Unlimited access to your world

SafeSign Identity Client Standard

Release Document for OS X

Table of Contents

Table of Figures

SafeSign
Identity Client

Document Information

Title: SafeSign Identity Client Standard Release Document for OS X

Document ID: SafeSign-IC-Standard_3.0.112_OSX_Release_Document.docx

Project: SafeSign IC Release Documentation

Document revision history

Version	Date	Author	Changes
7.0	15-07-2014	Drs. C.M. van Houten	First edition for SafeSign Standard Version 3.0.97 for MAC OS X
8.0	12-08-2015	Drs C.M. van Houten	First edition for SafeSign Standard Version 3.0.101 for OS X
9.0	15-04-2016	Drs C.M. van Houten	First edition for SafeSign Standard Version 3.0.112 for OS X

Document approval

Version	Date	Name	Function
9.0	15-04-2016	B. Smid MBT	Chief Development Officer

About SafeSign Identity Client

SafeSign Identity Client (IC) is a software package that can be used to enhance the security of applications that support hardware tokens through PKCS #11 and Microsoft CryptoAPI.

The SafeSign IC package provides a standards-based PKCS #11 Library as well as a Cryptographic Service Provider (CSP) and CNG Key Storage Provider (KSP) allowing users to store public and private data on a personal token, either a smart card, USB token or SIM card. It also includes the SafeSign IC PKI applet, enabling end-users to utilise any Java Card 2.1.1 / Java Card 2.2 and higher compliant card with the SafeSign IC middleware.

Combining full compliance with leading industry standards and protocols, with flexibility and usability, SafeSign IC can be used with multiple smart cards / USB tokens, multiple Operating Systems and multiple smart card readers.

SafeSign IC allows users to initialise and use the token for encryption, authentication or digital signatures and includes all functionality necessary to use hardware tokens in a variety of PKI environments.

SafeSign IC comes in a standard version with an installer for Windows, MAC and Linux environments. It is also available for many other environments like mobile devices.

Figure 1: SafeSign Identity Client Smart card bundle

For more information, refer to the latest SafeSign IC Product Description on www.aeteurope.com.

About A.E.T. Europe B.V.

No matter who you are or what you do; there is always a specific world you want, or need to access. AET makes this possible by creating the perfect technological solution in user identification, authentication and authorization: unlimited access, twenty-four/seven.

We do not only believe your world should be accessible anytime. We are also determined to make this access easy and secure. At a time when almost everything is digital, security has become our main focus. By creating unlimited, secure and convenient access to your world, we ensure that you have the power to control your own world. You, and nobody else.

In devising the best technological solutions, we need to be fast, smart and inventive. So that’s exactly what we are. We are also passionate: about technology; about our business; about the possibility of providing convenient access to different worlds.

In our vision, everyone can benefit from the technology we offer. Because everyone deserves reliable, safe and unlimited access to the world he or she wants to enter. Which world do you want to access?

aet

Unlimited access
to your world

1 About this Document

The aim of this document is to document the status of the release of SafeSign Identity Client for OS X.

This document is intended to be a reference to both end users and administrators.

While reading this document, take into account the notes with 📌.

This document is part of the release documentation for SafeSign Identity Client.

2 Release Information

SafeSign Identity Client for OS X includes all functionality necessary to use hardware tokens in a variety of Public Key Infrastructures (PKIs). This includes:

- The SafeSign PKCS #11 Library for use with applications supporting PKCS #11.
- PKCS #15 support. PKCS #15 may be used to integrate SafeSign IC enabled hardware tokens into embedded systems after prior approval of AET.
- .dmg package for installation on the OS X platform.

2.1 OS X versions

SafeSign Identity Client Standard Version 3.0.112 for OS X comes in a standard version for the following environments:

- OS X 10.10 (“Yosemite”)
- OS X 10.11 (“El Capitan”)

2.2 Date of Release

The release date of SafeSign Identity Client Standard Version 3.0.112 for OS X is 15 April 2016.

2.3 Release Details

The following table lists the version numbers of the (major) components installed by SafeSign Identity Client Standard Version 3.0.112 for OS X:

Description (9a13b5a9d59c)	File name	File version
Java Card Handling Library	libaetjcss.dylib	3.0.3931
PKCS #11 Cryptoki Library	libaetpkss.dylib	3.0.3930
Token Administration Utility	tokenadmin	3.0.3920

This information can also be found in the Version Information dialog of the Token Administration Utility.

2.4 Release Documents

Document Name	Version
SafeSign Identity Client Standard Release Document for OS X	9.0

3 Features

In principle, SafeSign Identity Client Standard Version 3.0.112 for OS X supports all the features of SafeSign Identity Client Version 3.0.112 for Windows, if such functionality is available for the OS X platform and unless mentioned otherwise in this document. The following features are supported by SafeSign Identity Client Standard Version 3.0 for OS X:

- Multiple token support;
- Multiple language support;
- Multiple reader support;
- Multiple application support;
- Support for PIN timeout;
- Support for maximum PUK and PIN length;
- Support for virtual readers in PKCS#11;
- Support for SHA-2;
- Support for new cards and applet functionality;
- Support for 3DES key storage on the card;
- Installation as an Application Bundle (≥ 3.0.112);
- Support for Crypto Token Kit (≥ 3.0.112).

SafeSign Identity Client Standard version 3.0.112 for OS X was tested with the smart cards, USB tokens, smart card readers, applications and OS X environments listed in this document (see section 6, 7 and 8).

Note that though SafeSign Identity Client is designed to support an extensive range of tokens, only a specific number of tokens / readers (combinations) have been tested with OS X, as part of AET's Quality Assurance procedures. This does not imply that all tested tokens / readers (combinations) work flawlessly, nor that other tokens / readers (combinations) do not work.

3.1 Multiple Token Support

A token is a chip with an on-board operating system either integrated into a smart card with ISO7816 interface or integrated into a device with USB interface (called "USB Token").

SafeSign Identity Client Standard Version 3.0.112 for OS X supports a number of different tokens, as listed in section 7.

