Product Description

SafeSign Identity Client Standard
Version 3.0 for Windows 64-bit

A.E.T. Europe B.V.

IJsselburcht 3

NL - 6825 BS Arnhem

The Netherlands

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 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.

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).

Contact Information: A.E.T. Europe B.V.

IJsselburcht 3
NL-6825 BS
P.O. Box 5486
NL-6802 EL Arnhem
The Netherlands
Tel. +31-26-365 33 50
Tel. Support +31-26-365 35 43
Fax +31-26-365 33 51

info@aeteurope.nl / support@aeteurope.nl
http://www.aeteurope.com/

SafeSign Identity Client is a product developed by A.E.T. Europe B.V.

Document Information

Filename: **Product Description**
SafeSign Identity Client Standard

Document ID: **SafeSign-IC-Standard_3.0-x64_Windows_Product_Description**

Project Information: **SafeSign Identity Client Release Documentation**

Document revision history

Version	Date	Author	Changes
1.0	18-11-2009	Drs. C.M. van Houten	First edition for SafeSign Identity Client Standard Version 3.0-x64 for Windows (release 3.0.33-x64)
1.1	10-08-2012	Drs. C.M. van Houten	Edited for SafeSign Identity Client Standard Version 3.0-x64 for Windows (release 3.0.40-x64)
1.2	28-04-2012	Drs. C.M. van Houten	Edited for SafeSign Identity Client Standard Version 3.0-x64 for Windows (release 3.0.45-x64)
1.3	05-07-2012	Drs. C.M. van Houten	Edited for SafeSign Identity Client Standard Version 3.0-x64 for Windows (release 3.0.70-x64)
1.4	17-07-2012	Drs. C.M. van Houten	Edited for SafeSign Identity Client Standard Version 3.0-x64 for Windows (release 3.0.74-x64)
1.5	17-08-2012	Drs. C.M. van Houten	Edited for SafeSign Identity Client Standard Version 3.0-x64 for Windows (release 3.0.76-x64)

WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE

Table of contents

About the Product

SafeSign Identity Client 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 Identity Client 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 Identity Client PKI applet, enabling end-users to utilise any Java Card 2.1.1 / Java Card 2.2 and higher compliant card with the SafeSign Identity Client middleware.

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

SafeSign Identity Client 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 Identity Client comes in a standard version with an installer for x64 Editions of the following Windows Operating Systems (with the latest Service Packs)[1]:

Windows XP (Professional), Windows Vista, Windows 7, Windows Server 2003 and Windows Server 2008.

In principle, SafeSign Identity Client supports any PC/SC (including PC/SC 2.01) compliant smart card reader. However, to avoid power problems, smart card readers must be capable to provide at least a current of 60mA. PC/SC driver software is available from the web site of the smart card reader manufacturer.

Note that 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.

[1] Windows NT 4.0 is supported up to SafeSign Identity Client 1.0.9.04, in line with Microsoft's end-of-life policy.
Windows 98 and Windows ME are supported up to SafeSign Identity Client 2.3.0 (< 2.3.0), in line with Microsoft's end-of-life policy.
Windows 2000 is supported up to SafeSign Identity Client 3.0.33 (≤ 3.0.33), in line with Microsoft's end-of-life policy.

About the Document

This product description defines the features of SafeSign Identity Client Standard and the supported configurations that were tested by its developer A.E.T. Europe B.V.

Note that the phrase "Windows Vista and higher" in this document means that the changes, features etc. described are included in Windows Vista, Windows 7 and Windows Server 2008.

1 Introduction

SafeSign Identity Client is a software package to enhance the security of applications that support PKCS #11 and Microsoft CryptoAPI (NG) by hardware tokens, i.e. smart cards, USB tokens or SIM cards.

The SafeSign Identity Client package provides the SafeSign Identity Client PKCS #11 Library and Cryptographic Service Provider / Key Storage Provider, which allow the user to generate and store public and private data on a personal token.

2 SafeSign Identity Client Functionality

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

Cryptographic Service Provider (CSP) for integration in applications supporting Microsoft CryptoAPI, including Microsoft Internet Explorer and Outlook.
Key Storage Provider (KSP) for integration in applications and Operating Systems supporting Cryptography API: Next Generation (CNG).
PKCS #11 for integration with applications supporting PKCS #11, including Mozilla Firefox.
PKCS #12 support.
PKCS #15 support.
PKCS #8 support (secure key wrap / unwrap).
Windows XP, Windows Vista, Windows 7, Windows Server 2003 and Windows Server 2008 logon support; Windows Server 2003 / Windows Server 2008 Terminal Server and Citrix logon support.
PC/SC v2.01 support.
End user and administrator documentation. All documentation is in the English language.
Installation procedure for SafeSign Identity Client components (including PKCS #11, CSP, Token Utilities).
SafeSign Identity Client GINA (Windows XP) and Credential Provider (Windows Vista and higher) to facilitate logon with protected authentication path readers (such as secure pinpad Class 2 and 3 readers).
Token Utilities for such operations as: token initialisation, token visualisation, import of Digital IDs (including certificate chains), change PIN/PUK and unlock PIN.

3 Features

The following (new) features are supported by SafeSign Identity Client Standard Version 3.0-x64 for Windows:

- Multiple token support;
- Multiple language support;
- Multiple OS support;
- Support for PIN timeout;
- Support for PC/SC 2.0 secure pinpad readers;
- Support for EFS;
- Support for maximum PUK and PIN length;
- Support for virtual readers in PKCS#11 (≥ 3.0.40);
- SafeSign IC Credential Provider (≥ 3.0.40);
- Support for SHA-2 (≥ 3.0.40);
- Support for AES (≥ 3.0.40);
- Support for Microsoft Certificate Propagation (≥ 3.0.45);
- Support for Cryptography API: Next Generation (CNG) Key Storage Provider (≥ 3.0.70);
- Support for Event Logging (≥ 3.0.70).

3.1 Multiple Token Support

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

SafeSign Identity Client Standard Version 3.0-x64 for Windows supports a number of different tokens, listed below with the SafeSign Identity Client version 64-bit version first supporting them.

Details of tokens are listed in Chapter 7.

3.1.1 Version 3.0.33-x64

- Athena IDProtect
- Athena IDProtect Duo
- NXP JCOP21 v2.3.1
- NXP JCOP31 v2.3.1
- NXP JCOP41 v2.3.1
- RSA SecurID Token[1]
- RSA Smart Card 5200[2]
- Sagem Orga J-IDMark 64
- Siemens CardOS 4.3B 32K/64K
- IDpendant IDp 1000
- Giesecke & Devrient Sm@rtCafé 4.0
- Oberthur IDOne Cosmo v7.0
- Gemalto GemXpresso R4 / TOP IM GX4
- Sagem Orga J-IDMark 64 Dual

[1] Read-only implementation.
[2] Read-only implementation.

