SafeSign Identity Client TokenLounge

Release Document

Table of Contents

Table of Figures

Document Information

Title: SafeSign Identity Client TokenLounge Release Document

Document ID: SafeSign-IC-TokenLounge_Release_Document.docx

Project: SafeSign IC Release Documentation

Document revision history

Version	Date	Author	Changes
1.0	15-04-2016	Drs. C.M. van Houten	First edition for SafeSign Identity Client TokenLounge Version 1.0.1

Document approval

Version	Date	Name	Function
1.0	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 TokenLounge.

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 Technical Background

2.1 Apple Keychain

The Apple Keychain provides storage for passwords, encryption keys and certificates. After an application requests access to a keychain, it can store and retrieve sensitive data, confident that untrusted apps cannot access that data without explicit action by the user. In OS X, the user is prompted for permission when an application needs to access the keychain; if the keychain is locked, the user is asked for a password to unlock it.

2.2 Tokend

Token daemon or tokend is a module (plug-in) running at the operating system level, serving as a bridge between the smartcard and the OS X security layer, allowing applications like Safari and Mail to make use of cryptographic services, such as authentication and document signing.

A Token daemon is responsible for reading the smart card objects into the keychain, making the keys and certificates on your smart card appear in Keychain and thereby available to applications.

2.3 PKCS #11

Use of PKCS#11 on OS X is not possible in all cases or applications, because Apple does not provide any integration for PKCS #11 based applications and PKCS #11 requires the user to specify for each application a PKCS #11 Library to be dynamically loaded for the token in question.

However, PKCS #11 still serves as the interface between Tokend and the smart card. Therefore, SafeSign Identity Client Standard for OS X must be installed.

2.4 TokenLounge

To be able to use OS X applications that make use of Apple Keychain, AET provides a product called SafeSign Identity Client TokenLounge, which serves as an add-on to SafeSign Identity Client Standard for OS X.

SafeSign Identity Client TokenLounge comes in an installation package to install the SafeSign IC Tokend and the 'SafeSignIC Tokenlounge' Application Bundle (to enable logon and binding the users to the certificates) and includes an uninstaller to uninstall TokenLounge (and all related components).

While a background process monitors smart card insertion / removal, SafeSign Identity Client Token Lounge will update the Keychain with certificates that have a corresponding private key, using the PKCS #11 interface to access the smart card. When an application (Keychain) requests access to a certificate on a token, SafeSign Identity Client TokenLounge will forward the request to the PKCS #11 interface and you will be allowed to log in and use the token in your application.

2.4.1 Smart Card Logon

SafeSign Identity Client TokenLounge also provides the ability to perform smart card logon.

When smart card logon is enabled and a smart card is present, (most) OS X logon password fields turn into a PIN field and the username becomes unmodifiable (greyed out).

Prerequisite for this to work is that both the user certificate and the root certificate are trusted in the keychain and that the user certificate is capable of logon (has the smart card logon attribute).

The 'SafeSignIC Tokenlounge' Application Bundle is a utility application that is used to enable / disable smart card logon support by linking a certificate on the smartcard to a user account.

Smart card logon is supported from OS X 10.11.4 onwards.

See section 5 for more details.

Note	*Note SafeSign IC TokenLounge Version 1.0.1 enables smart card logon to the local Operating System, not (Active Directory) Domain logon.*

3 Release Information

SafeSign Identity Client for TokenLounge includes all functionality necessary to use hardware tokens with applications that make use of the Apple Keychain.

3.1 OS X versions

SafeSign Identity Client TokenLounge Version 1.0.1 comes in a standard version for the following environments:

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

3.2 Date of Release

The release date of SafeSign Identity Client TokenLounge Version 1.0.1 for OS X is 15 April 2016.

3.3 Release Details

The following table lists the version numbers of the (major) components installed by SafeSign Identity Client TokenLounge Version 1.0.1:

Description	File name	File version
TokenLounge Application	SafeSignIC Tokenlounge	1.0.1 (3937)
TokenLounge Uninstaller	SafeSignIC Tokenlounge Uninstaller	-
SafeSign IC Token Daemon	Safesign.tokend	-

This information can also be found in the Version Information dialog of TokenLounge.

3.4 Release Documents

Document Name	Version
SafeSign Identity Client TokenLounge Release Document	1.0

4 Features

The following features are supported by SafeSign Identity Client TokenLounge Version 1.0.1 for OS X (in conjunction with SafeSign Identity Client Version 3.0.112 for OS X):

- Multiple token support;
- Multiple reader support;
- Multiple application support;
- Support for Crypto Token Kit.

SafeSign Identity Client TokenLounge Version 1.0.1 was tested with the smart cards, USB tokens, smart card readers, applications and OS X environments listed in this document (see section 7, 8 and 9).

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.

