**aet**

SafeSign Identity Client Standard Version 3.5

Release Document for Windows

# Table of Contents

# Warning Notice

All information herein is either public information or is the property of and owned solely by A.E.T. Europe B.V. who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

This information is subject to change as A.E.T. Europe B.V. reserves the right, without notice, to make changes to its products, as progress in engineering or manufacturing methods or circumstances warrant.

Installation and use of A.E.T. Europe B.V. products are subject to your acceptance of the terms and conditions set out in the license Agreement that accompanies each product. Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/ or industrial property rights of or concerning any of A.E.T. Europe B.V. information.

Cryptographic products are subject to export and import restrictions. You are required to obtain the appropriate government licenses prior to shipping this Product.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, A.E.T. Europe B.V. makes no warranty as to the value or accuracy of information contained herein. The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, A.E.T. Europe B.V. reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

A.E.T. EUROPE B.V. HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH REGARD TO THE INFORMATION CONTAINED HEREIN, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL A.E.T. EUROPE B.V. BE LIABLE, WHETHER IN CONTRACT, TORT OR OTHERWISE, FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER INCLUDING BUT NOT LIMITED TO DAMAGES RESULTING FROM LOSS OF USE, DATA, PROFITS, REVENUES, OR CUSTOMERS, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION CONTAINED IN THIS DOCUMENT.

SafeSign IC is a trademark of A.E.T. Europe B.V. All A.E.T. Europe B.V. product names are trademarks of A.E.T. Europe B.V. All other product and company names are trademarks or registered trademarks of their respective owners.

Credit Information:

 "This product includes cryptographic software written by Eric A. Young (eay@cryptsoft.com). "

"This product includes software written by Tim J. Hudson (tjh@cryptsoft.com). "

# Document Information

Document ID:          SafeSign IC Standard Version 3.5 Release Document for Windows

Project Information:  SafeSign IC Release Documentation

Document revision history:

| Version | Date | Author | Changes |
|---|---|---|---|
| 1.0 | 19 March 2018 | Drs C.M. van Houten | First edition for SafeSign IC Standard Version 3.5 for Windows, release 3.5.0.0-AET.000 |
| 2.0 | 02 May 2019 | Drs C.M. van Houten | First edition for SafeSign IC Standard Version 3.5 for Windows, release 3.5.2.0-AET.000 |
| 3.0 | 10 July 2019 | Drs C.M. van Houten | First edition for SafeSign IC Standard Version 3.5 for Windows, release 3.5.3.0-AET.000 |
|  |  |  |  |

Document Approval

| Version | Date | Name | Function |
|---|---|---|---|
| 1.0 | 19 March 2018 | B. Smid MBT | Chief Development Officer |
| 2.0 | 02 May 2019 | B. Smid MBT | Chief Development Officer |
| 3.0 | 10 July 2019 | B. Smid MBT | Chief Development Officer |
|  |  |  |  |

**WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE**

# About the Product

This competent all-rounder in terms of strong authentication, integration and compatibility gives you complete freedom and flexibility. Once rolled out, SafeSign Identity Client (IC) serves as the perfect guard for IT security and enables unlimited possibilities for securing your IT infrastructure.

SafeSign IC offers the most comprehensive support available on the market for (card) operating systems, smart cards, USB tokens, languages and functions. This means you have sustainable and permanent freedom of choice when it comes to manufacturer independence.

SafeSign IC enforces two- or multi factor authentication/logon to the network, client PC or application, requiring the end user to have both the USB token or smart card (something you have) and a Personal Identity Number (something you know). USB tokens and smart cards are physically and logically tamper-resistant, ensuring that the end user's digital credentials can not be copied, modified or shared. Authentication based on smart cards or USB tokens provides the highest degree of security.

SafeSign IC is available for both fixed and mobile devices like desktops, servers, laptops, tablets and smart phones. SafeSign IC is also found in Thin Clients, printers or any other devices requiring authentication.

# 1 About this Document

The aim of this document is to document the status of the release of SafeSign Identity Client (IC) Standard version 3.5 for Windows.

This document is part of the release documentation of SafeSign IC and is intended to be a reference to both end users and administrators.

