aet europe

SafeSign IC

Token Administration Utility Guide

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- 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.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

aet europe

Table of Contents

A.E.T. Europe B.V.

+31 26 365 33 50

info@aeteurope.com

aeteurope.com

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

Table of Figures

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

Document Information

Document revision history:

Version	Date	Author	Changes
1.0	12/17/2024	C.M. van Houten	Final version for SafeSign IC Version 4.2

Related documents

Document ID	Title	Author	Details

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

1 Introduction

The SafeSign IC software provides a management interface for your token, called the Token Administration Utility (TAU). It is available in both SafeSign IC Minidriver (for Windows) and SafeSign IC Standard (for Linux and macOS).

It allows you to prepare ("initialise") your token for use with PKI applications, as well as manage your token when prepared.

1.1 Menu Items

The TAU offers five menu items:

1. Digital IDs;
2. Token;
3. Integration;
4. Tasks;
5. Help.

- Note that the Tasks menu is only available on Windows, not on Linux or macOS.
- Note that the actual menu items and features visible / available can be configured in the registry. For more details, see the SafeSign IC Administrator's Guide.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

Sections 3 to 7 will describe the menu items and their features in detail:

- Chapter 3: Digital IDs
- Chapter 4: Token
- Chapter 5: Integration
- Chapter 6: Tasks
- Chapter 7: Help

The following section 2 will provide some general information on the TAU.

Section 8 will describe some advanced options that may be enabled in the registry.

A.E.T. Europe B.V.

- +31 26 365 33 50
- info@aeteurope.com
- aeteurope.com

2 General

2.1 Tokens and readers

You will find the Token Administration app in **Start > All Apps**.

Upon clicking Token Administration, the TAU will open:

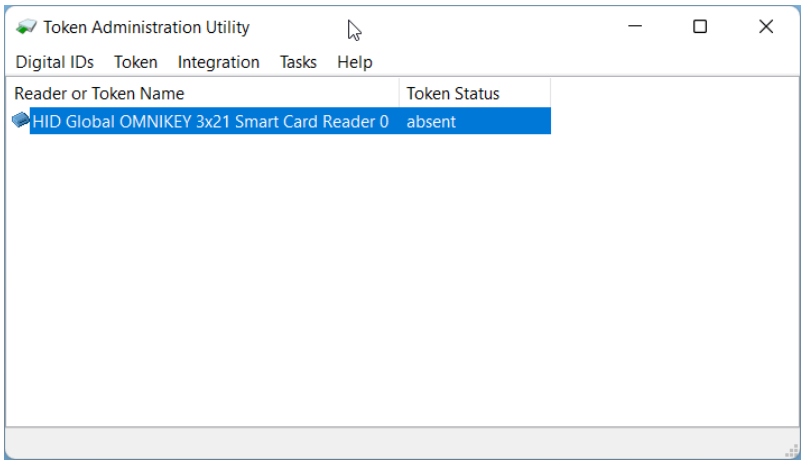


Figure 1: TAU: Token Status 'absent'

This window shows you which smart card reader(s) is (are) installed on your PC and the status of the token. When no token is inserted in the smart card reader, the name of the smart card reader will be listed and the Token Status will be 'absent' (as above). All smart card readers that are installed will be listed.

When no smart card reader is displayed, you will need to verify whether a smart card reader is attached and the correct drivers are installed and whether it is functioning properly. Without a functional smart card reader (and related services, such as the Smart Card service on Windows), SafeSign IC cannot be used.

Note that in this manual, we use "token", which may refer to a USB token or a smart card. Hence the phrase "a token in a smart card reader" may refer to a smart card inserted in a smart card reader or a USB token inserted in a USB port.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

When there is a token inserted in the smart card reader, the name of the token is displayed. In this case, there are two possibilities:

Either the token is blank, not yet initialised:

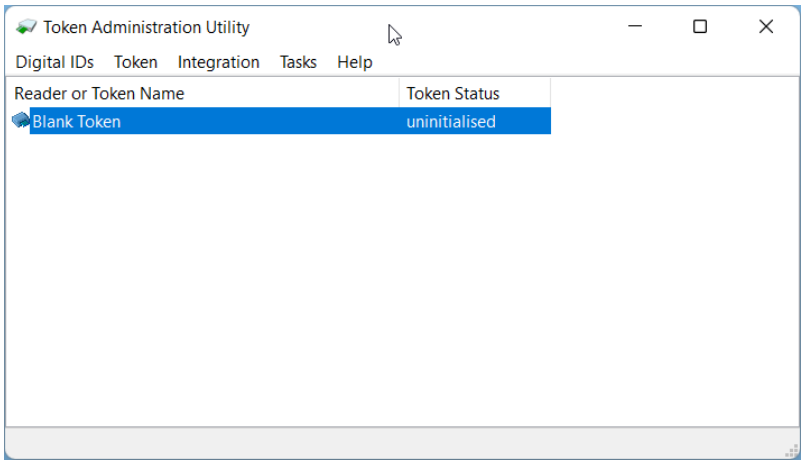


Figure 2: TAU: Token Status 'uninitialised'

Or the token has already been initialised and has a token name:

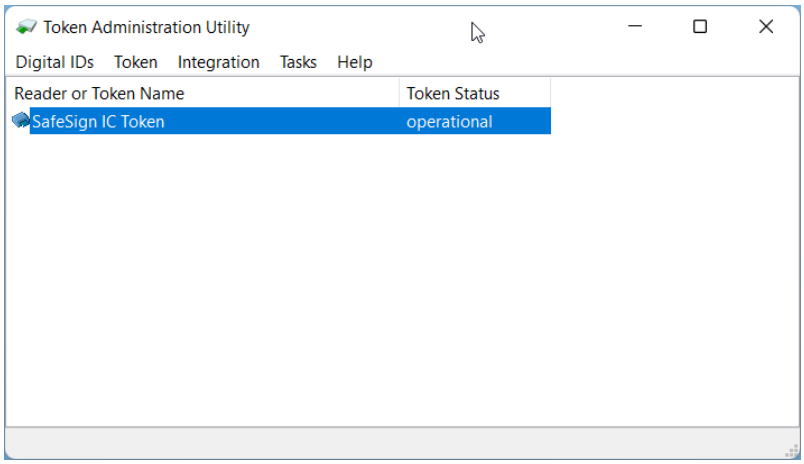


Figure 3: TAU: Token Status 'operational'

You may have multiple smart card readers or USB tokens installed (or a combination of both). You may have multiple (SafeSign IC supported) cards / tokens for different purposes and applications. Both can be present on one computer, in separate readers, and you can use the features of the SafeSign IC TAU for each of these cards / tokens.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

When there is one token in the reader, the TAU will automatically select this (highlighting it in blue). When there are two (or more) tokens in the readers, the last one inserted will be selected. You will need to select one of the tokens to perform such operations as Change PIN from the Token menu. This makes sense, as you need to specify first of / on which token you want to change the PIN or import a certificate.

2.2 Multi-language

Multi-language support has been implemented in such a way that it creates utmost flexibility for both administrator and user. The language of the installation program on the one hand and the TAU on the other hand, can be different.

The language of the installation program and the SafeSign IC items in the Start menu is determined by the language set for the installation of SafeSign IC and cannot be changed (without de-installing SafeSign IC).

The language of SafeSign IC (TAU and dialogs) will default to the format language set on the computer / system, without the need for the user to change any settings.

If the user wants to change the language of the TAU to the language he prefers to work with, he can do so in either Settings > Time & Language > Language & Region by selecting the desired Windows display language or in Control Panel > Region > Formats by selecting the desired language format.

Note that this may also affect other applications.

Here is an example of how the TAU looks in Dutch:

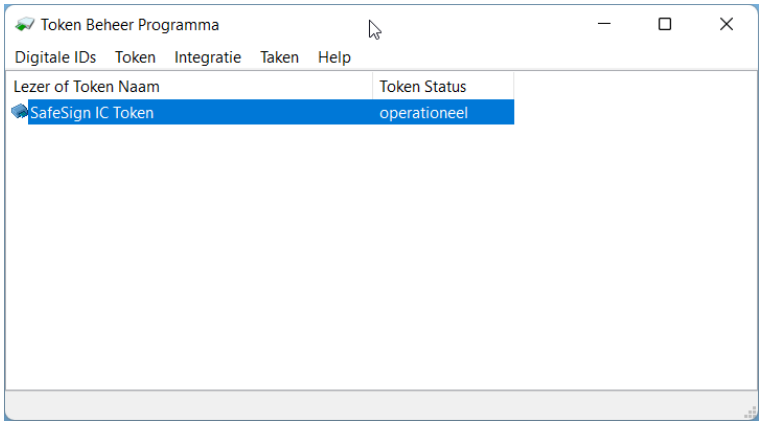


Figure 4: TAU in Dutch

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

Take the following into account with regard to localization:

- Note that the default language of SafeSign IC will match the Windows display language.
- When SafeSign IC does not support the selected language, the default language of SafeSign IC will be English (en-us).
- The language of the Firefox Installer will default to the system language (Format).
- Note that though SafeSign IC has been tested for its installation program and utilities to correctly display language-specific characters, language format and language display may differ on the various platforms used and may be dependent on the language pack and version of the Operating System used.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

3 Digital IDs

The **Digital IDs** menu in the Token Administration Utility allows users to view their Digital IDs and perform a number of operations related to Digital IDs.

- Note that the term 'Digital ID' is used to signify a key pair (private and public key) and a certificate, which can be used for operations such as signing and decrypting.

This section describes the following functionality:

- Section 3.1: Show Registered Digital IDs
- Section 3.2: Import Certificate
- Section 3.3: Exit

3.1 Show Registered Digital IDs

The menu item **Show Registered Digital IDs** opens a dialog to show the Digitals IDs that are registered / propagated in the local certificate store. This means that all certificates registered in the Microsoft (Current User) Personal Certificate Store will be displayed, whether they are on the token or not.

- Note that on Linux and macOS, this menu is called 'Show Digital IDs'.

This dialog (Digital IDs) will identify the Personal Digital IDs and the Digital ID details, i.e. the Certificate Contents and the Certification Path (when available).

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

When there are no Digital IDs, the Digital IDs dialog will be empty and look like this:

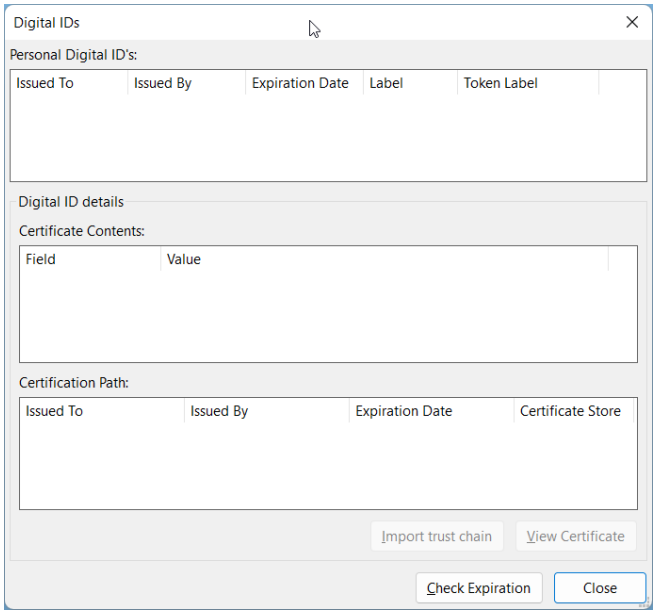


Figure 5: Digital IDs: No Personal Digital IDs

When a Digital ID is present on the token, the Digital IDs dialog will look like this:

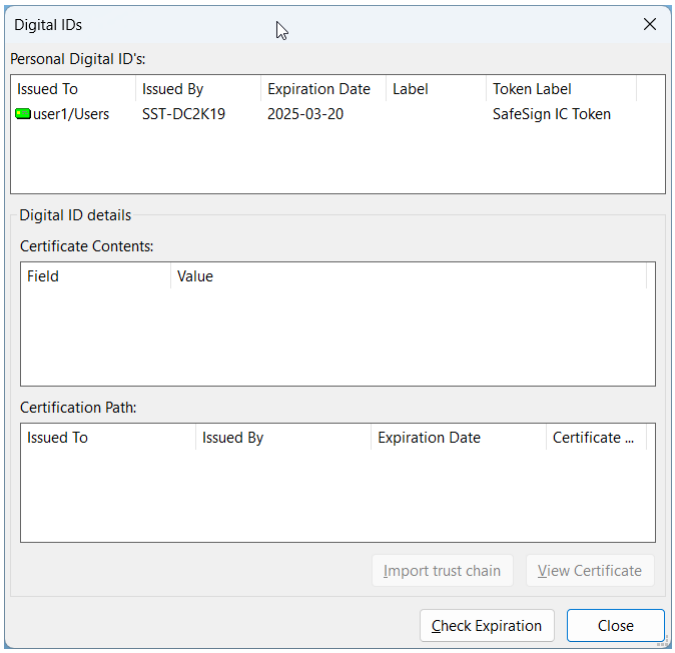


Figure 6: Digital IDs: Personal Digital ID on token

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

- When a Digital ID or CA certificate is on the token, this will be identified by the following symbol: 
- When a Digital ID or CA certificate is not on the token (but in the Microsoft Certificate Store) or when the token is removed, this will be identified by the following symbol: 
- When a Digital ID on the token is about to expire, this will be identified by the following symbol: 
- When a Digital ID on the token is expired, this will be identified by the following symbol: 

For more information regarding certificate expiration, refer to section 3.1.3.

- Note that certificates are propagated through the Microsoft Certificate Propagation Service. The Microsoft Certificate Propagation Service does not deregister certificates upon token removal, therefore when the token is removed, the certificates will remain in the certificate store and are displayed with the symbol  (though they will not be usable without the token that contains the corresponding key pair inserted).

The Digital IDs dialog also allows the user to perform a number of operations with regard to the Digital ID(s) stored on the token (by means of the buttons on the lower right-hand side of the dialog), as described in:

- Section 3.1.1: Import trust chain
- Section 3.1.2: View Certificate
- Section 3.1.3: Check Expiration
- Section 3.1.4: Close

- Note that on Linux and macOS, only the operation 'View Certificate' is available.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

3.1.1 Import Trust Chain

The operation Import trust chain allows you to import the trust chain for your Digital ID(s) onto the token, to ensure maximum flexibility and interoperability. When taking your token to another computer (where the appropriate trust chain may not be installed), your certificates can be registered.

You can use this functionality when the CA certificate(s) is not on the token, because you retrieved the CA certificates at a later time (with your Digital ID already on the token).

1 Select the Digital ID whose trust chain you wish to import to the token:

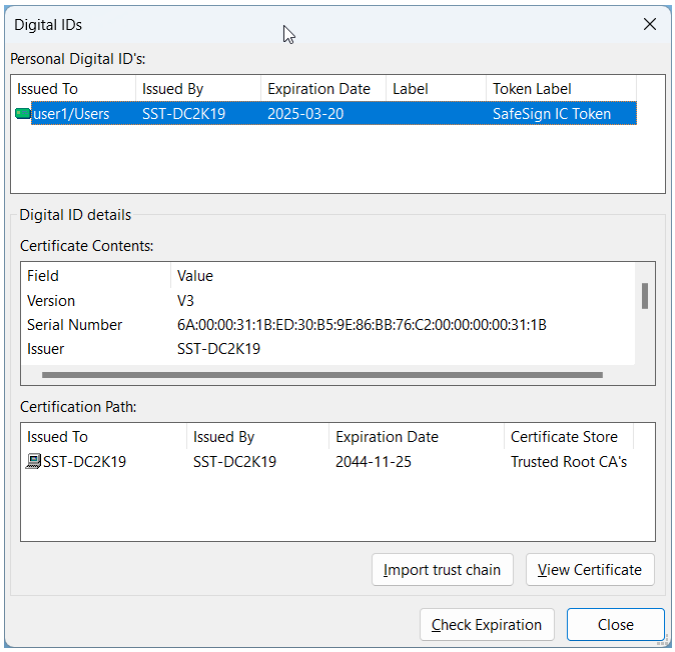


Figure 7: Digital IDs: Import trust chain

- Click **Import trust chain** to import the trust chain to the token

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

2 You will be asked to enter the PIN for your token:

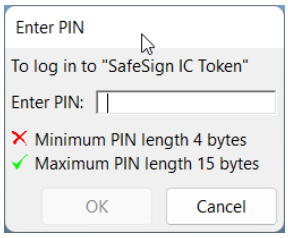


Figure 8: Enter PIN

- Enter the correct PIN and click **OK**

3 The certificate chain will now be imported and when the certificate chain has been successfully imported, you will be informed:

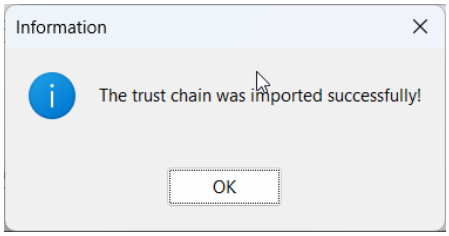


Figure 9: The trust chain was imported successfully

- Click **OK** to close this dialog

4 The certificate chain will now be on the token:

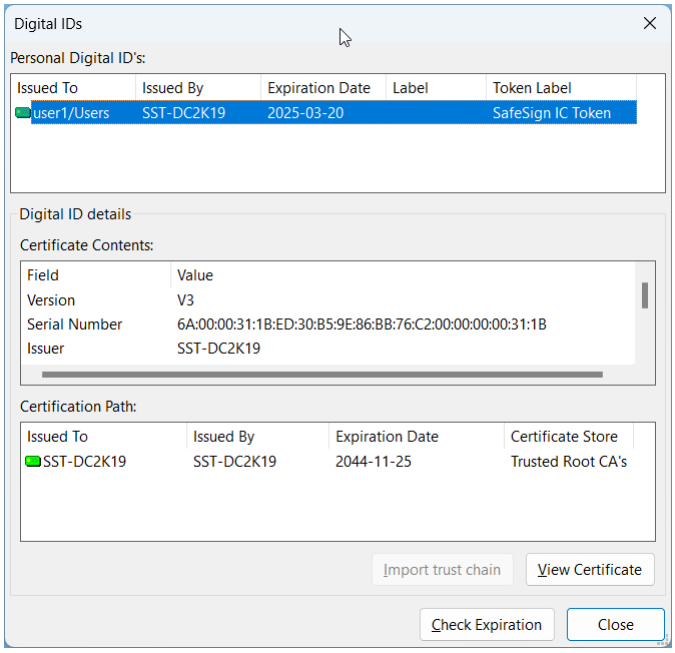


Figure 10: Digital IDs: Certification Path on token

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

3.1.2 View Certificate

The button **View Certificate** allows you to view the contents of the personal Digital ID(s), as well as of the CA certificate(s), when selected.