4.1 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 TokenLounge Version 1.0.1 supports a number of different tokens through SafeSign Identity Client Standard Version 3.0.112 for OS X, as listed in section 8 of this document and in the Release Document for SafeSign Identity Client Standard version 3.0.112 for OS X.

4.2 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

4.3 Applications

SafeSign Identity Client TokenLounge Version 1.0.1 supports a number of applications on the OS X platform.

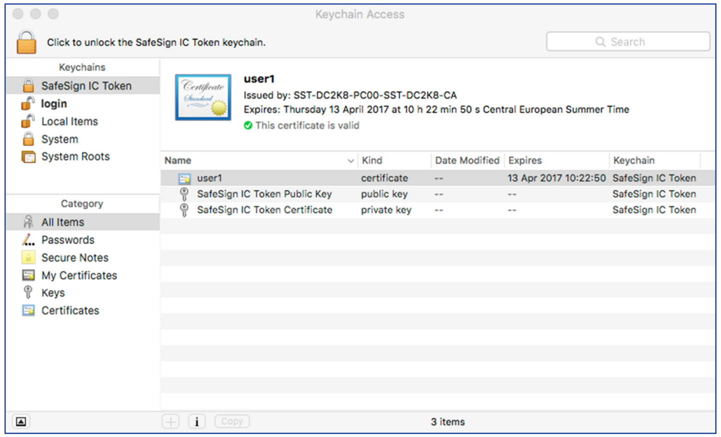
Prerequisite for SafeSign Identity Client TokenLounge is that SafeSign Identity Client Standard Version 3.0.112 for OS X is installed.

Note that once your Token Keychain is unlocked (by clicking the Unlock symbol or entering the PIN in an application), you will not have to enter your PIN again (until the token is removed and re-inserted or you manually lock the Keychain).

4.3.1 Keychain Access

When a token supported by SafeSign Identity Client TokenLounge is inserted, it will become available within Apple Keychain Access.

When your token is inserted, Keychain Access will display your token and its contents:



Click to unlock the SafeSign IC Token keychain.

user1
Issued by: SST-DC2K8-PC00-SST-DC2K8-CA
Expires: Thursday 13 April 2017 at 10 h 22 min 50 s Central European Summer Time
✓ This certificate is valid

Name	Kind	Date Modified	Expires	Keychain
user1	certificate	--	13 Apr 2017 10:22:50	SafeSign IC Token
SafeSign IC Token Public Key	public key	--	--	SafeSign IC Token
SafeSign IC Token Certificate	private key	--	--	SafeSign IC Token

3 items

Figure 2: Keychain Access: SafeSign IC Token

4.3.2 Safari

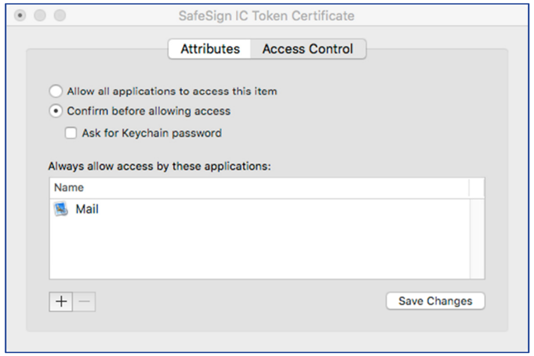
When using Safari to access a secure web site (that requires client authentication), you will be asked to enter the PIN for your token, because Safari wants to use your (token) Keychain.

Note that when you have multiple certificates on your token, Safari will only ask you to select the client certificate once, as it will cache the secure web site – certificate combination in the **login** Keychain.

4.3.3 Mail

When sending a signed message with Mail, you will be asked to enter the PIN for your token, as Mail wants to use your token.

In order to allow Mail to use Keychain, you need to set the correct Access Control rights in your token Keychain. Go to your Token Keychain ('SafeSign IC Token' in our example) and right-click on the Private Key on your token to select *Get Token Info*. Then select the *Access Control* tab and select "Confirm before allowing access" and add Mail. This will result in a dialog similar to the screenshot below:



○ Allow all applications to access this item
● Confirm before allowing access
□ Ask for Keychain password

Always allow access by these applications:

Name
Mail

Figure 3: SafeSign IC Token Certificate: Mail

Note

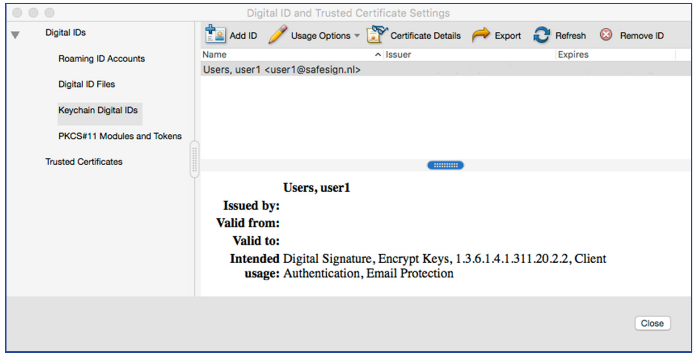
Note that you may be asked to enter a new password for your Token Keychain. When this happens, you can enter your current PIN as both current and new (confirmed) password.