# 2 Release Information

## 2.1 Deliverables

SafeSign IC Standard Version 3.5 for Windows is provided as an .msi installation file.

The InstallShield Wizard will guide you through the installation of SafeSign IC Standard for Windows.

Alternatively, the .msi installation package can be used for centralised distribution and installation within an enterprise context.

SafeSign IC Standard Version 3.5 for Windows includes the Token Administration Utility user interface for local smart card operations, such as Change PIN.

## 2.2 Date of Release

The date of the release is 10 July 2019.

## 2.3 Release Details

SafeSign IC Standard Version 3.5 for Windows reflects the new SafeSign IC version 3.5 product version numbering scheme, i.e. version number, build number and distribution number, which is reflected in the Version Information dialog of the Token Administration Utility and which now includes the version number for all components delivered with the release of SafeSign IC version 3.5 for Windows.

| Release version: Standard Release 3.5.3.0-AET.000 | | |
|---|---|---|
| Description | File Name | File Version |
| Crypto Next Generation Module | aetcngss.dll | 3.5.0.4233 |
| Certificate Expiration Check Utility | aetcrss1.exe | 3.5.0.4040 |
| CSP Library | aetcsss1.dll | 3.5.0.4234 |
| Common Dialogs | aetdlss1.dll | 3.5.0.4259 |
| Java Card Handling Library | aetjcss1.dll | 3.5.0.4220 |
| PKCS #11 Cryptoki Library | aetpkss1.dll | 3.5.0.4269 |
| PKCS #11 Library Wrapper with automatic login | aetpkssw.dll | 3.5.0.4045 |
| Task Manager | aettask.dll | 3.5.0.4042 |
| Credential Provider | aetcpss1.dll | 3.5.0.4132 |
| Token Administration Utility | tokenadmin.exe | 3.5.0.4257 |

Note that in the distribution number (AET.000), the prefix AET is unique and reserved for AET general releases only.

Note that when saving the version information to a file, there may be components listed that are not available in the SafeSign IC version installed. For example, in SafeSign IC Standard Version 3.5, the Read-write card-module 'aetrwcm1.dll' is listed, but as 'not installed'.

## 2.4 Windows 32-bit and 64-bit

SafeSign IC Standard Version 3.5 for Windows comes in a 32-bit version and a 64-bit version.

### 2.4.1 32-bit

The 32-bit version of SafeSign IC Standard is for 32-bit Windows Operating Systems only. Though it will install on 64-bit Windows Operating Systems, it will not work with either 32-bit or 64-bit applications.

This is due to the fact that information about the tokens (ATR) and the associated (SafeSign IC) CSP is missing from the appropriate 64-bit branch of the registry, causing certificates not to be registered by the Microsoft Certificate Propagation Service.

### 2.4.2 64-bit

For use on 64-bit Windows Operating Systems, a SafeSign IC Standard 64-bit version is available (which does not install on 32-bit Windows Operating Systems) that will work with both 32-bit and 64-bit applications.

> Note that there are two system directories on Windows 64-bit Operating Systems: System32, which is reserved for 64-bit applications and SysWOW64, which is reserved for 32-bit applications.

SafeSign IC Standard Version 3.5 system files will install in both directories (to ensure that both 32-bit and 64-bit applications can work with SafeSign IC), with the following exceptions, which are installed in the system32 directory only:

- The Certificate Expiration Check Utility (aetcrss1.exe);
- The Task Manager (aettask.dll);
- The SafeSign Credential provider (aetcpss1.dll).

The Token Administration Utility's Version Information dialog will indicate which installed files have a 32-bit and/or a 64-bit file version.

> Note that when de-installing the 64-bit version of SafeSign IC Standard, some entries related to SafeSign IC cards will remain in the registry. Although these entries should not interfere when a new version of SafeSign IC is installed, we strongly recommend to clean (remove all SafeSign IC related entries below) [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards] prior to installing a new version. Please contact AET SafeSign Support for a tool to uninstall SafeSign IC.

