

# Product Description

## SafeSign Identity Client Standard Version 3.0 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](mailto:eyay@cryptsoft.com))

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

<p><b>Contact Information: A.E.T. Europe B.V.</b></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><a href="mailto:info@aeteurope.nl">info@aeteurope.nl</a> / <a href="mailto:support@aeteurope.nl">support@aeteurope.nl</a> <a href="http://www.aeteurope.com/">http://www.aeteurope.com/</a></p> <p>SafeSign Identity Client is a product developed by A.E.T. Europe B.V.</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\_Windows\_Product\_Description

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

### Document revision history

Version	Date	Author	Changes
1.0	05-05-2008	Drs. C.M. van Houten	First edition for SafeSign Identity Client Standard Version 3.0 for Windows (release 3.0.11)
1.1	25-06-2008	Drs. C.M. van Houten	Edited for SafeSign Identity Client Standard Version 3.0 for Windows (release 3.0.15)
1.2	31-10-2008	Drs. C.M. van Houten	Edited for SafeSign Identity Client Standard Version 3.0 for Windows (release 3.0.18)
1.3	09-01-2009	Drs. C.M. van Houten	Edited for SafeSign Identity Client Standard Version 3.0 for Windows (release 3.0.23)
1.4	08-04-2009	Drs. C.M. van Houten	Updated for SafeSign Identity Client Standard Version 3.0 for Windows (release 3.0.23)
1.5	29-09-2009	Drs. C.M. van Houten	Edited for SafeSign Identity Client Standard Version 3.0 for Windows (release 3.0.33)
1.6	10-08-2010	Drs. C.M. van Houten	Edited for SafeSign Identity Client Standard Version 3.0 for Windows (release 3.0.40)

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

## Table of contents

---

<b>Warning Notice .....</b>	<b>II</b>
<b>Document Information.....</b>	<b>III</b>
<b>Table of contents.....</b>	<b>IV</b>
<b>About the Product .....</b>	<b>V</b>
<b>About the Document .....</b>	<b>VI</b>
<b>1 Introduction.....</b>	<b>1</b>
<b>2 SafeSign Identity Client Functionality .....</b>	<b>1</b>
<b>3 Features .....</b>	<b>2</b>
3.1 Multiple Token Support .....	2
3.2 Multiple language support .....	3
3.3 Multiple OS Support.....	3
3.4 Support for Remote Desktop Connection 6.0 .....	3
3.5 Support for Igel thin clients .....	4
3.6 Support for PIN timeout.....	5
3.7 Support for PC/SC 2.0 secure pinpad readers .....	5
3.8 Support for EFS.....	6
3.9 Support for maximum PUK and PIN length .....	6
3.10 Support for virtual readers in PKCS #11 .....	7
3.11 SafeSign IC Credential Provider.....	8
3.12 Support for SHA-2.....	9
3.13 Support for AES.....	9
<b>4 End User Documentation .....</b>	<b>10</b>
<b>5 Supported and Tested PC Operating Systems.....</b>	<b>10</b>
<b>6 Supported and Tested Smart Card Readers .....</b>	<b>11</b>
<b>7 Supported and Tested Hardware Tokens .....</b>	<b>14</b>
7.1 STARCOS .....	14
7.2 Java Cards.....	15
7.3 Belgium Identity Card .....	17
7.4 IDpendant.....	17
7.5 Multos .....	17
7.6 RSA.....	17
7.7 SECCOS .....	17
7.8 Siemens.....	17
<b>8 Supported Applications.....</b>	<b>18</b>
8.1 Public Key Infrastructure .....	18
8.2 Client Applications.....	19

---

## 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 comes in a standard version with an installer for the following Windows environments<sup>1</sup>:

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.

---

<sup>1</sup> 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.

## 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)<sup>1</sup>.

---

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.

---

---

<sup>1</sup> Applies to SafeSign IC versions prior to version 3.0.33 when used on Windows 2000 and Windows XP.

## 3 Features

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

- Multiple token support;
- Multiple language support;
- Multiple OS support;
- Remote Desktop Connection 6.0;
- Support for Igel thin clients ( $\geq 3.0.15$ );
- Support for PIN timeout ( $\geq 3.0.18$ );
- Support for PC/SC 2.0 secure pinpad readers ( $\geq 3.0.33$ );
- Support for EFS ( $\geq 3.0.33$ );
- Support for maximum PUK and PIN length ( $\geq 3.0.33$ );
- 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 for Windows supports a number of different tokens.