4.3.4 Adobe Reader DC

When using Adobe Reader DC to sign a document, you will be asked to enter the PIN for your token.

You can verify that Adobe Reader sees the certificate(s) in your Token Keychain, by going to:

Acrobat Reader > **Preferences** > **Signatures** > **Identities & Trusted Certificates** > **More** > **Keychain Digital IDs**:



Name	Issuer	Expires
Users, user1 <user1@safesign.nl>		

Users, user1
Issued by:
Valid from:
Valid to:
Intended usage: Digital Signature, Encrypt Keys, 1.3.6.1.4.1.311.20.2.2, Client Authentication, Email Protection

Figure 4: Adobe Reader DC: Keychain Digital IDs

4.3.5 Chrome

When using Chrome to access a secure web site (that requires client authentication), you will be asked to enter the PIN for your token, because Chrome wants to use your Token Keychain.

4.3.6 TokenLounge

The SafeSign Identity Client TokenLounge application ('SafeSignIC Tokenlounge) allows you to enable smart card logon in the OS and to bind a certificate to a user.

For more details, see section 5.

4.4 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 and SafeSign Identity Client TokenLounge Version 1.0.1 support the Crypto Token Kit.

5 Smart Card Logon

5.1 Requirements

SafeSign Identity Client TokenLounge allows you to use your token to logon to OS X.

Smart card logon is supported from OS X 10.11.4 onwards.

In order to logon with your token, the following prerequisites need to be fulfilled:

1. SafeSign Identity Client Standard Version 3.0.112 for OS X must be installed;
2. Smart card logon "detection" must be enabled in the OS;
3. The user certificate must be bound to a (OS X logon) user;
4. The user certificate must have the smart card logon attribute;
5. The user certificate and its CA must be marked as trusted inside the Keychain.

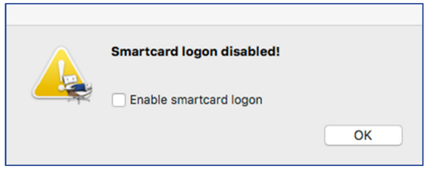
Step 2 and 3 need to be performed in the SafeSignIC Tokenlounge application, step 5 needs to be performed in Keychain Access.

5.2 Enable smart card logon

To enable smart card logon, you will need to enable smart card logon in the Operating System and link a user to an identity (section 5.2.1) as well as setting the appropriate trust settings (section 5.2.2).

5.2.1 SafeSign IC TokenLounge

The first time you open the SafeSignIC Tokenlounge application, it will inform you that smart card logon is disabled (not enabled):

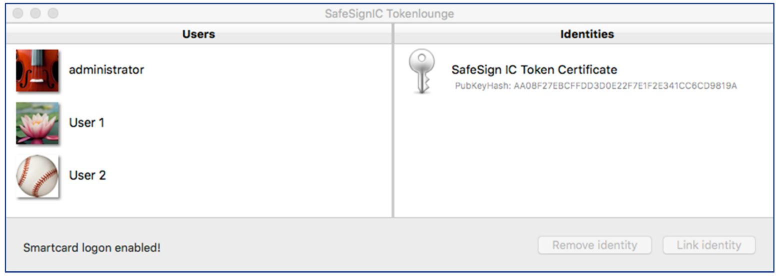

Smartcard logon disabled!

☐ Enable smartcard logon

Figure 5: SafeSignIC Tokenlounge: Smartcard logon disabled

> Tick the checkbox 'Enable smartcard logon' and click **OK**

After clicking **OK**, you will be asked to enter the administrator password, upon which smartcard logon will be enabled and you will be able to link a user to an identity in the following window:



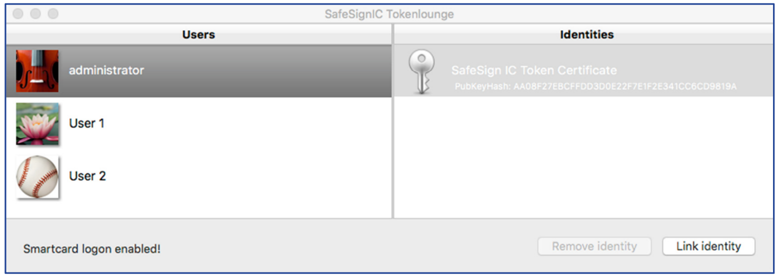
Smartcard logon enabled!

Figure 6: SafeSignIC Tokenlounge: Users and Identities

On the left-hand side, the users (that can log on to the OS X) are listed;

on the right-hand side, the Identities (certificate) in the Token Keychain are listed.

