aet europe

SafeSign Identity Client Minidriver Version 4.1

Release Document for Windows

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

trust accelerates growth

Warning Notice

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

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

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

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

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

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

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

Credit Information:

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

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

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

aet europe

Table of Contents

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

Document Information

Document ID: SafeSign IC Minidriver Version 4.1 Release Document for Windows
Project Information: SafeSign IC Release Documentation

Document revision history:

Version	Date	Author	Changes
1.0	12 March 2024	Drs. C.M. van Houten	First version for SafeSign IC Minidriver version 4.1 for Windows; release 4.1.0.0-AET.000

Document Approval:

Version	Date	Name	Function
1.0	15 March 2024	Dr. A.J.P. Jeckmans	Chief Technology Officer

WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

About the Product

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

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

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

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

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

1 About this Document

The aim of this document is to document the status of the release of SafeSign Identity Client Minidriver version 4.1 for Windows (henceforth referred to as “SafeSign IC Minidriver version 4.1”).

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

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

2 Release Information

2.1 Deliverables

SafeSign IC Minidriver version 4.1 is provided as a .msi installation file.

The InstallShield Wizard will guide you through the installation of SafeSign IC Minidriver version 4.1.

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

SafeSign IC Minidriver version 4.1 includes the Token Administration Utility user interface for local smart card operations, such as Change PIN.

2.2 Date of Release

The date of the release is 15 March 2024.

2.3 Release Details

SafeSign IC Minidriver version 4.1 reflects the SafeSign IC product version numbering scheme, i.e. version number, build number and distribution number, which is reflected in the Version Information dialog of the Token Administration Utility.

- Note that the file versions of the components delivered with the release of SafeSign IC Minidriver version 4.1.0.0 do not necessarily have the name format '4.1.0.xxxx'.

Release version: Minidriver Release 4.1.0.0-AET.000		
Description	File Name	File Version
Certificate Expiration Check Utility	aetcrss1.exe	3.7.16.1
Common Dialogs	aetdlss1.dll	3.7.20.1
Java Card Handling Library	aetjcss1.dll	3.9.8.1
PKCS #11 Cryptoki Library	aetpkss1.dll	3.9.21.1

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

Release version: Minidriver Release 4.1.0.0-AET.000		
PKCS #11 Library Wrapper with automatic login	aetpkssw.dll	3.7.14.1
Task Manager	aettask.dll	3.9.20.1
Secure Messaging Library	aetsm1.dll	3.9.16.1
Kit Library	aetkit1.dll	4.1.11.1
Read/write card-module	aetrwcm1x.dll (64-bit) aetrwcm1.dll (32-bit)	4.7.1.1
Read-only card-module	aetrocm1x.dll (64-bit) aetrocm1.dll (32-bit)	4.7.0.1
Token Administration Utility	tokenadmin.exe	3.8.43.1

- Note that in the distribution number (AET.000), the prefix AET is unique and reserved for AET general releases only.
- Note that when saving the version information to a file, there may be components listed that are not available in the SafeSign IC version installed. For example, in SafeSign IC Minidriver version 4.1, the Credential Provider 'aetcpss1.dll' is listed, but as 'not installed'.

2.4 Windows 64-bit

SafeSign IC Minidriver version 4.1 comes in a 64-bit version only (which does not install on 32-bit Windows Operating Systems) that will work with both 32-bit and 64-bit applications.

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

SafeSign IC Minidriver version 4.1 system files will install in both directories (to ensure that both 32-bit and 64-bit applications can work with SafeSign IC), with the following exceptions, which are installed in the System32 directory only:

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

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

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

2.5 Release Documents

SafeSign IC Minidriver version 4.1 provides at least the following release documentation:

Document Name	Version
SafeSign IC Minidriver 4.1 Release Document	1.0

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

3 Features

The following features are supported by SafeSign IC Minidriver version 4.1:

1 Multiple Token Support
2 Multiple Smart Card Reader Support
3 Multiple Application Support
4 Multiple Language Support
5 Activate QSCD Card Support
6 RSA 4096-bit Key Support
7 ECC Key Support
8 Microsoft WHQL certified (read-only) Minidriver

These features are described in the following paragraphs.

3.1 Multiple Token Support

SafeSign IC Minidriver version 4.1 supports a large number of smart cards and tokens, as listed in section 7.

SafeSign IC Minidriver version 4.1 now includes support for NXP JCOP 4 and JCOP 4.5 (non-QSCD ATRs).