3.1.1 Version 3.0.97

Added support for the following tokens:

- Identive SCT3522DI Mifare Flex USB Token (with NXP JCOP 2.4.2 R2)

3.1.2 Version 3.0.101

Added support for the following tokens:

- Giesecke & Devrient Sm@rtCafé 7.0 (CC and FIPS)
- Rijkspas 2[1]

3.1.3 Version 3.0.112

Added support for the following tokens:

- Giesecke & Devrient SkySIM CX Hercules
- Moprho STPay 38K
- Rijkspas 2.1

3.2 Multiple language support

SafeSign Identity Client Standard Version 3.0 for OS X supports a number of different languages, including but not limited to: German (DE), Dutch (NL), English (EN), Spanish (ES), French (FR), Portuguese (PT) and Brazilian (PT_BR).

3.3 Smart Card Readers

Note that only PCSC 2.0 Class 1 readers are supported.

For certain supported readers it is of essential importance which smartcard reader driver is installed and used.

The following reader was tested in combination with the default PCSC-lite version within OS X:

- OMNIKEY 3121 USB Desktop Reader

[1] Rijkspas 2 Release 1 with SafeSign applet version 3.0.1.10.

3.4 Applications

SafeSign Identity Client Standard version 3.0.112 for OS X supports a number of PKCS #11 applications on the OS X platform. For these applications to work, the SafeSign IC PKCS #11 Library needs to be loaded / installed as a security module.

Note

Note that the SafeSign PKCS #11 Library to be installed (libaetpkss.dylib) can be found in: /Applications/tokenadmin.app/Contents/Frameworks/.

Apart from applications using PKCS #11 to access tokens, there are other applications that use Apple keychain to access tokens, including:

- native OS X applications such as Safari and Apple Mail
- Chrome and Office for Mac
- Adobe Reader DC, which supports both PKCS #11 and Apple Keychain

For these applications to work, AET offers a product called SafeSign Identity Client TokenLounge. In addition to support for those applications working with Apple Keychain, SafeSign IC TokenLounge also supports OS X login and screen unlock[2]. Prerequisite for SafeSign IC TokenLounge is that SafeSign Identity Client Standard Version 3.0.112 for OS X is installed.

Please contact AET if you are interested in this functionality.

3.4.1 Mozilla Firefox

With the SafeSign PKCS #11 Library installed as a security module in Firefox (as described in section 9.4), 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).

3.4.2 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).

[2] Local login, not enterprise smart card logon (Active Directory).

3.4.3 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.

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.

3.4.4 LibreOffice

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

In order to digitally sign a LibreOffice document, "you must install a recent version of Thunderbird, Mozilla Suite, or Firefox software to install some system files that are needed for encryption" (https://help.libreoffice.org/Common/Applying_Digital_Signatures).

3.4.5 OpenOffice

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

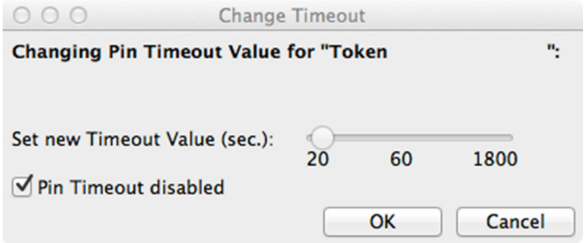
"On Macintosh systems, OpenOffice will use certificates from the Mozilla key store (used by Firefox)" (https://wiki.openoffice.org/wiki/Certificate_Detection).

3.5 Support for PIN timeout

In SafeSign Identity Client, it is possible to set a PIN timeout for PKCS #11 applications for Java Card v2.2+ cards.

By default, the PIN timeout is disabled. When the PIN timeout is enabled, you will be asked to (re-)login to the token, i.e. the SafeSign PIN dialog will be displayed. In practice, this means that for example when using Adobe Reader to sign a document, you will be asked to enter your PIN again when the maximum amount of time has passed since the last time you logged in to the token.

The timeout value for a particular token can be set in the Token Administration Utility, through the menu Token > Change PIN Timeout, if the (initialised) token is inserted and the correct PIN is entered. By default, the PIN Timeout is disabled. When enabled (by deselecting "Pin Timeout disabled"), you can set the timeout value:


Change Timeout

Changing Pin Timeout Value for "Token ":

Set new Timeout Value (sec.):

☑ Pin Timeout disabled

Figure 2: Change Timeout

The PIN Timeout cannot be set to 0 (zero) seconds, as this will expire the PIN immediately when it is entered and the credentials on the token cannot be used. Therefore the minimum PIN Timeout value is set to 20 seconds.

Note

The PIN Timeout feature does not work with secure pin pad readers, i.e. it cannot be set and does not work within applications.

3.5.1 Version 3.0.112

There was a(n) (known) issue when setting the PIN Timeout, which was that its value was not displayed in the Token Utility's Show Token Info dialog. When it is not set, this dialog would display "Disabled". When it is set, nothing (no value) would be displayed. This is fixed in SafeSign Identity Client Standard Version 3.0.112.

3.6 Support for maximum PUK and PIN length

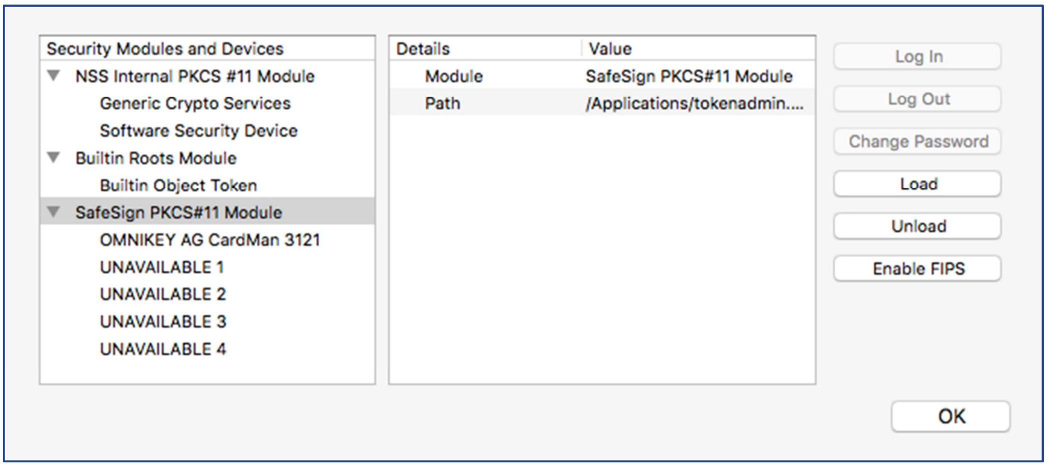
In SafeSign Identity Client a maximum PUK and PIN length is supported.