Select both a user and an identity, whereupon the **Link identity** button will become available:

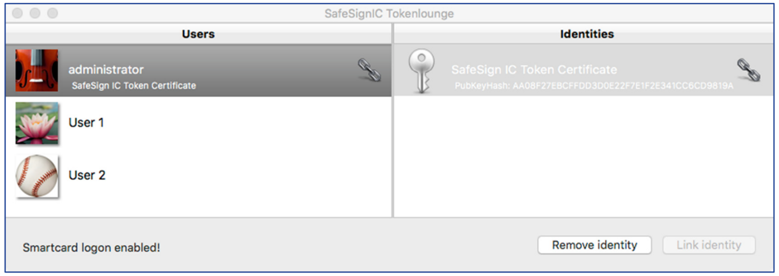


Smartcard logon enabled!

Figure 7: SafeSignIC Tokenlounge: Link identity

> Click **Link identity**

After clicking **Link Identity**, you will see the following window:


SafeSignIC Tokenlounge
Users
Identities
administrator
SafeSign IC Token Certificate
User 1
User 2
SafeSign IC Token Certificate
PubKeyHash: AA08F27EBCFFDD3D0E22F7E1F2E341CC6CD9819A
Remove identity
Link identity

Smartcard logon enabled!

Figure 8: SafeSignIC Tokenlounge: Identity linked

> Close the SafeSignIC Tokenlounge application.

Note

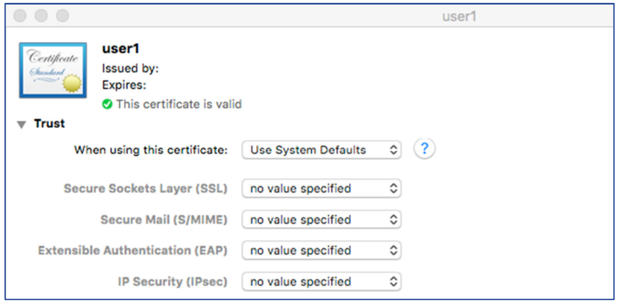
In SafeSign Identity Client Token Lounge Version 1.0.1, you can only link one user to one identity.

5.2.2 Keychain

After enabling smart card logon, you need to set the right trust settings for both the (user) certificate(s) and CA certificate(s) in your Token Keychain. Note that for smart card logon to work, it is required that the CA (root and intermediate) certificate(s) are on the token or in the 'System' keychain.

In Keychain Access, right-click the certificate on your token (that you have linked to a user logon account) and select **Get Info**.

When the certificate is displayed, expand **Trust**:

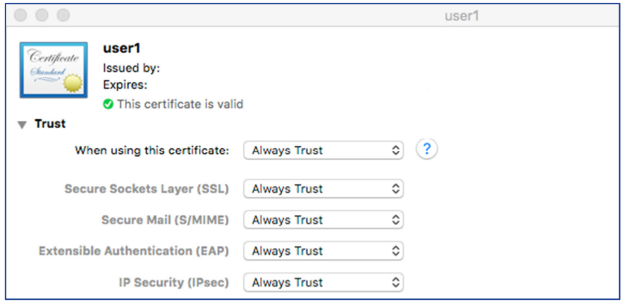


user1
Issued by:
Expires:
This certificate is valid

When using this certificate: Use System Defaults
Secure Sockets Layer (SSL) no value specified
Secure Mail (S/MIME) no value specified
Extensible Authentication (EAP) no value specified
IP Security (IPsec) no value specified

Figure 9: Keychain certificate: Use System Defaults

Change the option ‘When using this certificate’ from ‘Use System Defaults’ to ‘Always Trust’:



user1

user1
Issued by:
Expires:
✓ This certificate is valid

▼ Trust

When using this certificate:	Always Trust
Secure Sockets Layer (SSL)	Always Trust
Secure Mail (S/MIME)	Always Trust
Extensible Authentication (EAP)	Always Trust
IP Security (IPsec)	Always Trust

Figure 10: User certificate: Always Trust

> Do the same for the CA (root and intermediate) certificate(s).

Note

Although an administrator (user with administrator rights) may link a user to a (digital) identity with SafeSignIC Tokenlounge, the user will need to modify the trust settings in his own Keychain. If on the other hand, a user performs the procedure to enable smart card logon himself, he needs the administrator password.

5.2.3 Smart Card Logon

After performing the steps above, you will be able to logon on to OS X with your token.

When inserting a card, the password field will change to a PIN field automatically:

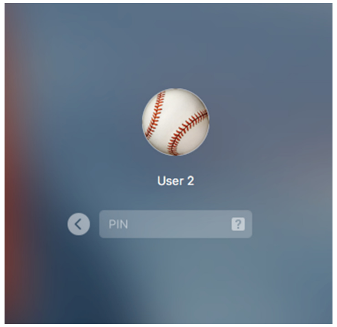


Figure 11: PIN dialog

5.3 Disable Smart Card Logon

Once enabled, smart card logon can be disabled again.