3.2 Multiple Smart Card Reader Support

SafeSign IC Minidriver version 4.1 supports the use of PC/SC v2.0 Class 1 smart card readers.

SafeSign IC Minidriver version 4.1 now includes support for the Neowave Linkeo-Y and Winkeo-A SIM smart card reader for extended APDU. See section 3.6 with regard to smart card readers and extended APDU.

SafeSign IC Minidriver version 4.1 has been tested to support a number of smart card readers, as listed in section 8.

3.3 Multiple Application Support

SafeSign IC Minidriver version 4.1 supports applications on Windows that work through PKCS #11 or Microsoft CryptoAPI (NG).

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

SafeSign IC Minidriver version 4.1 supports a number of applications, that provide the following functionality:

- Web authentication
- Email signing and encryption
- Document signing
- Smart card logon[1]
- Terminal Server logon

SafeSign IC Minidriver version 4.1 has been tested to support a number of applications, as listed in section 9.

3.4 Multiple Languages Support

SafeSign IC Minidriver version 4.1 supports a number of different languages.

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

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

3.5 Activate QSCD Card Support

In accordance with the (European) eIDAS Regulation and related standards for cryptographic modules, the legitimate user/signatory of a Qualified Signature Creation Device (QSCD) is responsible for activating the card (keys), i.e. to change the state of the card (keys) from non-operational to operational.

The SafeSign IC Token Administration Utility offers users of a QSCD the possibility to activate their card. When a QSCD is inserted in the smart card reader, the SafeSign IC middleware will enable the user to activate the card, based on the presence of the Common Criteria (CC) certified SafeSign IC applet and the card-specific ATR. If these conditions are met, the Token menu of the SafeSign IC Token Administration Utility will display the option 'Activate Card'.

- Note that the activation process for a particular card may be very specific. It may require the user to:
  - authenticate to the card by entering the PIN (UZI-pas 3, UZI-pas 4 and SafeSign QSCD);

[1] For smart card logon and terminal server logon, refer to section 9.10 and 9.11.

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

- change the Transport PIN set for the card (Defensiepas 3);

SafeSign IC Minidriver version 4.1 supports the following QSCD cards:

- Defensiepas 3[2]
- UZI-pas 3[3]
- SafeSign Default/Generic QSCD (JCOP 3)
- UZI-pas 4
- QSCD on JCOP 4

3.6 RSA 4096-bit Key Support

SafeSign IC Minidriver version 4.1 includes support for RSA 4096-bits keys.

Note that support for RSA 3072-bits keys is also included.

This functionality requires one of the following cards/tokens:

- A JCOP 4 QSCD card with the Common Criteria (CC) certified SafeSign IC applet (i.e. applet version 3.0.1.12 or 3.0.1.13) and a smart card reader that supports extended APDU.
- A G+D Sm@rtCafe Expert 7.0 FIPS card with SafeSign IC (StdR) applet (i.e. applet version 3.1.0.36 or 3.1.0.37).
- A G+D Sm@rtcafe Expert 7.0 CUT S (M) USB token with SafeSign IC (StdR) applet (i.e. applet version 3.1.0.35, 3.1.0.36 or 3.1.0.37).

Note that applet version 3.1.0.37 supports secure messaging for Brazil.

3.6.1 Extended APDU

An extended APDU is an APDU (command) with data and/or response of more than 256 bytes, as defined by ISO/IEC 7816-4.

Because sending extended APDUs can cause issues with readers/drivers that do not support it (such as the reader or drivers crashing), a whitelist is added in the registry with the names of the readers tested and are supported, that indicates per reader what the maximum APDU size possible is. When your reader is not in the list, the use of extended APDU is not possible.

[2] Defensiepas 3 is supported from SafeSign IC Minidriver version 3.5.4.0 onwards.
[3] UZI-pas 3 is supported from SafeSign IC Minidriver version 3.5.6.1 onwards.

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

- Note that the G+D Sm@rtCafe Expert 7.0 FIPS card does not need a smart card reader with extended APDU support for RSA 3072-bits and 4096-bit keys, as the applet supports command chaining.