The registry keys for the different profiles supported contain the values for maximum PUK length and maximum PIN length, which can be edited. It is possible to use different values for the maximum PIN length and maximum PUK length, for the Java Card v2.2+ cards supported.

3.7 Support for virtual readers in PKCS #11

In accordance with the PKCS #11 standard, the insertion and removal of smart card readers (devices) / slots is not detected once the PKCS #11 Library is loaded[3]. In practice, this means that when a user has started a PKCS #11 application such as Firefox, adding (or removing) a reader or USB token will not be detected. If a user then tries to use the token for authentication to a web site, this will fail. This has been solved by implementing virtual reader slots. The PKCS #11 Library will now not only provide a list of (physical) readers attached to the system, but it will also provide a list of virtual reader slots (which can be filled with additional readers when they become present on the system). When a user then plugs in a new reader or USB token, the virtual reader will be replaced by the actual reader plugged in.

This can be observed in e.g. Firefox, where a list of empty slots / virtual readers will be displayed, once the SafeSign PKCS #11 Library is installed as a security module:



Security Modules and Devices

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

Details	Value
Module	SafeSign PKCS#11 Module
Path	/Applications/tokenadmin....

Figure 3: Virtual Reader support in PKCS#11

3.8 Support for SHA-2

In SafeSign Identity Client support for SHA-2 has been implemented, with the following variants: SHA-256, SHA-348 and SHA-512.

Note

It is possible to use SHA-256 as hashing algorithm with a 1024 bits key pair, but it is not possible to use SHA-484 and SHA-512 in that case. This is a limitation for security reasons.

[3] The PKCS#11 specification states: “the set of slots accessible through a Cryptoki library is fixed at the time that C_Initialize is called. If an application calls C_Initialize and C_GetSlotList, and then the user hooks up a new hardware device, that device cannot suddenly appear as a new slot if C_GetSlotList is called again.”

3.9 Support for new cards and applet functionality

For certification purposes with the ICP-Brazil standard, some new functionality was implemented in SafeSign Identity Client (applet), described briefly in the following sections from a functional point of view.

For convenience, the SafeSign Identity Client Token Utility will display the applet version in its *Show Token Info* dialog. This functionality was implemented for various cards from different vendors. Should you be interested in this functionality, please contact us.

3.9.1 Support for the RIC card

SafeSign Identity Client supports the Brazilian Identity Card, issued by the *Registro de Identidade Civil* (RIC). Functionality for the RIC Card includes card wipe functionality, which will delete PKI objects only (and not authentication objects and RIC data), if the correct PUK and PIN are entered.

3.9.2 Support for PIN policy

SafeSign Identity Client supports cards with a (pre-)defined PIN policy, where the end user may not just select any PIN or PUK code for their token, but must adhere to certain complexity rules (so called PIN and PUK policies).

In SafeSign IC the following policy has been enabled[4]:

- PIN / PUK must have at least one (01) capitalized alphabetic character (A-Z);
- PIN / PUK must have at least one (01) lowercase alphabetic character (a-z);
- PIN / PUK must have at least one (01) numerical character (0-9);
- Allow the use of special characters. Example: “$”, “@”, “&” etc.;

For this functionality to work, a special applet is required. Currently, an applet is available with support for PIN policy and recycling (see the next section).

3.9.3 Support for recycling the token

In SafeSign Identity Client it is possible to ‘recycle’ the token, i.e. once the PIN and PUK are blocked due to too many attempts (i.e. entering an incorrect PIN / PUK until the retry counter is exceeded), it is possible to reset the token so that it returns to its original initialized state.

[4] This policy is called the Diversification policy.

If the token is locked, there will be an option in the Token Utility's Token menu, allowing you to set a new token label, PUK and PIN. The number of recycle attempt depends on the amount set during applet installation (the maximum number of recycle attempts that can be set is decimal 127 / hex 7F). The Token Utility's Show Token Info dialog will display the recycle count (used and maximum)[5].

For this functionality to work, a special applet is required, with special installation parameters.

3.9.4 Support for secure messaging

SafeSign Identity Client supports secure messaging, in accordance with the ICP Brazil standard, which requires that data communication to the token from the computer is enciphered. For this purpose, the SafeSign IC applet can be configured to use MACing and encryption. This is implemented for specific cards from different vendors.

3.10 Support for 3DES key storage on the card

SafeSign Identity Client includes support for the storage of 3DES / symmetric keys on the cards. When loaded on the token, the secret keys will be visible in the Token Utility, upon displaying the private objects on the card and dumping the token contents[6].

This functionality requires a special applet.

3.11 Installation as an Application Bundle

With the release of SafeSign Identity Client Standard Version 3.0.112 for OS X, SafeSign is no longer provided as a package installer, but as an Application Bundle (distributed in a .dmg file).

Apart from being in line with the way OS X applications are commonly installed, this is a great improvement from a usability point of view, making install and uninstall more convenient.

All you need to do is to drag and drop the tokenadmin Application Bundle to the Applications folder (see section 9).

[5] The recycle counter is treated as an initialization counter: a card loaded with a recycle counter of 5 can be initialised 5 times, of which 4 are recycles. After that, the recycle option is disabled.

[6] Note that when dumping the contents of a token, only public information on the token objects will be displayed.

3.12 Support for Crypto Token Kit (CTK)

With the release of OS X 10.10, a new library was introduced to communicate with tokens, called the Crypto Token Kit (Framework). The already existing PC/SC Framework / layer remained available, but became unstable, which manifested itself particularly when removing and/or re-inserting a card or token. The new release of SafeSign Identity Client Version 3.0.112 for OS X now supports the Crypto Token Kit.

3.12.1 CTK and Sandboxing

Another feature introduced with OS X 10.10 is 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 tokens through the Crypto Token Kit[7]. The SafeSign IC Token Administration Utility has this entitlement and can thus access the CTK layer.

On release of this document, Firefox does not request this permission. Thus, when the SafeSign PKCS #11 Library is loaded by Firefox, it gets the same permissions as Firefox has (or the intersection) and is unable to access the CTK Library (as Firefox is not entitled to the CTK, neither is the PKCS #11 Library below). Firefox is thus not able to (properly) communicate with the token and cannot perform such tasks as accessing a secure web site. To solve this, AET has submitted a bug report to Mozilla, requesting to sign the application and give it the right permissions to use the Crypto Token Kit.

