aet europe

SafeSign Identity Client

Administrator's Guide

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

Document Information

Document ID: SafeSign Identity Client Administrator's Guide

Project Information: SafeSign IC User Documentation

Document revision history:

Version	Date	Author	Changes
1.0	11 April 2024	Drs C.M. van Houten	First version for SafeSign IC Version 4.1, release 4.1.0.0-AET.000

Version	Date	Name	Function
1.0	11 April 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

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

Table of Figures

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 cannot 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

About the Manual

The aim of this document is to describe the registry settings and configuration options of SafeSign Identity Client (IC).

While reading this document, take into account the notes and warnings.

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

1 About the Administrator's Guide

1.1 Registry

The Registry contains information, settings, options, and other values for programs and hardware installed on all versions of Microsoft Windows operating systems. When SafeSign Identity Client (IC) is installed, a number of registry keys are created.

Some of these registry keys can be used to change the behaviour and functionality of the SafeSign IC Token Administration Utility (TAU) and middleware on a per-computer basis.

The SafeSign IC (registry) configuration file is also created on Linux and macOS. Therefore, this manual will explicitly indicate if and how a particular setting works for SafeSign IC Minidriver for Windows and / or SafeSign IC Standard on Linux and macOS (as well).

- This manual assumes that the registry editor used on Windows is the Microsoft application 'Registry Editor' ('regedit'). Microsoft provides this registry editor with your operating system. For the working of this registry editor please read the appropriate manuals from Microsoft. On Linux and macOS, you should use an editor such as TextEdit to change the contents of the SafeSign IC (registry) configuration file.

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

1.2 SafeSign IC

SafeSign IC comes in two product versions (64-bit only), SafeSign IC Minidriver for Windows and SafeSign IC Standard for Linux and macOS. The table below lists which cryptographic library / libraries are included in the product versions:

Product Version	OS	Library	DLL name
SafeSign IC Minidriver	Windows	PKCS #11 Minidriver	aetpkss1.dll aetrocm1.dll / aetrocm1x.dll aetrwcm1.dll / aetrwcm1x.dll
SafeSign IC Standard	Linux	PKCS #11	libaetpkss.so
	macOS	PKCS #11 Smart Card Extension	libaetpkss.dylib aetsce.appex

Table 1: Product Versions and Libraries

For each relevant key and/or value described in the sections below, the library it applies to will be specified.

1.3 Intended audience

This manual is intended for use by administrators.

Standard users (without administrator rights) of SafeSign IC are advised not to make registry changes, as this may cause irreparable damage and may lead to malfunctioning of SafeSign IC.

1.4 Prerequisites

1. Sufficient rights and knowledge to modify the registry.
2. Sufficient knowledge about tokens and their internal workings to modify the registry correctly.
3. SafeSign IC Minidriver (Windows) or SafeSign IC Standard (Linux, macOS) installed.
4. Knowledge of the SafeSign IC release and user documentation.
5. Possession of (one of) the supported tokens, as described in the latest Release Notes.

1.5 Initialisation

A number of SafeSign IC registry entries deal with the cards supported in SafeSign IC and their initialisation profile.

Initialisation of a token involves writing the PKCS #15 file structure on the token and setting such values as token label, PUK and PIN. The values written on the token during initialisation cannot be changed during the lifetime of the token. This means that during the lifetime of the token, the token keeps the so-called 'profile' that has been created during the initialisation. Note that this includes the maximum number of PIN and/or PUK retries and the length of the PIN and/or PUK.

Prior to initialisation, you may configure some initialisation values (such as PIN length), which this document describes.

- Note that this will only affect the initialisation of a token on the local computer by means of the TAU. If you need to initialise a large number of tokens, it is recommended to use a card management system, such as BlueX.

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

1.6 Additional warning

This manual contains information about modifying the registry. Before you modify the registry, make sure to back it up and understand how to restore the registry if a problem occurs. Modification of the registry is done at your own risk. A.E.T. Europe B.V. cannot accept liability for any malfunctioning of SafeSign Identity Client or applications due to changes in the registry.

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

2 SafeSign Registry

The 'SafeSign' user registry key / configuration file is located in the following locations:

- Windows: HKEY_LOCAL_MACHINE\Wow6432Node\SOFTWARE\A.E.T. Europe B.V.\
- Linux: /home/[user name]/.safesign/
- macOS: /Users/[user name]/Library/Application Support/safesign/

- Note that the location of the SafeSign IC registry configuration file on Linux and macOS mentioned above is the location where the user registry is stored (i.e. the user's home directory).

- The original / root registry configuration file is located in /usr/share/safesign (Linux) and /Applications/tokenadmin.app/Contents/Resources/Data (macOS) and is copied to the user's (home) directory the first time the SafeSign TAU is started. On a per-computer basis, you should edit the user registry configuration file. Editing of the original / root registry configuration file, for example when an Administrator wants to apply general settings to all users, is done at one's own risk and should be implemented only after careful testing.