The whitelists can be found here:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\A.E.T. Europe B.V.\SafeSign\2.0\Readers
```

⚠ These readers are verified by AET to work on all Operating Systems supported and must not be modified.

See also section 8.1.

3.7 ECC Key Support

SafeSign IC Minidriver version 4.1 includes support for ECC keys.

For this functionality to be available, the following is required:

- A JCOP 4 QSCD card with the Common Criteria (CC) certified SafeSign IC applet (i.e. applet version 3.0.1.13).
- A G+D Sm@rtCafe Expert 7.0 FIPS card with SafeSign IC (StdR) applet (i.e. applet version 3.1.0.36 or 3.1.0.37).
- A G+D Sm@rtcafe Expert 7.0 CUT S USB token with SafeSign IC (StdR) applet (i.e. applet version 3.1.0.36 or 3.1.0.37).

- Note that applet version 3.1.0.37 supports secure messaging for Brazil.

The following NIST named curves are supported:

- P-256
- P-384
- P-521

The following algoritms are supported for these curves:

- ECDSA
- ECDH

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

3.8 Microsoft WHQL certified (read-only) Minidriver

In/from Windows 11 22H2, Microsoft has made changes with regard to security, among which a more strict security with regard to authentication providers that are loaded into Local Security Authority Subsystem Service (LSASS) during logon to Windows.

This additional protection results in users of SafeSign IC not to be able to use their smart card for logon to local or remote connections on Windows (in which the Minidriver is involved), because the SafeSign IC (read/write) Minidriver is not Microsoft certified/signed.

With the release of SafeSign IC Minidriver version 4.1, we included the SafeSign read-only Minidriver that passed the Windows Hardware Lab Kit (HLK) testing and is digitally signed by WHQL.

This makes the SafeSign IC read-only Minidriver fully trusted in Windows, allowing smartcard logon.

Which Minidriver you need to install, depends on what purpose it needs to serve:

- The read-only Minidriver is ideal for essential tasks, such as authentication, smart card logon and secure remote access. It does not support key generation and certificate installation.
- The read/write Minidriver is best suited for comprehensive security operations such as key generation and certificate management.

By default, SafeSign IC Minidriver version 4.1 will install the read-only Minidriver, but the installation file allows you to install either the read-only (aetrocm) or read/write (aetrwcm) Minidriver or both.

- Note that you will have to uninstall both the SafeSign IC Card Minidriver and the SafeSign IC software (as described in the Installation Guide) to change the installation of either the read-only or read/write Minidriver.

When you install both the read-only and read/write Minidriver, only the read-only Minidriver .dll files will be installed in the system directories (System32/SysWOW64). In addition, in the Microsoft\Cryptography\Calais\SmartCards registry key, all ATRs will by default be associated with the read-only Minidriver.

The read/write Minidriver .dll files will be placed in ProgramData\A.E.T. Europe B.V\SafeSign IC\Minidriver\readwrite directory. If you want to use your card with the read/write Minidriver (e.g. for enrollment), you need to edit the registry entry for this particular card in the Microsoft\Cryptography\Calais\SmartCards registry key to contain the full path to the read/write Minidriver file. How to do this is described in the Administrators' Guide.

- Please note that although you can select both versions to be installed on your system, we strongly recommend you not to do so. We recommend that the read/write Minidriver is installed on

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

enrollment stations, whereas the read-only Minidriver is installed on users' workstations (as it allows for smart card logon) and on Terminal Servers (to allow for remote logon).

