Unlimited access
to your world

SafeSign Identity Client Standard

Release Notes for Windows

Table of Contents

Table of Figures

Document Information

Title: SafeSign Identity Client Standard Release Notes Windows

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

Project: SafeSign IC Release Documentation

Document revision history

Version	Date	Author	Changes
2.0	29-04-2015	Drs C.M. van Houten	First edition for SafeSign Standard Version 3.0 for Windows (release 3.0.101)
3.0	24-03-2016	Drs C.M. van Houten	First edition for SafeSign Standard version 3.0 for Windows (release 3.0.112)

SafeSign
Identity Client

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 release note is to document the status of the release of the SafeSign Identity Client Standard software, supporting the tokens defined in the SafeSign Identity Client Standard Product Description (SafeSign-IC-Standard_3.0.112_Windows_Product_Description).

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

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

This document is part of the release documentation for SafeSign IC

2 Release Declaration

2.1 Designation of the release

This document is the Release Notes for SafeSign Identity Client Standard Version 3.0.112(-x64) for Windows.

SafeSign Identity Client Standard Version 3.0.112 is designed to work on all platforms, client applications and with all tokens that are defined in the latest SafeSign Identity Client Standard Version 3.0.112 Product Description for Windows (SafeSign-IC-Standard-3.0.112_Windows_Product_Description).

2.2 Date of release

The release date is 24 March 2016.

2.3 Characteristics of the release

The SafeSign Identity Client Standard Version 3.0.112 Product Description defines all third-party products with which SafeSign Identity Client Standard Version 3.0.112 and/or 3.0.112-x64 functionality was tested successfully.

3 Object of the Release

3.1 Released programs

The following table lists all software components delivered with the release SafeSign Identity Client Standard Version 3.0.112 for Windows[1], both 32 and 64 bits.

SafeSign Standard 3.0.112 ()			
Component Name	Version	Location	Brief Description
aetcngss.dll[2]	3.0.0.3925	<system dir>\	Crypto Next Generation Module
aetcrss1.exe	3.0.0.3747	<system dir>\	Certificate Expiration Check Utility
aetcsss1.dll	3.0.0.3912	<system dir>\	CSP Library
aetdlss1.dll	3.0.0.3893	<system dir>\	Common dialogs
aetjcss1.dll	3.0.0.3931	<system dir>\	Java Card Handling Library
aetpkss1.dll	3.0.0.3930	<system dir>\	PKCS #11 Cryptoki Library
aetpksse.dll	3.0.0.3746	<system dir>\	PKCS #11 Library wrapper for Entrust
aetpkssw.dll	3.0.0.3746	<system dir>\	PKCS #11 Library wrapper with automatic login
aettask.dll	3.0.0.3748	<system dir>\	Task Manager
aetcpss1.dll[3]	3.0.0.3751	<system dir>\	Credential Provider
TokenManager.exe[4]	3.0.0.3920	<install dir>\	Token Management Utility
TokenAdmin.exe	3.0.0.3920	<install dir>\	Token Administration Utility

3.2 SafeSign IC Standard 32-bit

Note that the 32-bit version of SafeSign Identity Client Standard is for 32-bit Operating Systems only. Though it will install on 64-bit 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 Identity Client) CSP is missing from the appropriate 64-bit branch of the registry, causing certificates not to be registered by the Microsoft Certificate Propagation Service.

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

[1] The SafeSign Store Provider (aetsprov.dll) is not included in SafeSign Identity Client version 3.0.45 and higher anymore.

[2] Installed on Windows 7 and higher only.

[3] For use with Windows 7 and higher only.

[4] SafeSign Standard Version 3.0 for Windows is delivered in separate installers including either the Token Management Utility (TMU) or the Token Administration Utility (TAU).

3.3 SafeSign IC Standard 64-bit

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 Identity Client version 3.0.112-x64 system files will install in both directories (to ensure that both 32-bit and 64-bit applications can work with SafeSign Identity Client), 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; on Windows Vista and higher only).

The Token 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 Identity Client Standard, some entries 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 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 clean the smart card registry entries.

3.4 Evaluation version

SafeSign Identity Client Standard Version 3.0.112 for Windows comes in special evaluation versions, to which a special license agreement applies.

4 End User Documentation

SafeSign Identity Client Standard Version 3.0.112 for Windows provides at least the following end user documentation:

Document name	Document Version
SafeSign Identity Client Standard 3.0.112 Release Notes for Windows	3.0
SafeSign Identity Client Standard 3.0.112 Product Description for Windows	4.0

5 New Features and Enhancements

5.1 New Features

The following features are supported by SafeSign Identity Client Standard Version 3.0 for Windows:

- Multiple token support;
- Multiple language support;
- Multiple OS support;
- Remote Desktop Connection;
- Support for Igel thin clients;
- Support for PIN timeout;
- Support for PC/SC 2.0 secure pinpad readers;
- Support for maximum PUK and PIN length;
- Support for virtual readers in PKCS#11;
- SafeSign IC Credential Provider;
- Support for SHA-2;
- Support for AES;
- Support for Microsoft Certificate Propagation;
- Support for Cryptography API: Next Generation (CNG) Key Storage Provider;
- Support for Event Logging;
- Support for new cards and applet functionality;
- Support for 3DES key storage on the card.

