

## SafeSign Identity Client

Token Administration Utility Guide



## Table of Contents

<b>Table of Contents .....</b>	<b>I</b>
<b>Table of Figures .....</b>	<b>III</b>
<b>Warning Notice .....</b>	<b>VI</b>
<b>Document Information .....</b>	<b>VII</b>
<b>About the Product .....</b>	<b>VIII</b>
<b>About the Manual .....</b>	<b>IX</b>
<b>1      Token Administration Utility.....</b>	<b>1</b>
<b>1.1    Menu Items .....</b>	<b>1</b>
<b>2      General .....</b>	<b>2</b>
<b>2.1    Tokens and readers.....</b>	<b>2</b>
<b>2.2    Multi-language.....</b>	<b>3</b>
<b>3      Digital IDs .....</b>	<b>6</b>
<b>3.1    Show Registered Digital IDs.....</b>	<b>6</b>
<b>3.1.1 Transfer ID to token .....</b>	<b>8</b>
<b>3.1.2 Import trust chain .....</b>	<b>11</b>
<b>3.1.3 Delete Digital ID.....</b>	<b>13</b>
<b>3.1.4 View Certificate .....</b>	<b>15</b>
<b>3.1.5 Check Expiration.....</b>	<b>16</b>
<b>3.1.6 Close.....</b>	<b>17</b>
<b>3.2    Import Digital ID.....</b>	<b>17</b>
<b>3.3    Import Certificate.....</b>	<b>20</b>
<b>3.4    Exit.....</b>	<b>21</b>
<b>4      Token.....</b>	<b>22</b>
<b>4.1    Initialise Token .....</b>	<b>22</b>
<b>4.1.1 Initialise Token.....</b>	<b>23</b>
<b>4.1.1.1 Operation failed .....</b>	<b>26</b>
<b>4.1.2 Wipe Token.....</b>	<b>26</b>
<b>4.1.2.1 Operation failed .....</b>	<b>29</b>
<b>4.1.3 Recycle Token.....</b>	<b>29</b>
<b>4.1.3.1 Recycle Count .....</b>	<b>30</b>
<b>4.1.3.2 Recycle Process .....</b>	<b>30</b>
<b>4.1.3.3 Recycle Count exceeded .....</b>	<b>32</b>
<b>4.1.4 Initialise a Token with PIN Policy .....</b>	<b>32</b>
<b>4.1.4.1 Initialise Process .....</b>	<b>33</b>
<b>4.1.4.2 Change PIN .....</b>	<b>35</b>
<b>4.1.4.3 Enter PIN .....</b>	<b>36</b>
<b>4.1.5 Import CA Certificates.....</b>	<b>36</b>
<b>4.2    Change PIN .....</b>	<b>39</b>
<b>4.2.1 PIN Status .....</b>	<b>39</b>
<b>4.3    Change Transport PIN .....</b>	<b>41</b>
<b>4.4    Unlock PIN .....</b>	<b>43</b>
<b>4.4.1 Unlock using the PUK .....</b>	<b>43</b>
<b>4.4.2 Unlock via off-line PIN unlock .....</b>	<b>44</b>



<b>4.5</b>	<b>Change PUK .....</b>	<b>47</b>
4.5.1	PUK information .....	48
<b>4.6</b>	<b>Show Token Info .....</b>	<b>51</b>
4.6.1	Token Label.....	51
4.6.2	Token Serial Number .....	51
4.6.3	Token Model.....	51
4.6.4	Series Completion .....	52
4.6.5	Applet Version.....	52
4.6.6	Secure messaging enabled .....	52
4.6.7	Registry card type.....	52
4.6.7.1	Unknown ATR.....	52
4.6.8	CSP .....	54
4.6.9	PIN Status .....	54
4.6.10	PIN retries (Left / Maximum).....	54
4.6.11	PIN Length .....	54
4.6.12	PIN Timeout.....	54
4.6.13	Last PIN change .....	55
4.6.14	PUK Status .....	55
4.6.15	Public Memory / Private Memory.....	55
<b>4.7</b>	<b>Show Token Objects.....</b>	<b>56</b>
4.7.1	View Certificate .....	57
4.7.1.1	PKI Certificate .....	57
4.7.1.2	Attribute Certificate.....	58
4.7.2	Save Object.....	58
<b>4.8</b>	<b>Change PIN Timeout .....</b>	<b>59</b>
<b>5</b>	<b>Integration .....</b>	<b>61</b>
5.1	Install SafeSign in Firefox.....	61
<b>6</b>	<b>Tasks .....</b>	<b>62</b>
<b>6.1</b>	<b>Adding a Task.....</b>	<b>63</b>
6.1.1	Launch an application .....	63
6.1.2	Launch a plug-in .....	67
<b>7</b>	<b>Help .....</b>	<b>72</b>
<b>7.1</b>	<b>Version Info .....</b>	<b>72</b>
7.1.1	Windows 32-bit and 64-bit.....	72
7.1.2	Linux 64-bit .....	72
7.1.3	macOS.....	72
<b>7.2</b>	<b>About.....</b>	<b>72</b>
<b>8</b>	<b>Advanced Options.....</b>	<b>73</b>
<b>8.1</b>	<b>Analyse certificate quality .....</b>	<b>73</b>
<b>8.2</b>	<b>Dump token contents .....</b>	<b>74</b>
<b>8.3</b>	<b>Show PUK retry counter.....</b>	<b>76</b>