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

4 New Features and Fixes

SafeSign IC Minidriver version 4.1 has a number of new features and fixes/changes.

Section 4.1 will describe the new features and functionality.

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

4.1 New

- Added support for JCOP 4 P71 default/non-QSCD ATR.
- Added support for JCOP 4.5 default/non-QSCD (model and ATR).
- Some customers need to personalise JCOP (default) QSCD cards with user keys and certificates, which required a special SafeSign IC PKCS #11 Library that is able to generate non-operational keys. In order to prevent customers from having to use multiple libraries, we have implemented a registry switch, whose default setting is to create operational keys. The DWORD value is named '*NonOperationalKeysPkcs11*' and should be located in `HKEY_LOCAL_MACHINE\Software\A.E.T. Europe B.V.\SafeSign\2.0`. If not present, or set to 0, operational keys will be generated. When set to 1, non-operational keys will be generated.
- Added support for Neowave Winkeo-A SIM reader (for use with extended APDU).
- Added support for Neowave LinkeoA-Y smart card reader (for use with extended APDU).
- Added support for RSA and ECC key import in the Minidriver.

4.2 Fixed

- There was an issue in previous SafeSign IC Minidriver versions, that the token information of a locked token (with both PUK and PIN locked) was not displayed properly. Instead, the TAU would display "No token present in this slot". This has been fixed.
- SafeSign IC has been updated to use OpenSSL 3.0.x, in order to solve any potential vulnerabilities/issues with earlier versions.
- There was an issue in SafeSign IC Minidriver Version 4.0, that when deleting an ECC key through Delete Digital ID in the Token Administration App, the ECC key is not deleted, although a message says it is deleted successfully. This has been fixed.

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

5 Known Issues

5.1 General

- Firefox cannot handle a certificate that does not have a label. As a workaround, you can set a label on the keys and certificate in the Token Administration Utility's Show Token Objects dialog.
- As of Mozilla Firefox version 90, Firefox will automatically find and offer to use client authentication certificates provided by the operating system on Windows. See: https://blog.mozilla.org/security/2021/07/28/making-client-certificates-available-by-default-in-firefox-90/. As a consequence, it is no longer necessary to install the SafeSign IC PKCS #11 Library as a security module in Firefox.
- Encrypting and/or decrypting an e-mail message with an ECC key/certificate using the SafeSign IC PKCS #11 library installed as a security module in Thunderbird results in an error message (unable to encrypt message). This issue was reproduced with an ECC key generated in software as well and other evidence seems to point to this being a limitation within Thunderbird. It is expected that Thunderbird will start working once it has been implemented properly.
- Receiving an RSA-signed and encrypted message in Thunderbird with a G+D Sm@rtCafe Expert 7.0 card or token with SafeSign IC RIC applet (e.g. applet version 3.1.0.14 or 3.1.0.37) with secure messaging enabled, fails. Thunderbird reports that it cannot decrypt the message. Note that previous versions of Thunderbird (including that for testing the release of SafeSign IC Minidriver 4.0, i.e. 102.9.0) may work.

5.2 SafeSign IC

- When generating/importing a Digital ID file or certificate and the message that the token is full (out of memory: 0x80090023) is displayed, it may be that the whole or parts of the Digital ID file (and certificate chain) or the certificate have been placed on the smart card nevertheless. This will be clearly visible in the Token Administration Utility (Show Token Objects).
- When initialising or wiping a token with Root CA certificates, you can only select a particular directory. It is not possible to select a particular file.