- Note that you can also view the certificate content when double-clicking any of the Digital IDs listed under Personal Digital ID's or any of the certificates listed under Certificate chain.

1 Upon clicking on **View Certificates** when a Personal Digital ID is highlighted (blue), the following dialog will appear:

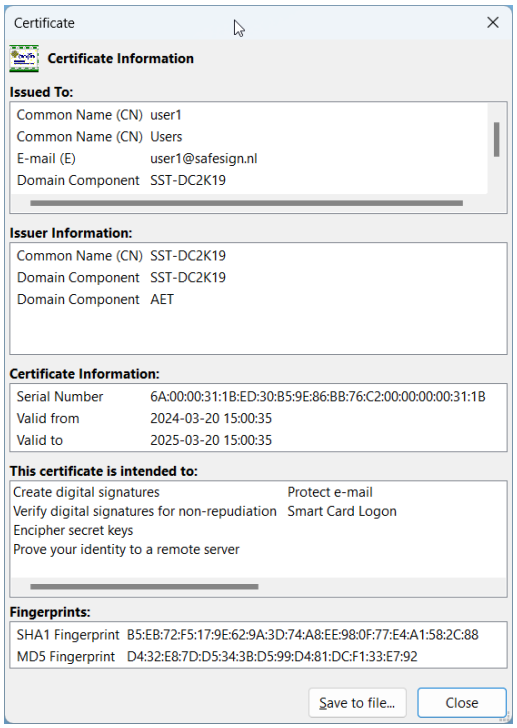


Figure 11: Digital IDs: Certificate Information

This dialog will display the available certificate information.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

It will also give additional information when appropriate, such as when the certificate is about to expire or expired, when the complete trust chain of the certificate cannot be located or a combination of these.

- Click **Close** to close this dialog.

You can save the certificate information to a file, by clicking **Save to file**. Upon clicking **Save to file**, you are allowed to save the file as a Certificate File type (*.cer).

3.1.3 Check Expiration

You may check the expiration status of the Digital ID(s) on the token by clicking the **Check Expiration** button.

When no certificates are about to expire / are expired, the following dialog will appear:

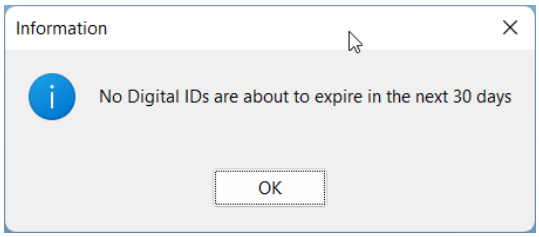


Figure 12: No Digital IDs are about to expire in the next 30 days

- Click **OK** to close this dialog.

When there are certificates about to expire / expired, the Certificate Expiration Warning dialog will appear:

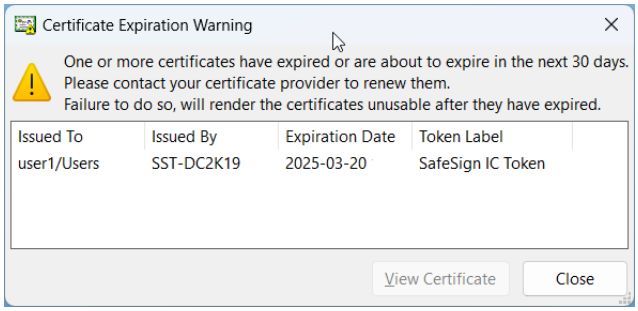


Figure 13: Certificate Expiration Warning

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

This dialog will display both the certificate(s) that will expire in the next 30 days and the certificates that have already expired.

- The days in advance are set default to thirty (30) days.

The Certificate Expiration Warning dialog will also 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:

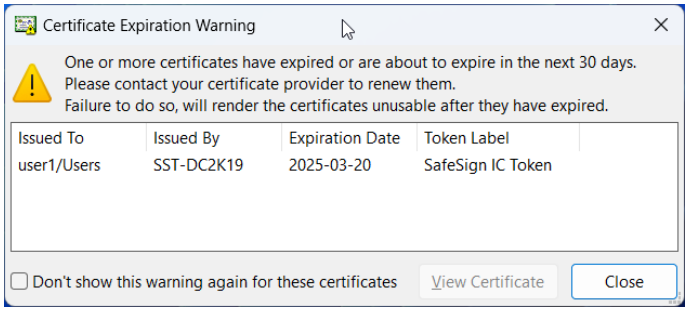


Figure 14: Certificate Expiration Warning

- Note that if you select "Don't show this warning again for these certificates", this warning will not be displayed again for the certificate(s) shown and cannot be activated again (for these certificates).

If you select the certificate(s) about to expire, you may view the contents of the certificate as registered in the Certificate Store, by double-clicking it or clicking **View Certificate**.

3.1.4 Close

Clicking the **Close** button will close the Digital IDs dialog.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

3.2 Import Certificate

The SafeSign IC TAU allows you to import a Certificate Authority (CA) Certificate or Attribute Certificate on your SafeSign IC token. By importing the file, the certificate is securely stored on your token, greatly enhancing the mobility and flexibility of your SafeSign IC token.

SafeSign IC supports the import of:

- DER encoded .CER certificates
- DER encoded .CRT certificates
- DER format certificates

CA certificates may also be imported during token initialisation, please refer to section 4.1.5.

1 To import a CA Certificate, click **Digital IDs > Import Certificate** to be able to specify the location where the Certificate is stored:

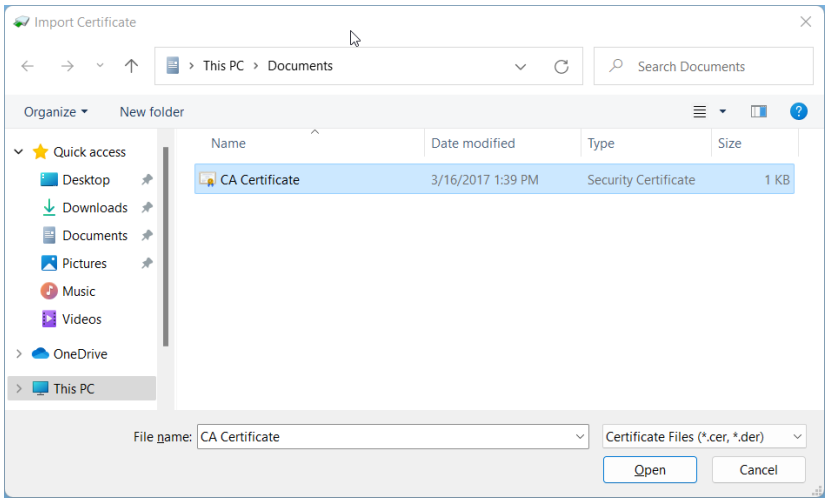


Figure 15: Import Certificate: Select Certificate

- Select the file by clicking on it, then click **Open**

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

2 After selecting the Certificate File to import, you will be asked to enter the PIN of your SafeSign IC Token:

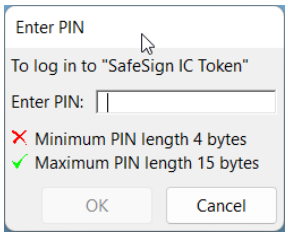


Figure 16: Enter PIN

- Enter the PIN and click **OK** to import the certificate file

3 When the Certificate File has been imported, you will be notified:

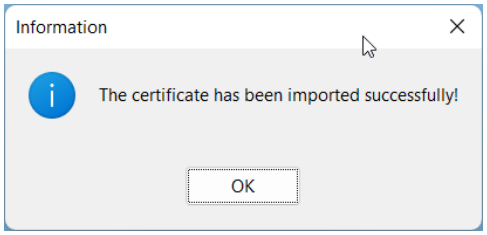


Figure 17: Import Certificate: The certificate has been imported successfully

- Click **OK** to finish the import certificate operation

3.3 Exit

The **Exit** item of the Digital IDs menu will close the SafeSign IC TAU.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4 Token

The **Token** menu of the Token Administration Utility includes the following functionality:

- Section 4.1: Initialise Token: Initialise, Wipe and Recycle
- Section 4.2: Activate Card
- Section 4.3: Change PIN: Change PIN and Change Transport PIN
- Section 4.4: Unlock PIN
- Section 4.5: Change PUK
- Section 4.6: Show Token Info
- Section 4.7: Show Token Objects
- Section 4.8: Change PIN Timeout

Note that the availability of a menu item depends on the type / status of the card inserted. For example, when a blank, uninitialised token is inserted, the option to initialise the token will be available. If an already initialised token is inserted, the option to wipe the token will be available.

4.1 Initialise Token

The menu item Initialise Token may come with different names, depending on the state of the token inserted:

- Initialise Token: when the token is blank, not yet initialised;
- Wipe Token: when the token is already initialised;
- Recycle Token: when the (initialised) token is blocked and has recycle functionality.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

The following sections will describe the different scenarios involved:

- Section 4.1.1: How to initialise a token.
- Section 4.1.2: How to wipe a token.
- Section 4.1.3: How to recycle a token.
- Section 4.1.4: How to initialise a token with PIN Policy.
- Section 4.1.5: How to import a CA Certificate during token initialisation / wiping.

4.1.1 Initialise Token

The first step after installing SafeSign IC is usually to initialise your token (if not yet initialised). This involves setting a token label, a PUK and a PIN for your token.

- 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.

As the correct functioning of SafeSign IC is dependent on a properly produced smart card or USB Token, AET Europe does not support smart cards and / or USB tokens being produced for use with SafeSign IC by vendors that are not approved AET Europe production sites and not in accordance with our QA policies (which require i.a. the SafeSign PKI applet to be pre-installed in a secure environment and a custom key set). Users are not eligible for any support by AET Europe in case of problems, even with a valid SafeSign IC Support Agreement.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

1 When you have not yet initialised your token, your token will be identified in the TAU as a Blank Token" with Token Status "uninitialised" and only the **Initialise Token** item (and the **Show Token Info** item) will be available:

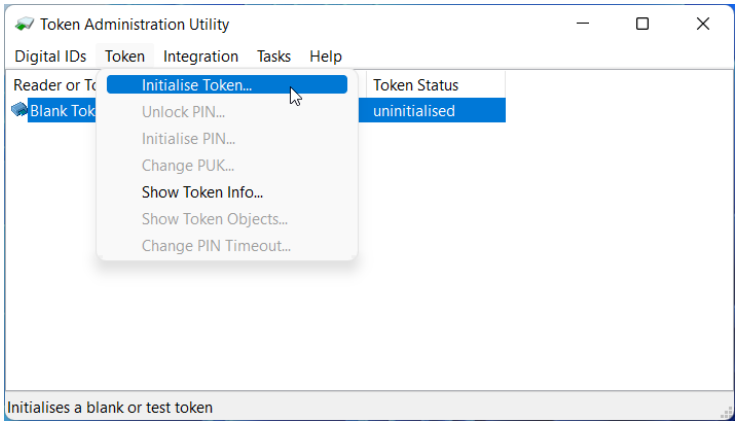


Figure 18: TAU: Initialise Token

- In order to initialise your token, click **Token > Initialise Token**

2 This will open the Initialise Token dialog box, enabling you to initialise your token:

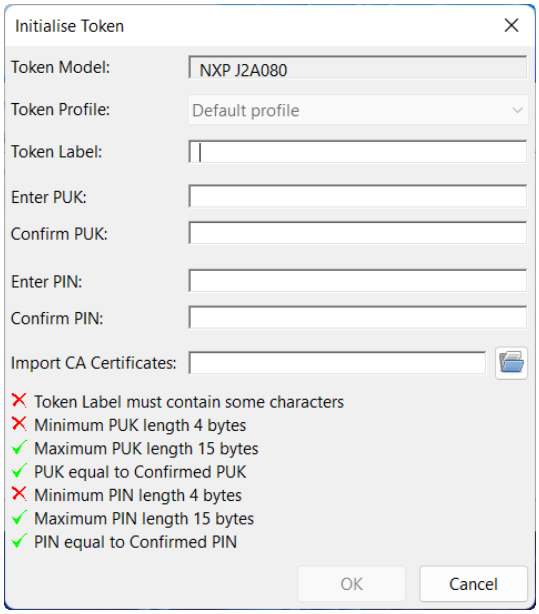


Figure 19: Initialise Token: empty

The 'Token Model' box will identify the type of token you have inserted and are about to initialise.

The 'Token Profile' box will allow you to select the profile to initialise the token with. This box usually contains only contain one (Default) profile. If greyed out, you do not have the (administrator) rights to modify it.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

In order to initialise your token, you must meet a number of requirements. When you have met a certain requirement, the ✗ will become a ✓.

- Fill in the required fields, taking into account the remarks and requirements below:

Field	Requirements	Remarks
Token profile	The Token Profile should be set.	For Java Card v2.2.2 (and higher) cards, there is only one profile available, called "Default profile".
Token Label	The Token Label must contain some characters, it cannot be empty.	Maximum number of characters is 32. Both the token label and the PIN and PUK code may consist in whole or in part of alphanumeric characters, i.e. letters (both small and capital letters), numbers, specials characters / symbols (such as @, # and &) and blank spaces. SafeSign IC enforces a minimum and maximum PIN / PUK length. If you enter a PIN / PUK of less than the minimum allowed or more than the maximum allowed, you will not be able to click the OK button in such instances where the PIN / PUK is required. The PIN / PUK will only be accepted when you enter a PIN / PUK of the required length.
Enter PUK	Minimum PUK length is 4 characters; Maximum PUK length is 15 characters.	
Confirm PUK	Confirmed PUK should be equal to the PUK.	
Enter PIN	Minimum PIN length is 4 characters; Maximum PIN length is 15 characters.	
Confirm PIN	Confirmed PIN should be equal to PIN.	

Table 1: Initialise Token fields

- By default, the PIN and PUK are limited to ASCII characters. However, because some languages use characters with diacrits (such as umlaut, accent grave, etc.) and such characters as ß and €, which consist of 2 or more bytes, it is possible to change this default setting to allow for such characters (as described in the Administrator's Guide). When that is the case, it should be taken into account that one such character may represent two (or more) bytes. Therefore, the dialogs for PIN and PUK entry mention "bytes" instead of "characters".

- Note that the Microsoft Windows Security dialog (to enter your PIN) does not support the use of non-ASCII characters.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

3 When all fields have been entered according to requirements, as follows:

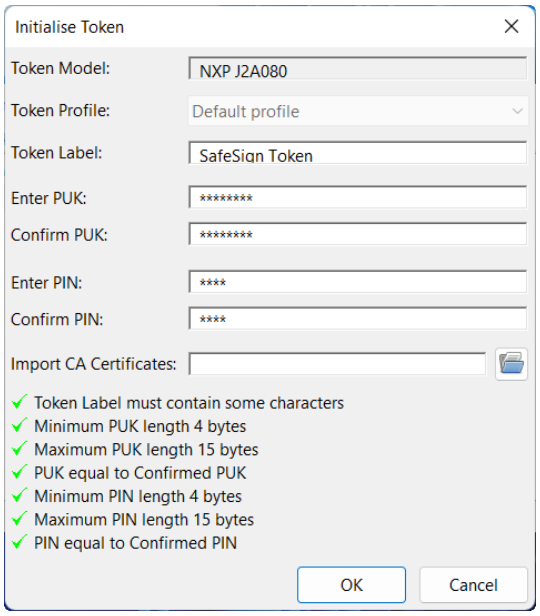


Figure 20: Initialise Token: completed

- Click **OK** to start initialising your SafeSign IC Token.

4 Upon clicking **OK**, you will be informed that your token is being initialised:

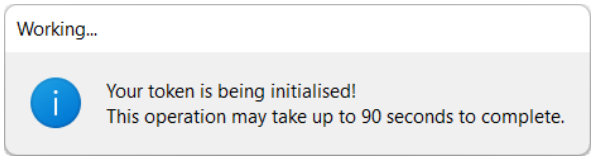


Figure 21: Initialise Token: Your token is being initialised

- Do not interrupt or remove your SafeSign IC token during the initialisation process. If you have a smart card reader with a LED, you may want to keep an eye on the LED of your smart card reader to see whether it is busy or not.

5 When the initialisation operation is completed, the following prompt will appear:

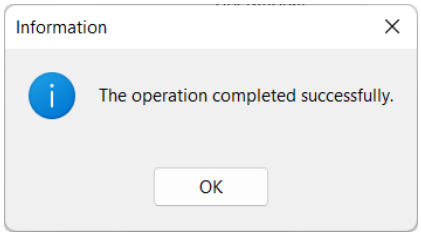


Figure 22: Initialise Token: The operation completed successfully

- Click **OK** to finish the initialisation

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

6 When your token is initialised, the token name will appear in the token window and all operations in the Token menu will be available:

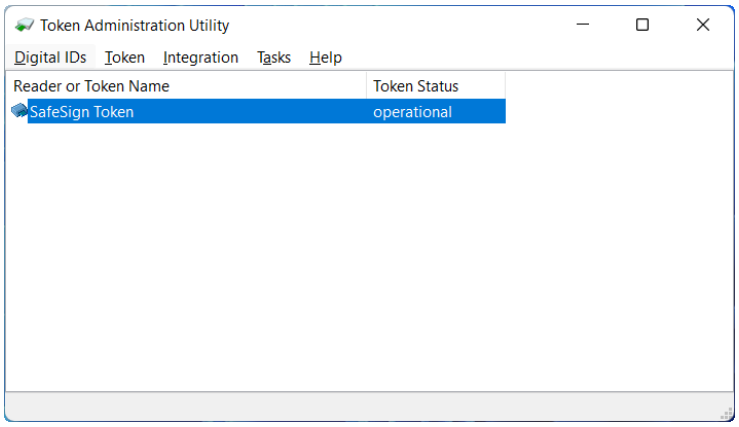


Figure 23: TAU: Token Status 'operational'

4.1.1.1 Operation Failed

When the Initialise Token operation failed, you may get a 'Device Error 0x30'. Check that your smart card reader is functioning properly and whether you have a correct token. Make sure that the token is inserted in the smart card reader and click OK to try to initialise the token again.

