SafeSign Identity Client Standard Version 3.6

Release Document for macOS

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.

SafeSign IC 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 3.6 Release Document for macOS

Project Information: SafeSign IC Release Documentation

Document revision history:

Version	Date	Author	Changes
1.0	15 September 2020	Drs C.M. van Houten	First edition for SafeSign IC Standard version 3.6 for macOS, release 3.6.0.0-AET.000

Document approval:

Version	Date	Name	Function
1.0	15 September 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 Standard version 3.6 for macOS (henceforth referred to as “SafeSign IC Standard version 3.6 for macOS”).

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 3.6 for macOS is provided as an Application Bundle distributed in a .dmg file.

All you need to do is drag and drop the tokenadmin Application Bundle to the Applications folder. This will install not only the Token Administration Utility, but will also make the PKCS #11 Library and Smart Card Extension available.

2.2 Date of Release

The date of the release is 14 August 2020.

2.3 Release Details

SafeSign IC Standard version 3.6 for macOS 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 3.6.0.0 for macOS have the name format '3.5.0.xxxx'. This is due to the fact that version 3.6.0.0 is a maintenance / consolidation release (with no new features not already in previous 3.5.x.x versions).

Release version: Standard Release 3.6.0.0-AET.000		
Description	File Name	File Version
Smart Card Extension	aetsce.appex	3.5.4448
Java Card Handling Library	libaetjcss.dylib	3.5.4427
PKCS #11 Cryptoki Library	libaetpkss.dylib	3.5.4458
Dialog Library	libaetdlglib.dylib	3.5.4315
CryptoTokenKit Library	libaetctk.dylib	3.5.4444
Secure Messaging Library	libaetsm.dylib	3.5.4445
Kit Library	libaetkit.dylib	3.5.4434
Token Administration Utility	tokenadmin	3.5.4455

2.4 Release Documents

SafeSign IC Standard version 3.6 for macOS provides at least the following release documentation:

Document Name	Version
SafeSign Identity Client Standard Version 3.6 Release Document for macOS	1.0

3 Features

The following features are supported by SafeSign IC Standard version 3.6 for macOS:

1. Multiple Token Support
2. Multiple Smart Card Reader Support
3. Multiple Application Support
4. Multiple Language Support
5. Activate QSCD Card Support

These features are described in the following paragraphs.

3.1 Multiple Token Support

SafeSign IC Standard version 3.6 for macOS supports a large number of smart cards and tokens, as listed in section 7.

Newly supported smart cards and tokens in SafeSign IC Standard version 3.6 for macOS are:

- Defensiepas 3
- UZI-pas 3
- SafeSign Default QSCD

3.2 Multiple Smart Card Reader Support

SafeSign IC Standard version 3.6 for macOS supports PCSC 2.0 Class 1 smart card readers.

The version of the CCID driver in macOS 10.14 (Mojave) is 1.4.27.
The version of the CCID driver in macOS 10.15 (Catalina) 1.4.31.

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

SafeSign IC Standard version 3.6 for macOS has been tested to support a number of smart card readers, as listed in section 8.

3.3 Multiple Application Support

SafeSign IC Standard version 3.6 for macOS supports applications on macOS that work through PKCS #11 or Smart Card Extension.

SafeSign IC Standard version 3.6 for macOS supports a number of applications, that provide the following functionality:

- Web authentication
- Email signing and encryption
- Document signing

SafeSign IC Standard version 3.6 for macOS has been tested to support a number of applications, as listed in section 9.

3.3.1 Crypto Token Kit (CTK)

With the release of OS X 10.10, Apple introduced a new native API to use a smart card and a smart card reader, called the Crypto Token Kit (CTK) Framework. The already existing PC/SC Framework remained available, but became unstable, which manifested itself particularly when removing and/or re-inserting a card or token.

Another new feature was the sandboxing of applications. Applications have to be signed and request certain permissions beforehand (entitlement) in order to be granted access. One such permissions is to access smart cards and tokens through the Crypto Token Kit.

The SafeSign IC Token Administration Utility (based on PKCS #11) is signed and has this entitlement and can thus access the CTK layer.

3.3.1.1 CTK and PKCS #11

If an application (based on PKCS #11) does not have CTK entitlement, the SafeSign PKCS #11 Library that is loaded by that application does not have this entitlement either. Such applications are then not able to (properly) communicate with the token and cannot perform such tasks as accessing a secure web site or digitally signing a document.