## Table of Figures

Figure 1: TAU: Token Status absent.....	2
Figure 2: TAU: Token Status uninitialized.....	2
Figure 3: TAU: Token Status operational.....	3
Figure 4: Control Panel: Language.....	4
Figure 5: TAU: Dutch .....	4
Figure 6: TAU: Thai .....	5
Figure 7: Digital IDs: No Personal Digital IDs .....	6
Figure 8: Digital IDs: Personal Digital ID on token.....	7
Figure 9: Digital IDs: Transfer ID to token .....	9
Figure 10: Digital IDs: Are you sure you want to transfer the Digital ID.....	9
Figure 11: Digital IDs: Should the CA certificates be imported .....	10
Figure 12: Enter PIN.....	10
Figure 13: The Digital ID was transferred successfully .....	10
Figure 14: Digital IDs: Digital ID transferred to token.....	11
Figure 15: Digital IDs: Import trust chain .....	12
Figure 16: Enter PIN.....	12
Figure 17: The trust chain was imported successfully.....	12
Figure 18: Digital IDs: Certification Path on token.....	13
Figure 19: Digital IDs: Are you sure you want to delete the Digital ID .....	14
Figure 20: Enter PIN.....	14
Figure 21: Digital IDs: The Digital ID was deleted successfully.....	14
Figure 22: Digital IDs: Certificate Information .....	15
Figure 23: No Digital IDs are about to expire in the next 30 days .....	16
Figure 24: Certificate Expiration Warning .....	16
Figure 25: Certificate Expiration Warning .....	16
Figure 26: Digital IDs: Import Digital ID .....	17
Figure 27: Import Digital ID: Select a Digital ID file.....	18
Figure 28: Import Digital ID: Digital ID file.....	18
Figure 29: Enter PIN.....	19
Figure 30: Import Digital ID: The Digital ID has been imported successfully .....	19
Figure 31: Import Certificate: Select Certificate .....	20
Figure 32: Enter PIN.....	21
Figure 33: Import Certificate: The certificate has been imported successfully .....	21
Figure 34: TAU: Initialise Token .....	23
Figure 35: Initialise Token: empty.....	23
Figure 36: Initialise Token: completed .....	24
Figure 37: Initialise Token: Your token is being initialised.....	25
Figure 38: Initialise Token: The operation completed successfully .....	25
Figure 39: TAU: Token Status operational.....	25
Figure 40: TAU: Wipe token .....	26
Figure 41: Wipe Token .....	27
Figure 42: Wipe Token: completed .....	28
Figure 43: Your token is being wiped!.....	28
Figure 44: Wipe Token: The operation completed successfully .....	29
Figure 45: Token Information: Recycle Count.....	30
Figure 46: TAU: Recycle Token.....	30
Figure 47: Initialise Token .....	31
Figure 48: Recycle Count decreased.....	31
Figure 49: TAU: Token locked .....	32



Figure 50: Initialise NR Token.....	33
Figure 51: Initialise NR Token: completed.....	34
Figure 52: Initialise NR Token: Password requirements missing .....	35
Figure 53: Change PIN NR Token .....	35
Figure 54: Enter PIN.....	36
Figure 55: Initialise Token .....	36
Figure 56: Import CA certificates: Browse For Folder .....	37
Figure 57: Initialise Token: Import CA certificates.....	37
Figure 58: Initialise Token: Now importing CA certificates .....	38
Figure 59: Initialise Token: The operation completed successfully .....	38
Figure 60: PKCS#11 objects: CA Certificate .....	38
Figure 61: Change PIN .....	39
Figure 62: Change PIN: Your PIN was successfully changed .....	39
Figure 63: Enter PIN.....	40
Figure 64: Enter PIN: You have 2 tries remaining .....	40
Figure 65: Enter PIN: You have only 1 attempt left .....	40
Figure 66: Enter PIN: PIN locked.....	41
Figure 67: Enter PIN: The PIN has previously been entered incorrectly. ....	41
Figure 68: Token Information: PIN is still set to transport value .....	41
Figure 69: TAU: Change transport PIN .....	42
Figure 70: Change transport PIN.....	42
Figure 71: Change transport PIN: Your PIN was successfully changed.....	42
Figure 72: Unlock PIN .....	43
Figure 73: Unlock PIN: Your PIN was successfully unlocked .....	43
Figure 74: Unlock PIN: unlocking methods .....	44
Figure 75: Off-line PIN unlock wizard: Welcome to the off-line PIN unlock wizard.....	44
Figure 76: Off-line PIN unlock wizard: Step 1: select unlock algorithm.....	45
Figure 77: Off-line PIN unlock wizard: Step 2: report challenge .....	45
Figure 78: Off-line PIN unlock wizard: Step 3: enter response and set a new PIN .....	46
Figure 79: Off-line PIN unlock wizard: PIN unlock successful .....	46
Figure 80: Off-line PIN unlock wizard: Off-line PIN unlock failed.....	47
Figure 81: Change PUK .....	47
Figure 82: Change PUK: Your PUK was successfully changed .....	48
Figure 83: TAU: Token Status locked .....	48
Figure 84: Change PUK.....	49
Figure 85: Change PUK: Repeated login failures may lock the token.....	49
Figure 86: Change PUK: : You have only 1 attempt left.....	49
Figure 87: PUK locked.....	50
Figure 88: Change PUK: The PUK has previously been entered incorrectly.....	50
Figure 89: Change PUK: retry counter enabled .....	50
Figure 90: Token Information: Blank Token .....	51
Figure 91: Token Information: SafeSign IC Token .....	51
Figure 92: Token Information: Unknown ATR.....	53
Figure 93: Unknown ATR.....	53
Figure 94: Unknown ATR: Copy to clipboard .....	53
Figure 95: TAU: PKCS #11 objects.....	56
Figure 96: PKCS #11 objects: Enter PIN .....	56
Figure 97: PKCS #11 Objects: All objects.....	57
Figure 98: Certificate Information .....	57
Figure 99: Certificate Information .....	58
Figure 100: Save certificate .....	58
Figure 100: Change Timeout: PIN Timeout disabled .....	59



Figure 101: Change Timeout: PIN Timeout enabled.....	59
Figure 102: Enter PIN.....	60
Figure 103: Change Timeout: Your PIN Timeout was successfully changed .....	60
Figure 104: Token Information: PIN Timeout value.....	60
Figure 105: Firefox Installer: Install SafeSign in Firefox.....	61
Figure 106: Firefox Installer: SafeSign has been successfully installed in Firefox .....	61
Figure 107: Manage tasks .....	62
Figure 108: Add new task wizard: Welcome to the add new task wizard.....	63
Figure 109: Add new task wizard: Step 1: Select the task type.....	63
Figure 110: Add a new task wizard: Step 2: Select the application .....	64
Figure 111: Add new task wizard: Step 3: Select the tokens the task applies to .....	65
Figure 112: Step 3: This task only applies to the following token.....	65
Figure 113: Add new task wizard: Step 4: Enter a name for the task.....	66
Figure 114: Add new task wizard: Task added successfully .....	66
Figure 115: Manage tasks: New task .....	67
Figure 116: Add new task wizard: Welcome to the add new task wizard.....	67
Figure 117: Add new task wizard: Step 1: Select the plug-in .....	68
Figure 118: Add a new task wizard: Step 2: Select the plug-in .....	68
Figure 119: Add new task wizard: Step 3: Select the tokens the task applies to .....	69
Figure 120: Step 3: This task only applies to the following token.....	69
Figure 121: Add new task wizard: Step 4: Enter a name for the task.....	70
Figure 122: Add new task wizard: Task added successfully .....	70
Figure 123: Manage tasks: New task .....	71
Figure 125: Certificate analysis: OK .....	73
Figure 126: Certificate analysis: Unusable .....	74
Figure 127: TAU: Dump Token Contents.....	75
Figure 128: Dump token contents: Question.....	75
Figure 129: Dump Token Contents: Save .....	75
Figure 130: Enter PIN.....	76
Figure 131: Dump Token Contents: Information .....	76
Figure 132: Change PUK .....	76
Figure 133: Change PUK with retry counter.....	77