Apart from Mozilla Firefox, the same applies to Mozilla Thunderbird, Adobe Reader DC and OpenOffice / LibreOffice (which rely on the Mozilla Suite to be installed for their security features).

To be able to use PKCS #11 applications such as Firefox that do not have CTK entitlement, AET has created a workaround in the form of a registry key that enables them 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][8]/Library/Application Support/safesign.

By default, this value is disabled (on 0). If this value is enabled (by changing its value from 0 to 1)[9], the token can be used in PKCS #11 applications.

Note that when enabled, performing token operations and removing and /or (re-)inserting the token, may result in unstable behaviour, such as your token not being recognised in the Token Administration Utility (for which you need to restart the application).

[7] Through the so-called com.apple.security.smartcard entitlement.
[8] In Finder, this is the home directory.
[9] The file “registry” can be edited by means of, for example, TextEdit or another editor.

4 Features and Enhancements

4.1 Version 3.0.97

4.1.1 New

- Added support for the Identive SCR3522DI Mifare Flex USB Token (with JCOP 2.4.2 R2).

4.1.2 Fixed

- From Firefox version 22 onwards, the Firefox Installer does not work anymore. It reports that SafeSign is installed, but no SafeSign IC PKCS #11 module is present in the "Security modules and devices" list. Adding the library manually (as described in section 9.4.2: Manual install in Firefox) does work. This has been fixed. It is now possible to use the Firefox installer again.
- The password input field in the Import Digital ID dialog was too small. This has been fixed.

4.1.3 Enhanced

- Although SafeSign Identity Client is not vulnerable to the OpenSSL heartbleed vulnerability, as the part of OpenSSL that is causing the vulnerability is not used in SafeSign Identity Client, OpenSSL has been updated to version 1.0.1h.

4.2 Version 3.0.101

4.2.1 New

- Added support for the Giesecke & Devrient SM@rtCafé 7.0 (CC and FIPS)
- Added support for the Rijkspas 2

4.3 Version 3.0.112

4.3.1 New

- As of SafeSign Identity Client Standard version 3.0.112, a new feature is added. When importing a certificate using the Token Utility, for already through SafeSign IC PKCS #11 Library generated keys (where the certificate has been removed in between), an additional check is performed to see if there is a matching private key. If this is the case, the CKA_ID of the certificate is set to that of the key.
- Added support for the Giesecke & Devrient SkySIM CX Hercules
- Added support for the Morpho STPay 38K
- Added support for the Rijkspas 2.1

4.3.2 Fixed

- There was a known issue in previous SafeSign Identity Client Standard versions that when the PIN Timeout is set, the value field of the PIN timeout was empty. This has been fixed in SafeSign Identity Client Standard version 3.0.112.
- There was an issue in previous SafeSign Identity Client Standard versions with CardOS 4.3 and 4.4 cards, where a PIN change in the Token Utility with a wrong PIN, which contains as prefix the old PIN, does not work. Although the PIN change is confirmed / OK, the retry counter is reduced by 1 and the value of the PIN is unknown (neither the new PIN nor the wrong PIN is valid). For example, if the old PIN is 1234, but it is entered wrongly as 12345 and the new PIN is set to 123456. This has been fixed in SafeSign Identity Client Standard version 3.0.112.
- There was a problem with SPK 2.3 cards and A003 / A004 applications with PKCS #1 padding. This did not work anymore from SafeSign Identity Client Standard version 3.0.97 onwards, but has been fixed in SafeSign Identity Client Standard version 3.0.112.

4.3.3 Enhanced

- Added support for the J3D081 smart card in contactless mode, by including its contactless ATR (T=CL) to the registry.
- Added the license for OpenSSL (LICENSE.txt) in a folder called ‘3rdparty/openssl’ in the (same) location as where the SafeSign License Agreement is located, i.e. /Applications/tokenadmin.app/Contents/Resources.

5 Known Issues

5.1 General

1. Although some USB tokens may be supported by the PCSC-Lite drivers on OS X, 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.
2. Note that removal and re-insertion events are not detected (for example in the Token Administration Utility or in Mozilla applications), when the USB token and/or smart card reader is inserted or removed after the application is started. It is not possible from a PKC #11 perspective to have readers and/or tokens appearing and disappearing on the fly (even if this is detected on PC/SC level).
3. 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.

5.2 SafeSign IC

4. SafeSign Identity Client Version 3.0.112 for OS X includes only a Token Administration Utility, no Token Management Utility.
5. In the Token Administration Utility, the Task Manager is not available.
6. The Token Administration Utility does not read new certificates until card update. For example, when you do a Show Token Objects after requesting a Digital ID (from Firefox), no certificates and keys are shown. When you remove the card and insert it again, then Show Token Objects does show the certificate and keys. The issue has been reproducible only if the Token Administration Utility's Show Token Objects dialog is open while the Firefox certificate enrolment takes place.
7. When a new version of SafeSign is installed to the system, the registry is not updated. If you have a previous version of SafeSign installed to the system with specific registry settings (such as ChangeTransportPIN), then after uninstalling the old version and installing the new one you still have the same registry settings. This can be manually solved by deleting the file called "registry" (in user home folder/Library/Application Support/safesign/). Then if you restart the Token Administration Utility, it will re-create a new file called "registry" without the old settings.
8. 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).
9. 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.
10. 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).
11. 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 3.0.97

12. The uninstaller in the TokenLounge minimal installer (.dmg) can be used to un-install TokenLounge again. When you first install SafeSign and then install TokenLounge minimal then the uninstallers are correct. When you first install TokenLounge and then Safesign, then the uninstallers are not correct and get corrupted. Therefore, please observe the correct sequence of installation for SafeSign Identity Client and TokenLounge. You should first install SafeSign Identity Client and then TokenLounge.
13. In OS X 10.7 an extra password window appears ("Enter password to open file: NSS Certificate DB") when you digitally sign a document. Also the OpenOffice application seems to hang but continues after some time when you sign. On OS X 10.8 and 10.9 the "NSS Certificate DB" password window does not appear and the application responds quickly.

5.2.2 Version 3.0.112

14. Some applications are not able to communicate with a token through the Crypto Token Kit, as they are not entitled to do so (see section 3.12.1). To be able to use your token, you should enable the 'EnableMacOSXPCSCLayerFallback' registry setting.