These features are described in detail in the SafeSign Identity Client Standard Version 3.0.112 Product Description (SafeSign-IC-Standard_3.0.112_Windows_Product_Description) and will not be separately listed in the (Major) enhancements section below.

5.2 Enhancements

The enhancements below describe the features and enhancements of SafeSign Identity Client Standard versions 3.0.x(-x64), for both 32-bit and 64-bit Operating Systems, unless explicitly mentioned otherwise. Descriptions of the features and enhancements of SafeSign IC versions prior to 3.0.97 can be found in earlier release notes.

5.2.1 Cosmetic enhancements

5.2.1.1 ≥ 3.0.97

- Copyright notices and information were updated.
- The password input field in the Import Digital ID dialog was too small. This has been fixed.
- References to the MartSoft Java Card have been removed from the registry.

5.2.1.2 ≥ 3.0.112

- Updated the installer splash screen to include the up-to-date copyright notice and new company logos.
- Created an evaluation version that better reflects its status as an evaluation version.

5.2.2 Functional enhancements

- In order to enable us to provide better support to end users, the unknown ATR dialog now mentions the e-mail address for the SafeSign Support department, i.e. safesignsupport@aeteurope.nl. When copying the ATR to the clipboard, not only the ATR, but also the SafeSign IC version (and build number) will be displayed.
- The SafeSign IC Key Storage Provider has been improved to better handle multiple threads.
- The JCOP ATRs from ChangingTec (Changing Information Technology Inc.) have been added.
- Some improvements have been made to the SafeSign Credential Provider, such as the ability to customise the available unblocking methods. For more details regarding these improvements, refer to the Product Description.

5.2.2.1 ≥ 3.0.97

- When saving the version information of SafeSign Identity Client installed on a Windows 8 / 8.1 or Windows Server 2012 R2 machine, the resulting file did not display the OS version correctly. This has been fixed.
- Added support for the J3A081 smart card in contactless mode, by including its contactless ATR (T=CL) to the registry.

- 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.
- A registry setting has been added to the SafeSign IC registry to improve performance of signing operations in complex infrastructures, by disabling the session check for each (intermediate) (web-based) signing request. The setting 'DisableSessionCheck' is located in HKEY_LOCAL_MACHINE\SOFTWARE\[Wow6432Node\]A.E.T. Europe B.V.\SafeSign\2.0\ and can be enabled by setting its value to 1 (value 1 means feature is on, check is skipped; other values mean off, check is performed). An example of an application that will benefit from this setting is the application Web-ELAN from the Netherlands' Cadastre, Land Registry and Mapping Agency (Kadaster).
- Fixed an issue in the SafeSign Key Storage Provider for signing certificates that do not have a public key.
- Microsoft revised the process of submitting a custom CSP to Microsoft for signing (see http://msdn.microsoft.com/en-us/library/ms953432.aspx). Microsoft will no longer sign CSPs, and the manual CSP signing service has been retired. Instead, all third-party CSPs can now be self-signed (see http://msdn.microsoft.com/en-us/library/windows/hardware/dn553410(v=vs.85).aspx). In accordance with this process, AET has signed and will sign its binary files with Authenticode as of SafeSign version 3.0.97.

5.2.2.2 ≥ 3.0.101

- In SafeSign Identity Client version 3.0.97, when you try to access a secure web page in Internet Explorer, an error may occur ("Page cannot be displayed") in the following scenario: an uninitialised (or unknown) token in the first reader / slot and another token containing an authentication certificate and inserted in the second reader / slot. In that case, the certificate selection dialog will appear, but you will not be asked for the PIN of your token (everything will work if the operational card is inserted in the first reader / slot) . This scenario may occur when you want to enroll a user's smart card after being logged in with an administrator card / enrollment certificate or when you have an unknown token inserted (but which is recognised as a Java card) in another reader. This has been fixed in SafeSign Identity Client version 3.0.101.
- With SafeSign Identity Client version 3.0.97, when signing an Adobe pdf document (form) in Internet Explorer, Adobe would crash ("Adobe Reader has stopped working"). This has been fixed in SafeSign Identity Client version 3.0.101.
- The installation of SafeSign Identity Client version 3.0.97 would fail on a Windows Server 2008 (SP2). This has been fixed in SafeSign Identity Client version 3.0.101.
- In SafeSign Identity Client version 3.0.97, there was an error decrypting messages in Outlook 2010 caused by an external process / program resetting the card (reproduced by running certutil –scinfo during decryption). This has been fixed in SafeSign Identity Client version 3.0.101.