## 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.

© Copyright A.E.T. Europe B.V., 2000-2019. All rights reserved.

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

Credit Information:

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

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



## Document Information

Document ID: SafeSign Identity Client Token Administration Utility Guide

Project Information: SafeSign IC User Documentation

Document revision history:

Version	Date	Author	Changes
1.0	2 November 2018	Drs C.M. van Houten	First edition for SafeSign IC Standard and Minidriver Version 3.5
1.1	06 June 2019	Drs C.M. van Houten	Modified for SafeSign IC Standard and Minidriver Version 3.5, release 3.5.2.0

## Document Approval

Version	Date	Name	Function
1.0	2 November 2019	B. Smid MBT	Chief Development Officer
1.1	06 June 2019	B. Smid MBT	Chief Development Officer

WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE



## About the Product

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

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

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

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



## About the Manual

The aim of this document is to describe the functionality of the SafeSign Identity Client (IC) Token Administration Utility (TAU), which enables you to perform token management functions, such as changing your PIN.

Every activity has a number of steps, indicated by a number: **1**

Each step will require you to take a certain action, indicated by an arrow:

Go through these steps and the actions you are required to take, in order to perform the desired activity.

While reading this document, take into account the notes:



## 1 Token Administration Utility

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

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 and 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.

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.

Screenshots were taken from the TAU on Windows 10.



## 2 General

### 2.1 Tokens and readers

You will find the SafeSign IC TAU in the Programs menu, as “Token Administration”.

Upon clicking Token Administration, the TAU will open:

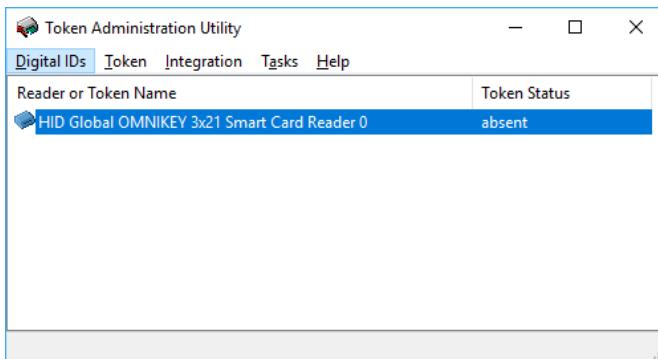


Figure 1: TAU: Token Status absent

This window shows you which smart card reader(s) 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 its drivers installed and whether it is functioning properly. Without a functional smart card reader (and related services, such as the Smart Card service), 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.

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:

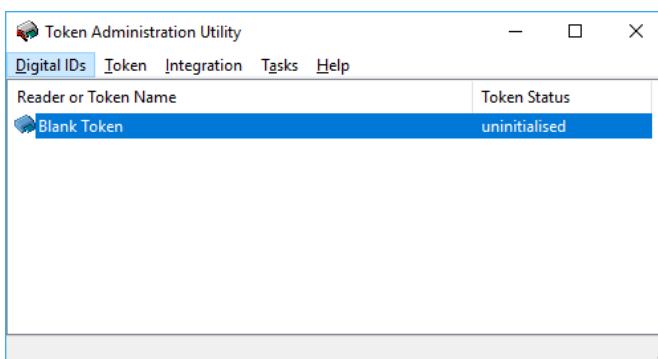


Figure 2: TAU: Token Status uninitialised



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

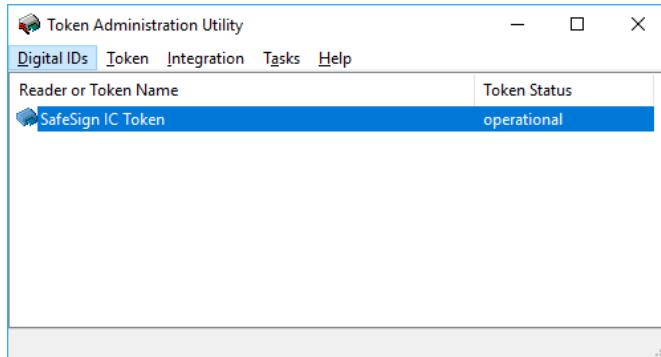


Figure 3: TAU: Token Status operational

You may have multiple smart card readers or USB tokens installed (or a combination of both). You may have multiple 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.

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 or Import Digital ID from the Digital IDs menu. This makes sense, as you need to specify first of/ on which token you want to change the PIN or import a Digital ID.

## 2.2 Multi-language

Multi-language support has been implemented such, to create utmost flexibility for both administrator and user. The language of the InstallShield Wizard on the one hand and the TAU on the other hand, can be different.

The language of the InstallShield Wizard 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 Control Panel > Clock and Region > Region by enabling the desired format:

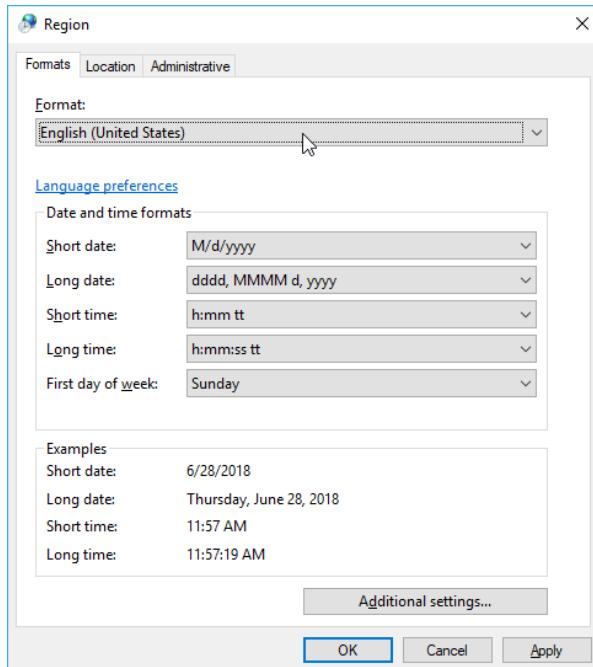


Figure 4: Control Panel: Language

- Note that on Windows 10, these settings can be found on: Windows Settings > Time & Language > Regio and Language > Additional date, time, & regional settings > Region.
- Note that this may also affect other applications.