## 2.5 Release Documents

SafeSign IC Standard Version 3.5 for Windows provides at least the following release documentation:

| Document Name | Version |
|---|---|
| SafeSign IC Standard Version 3.5 Release Document for Windows | 3.0 |

# 3 Features

The following features are supported by SafeSign IC Standard version 3.5 for Windows:

1 Multiple Token Support
2 Multiple Smart Card Reader Support
3 Multiple Application Support
4 Multiple Language Support
5 Attribute Certificate Support (≥ release 3.5.2.0)

These features are described in the following paragraphs.

## 3.1 Multiple Token Support

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

Newly supported smart card and tokens in SafeSign IC Standard version 3.5 for Windows are:

- Giesecke & Devrient StarSign Crypto USB-Token S
- Infineon Oracle JCOS Ed.1
- Morpho IDealCitiz v2.1
- NXP JCOP 3 SecID P60

## 3.2 Multiple Smart Card Reader Support

SafeSign IC Standard for Windows supports the use of PCSC 2.0 Class 1 smart card readers, as well as Class 2 and 3 secure pinpad readers.

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

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

## 3.3 Multiple Application Support

SafeSign IC Standard for Windows supports applications on Windows that work through PKCS #11 or Microsoft CryptoAPI (NG).

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

- Web authentication
- Email signing and encryption
- Document signing
- Smart card logon
- Terminal Server logon

SafeSign IC Standard version 3.5 for Windows has been tested to support a number of applications, as listed in section 9.

## 3.4　Multiple Languages Support

SafeSign IC Standard version 3.5 for Windows supports a number of different languages.

When installing the SafeSign IC Standard .msi package, the default language of the installation program will be English. In order to install the .msi in a particular language, you will need to install the .msi with specific parameters, to apply a transform.

Section 10.1 lists the Windows language code identifiers and transform files to do so.

## 3.5　Attribute Certificate Support

SafeSign IC Standard Version 3.5.2.0 allows you to view (information on) Attribute Certificates on the token and to import / export Attribute Certificates through the Token Administration Utility.

An attribute certificate (AC) is a structure similar to a Public Key certificate (PKC); the main difference being that the AC contains no public key. An AC may contain attributes that specify group membership, role, security clearance, or other authorization information associated with the AC holder (from: https://tools.ietf.org/html/rfc5755).

The Token Administration Utility (TAU) now includes the following information on ACs:

- *PKCS #11 objects* dialog (Show Token Objects): the column 'Type' indicates whether the certificate is a (PKC) 'Certificate' or an 'Attribute Certificate'.
- *Certificate* dialog (View certificate): the *Certificate* dialog includes information on 'Certificate Attributes' for an Attribute Certificate.
- *Certificate analysis* dialog (Analyse certificate quality): the (new) column 'Type' now indicates whether the certificate is a (PKC) 'Certificate' or an 'Attribute Certificate'.
- It is possible to import Attribute Certificates through the Import Certificate feature.
- It is possible to export Attribute Certificates through Save Object / Save to file.
- When making a dump file (Dump Token Contents), the resulting .tkn will include information on the certificate type; an Attribute Certificate will contain 'CKA_CERTIFICATE_TYPE: CKC_X_509_ATTR_CERT'.

  - Note that translations for Attribute Certificates and their attributes / extensions are only available in Dutch, Portuguese and Brazilian Portuguese.

# 4 New Features and Fixes

SafeSign IC Standard version 3.5 for Windows has a number of new features and fixes / changes.

Section 4.1 will describe the new features and functionality.

Section 4.2 will describe the improved and fixed features and functionality.

## 4.1 New

- Added support for Infineon Oracle JCOS Ed.1
- Added support for Morpho IDealCitiz 2.1
- Added support for StarSign Crypto USB-Token S
- Added support for NXP JCOP 3 SecID P60
- Added a number of new ATRs for supported cards.
- The Token Administration Utility reflects the new SafeSign IC version 3.5 product version numbering scheme and now includes the version number for all components included.
- In the Token Information dialog, the field 'Last Update of PIN' now includes the exact date of the last PIN change in the format YYYY-MM-DD (in accordance with the extended date representation of the ISO 8601 standard). When the last update of the PIN is the same day /today, the field includes the text 'today' (not the date in YYYY-MM-DD format).
- As users may want to be able to see the number of PUK retries left when entering the PUK (to prevent the PUK from getting blocked), a PUK retry counter has been implemented. This should be enabled by the registry setting 'ShowPUKRetryCounter'. When enabled, any dialog that includes PUK entry (such as Change PUK or Unlock PIN) will display not only that the PUK inserted was wrong (which is existing functionality), but also the remaining tries before the PUK will be blocked.
- A PIN retry counter has been added to the Change PIN dialog of the tokenadmin as well.