5.2.2.3 ≥ 3.0.112

- 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' in the (same) location as where the SafeSign License Agreement is located, i.e. ProgramData\A.E.T. Europe B.V\SafeSign\Documentation\.
- 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.
- 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.
- In SafeSign Identity Client Standard version 3.0.101, there was an issue with STARCOS (3.x) cards and Microsoft VPN on Windows 8.1. This has been fixed in SafeSign Identity Client Standard version 3.0.112.
- In SafeSign Identity Client version 3.0.101, there was an issue with RDP on Windows 10, using cards without logical channels (or only one logical channel enabled) and STARCOS (3.x) cards. 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.
- There was an issue in the SafeSign Key Storage Provider from SafeSign Identity Client Standard version 3.0.97 and higher, with SAP GUI 7.40 with SAP Secure Login Client Version 2 Support Package 5. The SAP GUI with SLC issues the following error message after entering card's PIN: "GSS-API(min): A2200209:Decryption: Private key operation failed." This did work with SAP SLC Version 2 SP4 and below, after which SAP changed the CryptoAPI used, from "legacy" (in SP4) to "CNG" (in SP5). This has been fixed in SafeSign Identity Client Standard version 3.0.112.
- In SafeSign Identity Client Standard version 3.0.101, it was not possible to enrol a certificate through MMC / Certificate Manager with the SafeSign Key Storage Provider. When trying to generate the keys, the *Insert Smart Card* dialog appears and you will not be able to select your smart card (reader). This has been fixed in SafeSign Identity Client Standard version 3.0.112.

5.2.3 Major enhancements

5.2.3.1 ≥ 3.0.97

- Added support for the Identive SCT3522DI Mifare Flex USB Token (with NXP JCOP 2.4.2 R2)

5.2.3.2 ≥ 3.0.101

Added support for the following tokens:

- Giesecke & Devrient Sm@rtCafé 7.0 (CC and FIPS)
- Yubico Yubikey NEO[5]
- Swissbit PS-100u SE Micro SD card
- Rijkspas 2[6]
- Vasco DP 920

5.2.3.3 ≥ 3.0.112

Added support for the following tokens:

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

[5] Please contact AET in case you are interested in using the Yubikey token.

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

6 Known Issues

This section provides an overview of the known issues in SafeSign Identity Client versions 3.0.x-x64, for both 32-bit and 64-bit Operating Systems, unless explicitly mentioned otherwise. Descriptions of the known issues of SafeSign IC Standard versions prior to 3.0.97 can be found in earlier release notes.

Known issues are divided into three categories:

1. Internal: issues with regard to the way SafeSign Identity Client and its utilities look and work.
2. Interoperability: issues with regard to the tokens, smart card readers and third-party applications that SafeSign Identity Client supports. These are divided into three categories:
   - General: issues related to the interaction between SafeSign Identity Client and Operating Systems, tokens and applications;
   - SafeSign: issues specific to SafeSign Identity Client and/or SafeSign Identity Client versions;
   - Credential Provider: issues related to the SafeSign Credential provider.
3. External: issues with regard to other dependencies, such as specific Operating System issues.

6.1 Internal

1. In the certificate expiration warning, the URL cannot be used to connect directly to a web site.
2. When you minimize the SafeSign Identity Client installer during installation (including a modify, repair and remove of the installation), the window moves for 90% out of screen.
3. The PIN Entry dialog that appears in the Taskbar on Windows Vista and higher, does not have an icon. This is in fact, the icon of the program that uses SafeSign Identity Client. If an application without icon is using SafeSign Identity Client, there will be no icon. We noticed that Outlook does present an (Outlook) icon, whereas Internet Explorer (for example during certificate enrolment) does not present an icon.
4. When initializing a token, the message “Token label must contain some characters” is also displayed when the label is too long. When the maximum length is exceeded, a red cross will appear instead of the green OK icon.
5. There registry setting ‘EditLabelAction’ removes the Edit Label button in the Show Token Objects dialog. However, it does not disable the button change / set the label in the Import Digital ID dialog.

6.2 Interoperability

6.2.1 General

6. Although different key sizes are supported, the key generation interval may be different. For example, for the G&D STARCOS 3.0 card, the interval is 8 bits (768, 776 – 2048); for the G&D Sm@rtCafé Expert 64K card, the interval is 16 bits (768, 784 – 2032, 2048); for the IBM JCOP41 (72K) card and the Oberthur IDone Cosmo64 v5.2 card, the interval is 64 bits (768, 832 – 1984, 2048).

7. The G&D Sm@rtCafé Expert 64K card does not work in combination with the CardMan 2020 reader .

8. In Windows XP, when using Word to edit e-mail messages in Outlook 2000 / 2002, the SafeSign Identity Client Login dialog may be out of focus. You will have to click in the SafeSign Identity Client Login dialog to be able to enter your PIN. We cannot solve this issue; however, you cannot close Outlook without having entered the PIN. This holds true for other applications as well, for example, you cannot close the Token Management Utility / Token Administration Utility when the PIN dialog is active.

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

10. With regard to Microsoft VPN token interoperability: (1) it is not possible to present the number of attempts left to enter the correct PIN in the VPN connection dialog (this is functionality that Microsoft does not enable); (2) Microsoft VPN does not abort the connection when the token is removed. Though it would be preferred that the VPN connection is aborted in such cases, this functionality is provided and controlled by the Microsoft VPN application, which does not allow for this.