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

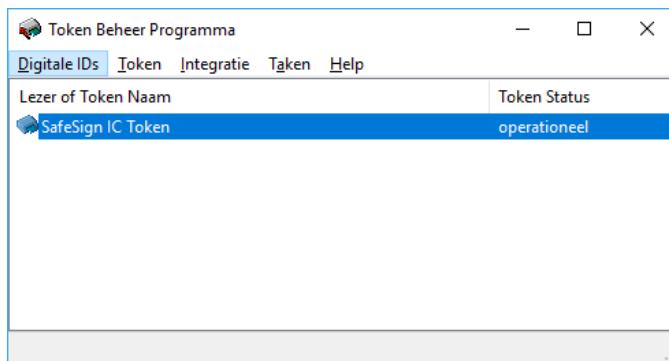


Figure 5: TAU: Dutch



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

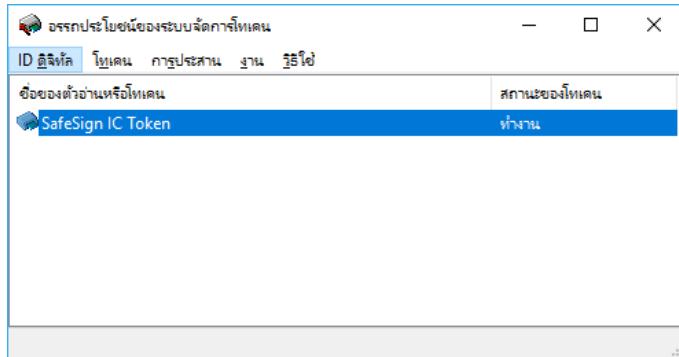


Figure 6: TAU: Thai

Some things to take into account with regard to localization:

- Note that when no specific language is set or SafeSign IC does not support the selected language, the default language of SafeSign IC will be English.
- The language of the Firefox Installer will default to the system language (Format).
- Note that though SafeSign IC has been tested for its InstallShield Wizard 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 Microsoft Operating System used.
- Note that for some applications, SafeSign IC cannot influence the language of the dialogs displayed. For example, Microsoft VPN dialogs will appear in the language of the Operating System installed.



## 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 Digital ID
- Section 3.3: Import Certificate
- Section 3.4: Exit

### 3.1 Show Registered Digital IDs

The menu item Show Registered Digital IDs opens a dialog to show the Digital 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 ID’s and the Digital ID details, i.e. the Certificate Contents and the Certification Path (when available).

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

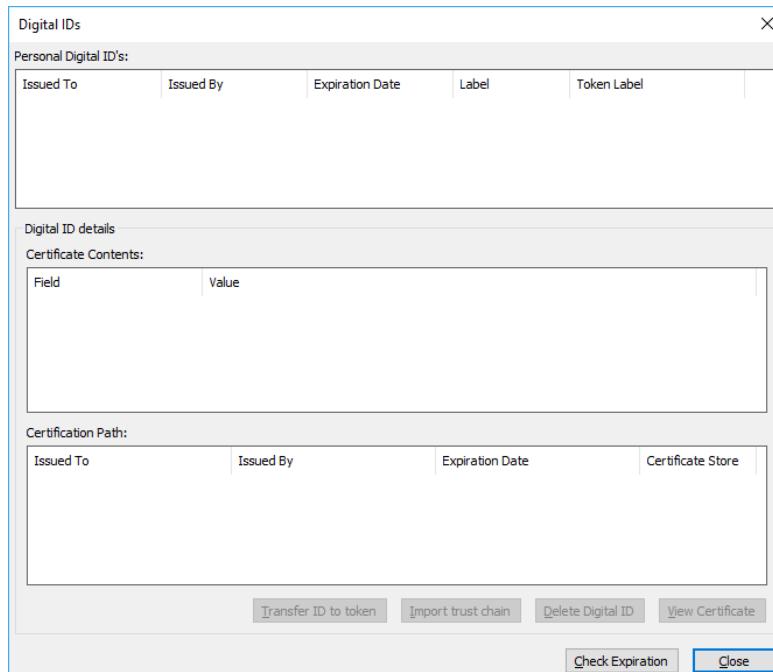


Figure 7: Digital IDs: No Personal Digital IDs



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

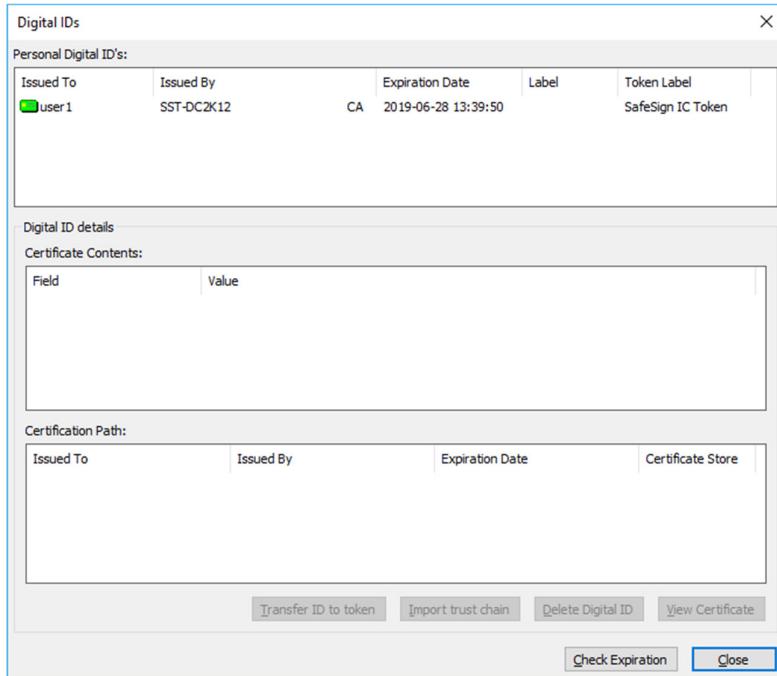


Figure 8: Digital IDs: Personal Digital ID on token

- 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 3.1.5.
- ☞ 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 (though they will not be usable without key pair).