Open the SafeSignIC Tokenlounge application and select **Smartcard Logon Status** from the menu:

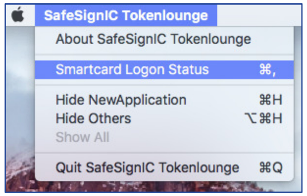
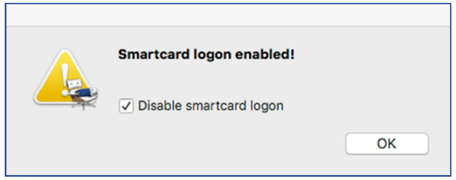

SafeSignIC Tokenlounge
About SafeSignIC Tokenlounge
Smartcard Logon Status ⌘,
Hide NewApplication ⌘H
Hide Others ⌥⌘H
Show All
Quit SafeSignIC Tokenlounge ⌘Q

Figure 12: SafeSignIC Tokenlounge: Menu

SafeSignIC Tokenlounge will inform you that smart card logon is enabled:



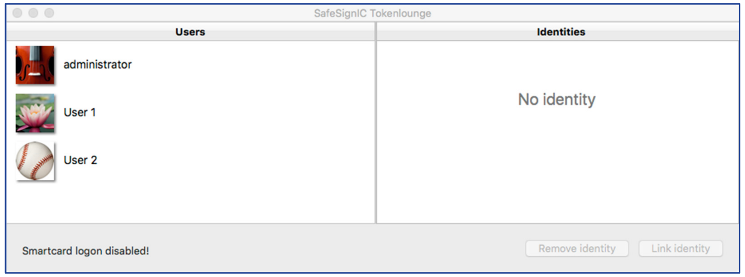
Smartcard logon enabled!

☑ Disable smartcard logon

Figure 13: SafeSignIC Tokenlounge: Smartcard logon enabled

> Tick the checkbox ‘Disable smartcard logon’ and click **OK**

After clicking **OK** and entering the user login password, smart card logon will be disabled:



SafeSignIC Tokenlounge

Users	Identities
administrator User 1 User 2	No identity

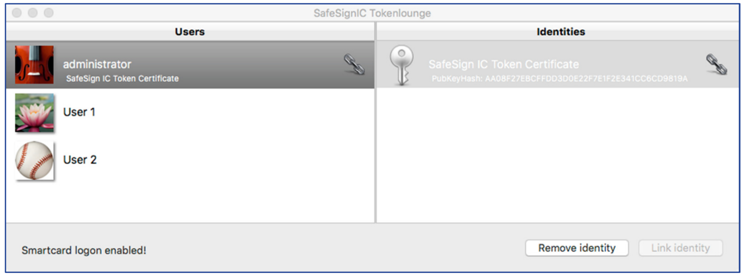
Smartcard logon disabled!

Figure 14: SafeSignIC Tokenlounge: Smartcard logon disabled

5.4 Remove Identity

It is possible to unlink (remove) an identity when it is linked.

To do so, insert the token and open the SafeSignIC Tokenlounge application, in order to select the user on the left-hand side and the linked identity on the right-hand side:



administrator
SafeSign IC Token Certificate
User 1
User 2

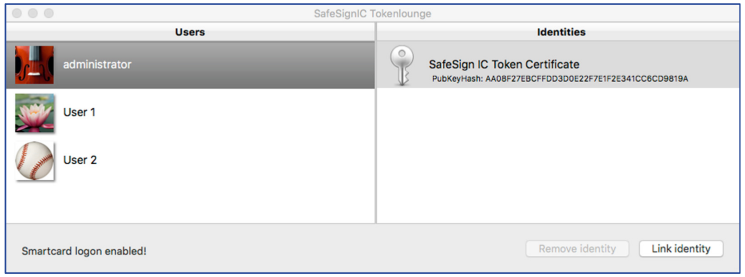
SafeSign IC Token Certificate
PubKeyHash: AA08F27EBCFFDD3D0E22F7E1F2E341CC6CD9819A

Smartcard logon enabled!

Figure 15: SafeSignIC Tokenlounge: Identity linked

> Click **Remove identity**

Upon entering the administrator password, the identity (link) will be removed:



administrator
User 1
User 2

SafeSign IC Token Certificate
PubKeyHash: AA08F27EBCFFDD3D0E22F7E1F2E341CC6CD9819A

Smartcard logon enabled!

Figure 16: SafeSignIC Tokenlounge: Users and Identities

Note

Note that because the token is inserted (to show the users and identities on the token), the administrator password dialog will ask for the PIN, rather than the password. Remove the token to be allowed to enter the password and remove the identity.