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

The following table provides an overview of the SafeSign IC registry keys and in which SafeSign IC product version they are included:

Section	Registry Key	Windows	Linux	macOS
2.1	2.0	√	√	√
2.2	Actions	√	√	√
2.3	Activation	√	√	√
2.4	CardModule	√	X	X
2.5	Cards	√	√	√
0	Expiration	√	√	√
2.7	Files	√	√	√
2.8	Java Card	√	√	√
2.9	Locales	√	X	X
2.10	Policies	√	√	√
2.11	Profiles	√	√	√
0	Readers	√	√	√
0	Readers.rocm	√	X	X
2.13	Tasks	√	√	√

Table 2: SafeSign Registry Keys

The screenshots in the sections below were taken from an installation of SafeSign IC Minidriver Version 4.1 on a 64-bit Windows 11 23H2 Operating System.

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

2.1 2.0

The registry key '2.0' contains the following values:

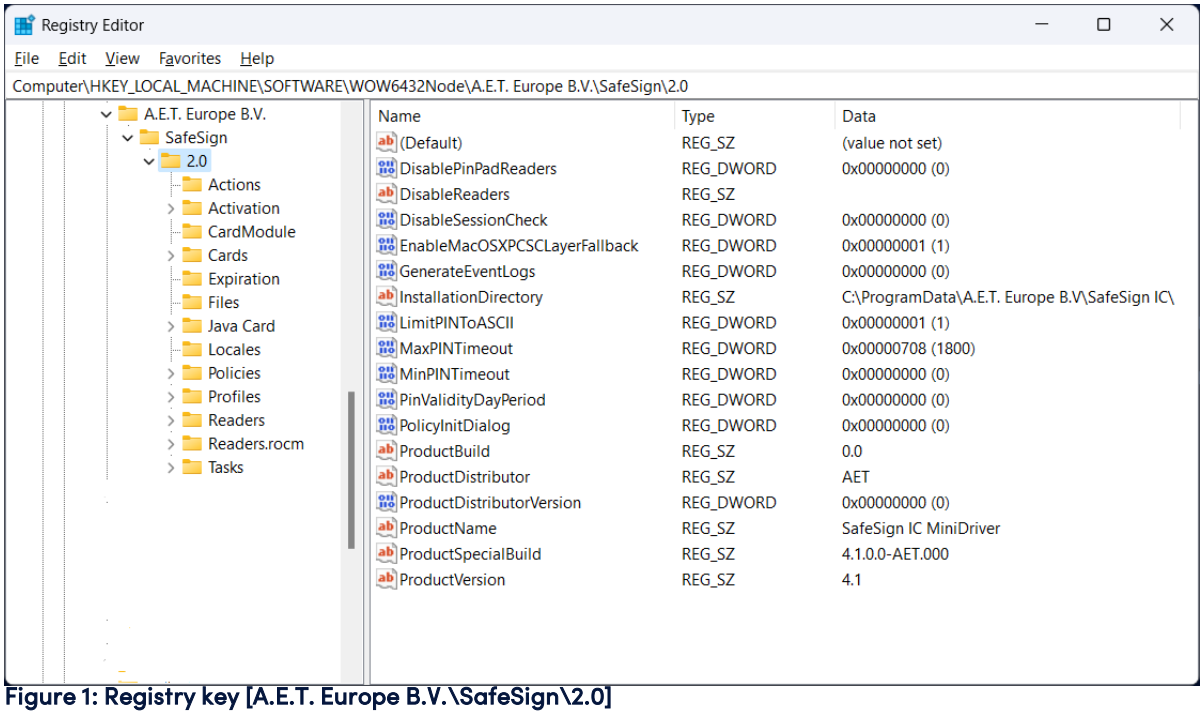

Figure 1: Registry key [A.E.T. Europe B.V.\SafeSign\2.0]

The next sections will describe the settings and whether they are enabled (1) or disabled (0) by default and to which library they apply on which Operating System.

- Note that the screenshot above is taken from a Windows system that has both the read-only and read/write Minidriver installed. When the read/write Minidriver only is installed, only the Readers key will be available.

2.1.1 DisablePinPadReaders

This value has been deprecated and will not be described in this document.

In SafeSign IC Minidriver and SafeSign IC Standard, only Class 1 smart card readers are supported.

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

2.1.2 DisableReaders (Windows only)

This string value manages the availability of PC/SC smart card readers. This setting only works on Windows, for PKCS #11 applications.

When entering the exact name (and slot number) of a particular smart card reader in this field (for example, 'OMNIKEY CardMan 3x21 0'), the SafeSign IC PKCS #11 will no longer (try to) access the smart card in this reader.

- Note that it is possible to disable multiple readers, by using a semi-colon (";") as separator. It does not work with a comma (",").

2.1.3 DisableSessionCheck (Windows only)

This value has been deprecated and will not be described in this document.

2.1.4 EnableMacOSXPCSCLayerFallback (macOS only)

If an application (based on PKCS #11) does not have CTK entitlement, the SafeSign PKCS #11 Library that is loaded by that application does not have this entitlement either. Such applications are then not able to (properly) communicate with the token and cannot perform such tasks as accessing a secure web site or digitally signing a document.

The registry value EnableMacOSXPCSCLayerFallback was added to the SafeSign IC registry to be able to use PKCS #11 applications on macOS that do not have CTK entitlement (such as LibreOffice).

It is by default enabled, to allow these applications to communicate with tokens through PC/SC, if the communication through CTK fails.

- Note that this value is not applicable to Windows and Linux and is a workaround only (for applications that do not have CTK entitlement yet) on macOS.