3.1.2 Version 3.0.40-x64

- Gemalto GemXpresso R4 / TOP IM GX4 MSA081
- Gemalto USB eSeal Token V2 TOP IM GX4
- Giesecke & Devrient STARCOS 3.0 DI
- Giesecke & Devrient STARCOS 3.2[1]
- Giesecke & Devrient STARCOS 3.4
- Giesecke & Devrient Sm@rtCafé 3.2
- Giesecke & Devrient Sm@rtCafé Expert 5.0
- Giesecke & Devrient Mobile Security Card SE 1.0
- NXP JCOP21 v2.4.1 / J2A080
- NXP JCOP31 v2.4.1 / J3A080
- Sagem Orga YpsID s2

3.1.3 Version 3.0.45-x64

- Athena IDProtect v3
- Athena IDProtect Key v2
- Gemalto TOP DL v2
- Giesecke & Devrient Sm@rtCafé 6.0
- Giesecke & Devrient Crypto USB Token
- Giesecke & Devrient Convego Join 4.01 40k/80k
- Sagem Orga YpsID s3
- Sagem Orga YpsID Key E-M
- Sagem Orga YpsID Key E2C
- Siemens CardOS 4.4
- Quovadis SuisseID (CardOS 4.3B)
- SwissSign SuisseID (CardOS 4.3B)[2]
- FMH / Swisscom Swiss Health Professional Card (CardOS 4.3B)
- Swisspost Schweizerische Krankenversicherungskarte KVG (STARCOS 3.4)

3.1.4 Version 3.0.70-x64

- Athena IDProtect v6
- Defensiepas
- Gemalto MultiApp ID v2.1
- Gemalto Optelio D72 FR1
- NXP JCOP21 v2.4.1 / J2A081
- Sasis Patient Data Card / Krankenversicherungskarte KVG
- SECCOS 5.0 and SECCOS 6.2
- Vasco DIGIPASS Key 101
- Vasco DIGIPASS Key 200
- Vasco DIGIPASS Key 202
- Vasco DIGIPASS Key 860

[1] For more information and details on the support of STARCOS 3.2 and STARCOS 3.4, please contact AET.
[2] Authentication certificate only.

3.2 Multiple language support

SafeSign Identity Client Standard Version 3.0-x64 for Windows supports a number of different languages.

Newly supported languages in SafeSign Identity Client Standard Version 3.0-x64 for Windows are:

- Korean language;
- Serbian language, Cyrillic and Latin (≥ 3.0.33-x64)[1];
- Ukrainian language (≥ 3.0.70-x64).

3.3 Multiple OS Support

SafeSign Identity Client Version 3.0-x64 supports a number of Windows Operating Systems, as listed below.

3.3.1 Version 3.0.33-x64

- Support for Windows XP x64 Edition
- Support for Windows Vista x64 Edition
- Support for Windows 7
- Support for Windows Server 2008

3.3.2 Version 3.0.40-x64

- Support for Windows Server 2008 SP2
- Support for Windows Server 2008 R2

3.3.3 Version 3.0.70-x64

- Support Windows 7 SP1
- Support for Windows 2008 R2 SP1

3.4 Support for PIN timeout

From SafeSign Identity Client Version 3.0.33-x64 (≥ 3.0.33-x64) onwards, it is possible to set a PIN timeout, for both PKCS #11 and CSP applications, for Java Card v2.2+ cards.

By default, the PIN timeout is disabled. When the PIN timeout is enabled, you will be asked to (re-)login to the token, i.e. the SafeSign PIN dialog will be displayed.

In practice, this means that for example when using Outlook to send signed e-mail messages or using Adobe Reader to sign a document, you will be asked to enter your PIN again when the maximum amount of time has passed since the last time you logged in to the token.

The timeout value for a particular token can be set in the Token Administration Utility[2], through the menu Token > Change PIN Timeout, if the (initialised) token is inserted and the correct PIN is entered.

1 SafeSign IC support both Serbian (Cyrillic) and Serbian (Latin). However, InstallShield (≤ 2010) does not support Serbian (Latin), therefore, during installation, it is only possible to select Serbian (Cyrillic) as the language of the installation wizard.
2 The Token Management Utility does not include this option.

By default, the PIN Timeout is disabled. When enabled (by deselecting "Pin Timeout disabled", as in the dialog below), you can set the timeout value:

Figure 1: Change Timeout

Note that the PIN Timeout cannot be set to 0 (zero) seconds, as this will expire the PIN immediately when it is entered and the credentials on the token cannot be used. Therefore, from SafeSign Identity Client 3.0.33-x64 onwards (≥ 3.0.33-x64), the minimum PIN Timeout value is set to 20 seconds.

There is an issue when setting the PIN Timeout, which is that its value is not displayed in the Token Utility's *Show Token Info* dialog. When it is not set, this dialog will display "No". When it is set, nothing (no value) will be displayed. This will be fixed in a next release.

Note that the PIN Timeout feature does not work with secure pinpad readers, i.e. it cannot be set and does not work within applications.

3.5 Support for PC/SC 2.0 secure pinpad readers

From SafeSign Identity Client Version 3.0.33-x64 onwards (≥ 3.0.33-x64), only secure pinpad readers supporting PC/SC 2.0 Part 10 are supported.

Note that this means that all (Class 2 and 3) secure pinpad readers previously supported are or may not be supported anymore.

The table below gives an overview of the readers that were supported in the previous SafeSign versions and states whether they are (still) supported in the new release:

Reader	**Supported in < 3.0.33**	**Supported in ≥ 3.0.33**
Cherry SmartBoard XX44	Yes	Yes
Omnikey CardMan 3610 Trust, serial	Yes	No
Omnikey CardMan 3620 Trust, USB	Yes	No
Omnikey CardMan 3621 Trust, USB	Yes	Yes
Omnikey CardMan 3821 Trust, USB	Yes	Yes

The PC/SC 2.0 readers supported in SafeSign Identity Client Version 3.0.33-x64 (and onwards) are:

- Cherry SmartBoard XX44;
- Cherry SmartTerminal ST-20000U (ST-20000UCZ / ST20000UC-R);
- OMNIKEY 3821 USB pinpad;
- Reiner SCT cyber*Jack* pinpad;
- Reiner SCT cyber*Jack* e-com;
- Reiner SCT cyber*Jack* secoder;
- SCM Microsystems SPR532 PINpad Reader[1];
- Todos eCode Connectable 217U.

[1] When upgraded to the latest firmware and drivers.

3.6 Support for EFS

SafeSign Identity Client support Microsoft Encrypting File System. The sections below describe the specific interaction of the respective SafeSign Identity Client versions with EFS.

For more information on the requirements and operation of EFS, refer to the Microsoft web site.

Note that on Vista and higher, EFS requires that the key that is specified for the certificate's private key has the AT_KEYEXCHANGE flag.

Note that generating a self-signed certificate for EFS with SafeSign Identity Client fails.

3.6.1 Version 3.0.33-x64

Support for EFS was first implemented in SafeSign Identity Client Version 3.0.33-x64, on Windows Vista, Windows 7 and Windows Server 2008[1].