6 Supported Versions

SafeSign Identity Client Standard has been tested to support the following OS X versions (both 32-bit and 64-bit):

Version	3.0.101	3.0.112
OS X 10.6.8 (“Snow Leopard”)	√	
OS X 10.7.5 (“Lion”)	√	
OS X 10.8.5 (“Mountain Lion”)	√	
OS X 10.9.4 (“Mavericks”)	√	
OS X 10.10 (“Yosemite”)		√
OS X 10.11 (“El Capitan”)		√

7 Supported Tokens

SafeSign Identity Client Standard supports a number of hardware tokens, as listed below.

These tokens have been tested to work at a certain time as part of the release testing for SafeSign Identity Client versions 3.0.x. The list does not imply that each token (still) works or will be supported in any or all versions of SafeSign Identity Client version 3.0.x. If you have problems with your (listed) token, please contact AET Support.

7.1 STARCOS

Note that STARCOS SPK 2.3 is only supported for customers with already deployed cards.

Token	Type	Additional remarks
G&D STARCOS SPK 2.3 v7.0	Smart Card	Series completion

7.2 Java Card 2.2.x

Token	Type	Additional remarks
Athena IDProtect	Smart Card	Java Card v2.2
Athena IDProtect Duo	Smart Card	Java Card v2.2
Athena IDProtect Duo V3	Smart Card	
Athena IDProtect v3	Smart Card	Java Card v2.2.2
Athena IDProtect v6	Smart Card	Java Card v2.2.2
Athena IDProtect Key v2	USB Token	Java Card v2.2.2
G&D Sm@rtCafé Expert 64K	Smart Card	Java Card v2.2.1
G&D StarKey400 (M) with Sm@rtCafé Expert 64K	USB Token	Java Card v2.2.1
G&D Sm@rtCafé Expert v3.0	Smart Card	Java Card v2.2.1
G&D Sm@rtCafé Expert v3.1	Smart Card	Java Card v2.2.1
G&D Sm@rtCafé Expert 3.2	Smart Card	Java Card v2.2.1
G&D Sm@rtCafé Expert v4.0	Smart Card	Java Card v2.2.1
G&D Sm@rtCafé Expert v5.0	Smart Card	Java Card v2.2.2
G&D Convego Join 4.01 40k/80k	Smart Card	Java Card v2.2.1
G&D Mobile Security Card SE 1.0	MicroSD card	Java Card v2.2.2
Gemalto GemXpresso Pro R4 72PK / TOP IM GX4	Smart Card	Java Card v2.2.1
Gemalto MultiApp ID v2.1	Smart Card	Java Card v2.2.1
Gemalto Optelio D72 FR1	Smart Card	Java Card v2.2.2

Token	Type	Additional remarks
Gemalto USB eSeal Token V2 TOP IM GX4	USB Token	Java Card v2.2.1
Gemalto TOP DL v2	Smart Card	Java Card v2.2.1
Gemalto Desineo ICP D72 FXR1 Java	Smart Card	Java Card v2.2.2
Gemalto IDCore	Smart Card	Java Card v2.2.2
HID Crescendo C700	Smart Card	Java Card 2.2.2
Identive SCT3522 USB Token	Smart Card	Java Card v2.2.2
Identive SCT3522DI Mifare Flex USB Token	Smart Card	Java Card v2.2.2
IBM JCOP 21 v2.2.1	Smart Card	Java Card v2.2.1
IBM JCOP31 v2.2.1	Smart Card	Java Card v2.2.1
IBM JCOP 41 v2.2.1	Smart Card	Java Card v2.2.1
Marx CrypToken MX2048-JCOP	USB Token	Java Card v2.2.1
Morpho JMV ProCL V3.0	Smart Card	
Morpho STPay 38K	Smart Card	
Neowave Weneo ID 2.0	USB Token	Java Card v2.2.1
NXP JCOP21 v2.3.1	Smart Card	Java Card v2.2.1
NXP JCOP31 v2.3.1	Smart Card	Java Card v2.2.1
NXP JCOP41 v2.3.1	Smart Card	Java Card v2.2.1
NXP JCOP21 v2.4.1 / J2A080	Smart Card	Java Card v2.2.2
NXP JCOP31 v2.4.1 / J3A080	Smart Card	Java Card v2.2.2
NXP JCOP21 v2.4.1 / J2A081	Smart Card	Java Card v2.2.2
NXP JCOP31 v2.4.1 / J3A081	Smart Card	Java Card v2.2.2
Oberthur IDone Cosmo64 v5.2	Smart Card	Java Card v2.2.1
Oberthur ID-One Cosmo 32 RSA v3.6	Smart Card	Java Card v2.2.1
Oberthur ID-One Cosmo 64 RSA D/T v5.4	Smart Card	Java Card v2.2.1
Oberthur ID-One Cosmo v7.0	Smart Card	Java Card v2.2.1
Oberthur ID-One Cosmo v7.01	Smart Card	Java Card v2.2.2
Sagem Orga J-ID Mark 64 Dual	Smart Card	Java Card v2.2.1
Sagem Orga ysID S3[10]	Smart Card	Java Card v2.2.2

[10] Only supported with the SafeSign PKI applet pre-installed.

Token	Type	Additional remarks
Sagem Orga ysID Key E-M	USB Token	
Sagem Orga ysID Key E2C[11]	USB Token	

7.3 Java Card 3.0

Token	Type	Additional remarks
G&D Sm@rtCafé Expert v6.0	Smart Card / USB Token	Java Card v3.0.1 Classic
G&D Sm@rtCafé Expert v7.0	Smart Card / USB Token	Java Card v3.0.4 Classic
G&D SkySIM CX Scorpius	SIM	Java Card v3.0.1 Classic
G&D SkySIM CX Hercules	SIM	Java Card v3.0.1 Classic
NXP JCOP v2.4.2 R2 / J2D081	Smart Card	Java Card v3.0.1 Classic
NXP JCOP v2.4.2 R3 / J2E081	Smart Card	Java Card v3.0.1Classic
Swissbit PS-100u SE MicroSD	MicroSD Card	Java Card v3.0.4 Classic
Yubico Yubikey NEO	USB Token	Java Card v3.01 Classic

[11] Only supported with the SafeSign PKI applet pre-installed.