### 4.1.1 Version 3.5.2.0

- SafeSign IC Standard Version 3.5.2.0 allows you to view (information on) Attribute Certificates on the token and import / export Attribute Certificates through the Token Administration Utility.
- Support for Microsoft Edge.
- Added support for Oberthur IDone Cosmo v7.0.2 (ATR).

## 4.2    Fixed

- In SafeSign IC Standard Version 3.5, a number of cards (and related data, including ATRs and CPLC data) have been removed. Basically, SafeSign IC will only support Java Card v2.2.2 and higher cards. See section 6 for more details.

- Applet loading functionality has been disabled. This functionality was included for evaluation and demonstration purposes only (working only for cards with a default Global Platform keyset) and use of the included applet has been deprecated.

- As a consequence of the above, the Token Administration Utility option 'QueryUnknownToken' has been removed.

- Applied a consistent name convention for Giesecke & Devrient cards, i.e. 'G&D Sm@rtCafe Expert'.

- The Firefox Installer has been renamed to 'SafeSign IC for Firefox Installer'.

- Solved an issue where the Token Administration Utility would crash when importing a Digital ID file containing Cyrillic characters.

- In the Unknown ATR message (displayed in the Token Utility when the ATR of a card is not known in SafeSign IC), the e-mail address for SafeSign Support has been updated (safesignsupport@aeteurope.com).

- There was an issue in SafeSign Standard Version 3.0.112, when installing the SafeSign IC PKCS #11 Library through the Firefox Installer in Firefox 58.0, due to changes Firefox made in the method for registering a PKCS #11 Library. This has been fixed in SafeSign IC Standard Version 3.5.

## 4.3    Version 3.5.2.0

- With the Token Administration Utility open, entering an incorrect PIN in another (external) application (e.g. when doing secure web authentication) will not update the PIN retry counter. This issue has been fixed.

- There was an issue when using a secure pinpad reader in SafeSign IC Standard Version 3.5.0.0, where the SafeSign PIN entry dialog would be displayed, rather than the secure pinpad entry dialog (instructing you to enter the PIN on the reader's pinpad). This issue has been fixed.

- There was an error opening the SafeSign License Agreement files installed with SafeSign IC Standard Version 3.5.0.0. This issue has been fixed.

- There was an issue in SafeSign IC Standard Version 3.5.0.0 on Windows 32-bit, where the uninstallation would not install 'aetpkssw.dll' from the system directory and registry. This issue has been fixed.

- SafeSign IC Standard Version 3.5.0.0 would crash on Windows 32-bit when a change PIN was performed on a card with secure message enabled and the SSD (Supplementary Security Domain) blocked. This issue has been fixed; the Token Administration Utility will now (correctly) give a Device Error.

- There was an issue in SafeSign IC Standard Version 3.5.0.0 that some characters in Serbian Latin (ć, č and đ) would be incorrectly displayed (e.g. the č character would be displayed as è). This issue has been fixed.

- In SafeSign IC Standard, the SafeSign IC Key Storage Provider (aetcngss.dll) would not be mentioned in the Version Information of the Token Administration Utility. This issue has been fixed.
- Although it is not possible to upgrade an existing installation of SafeSign IC Standard (version 3.0.112 or lower) to SafeSign IC Standard Version 3.5, it is now possible to upgrade from SafeSign IC Standard Version 3.5.0.0 to SafeSign IC Standard Version 3.5.2.0. Please refer to the Installation Guide for more details.
- In SafeSign IC Standard Version 3.0.112 and 3.5.0.0, you could resize the Token Administration Utility window to a very small size. The resize has been limited, to a size where the text of the menu items remains visible.

## 4.4    Version 3.5.3.0

- There was an issue identified in SafeSign IC Standard (from version 3.0.101 and higher) with Citrix XenApp 7.17 / Citrix Virtual Apps 1811, where after the reconnect of a disconnected Citrix ICA session, open applications would no longer interact with the token or detect card insertion / removal. This has been fixed in SafeSign IC Standard Version 3.5.3.0.

