

Product Description

SafeSign Identity Client Standard Version 3.0-x64 for Windows

This document contains information of a proprietary nature.
No part of this document may be reproduced or transmitted in any form or by any means electronic, mechanical or otherwise, including photocopying and recording for any purpose 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.

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.

© Copyright A.E.T. Europe B.V., 1997 - 2010.

All rights reserved.

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

Credit information:

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

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

<p>Contact Information: A.E.T. Europe B.V.</p> <p>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</p>	 <p>info@aeteurope.nl / support@aeteurope.nl http://www.aeteurope.com/</p> <p><i>SafeSign Identity Client is a product developed by A.E.T. Europe B.V.</i></p> <p>Copyright © 1997-2010 A.E.T. Europe B.V., Arnhem, The Netherlands. All rights reserved.</p>	
---	---	---

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	10-08-2010	Drs. C.M. van Houten	Edited for SafeSign Identity Client Standard Version 3.0-x64 for Windows (release 3.0.40-x64)

WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE

Table of contents

Warning Notice	II
Document Information.....	III
Table of contents.....	IV
About the Product	V
About the Document	VI
1 Introduction.....	1
2 SafeSign Identity Client Functionality	1
3 Features	2
3.1 Multiple Token Support	2
3.2 Multiple language support	3
3.3 Multiple OS Support.....	3
3.4 Support for PIN timeout.....	3
3.5 Support for PC/SC 2.0 secure pinpad readers	4
3.6 Support for EFS	4
3.7 Support for maximum PUK and PIN length	5
3.8 Support for virtual readers in PKCS #11	5
3.9 SafeSign IC Credential Provider.....	6
3.10 Support for SHA-2.....	7
3.11 Support for AES.....	7
4 End User Documentation	8
5 Supported and Tested PC Operating Systems.....	8
6 Supported and Tested Smart Card Readers	9
7 Supported and Tested Hardware Tokens	10
7.1 STARCOS	10
7.2 Java Cards.....	10
7.3 Belgium Identity Card	13
7.4 IDpendant.....	13
7.5 Multos	13
7.6 RSA	13
7.7 SECCOS	13
7.8 Siemens.....	13
8 Supported Applications.....	14
8.1 Public Key Infrastructure	14
8.2 Client Applications.....	14

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 and Cryptographic Service Provider (CSP), 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 64-bit comes in a standard version with an installer for the x64 Editions of the following Windows Operating Systems:

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

In principle, SafeSign Identity Client supports any PC/SC 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.

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.

1 Introduction

SafeSign Identity Client is a software package to enhance the security of applications that support PKCS #11 and Microsoft CryptoAPI 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, 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 (Express).

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, Vista, 7, 2003 and 2008 logon support; Windows 2003 / 2008 TS and Citrix logon support.

PC/SC v2.0 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).

PKCS #11 wrappers for applications from Entrust (6.x) and RSA SecurID.

SafeSign Identity Client GINA to facilitate logon with protected authentication path readers (such as secure pinpad Class 2 and 3 readers)¹.

Token Utilities for such operations as: token initialisation, token visualisation, import of Digital IDs (including certificate chains), visualisation/deletion of certificates/objects, change PIN/PUK and unlock PIN.

¹ Applies to SafeSign versions prior to Version 3.0-x64.33 when used on Windows 2000 and Windows XP.

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 ($\geq 3.0.40$);
- SafeSign IC Credential Provider ($\geq 3.0.40$);
- Support for SHA-2 ($\geq 3.0.40$);
- Support for AES ($\geq 3.0.40$).

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.