For such applications, AET has created a workaround in the form of a registry key that enables these applications (that do not have CTK entitlement) to communicate with tokens through PC/SC, if the communication through CTK fails. This value is called ‘EnableMacOSXPCSCLayerFallback’ and can be found in the file called “registry” in the folder Users/[user name] /Library/Application Support/safesign.

In SafeSign IC Standard version 3.6 for macOS, this value is enabled (on 1) by default. Note that when enabled, performing token operations and removing and /or (re-)inserting the token, may result in unstable behaviour (for which you need to restart the application). When disabled, (by changing its value from 1 to 0) , the token cannot be used in PKCS #11 applications.

> Please be aware that the setting is only a workaround and that AET cannot fix the original problem. If you are using a PKCS #11 application that does not have CTK entitlement, we recommend to contact the vendor or supplier of the application to have their application signed and given the right permissions to use the Crypto Token Kit.

Mozilla has solved the problem of their products Firefox and Thunderbird (see https://bugzilla.mozilla.org/show_bug.cgi?id=1593041), which means that Firefox and Thunderbird now communicate through CTK and do not require this setting anymore. However, Adobe Reader and LibreOffice still need the registry setting as a workaround, otherwise it is not possible to digitally sign documents.

3.3.2 Smart Card Extension

From macOS 10.12 (Sierra) onwards, macOS includes support for Smart Card Driver Extensions, which is defined as follows:

“You can now create NSExtension-based smart card drivers, allowing the contents of certain types of smart cards to be presented as part of the system keychain. This mechanism is intended to replace the deprecated Common Data Security Architecture, although for macOS 10.12, both architectures are supported. The driver extensions are limited to read-only mode, so that it is not possible to alter the contents of a smart card using the standard keychain interface.”

From:
https://developer.apple.com/library/content/releasenotes/MacOSX/WhatsNewInOSX/Articles/OSXv10.html

AET has created such a smart card driver extension, called ‘aetsce.appex’, which is located in the PlugIns folder in the Tokenadmin.app folder (Applications > tokenadmin > Contents > Plugins), after SafeSign IC has been installed.

This smart card extension is used for Apple (native) applications, such as Safari, replacing AET’s TokenLounge product, which was using the deprecated CDSA architecture (since OS X 10.7 / Lion).

Because the extension is read-only (by design), the contents of the smart card are not visible in the KeyChain.app (as with TokenLounge), in accordance with the description above and Apple requirements. The objects are imported in the user’s keychain database.

3.3.2.1 Smart Card Logon

With a smart card driver extension, it should be possible to use the smart card for logon purposes.

- Note that to be able to use the smart card for logon, it needs to contain a certificate suitable for smart card logon (key usage Smart Card Logon).

When a smart card is inserted for which a registered smart card extension is running, macOS will present the "SmartCard Pairing" dialog box. After successfully pairing the smartcard with the current (logged-in) user, you should be able to do smart card logon.

However, smart card logon does work from a locked screen, but it does not work when the user is logged off or the system is restarted. After a log out, you are not able to log in using the PIN because macOS does not change the text "Enter password" to "PIN" on the logon dialog box.

We have seen this issue on all versions of macOS starting from 10.12.6 up to 10.15.5.

AET has submitted a bug report to Apple and awaits their input and changes done at the OS level by Apple to allow for smart card logon with a SafeSign IC token. Until that time, users may choose to pair their smart card, as described in section 11.1.1, but should be aware that smart card logon will not work.

- There is also an issue that when a smart card or token containing a 1024 bits key is inserted, the Smart Card Pairing dialog does not appear, althoug the card / certificate can be used with the smart card driver extension. For this issue, a bug report has been filed as well.

3.4 Multiple Language Support

SafeSign IC Standard version 3.6 for macOS supports a number of different languages, as listed in section 10.

Although your Mac is (usually) set to display the language of the country in which it was purchased, you can choose a different language to use.

You can set language and region options in Language & Region preferences (under Apple menu > System Preferences).

See section 10.

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.

From SafeSign IC Standard Version 3.6.0.0 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 be very specific. It may require the user to:

- authenticate to the card by entering the PIN (UZI-pas 3);
- change the Transport PIN set for the card (Defensiepas 3);
- enter a label and a new PUK and PIN for the card (SafeSign Default QSCD).

SafeSign IC Standard version 3.6 for macOS supports the following QSCD cards:

- Defensiepas 3
- UZI-pas 3
- SafeSign Default QSCD

4 New Features and Fixes

SafeSign IC Standard version 3.6 for macOS 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 Defensiepas 3 (ATR) on NXP JCOP 3 SecID P60.
- Added support for UZI-pas 3 (ATR) on NXP JCOP 3 SecID P60.
- Added support for the SafeSign Default QSCD (ATR) on NXP JCOP 3 SecID P60.
- 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)
    - Import Digital ID (option in **Digital IDs** menu)
- Added support for OpenSSL 1.1.1 in the SafeSign IC Standard binaries.