# 5 Known Issues

## 5.1 General

- When installing the SafeSign IC Standard .msi package, the default language of the installation program will be English. In order to install the .msi in a particular language, you will need to install the .msi with specific parameters, to apply a transform.

- Firefox 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

- When you minimize the SafeSign IC installer during installation (including a Modify, Repair and Remove of the installation), the window moves for 90% out of screen.

- When initialising or wiping a smart card, the message "Token label must contain some characters" is also displayed (it does not change) when the label is too long. Nevertheless, when the maximum length for the label is exceeded, a red cross will appear instead of the green OK icon.

- When generating / importing a Digital ID file or certificate and the message that the token is full (out of memory: 0x80090023) is displayed, it may be that the whole or parts of the Digital ID file (and certificate chain) or the certificate have been placed on the smart card nevertheless. This will be clearly visible in the Token Administration Utility (Show Token Objects).

- When initialising or wiping a token with Root CA certificates, you can only select a particular directory. It is not possible to select a particular file.

- When importing a CA certificate file (either during initialisation or by the function Import Certificate), *.crt files are not selected by the default file extensions (*.cer, *.der), although the import does work.

- On Windows 7, the locale setting for displaying SafeSign IC in Serbian Cyrillic and Serbian Latin is "Serbian (Cyrillic, Serbia and Montenegro (Former))" and "Serbian (Latin, Serbia and Montenegro (Former))" respectively.

- Cards that do not support logical channels do not support challenge response authentication (unlock).

- It is not possible to set up a Microsoft VPN connection on Windows 8.1 with a card without logical channels enabled (or only one logical channel enabled).

- It is not possible to set up a VPN connection on Windows 10 (with any card).

- When creating a data object containing no data (done by using an empty CKA_VALUE), an error occurs (CKR_DEVICE_ERROR). According to the PKCS #11 standard, it is allowed to leave the CKA_VALUE empty. Although the SafeSign PKCS #11 implementation correctly handles the empty CKA_VALUE, the command to create the file fails. As a workaround, a null-byte should be used instead of an empty byte.

- On Windows 64-bit Operating Systems, when SafeSign IC Standard is uninstalled, the CSP gets unregistered. The installer then removes all ATR entries it made during installation in the 32-bit registry[1], but not under the 64-bit entry. The name of the associated CSP ("SafeSign Standard Cryptographic Service provider") is thereby changed (to "SafeSign CSP Version 1.0"), so these entries do not interfere when a new version of SafeSign IC is installed. Nevertheless, we strongly recommend to clean (remove all entries below) the 64-bit registry key[2] prior to installing a new version.  Please contact AET SafeSign Support for a tool to clean the smart card registry entries.

- There is no message when entering the wrong PUK during off-line PIN unlock (by means of the PUK) at smart card logon.

- It is not possible to set a PIN Timeout for the RIC Card, as this is not supported by the applet for the RIC Card.

- It is not possible to enrol a 1024 bits key pair on a RIC Card, as this is not supported (it is possible to generate a 2048 bits key pair).

- 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).

- When using the SafeSign Key Storage Provider to request a certificate through MMC / Certificate Manager, the resulting keys and certificate will not have a label, as can be seen from the Token Administration Utility's Show Token Objects dialog. This does not influence the functional operation of the Digital ID, except in the case of Firefox (See Known Issues: General).

- When enrolling for a certificate using MMC / Certificate Manager through the SafeSign IC Key Storage Provider (KSP), on a system with two readers attached and two smart cards inserted, you will not get a dialog to select the smart card (slot) to generate a certificate in. This option is not implemented in the SafeSign IC KSP.

- When the SafeSign IC Credential Provider is installed, it is not possible to set up a VPN connection (or access network shares), as there is no credential tile displayed. This is caused by the fact that the SafeSign IC Credential Provider does not support SSO (whereby it is not available). When you want to use VPN, you should not install the SafeSign IC Credential provider (as it is by default).

- When the SafeSign IC Credential Provider is installed, it is not possible to select which certificate to use, when the smart card contains more than one (suitable) certificate. This is acsued by the fact that the SafeSign IC Credential Provider does not support multiple certificates on one card.