When the error message appears that "Your Java Card may not be configured correctly", consider the following possible causes:

- The presence of other applets installed on the card;
- The card does not have the SafeSign IC applet installed correctly;
- The card is read-only;
- The token is not supported by SafeSign IC or the version of SafeSign IC installed.

Make sure that the token is inserted in the smart card reader and click OK to try to initialise the token again. Otherwise, contact your card / software supplier for assistance.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.1.2 Wipe Token

When your token is initialised, you will be able to wipe the token.

- If you want to wipe a card, you will need to enter the current PUK and comply with the settings regarding minimum PUK / PIN length, maximum PIN / PUK length and retry counter, which were set during initialisation and which the card will keep during its lifetime. Note that these settings may be different from the default settings (as mentioned in below).

1 If the token was initialised before, the Token menu will display the item **Wipe Token** (instead of **Initialise Token**, as in Figure 18):

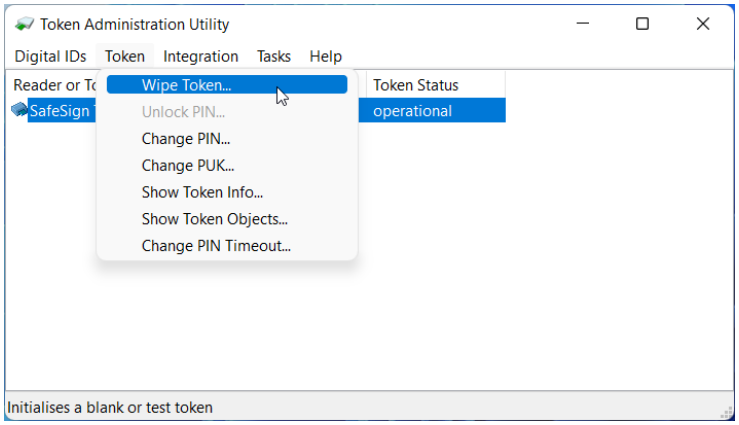


Figure 24: TAU: Wipe token

- In order to wipe your token, click **Token > Wipe Token**

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

2 This will open the Wipe Token dialog box:

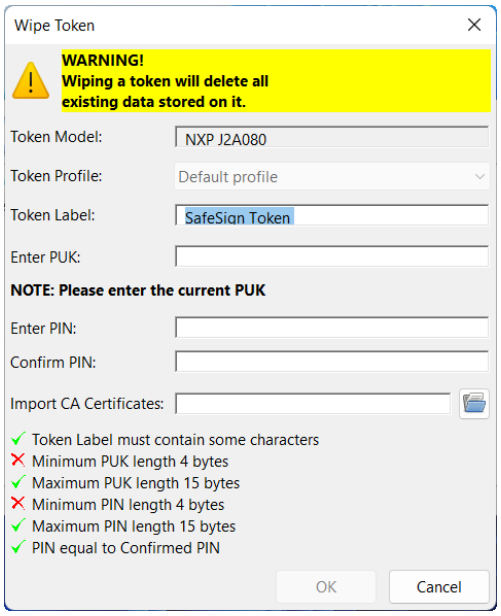


Figure 25: Wipe Token

- In order to wipe your token, you must meet a number of requirements. When you have met a certain requirement, the ✗ will become a ✓.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

- Fill in the required fields, taking into account the remarks and requirements below:

Field	Requirements	Remarks
Token profile	The Token Profile should be set.	For Java Card v2.2.2 (and higher) cards, there is only one profile available, called "Default profile".
Token Label	The Token Label must contain some characters, it cannot be empty.	Maximum number of characters is 32. Both the token label and the PIN and PUK code may consist in whole or in part of alphanumeric characters, i.e. letters (both small and capital letters), numbers, specials characters / symbols (such as @, # and &) and blank spaces. SafeSign IC enforces a minimum and maximum PIN / PUK length. If you enter a PIN / PUK of less than the minimum allowed or more than the maximum allowed, you will not be able to click the OK button in such instances where the PIN / PUK is required. The PIN / PUK will only be accepted when you enter a PIN / PUK of the required length.
Enter PUK	Minimum PUK length is 4 characters; Maximum PUK length is 15 characters.	
Confirm PUK	Confirmed PUK should be equal to the PUK.	
Enter PIN	Minimum PIN length is 4 characters; Maximum PIN length is 15 characters.	
Confirm PIN	Confirmed PIN should be equal to PIN.	

Table 2: Wipe Token fields

- By default, the PIN and PUK are limited to ASCII characters. However, because some languages use characters with diacrits (such as umlaut, accent grave, etc.) and such characters as ß and €, which consist of 2 or more bytes, it is possible to change this default setting to allow for such characters (as described in the Administrator's Guide). When that is the case, it should be taken into account that one such character may represent two (or more) bytes. Therefore, the dialogs for PIN and PUK entry mention "bytes" instead of "characters".

- Note that the Microsoft Windows Security dialog (to enter your PIN) does not support the use of non-ASCII characters

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

3 When all fields have been entered according to requirements, as follows:

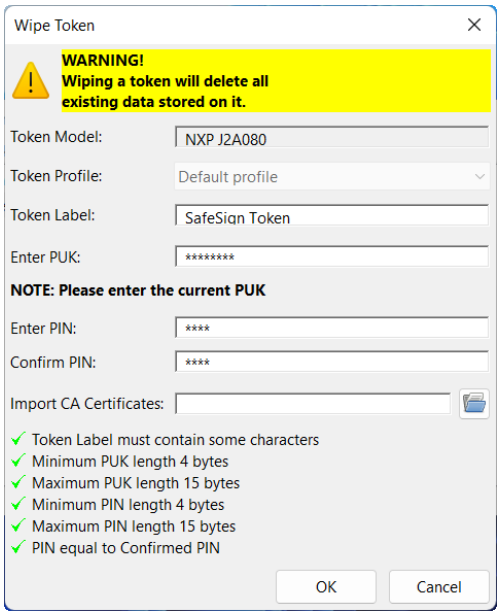


Figure 26: Wipe Token: completed

- Click **OK** to start wiping your SafeSign IC Token.

4 Upon clicking **OK**, you will be informed that your token is being wiped:

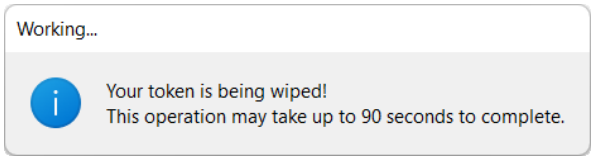


Figure 27: Your token is being wiped!

- Do not interrupt or remove your SafeSign IC token during the wiping process. If you have a smart card reader with a LED, you may want to keep an eye on the LED of your smart card reader to see whether it is busy or not.

5 When the wiping operation is completed, the following prompt will appear:

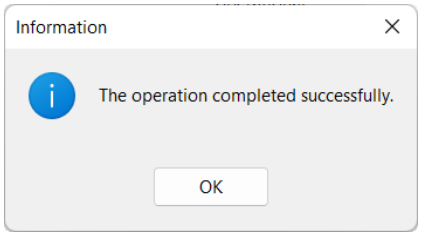


Figure 28: Wipe Token: The operation completed successfully

- Click **OK** to finish the wiping process

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.1.2.1 Operation failed

When the Wipe Token operation failed, you may get a 'Device Error 0x30'. Check that your smart card reader is functioning properly and whether you have a correct token. Make sure that the token is inserted in the smart card reader and click OK to try to initialise the token again.

When the error message appears that "Your Java Card may not be configured correctly", consider the following possible causes:

- The presence of other applets installed on the card;
- The card does not have the SafeSign IC applet installed correctly;
- The card is read-only;
- The token is not supported by SafeSign IC or the version of SafeSign IC installed.

Make sure that the token is inserted in the smart card reader and click OK to try to initialise the token again. Otherwise, contact your card / software supplier for assistance.

4.1.3 Recycle Token

When a special version of the SafeSign IC applet installed with specific applet install parameters is used (which are outside of the scope of this document), it is possible to 'recycle' the token. In that case, once the PIN and PUK are blocked due to too many attempts (i.e. entering an incorrect PIN / PUK until the retry counter is exceeded), it is possible to reset the token, so it can be brought back to a state in which it can be initialised.

- Note that this means that all Digital IDs on the token will be deleted.

If the token is locked, there will be an option in the TAU's Token menu, allowing you to recycle the token and set a new token label, PUK and PIN.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.1.3.1 Recycle Count

When the Recycle applet is installed correctly, the Token Information dialog will display the number of recycle attempts available:

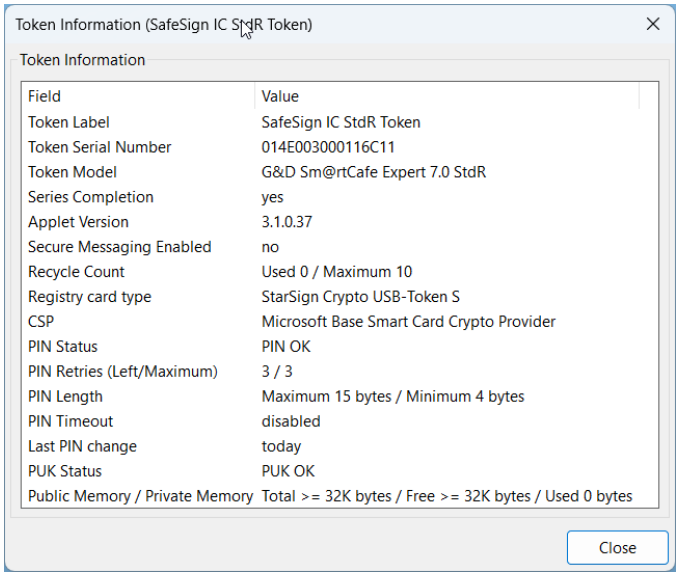


Figure 29: Token Information: Recycle Count

The number of recycle attempt depends on the amount set during applet installation. The TAU Token Information dialog will display the recycle count (used and maximum).

The total number of available recycles for the token in this example is 10.

- Note that the maximum number of recycle attempts that can be set is decimal 127 / hex 7F.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.1.3.2 Recycle Process

1 When the token is locked (i.e. both PIN and PUK are locked), the **Recycle Token** option will be available from the **Token** menu:

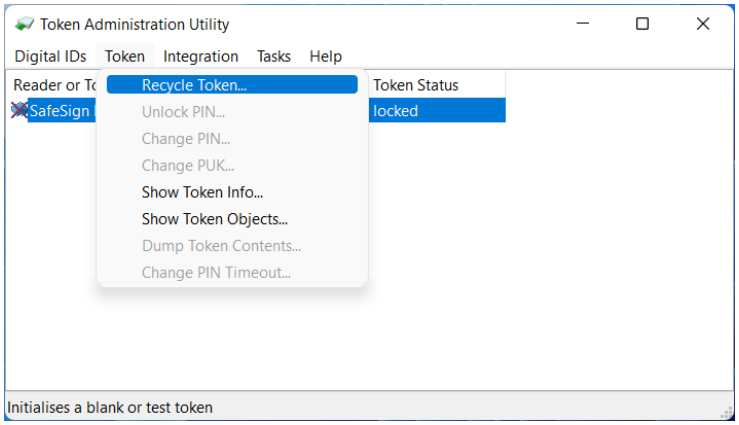


Figure 30: TAU: Recycle Token

- Click Recycle Token

2 After some seconds, the Initialise Token dialog will be opened:

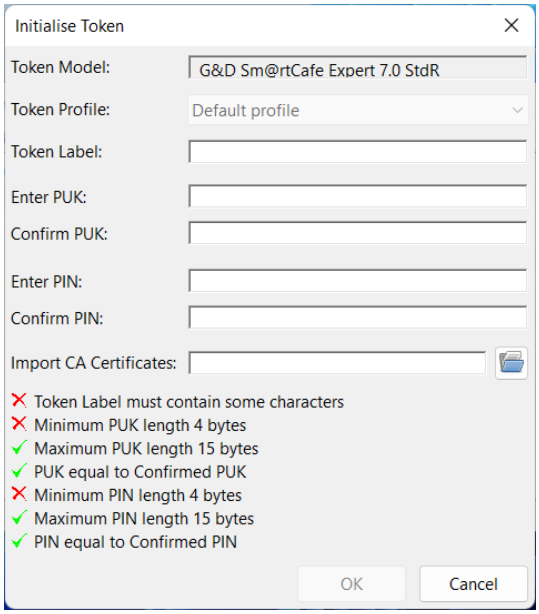


Figure 31: Initialise Token

- You can now initialise your token as described in section 4.1.1.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

If you click **Cancel** in this dialog, your token will be identified as a 'Blank token' and you will be able to initialise the token then, by selecting **Initialise Token** from the Token menu.

- Note that after initialisation, the recycle counter has decreased (by one):

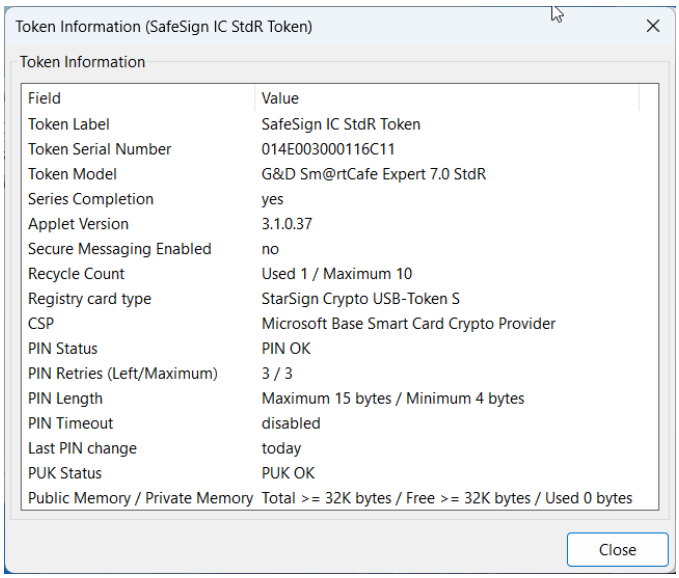


Figure 32: Recycle Count decreased

4.1.3.3 Recycle Count exceeded

When the maximum recycle count has been reached (in our example, this would be 'Used 10 / Maximum 10'), you will not be able to recycle your token anymore.

When you then lock your token again, the option **Recycle Token** will not be available anymore:

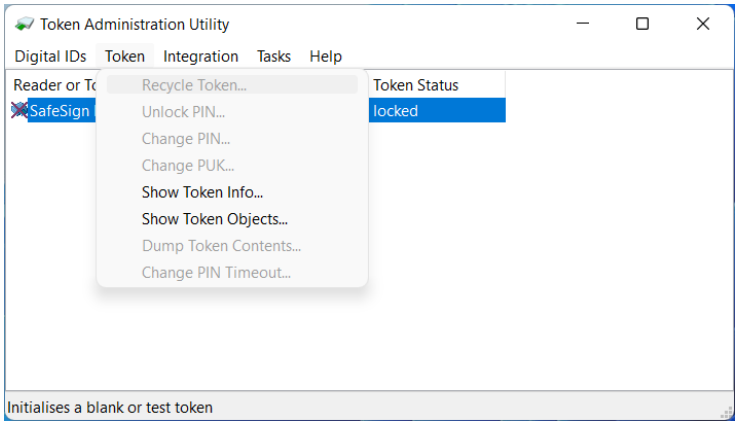


Figure 33: TAU: Token locked

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.1.4 Initialise a Token with PIN Policy

When a special version of the SafeSign IC applet installed with specific applet install parameters is used (which are outside of the scope of this document), it is possible to support cards with a (pre-) defined PIN policy, 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. Currently, an 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 so-called 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.;

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.1.4.1 Initialise Process

1 Upon selecting **Initialise Token** from the Token menu, this will open the Initialise Token dialog box, with the special "balls", displaying the requirements:

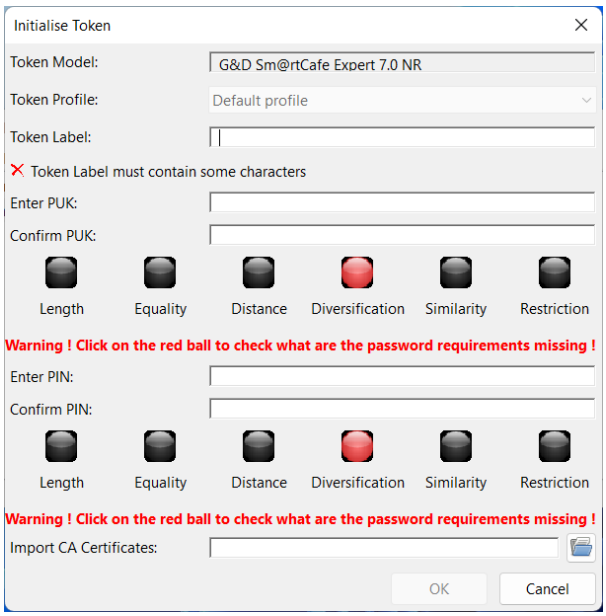


Figure 34: Initialise NR Token

- Hover over the "balls" to see the policy requirements. The policies "Distance", "Similarity" and "Restriction" are not enabled, hence the balls will remain grey

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

The following “balls” are active for this token:

Ball	Label	Description
Length	PIN / PUK length between 6 and 12 characters.	The length of the PIN / PUK should be at least 6 characters, but no more than 12 characters.
Equality	PIN / PUK equal to confirmed PIN / PUK.	The confirmed PIN / PUK entered should be the same as the PIN / PUK entered.
Diversification	Character classification: The length of the PIN / PUK code has to be at least 6 characters. The PIN code has to use a minimum number of 3 classes, chosen between lowercase letters, uppercase letters and numbers and each class has to be composed of a minimum of 1 character.	The PIN / PUK must consist of at least 6 characters and contain at least 1 uppercase letter, 1 lowercase letter and 1 number. When the PIN / PUK is not valid, you will be advised that: “PIN code is invalid. This PIN uses lower case letters, numbers. It is missing upper case letters.”