- When importing a CA certificate file (either during initialisation or by the function Import Certificate), *.crt files are not selected by the default file extensions (*.cer, *.der), although the import does work.
- When creating a data object containing no data (done by using an empty CKA_VALUE), an error occurs (CKR_DEVICE_ERROR). According to the PKCS #11 standard, it is allowed to leave the CKA_VALUE empty. Although the SafeSign PKCS #11 implementation correctly handles the empty CKA_VALUE, the command to create the file fails. As a workaround, a null-byte should be used instead of an empty byte.

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

- The Token Utility will only display and register Digital IDs that have a private key. When requesting a new Digital ID, the Token Utility may not display the new Digital ID with the green card icon. This is caused by the fact that the Minidriver does not update the token cache. This is a display issue only (the keys and certificates are stored on the token) and it does not affect the functionality of the SafeSign IC Minidriver/the Digital ID in any way.
- Starting from Windows 8, the way smart cards are handled, has changed. Most notably, if a transaction is started and no activity happens for 5 seconds, the transaction (and card) are automatically reset. This has consequences for enrolling a certificate with Microsoft FIM/MIM using the Microsoft Base Smart Card CSP (see the SafeSign IC Administrator's Guide) and for T=0 cards (see known issue below).
- In languages other than English, some items in the Version Information dialog are not translated (e.g. Build number, Distribution number and the names of the Secure Messaging libraries).
- When enabling the registry setting GenerateEventLogs (in `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\A.E.T. Europe B.V.\SafeSign\2.0`), events will be logged (such as incorrect PIN attempts), but also an error (EventID 258) will occur. This has been the case in previous SafeSign IC Minidriver versions as well.
- The copyright text in the About dialog (both in English and in foreign languages) may not be displayed in full.
- The NXP JCOP 4.5 is only supported in the SafeSign IC read/write Minidriver.
- During installation, the Custom Setup window will only include localisation of the read-only and read/write Minidriver components in Dutch, German, Portuguese, Brazilian Portuguese, Serbian Latin and Serbian Cyrillic.
- Note that on Windows 11 22H2/23H2, smart card logon fails on a G+D Sm@rtCafe Expert 7.0 CUT S token with SafeSign IC RIC applet (e.g. applet version 3.1.0.14, 3.1.0.16 or 3.1.0.37) with secure messaging enabled.
- The Readers and Readers.rocm whitelists in the registry are not an exact match. The Readers.rocm whitelist does not include the Neowave WinkeoSIM Reader, for example, but this reader is supported with extended APDU nevertheless.
- When setting up a connection to a remote Terminal Server and authenticating locally on the client, the error "No credentials are available in the security package" is shown with a smart card associated with read/write Minidriver (whether though installation or manually in Program Data).

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

6 Supported Operating Systems

SafeSign IC Minidriver version 4.1 has been tested to support the following x64 Windows Operating System(s):

Operating System	Version 4.1.0.0
Windows 10 (Pro, Enterprise)	√
Windows 11 (Pro)	√
Windows Server 2019	√
Windows Server 2022	√

Like every SafeSign IC release, SafeSign IC Minidriver version 4.1 was tested on the abovementioned Windows Operating Systems with the (latest) Service Pack and Updates available at that time. Though SafeSign IC Minidriver version 4.1 may work on older/other versions of these Operating Systems, only support requests for issues reproduced on the supported Windows Operating Systems listed above (up-to-date with the latest Windows Updates) will be taken into consideration.