The *Digital IDs* dialog also allows the user to perform a number of operations with regard to the Digital IDs 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: Transfer ID to token
  - Section 3.1.2: Import trust chain
  - Section 3.1.3: Delete Digital ID
  - Section 3.1.4: View Certificate
  - Section 3.1.5: Check Expiration
  - Section 3.1.6: Close
- ☞ Note that on Linux and macOS, only the operations ‘Delete Digital IDs’ and ‘View Certificate’ are available.

### 3.1.1 Transfer ID to token

It is possible to transfer (move) a Digital ID to a token, for example when you have a personal certificate (with a private key corresponding to this certificate) in the Microsoft Certificate Store . When transferring a Digital ID to the token, the private key will be moved to the token and will no longer be present on your hard disk. This greatly enhances the security of your Digital ID, now protected by two-factor authentication: to access it, you would need to have possession of the token and knowledge of the token’s PIN.

Two conditions must be satisfied before being able to transfer an ID to your token:

- 1 The Digital ID should not be on the token already, but should be (registered) in the Microsoft Personal Certificate Store (and have a private key associated with it on the local hard disk), otherwise the button Transfer ID to token will not be available (it is greyed out);
  - 2 You can only transfer the Digital ID when the private key is (marked as) exportable, which may depend on the certificate template that was used to request it.
- ☞ Note that even when the private key has been marked as exportable in the certificate template, if the Digital ID has been requested through the Microsoft Software Key Storage Provider, it is not possible to transfer it to the token (it will fail with an error).



**1** Select the Digital ID you wish to transfer to the token:

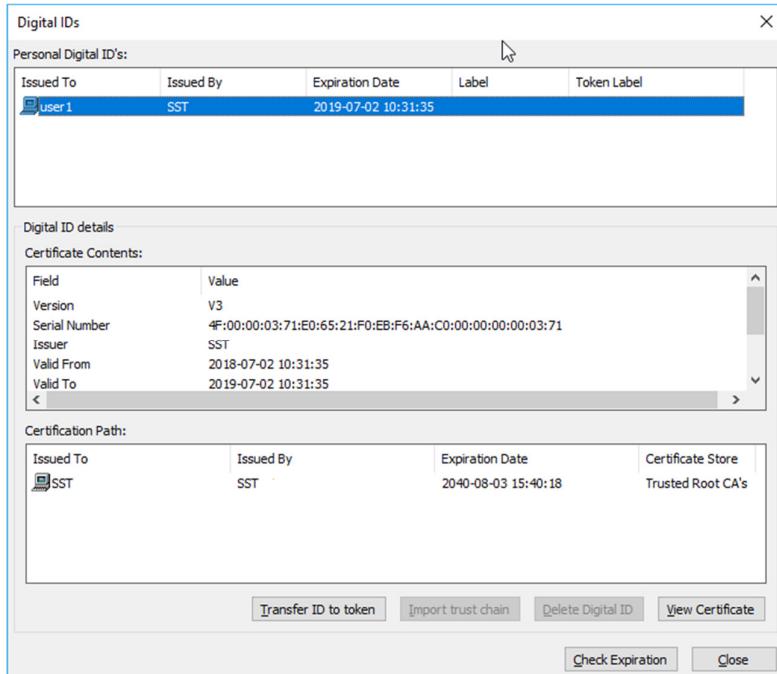


Figure 9: Digital IDs: Transfer ID to token

→ Click **Transfer ID to token** to move the Digital ID from its original location to the token

**2** You will be asked to confirm if you want to transfer the Digital ID with the specified data:

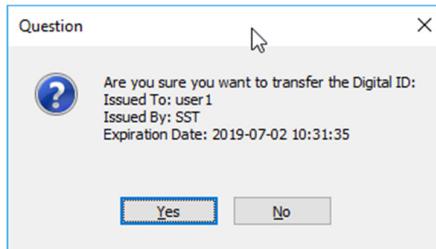


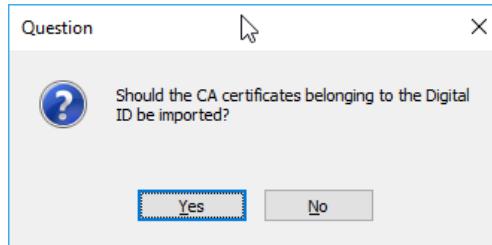
Figure 10: Digital IDs: Are you sure you want to transfer the Digital ID

→ Click **Yes** to transfer the Digital ID specified to the token.

If you click **No**, the process of transferring the Digital ID will abort and the Digital ID will not be transferred.



- 3** You will be asked if the CA certificates belonging to the Digital ID (“trust chain”) should be imported as well:



*Figure 11: Digital IDs: Should the CA certificates be imported*

→ Click **Yes** if you want to import the CA certificates belonging to the Digital ID.

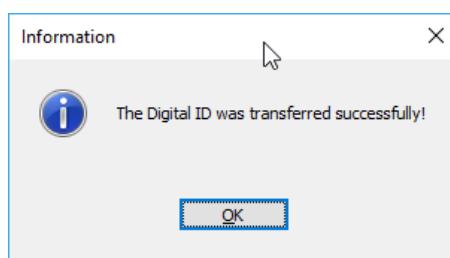
If you click **No**, the CA certificates belonging to the Digital ID will not be imported on the token (but the process of transferring the Digital ID will continue).

