aet europe

SafeSign IC Standard Version 4.2

Release Document for macOS

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

trust accelerates growth

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.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

Table of Contents

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

Table of Figures

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

Document Information

Document revision history:

Version	Date	Author	Changes
1.0	10/25/2024	C.M. van Houten	Final version for SafeSign IC Standard Version 4.2 for macOS: release 4.2.0.0-AET.000
1.1	12/17/2024	C.M. van Houten	Updated version for SafeSign IC Standard Version 4.2 for macOS: release 4.2.1.0-AET.000

Related documents

Document ID	Title	Author	Details

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

1 About this Document

The aim of this document is to document the status of the release of SafeSign Identity Client Standard version 4.2 for macOS (henceforth referred to as “SafeSign IC Standard version 4.2 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.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

2 Release Information

2.1 Deliverables

SafeSign IC Standard version 4.2 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 18 December 2024.

2.3 Release Details

SafeSign IC Standard version 4.2 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 4.2 do not necessarily have the name '4.2.xx.xx'.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

Release Version: Standard Release 4.2.0.0-AET.000		
Description	**File Name**	**File Version**
Smart Card Extension	aetsce.appex	4.5.12.1
Java Card Handling Library	libaetjcss.dylib	3.9.10.1
PKCS #11 Cryptoki Library	libaetpkss.dylib	3.9.24.1
CryptoTokenKit Library	libaetctk.dylib	4.3.12.1
Dialog Library	libaetdlglib.dylib	3.7.21.1
Secure Messaging Library	libaetsm.dylib	3.9.16.1
Kit Library	libaetkit.dylib	4.1.11.1
Token Administration Utility	tokenadmin	3.8.46.1

2.4 Release Documents

SafeSign IC Standard version 4.2 for macOS provides at least the following release documentation:

Document Name	Version
SafeSign IC Standard Version 4.2 Release Document for macOS	1.1

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

3 Features

The following features are supported by SafeSign IC Standard version 4.2 for macOS:

- Multiple Token Support
- Multiple Smart Card Reader Support
- Multiple Application Support
- Multiple Language Support
- Activate QSCD Card Support
- RSA 4096-bits Key Support
- ECC Key Support

These features are described in the following paragraphs.

3.1 Multiple Token Support

SafeSign IC Standard version 4.2 for macOS supports an large number of smart cards and tokens, as listed in section 7.

3.2 Multiple Smart Card Reader Support

SafeSign IC Standard version 4.2 for macOS supports the use of PC/SC v2.0 Class 1 smart card readers.

SafeSign IC Standard version 4.2 for macOS includes extended APDU support for some additional smart card readers. See section 3.6.1 with regard to smart card readers and extended APDUs.

SafeSign IC Standard version 4.2 for macOS has been tested to support a number of smart card readers, as listed in section 8.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

3.3 Multiple Application Support

SafeSign IC Standard version 4.2 for macOS supports applications on macOS that work through PKCS #11 and Smart Card Extension.

SafeSign IC Standard version 4.2 for macOS supports a number of applications, that provide the following functionality:

- Web authentication
- Email signing and encryption
- Document signing

SafeSign IC Standard version 4.2 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.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

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 Europe 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/[username]/Library/Application Support/safesign.

In SafeSign IC Standard version 4.2 for macOS, this value is enabled (set to 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 Europe cannot fix the original problem. If you are using a PKCS #11 application that does not have a 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.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

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 Europe 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 (mainly) used for Apple (native) applications, such as Safari and Mail.

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

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

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 15.2.

AET Europe 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 11.2.1, 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, although the card/certificate can be used with the smart card driver extension. For this issue, a bug report has been filed as well.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

3.4 Multiple Language Support

SafeSign IC Standard version 4.2 for macOS supports a number of different languages.

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.

- Note that not all languages may be fully supported by macOS.

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

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 responsible for activating the card (keys), i.e. to change the state of the card (keys) from non-operational to operational.