4.2 Fixed

- 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 3.6 for macOS. 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.
- 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.
- The Token Administration Utility should not be running in the background when other applications using the smart card or token are open. The Token Administration Utility is a user interface, intended for local smart card operations, such as changing the PIN. If the Token Administration Utility is running in the background and another application (using PKCS #11 or Smart Card Extension) is also running, they might interfere, resulting in for example, the application asking for the PIN multiple times when doing a secure web authentication or the Token Administration Utility to wait before doing a certain card operation (such as Show Token Objects).
- When a smart card PIN contains diacritics (such ö or é), as a result of personalizing the card or setting the PIN on Windows with the registry setting LimitPINToASCII disabled, the PIN will not work on macOS. When disabling this setting on macOS, the diacritics are ignored.
- When a smart card or token containing a 1024 bits key is inserted, the Smart Card Pairing dialog does not appear.

6 Supported Operating Systems

SafeSign IC Standard version 3.6 for macOS has been tested to support the following macOS Operating System(s):

Operating System	SafeSign IC 3.6.0.0
macOS 10.14.6	√
macOS 10.15.6	√

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 3.6 for macOS is not tested to work on beta versions of the mentioned Operating Systems.

7 Supported Tokens

SafeSign IC Standard version 3.6 for macOS 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 3.6 for macOS.

The number of cards supported in SafeSign IC for macOS 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 Identity Client 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
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

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

8 Supported Smart Card Readers

In principle, SafeSign IC Standard version 3.6 for macOS supports PC/SC 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.

The following table lists the specific readers that have been tested with SafeSign IC Standard version 3.6 for macOS:

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 Standard version for macOS, may not (still) work or be supported in any or all versions of SafeSign IC Standard version 3.6 for macOS.

9 Supported Applications

SafeSign IC Standard version 3.6 for macOS has been tested in accordance with AET's Quality Assurance procedures and the SafeSign IC Standard for macOS 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 3.6 for macOS:

Application	Version	Functionality
Token Administration Utility	3.5.4455	PKCS #11 token management functions
Google Chrome	85.0.4138.102	Authentication to a secure web site
Mozilla Firefox	80.0.1	Authentication to a secure web site
Mozilla Thunderbird	68.12.0	Signing and decrypting e-mail messages
Apple Safari	13.1.1	Authentication to a secure web site
Apple Mail	10.14: 12.4 10.15: 13.4	Signing and decypting e-mail messages
Adobe Reader DC	10.14: 2019.012.20034 10.15: 2020.012.20043	Digitally signing a document
LibreOffice	7.0.1.2	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.dylib') can be found in: /Applications/tokenadmin.app/Contents/Frameworks/.
- The Chrome browser supports Apple Smart Card Extension, thus making it possible to use a token for secure web authentication.
- 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 Users/[user name] /Library/Application Support/safesign. The features to be enabled (1) or disabled (0) are located under 'Actions'.

- The registry file also included the setting 'EnableMacOSXPCSCLayerFallback', under '2.0'.

9.2 Google Chrome

The Google Chrome browser works with the AET Smart Card Extension. When installed correctly, you can perform secure web authentication with a SafeSign IC token.

9.3 Mozilla Firefox

With the SafeSign PKCS #11 Library installed as a security module in Firefox (as described in section 11.2), 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).

9.4 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).

9.5 Apple Safari

The Apple Safari browser works with the AET Smart Card Extension. When installed correctly, you can perform secure web authentication with a SafeSign IC token.

9.6 Apple Mail

The Apple Mail application works with the AET Smart Card Extension. When installedc correctly, you can send and receive signed and/or encrypted message with a SafeSign IC token.

9.7 Adobe Reader DC

With the SafeSign PKCS #11 Library installed as a security module in Adobe, you can sign documents with a SafeSign IC token.

To verify whether the SafeSign PKCS #11 Library is installed as a security module in Adobe Reader DC, go to Acrobat Reader -> Preferences -> Signatures -> Identities & Trusted Certificates: More.

> Note that when you want to sign a document, you will first need to login to the PKCS#11 token, before your certificates for signing will be available / displayed.

9.8 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 11.2), you can sign documents with a SafeSign IC token.