- 4** You will be required to enter the PIN for the token:



*Figure 12: Enter PIN*

- Enter the correct PIN for the token and click **OK**
- When the private key belonging to the Digital ID is non-exportable, the transfer fails (after entering the PIN) and you will get an error dialog saying that the private key belonging to the Digital ID is non-exportable (0x8009000B).
- 5** The Digital ID will now be transferred and when the Digital ID has been successfully transferred to the token, you will be notified:



*Figure 13: The Digital ID was transferred successfully*

→ Click **OK**



6

The Digital ID will now be on the token:

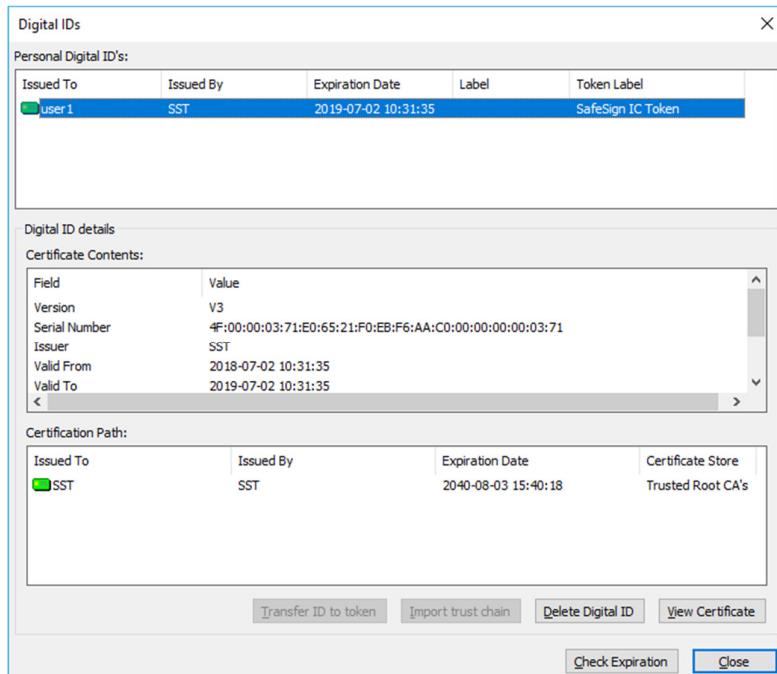


Figure 14: Digital IDs: Digital ID transferred to token

When you have clicked Yes at the prompt to import CA certificates belonging to the Digital ID to the token (Figure 11), the CA certificates for the Digital IDs will also be on the token (as indicated in the picture above, under Certification Path).

### 3.1.2 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 and in specific situations, such as when you have transferred a Digital ID from the Personal Certificate Store to the token and chose not to import the CA certificate(s) at the time (as described in section 3.1.1) or if you have 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:

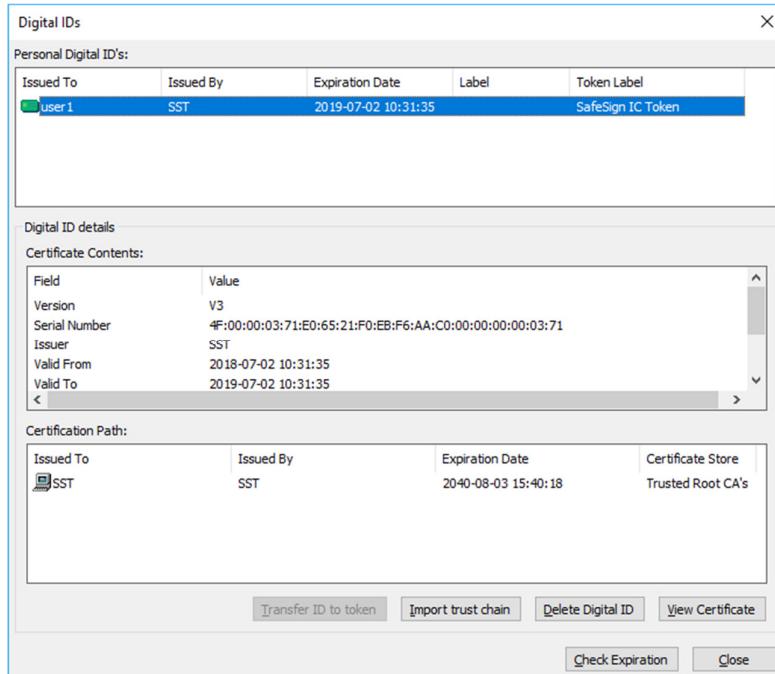


Figure 15: Digital IDs: Import trust chain

→ Click Import trust chain to import the trust chain to the token

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

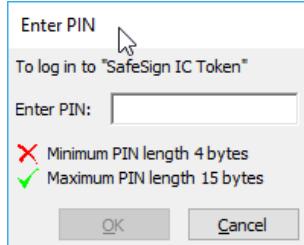


Figure 16: Enter PIN

→ 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:

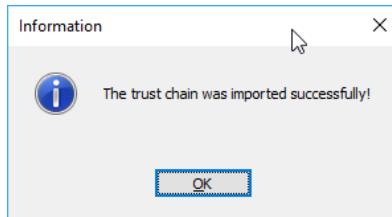


Figure 17: The trust chain was imported successfully

→ Click OK to close this dialog



- 4 The certificate chain will now be on the token:

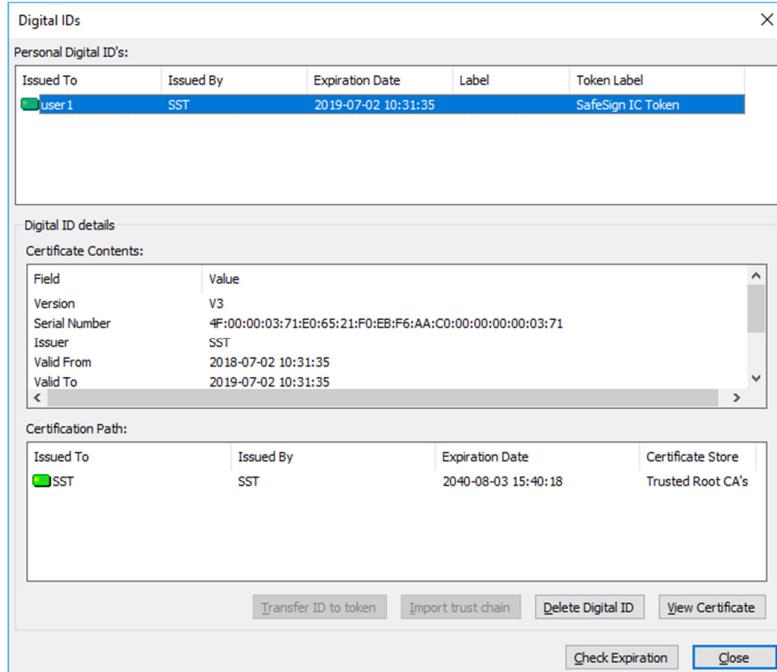


Figure 18: Digital IDs: Certification Path on token

### 3.1.3 Delete Digital ID

It is possible to delete a Digital ID stored on the token by means of the **Delete Digital ID** button in the Digital IDs dialog.