Supported tokens in SafeSign Identity Client Standard Version 3.0-x64 for Windows include:

- Athena IDProtect
- Athena IDProtect Duo
- Gemalto GemXpresso R4 / TOP IM GX4 ($\geq 3.0.33$)
- Gemalto GemXpresso R4 / TOP IM GX4 MSA081 ($\geq 3.0.40$)
- Gemalto USB eSeal Token V2 TOP IM GX4 ($\geq 3.0.40$)
- Giesecke & Devrient Sm@rtCafé 4.0 ($\geq 3.0.23$)
- Giesecke & Devrient STARCOS 3.0 DI ($\geq 3.0.40$)
- Giesecke & Devrient STARCOS 3.2¹ ($\geq 3.0.40$)
- Giesecke & Devrient STARCOS 3.4 ($\geq 3.0.40$)
- Giesecke & Devrient Sm@rtCafé 3.2 ($\geq 3.0.40$)
- Giesecke & Devrient Sm@rtCafé Expert 5.0 ($\geq 3.0.40$)
- Giesecke & Devrient Mobile Security Card SE 1.0 ($\geq 3.0.40$)
- IDpendant IDp 1000 ($\geq 3.0.15$)
- NXP JCOP21 v2.3.1
- NXP JCOP31 v2.3.1
- NXP JCOP41 v2.3.1
- NXP JCOP21 v2.4.1 ($\geq 3.0.40$)
- NXP JCOP31 v2.4.1 ($\geq 3.0.40$)
- Oberthur IDOne Cosmo v7.0 ($\geq 3.0.23$)
- RSA SecurID Token²
- RSA Smart Card 5200³

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

² Read-only implementation.

³ Read-only implementation.

- Sagem Orga J-IDMark 64
- Sagem Orga J-IDMark 64 Dual ($\geq 3.0.33$)
- Sagem Orga YpsID s2 ($\geq 3.0.40$)
- SECCOS 5.2 and SECCOS 6.0
- Siemens CardOS 4.3B 32K/64K

Details of tokens are listed in Chapter 7.

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 Latin¹.

3.3 Multiple OS Support

SafeSign Identity Client Standard Version 3.0-x64 for Windows supports a number of different Operating Systems:

- Windows XP x64 Edition
- Windows Vista x64 Edition;
- Windows Server 2003 x64 Edition;
- Windows Server 2008 x64 Edition;
- Windows Server 2008 R2 (x64) Edition;
- Windows 7 x64 Edition.

3.4 Support for PIN timeout

In SafeSign Identity Client Version 3.0.33-x64, 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, 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 Utility², 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:

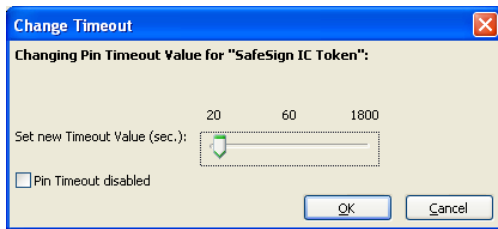


Figure 1: Change Timeout

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, 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.

3.5 Support for PC/SC 2.0 secure pinpad readers

From SafeSign Identity Client Version 3.0.33-x64 onwards ($\geq 3.0.33-x64$), 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 PC/SC 2.0 readers supported in SafeSign Identity Client Version 3.033-x64 (and onwards) are:

- Cherry SmartBoard XX44;
- Cherry SmartTerminal ST-20000U (ST-20000UCZ / ST20000UC-R);
- OMNIKEY 3821 USB pinpad;
- Reiner SCT cyberJack pinpad;
- Reiner SCT cyberJack e-com;
- Reiner SCT cyberJack secoder;
- SCM Microsystems SPR532 PINpad Reader¹;
- Todos eCode Connectable 217U.

Note that it is up to the reader manufacturers to supply working drivers for 64-bit Windows Operating Systems.

3.6 Support for EFS

SafeSign Identity Client Version 3.0.33-x64 supports EFS on Windows Vista, Windows 7 and Windows Server 2008².

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 can add (through the registry³) 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".

¹ When upgraded to the latest firmware and drivers.

² 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.

³ 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

This gives you the flexibility to use your (existing) Smart Card User certificates for EFS. 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.

Refer to the Microsoft web site for more information on the requirements and operation of EFS.

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

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.