11. Entrust system logon and Entrust ICE do not work with protected authentication path devices (i.e. a secure pin pad reader).

12. If you try to view a certificate in Windows XP, of which the complete trust chain is not available in the Microsoft Certificate Store, it may take a while to load / view the certificate. This is caused by Internet Explorer trying to find the root CA certificate.

13. There are a number of issues with both Citrix MetaFrame XP FR3 and Citrix MetaFrame Presentation Server and the use of tokens. These issues have been solved and have been made available by Citrix for the general public (≥ Presentation Server 4.0 / hotfixes). Note that SafeSign Identity Client works seamlessly with Citrix Presentation Server 4.0 and higher.

14. Token initialisation and/or key generation of 1,024 / 2,048 bits keys may fail when using Java Card v2.2 (and higher) Java cards (such as the IBM JCOP41) in contactless mode. This may be caused by the smart card reader not providing enough power for this operation or physical obstructions.

15. When initializing a (blank) token with Root CA certificates, you can only select a particular directory. It is not possible to select a particular file.

16. When importing a CA certificate file (either during initialisation or by the function Import certificate), the file *.crt is not selected by the default file extensions (*.cer, *.der).

17. The SCM SCR331 reader crashes when used in combination with Outlook 2000.

18. There is an issue with Windows 2003 Terminal Server, where trying to unlock the PC, may lead to a "requested key container could not be found" error. This occurs in a particular scenario: where the session that is open but locked on one PC (1), is disconnected upon logging in to another PC (2) and then locked again by removing the token from PC (2). This issue does not occur with Windows Server 2008.

19. There is an issue with Windows 2003 / 2008 Terminal Server and Citrix, where an application will not be able to access the token, when the application is (already) running on one PC, which is locked (by removing the token) and is opened again in a terminal session on another PC. This occurs in a particular scenario: the user logs in with the smart card to one PC (1) and opens an application requiring the access to the token (e.g. Outlook with signed mail), which works fine. Then the user removes the token from the reader on this PC (1), with Outlook still running, upon which the PC (1) gets locked. The user then logs in with the same token to another PC (2) and opens a Remote Desktop Connection to PC (1). When the user at this point, tries to use Outlook to send a signed mail, this does not work. Outlook reports an "Error in the underlying security layer". If the user at PC (2) exits from Outlook and starts it again, Outlook can access the token again and send signed mail. This is caused because the entire context, in which the token is used, has changed (for example, the smart card readers' slots may have been re-enumerated).

20. In Windows Server (CA) it is possible to request a new certificate with an existing key pair (through MMC / Certificate Manager), when for example, a certificate is expiring / expired. This functionality is supported by SafeSign Identity Client, but some applications cannot handle this. For example, when using Outlook Express and encrypted messages, it is not possible to decrypt messages when a new certificate is requested. Outlook Express cannot find the certificate that was used to encrypt the message and displays an error.

21. When generating a self-signed certificate for use with EFS, this fails with a "Cannot find object or property" error.

22. There is an issue when installing SafeSign IC on a system where the system locale / the language for non-Unicode programs) is set to Serbian Latin. In that case, the InstallShield Wizard drop-down box will default to Croatian. This has been brought to the attention of Flexera Software and the language may be introduced in a later version of InstallShield.

23. On Windows XP, Windows Vista and Windows Server 2003, in order to have the SafeSign utilities and dialogs displayed in Serbian (both Latin and Cyrillic), you need to select "Serbian (Cyrillic, Serbia)" or "Serbian (Latin, Serbia)". In Windows 7 and higher (including Windows Server 2008 R2), you will need to select "Serbian (Cyrillic, Serbia and Montenegro (Former))" or "Serbian (Latin, Serbia and Montenegro (Former))". Other combinations will not work.

24. Though SafeSign Identity Client supports the Ukrainian language, the InstallShield Wizard is not available in Ukrainian, as InstallShield does not support it.

25. The combination of a secure pin pad reader and a card without support for logical channels does not work reliably, for example, when doing (web) authentication in Firefox and Google Chrome.

26. Though SafeSign Identity Client supports the Lithuanian language, the InstallShield Wizard is not available in Lithuanian, as InstallShield does not support it.
27. When installing the SafeSign Identity Client .msi installer, 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 : msiexec /i "SafeSign.msi" TRANSFORMS=1027.mst.
28. It is not possible to use a secure pinpad reader (Class 2 or Class 3) with cards / applets that have secure messaging enabled. The reason for this is that when secure messaging is enabled, secure messaging encrypts the tunnel between the card and the software when PIN actions are required. As the pinpad reader is not part of this tunnel (is not part of the secure messaging), you will get an error when entering the (non-encrypted) PIN on the pinpad.
29. It is not possible to set up a Microsoft VPN connection on Windows 8.1 with a card without logical channels (or only one logical channel enabled). This issue does not occur on Windows 7.
30. It is not possible to set up a Microsoft VPN connection on Windows 10 (with any card).
31. Web authentication with Microsoft Edge does not work. You will get a certificate selection dialog, but no PIN dialog. This is due to the fact that the new browser is a Universal Windows App, which will always run in partial sandbox and will not work with unauthorized (external) DLL files[7]. For web authentication, please use Internet Explorer 11.
32. It is not possible to use a secure pinpad reader for both local and remote smart card logon (RDP) on Windows 8.1 and higher. When entering the PIN on the smart card logon desktop, you will get an error “Invalid handle”. This issue does not occur on Windows 7.
33. 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.