With the TAU, you can only delete Personal Digital IDs that are on the token; you cannot delete Digital IDs that are in the Certificate Store, as indicated in the Digital IDs dialog by the symbol: (in which case the Delete Digital ID button will be greyed out, as in Figure 9).

Upon deleting a Digital ID, all Digital ID objects (public key, private key and certificate) will be deleted from the token.

- Should a key pair have more than one certificate (as in the case of certificate renewal, where the same key pair is used to generate a certificate), the Digital IDs dialog will display two Digital IDs. Deleting one of them will not lead to a deletion of the (shared) key pair, but will only delete the certificate, so that the other certificate (and its certificate chain) can still be used.



- 1** When clicking the **Delete Digital ID** button, you will be asked if you are sure to delete the Digital ID with the specified data:

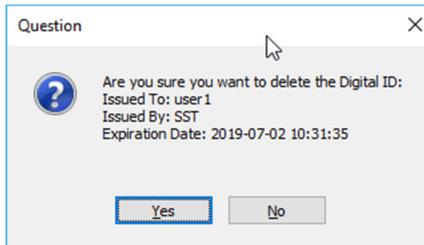


Figure 19: Digital IDs: Are you sure you want to delete the Digital ID

- Click **Yes** to delete the Digital ID

If you click **No**, the process of deleting the Digital ID will abort and the Digital ID will not be deleted.

- 2** Upon clicking **Yes**, you will be asked to enter the PIN for your token:

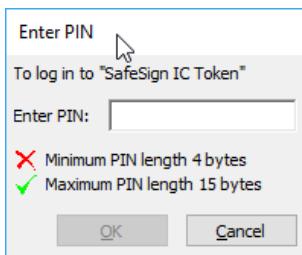


Figure 20: Enter PIN

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

- 3** When the Digital ID has been successfully deleted, you will be informed:

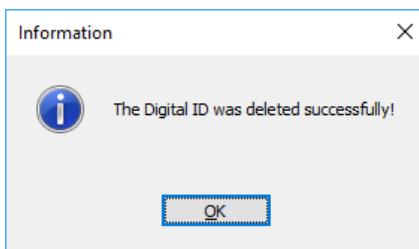


Figure 21: Digital IDs: The Digital ID was deleted successfully

- Click **OK** to close this dialog

The Digital ID and its corresponding certificate chain are now deleted from the token.

- >Note that the certificate will remain registered in the certificate store, as the Microsoft Certificate Propagation service does not deregister certificates (once they are registered).



### 3.1.4 View Certificate

The button **View Certificate** allows you to view the contents of the personal Digital IDs, 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*.

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

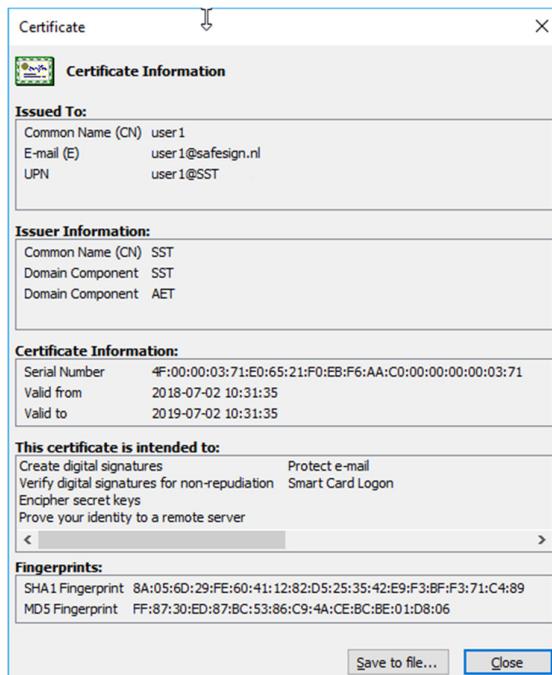


Figure 22: Digital IDs: Certificate Information

This dialog will display the available certificate information.

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).



### 3.1.5 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:

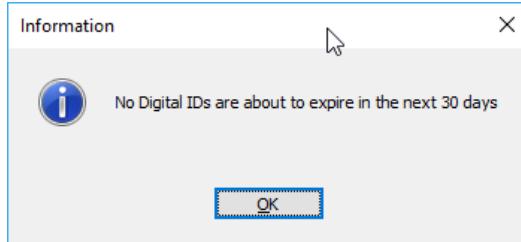


Figure 23: No Digital IDs are about to expire in the next 30 days

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

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

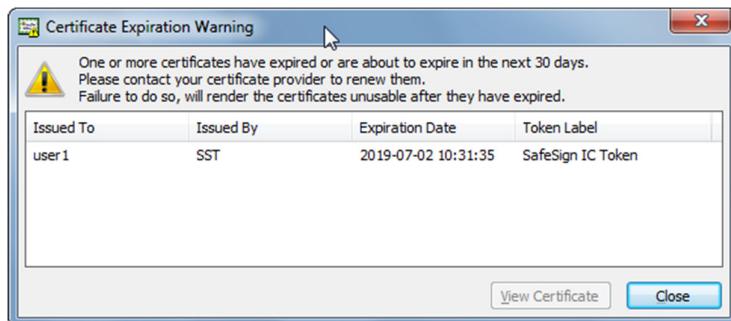


Figure 24: Certificate Expiration Warning

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:

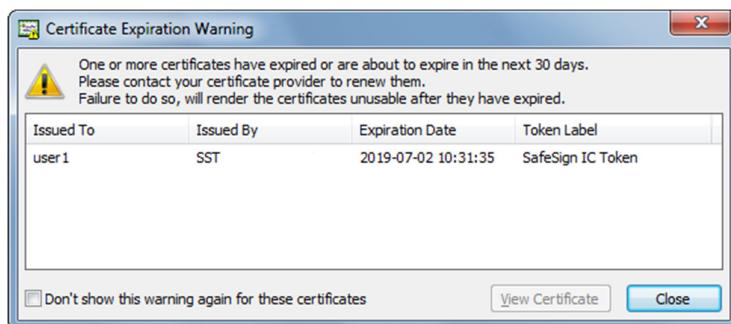


Figure 25: Certificate Expiration Warning



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**.