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

- Note that the activation process for a particular card may be very specific. It may require the user to:
  - authenticate to the card by entering the PIN (UZI-pas 3, UZI-pas 4 and SafeSign QSCD);
  - change the Transport PIN set for the card (Defensiepas 3);

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

SafeSign IC Standard for macOS version 4.2 supports the following QSCD cards:

- Defensiepas 3
- UZI-pas 3
- SafeSign Default/Generic QSCD (JCOP 3)
- UZI-pas 4
- QSCD on JCOP 4

3.6 RSA 4096-bits Key Support

SafeSign IC Standard version 4.2 for macOS includes support for RSA 4096-bits keys.

- Note that support for RSA 3072-bits keys is also included.

This functionality requires one of the following cards/tokens:

- A JCOP 4 QSCD card with the Common Criteria (CC) certified SafeSign IC applet, i.e. applet version 3.0.1.12 or 3.0.1.13 and a smart card reader that supports extended APDUs.
- A G+D Sm@rtCafe Expert 7.0 FIPS card with SafeSign IC (StdR) applet, i.e. applet version 3.1.0.36 or 3.1.0.37.
- A G+D Sm@rtcafe Expert 7.0 CUT S (M) USB token with SafeSign IC (StdR) applet, i.e. applet version 3.1.0.35, 3.1.0.36 or 3.1.0.37.

- Note that applet version 3.1.0.37 supports secure messaging for Brazil.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

3.6.1 Extended APDU

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

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

- Note that only the JCOP 4 QSCD card with the Common Criteria (CC) certified SafeSign IC applet, i.e. applet version 3.0.1.12 or 3.0.1.13, requires a smart card reader with extended APDU support for RSA 3072-bits and 4096-bit keys.

The registry can be found here: /Users/[username]/Library/Application Support/safesign

The list can be found in the registry under:
HKEY_LOCAL_MACHINE\SOFTWARE\A.E.T. Europe B.V.\SafeSign\2.0\Readers\

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

See also section 8.1.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

3.7 ECC Key Support

SafeSign IC Standard version 4.2 for macOS includes support for ECC keys.

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

- A JCOP 4 QSCD card with the Common Criteria (CC) certified SafeSign IC applet, i.e. applet version 3.0.1.13.
- A G+D Sm@rtCafe Expert 7.0 card with SafeSign IC (StdR) applet, i.e. applet version 3.1.0.36 or 3.1.0.37.
- A G+D Sm@rtcafe Expert 7.0 CUT S USB token with SafeSign IC (StdR) applet, i.e. applet version 3.1.0.36 or 3.1.0.37.

The following NIST named curves are supported:

- P-256
- P-384
- P-521

The following algorithms are supported for these curves:

- ECDSA
- ECDH

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

4 New Features and Fixes

4.1 New

- Added support for macOS 15 (Sequoia).
- Added support for the Gemalto IDBridge CT40 smart card reader (for use with extended APDUs).
- Added support for the Thales IDBridge K30 USB secure token (for use with extended APDUs).
- Added support for the ACS ACR40T (Standard) SIM-sized smart card reader (for use with extended APDUs).

4.2 Fixes

- The option Activate card has been added to the token context menu, so right-clicking on the token name will include the option to activate the card.
- Serbian translations (both Latin and Cyrillic) have been added for the activate card option and its associated success / failure messages.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

4.2.1 4.2.1.0

- From SafeSign IC version 4.1 onwards, SafeSign IC has been updated to use OpenSSL 3.0.x, in order to solve any potential vulnerabilities/issues with earlier versions. However, in the PKCS #11 Library, the OpenSSL 3 digest methods / digest-related sequence does not work correctly for SHA256withRSA. The Verify signature method fails with an invalid signature after signing. This has been fixed in SafeSign IC version 4.2.1.0.
- From SafeSign IC version 4.1 onwards, there was an issue when analysing certificate quality (Token > Analyse certificate quality) with ECDH/ECDSA P-521 keys with SafeSign IC applet version 3.1.0.36 and higher on a G&D Sm@rtCafé Expert 7.0 card / token. Note that although the certificate is reported to be unusable, because “the private key does not match with the public key in the certificate” and “the public key does not match with the public key in the certificate”, a dump of the token contents shows no errors and the key / certificate can be used in applications. This issue has been fixed in SafeSign IC version 4.2.1.0.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