Table 3: PIN Policy Balls

2 Only when you have entered a PIN and PUK that satisfy all these requirements, will you be able to initialise the token:

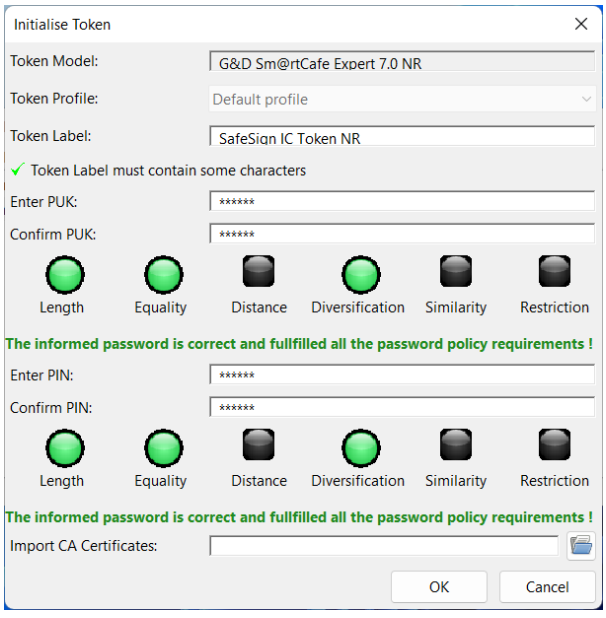


Figure 35: Initialise NR Token: completed

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

When a ball is / becomes green, this means that the policy is enabled and that the entered PIN / PUK fulfils the policy requirements.

- Click **OK** to initialise the token.

When a particular requirement is not met, the relevant ball will be red:

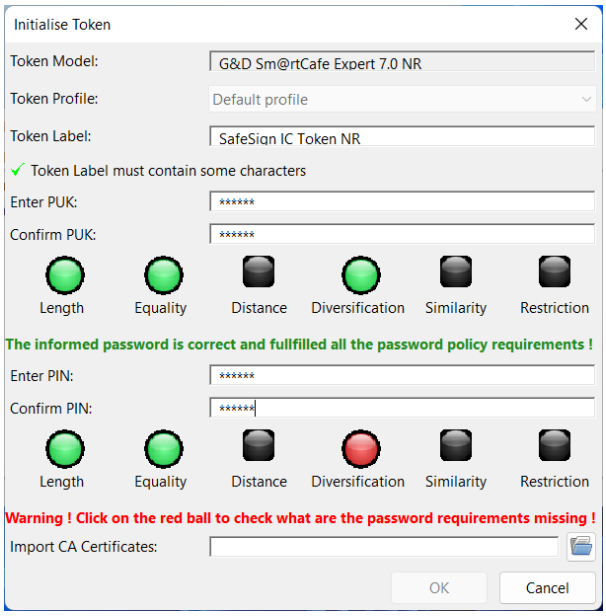


Figure 36: Initialise NR Token: Password requirements missing

In the screenshot above:

- The Length ball is green: the length of the PIN is correct;
- The Equality ball is green: the confirmed PIN matches the PIN;
- The Diversification ball is red: the PIN does not have the minimum number of 3 classes.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.1.4.2 Change PIN

When you change the PIN of a token that is PIN-policy enabled, the PIN policy is enforced:

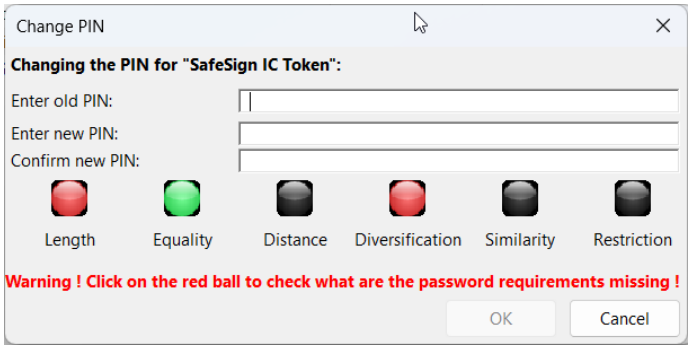


Figure 37: Change PIN NR Token

4.1.4.3 Enter PIN

When you need to enter the PIN for a token that is PIN-Policy enabled, the dialog is not "policy-enabled", for security reasons:

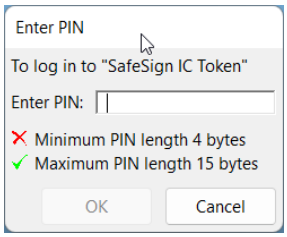


Figure 38: Enter PIN

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.1.5 Import CA Certificates

The SafeSign IC TAU enables the import of:

- DER encoded .CER (CA) certificates
- DER encoded .CRT (CA) certificates
- DER format (CA) certificates

There are two ways to do this:

1 By means of the item Import Certificates of the Digital ID menu, allowing you to select single CA certificates for import (“one at a time”), as described in section **Fout! Verwijzingsbron niet gevonden.**;

2 During token initialisation, by selecting a directory where one or multiple CA certificates is / are stored (“all at once”), as described in this section.

1

In the Initialise Token dialog, the option Import CA Certificates allows you to select a directory where the CA certificate(s) is (are) stored:

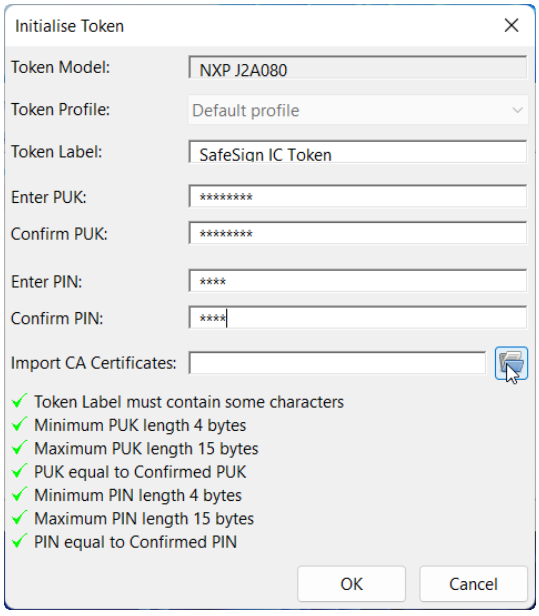


Figure 39: Initialise Token

- Click on the **Browse** icon

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

2 Upon clicking on the **Browse** icon, the Browse for Folder dialog will open, allowing you to select a directory containing CA Certificates:

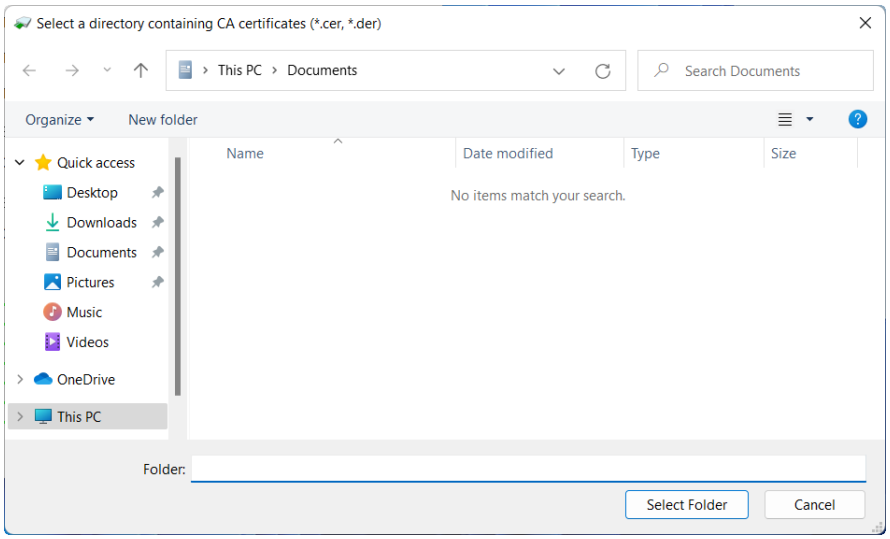


Figure 40: Import CA certificates: Browse For Folder

- Select a directory and click **OK**

3 Upon clicking **OK**, the directory will be indicated in the corresponding box:

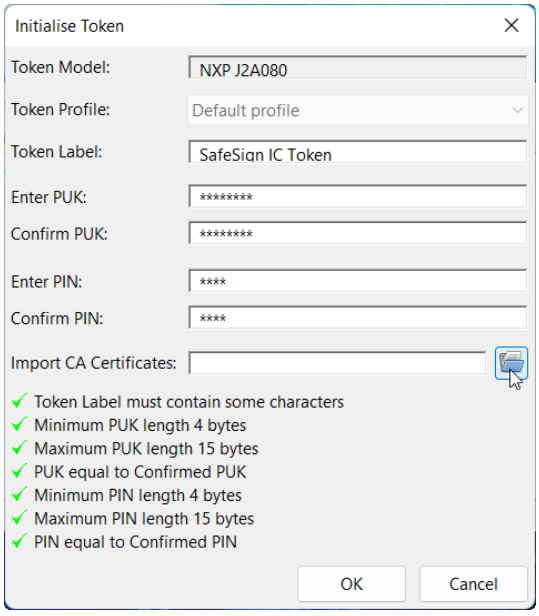


Figure 41: Initialise Token: Import CA certificates

- Note that all CA certificates present in the directory will be imported.

- Click **OK** to initialise the token

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4 Upon clicking **OK**, you token will be initialised, during which the CA certificate(s) is imported:

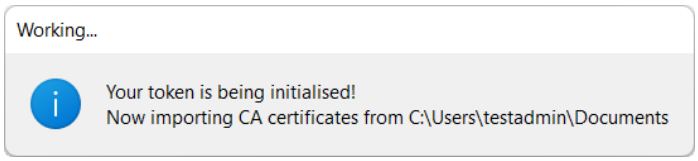


Figure 42: Initialise Token: Now importing CA certificates

5 When the initialisation operation is completed, the following prompt will appear:

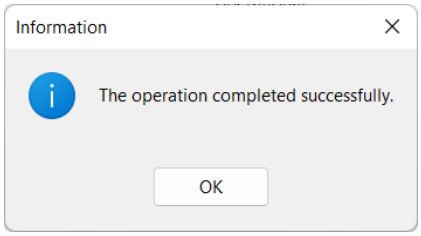


Figure 43: Initialise Token: The operation completed successfully

- Click **OK** to finish the initialisation

The PKCS#11 objects dialog will now display the (imported) CA certificate:

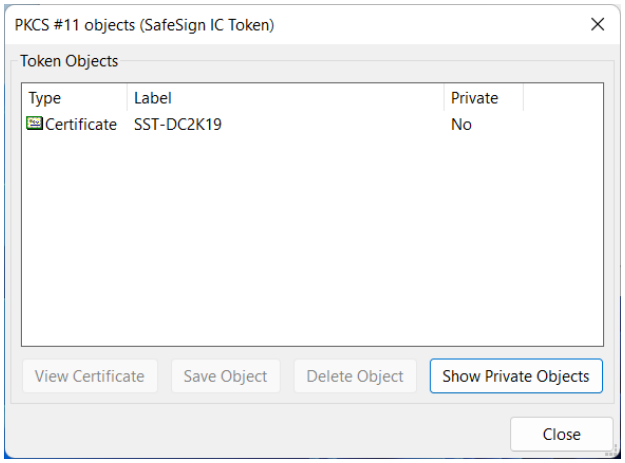


Figure 44: PKCS#11 objects: CA Certificate

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.2 Activate Card

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.

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 section below describes how to activate an UZI-pas QSCD card, as an example.

4.2.1 UZI-pas QSCD

The UZI-pas 3 card and UZI-pas 4 card need to be activated before they can be used.

If the user does not activate the card, the keys on the card cannot be used, although the card does have a valid PIN and the user enters it correctly. This means that if the user tries to use the card with PKI applications before it is activated, an error message will be displayed.

Activating the UZI-pas card requires the user to authenticate to the card by entering the correct PIN, as included in the PIN mailer the user has received; there is no separate or special activation code required.

When an UZI-pas 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 CC certified SafeSign IC applet and the specific UZI-pas ATR.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

If these requirements are met, the **Token** menu of the SafeSign IC Token Administration Utility will display the option **Activate card**:

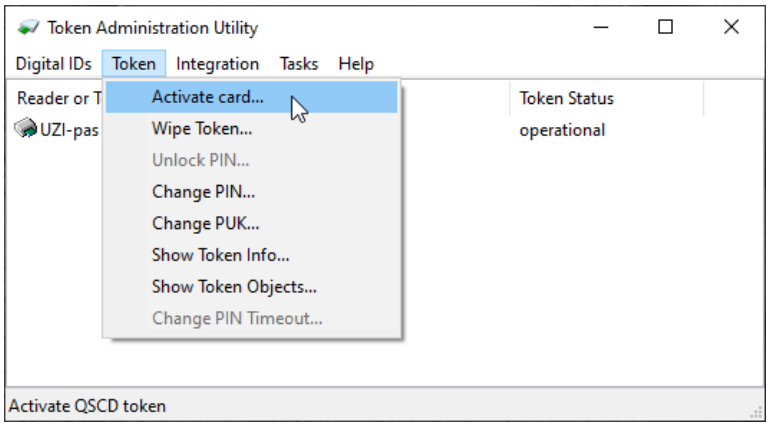


Figure 45: Token Administration Utility: Activate card

1 If this option is selected, the Activate card dialog will be displayed:

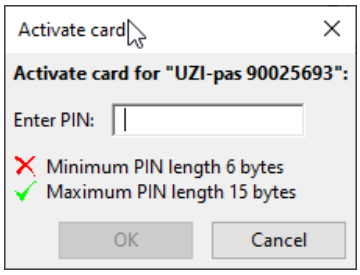


Figure 46: Activate card

This dialog will ask the user to enter the PIN (i.e. to authenticate with his PIN) for the UZI-pas, which is included in the PIN mailer the user has received.

- Enter the PIN and click **OK**

2 After entering the correct PIN and clicking **OK**, the card will be successfully activated:

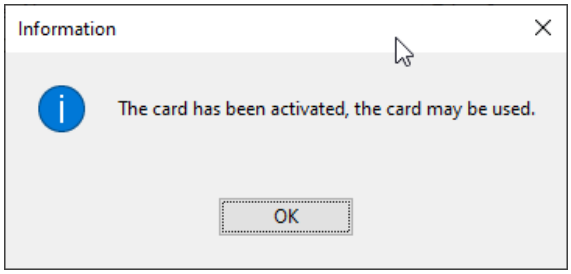


Figure 47: Activate card: Information

The keys on the card are activated now and ready to be used.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

When the UZI-pas has been activated, the card and its keys can be used in PKI applications.

If the card is already activated and the user tries to activate his card for the second time (or subsequent times), the following message will be displayed:

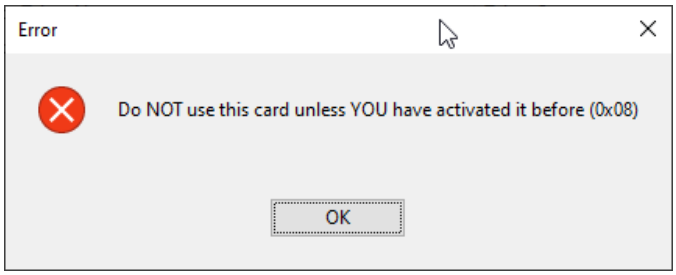


Figure 48: Activate card: Do NOT use this card unless YOU have activated it before

- It is important that activating the card is a one-time and conscious action of the user. If the user tries to activate the card and gets the error message above, and he did not activate the card himself / herself before, he should verify why this is so or who activated his card and not use it.

4.3 Change PIN

The menu item Change PIN may come with different names, depending on the state of the token inserted:

- Change PIN, as described in section 4.3.1;
- Change Transport PIN, as described in section 4.3.2.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.3.1 Change PIN

The SafeSign IC TAU enables you to change the PIN for your SafeSign IC Token.

1 In order to do so, select **Change PIN** from the **Token** menu. This will open the following dialog:

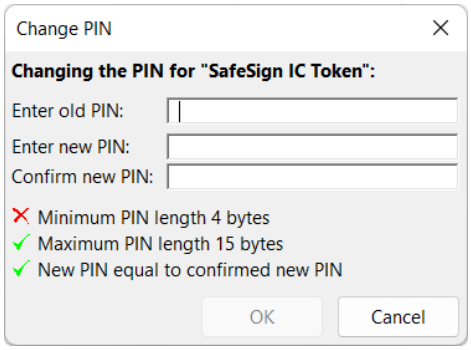


Figure 49: Change PIN

This dialog will identify the token (by its label) of which you want to change the PIN ("SafeSign IC Token" in our example). Only when you enter the correct old PIN and enter a new PIN and confirmed new PIN that are equal (and fulfil the PIN length requirements), will the **OK** button be available.

- Enter the old PIN, the new PIN and confirm new PIN, then click **OK** to change the PIN

2 When the PIN has been successfully changed, the following dialog will be displayed:

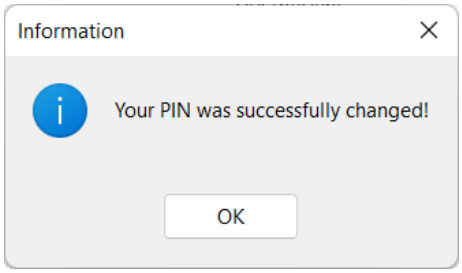


Figure 50: Change PIN: Your PIN was successfully changed

- Click **OK** to close this dialog box.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.3.1.1 PIN Status

Each time you enter your PIN for the SafeSign IC Token, either within the SafeSign IC TAU or when asked to do so in applications, the SafeSign IC TAU will provide you with information as to the status of the PIN.