[7] From https://blogs.windows.com/msedgedev/2015/11/17/microsoft-edge-module-code-integrity/: “Microsoft Edge defends the user’s browsing experience by blocking injection of DLLs into the browser unless they are Windows components or signed device drivers. DLLs that are either Microsoft-signed, or WHQL-signed, will be allowed to load, and all others will be blocked.”

34. Adobe Reader (DC) will not sign documents when the certificate is a smart card logon certificate. Adobe made changes with regard to certificates that can be used for signing. From http://www.adobe.com/devnet-ocs/acrobatetk/tools/DigSig/changes.html: "In version 11.0.9, Adobe introduced changes in the way digital certificates are filtered for signing. The changes were made in order to align certificate use more closely with the spec, RFC 5280. Starting in version 11.0.9, Acrobat/Reader filter off of the extended key usage (EKU) extensions in addition to the Key Usage (KU) extensions. Starting in version 11.0.9, certificates that are available for signing must have a Key Usage extension of digitalSignature or nonRepudiation. Or no KU extension. If an EKU extension is present, it must have a value of emailProtection or codeSigning or anyExtendedKeyUsage (OID 2.5.29.37.0)." A certificate based on the Smart Card User template satisfies these requirements, a certificate based on the Smart Card Logon template does not.

6.2.2 SafeSign Identity Client

6.2.2.1 General

35. The 64-bit installer adds values to the registry under the following node: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Calais\SmartCards]. When the CSP is registered, it reads the values from that key and fills the node [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards] with those values. When SafeSign Identity Client is uninstalled, the CSP gets unregistered. The installer then removes all entries it made during installation under the node [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Calais\SmartCards]. The entries under [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards] remain since the installer cannot remove anything it did not add himself. However, the name of the associated CSP ("SafeSign Standard Cryptographic Service provider") is 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) [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards] prior to installing a new version. Please contact AET SafeSign Support for a tool to clean the smart card registry entries.

36. Related to the issue above, when certain cards are not functioning in Internet Explorer (as a result of certificates not being registered) after updating SafeSign IC (64-bit) from an older version like 3.0.40 or 3.0.45, there may be an issue with older registry settings not being removed. In order to make sure no wrong registry settings are being used, clean the registry entries related to SafeSign (see Appendix 1 for more detail and instructions) before installing a new version.

37. In SafeSign Identity Client there is no message when entering the wrong PUK during off-line PIN unlock (by means of the PUK) at smart card logon.

38. 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.

39. 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.

40. 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).

41. It is not possible to use a secure pinpad reader with a card that has secure messaging enabled.

42. 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 below).

43. 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.

6.2.2.2 3.0.97

44. In SafeSign Identity Client Standard version 3.0.97, there is a problem with SPK 2.3 cards and A003 / A004 applications with PKCS #1 padding.

45. In SafeSign Identity Client Standard version 3.0.97, there is an compatibility with SAP GUI 7.40 with SAP Secure Login Client Version 2 Support Package 5, due to an issue in the SafeSign IC KSP.

6.2.2.3 3.0.101

46. In SafeSign Identity Client Standard version 3.0.101, it is not possible to enrol a certificate through MMC / Certificate Manager with the SafeSign Key Storage Provider. When trying to generate the keys, the Insert Smart Card dialog appears and you will not be able to select your smart card (reader).

47. In SafeSign Identity Client Standard version 3.0.101, it is not possible to use a STARCOS card to set up a Microsoft VPN connection on Windows 8.1.

48. In SafeSign Identity Client Standard version 3.0.101, it is not possible to set up a remote desktop connection with a card without logical channels (or only one logical channel enabled) or a STARCOS cards on Windows 10.

6.2.2.4 3.0.112

49. In SafeSign Identity Client Standard version 3.0.112, when enrolling for a certificate using MMC / Certificate Manager through the SafeSign IC Key Storage Provider, on a system with two smart card 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 has not been implemented in the SafeSign IC Key Storage Provider.

6.2.3 SafeSign IC Credential Provider

50. Note that as of SafeSign Identity Client version 3.0.70, the SafeSign IC Credential Provider is no longer installed by default anymore.

51. When the SafeSign IC Credential Provider is installed (on Windows Vista or higher), it is not possible to set up a VPN connection, 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, it is recommended not to install the SafeSign IC Credential Provider (as it is by default).

52. When the SafeSign IC Credential Provider is installed (on Windows Vista or higher), it is not possible to select which certificate to use, when the token contains more than one (suitable) certificate. This is caused by the fact that the SafeSign IC Credential Provider does not support multiple certificates on one card.