8 Supported Applications

The following applications have been tested with SafeSign Identity Client Standard on OS X:

Application	Version	Purpose
Token Administration Utility	3.0.3920	PKCS #11 Token management functions
Mozilla Firefox	45.0.1	Authentication to a secure web site
Mozilla Thunderbird	38.7.2	Signing and decrypting e-mail messages
LibreOffice	5.1.1	Signing a document
OpenOffice	4.1.2	Signing a document
Adobe Reader DC	2015.010.20060	Signing a document

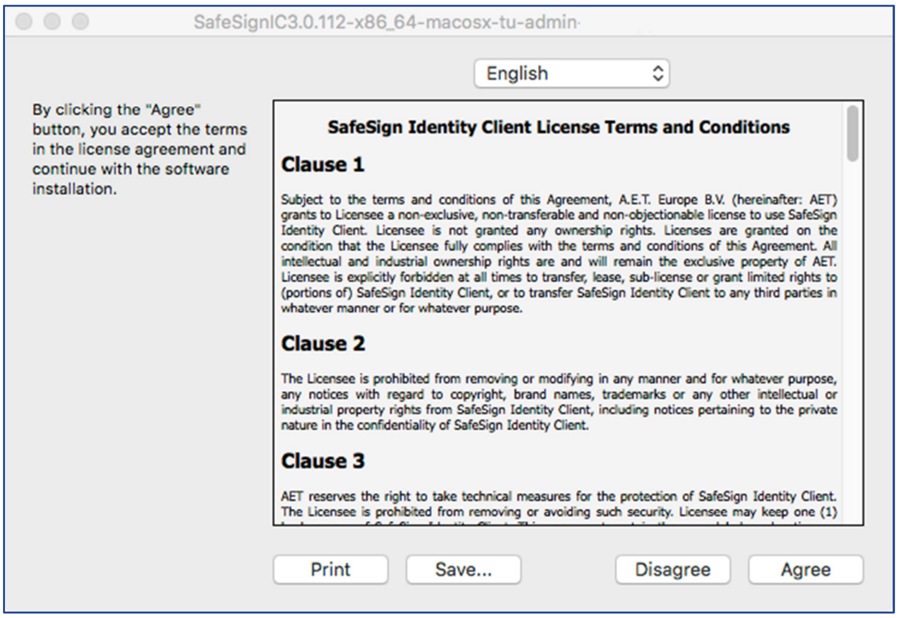
9 Installation

9.1 Installation Process

Note that users need to have sufficient privileges and basic knowledge of OS X to install SafeSign IC 3.0.112 for OS X.

① Save the installation file (.dmg) to a location on your MAC computer and open it (to mount it as a volume called “tokenadmin”).

② This will open the SafeSign Identity Client License Terms and Conditions window:



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)

Figure 4: Install SafeSign Identity Client: SafeSign Identity Client License Terms and Conditions

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

③ Upon clicking **Agree**, the following window will be displayed:

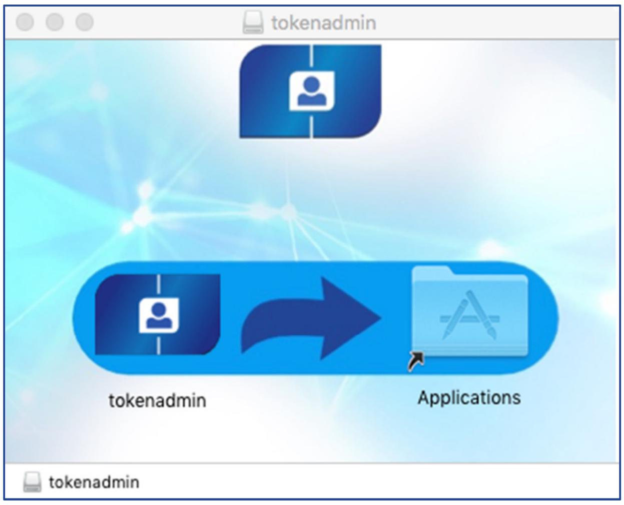


Figure 5: Install SafeSign Identity Client: tokenadmin

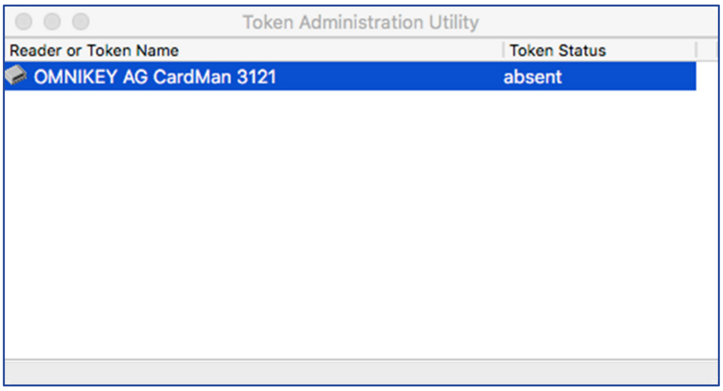
By dragging the tokenadmin Application Bundle to the Applications folder, SafeSign IC will be installed.

> Drag the tokenadmin icon to the Applications icon

④ Close the tokenadmin window and eject the "tokenadmin" volume.

9.2 Verify installation

When SafeSign Identity Client is installed, you can verify that installation is successful by checking for the presence of the Token Administration Utility (the *tokenadmin* application in the *Applications* folder):



Token Administration Utility

Reader or Token Name	Token Status
OMNIKEY AG CardMan 3121	absent

Figure 6: Token Administration Utility: Reader Name

Note that in the example above, the native OS X CCID smart card reader driver is installed and that a CCID compliant smart card reader is attached (in our case, the CardMan 3121 USB smart card reader).

When you insert a token, the Token Administration Utility will either display that a blank token is inserted (that can be initialised) or that a token with a token label has been inserted.

9.3 Uninstallation

It is possible to uninstall SafeSign Identity Client version 3.0.112 from your OS X.

The way to uninstall SafeSign Identity Client from OS X is to drag the *tokenadmin* Application Bundle to the Trash can or to right-click the *tokenadmin* application and select ‘Move to Trash’.

Note

Note that when uninstalling, you should not have the SafeSign Token Utility opened, otherwise the registry file in the user’s home directory will not be removed, which may lead to issues with new installations of SafeSign Identity Client.

9.4 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, 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[12].