10 Supported Languages

The following languages are supported in SafeSign IC Standard version 3.6 for macOS:

- Basque (EU);
- Brazilian (PT_BR);
- Catalan (CA);
- Chinese (ZH);
- Chinese Hong Kong (ZH_HK);
- Chinese Taiwan (ZH_TW).
- Croatian (HR);
- Czech (CS);
- Dutch (NL);
- English (EN);
- Finnish (FI);
- French (FR);
- German (DE);
- Hungarian (HU);
- Italian (IT);
- Japanese (JA);
- Korean (KO);
- Lithuanian language (LT);
- Portuguese (PT);
- Russian (RU);
- Serbian, Cyrillic and Latin (SR);
- Spanish (ES);
- Swiss Italian (IT_CH);
- Thai (TH);
- Turkish (TR);
- Ukrainian (UK);

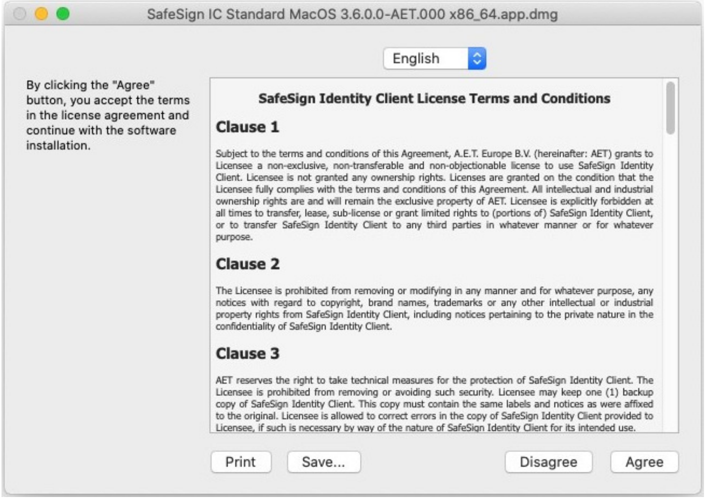
11 SafeSign IC Installation

Note that users need to have sufficient privileges and basic knowledge of macOS to install SafeSign IC Standard version 3.6 for macOS.

- Note that if any previous version of SafeSign IC for macOS and/or TokenLounge are installed, these should be uninstalled. Make sure to restart your computer after uninstallation.

Save the installation file (.dmg) to a location on your MAC computer and open it (to mount it as a volume called "tokenadmin").

This will open the *SafeSign Identity Client License Terms and Conditions* window:



SafeSign IC Standard MacOS 3.6.0.0-AET.000 x86_64.app.dmg

English

By clicking the "Agree" button, you accept the terms in the license agreement and continue with the software installation.

SafeSign Identity Client License Terms and Conditions

Clause 1

Subject to the terms and conditions of this Agreement, A.E.T. Europe B.V. (hereinafter: AET) grants to Licensee a non-exclusive, non-transferable and non-objectionable license to use SafeSign Identity Client. Licensee is not granted any ownership rights. Licenses are granted on the condition that the Licensee fully complies with the terms and conditions of this Agreement. All intellectual and industrial ownership rights are and will remain the exclusive property of AET. Licensee is explicitly forbidden at all times to transfer, lease, sub-license or grant limited rights to (portions of) SafeSign Identity Client, or to transfer SafeSign Identity Client to any third parties in whatever manner or for whatever purpose.

Clause 2

The Licensee is prohibited from removing or modifying in any manner and for whatever purpose, any notices with regard to copyright, brand names, trademarks or any other intellectual or industrial property rights from SafeSign Identity Client, including notices pertaining to the private nature in the confidentiality of SafeSign Identity Client.

Clause 3

AET reserves the right to take technical measures for the protection of SafeSign Identity Client. The Licensee is prohibited from removing or avoiding such security. Licensee may keep one (1) backup copy of SafeSign Identity Client. This copy must contain the same labels and notices as were affixed to the original. Licensee is allowed to correct errors in the copy of SafeSign Identity Client provided to Licensee, if such is necessary by way of the nature of SafeSign Identity Client for its intended use.