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

2.1.5 GenerateEventLogs (Windows only)

SafeSign IC supports the generation of Application Event logs on Windows, through the AETEventProvider. It is by default disabled, but when enabled, the following PKCS #11-related events will be logged:

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

These events will be logged during use of the Token Administration Utility or within PKCS #11 applications (e.g. Thunderbird).

- Note that the following known issue (as described in the Release Document) applies: when enabling the registry setting GenerateEventLogs, events will be logged (such as incorrect PIN attempts), but also an error (EventID 258) will occur.

2.1.6 InstallationDirectory

This string value reflects the name of the Installation Directory of SafeSign IC, as selected during the installation of SafeSign IC.

This value should not be edited.

2.1.7 LimitPINToASCII

This DWORD Value, which is enabled by default, limits the PIN entry to ASCII characters when setting the PIN (e.g. during initialisation) or changing the PIN in the Token Administration Utility.

This value has been implemented to prevent problems (in applications) with PINs with so-called diacritical marks (such as ä). When disabled, SafeSign IC will no longer limit the PIN entry to ASCII characters only and allow for a PIN with non-ASCII characters (such as ä, §).

- On Windows, the Microsoft Windows Security dialog (to enter your PIN for CryptoAPI applications) does not support the use of non-ASCII characters, i.e. non-ASCII characters cannot be used with applications using the SafeSign IC Minidriver.
- On Linux, it is strongly advised not to use non-ASCII characters, which may or may not work on different Linux distributions.
- On macOS, though it is possible to enter non-ASCII characters in different ways, this may not always actually enter the desired character (without the user being aware of it). Therefore, it is not recommended to use non-ASCII characters on macOS.

- Note that non-ASCII characters are usually composed of two bytes, which may affect the maximum PIN length.
- Note that when a token has a PIN with non-ASCII characters and the LimitPINToASCII value is enabled again, you will be able to enter your current PIN with the diacritical marks (when verifying or changing the PIN), but you will not be able to change the PIN into a new PIN with such characters.

2.1.8 MaxPINTimeout

When the PIN Timeout is enabled, you will need to enter the PIN in PKCS #11 applications (e.g. Thunderbird) on Windows, Linux and macOS, even when the token is not removed and the application is not closed, within a timeframe that is configurable in the TAU.

The MaxPINTimeout value reflects the maximum amount of time in seconds (by default 1800 seconds / 30 minutes) set in the TAU, after which you will need to (re-)login to the token.

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

2.1.9 MinPINTimeout

When the PIN Timeout is enabled, you will need to enter the PIN in PKCS #11 applications (e.g. Thunderbird) on Windows, Linux and macOS, even when the token is not removed and the application is not closed, within a timeframe that is configurable in the TAU.

The MinPINTimeout value reflects the minimum amount of time in seconds set in the TAU, after which you will need to (re-)login to the token.

- Note that although this seems to suggest that the minimum PIN Timeout is zero (0) seconds, the minimum PIN Timeout value in the TAU is actually set to 20 seconds (because a PIN Timeout of 0 seconds would immediately invalidate the PIN when it is entered).

2.1.10 PINValidityDayPeriod

This value, which is by default disabled, allows you to specify the number of days after which you will be notified that your PIN is expired or will expire.

When this value is enabled by entering a number (of days), you will be notified in the TAU on both Windows, Linux and macOS that your PIN is expired or will expire in a number of days and asked to change it.

- Note that changing the PIN to a new value is not enforced, i.e. you can enter the same / current PIN and the PIN does not have to conform to any PIN policies. Moreover, setting this value does not affect any (PKCS #11 or CryptoAPI) applications other than the TAU (i.e. no warning as to the validity of the PIN will be shown outside of the TAU).

2.1.11 PolicyInitDialog

This value has been deprecated and will not be described in this document.

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

2.1.12 Product Values

The values ProductBuild, ProductDistributor, ProductDistributorVersion, Productname, ProductSpecialBuild and ProductVersion determine the full name of the SafeSign IC product installed, as displayed in the Product Name Field in the TAU Version Information dialog.

These values should not be edited.

2.2 Actions

2.2.1 Actions and Features

The registry key 'Actions' allows you to view and modify the menu items and features of the TAU:

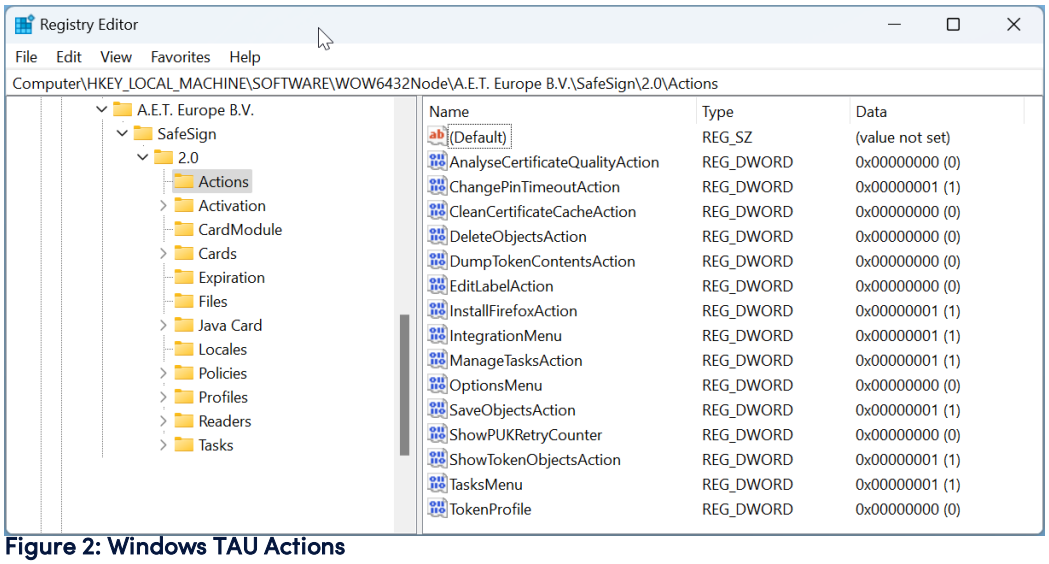

Figure 2: Windows TAU Actions

For those Features that have a corresponding Menu or Action in the registry (i.e. a DWORD Value), it is possible to enable or disable them, by changing the value from 0 to 1 and from 1 to 0 respectively.

- Note that it is not possible to disable the **Help** menu.

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

2.2.2 TAU

The following table lists the actions and features that are available in the registry and that can be enabled or disabled by setting its default value to 1 or 0 respectively (depending on the default value indicated in the table below):

Value Name	TokenAdmin Feature	Default Value
AnalyseCertificateQualityAction	Token > Analyse Certificate Quality	0
ChangePinTimeoutAction	Token > Change PIN Timeout	1
CleanCertificateCacheAction	Digital IDs > Clean Certificate Cache	0
DeleteObjectsAction	Token > Show Token Objects > Delete Object	0
DumpTokenContentsAction	Token > Dump Token Contents	0
EditLabelAction	Token > Show Token Objects > Edit Label	0
InstallFirefoxAction	Integration > Install SafeSign in Firefox	1
IntegrationMenu	Integration (menu)	1
ManageTasksAction	Tasks > Manage tasks	1
OptionsMenu	Options (menu)	0
SaveObjectsAction	Token > Show Token Objects > Save Object	1
ShowPUKRetryCounter	Show PUK retry counter in PUK dialogs	0
ShowTokenObjectsAction	Token > Show Token Objects	1
TasksMenu	Tasks (menu)	1
TokenProfile	Token > Initialise Token > Token profile (dropdown box)	0

Table 3: TAU Registry Actions

- Note that the **Task** menu (TasksMenu) and the features **Clean Certificate Cache** (CleanCertificateCacheAction) and **Manage Tasks** (ManageTasksAction) are not available in the TAU on Linux and macOS.

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

Some Actions or Menus are not available in the registry, because they are default settings in the TAU. These features can be enabled or disabled by first creating the corresponding registry key and then setting its value data to 1 or 0 respectively (depending on the default value indicated in the table below):

Value Name	TokenAdmin Feature	Default Value
ChangePINAction	Change PIN	1
ChangePUKAction	Change PUK	1
DeleteDigitalIDAction	Digital IDs > Delete Digital ID	0
DigitalIDsMenu	Digital IDs (menu)	1
ImportCertificatesAction	Digital IDs > Import Certificate	1
ImportChainAction	Digital IDs > Digital IDs > Import trust chain	1
ImportDigitalIDAction	Digital IDs > Import Digital ID	0
InitTokenAction	Token > Initialise / Wipe / Recycle Token	1
ShowDigitalIDsAboutToExpireAction	Digital IDs > Digital IDs > Check Expiration	1
ShowDigitalIDsAction	Digital IDs > Show (Registered) Digital IDs	1
ShowInfoAction	Token > Show Token Info	1
TokenMenu	Token (menu)	1
TransferIDAction	Digital IDs > Digital IDs > Transfer ID to token	0
UnlockPINAction	Token > Unlock PIN	1

Table 4: Windows TAU Additional Actions

- Note that the features **Import trust chain** (ImportChainAction), **Check Expiration** (ShowDigitalIDsAboutToExpireAction) and **Transfer ID to token** (TransferIDAction) cannot be made available in the TAU on Linux and macOS.

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

2.3 Activation

The SafeSign IC Token Administration Utility (TAU) offers users of a Qualified Signature Creation Device (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'.

The activation process for a particular card may be very specific. The registry key HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\A.E.T. Europe B.V.\SafeSign\2.0\Activation holds the information and requirements for the cards currently supported:

- UZI-pas 3 and UZI-pas 4;
- Defensiepas 3;
- SafeSign default / generic QSCD with JCOP 3 or JCOP 4.

None of the information contained in the registry key Activation can or should be removed or edited, otherwise the correct operation of SafeSign IC cannot be ensured and all warranty and support will become void.

2.4 CardModule (Windows only)

2.4.1 EnableKeepAlive

Starting from Windows 8, the way smart cards are handled has changed.

Most notably, if a transaction is started and no operations are happening on the card for 5 seconds, the transaction (and card) is reset (https://technet.microsoft.com/en-us/library/hh849637.aspx and https://learn.microsoft.com/nl-nl/windows/win32/api/winscard/nf-winscard-scardbegintransaction?redirectedfrom=MSDN).

Although a Minidriver is not responsible for transaction management (but the application), we have made a workaround to prevent the transaction from timing out. However, this is not desired behaviour of the Minidriver and should only be activated when absolutely necessary.