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

7 Supported Tokens

SafeSign IC Minidriver version 4.1 supports a number of smart cards and tokens, as listed below.

These tokens have been tested to work as part of the release testing for SafeSign IC Minidriver version 4.1.

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

As the correct functioning of SafeSign IC is depending on a properly produced smart card or USB Token, AET requires that smart cards and/or USB tokens are produced for use with SafeSign IC in accordance with our QA policies (which require i.a. the correct applet to be pre-installed in a secure environment and a custom keyset). This is a condition to be eligible for support by AET in case of problems, in addition to the purchase/existence of a valid SafeSign IC Support Agreement.

Card Type
Defensiepas 2
Defensiepas 3 (QSCD)
G&D Sm@rtCafé Expert 3.2
G&D Sm@rtCafé Expert 4.0
G&D Sm@rtCafé Expert 5.0
G&D Sm@rtCafé Expert 6.0
G&D Sm@rtCafé Expert 7.0
Gemalto IDCore 30
Infineon Oracle JCOS Ed.1
JCOP21 v2.3
NXP J2A080/J2A081 (JCOP 2.4.1 R3)
NXP J2D081 (JCOP 2.4.2 R2)
NXP J3A080 (JCOP 2.4.1 R3)
NXP JCOP 2.4.2 R3
NXP JCOP 3 SecID P60

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

Card Type
NXP JCOP 4 P71
NXP JCOP 4.5
Oberthur IDone Cosmo v7.0
RDW ABR kaart
Rijkspas
Rijkspas 2
StarSign Crypto USB Token S
UZI-pas 2
UZI-pas 3 (QSCD)
UZI-pas 4 (QSCD)

7.1 Supported ATRs

Below you will find a complete list of the ATRs supported by SafeSign IC Minidriver version 4.1.

Card Name	ATR
Changingtec JCOP	3b,f8,18,00,ff,81,31,fe,45,00,73,c8,40,00,00,90,00,7f
Defensiepas 2	3b,f9,18,00,00,81,31,fe,45,39,35,32,38,35,30,31,33,32,d9
Defensiepas 3	3b,dc,18,ff,81,91,fe,1f,c3,06,0a,2b,06,01,04,01,e9,10,05,01,03,d2
G&D Sm@rtCafe Expert 3.2 (T=CL) DSV	3b,7a,18,00,00,73,66,74,65,20,63,64,31,34,34
G&D Sm@rtCafe Expert 3.2 72k	3b,f7,18,00,00,80,31,fe,45,73,66,74,65,2d,6e,66,c4
G&D Sm@rtCafe Expert 3.2 80k	3b,fd,18,00,00,80,31,fe,45,73,66,74,65,2d,63,64,30,38,30,2d,6e,66,dc
G&D Sm@rtCafe Expert 3.2 FI	3b,fd,18,00,00,80,31,fe,45,73,66,74,65,20,63,64,31,34,34,2d,6e,66,d8
G&D Sm@rtCafe Expert 3.2 FI (T=CL)	3b,8d,80,01,73,66,74,65,20,63,64,31,34,34,2d,6e,66,3b
G&D Sm@rtCafe Expert 4.0	3b,78,13,00,00,00,73,c8,40,13,00,90,00
G&D Sm@rtCafe Expert 4.0 FI	3b,f8,18,00,00,80,31,fe,45,00,73,c8,40,13,00,90,00,92
G&D Sm@rtCafe Expert 4.0 FI (T=CL)	3b,88,80,01,00,73,c8,40,13,00,90,00,71

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

Card Name	ATR
G&D Sm@rtCafe Expert 5.0 (T=CL)	3b,89,80,01,53,46,2d,34,43,43,2d,30,31,28
G&D Sm@rtCafe Expert 6.0 (USB Token)	3b,fd,18,00,00,81,31,fe,45,53,43,45,36,30,2d,43,43,30,38,31,2d,46,c2
G&D Sm@rtCafe Expert 6.0 FIPS	3b,fd,18,00,00,80,31,fe,45,53,43,45,36,30,2d,43,44,30,38,31,2d,46,c4
G&D Sm@rtCafe Expert 6.0 FIPS (T=CL)	3b,8d,80,01,53,43,45,36,30,2d,43,44,30,38,31,2d,46,27
G&D Sm@rtCafe Expert 6.0 FIPS 144k (T=CL)	3b,8d,80,01,53,43,45,36,30,2d,43,44,31,34,35,2d,46,2e
G&D Sm@rtCafe Expert 6.0 Non FIPS	3b,fe,18,00,00,80,31,fe,45,53,43,45,36,30,2d,43,44,30,38,31,2d,6e,46,a9
G&D Sm@rtCafe Expert 6.0 Non FIPS (T=CL)	3b,8e,80,01,53,43,45,36,30,2d,43,44,30,38,31,2d,6e,46,4a
G&D Sm@rtCafe Expert 6.0 Non FIPS 144k	3b,fe,18,00,00,80,31,fe,45,53,43,45,36,30,2d,43,44,31,34,35,2d,6e,46,a0
G&D Sm@rtCafe Expert 6.0 Non FIPS 144k (T=CL)	3b,8e,80,01,53,43,45,36,30,2d,43,44,31,34,35,2d,6e,46,43
G&D Sm@rtCafe Expert 7.0 CC	3b,f9,96,00,00,80,31,fe,45,53,43,45,37,20,00,00,20,20,27
G&D Sm@rtCafe Expert 7.0 CC (T=CL)	3b,89,80,01,53,43,45,37,20,00,00,20,20,4a
G&D Sm@rtCafe Expert 7.0 FIPS	3b,f9,96,00,00,80,31,fe,45,53,43,45,37,20,03,00,20,46,42
G&D Sm@rtCafe Expert 7.0 FIPS (T=CL)	3b,89,80,01,53,43,45,37,20,03,00,20,46,2f
G&D Sm@rtCafe Expert 7.0 NXP	3b,f9,96,00,00,80,31,fe,45,53,43,45,37,4e,58,50,20,20,41
G&D Sm@rtCafe Expert 7.0 NXP (T=CL)	3b,89,80,01,53,43,45,37,4e,58,50,20,20,2c
Gemalto IDCore 30	3b,7f,96,00,00,80,31,80,65,b0,84,41,3d,f6,12,00,4c,82,90,00