Figure 1: SafeSign Identity Client License Terms and Conditions

- Carefully read the License and click **Agree** to continue with the software installation

Upon clicking **Agree**, the following window will be displayed:

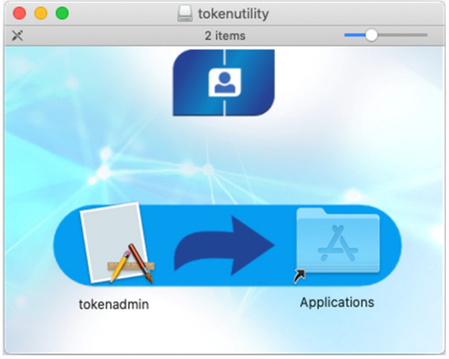


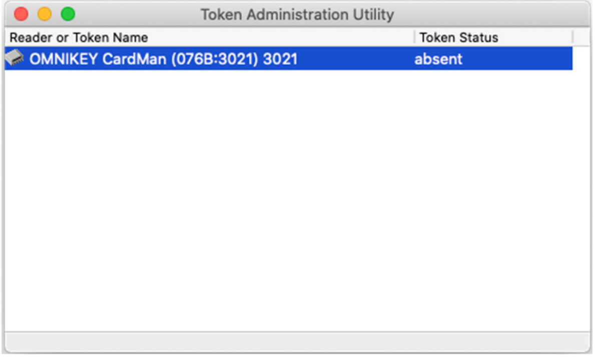
Figure 2: tokenadmin

By dragging the tokenadmin Application Bundle to the Applications folder, SafeSign IC will be installed.

- Drag the tokenadmin icon to the Applications icon
- Close the tokenadmin window and eject the "tokenadmin" volume.

11.1 Register Smart Card Extension

In order to be able to use your token with macOS (native) applications that support Smart Card Extension, you should start the tokenadmin.app (available in the Applications folder) at least once, with a smart card reader attached or a USB token inserted (so that the system is told where to look for the smart card extension):



Token Administration Utility

Reader or Token Name	Token Status
OMNIKEY CardMan (076B:3021) 3021	absent

Figure 3: Token Administration Utility: Reader Name

This will register the AET Smart Card Extension.

- In some cases, this action may not be enough and either a logout or login is necessary (and in some very rare cases, a complete restart of the machine).

After the smart card extension is registered, when inserting a smart card, macOS will try to match the AID of the inserted card with a registered smart card extension. When this is done, the smart card objects will be imported into the user's keychain database. Note that this is read-only, it is not possible to alter the contents of a smart card using the standard keychain interface (application).

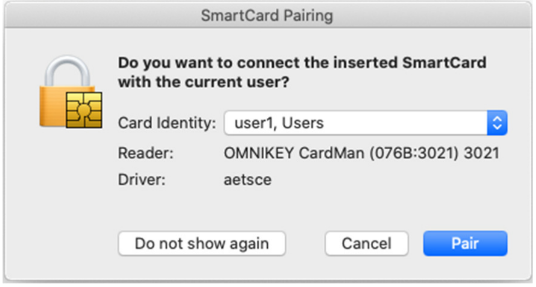
When the Smart Card Extension is registered successfully and the smart cards objects imported in the keychain database, you will be able to use your smart card for such applications as Safari.

11.1.1 Smart Card Pairing

When the initial process described above has taken place, the macOS security layer will show a pairing dialog, intended to enable your smart card for logon. However, there is an issue with smart card logon on macOS, as described in section 3.3.2.1. Once this is fixed, it will be possible to use the smart card for logon.

Though the pairing process can be completed successfully, users are advised not to do so. The description below is for information only.

When the dialog appears, you can choose to:



Do you want to connect the inserted SmartCard with the current user?

Card Identity: user1, Users

Reader: OMNIKEY CardMan (076B:3021) 3021

Driver: aetsce

Figure 4: SmartCard Pairing: Card Identity

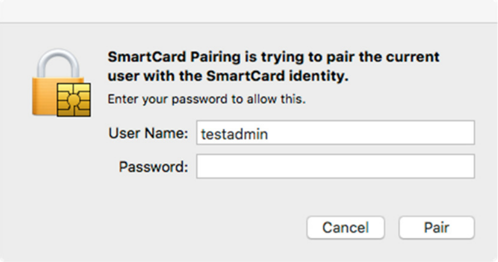
- Cancel: the dialog will re-appear each time you insert a card (even the same card)
- Pair: the pairing process will commence
- Do not show again: this dialog will not re-appear for any card you insert.

Note that if you opt for pairing, you should finish the whole pairing process.

Note that if you opt not to show the dialog again, its (re-)appearance can only be re-enabled though an appropriate command in a Terminal window.

If the user opts for pairing, the following process will take place:

1 Ask permission for writing into the DirectoryService:



SmartCard Pairing is trying to pair the current user with the SmartCard identity.