By default, you have three attempts to enter the correct PIN and SafeSign IC will keep a counter and give you information as to the status of the PIN. When you enter an incorrect PIN three times, the token will be LOCKED and you should use the Unlock PIN item from the Token menu (as described in section 4.4).

The counter for incorrect PIN entries will be reset (to three attempts to enter the PIN) if you enter a correct PIN after entering an incorrect PIN (but no more than three times).

In the Token Information dialog (**Token > Show Token Info**), the status of the PIN is displayed.

There are four possible scenarios:

1 OK

2 PIN has been entered incorrectly at least once

3 One final attempt left to enter the PIN correctly

4 LOCKED

In addition, when you perform an operation within the SafeSign IC TAU, such as Enter PIN (or any other item for which PIN entry is required), you will receive information on the status of the PIN in the dialog involved.

Here also, four notifications are possible:

1 When the PIN is OK (has not been entered incorrectly before):

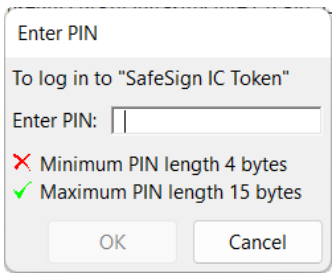


Figure 51: Enter PIN

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

2 When the PIN has been entered incorrectly (once):

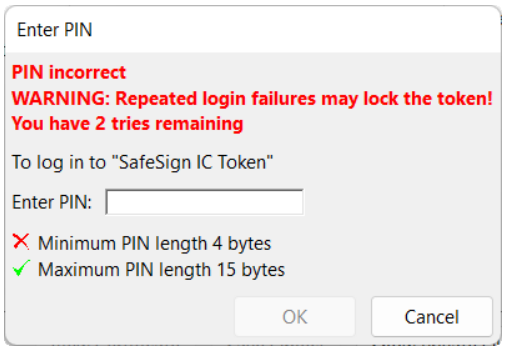


Figure 52: Enter PIN: You have 2 tries remaining

3 When one final attempt is left to enter the PIN correctly:

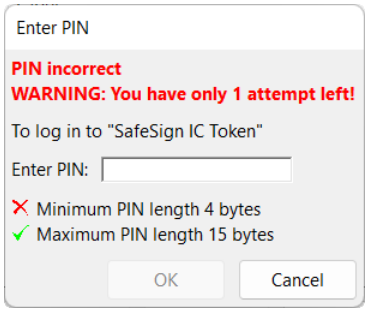


Figure 53: Enter PIN: You have only 1 attempt left

4 When the PIN is locked:

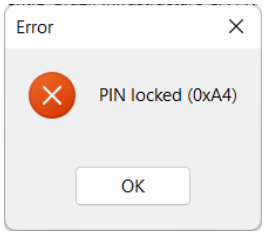


Figure 54: Enter PIN: PIN locked

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

When you close one menu item in the SafeSign IC TAU and you enter an incorrect PIN in another (or the same) dialog, you will be notified of this fact and the status of incorrect PIN entries. For example, the dialog below indicates you have already entered an incorrect PIN once and that you have only two attempts left to enter the correct PIN:

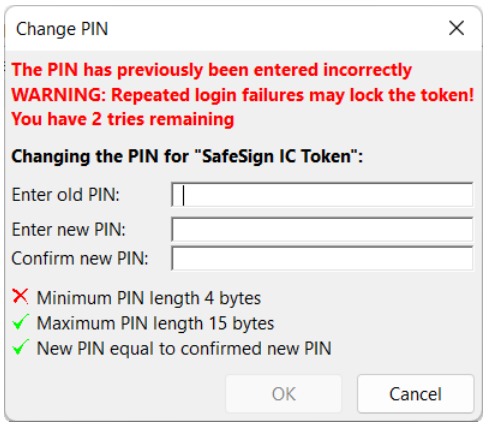


Figure 55: Enter PIN: The PIN has previously been entered incorrectly

4.3.2 Change Transport PIN

Your SafeSign IC token may have been initialised with a Transport PIN.

A Transport PIN is a temporary PIN on the token that has to be changed into a personalised PIN before the token can be used.

If a Transport PIN is set on the token, the Token Information dialog will display the PIN Status:

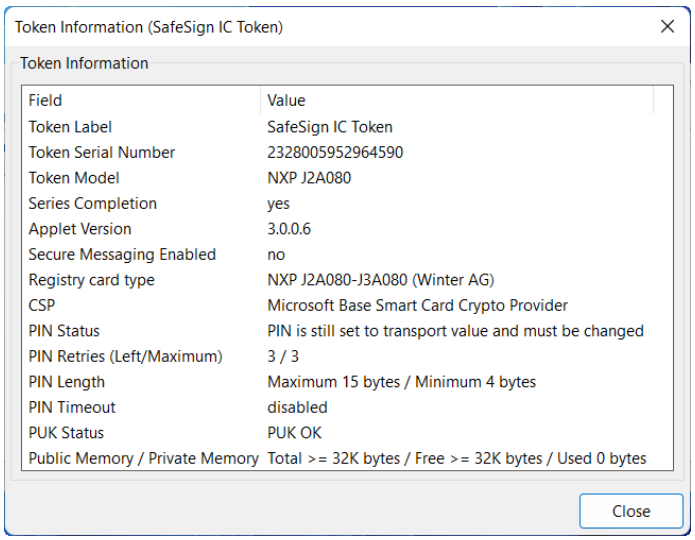


Figure 56: Token Information: PIN is still set to transport value

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

1 In the TAU, the option **Change transport PIN** is available:

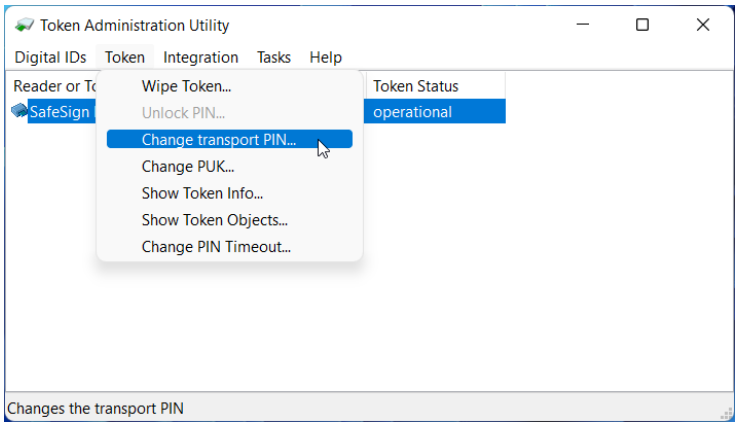


Figure 57: TAU: Change transport PIN

- Select Change transport PIN (as above)

2 This will open the Change transport PIN dialog:

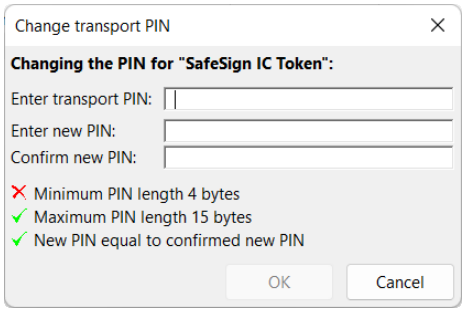


Figure 58: Change transport PIN

- Enter the correct transport PIN, a new PIN for the token and confirm the new PIN

3 The transport PIN will now be changed into the new PIN, after which you will be informed:

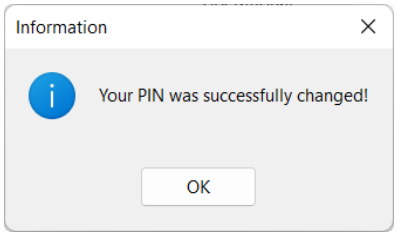


Figure 59: Change transport PIN: Your PIN was successfully changed

- Click **OK:** You can now use your token with your own PIN.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.4 Unlock PIN

The SafeSign IC TAU enables you to unlock the PIN for your SafeSign IC Token when your PIN is locked.

- Note that the Unlock PIN item will only be available when the PIN is actually locked. If not, the item will be greyed out.

The most common way is to unlock the PIN using the PUK. If a challenge response key is generated on the token, it is also possible to unlock the PIN by means of off-line PIN unlock.

- Section 4.4.1 describes how to unlock the PIN using the PUK.
- Section 4.4.2 describes how to unlock the PIN using challenge response.

4.4.1 Unlock using the PUK

1 If your PIN is locked, select **Unlock PIN** from the **Token** menu to open the Unlock PIN dialog:

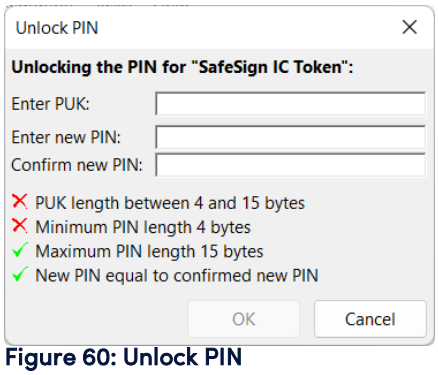


Figure 60: Unlock PIN

This dialog will identify the token (label) of which you want to unlock the PIN ("SafeSign IC Token" in our example). Only when you enter the correct PUK and a new and confirmed PIN that are equal (and fulfil the PIN length requirements), will the OK button be available.

- Enter the current PUK, a new PIN and confirm the new PIN and click **OK** to unlock the PIN

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

2 When the PIN has been successfully unlocked, the following dialog will be displayed:

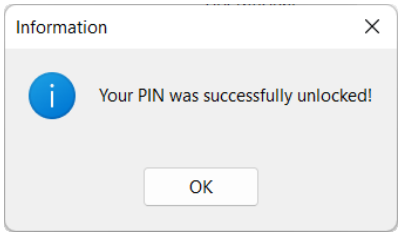


Figure 61: Unlock PIN: Your PIN was successfully unlocked

- Click **OK** to close this dialog box.

Your PIN should be unlocked and ready to use again, which you may check by being able to use all menu items again.

4.4.2 Unlock via off-line PIN unlock

The SafeSign IC TAU has built-in support for off-line PIN unlock. When enabled, the user will be allowed to choose how to unlock the PIN, either using the PUK or via off-line PIN unlock.

- Note that this scenario assumes that a system is in place to generate challenge-response keys on a token and a helpdesk to assist you in the process. For more information, contact AET Europe SafeSign Support.

1 If your PIN is locked, selecting **Unlock PIN** from the **Token** menu will open the Unlock PIN dialog allowing to choose the unlocking method:

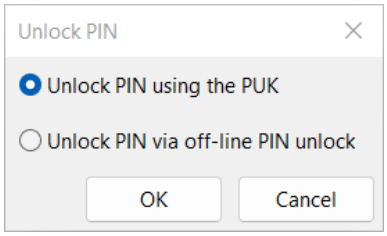


Figure 62: Unlock PIN: unlocking methods

- Select the option Unlock PIN via off-line PIN unlock

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

2 This will open the Off-line PIN unlock wizard:

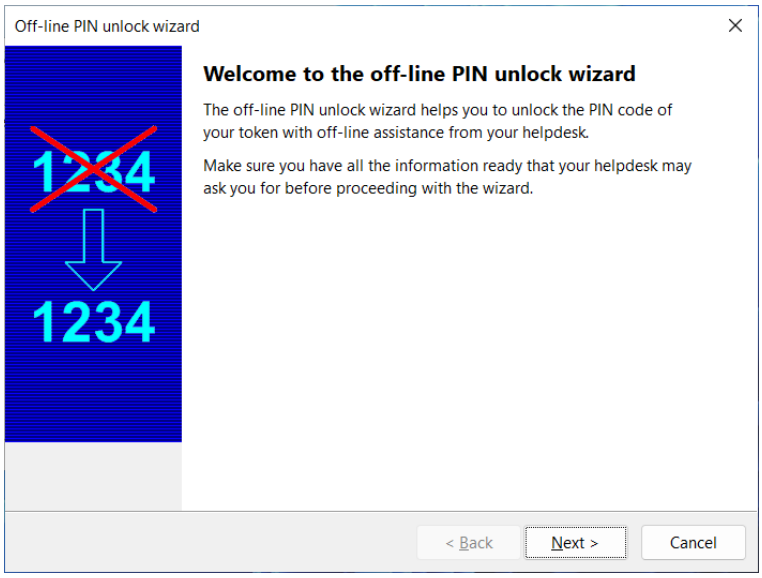


Figure 63: Off-line PIN unlock wizard: Welcome to the off-line PIN unlock wizard

- Click **Next** to continue

3 The first step is to select the unlock algorithm to use. The helpdesk employee should tell you which algorithm to use:

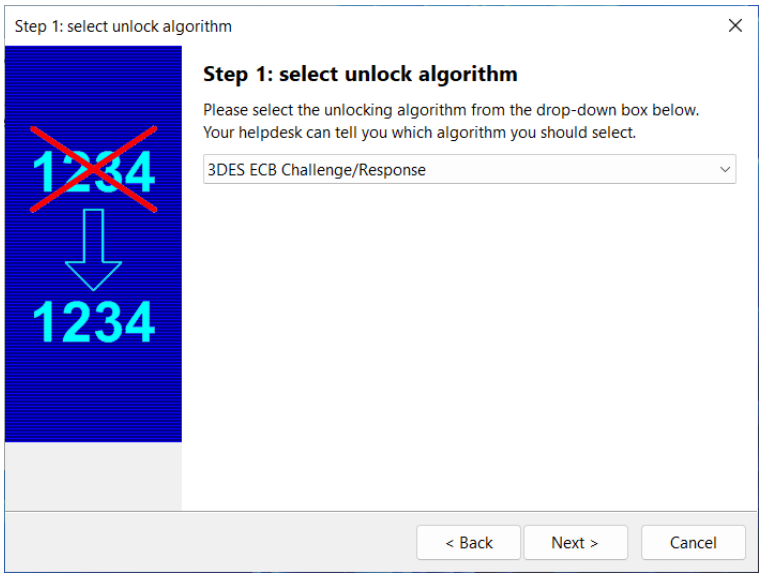


Figure 64: Off-line PIN unlock wizard: Step 1: select unlock algorithm

- Select the unlocking algorithm and click **Next** to continue

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4 Once you have selected an algorithm, the next step is to report the challenge requested from the card:

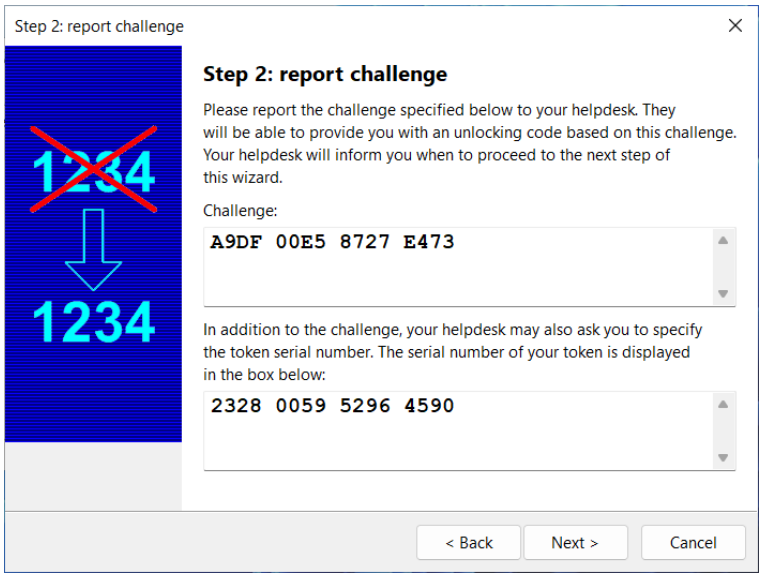


Figure 65: Off-line PIN unlock wizard: Step 2: report challenge

- Report the challenge to your helpdesk and click **Next** to continue

5 When you have received the response, you can enter the response and a new PIN code for the token:

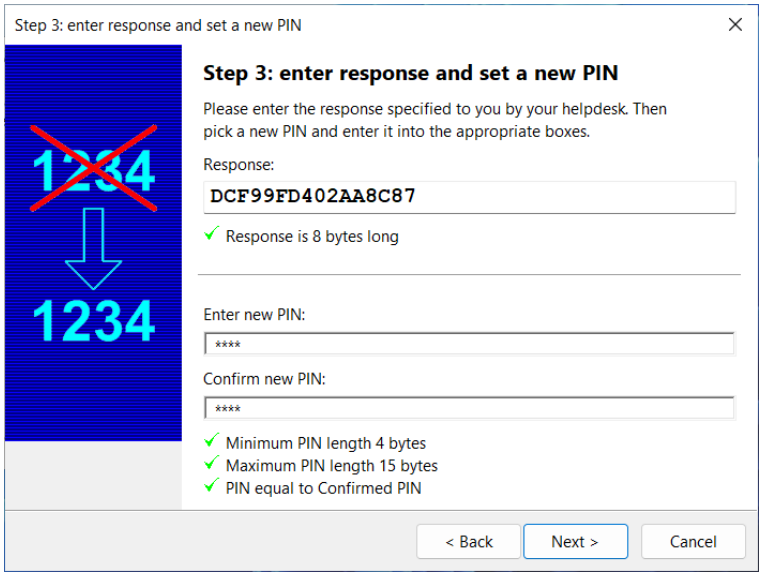


Figure 66: Off-line PIN unlock wizard: Step 3: enter response and set a new PIN

The wizard checks the response length as well as the length of the new PIN.