The behaviour is controlled by the following registry entry (available after installing SafeSign IC Minidriver): HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\A.E.T. Europe B.V.\SafeSign\2.0\CardModule\EnableKeepAlive.

Possible values are:

- Value 0: off (default)
- Any other value is on, specifying the time interval in milliseconds. Note that the time interval should be less than 5000 to ensure proper functioning.

2.4.2 VerifyCachedCardGuid

In SafeSign IC Minidriver, a workaround for an issue with Citrix has been implemented, in the form of a registry entry that can be enabled. The issue occurred in a very specific use case, which involves the insertion and removal of different cards during logon and has to do with cached card states and resulted in an error being displayed during logon (“the requested key container does not exist on the smart card”).

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

The behaviour is controlled by the following registry entry (available after installing SafeSign IC Minidriver: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\A.E.T. Europe B.V.\SafeSign\2.0\Card Module\VerifyCachedCardGuid.

Possible values are:

- Value 0: off (default)
- Value 1: on

2.5 Cards

Every token supported in SafeSign IC can be found below the entry 'Cards'.

Each token has its unique model ID, which is set during installation of the applet and by which the token is identified in the TAU (Token Information > Token Type).

- Note that a token may have different names and model IDs.

The entries for the tokens include the modelID that applies to the token. For example, the modelID for the NXP JCOP 3 SecID P60 is 'JC118':

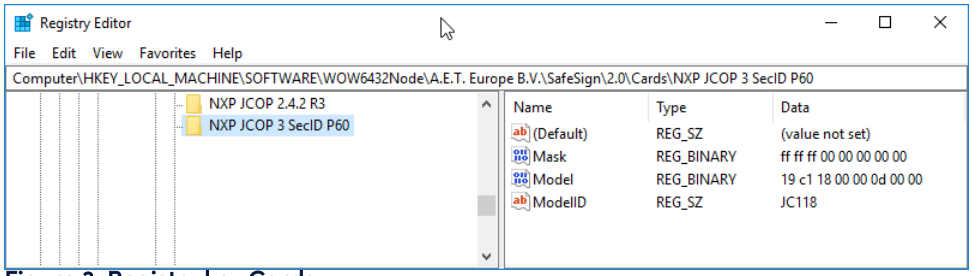

Figure 3: Registry key Cards

This model ID is also listed in the profile applying to the token (see section 2.11).

None of the information contained in these registry keys should be edited.

- For an overview of the cards and tokens supported in SafeSign IC Minidriver and SafeSign IC Standard, please refer to the appropriate release documentation.

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

2.6 Expiration (Windows only)

By default SafeSign IC warns an end-user that a certificate is about to expire the moment a token is inserted into a reader / machine. This is done by the Certificate Expiration Check Utility (aetcrss1.exe), which by default executes the task of 'Certificate Expiration Check'.

The default days in advance that SafeSign Identity Client warns an end-user, is 30 days.

This value can be changed, by changing the WarnDaysInAdvance entry in:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\A.E.T. Europe B.V.\SafeSign\2.0\Expiration

The actual language of the dialog cannot be customised.

- Note that although the SafeSign IC (registry) configuration file on Linux and macOS includes the relevant registry entries (**Task** menu, see section 2.2.2) above, the expiration functionality does not work, as there is no Certificate Expiration Check Utility running on those Operating Systems.

2.7 Files

The registry key 'Files' indicates where SafeSign IC can find the necessary files for its correct functioning.

This is also the place where the Version Info item in the **Help** menu retrieves their information from.

You should not edit this information, nor change the location of the files, otherwise the correct operation of SafeSign IC cannot be ensured.

2.8 Java Card

The registry key 'Java Card' applies to the Java Cards supported by SafeSign IC.

Note that none of the keys and values in 'Java Card' should be edited, to ensure a proper operation of SafeSign IC.

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

2.9 Locales

The registry key 'Locales' contains the path to the language files of SafeSign IC (in ProgramData).

Note that these language files cannot be edited. If you are interested in localization of SafeSign IC in your own language, please contact safesignsupport@aeteurope.com

2.10 Policies

The registry key 'Policies' contains the PIN policies supported by SafeSign IC.

For certification purposes with the ICP-Brazil standard, SafeSign IC Minidriver and SafeSign Standard support cards with a (pre-)defined PIN policy (applet), where the end user may not just select any PIN or PUK code for their token, but must adhere to certain complexity rules (so called PIN and PUK policies).

- Note that for this functionality to work, for the PIN Policy functionality to be enabled, a special version of the applet and specific applet install parameters are required (which are outside of the scope of this document).

Currently, one applet (non-RIC) is available that combines PIN policy and recycling functionality.

Apart from requirements regarding PIN and PUK length and equality, the PIN policy checks diversification with the following requirements:

1. PIN / PUK must have at least one (01) capitalized alphabetic character (A-Z);
2. PIN / PUK must have at least one (01) lowercase alphabetic character (a-z);
3. PIN / PUK must have at least one (01) numerical character (0-9);
4. Allow the use of special characters. Example: "$", "@", "&" etc.;

The elements that make up the Non-RIC PIN policy are contained in the 'NONRIC' key.

Note that none of the keys and values in 'Policies' should be edited, to ensure a proper operation of SafeSign IC.