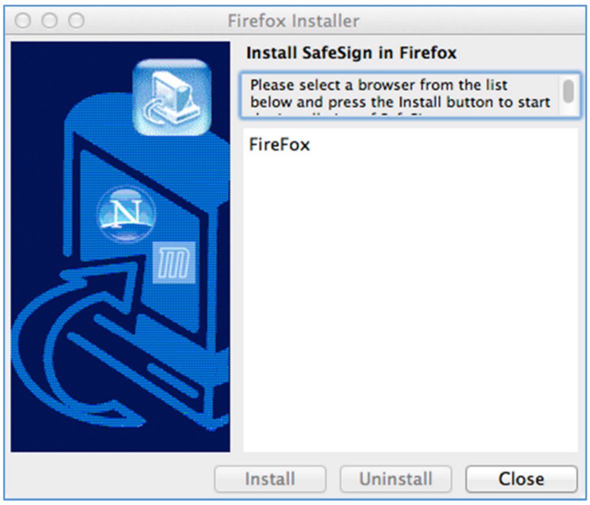
For Firefox, this functionality is included in the Token Administration Utility. Please refer to section 9.4.1.

For other applications such as Thunderbird and Adobe Reader DC, you will need to do so manually (see section 3.4). As an example of a manual installation, the manual installation of the SafeSign PKCS #11 Library in Firefox is described. Please refer to section 9.4.2.

[12] This is customary for PKCS #11 applications, where you need to load the cryptographic library or make reference to the library to be used for cryptographic / token support.

9.4.1 Firefox Installer

① 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 Firefox Installer:



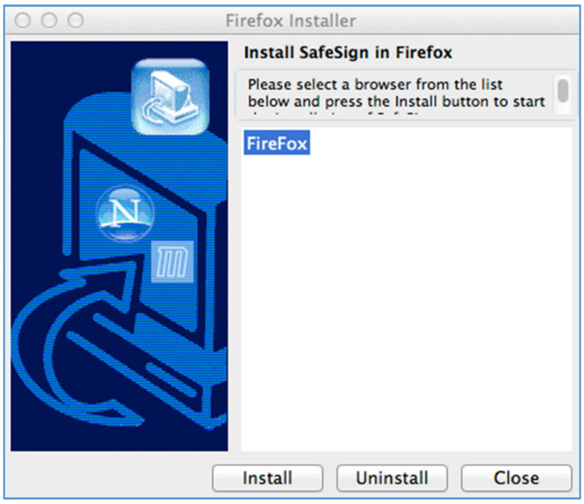
Install SafeSign in Firefox

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

FireFox

Figure 7: Firefox Installer: Install SafeSign in Firefox

② Select Firefox as in the picture below:



Install SafeSign in Firefox

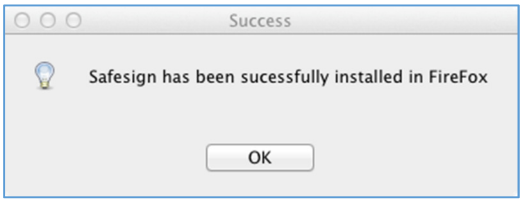
Please select a browser from the list below and press the Install button to start

FireFox

Figure 8: Firefox Installer: FireFox

> Click **Install**

③ When SafeSign is successfully installed in Firefox, you will be notified that:


Success

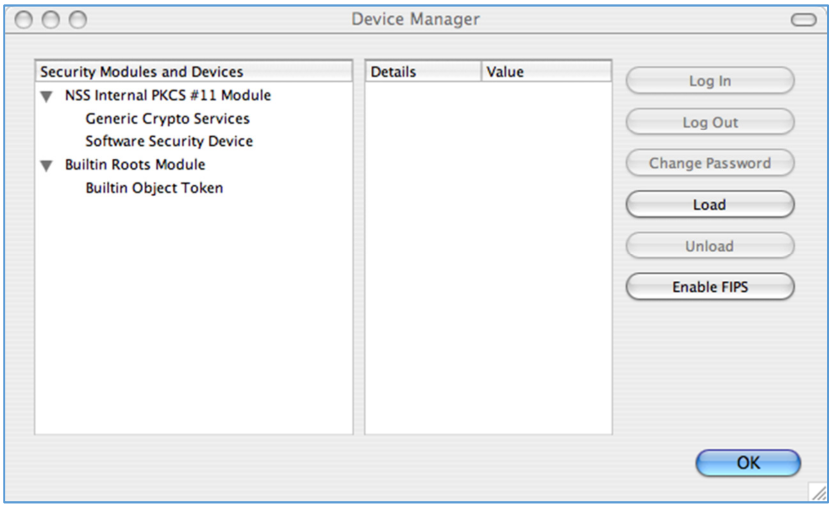
Safesign has been sucessfully installed in FireFox

Figure 9: Firefox Installer: Success

> Click **OK**

9.4.2 Manual install in Firefox

① In Firefox, go to Firefox > Preferences > Advanced > Encryption (tab) > Security Devices (button):


Device Manager

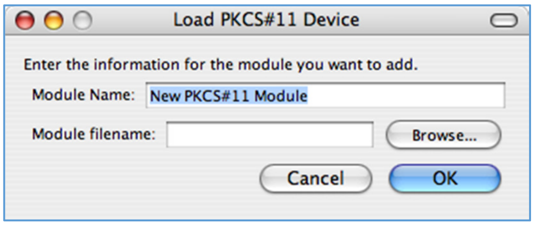
Security Modules and Devices
- NSS Internal PKCS #11 Module
  - Generic Crypto Services
  - Software Security Device
- Builtin Roots Module
  - Builtin Object Token

Figure 10: 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

② Upon clicking on **Load**, you can enter the information for the module you want to add:


Load PKCS#11 Device

Enter the information for the module you want to add.

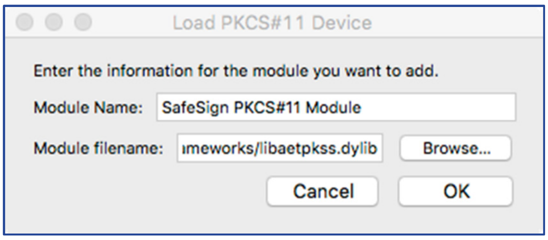
Module Name: New PKCS#11 Module

Module filename:

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

> Enter a name for the security module, e.g. *SafeSign PKCS #11 Module* 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:



Load PKCS#11 Device

Enter the information for the module you want to add.