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.
- Web authentication with an ECC key/certificate using the SafeSign IC PKCS #11 library installed as a security module in Firefox fails, with the web site not loading after entering the PIN and selecting a certificate. This happens in the latest versions of Firefox 131.x and 133.x (while version 123.x and 127.x are still working). This issue has been observed on other Operating Systems as well. Note that there is no issue when using the OS client integration (with the Smart Card Extension).
- Signing and encrypting and/or decrypting an e-mail message with an ECC key/certificate using the SafeSign IC PKCS #11 library installed as a security module in Thunderbird results in an error message (unable to sign / encrypt message). However, this issue was reproduced with an ECC key generated in software as well and other evidence seems to point to this being a limitation within Thunderbird. It is expected that Thunderbird will start working once it has been implemented properly.
- When signing a document with Adobe Reader with an ECC key/certificate (ECDH or ECDSA), there is an error when the issuer type of the certificate is RSA ("The credential selected for signing is invalid"). This issue was reproduced with an ECC key generated in software as well, so this seems to points to an issue within Adobe Reader. Possibly, Adobe Reader determines the signature algorithm type on the signature algorithm used to sign the certificate, requiring the issuer's certificate to be the same type. Note that there is no error message when signing (which seems to succeed), but when clicking the signature, it says "The document has been altered or corrupted since the Signature was applied".

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

- There is an issue with encrypting/decrypting in Apple Mail, when using an ECC certificate. It seems that the key usage extension plays a role in mail encryption in macOS. Apparently, a key/certificate with a key encipherment key usage extension set is needed. This issue was reproduced with an ECC key generated in software as well, so this seems to point to a limitation within Apple Mail. Note that this issue does not exist when using an RSA key for encrypting/decrypting.
- For the pairing dialog to appear, an RSA or ECDSA key/certificate needs to be present on a JCOP 4 QSCD card; on a G+D Sm@rtCafe Expert 7.0 card/token, an RSA key/certificate needs to be present.
- There is an issue with signing a document in LibreOffice when using a JCOP 4 card or G+D Sm@rtCafe Expert 7.0 card or token with RSA 3072-bits/4096-bits keys. Signing a document seems to succeed, but the "signatures in this document are invalid". This is caused by the fact that LibreOffice does not have a CTK entitlement, whereupon it will fall back to PC/SC, making the use of extended APDUs not possible.
- There is an issue with LibreOffice signing documents with an ECC key, where you can select the certificate, but no signing taking place. This seems to be related to the aforementioned issue with the use of the PKCS #11 Library in Firefox 131.x and ECC keys.
- Receiving an RSA-signed and encrypted message in Thunderbird with a G+D Sm@rtCafe Expert 7.0 card or token with SafeSign IC RIC applet (e.g. applet version 3.1.0.14 or 3.1.0.37) with secure messaging enabled, fails. Thunderbird reports that it cannot decrypt the message. Note that previous versions of Thunderbird may work.
- There is an issue with Safari web authentication using an UZI-pas 3 or UZI-pas 4, where there is an error "Safari can't open the page "..." because the server unexpectedly dropped the connection". When reloading the page and entering the PIN (again), the web page is displayed.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

5.2 SafeSign IC

- 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 or token containing an RSA 1024-bits key is inserted, the Smart Card Pairing dialog does not appear.
- The message that appears when a card is successfully activated is cut off. Instead of “The card has been activated, the card may be used”, the message says “The card has been activated, the card may be”.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

6 Supported Operating Systems

SafeSign IC Standard version 4.2 for macOS has been tested to support the following macOS Operating System(s):

Operating System	Version 4.2.0.0	Version 4.2.1.0
macOS 14 (Sonoma)		
macOS 14.4	√	
macOS 14.7.2		√
macOS 15 (Sequoia)		
macOS 15.0.1	√	
macOS 15.2		√

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

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

7 Supported Tokens

SafeSign IC Standard version 4.2 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 4.2 for macOS.

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

As the correct functioning of SafeSign IC is depending on a properly produced smart card or USB Token, AET Europe requires that smart cards and/or USB tokens are produced for use with SafeSign IC 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 Europe in case of problems, in addition to the purchase/existence of a valid SafeSign IC Support Agreement.