In order to be able to use a certificate on a token with EFS, you need to copy the certificate to the Windows registry store. To do this, you have to add (through the registry[2]) a button in the *Show Registered Digital IDs* dialog that will add the certificate selected to the registry store. This button is called "Copy Cert. to System Store". This gives you the flexibility to use your (existing) Smart Card User certificates for EFS.

3.6.2 Version 3.0.40-x64

In SafeSign Identity Client Version 3.0.40-x64, you will need to use the same procedure to add the certificate for EFS to the registry store. However, because the SafeSign Credential Provider, which is installed by default, does not support SSO, you will not be able to select the certificate. In order to do so, you will need to have the Microsoft Credential Provider installed[3].

3.6.3 Version 3.0.45-x64

In SafeSign Identity Client Version 3.0.45-x64, the SafeSign Credential Provider is installed by default as well, so in order to be able to select a certificate, you will need to install the Microsoft Credential Provider.

However, with SafeSign Identity Client Version 3.0.45-x64 (and higher versions), there is no need to add the abovementioned button and register / copy the certificate you want to use for EFS in the registry store, as this is done by default by the Microsoft Certificate Propagation service. See section 3.0.14 for more details.

Nevertheless, there is an issue in SafeSign Identity Client Version 3.0.45-x64 with EFS, as upon selecting the certificate and entering the PIN for the token (using the Microsoft Credential Provider), you will get an error: "Provider could not perform the action since the context was acquired as silent".

3.6.4 Version 3.0.70-x64

In SafeSign Identity Client Version 3.0.70-x64 and higher (≥ 3.0.70-x64), as in SafeSign Identity Version 3.0.45-x64, the Microsoft Certificate Propagation Service will take care of registering the certificate. As the SafeSign Credential Provider is not installed by default, you will be able to select the certificate and open the encrypted file / directory.

Nevertheless, there is an issue in SafeSign Identity Client Version 3.0.70-x64 with EFS, as upon selecting the certificate and entering the PIN for the token (using the Microsoft Credential Provider), you will get an error: "Provider could not perform the action since the context was acquired as silent".

---

[1] Note that SafeSign does not support EFS in Windows 2000 or Windows XP, as it is only in Windows Server 2008 and Windows Vista / windows 7 that EFS supports the storage of users' private keys on smart cards.

[2] The button will appear when adding the action "CopyIDToSystemAction" in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\A.E.T. Europe B.V.\SafeSign\2.0\Actions

[3] You can de-install the SafeSign Credential Provider through the original SafeSign Identity Client installer. This will allow you to modify an existing installation and deselect the SafeSign Credential Provider. By doing so, the Microsoft Credential Provider will be restored again.

3.7 Support for maximum PUK and PIN length

From SafeSign Identity Client Version 3.0.33-x64 onwards, a maximum PUK and PIN length is supported.

The registry keys for the different profiles supported now contain the values for maximum PUK length and maximum PIN length, which can be edited.

Note that when setting these values to a specific length, you should keep both values the same, i.e. you cannot set a different value for the maximum PUK length than for the maximum PIN length.

From SafeSign Identity Client Version 3.0.70-x64 onwards (≥ 3.0.70-x64), it is possible to use different values for the maximum PIN length and maximum PUK length, for the Java Card v2.2+ cards supported.

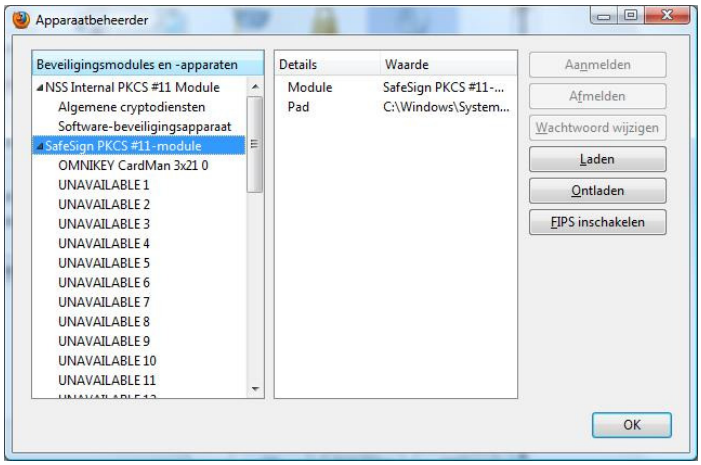
3.8 Support for virtual readers in PKCS #11

In SafeSign Identity Client Version 3.0.40-x64 (≥ 3.0.40-x64) a new concept is introduced in our PKCS #11 library, called "Virtual Readers".

In accordance with the PKCS #11 standard, the insertion and removal of smart card readers (devices) / slots is not detected once the PKCS #11 Library is loaded[1]. In practice, this means that when a user has started a PKCS #11 application such as Firefox, adding (or removing) a reader or USB token will not be detected. If a user then tries to use the token for authentication to a web site, this will fail.

This has been solved by implementing virtual reader slots. The PKCS #11 Library will now not only provide a list of (physical) readers attached to the system, but it will also provide a list of virtual reader slots (which can be filled with additional readers when they become present on the system). When a user then plugs in a new reader or USB token, the virtual reader will be replaced by the actual reader plugged in.

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



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

3.9 SafeSign IC Credential Provider

In Windows Vista and higher, the Microsoft GINA (msgina.dll) has been removed, and custom GINAs will not be loaded on systems running Windows Vista and later versions. Instead, the Winlogon behaviour can be customized by implementing and registering a custom Credential Provider.

3.9.1 Features

The SafeSign Credential provider is a smart card credential provider, interacting with the SafeSign IC components.

The SafeSign Credential Provider will only display one tile for each token / user credential. When the SafeSign Credential provider is installed, the Microsoft Credential Provider will be deregistered, to ensure that users can benefit from all the features of the SafeSign IC Credential provider.

The SafeSign Credential provider includes the following features:

- Support of secure pinpad readers;
- Display tiles for workstation smart card logon;
- Display tiles for remote smart card logon (through RDP);
- Display tiles to allow the user to change the PIN of his token;
- Display tiles to allow the user to unlock the token's PIN through the PUK;
- Display tiles to allow the user to unlock the token's PIN through challenge-response;
- Display tiles to allow the user to change the Transport PIN of a token;
- Display smart card credentials on UAC elevation;
- Display tiles for unlocking a workstation;
- Display a meaningful message when the token is not initialized or does not contain a valid certificate.

3.9.2 Limitations

The current SafeSign Credential Provider does not support multiple certificates on one token. When you have more than one (smartcard logon) certificate on a token, it is recommended not to install the SafeSign Credential Provider, but to use the Microsoft Credential Provider instead.