53. When the SafeSign IC Credential Provider is installed both on Windows Vista or higher you will have to enter your PIN again in the remote desktop logon screen, even if you have already entered your PIN in the local Windows Security *Enter your credentials* dialog. This does not happen if the Microsoft Credential Provider is installed on the remote computer[8].

54. The SafeSign IC Credential Provider does not support / will not display upon EFS or accessing network shares. In that case, no Credential Provider will show up. This is caused by the fact that the SafeSign IC Credential Provider does not support SSO (whereby it is not available).

55. When accessing a secure web site in Internet Explorer, there is no SafeSign IC Credential Provider tile to select from, even when the SafeSign IC Credential Provider is installed. This is because for secure web authentication in Internet Explorer, the Smart Card Credential Provider is not used (as is used for example for logon). Internet Explorer displays a Windows Security dialog to select a certificate, enumerating the certificates that are available in the local Personal store.

56. By default, the SafeSign IC Credential Provider is not selected for installation on Windows XP and Windows Server 2003, as these Operating Systems only support the GINA. When it is selected manually, an error will occur during installation, saying that module registration fails.

[8] When the Microsoft Credential Provider is installed on the server, there is a difference in behaviour. When using a normal reader, you will need to enter your PIN only once, i.e. on the client, when setting up the remote desktop connection (not on the remote desktop). When using a secure pinpad reader, you may be asked to enter your PIN more than once. If you do not enter your PIN after the first PIN entry, after some time, the remote desktop screen will ask for username and password or to switch the user, upon which you can select the Microsoft Credential tile and enter the PIN.

6.3 External

57. There is a known issue for the CSP that there seems to be a time period where you do not need to re-login to the token when e.g. signing email. This is in no way due to PIN caching. This is a known issue of Microsoft unloading the CSP. Tests showed that e.g. under Windows 2000 / XP, you will not be asked to log in to your token each time you sign a message (while the application remains opened), whereas under Windows 98, you will have to log in to the token every time. This is caused by the fact that although the SafeSign Identity Client CSP tries to maintain a logged-in session with the PKCS#11 Library as long as possible, the CSP itself is loaded by the implementation of CryptoAPI on the Windows Operating System and may also be unloaded by it. If this unloading is programmed such that the CSP is unloaded every time it is used, a user will for example, have to log in to his token every time he wants to sign a message. Furthermore, this unloading is different on all the different Operating Systems and is determined by Microsoft. This behaviour is independent from and cannot be influenced by the CSP.

58. In line with Microsoft's end-of-life policy, Windows NT 4.0 is not supported.

59. In line with Microsoft's end-of-life policy, Windows 98 and Windows ME are not supported.

60. In line with Microsoft's end-of-life policy, Windows 2000 are not supported.

61. Note that Microsoft ended support for Windows XP on April 8, 2014, meaning that there will be no more security updates or technical support for the Windows XP operating system. Support for Windows Server 2003 R2 ended on July 14, 2015. In line with Microsoft's end of (extended) support policy, Windows XP and Windows Server 2003 are supported up to SafeSign Identity Client Standard version 3.0.101.

62. With Microsoft Vista and higher, the Windows logon PIN prompt will not appear automatically when inserting a token. Even when using a token, you are required to press CTRL+ALT+DELETE (initiating a Secure Authentication Sequence), before being able to select the method of logging in, either with a username and password or with a smart card ("*Insert a smart card*"). This is part of the new architecture of Windows Vista and higher.

63. On Windows 8 and Windows Server 2012, changes were made to the "smart card sign-in experience", as described in http://technet.microsoft.com/en-us/library/hh849637.aspx: "For end users, the sign-in experience on Windows Server 2012 and Windows 8 has improved detection of whether a smart card reader was installed and whether a smart card or a password was used to sign in or unlock the computer the last time. If a smart card was not installed previously, and the user selects the smart card sign-in icon, a message appears telling the user to connect a smart card. After a card is connected, the smart card PIN dialog box appears. If the user does not want to use the sign-in option that automatically appears (if their smart card is not readily available, for example), a second message allows the user to select from different sign-in options." The same also applies to Windows 10.

64. The option in the Internet Explorer web enrollment pages to request a certificate on behalf of another user (through the so-called Smart Card Enrollment Station) is no longer available. From the same knowledge base article as referred to above: "The Windows Vista certificate enrollment client component has been enhanced over that of earlier versions of Windows. Some of the functionality that was formerly accessed by using Web pages is now included in the client component. Therefore, this functionality has been removed from the updated certificate enrollment Web pages. Functionality that has been removed includes the following: The Enroll on Behalf of operation. An enrollment agent uses this feature to enroll for a certificate on behalf of another user." See http://technet.microsoft.com/en-us/library/cc770802.aspx on how to enroll on behalf of another user in Windows 7 and higher.

65. SafeSign Identity Client supports virtualization type I (or native, bare-metal hypervisors), i.e. SafeSign Identity Client installed on servers/desktops which run for example on VMware ESX or Citrix XenDesktop or Oracle/Sun VM VirtualBox directly on bare-metal hypervisors. Virtualization Type II (or hosted hypervisors), such as VMware Workstation, is not supported.