Newly supported tokens in SafeSign Identity Client Standard Version 3.0 for Windows are:

- 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 3.2<sup>1</sup> ( $\geq 3.0.40$ )
- 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 Token<sup>2</sup>
- RSA Smart Card 5200<sup>1</sup>

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

<sup>2</sup> Read-only implementation.

- Sagem Orga J-IDMark 64
- Sagem Orga J-IDMark 64 Dual (≥ 3.0.33)
- Sagem Orga YpsID s2 (≥ 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 for Windows supports a number of different languages.

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

- Korean language (≥ 3.0.23);
- Serbian language, Cyrillic and Latin (≥ 3.0.33)<sup>2</sup>.

## 3.3 Multiple OS Support

- Support for Windows XP SP3 (≥ 3.0.15);
- Support for Vista SP1 (≥ 3.0.15);
- Support for Vista SP2 (≥ 3.0.15);
- Support for Windows Server 2008 (≥ 3.0.33);
- Support for Windows 7 (≥ 3.0.33);

## 3.4 Support for Remote Desktop Connection 6.0

SafeSign Identity Client now supports Microsoft Remote Desktop Connection 6.0.

In previous versions (< version 3.0.11), the connection would fail with an error:

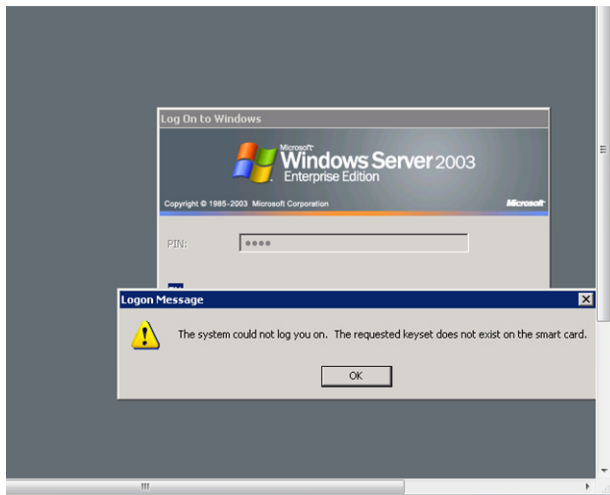


Figure 1: Remote Desktop: Logon Message

Note that after this (when clicking OK in the Logon Message dialog), it was possible to enter the PIN again and successfully set up the connection.

From SafeSign Identity Client Version 3.0 onwards (≥ 3.0.11), this has been solved.

<sup>1</sup> Read-only implementation.

<sup>2</sup> 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.

First you will need (or be allowed) to select the credentials on the smart card and enter the PIN in the *Remote Desktop Connection* dialog:

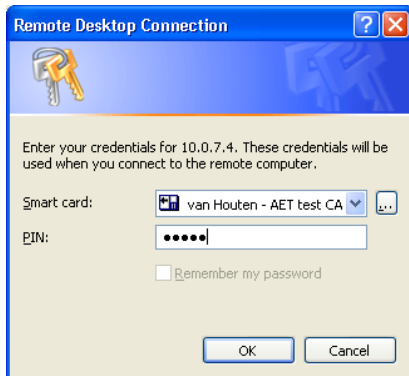


Figure 2: Remote Desktop Connection: Enter credentials

After clicking **OK**, the connection will be made, without the need to enter the PIN again in the *Log On to Windows* dialog:

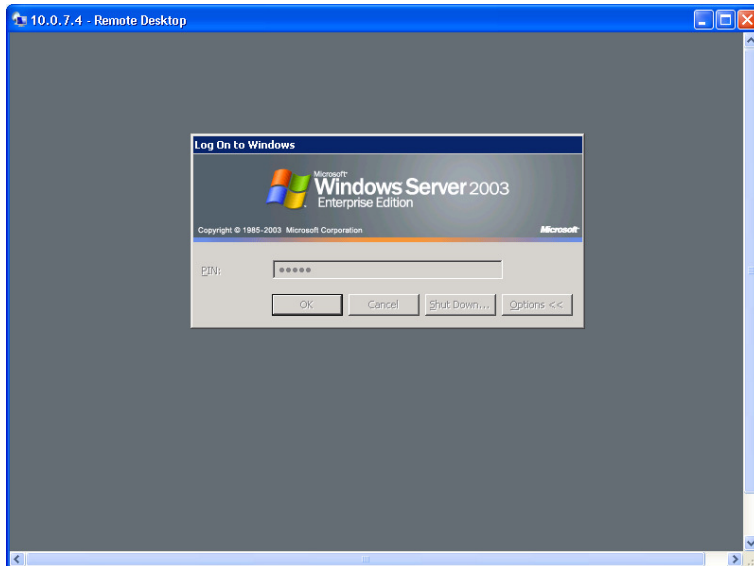


Figure 3: Remote Desktop: Log On to Windows dialog

### 3.5 Support for Igel thin clients

Support for IGEL Linux-based thin clients is now activated by default in SafeSign Identity Client, for the supported Java Card v2.2 (and higher) cards.

This means that because the SafeSign Libraries are integrated into the Thin Client firmware by default, you can use your token to allow access to the terminal and associated sessions.

Note that this applies only to cards personalised with SafeSign 3.0.15 (or higher)<sup>1</sup>.

<sup>1</sup> Because this is set during initialization (i.e. writing the PKCS#15 structure) of the token, with a token label, PUK and PIN.

### 3.6 Support for PIN timeout

In SafeSign Identity Client version 3.0.18 ( $\geq 3.0.18$ ), 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 Utility<sup>1</sup>, through the menu Token > Change PIN Timeout, if the (initialised) token is inserted and the correct PIN is entered.

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:

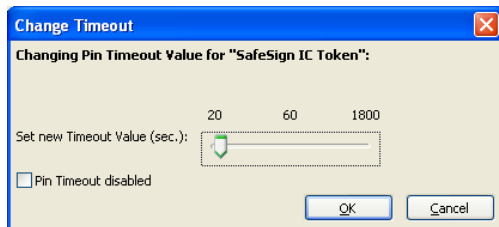


Figure 4: Change Timeout

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.

From SafeSign Identity Client 3.0.33 onwards ( $\geq 3.0.33$ ), 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.

### 3.7 Support for PC/SC 2.0 secure pinpad readers

From SafeSign Identity Client version 3.0.33 onwards ( $\geq 3.0.33$ ), 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 $\geq 3.0.33$
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

<sup>1</sup> The Token Management Utility does not include this option.

The PC/SC 2.0 readers supported in SafeSign Identity Client version 3.0.33 (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 Reader<sup>1</sup>;
- Todos eCode Connectable 217U.

### 3.8 Support for EFS

SafeSign Identity Client version 3.0.33 supports EFS on Windows Vista, Windows 7 and Windows Server 2008<sup>2</sup>.

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 registry<sup>3</sup>) 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. 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.

### 3.9 Support for maximum PUK and PIN length

From SafeSign Identity Client version 3.0.33 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.

---

<sup>1</sup> When upgraded to the latest firmware and drivers.

<sup>2</sup> 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.

<sup>3</sup> 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

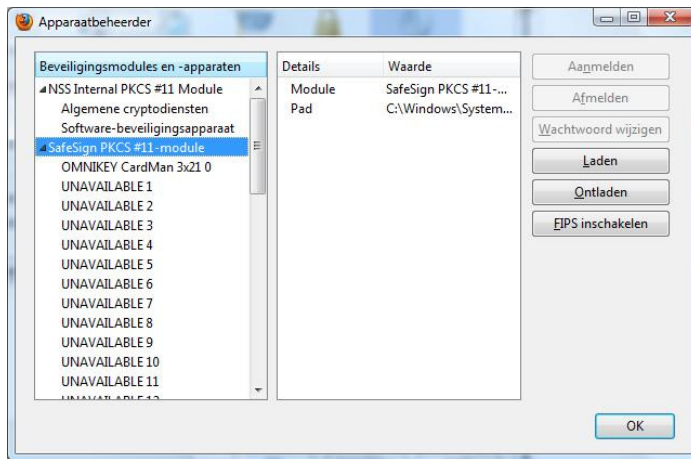
### 3.10 Support for virtual readers in PKCS #11

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 loaded<sup>1</sup>. 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:

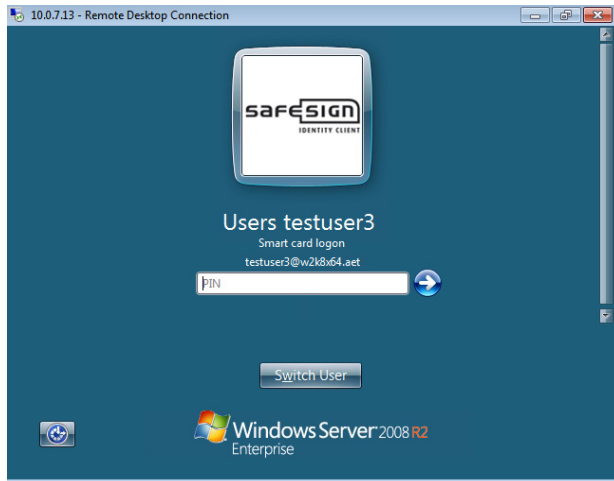


<sup>1</sup> The PKCS#11 specification states: "the set of slots accessible through a Cryptoki library is fixed at the time that C\_Initialize is called. If an application calls C\_Initialize and C\_GetSlotList, and then the user hooks up a new hardware device, that device cannot suddenly appear as a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

### 3.11 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 instead.

Note that the SafeSign Credential Provider does not support PLAP / Single Sign-On<sup>1</sup>. 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.

<sup>1</sup> 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.

### 3.12 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.

### 3.13 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 for Windows provides at least the following end-user documentation:

Document name	Document Version
SafeSign Identity Client Standard 3.0 Release Notes for Windows	1.7
SafeSign Identity Client Standard 3.0 Product Description	1.6
SafeSign Identity Client Standard User Guide for Installation	3.1
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-IC versions 2.3.x.

## 5 Supported and Tested PC Operating Systems

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

Operating System	Version
Windows	Windows XP Professional (SP3)
	Windows XP Embedded
	Windows XP Tablet PC Edition
	Windows 2003 Server (SP2)
	Windows 2003 Server R2 (SP2)
	Windows Vista Ultimate (SP2)
	Windows Vista Business (SP2)
	Windows Vista Enterprise (SP2)
	Windows Server 2008 Enterprise (SP2)
	Windows 7 Professional
	Windows 7 Ultimate

## 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. 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 a small fee, AET can qualify such readers for use with SafeSign Identity Client on request of vendors and customers.

Moreover, the list does not imply that each smart card reader and reader driver listed works with each SafeSign Identity Client supported smart card. For example, the Sm@rtCafé Expert 64K requires an EMV compliant buffer size, which not all readers in the list provide. 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
ACS ACR38-IPC <sup>1</sup>	USB	1	1.1.2.0
ACS ACR38T	USB	1	1.1.2.0
Axalto e-Gate	USB	1	e-gate_W98_Me_24.zip e-gate_W2k_XP_24.zip
Cherry SmartCard Keyboard G83-6700 <sup>2</sup>	RS232	1	SmartBoard_26_US.zip
Cherry SmartCard Keyboard G83-6702 (compatible with CardMan 2020)	USB	1	CardMan2020_6020_V3_7_3_21.exe
Cherry SmartCard Keyboard G83-6744LUA (secure PIN entry, EMV 2000 level 1)	USB	1	CardMan3x21_V1_1_2_4.exe
Cherry SmartCard Keyboard G83-6744LUZ (secure PIN entry, EMV 2000 level 1, certification Common Criteria EAL 3+)	USB	1	CardMan3x21_V1_1_2_4.exe
Cherry SmartTerminal ST-20000U	USB	2	Cherry-SmartDeviceSetup_19_EN.msi
Eutron CryptoIdentity / CryptoCombo ITSEC-P	USB	1	setup_driver.exe (CryptoIdentity5 Drivers)
G&D StarKey100	USB	1	StarKey100V30.exe
G&D StarKey300	USB	1	Omnikey SmartLink_USB_V1_1_1_5 Setup Generic Hot Plug Enabler.zip
G&D StarKey400	USB	1	StarKey100V30.exe
G&D CashMouse* (identical to SCM STR 391) (< SafeSign 3.0.33)	RS232, USB	3	CashMouse Setup V1.64.zip (Firmware 1.35)
GemPlus GemPC430	USB	1	GemPC430_PC_SC_Installer.exe (3.11)
GemPlus GemPC Twin	USB	1	GemPCTwin_PC_SC_Installer.exe (3.14)
HP USB Smart Card Keyboard <sup>3</sup>	USB	1	

<sup>1</sup> ACS readers have been tested by their supplier / reseller or their partner.