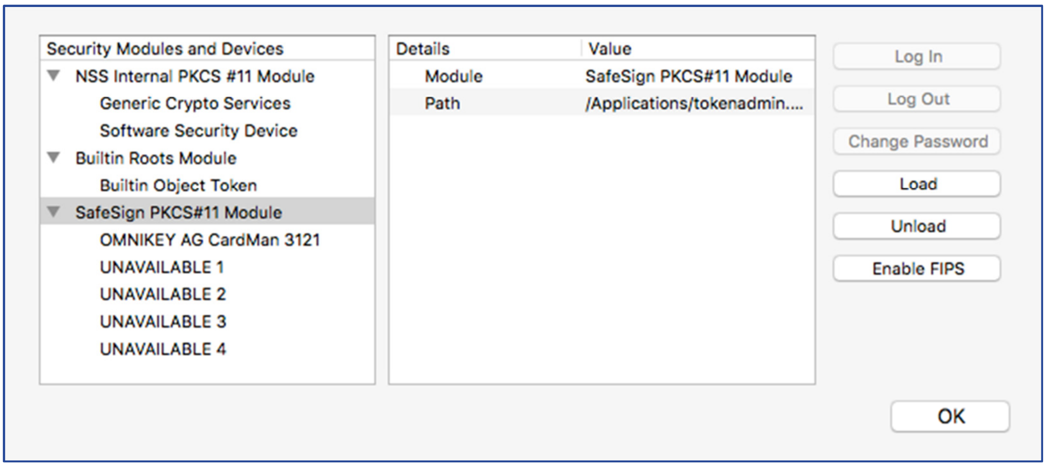
Module Name: SafeSign PKCS#11 Module

Module filename: ımeworks/libaetpkss.dylib

Figure 12: Firefox Device Manager: Load SafeSign PKCS #11 Module

> Click **OK**

③ The SafeSign Identity Client PKCS #11 Library will now be available as a security module in Firefox:



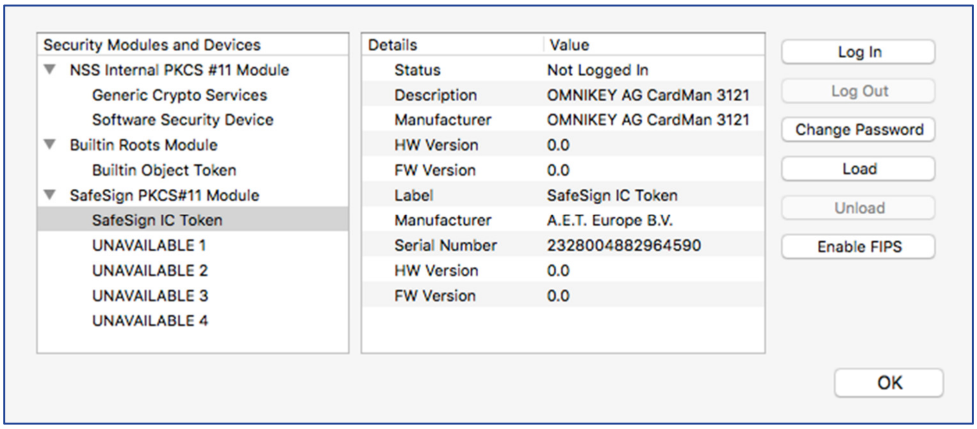
Security Modules and Devices
- NSS Internal PKCS #11 Module
  - Generic Crypto Services
  - Software Security Device
- Builtin Roots Module
  - Builtin Object Token
- SafeSign PKCS#11 Module
  - OMNIKEY AG CardMan 3121
  - UNAVAILABLE 1
  - UNAVAILABLE 2
  - UNAVAILABLE 3
  - UNAVAILABLE 4

Details	Value
Module	SafeSign PKCS#11 Module
Path	/Applications/tokenadmin....

Figure 13: Firefox Device Manager: SafeSign PKCS #11 Module

> Under the name of the security module (‘SafeSign PKCS #11 Module’, as specified in step 2), 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’. No token is inserted in the reader.

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



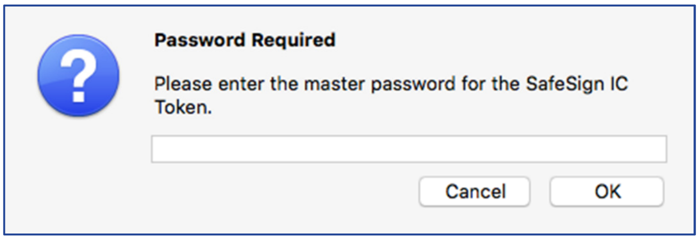
Security Modules and Devices
- NSS Internal PKCS #11 Module
  - Generic Crypto Services
  - Software Security Device
- Builtin Roots Module
  - Builtin Object Token
- SafeSign PKCS#11 Module
  - SafeSign IC Token
  - UNAVAILABLE 1
  - UNAVAILABLE 2
  - UNAVAILABLE 3
  - UNAVAILABLE 4

Details	Value
Status	Not Logged In
Description	OMNIKEY AG CardMan 3121
Manufacturer	OMNIKEY AG CardMan 3121
HW Version	0.0
FW Version	0.0
Label	SafeSign IC Token
Manufacturer	A.E.T. Europe B.V.
Serial Number	2328004882964590
HW Version	0.0
FW Version	0.0

Figure 14: 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:

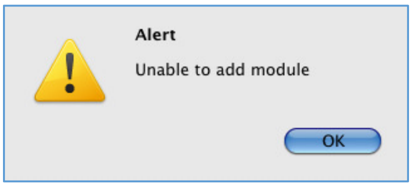


Password Required

Please enter the master password for the SafeSign IC Token.

Figure 15: Firefox: Prompt

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



Alert

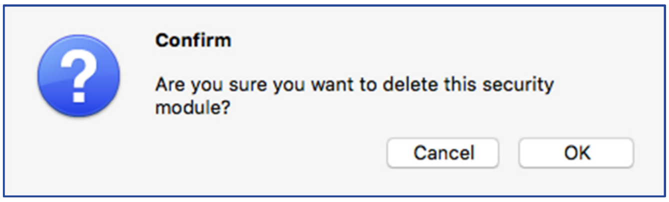
Unable to add module

Figure 16: Firefox: Unable to add module

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

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 17: Firefox: Confirm

Legal Notice

This document contains information of a proprietary nature. No part of this manual may be reproduced or transmitted in any form or by any means electronic, mechanical or otherwise, including photocopying and recording for any purpose other than the purchaser's personal use without written permission of A.E.T. Europe B.V. Individuals or organisations, which are authorised by A.E.T. Europe B.V. in writing to receive this information, may utilise it for the sole purpose of evaluation and guidance.

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 which 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.