HID Crescendo C700	3b,df,18,ff,81,31,fe,45,80,59,01,80,48,49,44,43,37,30,30,73,00,01,1b,33
Infineon Oracle JCOS Ed.1	3b,fd,96,00,00,80,31,fe,45,53,4c,4a,35,32,47,78,78,79,79,79,7a,52,25
JCOP21 v2.3.1 (Winter AG)	3b,fa,18,00,ff,81,31,fe,45,4a,43,4f,50,32,31,56,32,33,31,65
NXP J2A080 (Winter AG GTN)	3b,fd,18,00,00,81,31,fe,45,06,0b,60,84,10,01,87,6b,01,03,05,04,02,fb
NXP J2A080-J3A080 (TA1=96)	3b,f8,96,00,ff,81,31,fe,45,4a,43,4f,50,76,32,34,31,cd
NXP J2A080-J3A080 (Winter AG)	3b,f8,18,00,ff,81,31,fe,45,4a,43,4f,50,76,32,34,31,43
NXP J2D081	3b,f5,13,00,00,81,31,fe,45,73,74,64,31,30,8f
NXP J3A080	3b,f8,13,00,00,81,31,fe,45,4a,43,4f,50,76,32,34,31,b7
NXP J3D081 (T=CL)	3b,89,80,01,4a,43,4f,50,32,34,32,52,32,4a

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

Card Name	ATR
NXP JCOP 2.4.2 R3 (Austriacard)	3b,f9,18,00,00,81,31,fe,45,4a,43,4f,50,32,34,32,52,33,a9
NXP JCOP 2.4.2 R3 (exceet Card AG)	3b,f9,18,00,ff,81,31,fe,45,4a,43,4f,50,32,34,32,52,33,56
NXP JCOP 3 SecID P60	3b,dc,18,ff,81,91,fe,1f,c3,80,73,c8,21,13,66,05,03,63,51,00,02,50
NXP JCOP 4 P71	3b,dc,18,ff,81,91,fe,1f,c3,06,0a,2b,06,01,04,01,e9,10,04,01,04,d4
NXP JCOP 4.5	3b,dc,18,ff,81,B1,fe,45,1f,c3,06,0a,2b,06,01,04,01,e9,10,04,01,05,b0
Oberthur IDone Cosmo v7.0.1	3b,db,96,00,80,b1,fe,45,1f,83,00,31,c0,64,1a,18,01,00,07,90,00,5a
Oberthur IDone Cosmo v7.0.2	3b,db,96,00,80,b1,fe,45,1f,83,00,31,c0,64,1f,18,01,00,01,90,00,59
QSCD on JCOP 4 P71	3b,db,18,ff,81,91,fe,1f,c3,06,09,2b,06,01,04,01,e9,10,05,04,d0
RDW ABR kaart	3b,fa,18,00,00,81,31,fe,45,06,08,2a,84,10,01,87,6e,08,08,b1
Rijkspas	3b,fa,18,00,00,81,31,fe,45,06,08,2a,84,10,01,87,6e,08,05,bc
Rijkspas 2	3b,fa,18,00,00,81,31,fe,45,06,08,2a,84,10,01,87,6e,08,07,be
SafeSign Default QSCD	3b,db,18,ff,81,91,fe,1f,c3,06,09,2b,06,01,04,01,e9,10,05,03,d7
StarSign Crypto USB-Token S	3b,f9,96,00,00,81,31,fe,45,53,43,45,37,20,0e,00,20,20,28
UZI-pas 2	3b,fd,18,00,ff,81,31,fe,45,43,49,42,47,55,5a,49,4a,32,41,30,38,31,58
UZI-pas 3	3b,dc,18,ff,81,91,fe,1f,c3,06,0a,2b,06,01,04,01,e9,10,05,02,03,d1
UZI-pas 4	3b,dc,18,ff,81,91,fe,1f,c3,06,0a,2b,06,01,04,01,e9,10,05,02,04,d6

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

8 Supported Smart Card Readers

SafeSign IC Minidriver version 4.1 provides support for PC/SC v2.0 Class 1 readers.

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

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

The following table lists the specific readers that have been tested with SafeSign IC Minidriver version 4.1:

Smart Card Reader Manufacturer and Model	Class
HID® OMNIKEY® 3121 USB Smart Card Reader Revision D/2019	1

- Note that smart card readers that have been tested or have been working at a given time with a previous SafeSign IC Minidriver versions, may not (still) work or be supported in any or all versions of SafeSign IC Minidriver version 4.1.

8.1 Extended APDU

In order to be able to generate RSA 4096-bits (and 3072-bits) keys on a JCOP 4 QSCD card, the smart card reader should support extended APDU.

The ISO 7816-4:2013 specification defines an extended APDU as any APDU whose payload data, response data or expected data length exceeds the 256 byte limit.

The following readers have been tested with RSA 4096-bits keys and extended APDU:

- HID OMNIKEY 3121 USB (Part No. R31210320-01, revision B/2016 and revision D/2019)
- Gemalto/Thales IDBridge CT30
- Gemalto GemPC Twin
- ACS ACR38 (P/N ACR38U-N1)
- Neowave LinkeoA-Y
- Neowave Winkeo-A SIM

These card readers have been tested using the OS CCID driver, i.e. the native CCID driver on Windows.

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

Depending on the Operating System, the reader name may be different. This explains the different names in the whitelists in the registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\A.E.T. Europe B.V.\SafeSign\2.0\Readers
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\A.E.T. Europe B.V.\SafeSign\2.0\Readers.rocm
```