<sup>2</sup> Tested by supplier, Cherry GmbH

<sup>3</sup> Model tested: KUS0133

IDPendant IDp 100	USB	1	IDpendantToken.exe (10.0.159)
IDPendant IDp 200	USB	1	Omniquey iccd_V1_0_0_3 Smart Enabler okicddo_1.0.0.0
IDpendant IDp 1000	USB	1	Omniquey SmartLink_USB_V1_1_1_5 Setup Generic Hot Plug Enabler.zip
Marx® CrypToken® MX2048-JCOP	USB	1	CCID compatible
O2Micro OZ776 USB CCID Smartcard Reader <sup>1</sup>	USB	1	1.1.3.9 (+EMV1.3.7.3)
Omniquey CardMan Desktop serial 2011	RS232	1	CardMan2011_V1_0_1_1.exe
Omniquey CardMan Desktop USB 2020	USB	1	CardMan2020_6020_V3_7_3_21.exe
Omniquey CardMan Mobile PCMCIA 4000	PCMCIA	1	CardMan4000_V3_5_0_12.exe
Omniquey CardMan Mobile PCMCIA 4040	PCMCIA	1	CardMan4040_V1_1_0_38.exe
Omniquey CardMan Desktop serial 3110	RS232	1	CardMan3110_V1_0_2_3.exe
Omniquey CardMan Desktop serial 3111	RS232	1	CardMan_3111_V1_1_0_24.exe
Omniquey CardMan Desktop USB 3121	USB	1	OMNIKEY_3x21_V1_2_2_8.exe
Omniquey CardMan Trust* 3610 ( < SafeSign 3.0.33)	RS232	2	CardMan3610_V01_0_2_2.exe
Omniquey CardMan Trust* 3620 ( < SafeSign 3.0.33)	USB	2	CardMan3620_V01_0_3_0.exe
Omniquey CardMan Trust* 3621	USB	2	CardMan3x21_V1_1_2_4.exe
Omniquey 3821 USB pinpad ( ≥ SafeSign 3.0.33)	USB	2	OMNIKEY_3x21_V1_2_2_8.exe
Omniquey CardMan RFID 5121	USB	1	CardMan5x21_V1_1_1_5.exe
Omniquey CardMan 6121	USB	1	CardMan3x21_V1_2_2_8.exe
ORGA CardMouse USB V1.1	USB	1	CardMouse_V2.1.zip
Perto PertoSmart	USB	1	Pusrinst.exe (1.0.0.3)
Reiner-SCT Cyberjack pinpad* ( < SafeSign 3.0.33)	RS232, USB	2	cjBase_V5.5.3.exe + cjPCSC_V2.1.1.exe
Reiner SCT cyber <i>Jack</i> pinpad ( ≥ SafeSign 3.0.33)	USB	2	bc_6_9_6.exe
Reiner SCT cyber <i>Jack</i> e-com ( ≥ SafeSign 3.0.33)	USB	3	bc_6_9_6.exe
Reiner SCT cyber <i>Jack</i> secoder ( ≥ SafeSign 3.0.33)	USB	3	bc_6_9_6.exe
Renesas SecureMMC Reader (JAE USB X Mobile Card Reader PC-RNS7)	USB	1	Setup.exe (1.0.731.0)

<sup>1</sup> Tested on Dell D420 / D620 Latitude notebooks only.

SCM Microsystems SCR241 <sup>1</sup>	PCMCIA	1	SCR241-ENGV.4.02.001
SCM Microsystems SCR131	RS232	1	SCRx31-ENGV.8.00.000
SCM Microsystems SCR331	USB	1	SCRx3xx_4.27.00.01 SCRx31_USB_1.40_signed.zip
SCM Microsystems SCR531 (dual connection)	RS232, USB	1	SCRx31-ENGV.8.00.000
SCM Microsystems SCR335	USB	1	HBCI-SCR335ENGV9.00.002
SCM Microsystems SPR 532 PINpad Reader (≥ SafeSign 3.0.33)	USB	2	SPR532_USB_V4.34_4.45
Todos eCode Connectable 217U (≥ SafeSign 3.0.33)	USB	3	1.0.1.3
ACR38 USB Smart Card Reader/Writer <sup>2</sup>	USB	1	Setup.exe (Version 1.1.5.9)

\*) Note: Supported in versions previous to SafeSign IC version 3.0.33, 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.