---

[1] [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Calais\SmartCards]
[2] [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards]

- On Windows 10, when the SafeSign IC Credential Provider is installed, it is not possible to use the function 'Change a password' (Ctrl+Alt+Delete and then click Change a password) to change the password, whether you are logged in with username and password or a smart card. In that case, it is only possible to change the PIN for the smart card inserted by means of the SafeSign IC Credential Provider.

- On Windows 10, when the SafeSign IC Credential Provider is not installed and you select the smart card as sign-in option, you cannot change the PIN for the smart card by means of the function 'Change a password' (Ctrl+Alt+Delete and then click Change a password). You will get a smart card error ("The smart card requires drivers that are not present on this system."). The Microsoft Smart Card Credential Provider does not interact with the SafeSign IC smart card (CSP).

- There is an issue that when using a secure pinpad reader, the SafeSign PIN entry dialog will be displayed, rather than the secure pinpad entry dialog. This issue was also present in SafeSign IC Standard Version 3.0.112 and may be fixed in a future release.

### 5.2.1 Version 3.5.0.0

- On Windows 10, the locale settings "Serbian (Cyrillic, Serbia)" and "Serbian (Latin, Serbia)" are not working. Microsoft changed handling of the Serbian language on Windows 10, which causes wxwidgets to not recognize the language (language unknown).

- In languages other than English, some items in the Version Information dialog are not translated (e.g. Build number, Distribution number and the names of the Secure Messaging libraries).

### 5.2.2 Version 3.5.2.0

- In Firefox version 65.0 and higher, the reader name is displayed in the Security Devices column, not the token label (even when the token is inserted).

# 6       Supported Operating Systems

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

| Operating System | Version 3.5.0.0 – 3.5.3.0 |
| --- | --- |
| Windows 7 SP1 (Enterprise) | √ |
| Windows 8.1 (Enterprise) | √ |
| Windows 10 (Professional, Enterprise) | √ |
| Windows Server 2008 R2 SP1 Enterprise | √ |
| Windows Server 2012 R2 Datacenter | √ |
| Windows Server 2016 | √ |

Like every SafeSign IC release, SafeSign IC Standard Version 3.5 for Windows was tested on the abovementioned Windows Operating Systems with the (latest) Service Pack and Updates available at that time. Though SafeSign IC Standard Version 3.5 may work on older / other versions of these Operating Systems, only support requests for issues reproduced on the supported Windows Operating Systems listed above (up-to-date with the latest Windows Updates) will be taken into consideration.

⚡ Note that Windows Server 2012 (R2) and 2016 only run on x64 processors, so you should install the 64-bit version of SafeSign IC on Windows Server 2012 / 2016.

⚡ Note that in order to use SafeSign IC Standard Version 3.5 on Windows 10, we recommend to install the latest version of Windows 10 (Professional or Enterprise), which is currently 1903, OS Build 18362.175.

# 7 Supported Tokens

SafeSign IC for Windows supports a number of smart cards and tokens, as listed below.

These tokens have been tested to work as part of the release testing for SafeSign IC version 3.5 for Windows.

The number of cards supported in SafeSign IC for Windows has been decreased, to support only those cards that are non-proprietary and are compliant with at least Java Card 2.2.2 and higher.

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

From SafeSign IC version 3.5, applet loading functionality has been disabled. In previous versions, an old and deprecated version of the SafeSign IC applet was included, which could be installed on Java cards (during initialisation through the Token Utility) for demonstration and evaluation purposes, if such a card contained a default GlobalPlatform keyset. Obviously, this is not desirable in production (use), where the proper applet should not only be pre-installed, but the default keyset changed to a custom(er) keyset, in a secure production facility / environment.