66. As stated in the Certification Authority Web Enrollment Guidance, on http://technet.microsoft.com/en-us/library/hh831649.aspx, "in Windows 8, CA Web Enrollment pages will work only with Internet Explorer 10 for the desktop". This means that in the Windows 8 modern UI mode of Internet Explorer 10 and 11, enrollment is disabled. Therefore, when requesting a certificate from the Microsoft CA through Internet Explorer 10/11 web enrolment pages, you will get an error saying that "this Web Browser does not support the generation of certificate requests". This can be solved in Internet Explorer 10 by setting the Browser Mode to Internet Explorer 10 Compatibility view and in Internet Explorer 11 by adding the web site to the Compatibility View (https://support.microsoft.com/en-us/kb/3073944). Until now Internet Explorer 10 (and below) needed Microsoft Visual C++ 2005 SP1 Redistributable Package MFC Update_x64 to work correctly for Microsoft Certificate Enrolment. Internet Explorer version 11 (and up) needs Microsoft Visual Studio C++ version 2010 SP1_x64 to work correctly for Microsoft Certificate Enrolment.

67. Version 3 certificate templates cannot be requested via web enrollment using the "out of box" certificate web enrollment pages.

7 FAQ

1. **Certificates are registered even when they are expired**: The Certificate Expiration Warning will also be displayed when certificates are already expired. You can take this into account for the text in the dialog, for example: “One or more certificates are about to expire in the next 30 days or have already expired”. This is caused by the fact that the Certificate Expiration Warning is called for when a token is inserted and will check the status of certificates and display the certificates that will expire or are already expired on the date (days in advance) specified. Certificate registration is independent from this process: expired certificates will also be registered. This also applies to PKCS #12 / PFX files a user imports in the Microsoft Certificate Store: these can be imported as well, without a warning these are expired. This does not affect their use: expired certificates cannot be used (e.g. for web authentication). Note that from SafeSign Identity Client 3.0.45 onwards, the Microsoft Certificate Propagation service registers the certificates (not the SafeSign Store Provider).

2. **The SafeSign Identity Client Login dialog only displays the token name**: The SafeSign Identity Client Login dialog only displays the token name. It does not display the friendly name of the certificate, because (a) this information is not always available to SafeSign Identity Client and (b) a user logs in to the card, not to a particular key pair / certificate.

3. **Can a user change the registry and reset the number of PIN retries to any number he likes?** No, the amount of PIN retries is set during the initialisation of the token. It cannot be changed once the token has been initialised.

4. **When importing a Digital ID, the public key is not imported?** When a Digital ID is imported, the public key is not imported on the token. The reason for this is that (a) it saves space and (b) a public key can be extracted from the certificate that corresponds to the private key.

5. **The Token Utility displays “Unknown token”**: Please verify that you have inserted a token that is supported by SafeSign Identity Client (as listed in the Product Description). Also verify that you have a (Java) token with a test key-set. You may contact your administrator to verify if you have an as yet unrecognised version of a supported Java card. If the problem persists, first contact your local supplier, before contacting AET Support.

6. **The Token Utility displays a dialog “Unknown ATR”**: This dialog will appear for tokens of which the ATR is not registered correctly for use in Microsoft CryptoAPI applications, resulting in problems with e.g. smart card logon. Please contact first your local supplier for a solution (possibly a newer version of SafeSign Identity Client). You can also copy the ATR of the card to the clipboard and paste it in an e-mail message to safesignsupport@aeteurope.com, together with the type of card. This will enable us to provide you with the details on how to add this card to the registry and to incorporate it, so it will be recognised by default in future releases. This will only be done with the token is provided by either AET or an AET certified partner.

7. **Does SafeSign Identity Client support PIN caching?** No, SafeSign Identity Client does not support PIN caching, for obvious security reasons. No private information will ever leave the token. The fact that you may not have to enter your PIN every time in an application is not the result of PIN caching. The loading and unloading of the CSP is done by the (Microsoft) Operating System, which may mean that you have to enter your PIN only once or multiple times. Also, PKCS #11 and CSP applications may make PIN entry silent (i.e. suppress the PIN dialog), Single Sign-On applications may fill in the PIN for an application and an application may not close the connection with the token when it is removed. Note that this has nothing to do with PIN caching.

8. **Should I install the SafeSign IC Credential Provider?** The SafeSign IC Credential Provider is not installed by default. Use of the SafeSign IC Credential Provider has a number of significant benefits, described in the SafeSign Identity Client Product Description. It is recommended to install it when you are using a secure pin pad reader and/or want to use such features as PIN unlock and PIN change during logon. Note that it does not support Microsoft VPN.

9. **Can I have two smart card logon certificates on one token?** From Windows Vista onwards, Microsoft supports multiple logon certificates and containers on one token. When logging in to Windows Vista or higher with the Microsoft Credential Provider, each logon certificate on the token will get a separate credential tile. Note that the SafeSign Credential Provider does not support multiple certificates for logon. The certificate placed first on the token will be the logon certificate.