<sup>1</sup> All SCM readers have been tested by their supplier, SCM Microsystems.

<sup>2</sup> 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.

## 7 Supported and Tested Hardware Tokens

SafeSign Identity Client Standard version 3.0 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
Eutron CryptoIdentity / CryptoCombo FIPS with G&D STARCOS SPK 2.4 FIPS chip	Smart Card	Test completion: CP5WxSPKI24-01-3-T_V0330 Series completion: CP5WxSPKI24-01-3-S_V0330
Eutron CryptoIdentity / CryptoCombo ITSEC-P with G&D STARCOS SPK 2.3 chip	Smart Card	Test completion: CP5WxSPKI23-1-7-T_V0700 Series completion: CP5WxSPKI23-1-7-S_V0700
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
SafeNet iKey 3000 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 <sup>1</sup>	Smart Card	
G&D STARCOS 3.4	Smart Card	

<sup>1</sup> 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. 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).

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 2000, XP, 2003 Server) 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
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 v2.2 <sup>1</sup>
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

<sup>1</sup> Implemented with support for key generation of 1024 bits only.

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

### 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 SECCOS<sup>1</sup>

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

<sup>1</sup> 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 for Windows has been tested in accordance with AET's Quality Assurance procedures and the SafeSign Identity Client Standard Version 3.0 for Windows test matrix. 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.

Note that this may imply that some of the applications listed below have not been tested explicitly with SafeSign Identity Client Standard Version 3.0 for Windows, if interoperability with regard to PKCS #11 or Microsoft CryptoAPI has been established with previous versions of these applications in combination with SafeSign Identity Client (on the assumption that PKCS #11 / Microsoft CryptoAPI interoperability remained stable).

### 8.1 Public Key Infrastructure

Public key Infrastructure	
Application	<a href="#">Baltimore</a> UniCERT CA
Application version	3.5.3
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	<a href="#">Entrust</a> Authority: Security Manager
Application version	6.0.1, 7.0
Supported by SafeSign-IC versions	1.0.9.04-Update, 2.0, 2.1, 2.2, 2.3, 3.0
Application	<a href="#">Entrust</a> Authority: Self-Administration Server
Application version	6.0
Supported by SafeSign-IC versions	1.0.9.04-Update, 2.0, 2.1, 2.2, 2.3, 3.0
Application	Computer Associates <a href="#">eTrust</a> PKI (tested by partner)
Application version	1.0
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	<a href="#">GlobalSign</a>
Application version	N/A (Not Applicable)
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	<a href="#">Microsoft</a> Standalone and Enterprise Certificate Server
Application version	Windows 2000, Windows 2003 Server <sup>1</sup> , Windows 2008 Server <sup>2</sup>
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	<a href="#">RSA</a> Keon PKI
Application version	4.7, 5.7, 6.0, 6.5
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	<a href="#">SafeGuard</a> PKI (tested by supplier: Utimaco)
Application version	2.50 and up
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	<a href="#">Safelayer</a> KeyOne <sup>®</sup> product family <sup>3</sup> (tested by supplier: Safelayer)
Application version	2.1
Supported by SafeSign-IC versions	1.0.9.04, 1.0.9.04-Update, 2.0, 2.1, 2.2, 2.3, 3.0


<sup>1</sup> Windows 2003 Server key archival is not supported.

<sup>2</sup> Windows 2008 Server is supported from SafeSign IC version 3.0.33 onwards.

<sup>3</sup> Only those components requiring PKCS#11 interface, which includes certificate management modules: KeyOne<sup>®</sup> CA, KeyOne<sup>®</sup> LRA and KeyOne<sup>®</sup> Register components.