Also, the SafeSign Credential Provider will assign the first certificate (loaded) on the card as the certificate for logon. When there are multiple certificates on the card (such as CA certificates and personal certificates), the first certificate should be the smart card logon certificate, if the card is to be used for smart card logon. This means that if the first certificate(s) loaded on the card is a CA certificate, this certificate will be selected during logon (making logon impossible). Note that in SafeSign Identity Client Version 3.0-x64.40, the CA certificate was displayed at logon (as if it was possible to use it), whereas in SafeSign Identity Client Version 3.0-x64.45 and higher, the certificate will not be displayed and the message that no valid credentials for logon were found is displayed.

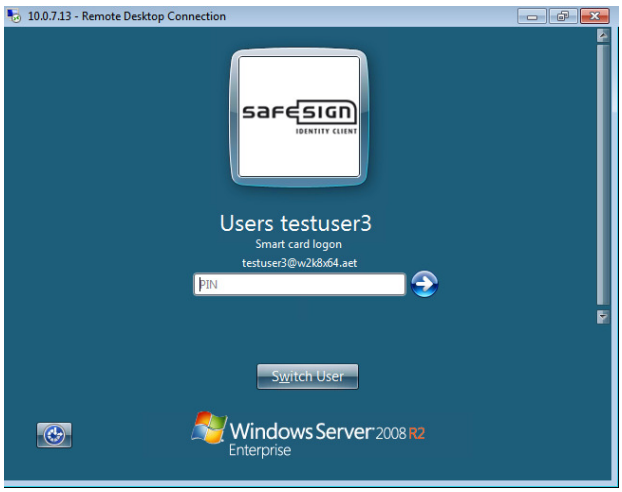
Also, if the features of the Credential Provider are not required, it is recommended not to install the Credential Provider on the Windows Server 2008 (R2). If you do install it, you will be asked to authenticate twice: once on the local desktop, once on the remote desktop.

Note that the SafeSign Credential Provider does not support PLAP / Single Sign-On[1]. This means that when setting up a (Microsoft) VPN connection, the SafeSign Credential Provider will not be available. Also, when setting up a remote desktop connection to a Terminal Server and entering your credentials locally, you will be asked for your credentials again upon connecting.

[1] Single Sign-On (SSO) API represents a set of methods used to obtain EAP method specific credentials for a network user or computer account in a secure fashion without having to raise multiple UI instances.

3.9.3 Version 3.0.40-x64, 3.0.45-x64

From SafeSign Identity Client Version 3.0.40-x64 onwards (≥ 3.0.40-x64), the functionality provided by the SafeSign GINA (on Windows XP) is now provided by the SafeSign IC Credential Provider for Windows Vista and higher:



In SafeSign Identity Client Version 3.0.40-x64 and 3.0.45-x64, the SafeSign Credential Provider is installed by default.

3.9.4 Version 3.0-x64.70

In view of the fact that the SafeSign Credential Provider does not support multiple certificates on a token and that it is also installed on standalone machines (not connected to a domain or where smart card logon is not used), the SafeSign Credential Provider will not be installed by default in SafeSign Identity Client Version 3.0.70-x64 (≥ 3.0.70-x64). This means that in SafeSign Identity Client Version 3.0-x64.70, the Microsoft Credential Provider will be used.

For those users who would like to use the features of the SafeSign Credential Provider (as listed in paragraph 3.9.1), for example because they are using a secure pinpad reader or want to offer their users the ability to change their PIN during logon, the SafeSign Identity Client version that was used to install SafeSign Identity Client can be run again to modify the existing installation, upon which the SafeSign Credential Provider can be selected.

3.10 Support for SHA-2

In SafeSign Identity Client Version 3.0.40-x64 (≥ 3.0.40-x64) support for SHA-2 has been implemented, with the following variants: SHA-256, SHA-348 and SHA-512.

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

3.11 Support for AES

In SafeSign Identity Client Version 3.0.40-x64 (≥ 3.0.40-x64), support for AES encryption / decryption has been implemented. SafeSign Identity Client now offers both a type 1 CSP (PROV_RSA_FULL) and a type 24 CSP (PROV_RSA_AES), supporting AES-128, AES-192 and AES-256.

See also:

http://msdn.microsoft.com/en-us/library/aa387447(VS.85).aspx

3.12 Certificate Propagation

In SafeSign Identity Client versions up to 3.0.45-x64 (< 3.0.45-x64), certificate registration and de-registration was performed by the SafeSign Store Provider (aetsprov.dll). However, as a result of changed functionality in Windows Vista and higher, changes have been made to the way certificates are registered / propagated. Certificates are now registered by the appropriate Microsoft services and processes, i.e. through the Microsoft Certificate Propagation service[1], starting with SafeSign Identity Client Version 3.0.45-x64.

The Certificate Propagation (Service) applies when a logged-in user inserts a smart card in a reader that is attached to the computer. This action causes the certificate(s) to be read from the smart card. The certificates are then added to the user's Personal store. The service action is controlled by using Group Policy. For more information on the Microsoft Certificate Propagation Service and the relevant policy settings, refer to http://technet.microsoft.com/en-us/library/ff404288(WS.10).aspx.

For that reason, from SafeSign Identity Client Version 3.0.45-x64 onwards, the SafeSign Store Provider (aetsprov.dll) has been removed, leaving it up to the Microsoft Certificate Propagation Service to register the certificates.

The SafeSign Store Provider did not only register certificates, but also deregistered them when the token was removed. As the SafeSign Store Provider is removed / no longer available, the deregistration feature provided by the SafeSign Store Provider in previous versions does not exist anymore. The Microsoft Certificate Propagation Service does not deregister certificates upon token removal, therefore when the token is removed, the certificates will remain visible in the certificate store (though they will not be usable without key pair) [2].

There is no custom method implemented for deregistering certificates as there is no Microsoft approved way of doing so. Any method adding this functionality is considered proprietary and may cause problems in the Operating Systems involved (which rely on the availability of certificates) and with obtaining support from Microsoft.

3.13 Support for CNG Key Storage Provider

From SafeSign Identity Client Version 3.0.70-x64 onwards, SafeSign includes the SafeSign Key Storage Provider.

Starting from Windows Vista / Windows Server 2008, Microsoft introduced a new version of the Cryptographic API (CryptoAPI), so called Cryptography API: Next Generation (CNG). Unlike CryptoAPI, CNG separates Cryptographic Service Providers from Key Storage Providers (KSPs).

Before, a Cryptographic Service Provider was required to support non-smart card specific operations (such as padding and hashing), but with the CNG, the key provider only needs to support operations related to keys and cannot be run without a smartcard.

It is up to the Operating System to decide when and which interface (CryptoAPI or CryptoAPI NG) to call.

For more information on Cryptography API: Next Generation, see: http://msdn.microsoft.com/en-us/library/windows/desktop/aa376210(v=vs.85).aspx.

[1] In Windows XP, the Windows Smart Card Service takes care of certificate registration as part of winlogon.exe.
[2] Thus it may happen that on secure web authentication with Internet Explorer, you are able to select the certificate, but you will not be asked for the PIN and get an immediate error: "Internet Explorer cannot display the web page".