6 Known Issues

6.1 General

1. Because there is only one Crypto Token Kit layer on the OS X platform, which multiple applications may access, it may happen that applications conflict. In particular, when having Keychain Access open and opening the Token Administration Utility (both of which communicate through PKCS #11 to the Crypto Token Kit), the latter may not detect the token or may identify it as unknown. Another example is to have both Keychain Access and SafeSignIC Tokenlounge open, which causes refresh issues in both applications. Workaround in these cases is to quit the application (keeping the token inserted) and restarting it. It is recommended not to have the Token Administration Utility or Keychain Access applications open when using the token in applications.
2. Once your token Keychain is unlocked, you will not be asked for your PIN in other applications using your token keychain, until you remove and re-insert your token or lock it manually.
3. When performing secure web access through Safari with a token containing more than one certificate, you will be asked to select the certificate to use for client authentication. Safari will then cache your choice of certificate in the **login** Keychain.
4. When you enable smart card logon and switch with multiple users via the top bar, the PIN login is not coming, only password request. Workaround is to select the option “Login Window” instead of the required user.
5. When changing the token label (for example, by wiping the token in the Token Administration Utility and setting a new label), Keychain will not display the new label. This is caused by the fact that the token label is cached in the folder “/private/var/db/TokenCache/tokens”, based on the serial number of the token. You can remove the entire cache contents (which will be recreated when inserting the token) or remove the entry for your token (in the format ‘com.aet.tokend.safesign:aetToken-[token serial number]’).
6. You may be asked for your **login** Keychain password after logging in with your PIN. Logging in with the PIN unlocks the Token Keychain, not the **login** keychain. Workaround is to make the **login** Keychain password equal to the PIN of your token.

6.2 TokenLounge

7. If you did not eject the ‘tokenadmin’ disk after installing SafeSign Identity Client Standard for OS X Version 3.0.112, the background image of the ‘SafeSign Tokenlounge’ installer will be incorrect when installing TokenLounge.
8. The SafeSignIC Tokenlounge application does not refresh the status of the user(s) and identities correctly after linking. You may see two identical identities for one user, but linking will work correctly nevertheless. Workaround is to close and restart the SafeSignIC TokenLounge application and restart it (with the token inserted). This will be fixed in a future release.
9. It is not possible to link a user to multiple identities or to link multiple identities to one user.

7 Supported Versions

SafeSign Identity Client TokenLounge Version 1.0.1 has been tested to support the following OS X versions (both 32-bit and 64-bit):

OS X	SafeSign Identity Client Standard for OS X Version	Token Lounge 1.0.1
OS X 10.10 (“Yosemite”)	3.0.112	√
OS X 10.11 (“El Capitan”)	3.0.112	√

8 Supported Tokens

SafeSign Identity Client TokenLounge supports a number of hardware tokens in conjunction with SafeSign Identity Client Standard Version 3.0.112 for OS X, 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.

8.1 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

8.2 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

Token	Type	Additional remarks
Gemalto Optelio D72 FR1	Smart Card	Java Card v2.2.2
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

Token	Type	Additional remarks
Sagem Orga ysID S3[1]	Smart Card	Java Card v2.2.2
Sagem Orga ysID Key E-M	USB Token	
Sagem Orga ysID Key E2C[2]	USB Token	

8.3 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

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

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

9 Supported Applications

The following applications have been tested with SafeSign Identity Client TokenLounge:

Application	Version	Purpose
Apple Keychain Access	9.0	Certificate management functions
Apple Safari	9.1	Authentication to a secure web site
Apple Mail	9.3	Signing e-mail messages
Adobe Reader DC	2015.010.20060	Signing a document
Google Chrome	49.0.2623.112	Authentication to a secure web site
TokenLounge App	1.0.1 (3937)	Enable smart card logon
Smart Card Logon	OS X 10.11.4	Smart Card Logon

Note

Note that smart card logon is supported from OS X 10.11.4 onwards.

10 Installation

10.1 Installation Process

Note that users need to have sufficient privileges and basic knowledge of OS X to install SafeSign Identity Client TokenLounge Version 1.0.1.

Before installing SafeSign Identity Client TokenLounge, make sure that you have SafeSign Identity Client Standard for OS X Version 3.0.112 installed and ejected the volume.

① Save the installation file (.dmg) to a location on your MAC computer and open it (to mount it as a volume / disk called "SafeSignIC Tokenlounge").