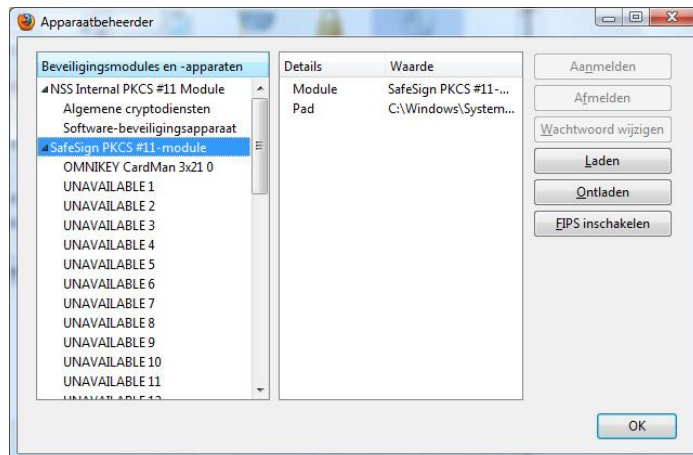
3.8 Support for virtual readers in PKCS #11

In SafeSign Identity Client version 3.0.40 ($\geq 3.0.40$) 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 loaded¹. 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:

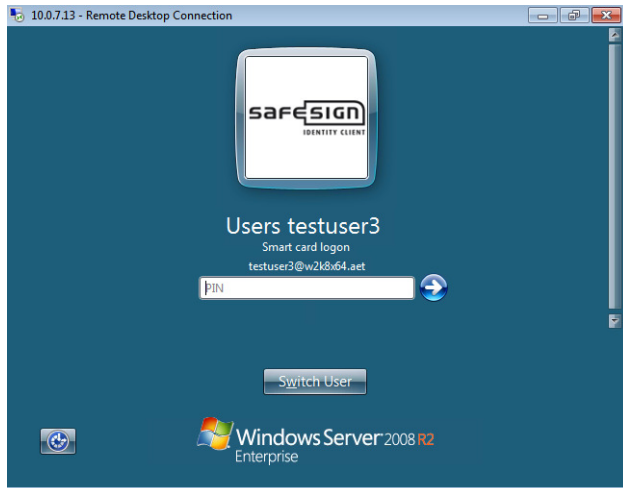


¹ The PKCS#11 specification states: "the set of slots accessible through a Cryptoki library is fixed at the time that C_Initialize is called. If an application calls C_Initialize and C_GetSlotList, and then the user hooks up a new hardware device, that device cannot suddenly appear as a new slot if C_GetSlotList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

From SafeSign Identity Client version 3.0.40 onwards ($\geq 3.0.40$), the functionality provided by the SafeSign GINA (on Windows XP) is now provided by the SafeSign IC Credential Provider for Windows Vista and higher:



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

The SafeSign Credential Provider will only display one tile for each token / user credential, unlike the Windows Credential provider, which will display a large number of tiles when using multiple readers and cards. For example, when inserting two cards in two different readers, SafeSign will display two tiles, whereas Microsoft will display four tiles.

In fact, 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.

Note that the current SafeSign Credential Provider does not support multiple certificates on one token. When you have more than one certificate on a token, it is recommended not to install the SafeSign Credential Provider, but to use the Microsoft Credential Provider.

Note that the SafeSign Credential Provider does not support PLAP / Single Sign-On¹. 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.

Both features are planned to be included in a future release.

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.

3.10 Support for SHA-2

SafeSign Identity Client version 3.0.40 ($\geq 3.0.40$) now supports SHA-2, with the following variants: SHA-256, SHA-384 and SHA-512.

3.11 Support for AES

In SafeSign Identity Client version 3.0.40 ($\geq 3.0.40$), 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](http://msdn.microsoft.com/en-us/library/aa387447(VS.85).aspx)

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	1.1
SafeSign Identity Client Standard 3.0-x64 Product Description	1.1
SafeSign Identity Client Standard x64 User Guide for Installation	1.1
SafeSign Identity Client Standard User Guide for Token Management Utility	3.1
SafeSign Identity Client Standard User Guide for Token Administration Utility	3.1
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	3.2
SafeSign Identity Client User Guide for Authentication	2.1

Note that the (2.1) User Guides mentioned above were written for SafeSign Identity Client versions 2.3.x and is in the process of being updated.