3.14 Support for Event Logging

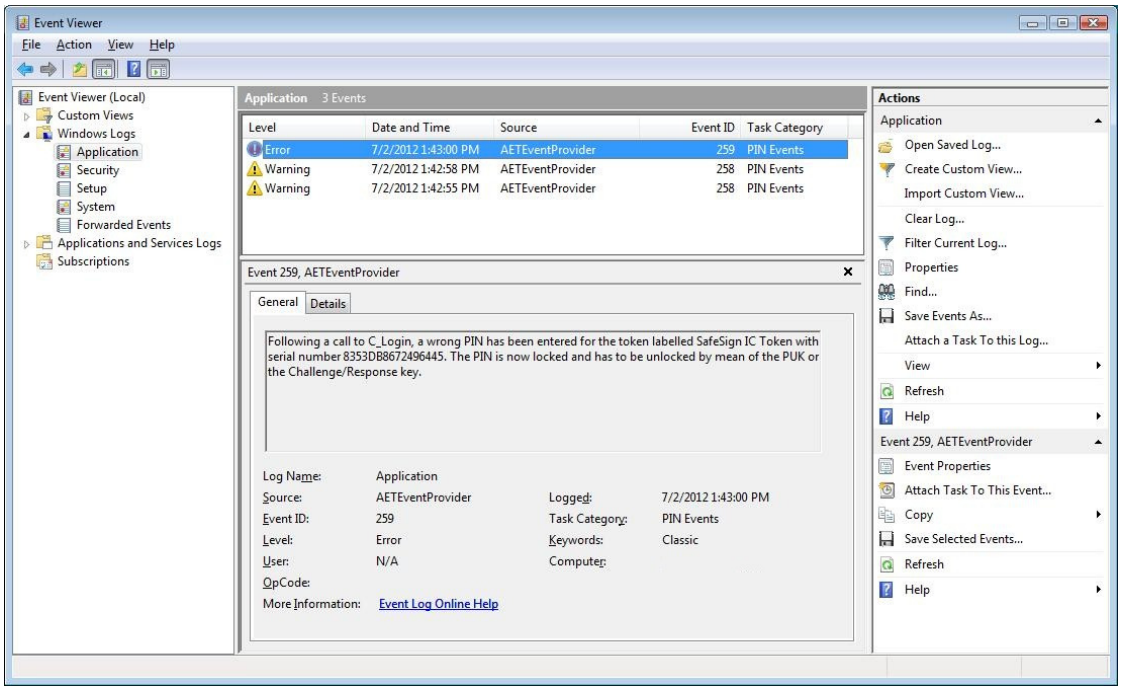
From SafeSign Identity Client Version 3.0.70-x64 onwards, SafeSign Identity Client supports the generation of Application Event logs.

When enabled in the registry[1], the following events will be logged:

- PIN changes;
- Wrong PIN entered;
- PIN expired;
- PIN blocked.

These events will be logged whether done during smart card logon, use of the Token Utility or within applications.

Here is an example of what the Event Viewer will look like when the PIN is locked:



[1] By changing the DWORD value "GenerateEventLogs" in [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\A.E.T. Europe B.V.\SafeSign\2.0\] on 64-bit and [HKEY_LOCAL_MACHINE\SOFTWARE\A.E.T. Europe B.V.\SafeSign\2.0\] in 32-bit to a value of "1".

4 End User Documentation

SafeSign Identity Client Standard Version 3.0-x64 for Windows provides at least the following end-user documentation:

Document name	Document Version
SafeSign Identity Client Standard 3.0-x64 Release Notes for Windows	1.6
SafeSign Identity Client Standard 3.0-x64 Product Description	1.5
SafeSign Identity Client Standard x64 User Guide for Installation	1.2
SafeSign Identity Client Standard User Guide for Token Management Utility	3.2
SafeSign Identity Client Standard User Guide for Token Administration Utility	3.2
SafeSign Identity Client User Guide for Microsoft and Outlook 2000	2.1
SafeSign Identity Client User Guide for Microsoft and Outlook XP	2.1
SafeSign Identity Client User Guide for Microsoft and Outlook Express	2.1
SafeSign Identity Client User Guide for Microsoft VPN in Windows 2000	2.1
SafeSign Identity Client User Guide for Microsoft VPN in Windows XP	2.1
SafeSign Identity Client User Guide for Microsoft Windows 2000	2.1
SafeSign Identity Client User Guide for Microsoft Windows 2003	2.1
SafeSign Identity Client User Guide for Microsoft Windows 2003 Terminal Services	2.1
SafeSign Identity Client User Guide for Citrix Presentation Server 4.5	1.0
SafeSign Identity Client Administrator's Guide	3.3
SafeSign Identity Client User Guide for Authentication	2.1

Note that the (2.1) User Guides mentioned above were written for SafeSign-IC versions 2.3.x.

5 Supported and Tested PC Operating Systems

SafeSign Identity Client Standard Version 3.0-x64, release 3.0.76-x64, for Windows has been tested to support the following PC Operating Systems:

Operating System	Version
Windows	Windows XP Professional x64 Edition SP2
	Windows Vista Professional / Ultimate x64 Edition SP2
	Windows 7 Professional / Ultimate x64 Edition SP1
	Windows Server 2003 Enterprise x64 Edition SP2
	Windows Server 2008 Enterprise x64 Edition SP2
	Windows Server 2008 Enterprise R2 SP1

6 Supported and Tested Smart Card Readers

In principle, SafeSign Identity Client 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 Identity Client.

The following table lists the readers and reader drivers that were tested and qualified for use with SafeSign Identity Client Version 3.0.76-x64. This list is not complete, in the sense that there can be other readers and reader drivers that are also interoperable with SafeSign Identity Client.

For such a list, refer to Appendix 1, which lists the readers that have been tested to work at a certain time as part of the release testing for SafeSign Identity Client versions 3.0.x. The list does not imply that each smart card reader and reader driver listed works with each SafeSign Identity Client supported smart card. Though it is beyond the scope of AET / SafeSign Identity Client to provide an all-inclusive list of smart card and reader combinations supported, AET Support can assist customers in selecting the proper card – reader combination.

If you have problems with your (listed) smart card reader, please contact AET Support.

The following table lists the specific readers that have been tested with SafeSign Identity Client Version 3.0.76-x64:

Smart Card Reader Manufacturer and Model	Class	Driver Version
HID OMNIKEY 3121 USB Desktop Reader	1	V1.2.6.5_x64
HID OMNIKEY 1021 USB Desktop Reader	1	V1.2.6.5_x64

7 Supported and Tested Hardware Tokens

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

These tokens have been tested to work at a certain time as part of the release testing for SafeSign Identity Client versions 3.0.x. The list does not imply that each token (still) works or will be supported in any or all versions of SafeSign Identity Client Version 3.0-x64.

If you have problems with your (listed) token, please contact AET Support.

7.1 STARCOS Cards

A token with STARCOS (SPK) operating system must be *completed*, before it can be used with SafeSign Identity Client. This completion includes parts of the smart card operating system STARCOS, which are written into the EEPROM of the smart card by G&D. Completed tokens do not contain any files, keys, certificates, PIN, PUK or token label.