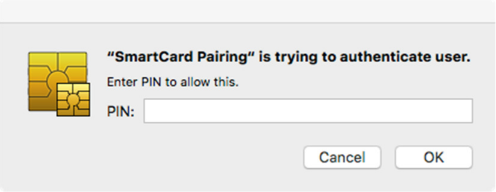
Enter your password to allow this.

User Name: testadmin

Password:

Figure 5: SmartCard Pairing is trying to pair the current user with the SmartCard identity

2 Ask for the PIN of the smart card:



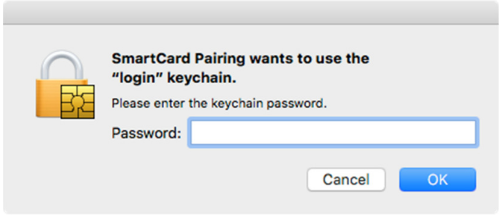
"SmartCard Pairing" is trying to authenticate user.

Enter PIN to allow this.

PIN:

Figure 6: SmartCard Pairing is trying to authenticate user

3 Ask for the Login Keychain password:


SmartCard Pairing wants to use the “login” keychain.

Please enter the keychain password.

Password:

Figure 7: SmartCard Pairing wants to use the “login” keychain

11.2 Installation of Security Module

When you have installed SafeSign IC Standard version 3.6 for macOS, 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, such as Adobe Reader DC. In order to do so, you should install or “load” the SafeSign Identity Client PKCS #11 library as a security module in these applications .

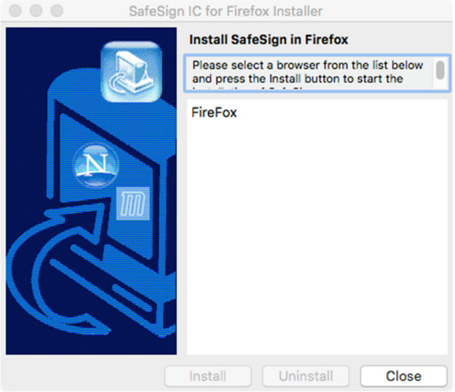
For Firefox, this functionality is included in the Token Administration Utility. Please refer to section 11.2.1.

For other applications such as Thunderbird and Adobe Reader DC, 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 11.2.2.

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).

11.2.1 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:



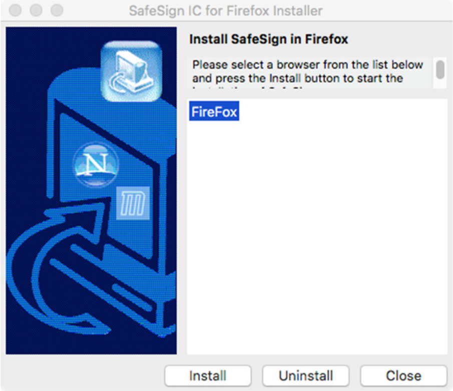
Install SafeSign in Firefox

Please select a browser from the list below and press the Install button to start the

FireFox

Figure 8: SafeSign IC for Firefox Installer: Install SafeSign in Firefox

Select Firefox as in the picture below:

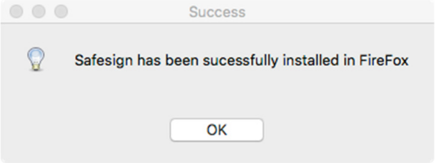

SafeSign IC for Firefox Installer
Install SafeSign in Firefox
FireFox
Install
Uninstall
Close

Please select a browser from the list below and press the Install button to start the