The reason for two whitelists in the registry for readers supporting extended APDU lies in the fact that SafeSign IC Minidriver version 4.1 now includes both the read-only and the read/write Minidriver (see section 3.8). When the read-only Minidriver is installed or both the read-only and read/write Minidriver are installed, both whitelists will be available.

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

9 Supported Applications

SafeSign IC Minidriver version 4.1 has been tested in accordance with AET's Quality Assurance procedures and the SafeSign IC Minidriver test plan. This includes testing of a number of defined and representative applications to verify a correct functioning of the SafeSign IC components and Libraries.

The following applications have been tested with SafeSign IC Minidriver version 4.1.0.0:

Application	Version	Purpose
Token Administration Utility	3.8.43.1	PKCS #11 token management functions
Mozilla Firefox	123.0.1	Authentication to a secure web site
Microsoft Edge	122.0.2365.80	Authentication to a secure web site
Google Chrome	122.0.6261.112	Authentication to a secure web site
Microsoft Outlook	2021	Signing and decrypting e-mail messages
Mozilla Thunderbird	115.8.1	Signing and decrypting e-mail messages
Adobe Reader DC	2023.008.20555	Digitally signing a document
Microsoft Word	2021	Digitally signing a document
LibreOffice	7.6.5	Digitally signing a document
Windows Smart Card Logon	-	Log on to a local Windows client system
Terminal Server Logon	-	Log on to a Windows Terminal Server

- Note that PKCS #11 applications need the PKCS #11 Library to be loaded/installed as a security module. The SafeSign IC PKCS #11 Library (called 'aetpkss1.dll') can be found in the system directory.
- Note that (Microsoft) applications do not normally require any configuration, i.e. you do not need to select or install the SafeSign IC card Minidriver.
- Note that for smart card logon and terminal server logon, you need to have the read-only Minidriver installed.

9.1 Token Administration Utility

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

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

Refer to the Administrator's Guide for more details.

9.2 Mozilla Firefox

With SafeSign IC Minidriver installed, you can perform secure web authentication with a SafeSign IC Token.

- Note that as of Firefox 90, you no longer need to install the SafeSign PKCS #11 Library as a security module in Firefox.

9.3 Mozilla Thunderbird

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

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

9.4 Microsoft Edge

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

9.5 Google Chrome

With SafeSign IC Minidriver installed, you can perform secure web authentication in Google Chrome.

9.6 Microsoft Outlook

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

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

9.7 Adobe Reader DC

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

9.8 Microsoft Word

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

9.9 LibreOffice

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

9.10 Windows Smart Card Logon

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

9.11 Terminal Server Logon

With SafeSign IC read-only Minidriver installed, you can use your SafeSign IC token to log on to a remote Windows Terminal Server.

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

10 Supported Languages

The following languages are supported in SafeSign IC Minidriver version 4.1 (Token Administration Utility):

- Basque (Basque);
- Catalan (Catalan);
- Chinese (Simplified, China);
- Chinese (Traditional, Hong Kong SAR; Traditional, Taiwan);
- Croatian (Croatia);
- Czech (Czechia);
- Dutch (Netherlands);
- English (United States);
- Finnish (Finland);
- French (France);
- German (Germany);
- Hungarian (Hungary);
- Italian (Italy);
- Italian (Switzerland);
- Japanese (Japan);
- Korean (Korea);
- Lithuanian (Lithuania);
- Portuguese (Portugal);
- Portuguese (Brazil);
- Russian (Russia);
- Serbian (Cyrillic, Serbia)
- Serbian (Latin, Serbia);
- Spanish (Spain);
- Thai (Thailand);
- Turkish (Turkey);
- Ukrainian (Ukraine).

10.1 Installation language files and codes

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

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

For example, to install SafeSign IC Minidriver version 4.1 in Portuguese (Brazil):

```
msiexec /I “SafeSign IC MiniDriver 4.1.0.0-AET.000 64-bits.msi” TRANSFORMS=pt-PT.mst
```

- Note that WiX does not support all languages, hence the SafeSign IC Installer is not available in the following languages: Italian (Swiss), Lithuanian and Ukrainian.

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

Language	File
Catalan	ca-ES.mst
Chinese (Simplified characters)	zh-CN.mst
Chinese (Traditional characters)	zh-TW.mst
Croatian	hr-HR.mst
Czech	cs-CZ.mst
Dutch	nl-NL.mst
Finnish	fi-FI.mst
French (France)	fr-FR.mst
German	de-DE.mst
Hungarian	hu-HU.mst
Italian	it-IT.mst
Japanese	ja-JA.mst
Korean	ko-KO.mst
Portuguese (Portugal)	pt-PT.mst
Portuguese (Brazil)	pt-PT.mst
Russian	ru-RU.mst
Serbian (Latin)	sr-latn-cs.mst
Serbian (Cyrillic)	sr-cyrl-cs.mst
Spanish	es-ES.mst
Thai	th-TH.mst
Turkish	tr-TR.mst

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com

- Note that during installation, the Component Setup windows will only include localisation of the Minidriver components in Dutch, German, Portuguese, Brazilian Portuguese, Serbian Latin and Serbian Cyrillic.

A.E.T. Europe B.V.
+31 26 365 33 50
info@aeteurope.com
www.aeteurope.com