- Complete the fields and click **Next** to continue

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

6 The final page of the wizard shows whether the unlock procedure succeeded:

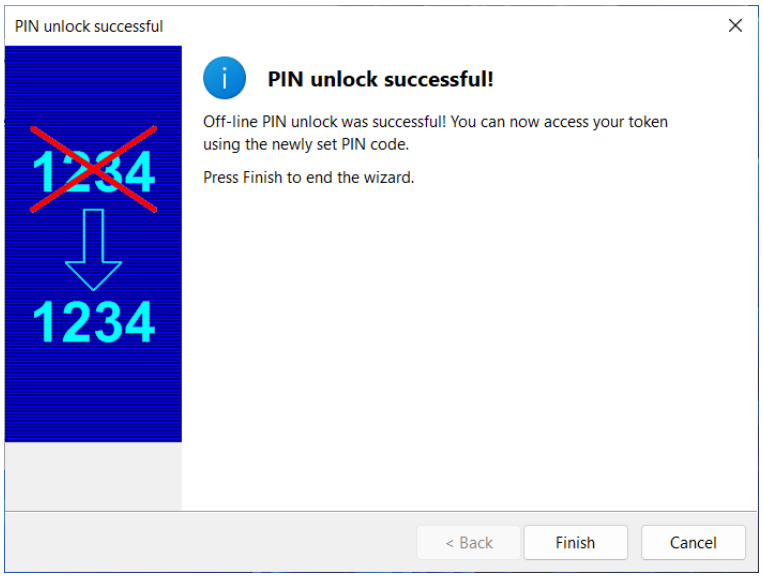


Figure 67: Off-line PIN unlock wizard: PIN unlock successful

- Click **Finish** to end the wizard.

If the unlock failed (for example when the response is incorrect), the following dialog will be displayed:

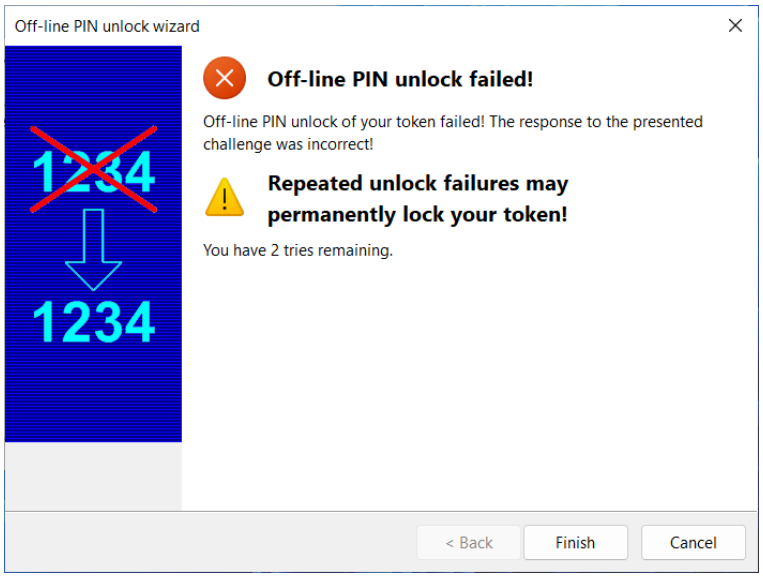


Figure 68: Off-line PIN unlock wizard: Off-line PIN unlock failed

If off-line PIN unlock fails after the two remaining tries, you can only unlock the PIN using the PUK, as described in section **Fout! Verwijzingsbron niet gevonden.**.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.5 Change PUK

The SafeSign IC TAU enables you to change the PUK for your SafeSign IC Token.

1 In order to do so, select **Change PUK** from the **Token** menu to open the following dialog:

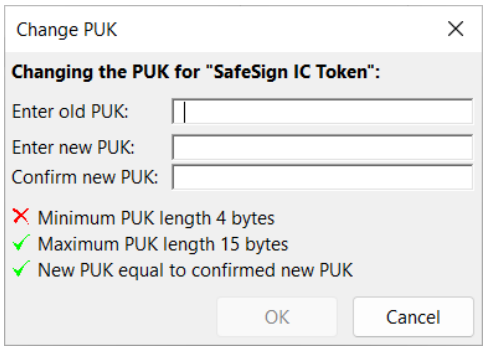


Figure 69: Change PUK

This dialog will identify the token (label) of which you want to change the PUK ("SafeSign IC Token" in our example). Enter the old PUK, a new PUK and confirm the new PUK. Only when you enter the correct old PUK and a new and confirmed PUK that is equal (and fulfill the PUK length requirements), will the OK button be available.

- Click **OK** to change the PUK

2 When the PUK has been successfully changed, the following dialog will be displayed:

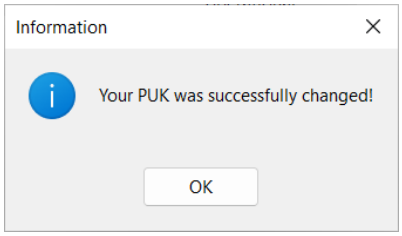


Figure 70: Change PUK: Your PUK was successfully changed

- Click **OK** to close this dialog box.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.5.1 PUK information

Every time you enter your PUK for the SafeSign IC Token, the SafeSign IC TAU will provide you with information as to the status of the PUK.

By default, you have three attempts to enter the correct PUK and SafeSign IC will keep a counter and give you information as to the status of the PUK. When you enter an incorrect PUK three times, the PUK will be LOCKED and cannot be unlocked.

The counter for incorrect PUK entries will be reset (to three attempts to enter the PUK) if you enter a correct PUK after entering an incorrect PUK (but no more than three times).

In the Token Information dialog (**Token > Show Token Info**), the status of the PUK is displayed. There are four possible scenarios:

1. OK
2. PUK has been entered incorrectly at least once
3. One final attempt left to enter the PUK correctly
4. LOCKED

When you enter an incorrect PUK three times, the PUK will be locked and cannot be unlocked. However, you can still use the token with the PIN.

- Note that when both PIN and PUK are locked, the Token Status will be “locked” and the token cannot be used anymore.

In addition, when you perform an operation within the SafeSign IC TAU, such as Change PUK (or any other item for which PUK entry is required), you will receive information on the status of the PUK in the dialog involved.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

Here also, four notifications are possible:

1 When the PUK is OK (has not been entered incorrectly before):

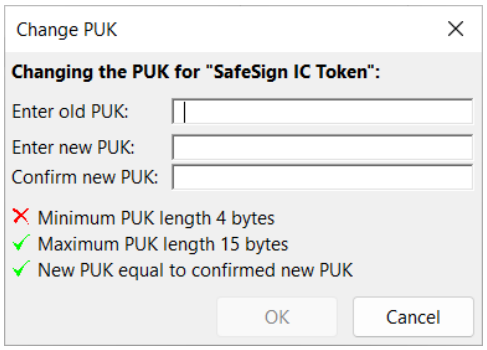
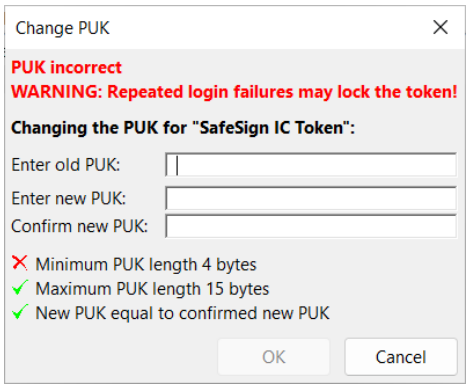


Figure 71: Change PUK

2 When the PUK has been entered incorrectly:



FFigure 72: Change PUK: Repeated login failures may lock the token

3 When one final attempt is left to enter the PUK correctly:

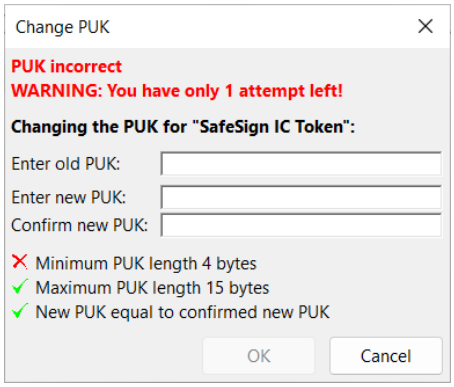


Figure 73: Change PUK: You have only 1 attempt left

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4 When the PUK is locked:

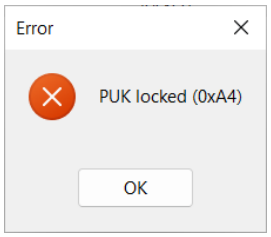


Figure 74: PUK locked

When you close one menu item in the SafeSign IC TAU and you enter an incorrect PUK in another (or the same) dialog, you will be notified of this fact and the status of incorrect PUK entries. For example, the dialog below indicates you have already entered an incorrect PUK previously:

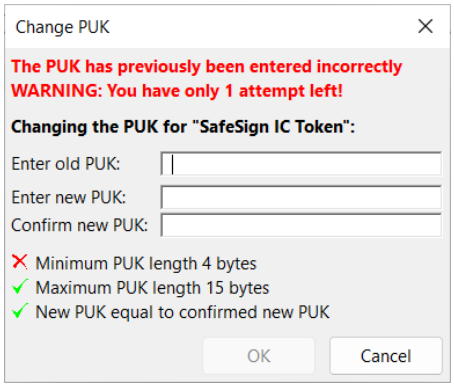


Figure 75: Change PUK: The PUK has previously been entered incorrectly

- Just as for the PIN, it is also possible to enable a retry counter for the PUK (in the registry). When the PUK retry counter is enabled, the dialogs that require PUK entry will also display how many attempts are left:

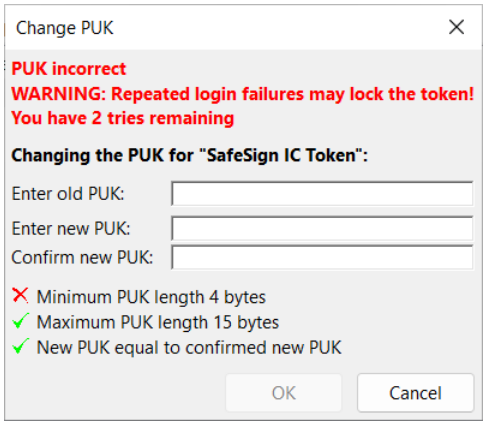


Figure 76: Change PUK: You have 2 tries remaining

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.6 Show Token Info

The Token Information dialog (**Token > Show Token Info**) displays information on the token inserted.

When the token is not initialised, the Token Information dialog will look like this:

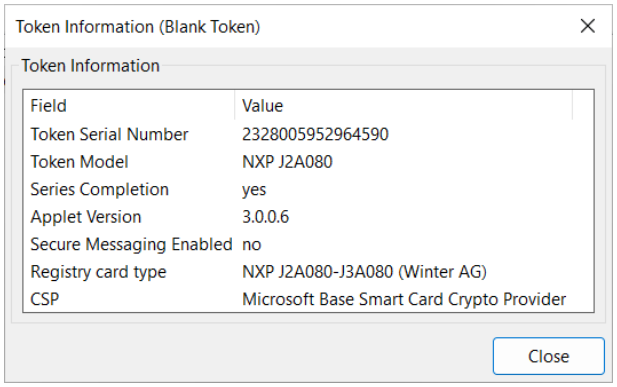


Figure 77: Token Information: Blank Token

When the token is initialised, the Token Information dialog will look like this:

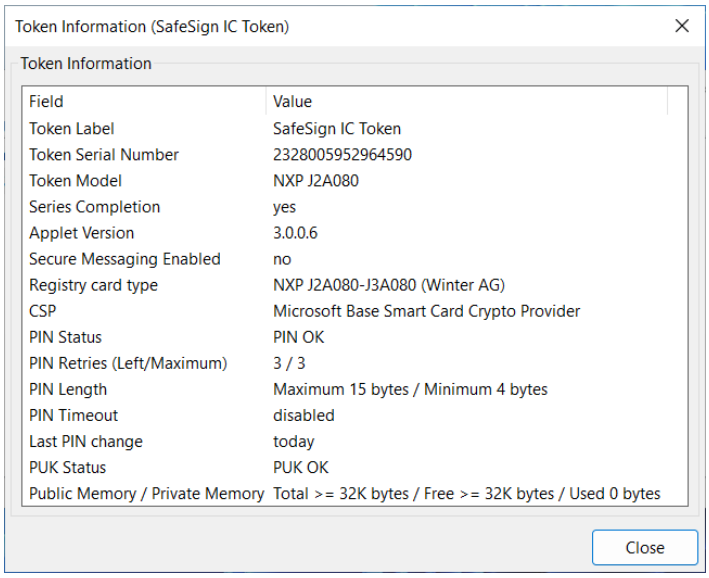


Figure 78: Token Information: SafeSign IC Token

The following sections will describe the information displayed in the Token Information fields.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.6.1 Token Label

Displays the label of the token, as given to it upon initialisation.

4.6.2 Token Serial Number

Displays the serial number of the token, which usually includes the chip serial number.

4.6.3 Token Model

Displays the token model / type by which it is known to the SafeSign IC software.

4.6.4 Series Completion

Displays whether the token is a test token or a production token.

1. When series completion is [No], the token is a test token.
2. When series completion is [Yes], the token is a production token.

- Customers should have a production token (where series completion is [Yes]), with the SafeSign IC applet installed in a secure way by an AET Europe approved card vendor. The use of a test token is not secure and any use of a test token makes all support and/or warranty null and void.

4.6.5 Applet Version

Displays the version of the SafeSign IC applet installed on the token.

- Note that there may be different applet versions for different cards.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.6.6 Secure messaging enabled

The Secure Messaging Enabled field indicates whether the card you are using has secure messaging enabled (in addition to having a specific Brazilian RIC applet installed).

4.6.7 Registry card type

In addition to the token model, a token should also have a registry card type name. This field displays the name of the token as it is registered with in the registry key where the ATRs of cards are stored for use in Microsoft CryptoAPI (NG) applications with the Microsoft Base Smart Card Crypto Provider.

On 64-bit Operating Systems, the card ATRs are stored in both the 64-bit and 32-bit registry respectively:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Calais\SmartCards\

See also section 4.6.8.

4.6.7.1 Unknown ATR

When the ATR of a token is not registered correctly, the Token Information dialog will display that the ATR of the token is unknown. In that case, you will not be able to use the token in Microsoft CryptoAPI (NG) applications.

For example, when trying to log on to Windows with a token with an unknown ATR (when it does contain a smart card user or smart card logon certificate), an error message will appear when logging on: “The smart card supplied requires drivers that are not present on this system”.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

If the token has an unknown ATR, the registry card type will say “Unknown ATR” and no CSP will be available for it:

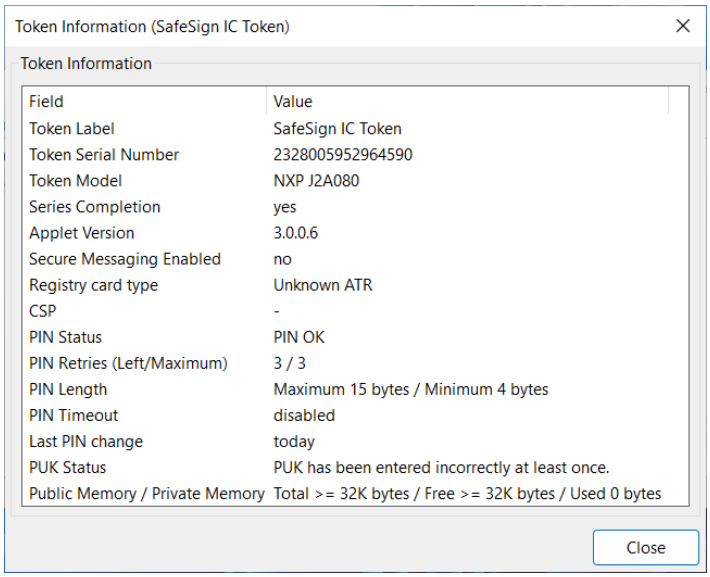


Figure 79: Token Information: Unknown ATR

In addition, each time you either insert the token with the TAU opened or open the TAU with the token inserted, the following dialog will be displayed:

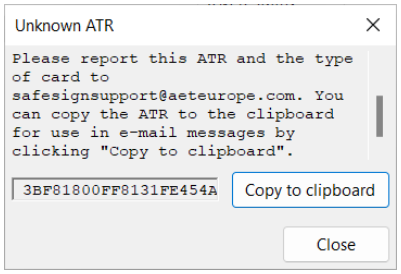


Figure 80: Unknown ATR

This dialog will not only inform you that the ATR is unknown, but also allow you to copy the ATR of the token (including your version of SafeSign IC and the Cryptographic Service Provider) to the clipboard.

- If your token has an unknown ATR, you should contact your (local) supplier to provide you with a SafeSign IC version that does support this token or take further action towards obtaining such a version.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.6.8 CSP

Displays the CSP that is associated with the token (see also section 4.6.7).

With SafeSign IC Minidriver (read-only and read/write) installed, the CSP is: Microsoft Base Smart Card Crypto Provider.

4.6.9 PIN Status

See also section 4.3.1.1.

Displays the status of the PIN:

1 OK

2 PIN has been entered incorrectly at least once

3 One final attempt left to enter PIN incorrectly

4 LOCKED

4.6.10 PIN retries (Left / Maximum)

Displays the maximum number of PIN retries and the number of PIN retries left.

4.6.11 PIN Length

Displays the maximum and minimum number of bytes for the PIN length.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.6.12 PIN Timeout

Displays the status of the PIN Timeout setting.

The PIN Timeout is disabled by default. When the PIN timeout is enabled, the PIN Timeout field will display its value (in seconds).

The timeout value for a particular token can be set in the TAU, through the menu Token > Change PIN Timeout, if the (initialised) token is inserted and the correct PIN is entered. See also section 4.8.

With SafeSign IC Minidriver installed, the PIN Timeout functionality will work for applications using SafeSign IC PKCS #11, but not for applications using the Microsoft Base Smart Card Crypto Provider.

4.6.13 Last PIN change

Display the status of the last PIN change (in days).

- Note that the last PIN change may not be available for your (type of) card.

4.6.14 PUK Status

Displays the status of the PUK:

1. OK
2. PUK has been entered incorrectly at least once
3. One final attempt left to enter PUK incorrectly
4. LOCKED

See also section 4.5.1.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.6.15 Public Memory / Private Memory

Displays the total amount of bytes, the free amount of bytes and the used amount of bytes available in the public memory on the token (after initialisation).

Note that the memory information is an indication of how much memory is available on the card. For cards with more than 32Kb of memory it always displays: “>= 32K bytes”.

