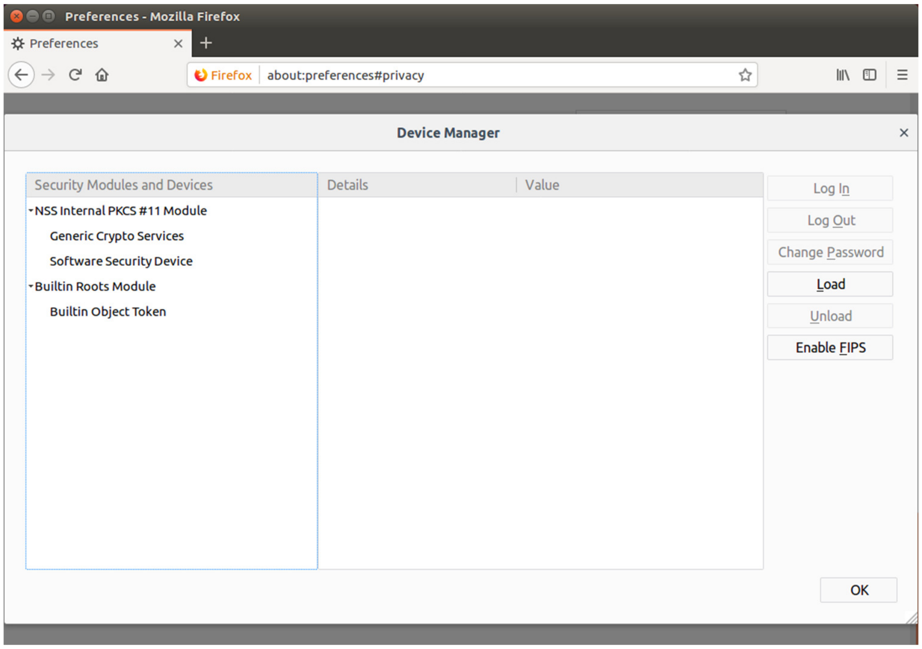
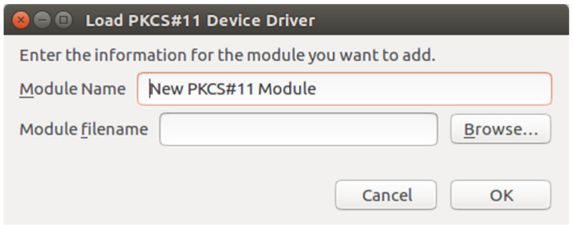


Figure 8: Firefox Device Manager: Security Modules and Devices

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:



Enter the information for the module you want to add.

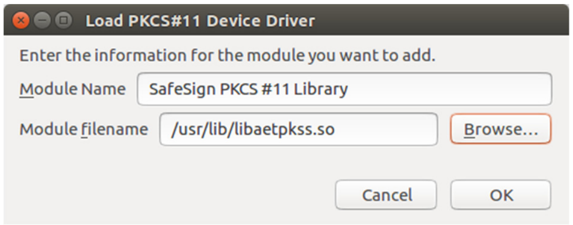
Module Name: New PKCS#11 Module

Module filename:

Figure 9: 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:



Enter the information for the module you want to add.

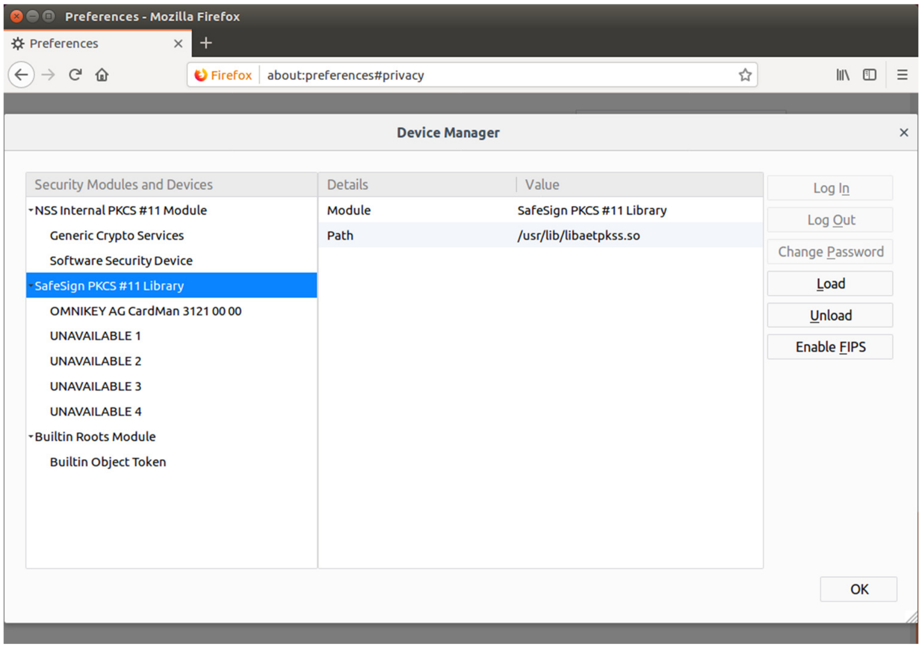
Module Name: SafeSign PKCS #11 Library

Module filename: /usr/lib/libaetpkss.so

Figure 10: 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:



Security Modules and Devices

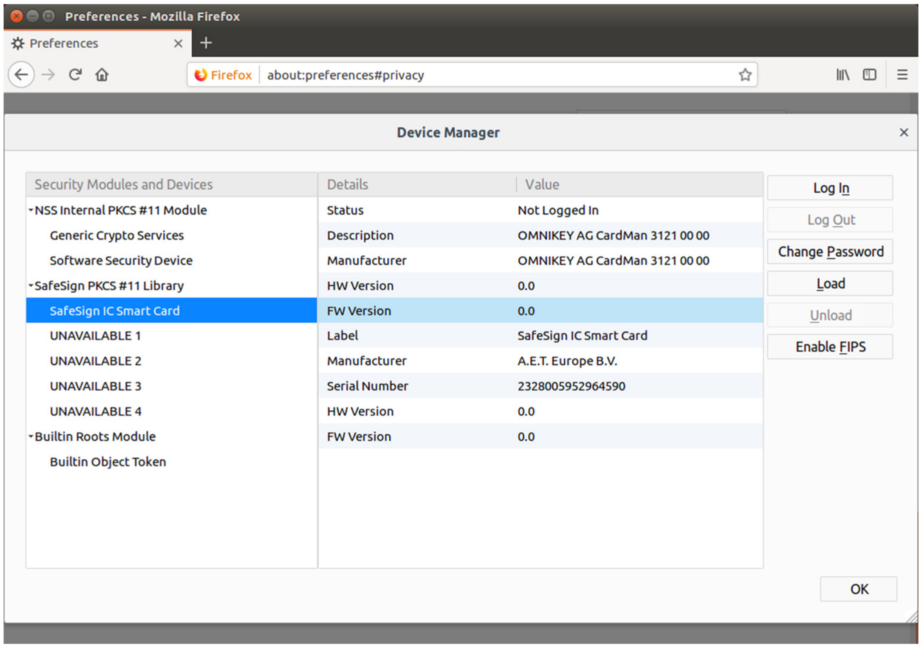
- NSS Internal PKCS #11 Module
  - Generic Crypto Services
  - Software Security Device
- SafeSign PKCS #11 Library
  - OMNIKEY AG CardMan 3121 00 00
  - UNAVAILABLE 1
  - UNAVAILABLE 2
  - UNAVAILABLE 3
  - UNAVAILABLE 4
- Builtin Roots Module
  - Builtin Object Token

Details	Value
Module	SafeSign PKCS #11 Library
Path	/usr/lib/libaetpkss.so

Figure 11: 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 'OMNIKEY AG CardMan 3121 00 00'. No card is inserted in the reader.

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



Security Modules and Devices

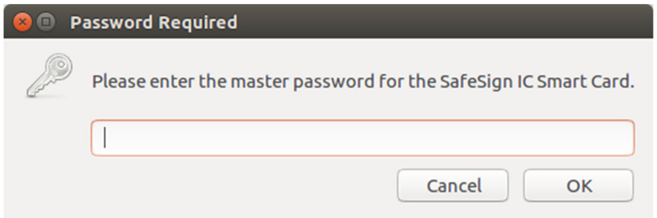
- NSS Internal PKCS #11 Module
  - Generic Crypto Services
  - Software Security Device
- SafeSign PKCS #11 Library
  - SafeSign IC Smart Card
  - UNAVAILABLE 1
  - UNAVAILABLE 2
  - UNAVAILABLE 3
  - UNAVAILABLE 4
- Builtin Roots Module
  - Builtin Object Token

Details	Value
Status	Not Logged In
Description	OMNIKEY AG CardMan 3121 00 00
Manufacturer	OMNIKEY AG CardMan 3121 00 00
HW Version	0.0
FW Version	0.0
Label	SafeSign IC Smart Card
Manufacturer	A.E.T. Europe B.V.
Serial Number	2328005952964590
HW Version	0.0
FW Version	0.0

Figure 12: Firefox Device Manager: SafeSign IC Token

- 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.
- Note that from Firefox 65.0 onwards, the reader name (as in Figure 11) is displayed, rather than the label of the 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:

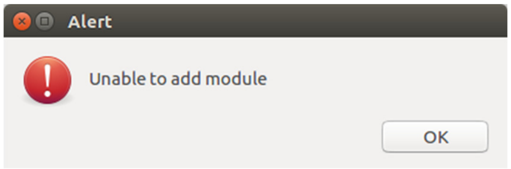


Please enter the master password for the SafeSign IC Smart Card.

Figure 13: 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:


Alert

Unable to add module

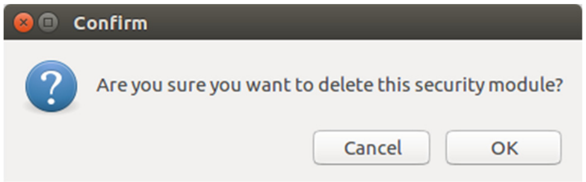
Figure 14: Firefox: Unable to add module

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:


Confirm

Are you sure you want to delete this security module?

Figure 15: Firefox: Confirm

11.2 Uninstallation

It is possible to uninstall SafeSign IC Standard version 3.5 for Linux from your Linux computer, however, there is no uninstaller for SafeSign IC for Linux.

- Note that uninstalling SafeSign IC Standard version 3.5 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.

You should uninstall SafeSign IC Standard version 3.5 for Linux through the appropriate means of your Linux distribution (such as through YaST or Synaptic Package Manager).

- Note that in all supported distributions, you can uninstall SafeSign IC through a terminal.