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

2.11 Profiles

When you initialise a token by means of the TAU (in the Initialise Token dialog), the token will be initialised in accordance with a token profile.

The different profiles that are by default delivered with SafeSign IC are stored in the 'Profiles' key.

This key contains 6 profiles:

Profile Name	Card
Java Card Minimal profile (v1)	G&D Sm@rtCafe Expert 64
(default08) Java card Medium profile (v1)	
G&D Tiger 64K Maximal profile (v1)	
Javacard NON-RIC profile	Java cards with non-RIC applet
(default11) Java Card default profile (v2)	Java Cards v2.2.2 and higher
Rijkspas 2	Rijkspas 2.1

Table 5: Registry Key Profiles

The profiles for the G&D Sm@rtCafe Expert 64 card are deprecated, as this card is no longer supported.

The only profile that may / can be edited is the '(default11) Java Card default profile (v2)' for Java Cards v2.2.2 and higher Java cards.

For such cards, the PKCS #15 structure is created on the fly and not all memory that will be used during the lifecycle of the card has to be allocated at initialisation time. Therefore, there is only one profile available. As the profile values have already been optimised, you may only edit such values as the Transport PIN and the maximum / minimum PUK and PIN length (see section 2.11.3).

- Note that creating or editing a profile will only affect the initialisation of a token on the local computer by means of the TAU. If you need to initialise a large number of tokens, it is recommended to use a card management system, such as BlueX.

2.11.1.1 Active profile

During initialisation of a token, the PKCS #11 library uses the 'Active profile' key in the registry to determine which token profile should be used for the initialisation of the token.

The registry string value 'Active profile' should have the name of the profile that is (to be) used during initialisation of a token, because a (domain) user will only be able to initialise the token according to the active profile set in the registry (the Token Profile drop-down list in the TAU will be greyed out); i.e. he cannot choose which profile to use for initialisation.

2.11.2 Values

The following values that may be edited in the "(default11) Java Card default profile (v2)" are:

Value	Meaning	Default	Description
MinPinLen	Minimum PIN length	4	The minimum PIN length value is 4.
MaxPinLen	Maximum PIN length	15	The maximum PIN length value is 15.
MinPukLen	Minimum PUK length	4	The minimum PUK length value is 4.
MaxPUKLen	Maximum PUK length	15	The maximum PUK length value is 15.
MaxPinRetries	Maximum PIN retries	3	The number of incorrect PIN entries before the PIN is locked. The minimum value is 3, the maximum value is 15.
MaxPUKRetries	Maximum PUK retries	3	The number of incorrect PUK entries before the PUK is locked. The minimum value is 3, the maximum value is 15.
TransportPin	Transport PIN	-	The Transport PIN of the token should be of equal or greater length than the PIN.

Table 6: Default Profile Values

- A Transport PIN is a temporary PIN on the token that has to be changed into a personalized PIN code before the token can be used. The preferred way to set a Transport PIN is to set it programmatically (as an expired PIN) and not in the profile, in accordance with the PKCS #11 standard, which defines: "If a PIN is set to the default value, or has expired, the appropriate CKF_USER_PIN_TO_BE_CHANGED or CKF_SO_PIN_TO_BE_CHANGED flag is set to TRUE. When either of these flags are TRUE, logging in with the corresponding PIN will succeed, but only the C_SetPIN function can be called. Calling any other function that required the user to be logged in will cause CKR_PIN_EXPIRED to be returned until C_SetPIN is called successfully." This may be done using a smart card management system such as BlueX.

2.11.3 Create profile

If for some reason you do not wish to use the default profile that SafeSign IC provides, we strongly recommend creating your own token profile and naming it accordingly, instead of changing the existing profile.

Note that AET cannot be held responsible and will not provide support for any problems arising from the fact that the default profile was edited or a profile was created.

If you want to change certain values, you should copy the default profile and take the following entries into account, to be able to distinguish between the default profile and your own profile:

- "Name": The name of the profile. It is recommended that you choose your own identifying name. You can also modify the Active profile value to include your own profile name (see section 2.11.1.1).
- "ModelID": The cards that your profile applies to. The default profile contains a large number of ModelIDs. If you create your own profile, you can include the (only) model ID that your profile should apply to. You can find the modelID for your token in the registry entry 'Cards' (see section 2.5).

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

2.12 Readers / Readers.rocm

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

The list can be found here:

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

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

The following readers have been tested with RSA 4096-bits keys and extended APDU for the release of SafeSign IC Minidriver / Standard 4.1:

- 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

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. For example, the HID OMNIKEY 3121 USB is called 'HID Global OMNIKEY 3x21 Smart Card Reader' on Windows and 'HID Global OMNIKEY 3x21 Smart Card Reader [OMNIKEY 3x21 Smart Card Reader]' on Linux.

On Windows, when the read-only Minidriver is installed or both the read-only and read/write Minidriver are installed, two whitelists will be available:

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 includes both the read-only and the read/write Minidriver (see section 3.8).

2.13 Tasks (Windows only)

Through the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\A.E.T. Europe B.V.\SafeSign\2.0\Tasks on Windows you can modify the settings of the Task Manager, which is included in the TAU.