Completed tokens are completed with a 'series' (or 'test') completion indicated by an 'S' (respectively 'T') in the STARCOS completion file name. Test completed tokens allow deletion of the SafeSign Identity Client application and re-completion and should only be used for evaluation purposes. Export versions ('E' instead of 'I' in the completion name) are *not* supported. For STARCOS SPK2.5 DI there is only one completion that allows secure deletion of file system.

Token	Type	Tested Completion Versions
G&D STARCOS SPK 2.3 v7.0	Smart Card	Test completion: CP5WxSPKI23-1-7-T_V0700 Series completion: CP5WxSPKI23-1-7-S_V0700
G&D STARCOS RawRSA SPK 2.3 v7.0	Smart Card	Test completion: CP5WxSPKI23-1-D-T_V0700 Series completion: CP5WxSPKI23-1-D-S_V0700
G&D STARCOS SPK 2.4 v3.0	Smart Card	Test completion: CP5WxSPKI24-01-0-T_V0300 Series completion: CP5WxSPKI24-01-0-S_V0300
G&D STARCOS FIPS SPK 2.4 v3.3	Smart Card	Test completion: CP5WxSPKI24-01-3-T_V0330 Series completion: CP5WxSPKI24-01-3-S_V0330
G&D STARCOS SPK 2.5 DI v1.0	Smart Card	Series completion: CP7G1SPKI25DI-1C-0-S_V0100
G&D StarKey100 / StarKey200 with G&D STARCOS SPK 2.3 or 2.4 chip	USB Token	Test completion: CP5WxSPKI23-1-7-T_V0700 Series completion: CP5WxSPKI23-1-7-S_V0700 Test completion: CP5WxSPKI24-01-0-T_V0300 Series completion: CP5WxSPKI24-01-0-S_V0300
G&D StarKey220 HID with G&D STARCOS SPK 2.3 v7.0	USB Token	Test completion: CP5WxSPKI23-1-7-T_V0700
G&D STARCOS 3.0 (Standard Version)	Smart Card	Series completion: CPAZ0SCSI30-01A-0V300
G&D StarKey 350 USB Card Token with STARCOS 3.1.2	Smart Card	-
G&D STARCOS 3.2[1]	Smart Card	-
G&D STARCOS 3.4	Smart Card	-

[1] For more information and details on the support of STARCOS 3.2 and STARCOS 3.4, please contact AET.

7.2 Java Cards

The SafeSign Identity Client PKI applet enables end-users to utilise any Java Card 2.1.1 / 2.2+ compliant card with the SafeSign Identity Client middleware. A Java Card token must contain an installed SafeSign Identity Client applet before it can be used with SafeSign Identity Client.

In the special case that a blank token (that does not yet contain a SafeSign Identity Client applet) is used with standard test keys for applet loading, the built-in applet loader of SafeSign Identity Client can be used to load and install the SafeSign Identity Client applet[1]. This universal Java Card applet loader included in SafeSign Identity Client can load the SafeSign Identity Client PKI applet out-of-the-box onto a variety of Java Cards equipped with a test key set (this includes most sample cards that can be purchased from Java Card vendors). For deployment / production, you should use cards with a production key set that have the applet pre-installed.

Note

As the correct functioning of SafeSign Identity Client is depending on a properly produced smart card or USB Token, AET would like to emphasize that smart cards and / or USB tokens being produced for use with SafeSign Identity Client by vendors that are not approved AET production sites and not in accordance with our QA policies (which require i.a. the applet to be pre-installed in a secure environment and a custom keyset) are not eligible for any support by AET in case of problems, even if the user has purchased a SafeSign Identity Client Maintenance and Support Agreement.

7.2.1 Java Card 2.1.1

There are three default profiles of SafeSign Identity Client applets available with different sizes for Java Card 2.1.1 tokens:

SafeSign Identity Client Applet	Max. number of RSA keys (PKCS#15)	Available private space in bytes (PKCS#15)	Available public space in bytes (PKCS#15)	Approx. Number of certificates that can be stored
Minimal	1	1	3328	1
Default	3	1	4454	6
Maximal	*	*	*	12

The minimum and default (medium) applet is the same for all supported Java cards, whereas the maximal profile differs per card (hence the *).

The minimum sized SafeSign Identity Client applet can only be used for Windows smart card logon or for SSL client authentication and secure email.

[1] Note that the SafeSign Java PKI applet that is loaded in this case, may not be the latest one, nor include all functionality listed in this Product Description.

Token	Type	Additional remarks
Aspects OS755 v2.8	Smart Card	Java Card v2.1.1
Atmel ATOP36	Smart Card	Java Card v2.1.1
Axalto e-Gate	Smart Card	Java Card v2.1.1
Axalto Cyberflex Developer	Smart Card	Java Card v2.1.1
Axalto Cyberflex 64Kv1	Smart Card	Java Card v2.1.1
Axalto Cyberflex 64Kv2	Smart Card	Java Card v2.1.1
Axalto Cyberflex 64kv3	Smart Card	Java Card v2.1.1
Axalto Cyberflex Palmera	Smart Card	Java Card v2.1.1
G&D Sm@rtCafé Expert v2.0	Smart Card	Java Card v2.1.1
G&D STARSIM Java	Smart Card	Java Card v2.1.1
Gemalto GemXpresso 211PK	Smart Card	Java Card v2.1.1
Gemalto GemXpresso Pro R3 (16K, 32K and 64K)	Smart Card	Java Card v2.1.1
Gemplus GemXplore 3G (Gem10.64 GX3GV22 128K-PK)	Smart Card	Java Card v2.1.1
IBM JCOP 20	Smart Card	Java Card v2.1.1
IBM JCOP 21id	Smart Card	Java Card v2.1.1
IBM JCOP 30	Smart Card	Java Card v2.1.1
IBM JCOP 31bio	Smart Card	Java Card v2.1.1
MartSoft Java card	Smart Card	Java Card v2.1.1
ORGA JCOP 20	Smart Card	Java Card v2.1.1
ORGA JCOP 30	Smart Card	Java Card v2.1.1
ORGA JCOP21	Smart Card	Java Card v2.1.1
Renesas X-Mobile Card	SD Card	Java Card v2.1.1
Sagem Orga J-ID Mark 64	Smart Card	Java Card v2.1.1
Oberthur CosmopolIC v4	Smart Card	Java Card v2.1.1
Sagem Orga ysID S2	Smart Card	Java Card v2.1.2

7.2.2 Java Card 2.2.x

For the Java Card 2.2 (and higher) supported cards, the default profile is the only profile available, as the applet supports dynamic use of memory.

