



SafeSign Identity Client Standard Version 3.5

Release Document for Linux



Table of Contents

Table of Contents	I
Table of Figures	III
Warning Notice	IV
Document Information	V
About the Product	VI
1 About this Document	1
2 Release Information	2
2.1 Deliverables	2
2.2 Date of Release	2
2.3 Release Details	2
2.4 Release Documents	2
3 Features	3
3.1 Multiple Token Support	3
3.2 Multiple Smart Card Reader Support	3
3.3 Multiple Application Support	3
3.4 Multiple Language Support	4
4 New Features and Fixes	5
4.1 New	5
4.2 Fixed	5
5 Known Issues	7
5.1 General	7
5.2 SafeSign IC	7
5.2.1 Version 3.5.0.0	7
6 Supported Operating Systems	8
6.1 CentOS 7	8
6.2 SUSE Linux Enterprise 12	9
6.2.1 GPG Check Handling	10
7 Supported Tokens	11
8 Supported Smart Card Readers	13
9 Supported Applications	14
9.1 Token Administration Utility	14
9.2 Mozilla Firefox	14
9.3 Mozilla Thunderbird	14
9.4 LibreOffice	15
10 Supported Languages	16



11	SafeSign IC Installation.....	17
11.1	Installation of Security Module	17
11.1.1	SafeSign IC for Firefox Installer.....	17
11.1.2	Manual install in Firefox.....	19
11.1.3	Unable to add module	21
11.1.4	Unload.....	22
11.2	Uninstallation.....	22



Table of Figures

Figure 1: Nautilus File Manager	8
Figure 2: YaST: Warning	9
Figure 3: YaST: Installed Add-on Products	9
Figure 4: YaST2: Integrity check has failed	10
Figure 5: SafeSign IC for Firefox Installer: Install SafeSign in Firefox	17
Figure 6: safeSign IC for Firefox Installer: FireFox.....	18
Figure 7: SafeSign for Firefox Installer: Success.....	18
Figure 8: Firefox Device Manager: Security Modules and Devices.....	19
Figure 9: Firefox Device Manager: Load PKCS#11 Device	19
Figure 10: Firefox Device Manager: Load SafeSign PKCS #11 Module	20
Figure 11: Firefox Device Manager: SafeSign PKCS #11 Module	20
Figure 12: Firefox Device Manager: SafeSign IC Token	21
Figure 13: Firefox: Prompt	21
Figure 14: Firefox: Unable to add module	21
Figure 15: Firefox: Confirm	22



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.

© Copyright A.E.T. Europe B.V., 2000-2018. All rights reserved.

BlueX 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)."



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 2018	Drs C.M. van Houten	First edition for SafeSign IC Standard Version 3.5 for Linux, release 3.5.0.0-AET.000

Document approval:

Version	Date	Name	Function
1.0	19 March 2018	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 19 March 2018.

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 3.5.0.0-AET.000		
Description	File Name	File Version
Java Card Handling Library	libaetjcss.so	3.5.0.4125
PKCS #11 Cryptoki Library	libaetpkss.so	3.5.0.4112
Dialog Library	libaetdlglib.so	3.5.0.4124
Common Dialogs	libaetdlss.so	3.5.0.4126
Token Administration Utility	tokenadmin	3.5.0.4148

 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	1.0



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

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 IDDealCitiz 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.



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 IDDealCitiz 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.

4.2 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.



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.

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).



6 Supported Operating Systems

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

Operating System	Version 3.5.0.0
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 16.04.3 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:

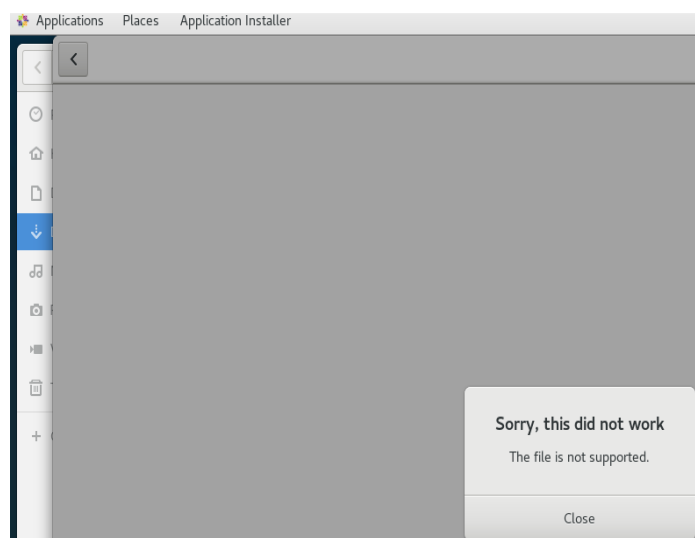


Figure 1: Nautilus File Manager



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:

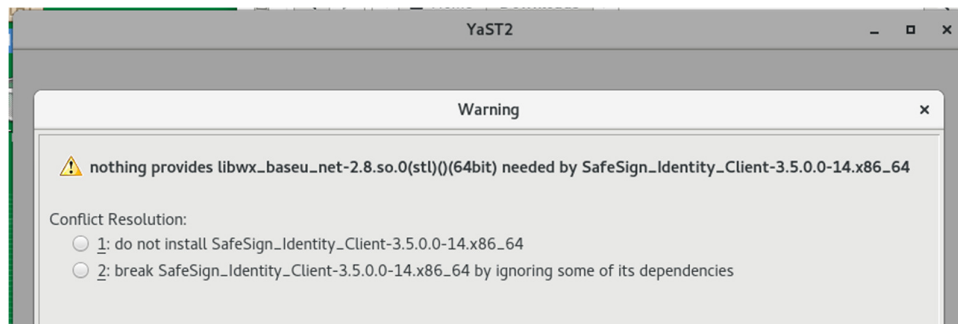


Figure 2: YaST: Warning

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:

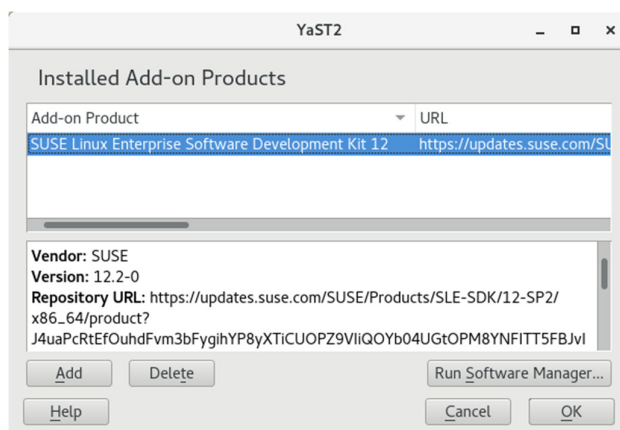


Figure 3: YaST: Installed Add-on Products



6.2.1 GPG Check Handling

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

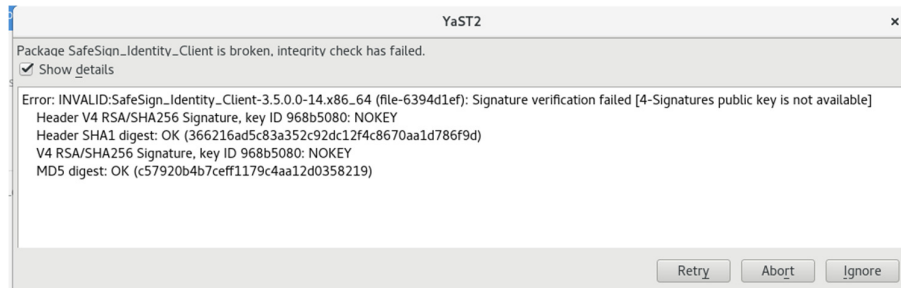


Figure 4: YaST2: Integrity check has failed

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
G&D Convego Join 4.01 40k/80k
G&D SkySIM Hercules
G&D SkySIM Scorpis
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
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 IDDealCitiz 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
UZI-pas
UZI-pas 2

-  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 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	3.5.0.4112	PKCS #11 token management functions
Mozilla Firefox	59.0	Certificate enrollment with key pair generation; Authentication to a secure web site
Mozilla Thunderbird	52.6.0	Signing and decrypting e-mail messages
LibreOffice	6.0.2	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/.

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.

“If you are using Solaris or Linux, you must install a recent version of Thunderbird or Firefox to install some system files that are needed for encryption.”

(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 send and receive signed and/or encrypted message with a SafeSign IC token.



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.

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

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).

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:

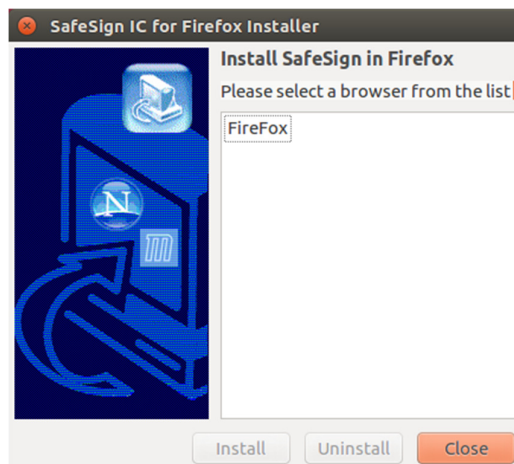


Figure 5: SafeSign IC for Firefox Installer: Install SafeSign in Firefox



Select Firefox as in the picture below:

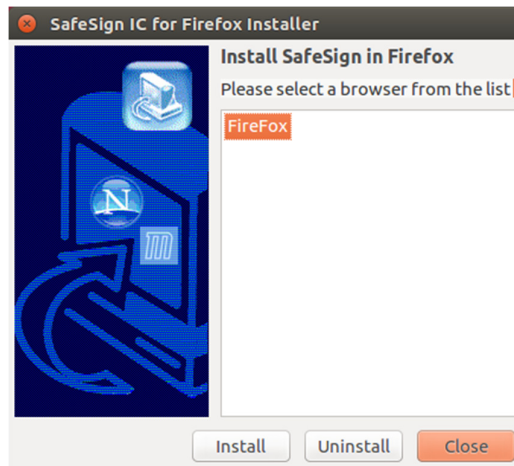


Figure 6: safeSign IC for Firefox Installer: FireFox

➡ Click Install

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

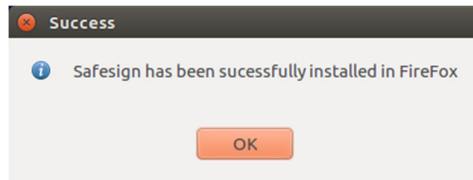


Figure 7: SafeSign for Firefox Installer: Success

➡ Click OK



11.1.2 Manual install in Firefox

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

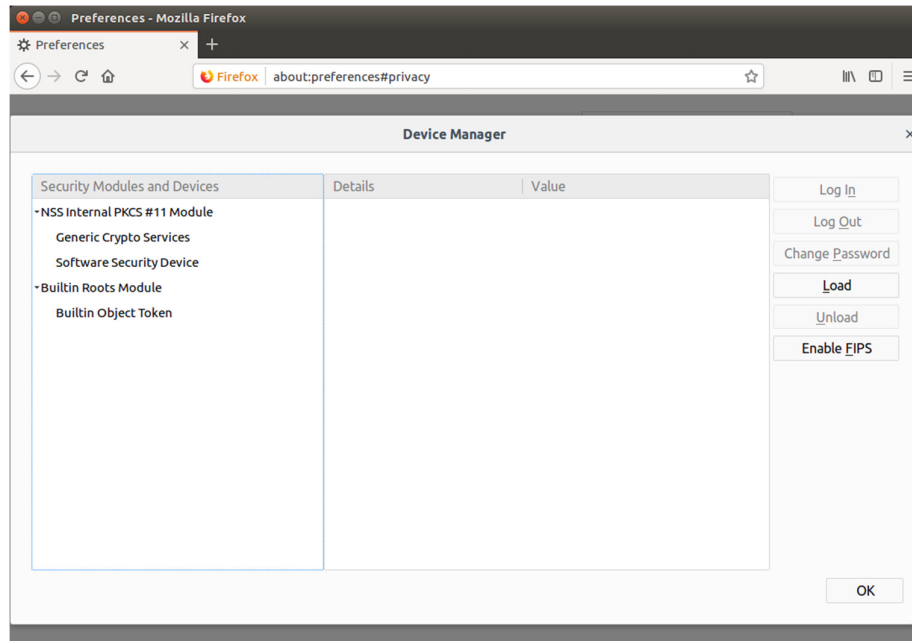


Figure 8: Firefox Device Manager: Security Modules and Devices

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:

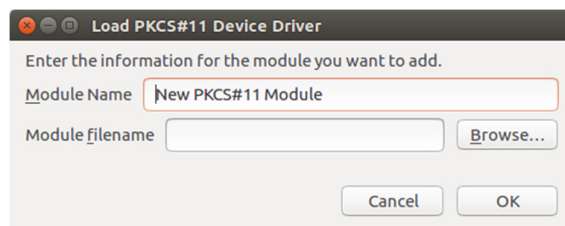


Figure 9: Firefox Device Manager: Load PKCS#11 Device

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:

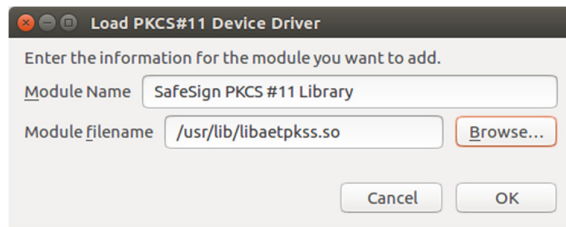


Figure 10: Firefox Device Manager: Load SafeSign PKCS #11 Module

➡ Click OK

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

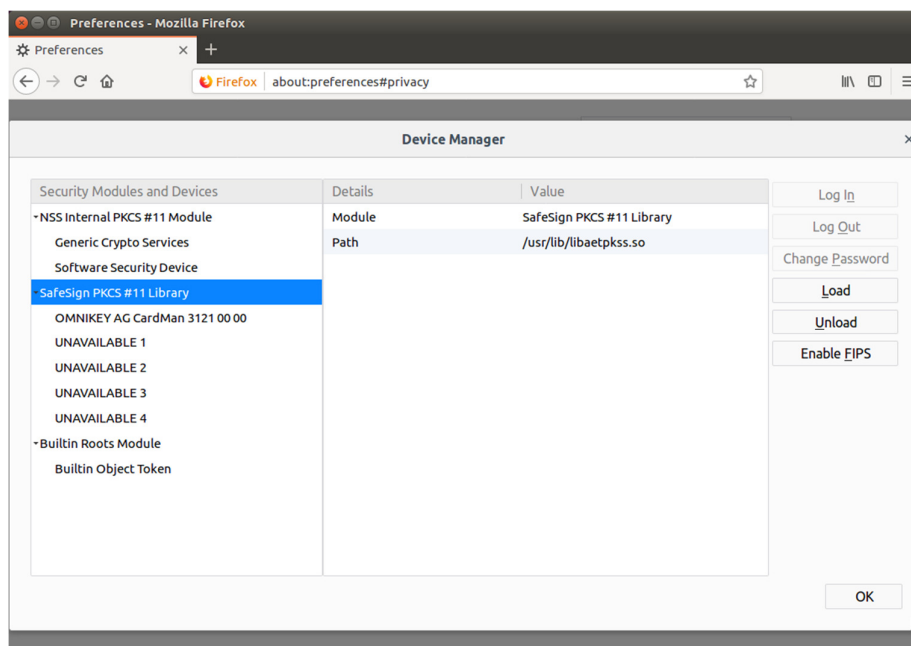


Figure 11: Firefox Device Manager: SafeSign PKCS #11 Module

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:

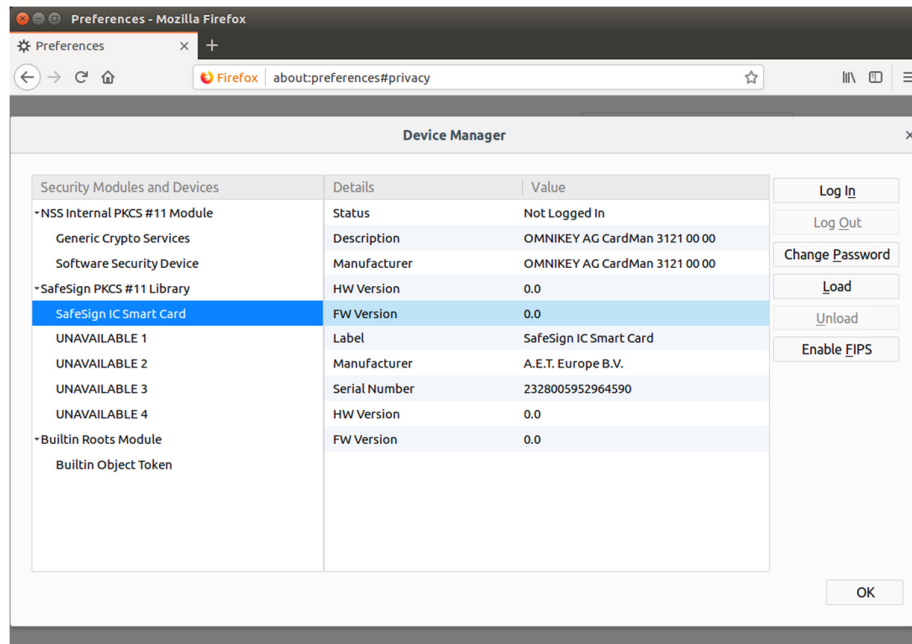


Figure 12: Firefox Device Manager: SafeSign IC Token

- 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.

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:

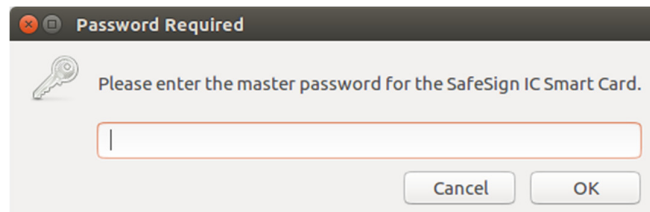


Figure 13: Firefox: Prompt

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:



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:

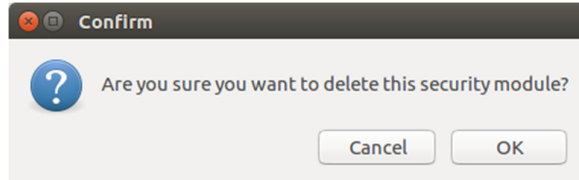


Figure 15: Firefox: Confirm

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.