If you have any questions, please contact us (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

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

Gemalto IDCore 30
Infineon Oracle JCOS Ed.1
JCOP21 v2.3
NXP J2A080/J2A081 (JCOP 2.4.1 R3)
NXP J2D081 (JCOP 2.4.2 R2)
NXP J3A080 (JCOP 2.4.1 R3)
NXP JCOP 2.4.2 R3
NXP JCOP 3 SecID P60
NXP JCOP 4 P71
NXP JCOP 4.5
Oberthur IDone Cosmo v7.0
RDW ABR kaart
Rijkspas
Rijkspas 2
StarSign Crypto USB Token S
UZI-pas 2
UZI-pas 3 (QSCD)
UZI-pas 4 (QSCD)

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

8 Supported Smart Card Readers

SafeSign IC Standard version 4.2 for macOS provides support for PC/SC v2.0 Class 1 readers.

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

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

The following table lists the specific readers that have been tested with SafeSign IC Standard version 4.2 for macOS :

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

- Note that smart card readers that have been tested or have been working at a given time with a previous SafeSign IC Standard version for macOS, may not (still) work or be supported in any or all versions of SafeSign IC Standard version 4.2 for macOS.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

8.1 Extended APDU

In order to be able to generate RSA 4096-bits (and 3072-bits) keys on a JCOP 4 card, the smart card reader should support extended APDUs.

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

The following readers have been tested with RSA 4096-bit keys and extended APDUs:

- HID OMNIKEY 3121 USB (Part No. R31210320-01, revision B/2016 and revision D/2019)
- Neowave LinkeoA-Y
- Neowave Winkeo-A SIM
- ACS ACR38 (P/N ACR38U-N1)
- ACS ACR40T (Standard) SIM-sized smart card reader
- Gemalto/Thales IDBridge CT30
- Gemalto IDBridge CT40 smart card reader
- Gemalto GemPC Twin
- Thales IDBridge K30 USB secure token

These card readers have been tested using the OS CCID driver, i.e. the native CCID driver on macOS, with one exception, i.e. the ACS ACR40T. This reader does require driver installation on macOS.

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

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

9 Supported Applications

SafeSign IC Standard version 4.2 has been tested in accordance with AET Europe's Quality Assurance procedures and the SafeSign IC 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 4.2.1.0 (on macOS 15):

Application	Version	Purpose
Token Administration Utility	3.8.46.1	PKCS #11 token management functions
Google Chrome	131.0.6778.140	Authentication to a secure web site
Mozilla Firefox	133.0.3	Authentication to a secure web site
Mozilla Thunderbird	128.5.2esr	Signing and decrypting e-mail messages
Safari	18.2	Authentication to a secure web site
Apple Mail	16.0	Signing and decrypting e-mail messages
Adobe Reader	2024.005.20320	Digitally signing a document
LibreOffice	24.8.3	Digitally signing a document

- Note that PKCS #11 applications 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 the system directory.
- Firefox can no longer be used to do certificate enrollment with key pair generation.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

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.

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

As of Mozilla Firefox version 90, Firefox will automatically find and offer to use client authentication certificates provided by the operating system (Windows and macOS). See: https://blog.mozilla.org/security/2021/07/28/making-client-certificates-available-by-default-in-firefox-90/.

This means that on macOS, Firefox works with the AET Smart Card Extension and you no longer need to install the SafeSign PKCS #11 Library installed as a security module in Firefox.

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).

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

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 installed correctly, you can send and receive signed and/or encrypted message with a SafeSign IC token.

9.7 Adobe Reader DC

Adobe Reader DC works with the AET Smart Card Extension. When installed correctly, you can sign documents with a SafeSign IC token.

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 or Thunderbird (as described in section 11.3), you can sign documents with a SafeSign IC token.

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

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

10 Supported Languages

The following languages are supported in SafeSign IC Standard version 4.2 for macOS:

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

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

11 SafeSign IC Installation

Note that users need to have sufficient privileges and basic knowledge of macOS to install SafeSign IC Standard version 4.2 for macOS.