This is done because the maximum value the card can return is 32767 bytes and no information can be given for the amount of memory on the card above that value (hence “Total” displays “>= 32767”). Once the return value drops below the maximum value, "Free" will give the actual value returned by the card:

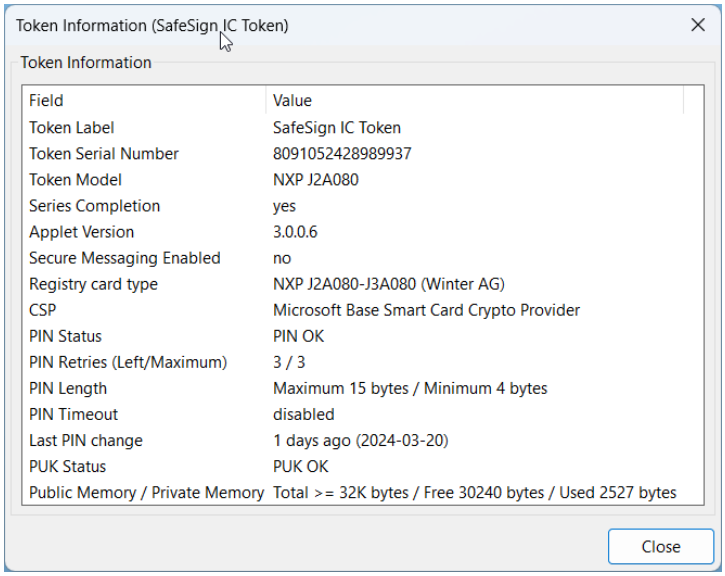


Figure 81: Token Information: Memory

4.7 Show Token Objects

The option **Show Token Objects** provides a detailed and technical view of the contents of the token, displaying all the separate objects on the token. It is not designed to give a correlated structure between the objects on the token (where such distinction is not possible by the friendly name / label of the objects). This is the purpose of Show Registered Digital IDs, which shows the relation between the objects on the token i.e. which objects go together and make up a Digital ID that can be used.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

1 Select **Show Token Objects** from the **Token** menu to open the PKCS#11 objects ([Token Name]) dialog:

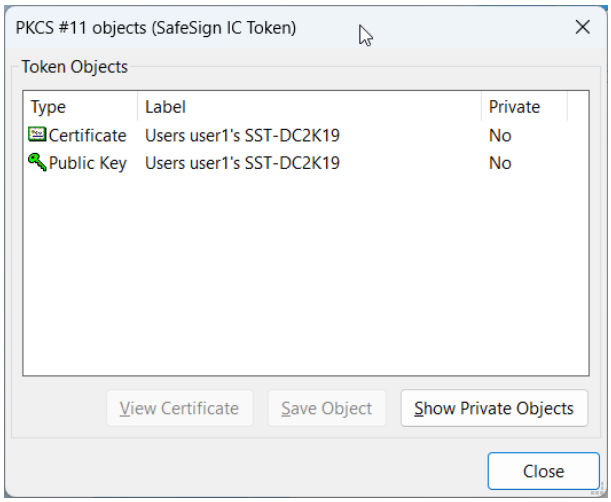


Figure 82: TAU: PKCS #11 objects

This dialog will display the Public token objects, including Public Keys, (PKI) Certificates and (when available) Attribute Certificates.

- In order to view all objects / private objects on the token, click **Show Private Objects**

2 Upon selecting **Show Private Objects**, You will be asked for the PIN of the token:

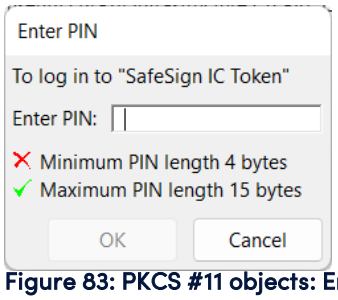


Figure 83: PKCS #11 objects: Enter PIN

- Enter the correct PIN to display the private objects on the token (and click **OK**)

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

3 Upon entering the correct PIN, the private objects on the token will also be displayed:

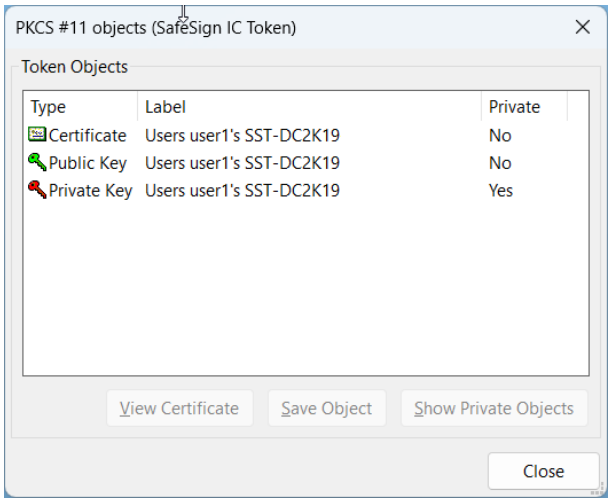


Figure 84: PKCS #11 Objects: All objects

A number of operations are possible with regard to the certificate on the token, which are described in the following sections:

- Section 4.7.1: View Certificate
- Section 4.7.2: Save Object

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.7.1 View Certificate

This allows you to view the contents of a certificate. Select the certificate on the token and click on **View Certificate** to view the contents of the certificate.

In case of a PKI certificate, the following information will be displayed:

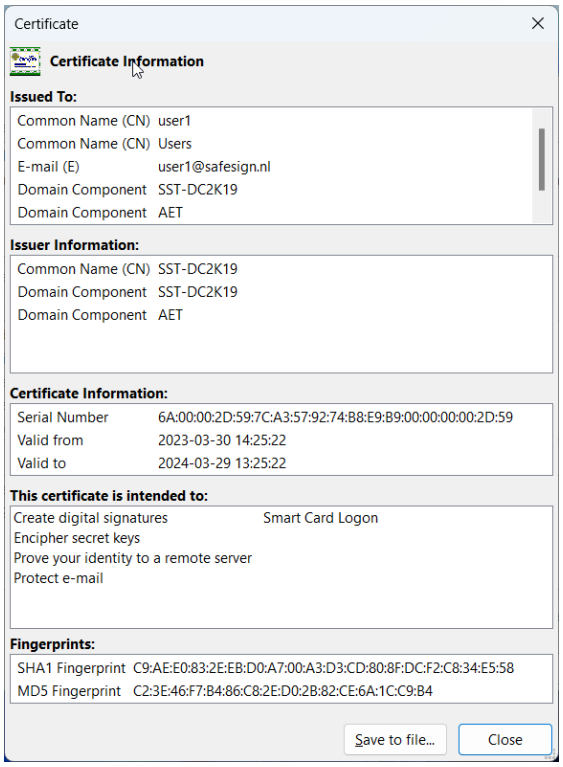


Figure 85: Certificate Information

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4.7.2 Save Object

This allows you to save certificates in *.cer format as well as data objects on the token, for purposes of making your certificate with public key available to others.

Click on **Save Object** to select a location to save the file in:

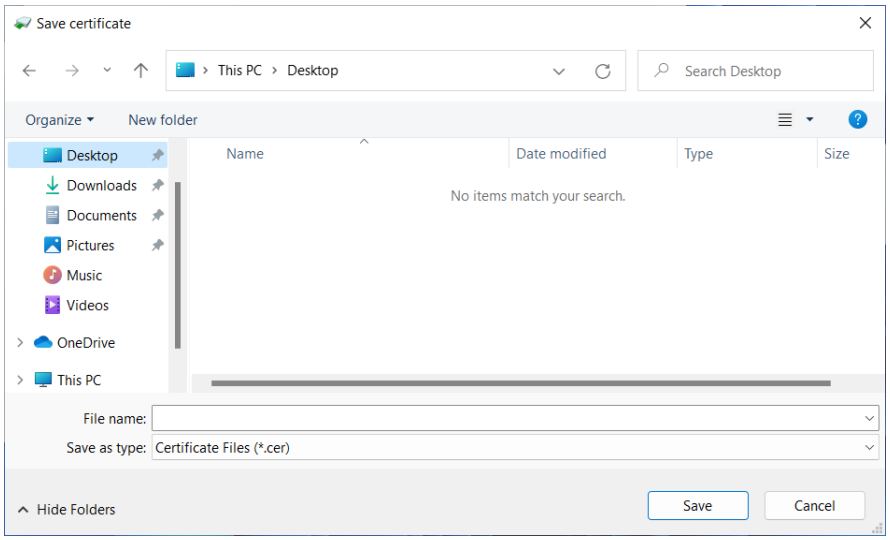


Figure 86: Save certificate

- Select a location and click **Save**

4.8 Change PIN Timeout

PIN Timeout functionality is only supported for the SafeSign IC PKCS #11 Library.

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.

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

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

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

1 Select Change PIN Timeout from the **Token** menu to open the Change Timeout dialog:

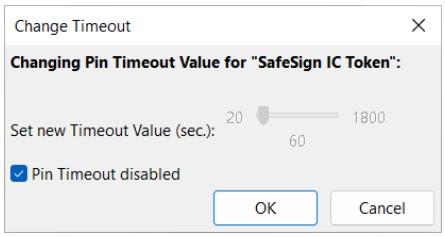


Figure 87: Change Timeout: PIN Timeout disabled

By default, the PIN Timeout is disabled.

- Uncheck 'Pin Timeout disabled'

2 You can now drag the slider to the desired value (60 seconds in our example):

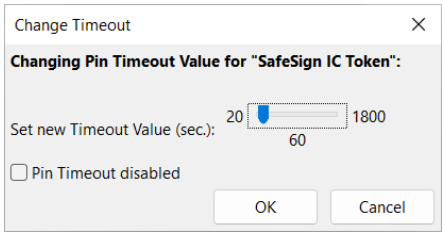


Figure 88: Change Timeout: PIN Timeout enabled

- Click **OK**

3 You will be asked to enter the PIN of your token:

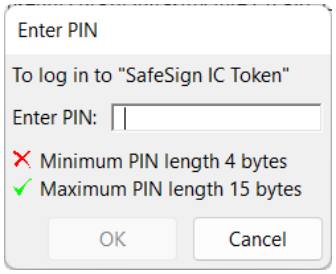


Figure 89: Enter PIN

- Enter the PIN and click **OK**

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4 Upon entering the correct PIN, the Timeout will be enabled:

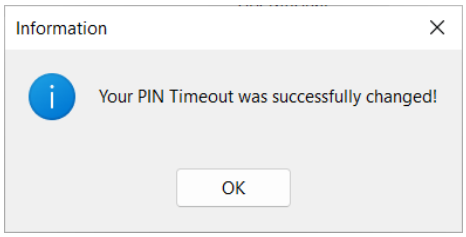


Figure 90: Change Timeout: Your PIN Timeout was successfully changed

- Click **OK**

5 When the PIN Timeout is enabled, the Token Information dialog will display the new PIN Timeout value:

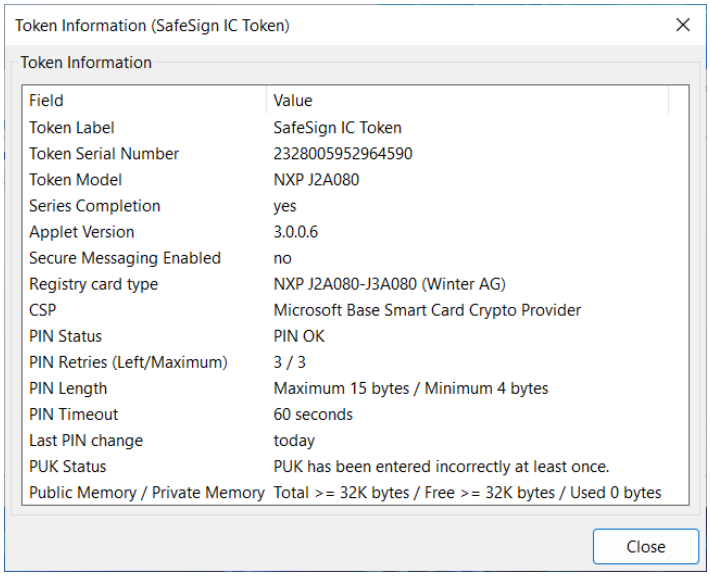


Figure 91: Token Information: PIN Timeout value

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

5 Integration

As of Mozilla Firefox version 90, Firefox will automatically find and offer to use client authentication certificates provided by the operating system on Windows, though a library / module called 'OS Client Cert Module'.

This means that Firefox now works with the SafeSign IC Card Minidriver and that it is no longer necessary to install the SafeSign IC PKCS #11 Library as a security module in Firefox.

Although the Firefox Installer is still available in the Token Administration Utility's Integration menu, installing the SafeSign IC PKCS #11 Library as a security module in Firefox is not recommended and may result in issues (such as having to enter the PIN for your token twice, once for the PKCS#11 Library, once for the Minidriver).

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

6 Tasks

The Task Manager allows you to start (a) certain task(s) when a (specific) token is inserted.

This is managed by the SafeSign IC Certificate Expiration Check Utility ('aetcrss1.exe').

- Note that the TAU on Linux and macOS does not include the **Tasks** menu item.

Clicking on **Manage tasks** in the TAU will open the Manage tasks dialog, which already contains one task by default (that apply to all cards):

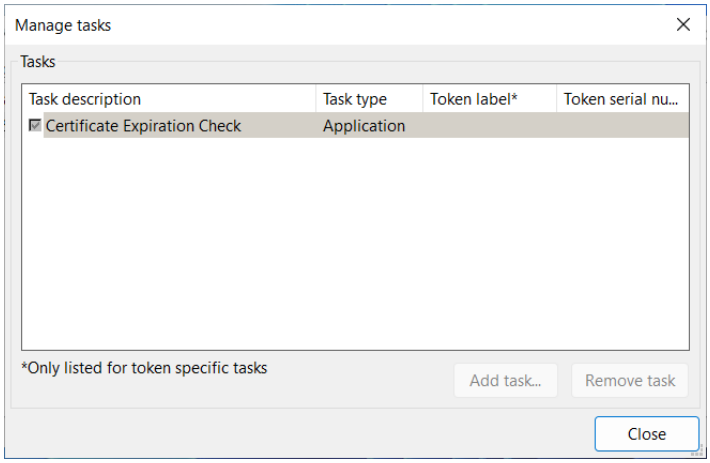


Figure 92: Manage tasks

The task "Certificate Expiration Check" will prompt a dialog when a certificate is expired or is about to expire.

If you want to disable this task, it is recommended that the task is deselected (as you may want to enable it again at a later time), rather than removed (by clicking Remove task) from the **Task** menu of the TAU.

- Note that only an administrator can add / remove tasks.
- Note that it is not possible to edit a(n) (existing) task.

When the task are deselected, the process 'aetcrss1.exe' will be ended automatically, so that it does not interfere with other processes.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

6.1.1 Adding a Task

You can add a task by clicking Add task.

You can select two task types:

1. Launch an application when a token is inserted: e.g. open the TAU, open a browser or set up a Remote Desktop Connection;
2. Launch a plug-in when a token is inserted: e.g. change the Transport PIN of the token.

- Note that the procedure for adding a task is the same for each task type, hence only the procedure for launching an application is described.

1 Upon clicking **Add task**, the Welcome to the add new task wizard dialog opens:

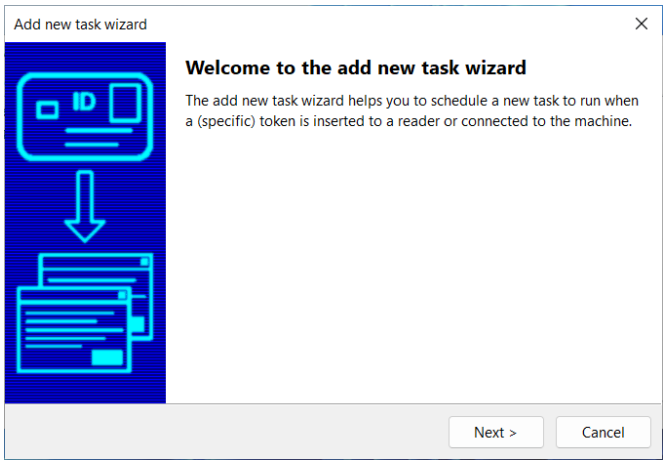


Figure 93: Add new task wizard: Welcome to the add new task wizard

- Click **Next**

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

2 Upon clicking **Next** in the Welcome to the add new task wizard window, step 1 will allow you to select a task type:

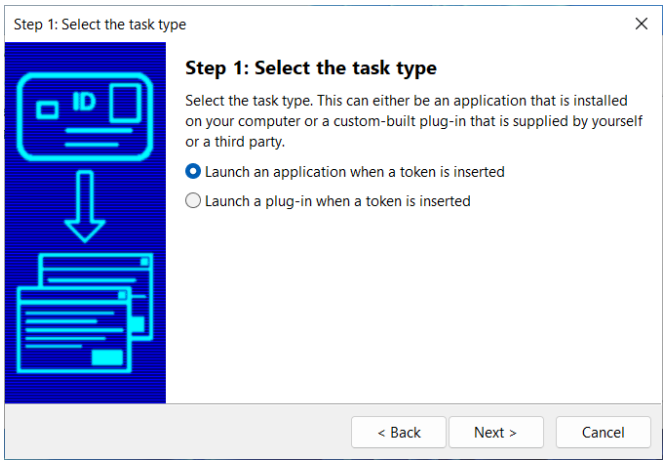


Figure 94: Add new task wizard: Step 1: Select the task type

- Select the option "Launch an application when a token is inserted" and click **Next**

3 The next step 2 will allow you to select the application to launch and specify its parameters (if required / desired):

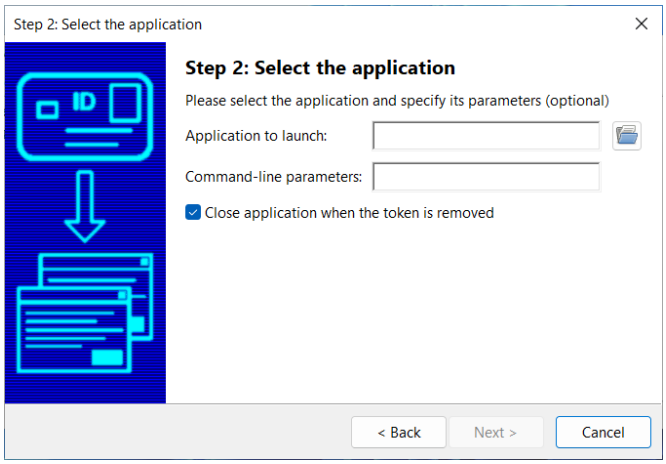


Figure 95: Add a new task wizard: Step 2: Select the application

After selecting the application to launch, you can also specify command-line parameters for this application.