Application	<a href="#">SECUDE</a> Trustmanager Enterprise (tested by supplier)
Application version	5.9.2
Supported by SafeSign-IC versions	2.1, 2.2, 2.3, 3.0
Application	<a href="#">Verisign</a> Key Manager
Application version	3.0
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	<a href="#">Verisign</a> Managed PKI Manager
Application version	5.0
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	<a href="#">Verisign</a> Public / Private CA
Application version	N/A (Not Applicable)
Supported by SafeSign-IC versions	1.0.9.04, 1.0.9.04-Update, 2.0, 2.1, 2.2, 2.3, 3.0

## 8.2 Client Applications

Client Applications	
Application	<a href="#">Baltimore</a> MailSecure
Application version	3.1.1
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	<a href="#">Checkpoint</a> VPN  (VPN-1 SecuRemote / SecureClient)
Application version	NG FP3, R56, R60, R65
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	<a href="#">Cisco</a> VPN client (tested by supplier: Cisco)
Application version	3.6
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	<a href="#">Citrix</a> MetaFrame XP Server
Application version	FR3/SP3
Supported by SafeSign-IC versions	2.0, 2.1, 2.2, 2.3, 3.0
Application	<a href="#">Citrix</a> MetaFrame Presentation Server
Application version	3.0, 4.0, 4.5
Supported by SafeSign-IC versions	2.1, 2.2, 2.3, 3.0
Application	<a href="#">Digitronic</a> Authentication (tested by partner)
Application version	2.0.1
Supported by SafeSign-IC versions	2.0, 2.1, 2.2, 2.3, 3.0
Application	<a href="#">Control Break</a> SafeBoot
Application version	4.2
Supported by SafeSign-IC versions	2.0, 2.1, 2.2, 2.3, 3.0
Application	<a href="#">E-Lock</a> ProSigner
Application version	6.1.2.0, 6.1.3
Supported by SafeSign-IC versions	2.0 (≥ version 2.0.3 <sup>1</sup> ), 2.1, 2.2, 2.3, 3.0

<sup>1</sup> Supported by SafeSign Identity Client version 2.0.3, which takes into account certain expectations of the ProSigner application with regard to encryption algorithms.

Application	<a href="#">Entrust</a> Entelligence: Desktop Manager, E-mail Plug-in, File Plug-in, Web Plug-in <sup>1</sup>
Application version	6.1 SP1
Supported by SafeSign-IC versions	1.0.9.04-Update, 2.0, 2.1, 2.2, 2.3, 3.0
Application	<a href="#">Entrust</a> Entelligence: Security Provider
Application version	7.0
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	<a href="#">Entrust</a> TruePass: TruePass
Application version	6.0
Supported by SafeSign-IC versions	1.0.9.04-Update, 2.0, 2.1, 2.2, 2.3, 3.0
Application	<a href="#">eTrust</a> SSO (tested by partner)
Application version	6,5 SP2
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	<a href="#">Gemplus</a> eSigner Integrator package
Application version	2.0
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	<a href="#">IBM</a> Lotus Notes (Tested by partner)
Application version	6.01, 6.5
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	<a href="#">Microsoft</a> CAPICOM
Application version	2.0
Supported by SafeSign-IC versions	1.0.9.04, 1.0.9.04-Update, 2.0, 2.1, 2.2, 2.3, 3.0.33
Application	<a href="#">Microsoft</a> Internet Explorer
Application version	5.0, 5.5, 6.0, 7.0, 8.0
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	<a href="#">Microsoft</a> Outlook
Application version	98, 2000, XP, 2003, 2007, 2010
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	<a href="#">Microsoft</a> Outlook Express
Application version	5.0, 5.5, 6.0
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	<a href="#">Microsoft</a> Outlook Web Access
Application version	Exchange Server 5.0 and higher
Supported by SafeSign-IC versions	2.1 (≥ release 2.1.6), 2.2, 2.3, 3.0
Application	<a href="#">Microsoft</a> VPN
Application version	Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 2003, Windows 2008
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	<a href="#">Microsoft</a> Windows Mail
Application version	6.0
Supported by SafeSign-IC versions	3.0
Application	<a href="#">Microsoft</a> Office
Application version	2007, 2010
Supported by SafeSign-IC versions	3.0.40

<sup>1</sup> Formerly known as Entrust/Direct, this product is now a component of the Entrust Entelligence product portfolio.