Note that if any previous version of SafeSign IC for macOS is installed, it 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:

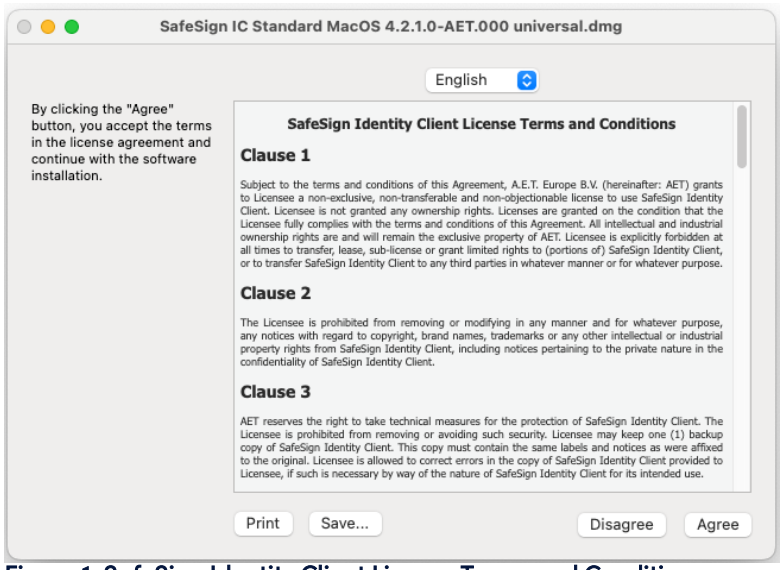

Figure 1: SafeSign Identity Client License Terms and Conditions

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

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

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

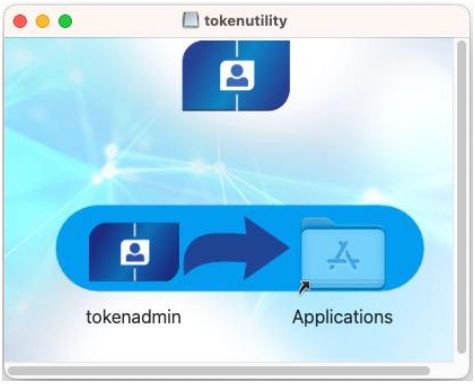

Figure 2: tokenutility

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.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

11.1 Apple Notarization

Beginning in macOS 10.15, all software built after June 1, 2019, and distributed with Developer ID must be notarized. When software is notarized, Gatekeeper places descriptive information in the initial launch dialog to help the user make an informed choice about whether to launch the app.

The SafeSign IC software has been notarised by Apple and the following message will be displayed in accordance with Apple's policy:

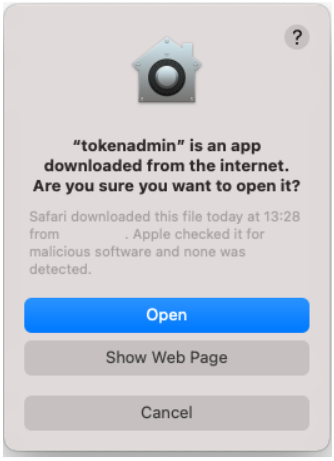

Figure 3: Gatekeeper: Are you sure you want to open it?

Once you have opened the app, this message will no longer appear.

11.1.1 Security Settings

Note that when macOS Privacy & Security Settings specify that applications are only allowed to be downloaded from the "App Store", the Tokenadmin app cannot be opened:

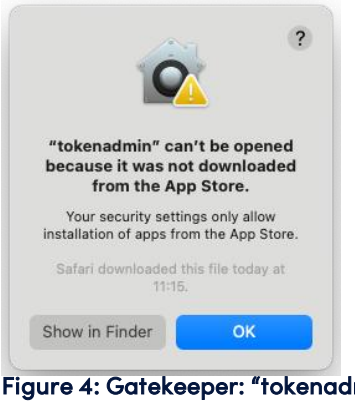

Figure 4: Gatekeeper: "tokenadmin" can't be opened

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

In order to be able to open the app, you either need to change the security setting to allow applications from the “App Store and Known Developers” (macOS 15) or “App Store and identified developers” (macOS14):