The defined tasks can apply either to all tokens or to a specific token (identified on the basis of token label and serial number). Below the entry 'All cards' you will find those tasks that apply to all tokens; below the entry 'Specific cards' (which will only be created when a task for a specific card is added) you will find those tasks that apply to one (or more) specific token(s). Note that it is recommended to add and/or remove tasks in the TAU, not in the registry.

There is one predefined task that applies to all cards, described below.

- Tasks are run by the Certificate Expiration Check Utility (aetcrss1.exe). When the predefined task (or additional tasks) are removed, this application will be stopped.

2.13.1 Certificate Expiration Check

The Certificate Expiration Warning dialog will appear by default every time a token is inserted (without the TAU open), which contains certificates that are about to expire in the time period specified.

The settings for this task being enabled, started and closed are recorded in the registry and can be enabled / disabled through the registry (apart from in the TAU).

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

3 Minidriver (Windows only)

Smart card vendors can write card minidrivers to present a consistent interface to their smart card type to the Microsoft Smart Card Base Cryptographic Service Provider (CSP) or Crypto Next Generation (CNG) Key Storage Provider (KSP) and to the Smart Card Management Interface.

For more general information on Smart Card Minidrivers, see: https://msdn.microsoft.com/en-us/windows/hardware/drivers/smartcard/smart-card-minidrivers.

SafeSign IC Minidriver 4.1 includes both a read-only and read/write Card Minidriver for use of the cards supported by SafeSign IC with the Microsoft Base Smart Card Crypto Provider / Microsoft Smart Card Key Storage Provider, i.e.:

- Card Minidriver for 32-bit applications: aetrwcm1.dll / aetrocm1.dll
- Card Minidriver for 64-bit applications: aetrwcm1x.dll / aetrocm1x.dll

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). The read/write Minidriver .dll files will be placed in ProgramData\A.E.T. Europe B.V\SafeSign IC\Minidriver\readwrite directory.

It is important to take the following into account with regard to the use of SafeSign IC Minidriver:

- It has support for Windows only (the concept of a Minidriver is a Microsoft one);
- 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.
- It has no support for initialisation through the Card Minidriver (initialisation with PKCS #11 only).

The SafeSign IC Card Minidriver is installed in accordance with Microsoft procedures: “An INF-based approach should be used for the registration of a smart card minidriver. The INF file allows for the creation of the necessary registry entries as well as the copy of files from the driver package to the appropriate directories.” (https://msdn.microsoft.com/en-us/windows/hardware/drivers/smartcard/minidriver-registration.

3.1 ATR

The Winscard (Winscard.dll) discovery process is used to associate a card in the system with an installed CSP or Minidriver, for which it looks in the registry under the Calais key for various subkeys that represent smart cards that are installed in the computer. Winscard searches each subkey under the SmartCards subkey for a match between the subkey's ATR value and an ATR value that is obtained from the smart card.

For SafeSign IC Minidriver on 64-bit Windows, the ATRs are recorded in: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards and HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Calais\SmartCards.

This is done to allow both 32-bit and 64-bit applications to work with a CSP.

When (only) one Minidriver is installed (i.e. read-only or read/write), all ATRs are by default associated with that Minidriver.

- If the read-only Minidriver (only) is installed, the Microsoft\Cryptography\Calais\SmartCards registry keys will associate the ATRs with aetrocm1x.dll / aetrocm1.dll, for example:

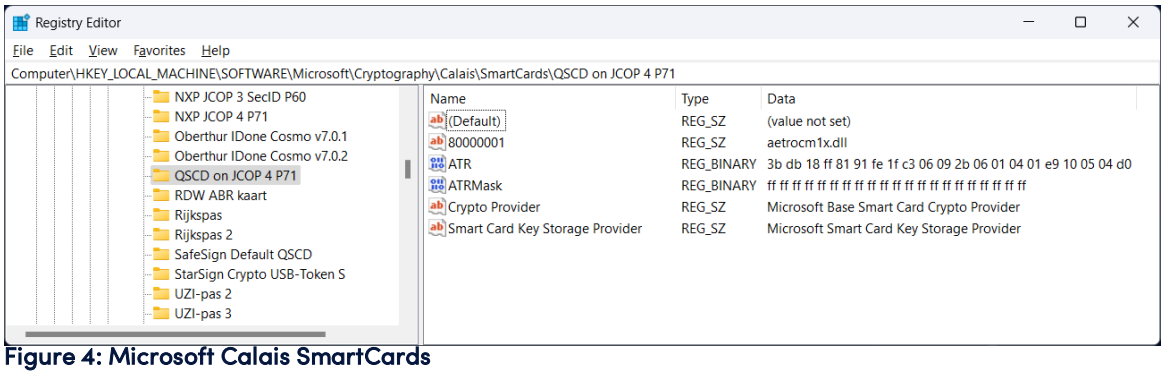

Figure 4: Microsoft Calais SmartCards

- If the read/write Minidriver (only) is installed, the Microsoft\Cryptography\Calais\SmartCards registry keys will associate the ATRs with aetrwcm1x.dll / aetrwcm1.dll.