Token	Type	Additional remarks
Aspects OS755 Java Card 2.2.1	Smart Card	Java Card v2.2
Athena IDProtect	Smart Card	Java Card v2.2
Athena IDProtect Duo	Smart Card	Java Card v2.2
Athena IDProtect v3	Smart Card	Java Card v2.2.2
Athena IDProtect v6	Smart Card	Java Card v2.2.2
Athena IDProtect Key v2	USB Token	Java Card v2.2.2

G&D Sm@rtCafé Expert 64K	Smart Card	Java Card v2.2.1 Config1 (FIPS with 2048 bit, level 3): CH463JC_INABFOP003901_V101 (FIPS) Config2 (FIPS with 1024 bit, level 3) Config3 (non-FIPS): CH463JC_INABFOP003901_V103 (non-FIPS) Config10 (FIPS with 2048 bit, level 2): CH463JC_INABFOP003901_V101 (FIPS)
G&D StarKey400 (M) with Sm@rtCafé Expert 64K	USB Token	Java Card v2.2.1 Config1 (FIPS with 2048 bit, level 3): CH463JC_INABFOP003901_V101 (FIPS) Config2 (FIPS with 1024 bit, level 3) Config3 (non-FIPS): CH463JC_INABFOP003901_V103 (non-FIPS)
G&D Sm@rtCafé Expert v3.0	Smart Card	Java Card v2.2.1
G&D Sm@rtCafé Expert v3.1	Smart Card	Java Card v2.2.1
G&D Sm@rtCafé Expert 3.2	Smart Card	Java Card v2.2.1
G&D Sm@rtCafé Expert v4.0	Smart Card	Java Card v2.2.1
G&D Sm@rtCafé Expert v5.0	Smart Card	Java Card v2.2.2
G&D Convego Join 4.01 40k/80k	Smart Card	Java Card v2.2.1
Mobile Security Card SE 1.0	MicroSD card	Java Card v2.2.2
Gemalto GemXpresso Pro R4 72PK / TOP IM GX4	Smart Card	Java Card v2.2.1
Gemalto MultiApp ID v2.1	Smart Card	Java Card v2.2.1
Gemalto Optelio D72 FR1	Smart Card	Java Card v2.2.2
Gemalto USB eSeal Token V2 TOP IM GX4	USB Token	Java Card v2.2.1
Gemalto TOP DL v2	Smart Card	Java Card v2.2.1
IDpendant IDp 200	USB Token	Java Card v2.2.1
IDpendant IDp 1000	USB Token	Java Card v2.2.1
IBM JCOP 21 v2.2.1	Smart Card	Java Card v2.2.1
IBM JCOP31 v2.2.1	Smart Card	Java Card v2.2.1
IBM JCOP 41 v2.2.1	Smart Card	Java Card v2.2.1
KEBT KONA10 v1.6, KONA11 v1.0, KONA12 v1.1, KONA20 v1.4, KONA27 v1.1	Smart Card	Java Card v2.2[1]
KEBT KONA 21T	Smart Card	Java Card v2.2
Marx CrypToken MX2048-JCOP	USB Token	Java Card v2.2.1
NXP JCOP21 v2.3.1	Smart Card	Java Card v2.2.1
NXP JCOP31 v2.3.1	Smart Card	Java Card v2.2.1
NXP JCOP41 v2.3.1	Smart Card	Java Card v2.2.1
NXP JCOP21 v2.4.1 / J2A080	Smart Card	Java Card v2.2.2
NXP JCOP31 v2.4.1 / J3A080	Smart Card	Java Card v2.2.2
NXP JCOP21 v2.4.1 / J2A081	Smart Card	Java Card v2.2.2
NXP JCOP31 v2.4.1 / J3A081	Smart Card	Java Card v2.2.2

[1] Implemented with support for key generation of 1024 bits only.

Oberthur IDone Cosmo64 v5.2	Smart Card	Java Card v2.2.1
Oberthur ID-One Cosmo 32 RSA v3.6	Smart Card	Java Card v2.2.1
Oberthur ID-One Cosmo 64 RSA D/T v5.4	Smart Card	Java Card v2.2.1
Oberthur ID-One Cosmo v7.0	Smart Card	Java Card v2.2.1
Sagem Orga J-ID Mark 64 Dual	Smart Card	Java Card v2.2.1
Sagem Orga ysID S3[1]	Smart Card	Java Card v2.2.2
Sagem Orga ysID Key E-M	USB Token	
Sagem Orga ysID Key E2C[2]	USB Token	

7.2.3 Java Card 3.0

Token	Type	Additional remarks
G&D Sm@rtCafé Expert v6.0	Smart Card	Java Card v3.0.1 Classic

7.3 Belgium Identity Card

Token	Type	Additional remarks
Belgium eID card	Smart Card	Only for authentication

7.4 IDpendant

Token	Type	Additional remarks
IDp 100	Smart Card	None

7.5 Multos

Token	Type	Additional remarks
KeyCorp Multos v4.2 48K card	Smart Card	None
KeyCorp Multos v4.2 64K card	Smart Card	None

7.6 RSA

Token	Type	Additional remarks
RSA SecurID Token	USB token	Read-only implementation
RSA Smart Card 5200	Smart Card	Read-only implementation

7.7 SECCOS[3]

Token	Type	Additional remarks
SECCOS 5.0	Smart Card	None
SECCOS 6.2	Smart Card	None

[1] Only supported with the SafeSign PKI applet pre-installed.
[2] Only supported with the SafeSign PKI applet pre-installed.
[3] Note that the ATR of SECCOS cards depends on specific card capabilities and may be project-related. Therefore, the Token Utility may report an Unknown ATR. ATRs can be added to the Windows registry manually or by using an appropriate tool.

7.8 Siemens

Token	Type	Additional remarks
CardOS 4.3B 32 / 64K	Smart Card	None
CardOS 4.4	Smart Card	None

7.9 Swiss Cards

Token	Type	Additional remarks
Quovadis SuisseID	Smart Card	CardOS 4.3B
SwissSign SuisseID	Smart Card	CardOS 4.3B
FMH / Swisscom Swiss Health Professional Card	Smart Card	CardOS 4.3B
Swisspost Schweizerische Krankenversicherungskarte KVG	Smart Card	STARCOS 3.4
Sasis PDC / Krankenversicherungskarte KVG	Smart Card	MTCOS

8 Supported Applications

SafeSign Identity Client supports an ever-increasing list of applications.

SafeSign Identity Client Standard Version 3.0-x64 for Windows has been tested in accordance with AET's Quality Assurance procedures and the SafeSign Identity Client Standard Version 3.0-x64 for Windows test plan. This includes testing of a number of defined and representative applications to verify a correct functioning of the SafeSign Identity Client PKCS #11 and Microsoft CryptoAPI Libraries.

The list below lists those 64-bit applications that were explicitly tested by AET and may include 32-bit applications running on the 64-bit Operating Systems (such as Firefox and Thunderbird).

The list below is not all-inclusive: it does not imply that other 64-bit applications do not work with SafeSign Identity Client. If you have an application that works with SafeSign Identity Client that you wish to have listed, please contact us.