② The contents of the "SafeSignIC Tokenlounge" disk will be displayed:

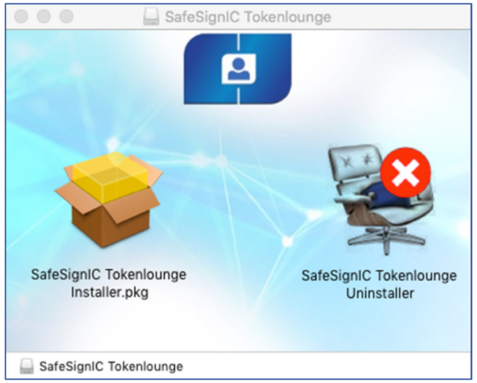
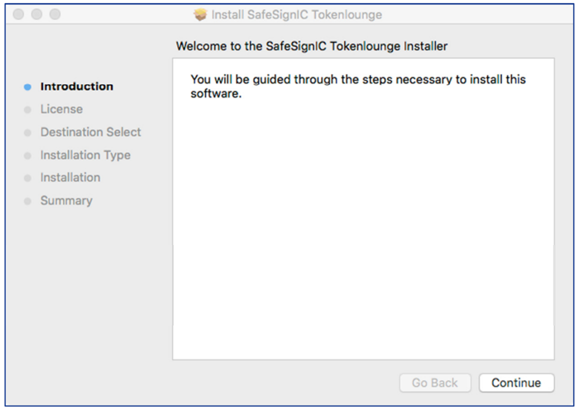

SafeSignIC Tokenlounge
SafeSignIC Tokenlounge Installer.pkg
SafeSignIC Tokenlounge Uninstaller
SafeSignIC Tokenlounge

Figure 17: SafeSignIC Tokenlounge

> Double-click the 'SafeSignIC Tokenlounge Installer.pkg' package installer

③ Upon double-clicking the package, the *Welcome to the SafeSignIC Tokenlounge Installer* window will be displayed:



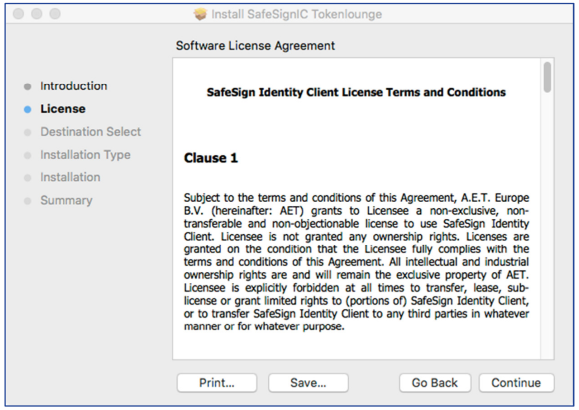
Welcome to the SafeSignIC Tokenlounge Installer

You will be guided through the steps necessary to install this software.

Figure 18: Install SafeSignIC Tokenlounge: Introduction

> Click **Continue** to install SafeSignIC Tokenlounge

④ Upon clicking **Continue**, the SafeSign Software License Agreement will be displayed:



Software License Agreement

SafeSign Identity Client License Terms and Conditions

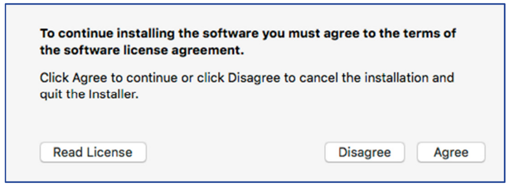
Clause 1

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.

Figure 19: Install SafeSignIC Tokenlounge: License

> Read the License Agreement and click **Continue**

⑤ Upon clicking **Continue**, you will be asked to agree to the terms of the software license agreement:



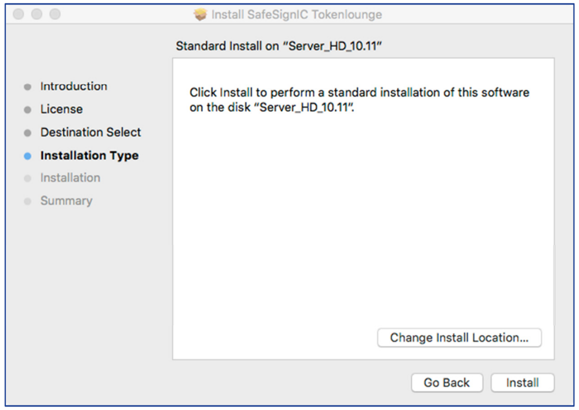
To continue installing the software you must agree to the terms of the software license agreement.

Click Agree to continue or click Disagree to cancel the installation and quit the Installer.

Figure 20: Install SafeSignIC Tokenlounge: Agree

> Click **Agree** to agree to the License and continue

⑥ Upon agreeing to the terms of the License Agreement, you will be allowed to install the software:



Standard Install on "Server_HD_10.11"

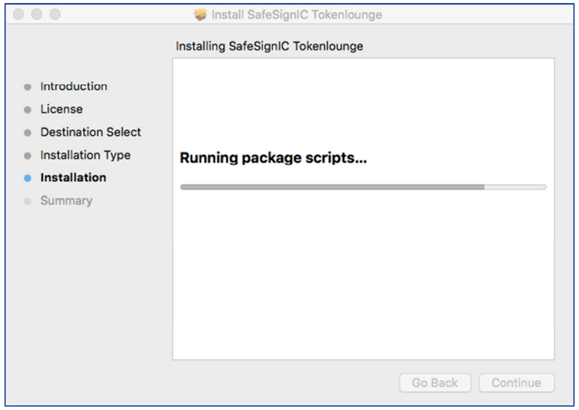
Click Install to perform a standard installation of this software on the disk "Server_HD_10.11".