- If you have both the read-only and read/write Minidriver installed and you want to use your card with the read/write Minidriver (e.g. for enrollment), you need to edit the value of the registry entry '80000001' for this particular card to contain the correct and full path to the read/write Minidriver file:

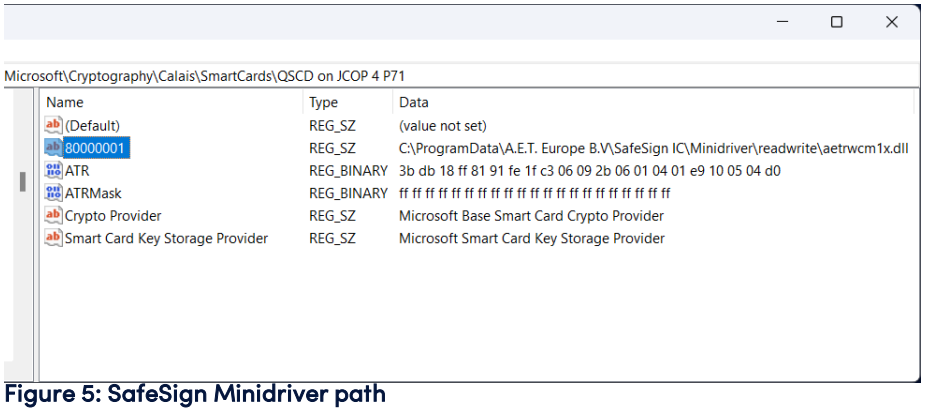

Figure 5: SafeSign Minidriver path

- Make sure you enter the correct file name, i.e. aetrwcm1x.dll for 64-bit applications and aetrwcm1.dll for 32-bit applications in the appropriate Microsoft\Cryptography\Calais\SmartCards registry keys.

- Do not change the (two) providers that are associated with this card's ATR. In accordance with Microsoft: "If the minidriver supports loading under CAPI, the following line should be included in the registry file: "Crypto Provider"="Microsoft Base Smart Card Crypto Provider". If the minidriver supports loading under CNG, the following line should be included in the registry file: "Smart Card Key Storage Provider"="Microsoft Smart Card Key Storage Provider". (see: https://msdn.microsoft.com/en-us/windows/hardware/drivers/smartcard/minidriver-registration).

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

4 Cache (Windows only)

For performance reasons, caching is done for the SafeSign IC PKCS #11 Library. With SafeSign IC Minidriver installed, all certificate information from all tokens that are or were inserted, is stored in the key HKEY_CURRENT_USER\SOFTWARE\A.E.T. Europe B.V.\SafeSign\2.0\Cache\Tokens:

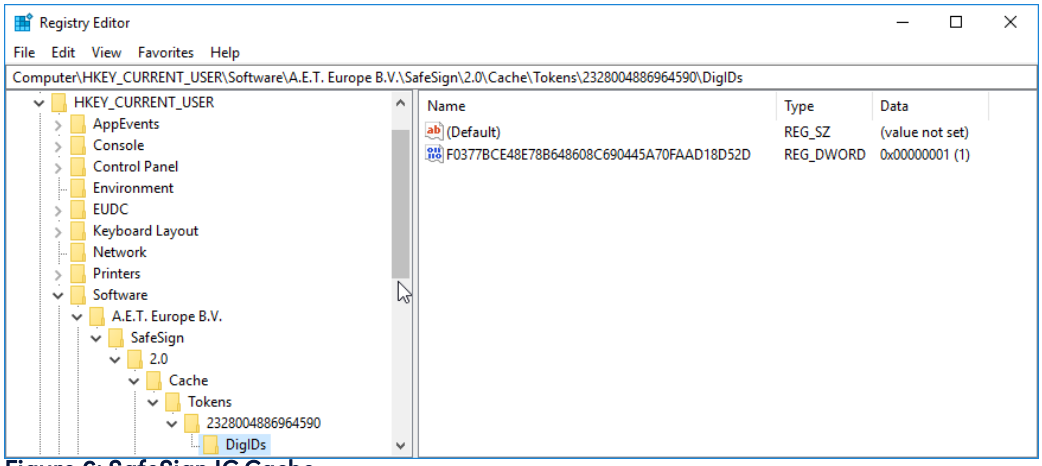

Figure 6: SafeSign IC Cache

This key includes the serial number of the Token(s) and the SHA-1 fingerprints of the Digital IDs ('DigIDs') it contains.

When a token is inserted that is already known in the cache and the contents of which have not changed, the information is not retrieved from the token, but from the registry entries, thereby increasing speed considerably. When the content of the token has changed between removal and insertion, the cache is updated the moment the token is inserted.

SafeSign IC will also store the SHA-1 fingerprint of the certificates on the local machine, for purposes of speed, in C:\Users\[name logged-on user]\AppData\Local\ A.E.T. Europe B.V\SafeSign\2.0\Cache. Note that you may not be able to see this directory, as these files are hidden by default.

- Note that when de-installing / removing SafeSign IC, the entry HKEY_CURRENT_USER\SOFTWARE\A.E.T. Europe B.V.\SafeSign\2.0\Cache will not be removed, to ensure that the certificate and token cache are available for future installed versions of SafeSign IC.

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

4.1.1 Clean certificate cache

The feature called ‘Clean Certificate Cache’ was created for older SafeSign IC versions, in which certificates were registered in a different way and is no longer needed.

Though not enabled by default (see section 2.2.2), the action ‘CleanCertificateCacheAction’ may be enabled to clean the cache, thereby forcing an update. This will only affect the view of certificates in the TAU.

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