- When you have completed the fields, click **Next** to continue

- Note that these parameters are application-specific. For example, in order to start up a Remote Desktop Connection (mstsc.exe), you should enter: /v:<server name>. You can also select whether you want to close the task when the token is removed.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

- Note that when selecting the option to “Close the application when the token is removed”, the Task Manger will try to close the application launched, when possible. However, there are some scenarios in which this is not possible, for example when launching the remote desktop application (mstsc.exe) with parameters to connect to a particular session. In that case, the SafeSign IC Task Manager cannot close the session for the user or the application itself.

4 The next step 3 is to select whether the task should apply to all tokens, or only to a specific token:

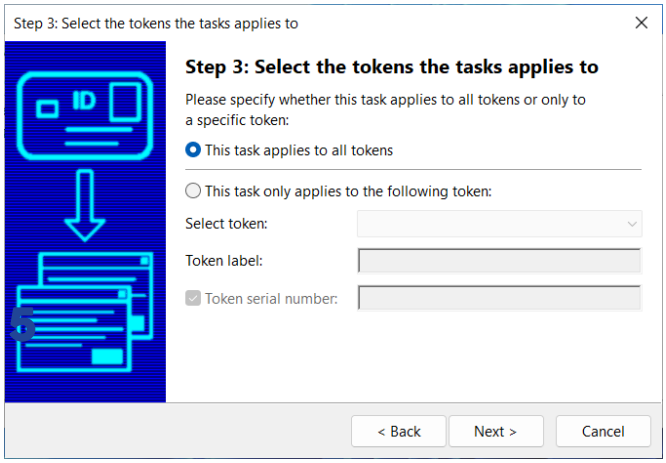


Figure 96: Add new task wizard: Step 3: Select the tokens the task applies to

When no token is inserted in the reader, the task will be set to apply to all tokens (as above).

5 When a token is inserted, the option ‘This task only applies to the following token’ is selectable:

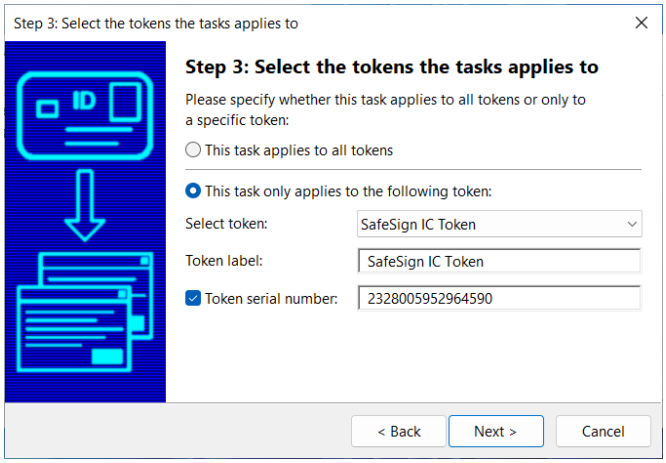


Figure 97: Step 3: This task only applies to the following token

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

- Note that you can also also select the task to apply to any token(s) with the specified token label, if the “Token serial number” checkbox is not checked.

- When you have selected the desired configuration, click **Next**

6 The next step is to enter a name for your task (to make it easily identifiable in the task list):

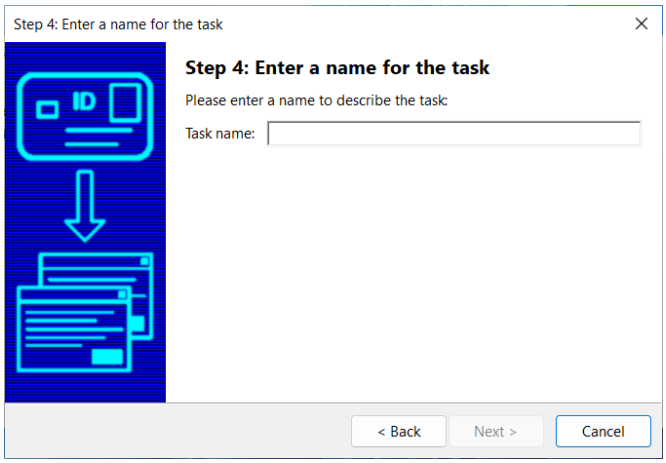


Figure 98: Add new task wizard: Step 4: Enter a name for the task

- Enter a name and click **Next** to continue

7 These four steps conclude the Add a new task wizard:

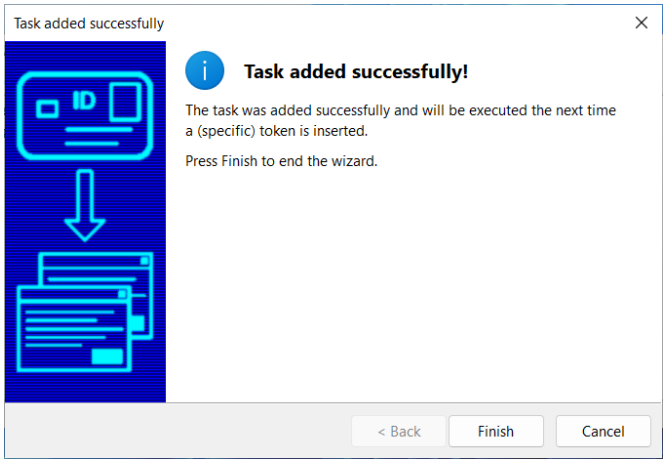


Figure 99: Add new task wizard: Task added successfully

- Click **Finish**

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

The task will now be added to the Manage task window in the TAU:

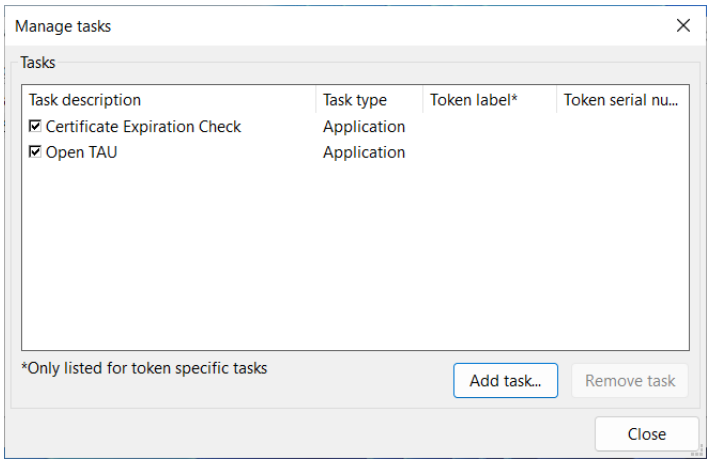


Figure 100: Manage tasks: Launch application task

When a token is inserted, the application will start.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

7 Help

The Help menu of the SafeSign IC TAU Utility features two items: **Version Info** and **About**.

The Version Information dialog will inform you of the version of SafeSign IC you are running and the file versions of the components installed by your SafeSign IC version. The About dialog will display the version of the TAU and some copyright information (with regard to SafeSign IC, OpenSSL and SSLeay).

7.1 Version Info

The **Versions Info** item opens the Version Information dialog, which displays (file) information on the SafeSign IC version installed and which is particularly useful for support issues, enabling AET Europe SafeSign Support to quickly identify the version you are running.

For that purpose, you can save this information in a text file, by clicking **Save information** (and name it accordingly) or you can make a screenshot and include it when submitting a support request to AET Europe SafeSign Support.

7.1.1 Windows

SafeSign IC Minidriver for Windows comes in a 64-bit version, therefore the Version Information dialog will reflect this. When SafeSign IC 64-bit is installed, both the 32-bit file versions and the 64-bit file versions will be displayed (when available).

- Note that the read-only Minidriver will always be included, either by version number when it is installed or by a horizontal line (-) when it is not installed.

7.1.2 Linux

SafeSign IC Standard for Linux supports 64-bit Linux distributions only.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

7.1.3 macOS

SafeSign IC Standard for macOS includes the AET Smart Card Driver extension (aetsce.appex).

7.2 About

The About dialog displays the version number of the TAU and copyright information.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

8 Advanced Options

There are some advanced options in the TAU, which an administrator may have made available to the user, by enabling them in the registry.

- Please refer to the SafeSign IC Administrator's Guide for a complete overview.

The following three features are described in this document:

1. Section 8.1: Analyse certificate quality
2. Section 8.2: Dump token contents
3. Section 8.3: Show PUK retry counter

8.1 Analyse certificate quality

This function analyses the quality of the PKI Certificate(s) and Attribute Certificate(s) stored on the token. It analyses the attributes of the certificate(s) for optimal performance for applications that will use the certificate. This allows administrators to identify possible issues with certificate quality and ensure that the right attributes are set and/or set with the right values.

When the certificate status is OK, this means that the certificate has been stored correctly on the token and is suitable for optimal use:

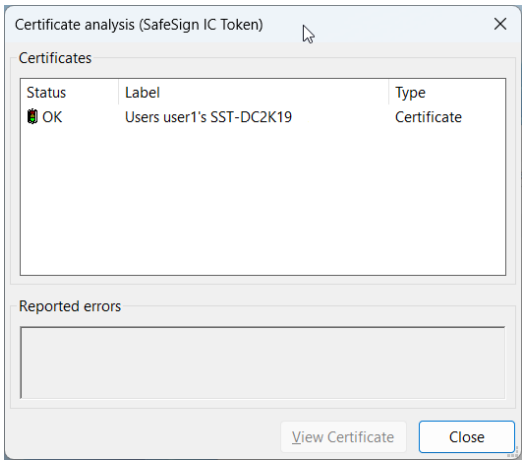


Figure 101: Certificate analysis: OK

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

When the certificate status is Unusable, this means that the certificate is unusable for any application, as for example, the private key could not be found on the token or the private key does not match the public key in the certificate:

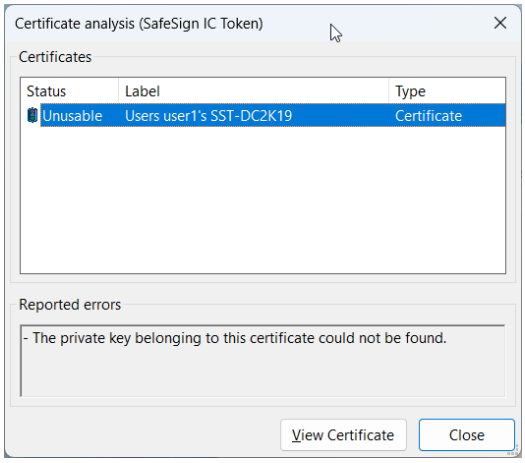


Figure 102: Certificate analysis: Unusable

When the certificate status is Not optimal, this may result in suboptimal performance of the certificate registration process. In that case, the certificate analysis tool will indicate a number of causes why this could be the case (for example, because certain values in the certificate do not match). When this is the case, a dump of the token contents (as described in section 8.2) can give more detail.

8.2 Dump token contents

This function allows you to dump the contents of the token, identifying the (PKCS #11) objects on the token, including the Private Key(s), Public Key(s), (Attribute) Certificate(s) and their attributes.

Such a dump can be useful for support purposes, in particular when used in combination with the SafeSign Diagnostic Tool and the **Analyse Certificate Quality** feature (**Token > Analyse Certificate Quality**).

If the certificate quality is indicated as being Not optimal, the dump will give more information on whether the attributes are set and whether they are set correctly. This is important for applications trying to use the token (and the certificate it contains).

- Note that the actual objects on the token are not saved or placed off the card in any way. Only the public information of the contents of the token will be exported.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

1 To dump the token contents, go to **Token > Dump Token Contents**:

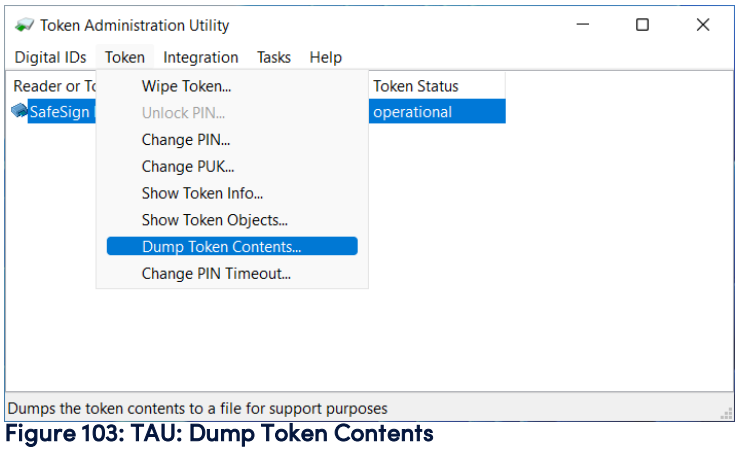


Figure 103: TAU: Dump Token Contents

2 You will be asked for confirmation to continue with the dump:

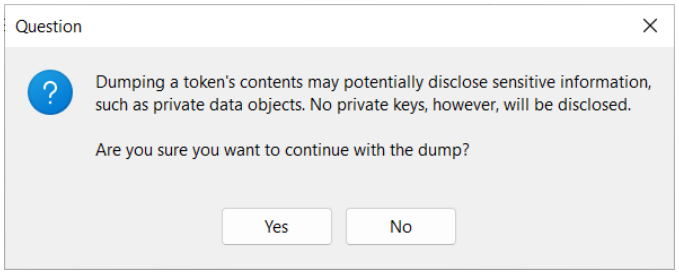


Figure 104: Dump token contents: Question

- Click **Yes** to continue with the dump

3 You will be asked to select a location and a name for the resulting file:

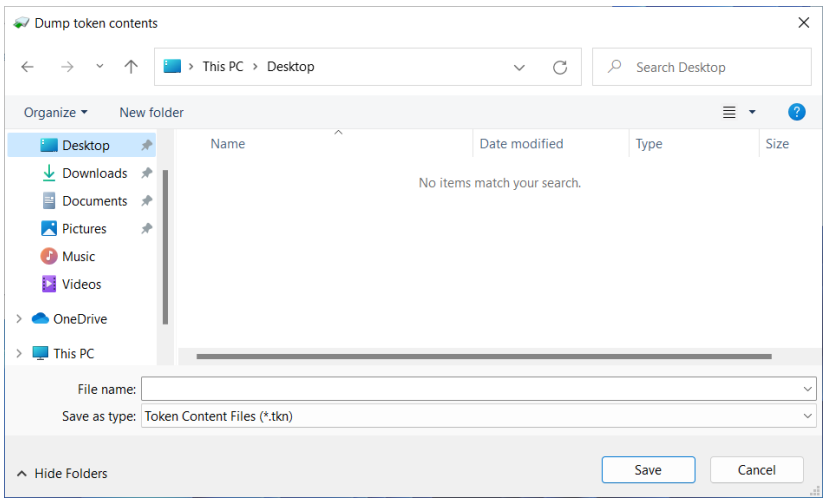


Figure 105: Dump Token Contents: Save

- Select a location and a name for the file and click **Save**

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

4 You will be asked to enter the PIN for the token:

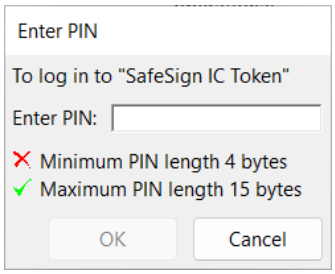


Figure 106: Enter PIN

- Enter the correct PIN and click **OK**

5 The token contents will now be written to a file in the location specified and you will be notified when this is completed:

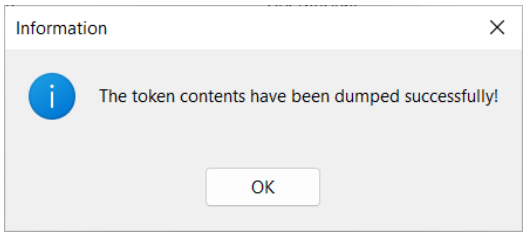


Figure 107: Dump Token Contents: Information

- Click **OK**

You can now view the contents of the file in the location where you saved it.

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com

8.3 Show PUK retry counter

It is possible to enable the display of the PUK retry counter (see section 4.5.1), like this is done for the PIN retry counter in those dialogs where the PIN is involved (such as Enter PIN and Change PIN).

When the PUK retry is not enabled, the following Change PUK dialog is displayed when the PUK is entered incorrectly:

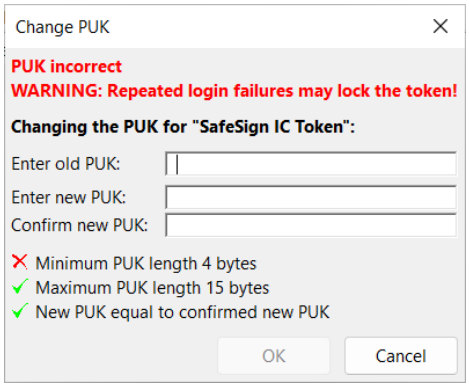


Figure 108: Change PUK

When the PUK retry is enabled, the following Change PUK dialog is displayed when the PUK is entered incorrectly, including information on the number of retries:

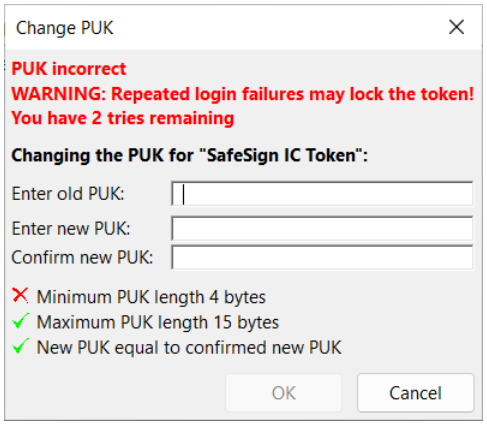


Figure 109: Change PUK with retry counter

A.E.T. Europe B.V.

+31 26 365 33 50
info@aeteurope.com
aeteurope.com