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

| Card Type |
|---|
| Defensiepas |
| Defensiepas 2 |
| G&D Convego Join 4.01 40k/80k |
| G&D SkySIM Hercules |
| G&D SkySIM Scorpius |
| G&D Sm@rtCafé Expert 3.2 |
| G&D Sm@rtCafé Expert 4.0 |
| G&D Sm@rtCafé Expert 5.0 |
| G&D Sm@rtCafé Expert 6.0 |
| G&D Sm@rtCafé Expert 7.0 |
| G&D Sm@rtCafé Expert 64 |
| Gemalto Desineo ICP D72 FXR1 Java |
| Gemalto IDCore 30 |

| Card Type |
| --- |
| Gemalto MultiApp ID v2.1 |
| Gemalto Optelio D72 FR1 |
| Gemalto TOP DL v2 |
| Infineon Oracle JCOS Ed.1 |
| JCOP21 v2.3 |
| Morpho IDealCitiz v2.1 |
| Morpho JMV ProCL V3.0 |
| NXP J2A080 / J2A081 (JCOP 2.4.1 R3) |
| NXP JD081 (JCOP 2.4.1 R3) |
| NXP J3A080 (JCOP 2.4.1 R3) |
| NXP JCOP 2.4.2 R3 |
| NXP JCOP 3 SecID P60 |
| Oberthur IDOne Cosmo v7.0 |
| RDW ABR kaart |
| Rijkspas |
| Rijkspas 2 |
| Sagem YpsID s2 |
| Sagem YpsID s3 |
| StarSign Crypto USB Token S |
| Swissbit PS-100u SE |
| UZI-pas |
| UZI-pas 2 |

# 8 Supported Smart Card Readers

SafeSign IC Standard provides support for PCSC 2.0 Class 1 readers, as well as Class 2 and 3 secure pinpad readers (≥ 3.5.2.0).

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

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

The following table lists the specific readers that have been tested with SafeSign IC Standard Version 3.5.2.0 for Windows:

| Smart Card Reader Manufacturer and Model | Class |
|---|---|
| HID Global CardMan 3x21 | 1 |
| Cherry ST-20000U | 2 |
| Reiner-SCT Secoder | 3 |

Note that smart card readers that have been tested or have been working at a given time with a previous SafeSign IC version for Windows, may not (still) work or be supported in any or all versions of SafeSign IC version 3.5 for Windows.

# 9      Supported Applications

SafeSign IC Standard version 3.5 for Windows has been tested in accordance with AET's Quality Assurance procedures and the SafeSign IC Standard for Windows test plan. This includes testing of a number of defined and representative applications to verify a correct functioning of the SafeSign IC components and Libraries.

The following applications have been tested with SafeSign IC for Windows:

| Application | Version | Purpose |
|---|---|---|
| Token Administration Utility | 3.5.0.4257 | PKCS #11 token management functions |
| Mozilla Firefox | 66.0.3 | Certificate enrollment with key pair generation; Authentication to a secure web site |
| Mozilla Thunderbird | 60.6.1 | Signing and decrypting e-mail messages |
| Internet Explorer | 11 | Certificate enrollment with key pair generation; Authentication to a secure web site |
| Microsoft Edge | - | Authentication to a secure web site |
| Microsoft Outlook | 2016 | Signing and decypting e-mail messages |
| Adobe Reader DC | 2019.010.20099 | Digitally signing a document |
| Microsoft Word | 2016 | Digitally signing a document |
| Windows Smart Card Logon | - | Log on to a local Windows client system |
| Terminal Server Logon | - | Log on to a Windows Terminal Server |

🖈 Note that PKCS #11 applications (such as Firefox) need the PKCS #11 Library to be loaded / installed as a security module. The SafeSign IC PKCS #11 Library (called 'aetpkss1.dll') can be found in the system directory.

🖈 Note that (Microsoft) applications using the CSP / KSP do not normally require any configuration, i.e. you do not need to select or install the SafeSign CSP / KSP Library.

## 9.1     Token Administration Utility

With the SafeSign IC Token Administration Utility, you can perform (local) smart card related operations, such as changing the PIN for your smart card or token.

The features available in the Token Administration Utility, can be modified in the Windows registry. The features to be enabled (1) or disabled (0) are located in 'Actions'.

Refer to the Administrator's Guide for more details.

## 9.2 Mozilla Firefox

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

Refer to the 'SafeSign Identity Client Standard Installation Guide' and 'SafeSign Identity Client Token Utility Guide' how to install SafeSign IC Standard in Firefox during the installation process and by means of the Token Administration Utility.