Unless mentioned otherwise, please note that the documentation mentioned above was written for 32-bit SafeSign Identity Client versions (2.3.x and 3.0.x).

5 Supported and Tested PC Operating Systems

SafeSign Identity Client Standard Version 3.0-x64, release 3.0.40, for Windows has been tested to support the following PC Operating Systems:

Operating System	Version
Windows	Windows XP Professional x64 Edition (SP2)
	Windows Vista Ultimate x64 Edition (SP2)
	Windows Vista Business x64 Edition (SP2)
	Windows Vista Enterprise x64 Edition (SP2)
	Windows 7 Professional x64 Edition
	Windows 7 Ultimate x64 Edition
	Windows Server 2003 Enterprise x64 Edition
	Windows Server 2003 R2 Enterprise x64 Edition (SP2)
	Windows Server 2008 Enterprise x64 Edition (SP2)
	Windows Server 2008 R2 Enterprise x64 Edition

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.

To facilitate the choice of a smart card reader, the following table lists the readers and reader drivers that were tested and qualified for use with SafeSign Identity Client 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.

Moreover, this list does not imply that each smart card reader and reader driver listed works with each SafeSign Identity Client supported smart card on each Windows x64 Operating System supported. For example, drivers may be supplied but not supported or drivers may exist for Windows XP and Vista, but not for Windows 7. 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.

Smart card reader manufacturer and model	Interface	Class	Reader Driver version
Cherry SmartTerminal ST-20000U	USB	2	Cherry-SmartDeviceSetup_19_EN.msi
Marx® CrypToken® MX2048-JCOP	USB	1	OMNIKEY_3x21_V1_2_1_2_W64_AMD.exe
Omniquey CardMan Desktop USB 3121	USB	1	OMNIKEY_3x21_V1_2_1_2_W64_AMD.exe
Omniquey 3821 USB pinpad	USB	2	OMNIKEY_3x21_V1_2_1_2_W64_AMD.exe
Omniquey CardMan 6121	USB	1	OMNIKEY_3x21_V1_2_1_2_W64_AMD.exe
Reiner SCT cyberJack pinpad	USB	2	bc_6_8_0.exe
Reiner SCT cyberJack e-com	USB	3	bc_6_8_0.exe
Reiner SCT cyberJack secoder	USB	3	bc_6_8_0.exe
SCM Microsystems SPR 532 PINpad Reader	USB	2	SPR532_USB_V4.34_4.45
Todos eCode Connectable 217U	USB	3	1.0.1.3

7 Supported and Tested Hardware Tokens

SafeSign Identity Client Standard Version 3.0-x64 for Windows has been tested to support the following hardware tokens:

7.1 STARCOS

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 STARCOS 3.0 (Standard Version)	Smart Card	Series completion: CPAZ0SCSI30-01A-0V300
G&D STARCOS 3.2 ¹	Smart Card	
G&D STARCOS 3.4	Smart Card	

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. 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). Note that for deployment / production, you would want to use cards with a production key set (for which the SafeSign Identity Client applet loader can be configured).

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

There are three default profiles of SafeSign Identity Client applets available with different sizes for Java 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 *).

Note that 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.

The minimum sized SafeSign Identity Client applet can only be used for Windows smart card logon (Windows XP, Vista, 7, Server 2003 / 2008) or for SSL client authentication and secure email.