8.1 Public Key Infrastructure

Public key Infrastructure	
Application	**Microsoft** Standalone and Enterprise Certificate Server
Application version	Windows Server 2003 x64 Edition (R2)[1], Windows Server 2008 x64 Edition, Windows Server 2008 R2[2]
Supported by SafeSign-IC versions	3.0.33-x64, 3.0.40-x64, 3.0.45-x64, 3.0.70-x64

8.2 Client Applications

Client Applications	
Application	**Adobe Reader X**
Application version	10.0, 10.0.1, 10.1.0
Supported by SafeSign-IC versions	3.0.45-x64, 3.0.70-x64
Application	**Microsoft** Internet Explorer[3]
Application version	8.0, 9.0
Supported by SafeSign-IC versions	3.0.40-x64, 3.0.45-x64, 3.0.70-x64
Application	**Microsoft** Office
Application version	2010
Supported by SafeSign-IC versions	3.0.40-x64, 3.0.45-x64, 3.0.70-x64
Application	**Microsoft** Outlook Express
Application version	6.0
Supported by SafeSign-IC versions	3.0.33-x64, 3.0.40-x64, 3.0.45-x64, 3.0.70-x64
Application	**Microsoft** VPN
Application version	-
Supported by SafeSign-IC versions	3.0.33-x64, 3.0.40-x64, 3.0.45-x64, 3.0.70-x64
Application	**Microsoft** Windows Mail
Application version	6.0
Supported by SafeSign-IC versions	3.0.33-x64, 3.0.40-x64, 3.0.45-x64, 3.0.70-x64
Application	**Mozilla** Firefox[4]
Application version	1.0.x, 1.5, 2.0, 3.0, 3.5, 3.6, 13.0.1
Supported by SafeSign-IC versions	1.0.9.04, 1.0.9.04-Update, 2.0, 2.1, 2.2, 2.3, 3.0
Application	**Mozilla** Thunderbird

[1] Windows 2003 Server key archival is not supported.
[2] Windows 2008 Server is supported from SafeSign IC version 3.0.33-x64 onwards.
[3] Internet Explorer 9 is not supported in SafeSign Identity Client version 3.0.45, but it is in 3.0.70.
[4] Mozilla Firefox 4 is not supported in SafeSign Identity Client version 3.0.45.

Application version	1.0.x, 1.5, 2.0, 2.0.0.23, 3.1, 13.0.1
Supported by SafeSign-IC versions	1.0.9.04, 1.0.9.04-Update, 2.0, 2.1, 2.2, 2.3, 3.0
Application	**Microsoft** Remote Desktop Connection (Client)
Application version	Windows XP, Windows Vista, Windows 7
Supported by SafeSign-IC versions	3.0.33-x64, 3.0.40-x64, 3.0.45-x64, 3.0.70-x64
Application	**Microsoft** Remote Desktop Services
Application version	Windows Server 2003 x64 Edition, Windows Server 2008 x64 Edition, Windows Server 2008 R2
Supported by SafeSign-IC versions	3.0.33-x64, 3.0.40-x64, 3.0.45-x64, 3.0.70-x64
Application	OpenOffice Writer
Application version	3.3.0, 3.4.0
Supported by SafeSign-IC versions	3.0.45-x64, 3.0.70-x64

Appendix 1

The table below lists the smart card readers that have been tested at a given time with a SafeSign Identity Client Version 3.0-x64.x release. This does not imply that these readers will (still) work or will be supported in any or all versions of SafeSign Identity Client Version 3.0-x64.x.

If you have problems with your specific smart card reader, please contact AET Support.

Smart card reader manufacturer and model	Interface	Class
ACS ACR38-IPC[1]	USB	1
ACS ACR38T	USB	1
ACR38 USB Smart Card Reader/Writer[2]	USB	1
Cherry SmartCard Keyboard G83-6744LUA (secure PIN entry, EMV 2000 level 1)	USB	1
Cherry SmartCard Keyboard G83-6744LUZ (secure PIN entry, EMV 2000 level 1, certification Common Criteria EAL 3+)	USB	1
Cherry SmartTerminal ST-20000U	USB	2
G&D Crypto USB Token	USB	1
G&D StarKey100	USB	1
G&D StarKey300	USB	1
G&D StarKey400	USB	1
GemPlus GemPC430	USB	1
GemPlus GemPC Twin	USB	1
HP USB Smart Card Keyboard[3]	USB	1
IDPendant IDp 100	USB	1
IDPendant IDp 200	USB	1
IDpendant IDp 1000	USB	1
Marx® CrypToken® MX2048-JCOP	USB	1
O2Micro OZ776 USB CCID Smartcard Reader[4]	USB	1
Omnikey CardMan Mobile PCMCIA 4000	PCMCIA	1
Omnikey CardMan Mobile PCMCIA 4040	PCMCIA	1
Omnikey CardMan Desktop USB 3121	USB	1
Omnikey CardMan Trust* 3620 (< SafeSign 3.0.33)	USB	2
Omnikey CardMan Trust* 3621	USB	2
Omnikey 3821 USB pinpad (≥ SafeSign 3.0.33)	USB	2
Omnikey CardMan RFID 5121	USB	1
Omnikey CardMan 6121	USB	1
ORGA CardMouse USB V1.1	USB	1
Perto PertoSmart	USB	1

[1] ACS readers have been tested by their supplier / reseller or their partner.
[2] The ACR38U has a maximum supply current of 50mA. This card reader has been tested by A.E.T. Europe B.V. The results were positive. Nevertheless, to avoid power problems, we advise that smart card readers must be capable to provide at least a current of 60mA.
[3] Model tested: KUS0133
[4] Tested on Dell D420 / D620 Latitude notebooks only.

Reiner-SCT Cyberjack pinpad* (< SafeSign 3.0.33)	RS232, USB	2
Reiner SCT cyber*Jack* pinpad (≥ SafeSign 3.0.33)	USB	2
Reiner SCT cyber*Jack* e-com (≥ SafeSign 3.0.33)	USB	3
Reiner SCT cyber*Jack* secoder (≥ SafeSign 3.0.33)	USB	3
Renesas SecureMMC Reader (JAE USB X Mobile Card Reader PC-RNS7)	USB	1
SCM Microsystems SCR241[1]	PCMCIA	1
SCM Microsystems SCR131	RS232	1
SCM Microsystems SCR331	USB	1
SCM Microsystems SCR531 (dual connection)	RS232, USB	1
SCM Microsystems SCR335	USB	1
SCM Microsystems SPR 532 PINpad Reader (≥ SafeSign 3.0.33)	USB	2
Todos eCode Connectable 217U (≥ SafeSign 3.0.33)	USB	3
XIRING Leo	USB	3
XIRING MyLeo	USB	3

*) Note: Supported in versions previous to SafeSign IC Version 3.0-x64.33, where the PC/SC 1.0 reader driver of the pinpad readers above (either class 2 readers with additional PIN pad or class 3 readers with additional PIN pad and own display) is extended by proprietary functions for PIN pad support.

[1] All SCM readers have been tested by their supplier, SCM Microsystems.