Figure 21: Install SafeSignIC Tokenlounge: Installation Type

If you need to install SafeSignIC Tokenlounge in a different location, you can click **Change Install Directory** to go to the *Destination Select* window to change the install location.

> If you want to install SafeSignIC Tokenlounge in the location displayed, click **Install**

⑦ Upon clicking **Install**, you will be asked for the administrator password to allow installation, after which the software will be installed:

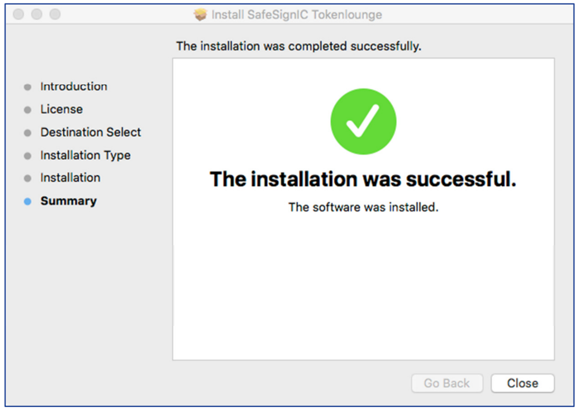


Installing SafeSignIC Tokenlounge

Running package scripts...

Figure 22: Install SafeSignIC Tokenlounge: Installation

⑧ When the installation is finished, you will be informed that installation was succesful:



The installation was completed successfully.

The installation was successful.

The software was installed.

Figure 23: Install SafeSignIC Tokenlounge: Summary

> Click **Close** to close the installer.

> As a final step, close the SafeSignIC Tokenlounge window (Figure 17) and eject the "SafeSignIC Tokenlounge" volume.

10.2 Verify installation

When SafeSign Identity Client TokenLounge is installed, you can verify that installation is successful by checking for the presence of the 'SafeSignIC Tokenlounge' application(s) in the *Applications > Utilities* folder:

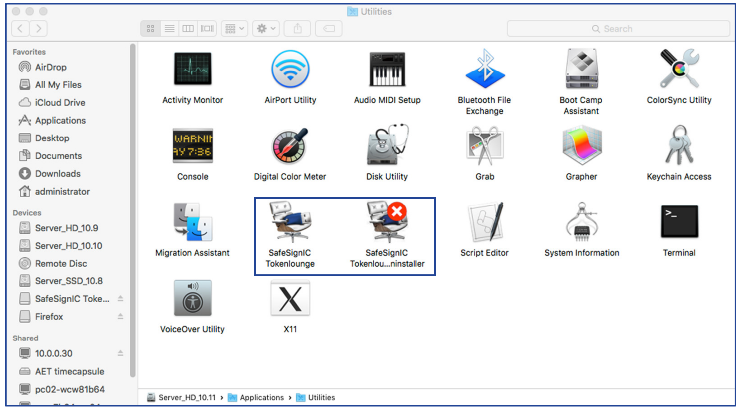
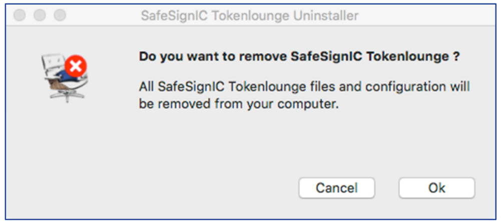


Figure 24: Utilities: SafeSignIC Tokenlounge

10.3 Uninstallation

It is possible to uninstall SafeSign Identity Client TokenLounge from your OS X, by means of the 'SafeSignIC Tokenlounge Uninstaller'.

① Double-click the 'SafeSignIC Tokenlounge Uninstaller' application:



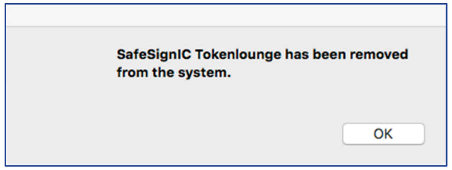
Do you want to remove SafeSignIC Tokenlounge ?

All SafeSignIC Tokenlounge files and configuration will be removed from your computer.

Figure 25: SafeSignIC Tokenloune Uninstaller: Remove

> Click **OK** to remove SafeSignIC Tokenlounge

② Upon clicking **OK**, SafeSign IC TokenLounge will be removed and you will be informed:



SafeSignIC Tokenlounge has been removed from the system.

Figure 26: SafeSignIC Tokenlounge Uninstaller: Removed

Note

Note that when uninstalling with the SafeSignIC TokenLounge application opened, uninstall will succeed, but you will need to close the SafeSignIC Tokenlounge application manually afterwards.

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.