Token	Type	Additional remarks
Aspects OS755 v2.8	Smart Card	Java Card v2.1.1
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
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 Palmera	Smart Card	Java Card v2.1.1
G&D Sm@rtCafé Expert v2.0	Smart Card	Java Card v2.1.1
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)
Token	Type	Additional remarks
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 v4.0	Smart Card	Java Card v2.2.1
G&D Sm@rtCafé Expert v5.0	Smart Card	Java Card v2.2.2
Mobile Security Card SE 1.0	MicroSD card	Java Card v2.2.2
G&D STARSIM Java	Smart Card	Java Card v2.1.1

Token	Type	Additional remarks
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
Gemalto GemXpresso Pro R4 72PK	Smart Card	Java Card v2.2.1
Gemalto USB eSeal Token V2 TOP IM GX4	USB Token	Java Card v2.2.1
Gemplus GemXplore 3G (Gem10.64 GX3GV22 128K-PK)	Smart Card	Java Card v2.1.1
IDpendant IDp 200	USB Token	Java Card v2.2.1
IDpendant IDp 1000	USB Token	Java Card v2.2.1
IBM JCOP 20	Smart Card	Java Card v2.1.1
IBM JCOP 21id	Smart Card	Java Card v2.1.1
IBM JCOP 21 v2.2.1	Smart Card	Java Card v2.2.1
IBM JCOP 30	Smart Card	Java Card v2.1.1
IBM JCOP 31bio	Smart Card	Java Card v2.1.1
IBM JCOP31 v2.2.1	Smart Card	Java Card v2.2.1
IBM JCOP 41 v2.2.1	Smart Card	Java Card v2.1.1
KEBT KONA10 v1.6, KONA11 v1.0, KONA12 v1.1, KONA20 v1.4, KONA27 v1.1	Smart Card	Java Card v2.21
KEBT KONA 21T	Smart Card	Java Card v2.2
MartSoft Java card	Smart Card	Java Card v2.1.1
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
Oberthur CosmopolIC v4	Smart Card	Java Card v2.1.1
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
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
Sagem Orga J-ID Mark 64 Dual	Smart Card	Java Card v2.2.1
Sagem Orga ypsID S2	Smart Card	Java Card v2.2.1

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

7.3 Belgium Identity Card

Token	Type	Additional remarks
Belgium eID card	Smart Card	None

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 SECCOS¹

Token	Type	Additional remarks
SECCOS 5.2	Smart Card	None
SECCOS 6.0	Smart Card	None

7.8 Siemens

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

¹ 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.

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. 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 does not include 32-bit applications running on the 64-bit Operating Systems (such as Firefox or Thunderbird), although they (may) have been tested successfully.

Note that the list is not all-inclusive: it does not imply that other 64-bit applications do not work with SafeSign Identity Client.

8.1 Public Key Infrastructure

Public key Infrastructure	
Application	Microsoft Standalone and Enterprise Certificate Server
Application version	Windows Server 2003 (R2) ¹ , Windows Server 2008 (R2) ²
Supported by SafeSign-IC versions	3.033-x64, 3.0.40-x64

8.2 Client Applications

Client Applications	
Application	Microsoft Internet Explorer
Application version	8.0
Supported by SafeSign-IC versions	3.0.33-x64, 3.0.40-x64
Application	Microsoft Office
Application version	2010
Supported by SafeSign-IC versions	3.0.40-x64
Application	Microsoft Outlook
Application version	2010
Supported by SafeSign-IC versions	3.0.40-x64
Application	Microsoft Outlook Express
Application version	6.0
Supported by SafeSign-IC versions	3.0.33-x64, 3.0.40-x64
Application	Microsoft VPN
Application version	-
Supported by SafeSign-IC versions	3.0.33-x64, 3.0.40-x64
Application	Microsoft Windows Mail
Application version	6.0
Supported by SafeSign-IC versions	3.0.33-x64, 3.0.40-x64
Application	Microsoft Windows Terminal Server
Application version	Windows Server 2003, Windows Server 2008
Supported by SafeSign-IC versions	3.0.33-x64, 3.0.40-x64

¹ Windows 2003 Server key archival is not supported.

² Windows 2008 Server is supported from SafeSign IC Version 3.0-x64.33 onwards.