Figure 9: safeSign IC for Firefox Installer: FireFox

- Click Install

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



Safesign has been sucessfully installed in FireFox

Figure 10: SafeSign for Firefox Installer: Success

- Click OK

11.2.2 Manual install in Firefox

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

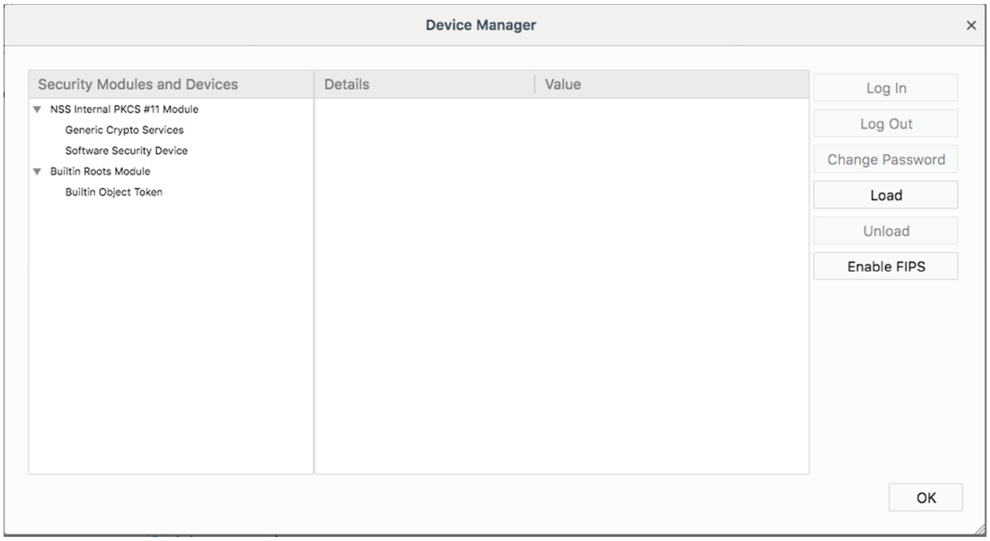
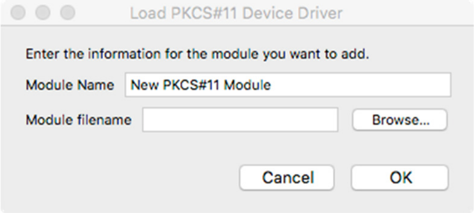


Figure 11: Firefox Device Manager: Security Modules and Devices

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.

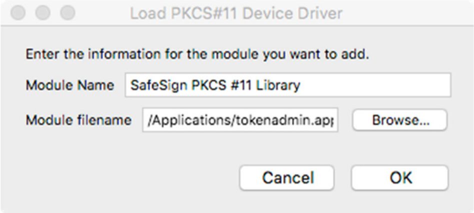
Module Name: New PKCS#11 Module

Module filename:

Figure 12: 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. /Applications/tokenadmin.app/Contents/Frameworks/libaetpkss.dylib

The dialog will now look like this:



Enter the information for the module you want to add.

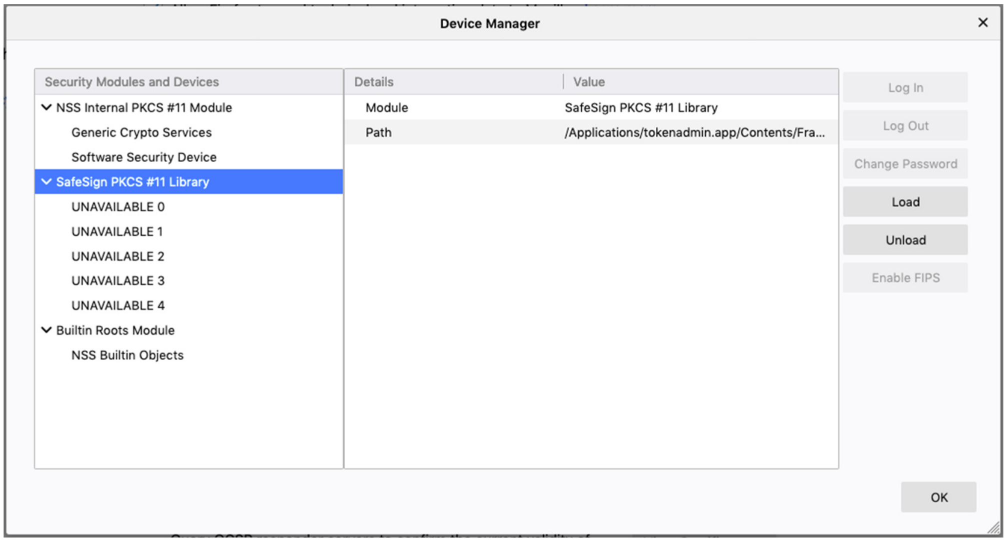
Module Name: SafeSign PKCS #11 Library

Module filename: /Applications/tokenadmin.app

Figure 13: 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:

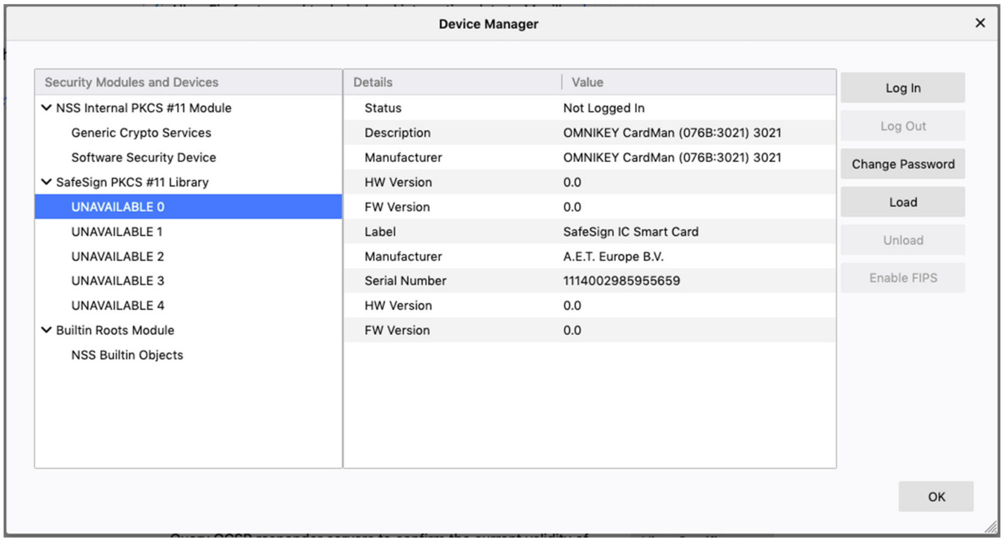


Security Modules and Devices
- NSS Internal PKCS #11 Module
  - Generic Crypto Services
  - Software Security Device
- SafeSign PKCS #11 Library
  - UNAVAILABLE 0
  - UNAVAILABLE 1
  - UNAVAILABLE 2
  - UNAVAILABLE 3
  - UNAVAILABLE 4
- Builtin Roots Module
  - NSS Builtin Objects

Details	Value
Module	SafeSign PKCS #11 Library
Path	/Applications/tokenadmin.app/Contents/Fra...

Figure 14: Firefox Device Manager: SafeSign PKCS #11 Module

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



Device Manager

Security Modules and Devices

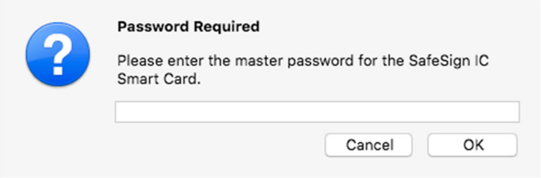
- NSS Internal PKCS #11 Module
  - Generic Crypto Services
  - Software Security Device
- SafeSign PKCS #11 Library
  - UNAVAILABLE 0
  - UNAVAILABLE 1
  - UNAVAILABLE 2
  - UNAVAILABLE 3
  - UNAVAILABLE 4
- Builtin Roots Module
  - NSS Builtin Objects

Details	Value
Status	Not Logged In
Description	OMNIKEY CardMan (076B:3021) 3021
Manufacturer	OMNIKEY CardMan (076B:3021) 3021
HW Version	0.0
FW Version	0.0
Label	SafeSign IC Smart Card
Manufacturer	A.E.T. Europe B.V.
Serial Number	1114002985955659
HW Version	0.0
FW Version	0.0

Figure 15: 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:



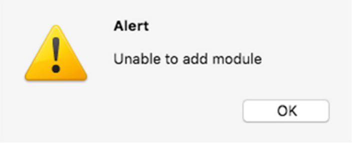
Password Required

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

Figure 16: Firefox: Prompt

11.2.3 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

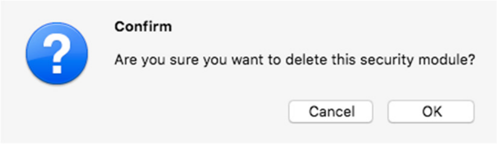
Figure 17: Firefox: Unable to add module

Verify that you have provided the correct path and name, i.e. /Applications/tokenadmin.app/Contents/Frameworks/libaetpkss.dylib.

11.2.4 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 18: Firefox: Confirm

11.3 Uninstallation

It is possible to uninstall SafeSign IC Standard version 3.6 for macOS from your macOS computer.

Before uninstalling SafeSign IC, you need to take into account the following requirements:

1 Make sure that no smart card or token is inserted;

2 Close the Token Administration Utility / make sure that the Token Administration Utility is not open / running;

3 Restart the computer.

You can then uninstall SafeSign IC Standard version 3.6 for macOS, by dragging the tokenadmin Application Bundle to the Trash can or to right-click the tokenadmin application and select ‘Move to Trash’ (macOS 10.14) / ‘Move to Bin’(macOS 10.15).

This procedure is required because the Smart Card Extension process may still be running, making it impossible to uninstall SafeSign IC.

Note that more experienced users may use a Terminal to kill the Smart Card Extension process.