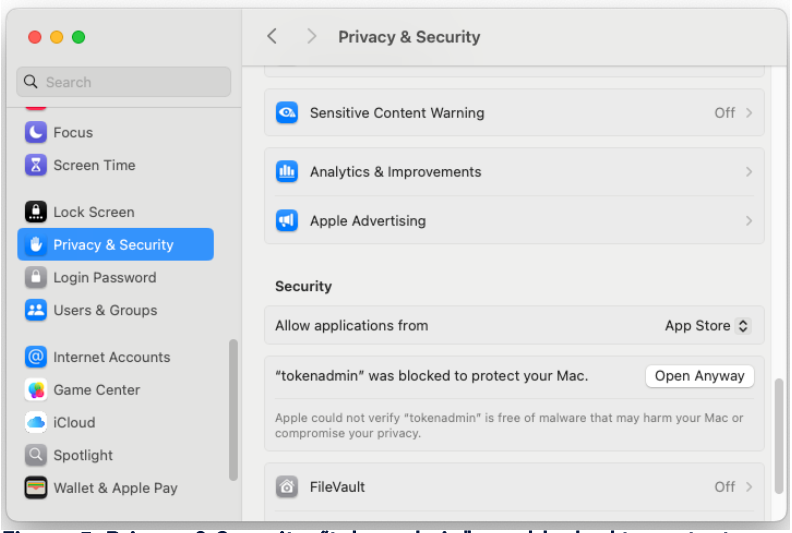

Figure 5: Privacy & Security: “tokenadmin” was blocked to protect your Mac

11.2 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).

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.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

11.2.1 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 you select a smart card, the Smart Card Pairing dialog will appear:

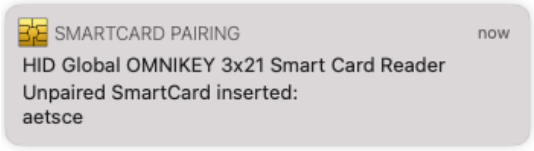

Figure 6: Smartcard Pairing: Unpaired SmartCard inserted

- Close it or click on it to start the pairing process.

If you clicked the dialog to pair your smart card, you can choose to:

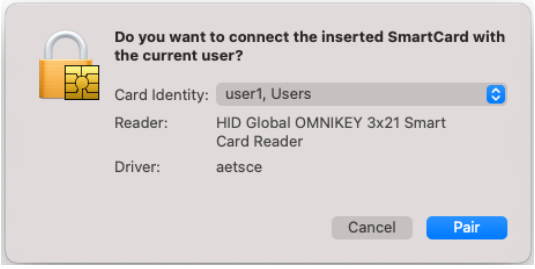

Figure 7: Smartcard Pairing: Do you want to connect

- Cancel: the dialog will reappear each time you insert a card (even the same card)
- Pair: the pairing process will commence

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

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

1. Enter the administrator's password to allow pairing;
2. Enter the PIN of the smart card;
3. Enter the Login Keychain password.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

11.3 Installation of Security Module

When you have installed SafeSign IC Standard version 4.2 for macOS, you may want to use SafeSign Identity Client with 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.

As of Mozilla Firefox version 90, Firefox will automatically find and offer to use client authentication certificates provided by the operating system on macOS, through a library/module called 'OS Client Cert Module'.

This means that Firefox now works with the SafeSign IC Smart Card Extension and that it is no longer necessary to install the SafeSign IC PKCS #11 Library as a security module in Firefox.

Note that even though the Firefox Installer is still available in the Token Administration Utility's Integration menu, installing the SafeSign IC PKCS #11 Library as a security module in Firefox is not recommended.

For other applications such as Thunderbird, you will need to do so manually, by pointing to the location and name of the SafeSign Identity Client PKCS #11 library, i.e. /Applications/tokenadmin.app/Contents/Frameworks/libaetpkss.dylib.

11.4 Uninstallation

It is possible to uninstall SafeSign IC Standard version 4.2 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.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

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

You can then uninstall SafeSign IC Standard version 4.2 for macOS, by dragging the tokenadmin Application Bundle to the Trash can or to right-click the tokenadmin application and select 'Move to Bin'.

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

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com