Application	<a href="#">Mozilla</a> Firefox
Application version	1.0.x, 1.5, 2.0, 3.0, 3.5, 3.6
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	<a href="#">Mozilla</a> Mail
Application version	1.3.1, 1.4, 1.7.x
Supported by SafeSign-IC versions	1.0.9.04, 1.0.9.04-Update, 2.0, 2.1, 2.2, 2.3
Application	<a href="#">Mozilla</a> Navigator
Application version	1.3.1, 1.4, 1.7.x
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	<a href="#">Mozilla</a> Thunderbird
Application version	1.0.x, 1.5, 2.0, 2.0.0.23, 3.1
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	<a href="#">NCP</a> VPN/PKI Client
Application version	7.21, 8.0, 8.05, 8.22
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	<a href="#">Netscape</a> Navigator
Application version	4.72 - 4.79, 4.8, 7.1 <sup>1</sup> , 8.02
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	<a href="#">Netscape</a> Messenger
Application version	4.72 - 4.79, 4.8, 7.1
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	<a href="#">Nortel</a> Networks Contivity VPN client
Application version	6.02
Supported by SafeSign-IC versions	2.3, 3.0
Application	<a href="#">Novell</a> Groupwise 6.0 client
Application version	6.0
Supported by SafeSign-IC versions	1.0.9.04, 1.0.9.04-Update, 2.0, 2.1, 2.2, 2.3
Application	<a href="#">Novell</a> NMAS
Application version	2.0
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	<a href="#">OpenDomain</a> Sphinx Logon Manager
Application version	Sphinx Standalone, Sphinx Enterprise, Sphinx Enterprise PKI
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	<a href="#">PGP</a> Corporate Desktop
Application version	7.1, 8.0, 8.02, 8.1, 9.0x
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	<a href="#">PKWare</a> SecureZIP
Application version	v8
Supported by SafeSign-IC versions	2.1 (≥ release 2.1.6), 2.2, 2.3, 3.0
Application	<a href="#">Pointsec</a> PC for Windows 6.3.1
Application version	6.3.1
Supported by SafeSign-IC versions	2.3 (≥ release 2.3.6), 3.0
Application	<a href="#">Protocom</a> SecureLogin SSO (Tested by supplier: Protocom)
Application version	3.5.1, 3.6
Supported by SafeSign-IC versions	2.0, 2.1, 2.2, 2.3, 3.0

<sup>1</sup> Netscape 7.02 has been tested, but has proved to be not very stable; therefore it is not (officially) supported.

Application	<a href="#">Protocom</a> SecureLogin Advanced Authentication (tested by supplier: Protocom)
Application version	1.90
Supported by SafeSign-IC versions	2.0, 2.1, 2.2, 2.3, 3.0
Application	<a href="#">RSA SecurID</a>
Application version	2.51, 3.0
Supported by SafeSign-IC versions	1.0.9.04-Update, 2.0, 2.1, 2.2, 2.3, 3.0
Application	<a href="#">SafeGuard</a> PrivateDisk
Application version	All versions
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	<a href="#">SafeGuard</a> Sign & Crypt (tested by supplier: Utimaco) for Office
Application version	3.00 and up
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	<a href="#">SafeGuard</a> Sign & Crypt (tested by supplier: Utimaco) for Outlook
Application version	3.00 and up
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	<a href="#">SafeGuard</a> Sign & Crypt (tested by supplier: Utimaco) for Lotus Notes
Application version	3.10 and up
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	<a href="#">SafeGuard</a> Transaction Client (tested by supplier: Utimaco)
Application version	3.0 and up
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	<a href="#">SafeNet</a> SoftRemote (VPN client) (tested by partner)
Application version	8.0.0
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	<a href="#">SECUDE</a> signon (tested by supplier)
Application version	5.9.2
Supported by SafeSign-IC versions	2.1, 2.2, 2.3, 3.0
Application	<a href="#">SECUDE</a> signon & secure (tested by supplier)
Application version	4.2.7
Supported by SafeSign-IC versions	2.1, 2.2, 2.3, 3.0
Application	<a href="#">SECUDE</a> FinallySecure (tested by supplier)
Application version	9.1
Supported by SafeSign-IC versions	2.1, 2.2, 2.3, 3.0
Application	<a href="#">SSH</a> Tectia Client (formerly known as Secure Shell for Workstations) (tested by supplier)
Application version	3.2, 4.2
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	Windows Terminal Server
Application version	Windows Server 2003
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	Windows Terminal Server
Application version	Windows Server 2008
Supported by SafeSign-IC versions	3.0
Application	<a href="#">Winmagic</a> SecureDoc
Application version	4.1
Supported by SafeSign-IC versions	2.1, 2.2, 2.3, 3.0