10. **When using a Class 2 / Class 3 secure pinpad smart card reader, why can't I use my reader's keypad when initialising a token?** The reason why this is not implemented is of a practical nature. CT-API does not have the concept of a PUK (SO-PIN) code; it has only the concept of a PIN code. As a result of this, it cannot be communicated to the end user which code an end user must enter during initialisation. It can be a PIN or a PUK code. A secure pinpad reader would in that case prompt the user to enter a code for about 6 times in total, without the ability to distinguish / indicate the PIN or PUK is requested.

11. **When trying to initialise a Java card, I get a dialog saying that my card may not be configured correctly for use with SafeSign Identity Client?** This (device) error may have different causes. It may be that the token memory is full, i.e. that there is not enough free space on the card. It may also be that the token already contains other applets. It may also have to do with the smart card reader you are using. Please contact your local supplier and/or AET Support for means to determine the cause and solution for this error.

12. **When logging out of a secured connection (https://) in Internet Explorer, I do not have to enter the PIN for my token when logging back on (without closing the browser)?** This is caused by the fact that the client application (Internet Explorer) does not close the connection (disconnect the session) the moment the token is removed. Internet Explorer will only close the connection the moment the application is closed. Internet Explorer should check if all prerequisites for the connection are still there (proper token inserted, correct PIN entered). However, Microsoft CryptoAPI is not “rich” enough in terms of functionality to detect whether there is a token in the reader or not (and thus, to disconnect if the token is removed). This is a functionality that cannot be implemented in the Microsoft CryptoAPI interface or the SafeSign Identity Client CryptoAPI implementation (CSP).

8 Tests Conducted

This release has been tested by A.E.T. Europe B.V. for different configurations, according to the product Description of SafeSign Identity Client Standard Version 3.0.112 for Windows.

9 Error Handling and Reporting

A.E.T. Europe B.V. provides online support for SafeSign Identity Client from Monday through Friday. Every time an error or bug is detected in a version of SafeSign Identity Client, this can be reported to the A.E.T. Europe B.V. SafeSign Support Team at safesignsupport@aeteurope.com.

Note that support depends on a (separate) maintenance and support agreement with either AET (directly); or with your supplier. In case you have obtained SafeSign Identity Client through your local supplier, please contact their office for support first.

Consider that errors may arise from both client applications and SafeSign Identity Client modules. Actually only the second ones will be taken into consideration.

Consider also that A.E.T. Europe B.V. can only take into account support requests for problems that have been experienced on a clean machine, i.e. a computer on which no other middleware or drivers for other tokens have been installed.

9.1 How to report an error

Before reporting an error, first consider the known issues and frequently asked questions for the release. In order to ensure a quick and accurate response to your support questions, please ensure that you provide us with a completed Support Request Form (available from our web site https://www.aeteurope.com/support/ or upon request from SafeSign Support), including a detailed description / scenario in which the error occurs.

9.1.1 Log files

A.E.T. Europe B.V. may provide logging utilities upon specific request and when an error is accepted as a possible SafeSign Identity Client error. Note that loggers are only provided when a detailed and clear scenario is presented.

10 Supported Operating Systems

SafeSign Identity Client Standard Version 3.0.112 for Windows has been tested to support the following Windows PC Operating Systems (both 32-bit and 64-bit):

SafeSign IC version:	3.0.101	3.0.112
XP Professional SP3	✓	
7 SP1	✓	✓
8.1	✓	✓
10		✓
Server 2003 R2 SP2	✓	
Server 2008 R2 SP1	✓	✓
2012 R2 Datacenter	✓	✓

Note that Microsoft ended support for Windows XP on April 8, 2014, meaning that there will be no more security updates or technical support for the Windows XP operating system. Support for Windows Server 2013 R2 ended on July 14, 2015.

Like every SafeSign Identity Client release, SafeSign Identity Client version 3.0.112 was tested on the Windows Operating Systems with the (latest) Service Pack and Updates available at that time. Though SafeSign Identity Client version 3.0.112 may work on older / other versions of these Operating Systems (e.g. Windows 2008 R2 without SP1), 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

Windows Server 2012 (R2) only runs on x64 processors, so you should install the 64-bit version of SafeSign Identity Client on Windows Server 2012 (R2).

Note

In Terminal Server configurations, where a user does not use his SafeSign Identity Client token with applications on the local client or does not use his token for Terminal Server logon, SafeSign Identity Client does not have to be installed on the local client, but on the Windows (Terminal) Server only.

This does not apply when Network Level Authentication (NLA) is configured.

Network Level Authentication is an authentication method that can be used to enhance RD Session Host server security by requiring that the user be authenticated to the RD Session Host server before a session is created. Network Level Authentication completes user authentication before you establish a remote desktop connection and the logon screen appears. This is a more secure authentication method that can help protect the remote computer from malicious users and malicious software. (from https://technet.microsoft.com/en-us/library/cc732713.aspx).

In that case, SafeSign Identity Client should be installed on the local client as well, so user authentication with the SafeSign Identity Client token can be done on the local client.

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.