## 9.3 Mozilla Thunderbird

With the SafeSign PKCS #11 Library installed as a security module in Thunderbird, you can send and receive signed and/or encrypted message with a SafeSign IC token.

To verify whether the SafeSign PKCS #11 Library is installed as a security module in Thunderbird, go to Preferences -> Advanced -> Certificates (tab) -> Security Devices (button).

## 9.4 Internet Explorer

With SafeSign IC Standard installed, you can perform certificate enrollment (i.e. Certificate Services web enrollment for version 2 templates) and secure web authentication in Internet Explorer.

## 9.5 Microsoft Edge

With SafeSign IC Standard installed, you can perform secure web authentication in Microsoft Edge.

## 9.6 Microsoft Outlook

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

## 9.7 Adobe Reader DC

With SafeSign IC Standard installed, you can sign documents with a SafeSign IC token.

Adobe Reader DC supports the use of Windows Digital IDs through CryptoAPI, which is the recommended method.

It is also possible to use a PKCS #11 Library, but note that Adobe Reader Protected Mode is not able to interact with your smart card reader or token, so you will not be able to add a PKCS #11 Library, unless you disable Protected Mode, which is not recommended.

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.

## 9.8        Microsoft Word

With SafeSign IC Standard installed, you can sign documents with a SafeSign IC token.

## 9.9        Windows Smart Card Logon

With SafeSign IC Standard installed, you can use your SafeSign IC token to log on to a local Windows client machine. This client should be part of a Windows Server domain.

## 9.10      Terminal Server Logon

With SafeSign IC Standard installed, you can use your SafeSign IC token to log on to a remote Windows Terminal Server.

# 10    Supported Languages

The following languages are supported in SafeSign IC:

- Basque;
- Catalan;
- Chinese (Simplified);
- Chinese (Traditional);
- Croatian;
- Czech;
- Dutch;
- English;
- Finnish;
- French (France);
- German;
- Hungarian;
- Italian;
- Italian (Swiss);
- Japanese;
- Korean;
- Lithuanian;
- Portuguese (Portugal);
- Portuguese (Brazil);
- Russian;
- Serbian (Cyrillic);
- Serbian (Latin);
- Spanish;
- Thai;
- Turkish;
- Ukrainian.

## 10.1    Installation language files and codes

When installing the SafeSign IC Standard .msi file, you may apply a transform for the installation language (as described in section 3.4).

For example, to install SafeSign IC Standard Version 3.5 in Portuguese (Brazil):
msiexec /I "SafeSign IC Standard x64 3.5.2.0-AET.000.msi" TRANSFORMS=1046.mst

🎣 Note that InstallShield does not support all languages[3], hence the SafeSign IC InstallShield Wizard is not available in the following languages: Italian (Swiss), Lituanian, Serbian (Latin) and Ukranian.

The table below lists the Windows language code identifiers and corresponding transform files:

| Language | Code | File |
| --- | --- | --- |
| English | 1033 | 1033.mst |
| Basque | 1069 | 1069.mst |
| Catalan | 1027 | 1027.mst |
| Chinese (Simplified) | 2052 | 2052.mst |
| Chinese (Traditional) | 1028 | 1028.mst |
| Croatian | 1050 | 1050.mst |
| Czech | 1029 | 1029.mst |
| Dutch | 1043 | 1043.mst |
| Finnish | 1035 | 1035.mst |
| French (France) | 1036 | 1036.mst |
| German | 1031 | 1031.mst |
| Hungarian | 1038 | 1038.mst |
| Italian | 1040 | 1040.mst |
| Japanese | 1041 | 1041.mst |
| Korean | 1042 | 1042.mst |
| Portuguese (Portugal) | 2070 | 2070.mst |
| Portuguese (Brazil) | 1046 | 1046.mst |
| Russian | 1049 | 1049.mst |
| Serbian (Cyrillic) | 3098 | 3098.mst |
| Spanish | 1034 | 1034.mst |
| Thai | 1054 | 1054.mst |
| Turkish | 1055 | 1055.mst |

[3] http://helpnet.flexerasoftware.com/installshield19helplib/helplibrary/IHelpGlobLangIdentifiers.htm#CreatingMultilingual_2070637897_1021572