### 3.1.6 Close

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

## 3.2 Import Digital ID

The SafeSign IC TAU allows you to import a Digital ID on your SafeSign IC token. By importing the file, your keys and certificate will be securely stored on your token and can be used for secure communication. This greatly enhances the security of your Digital ID, now protected by two-factor authentication: to access it, you would need to have possession of the token and knowledge of the token’s PIN.

The function Import Digital ID can be used to import Digital ID files stored in PKCS #12 (.p12) or Personal Information Exchange (.pfx) format on your hard disk (or removable media).

- ☞ Note that the function Transfer ID to token (as available under Show Registered Digital IDs) should be used for Digital IDs that are already present / imported in the Microsoft Personal Certificate Store.
- ☞ Note that when SafeSign IC imports a Digital ID, the public key is not stored on the token. The reason behind this is to save space on the token, as the public key does not have to be on the token, for it is embedded in the certificate and used for public key operations only (and does not have to be kept secret).

1 To import a Digital ID, click **Digital IDs > Import Digital ID**, to open the following dialog:

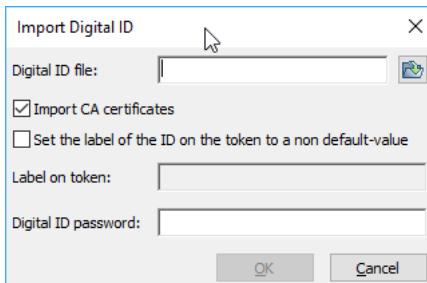


Figure 26: Digital IDs: Import Digital ID



- 2** First, you will need to specify the location where the Digital ID file is stored. The Digital ID file can be stored anywhere, either on a hard disk or on removable media. Click on the symbol to select the location:

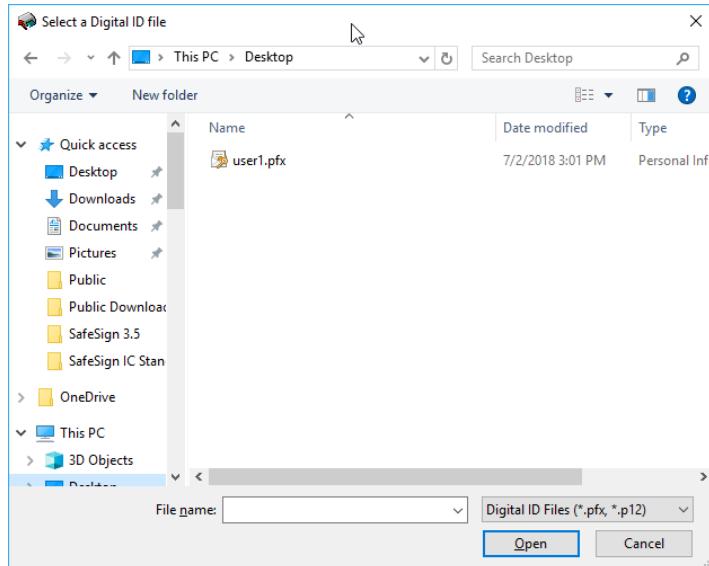


Figure 27: Import Digital ID: Select a Digital ID file

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

- 3** The *Import Digital ID* dialog will now show the (path to the) Digital ID file you have just selected:

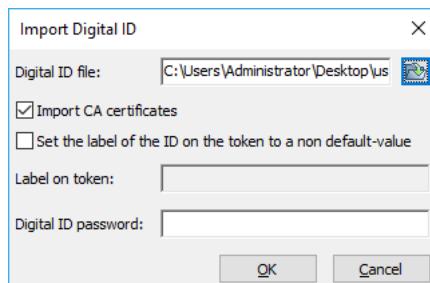


Figure 28: Import Digital ID: Digital ID file

- Enter the Digital ID password and click **OK**

Take the following into account when completing this dialog:

- The Digital ID password that you are requested to enter is the password that was used to protect the Digital ID. If you do not enter the correct password, you will get a prompt saying that the Digital ID needs a different password. You will then have to start the import a Digital ID procedure again by clicking **Digital IDs > Import Digital ID**.



- When importing a Digital ID, the label of the Digital ID as set by the application used to obtain the Digital ID, will be copied. If you wish to set your own label to the certificate and private key, select “Set the label of the ID on the token to a non-default value” and enter a label in the Label on token box. Note that this will only change the label as visible in the Show Token Objects dialog for the certificate and private key.
- Note that when importing a Digital ID, you may choose whether you want to import the CA certificates as well. By default, the option Import CA certificates is selected. If you do not wish to import the CA certificates on the token, deselect the checkbox.

**4** When you have clicked **OK** after entering the correct password for the Digital ID file, you will be asked to enter the PIN for the token:

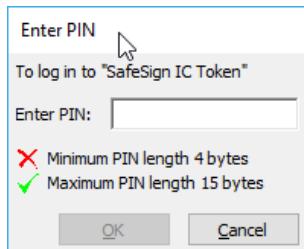


Figure 29: Enter PIN

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

**5** When the Digital ID has been successfully imported, the following prompt will inform you:

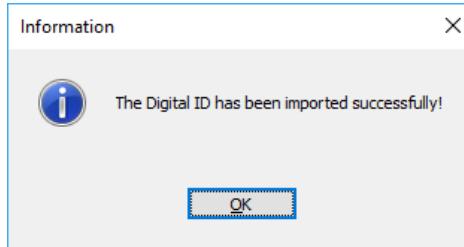


Figure 30: Import Digital ID: The Digital ID has been imported successfully

→ Click **OK** to close this dialog

- When you try to import a Digital ID that does not comply with the key length constraints of the supported token, you will get a key size error.
- When the token is full, i.e. does not have enough memory to import a / another Digital ID, you will get a 'Token out of memory' error. Note that you may not always be able to see why the token is out of memory; the amount of free public space may give an indication only.



### 3.3 Import Certificate

The SafeSign IC TAU allows you to import a Certificate Authority (CA) certificate on your SafeSign IC token. By importing the file, the CA 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.

→ Note that the Import Certificate feature can also be used to import Attribute Certificates.

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

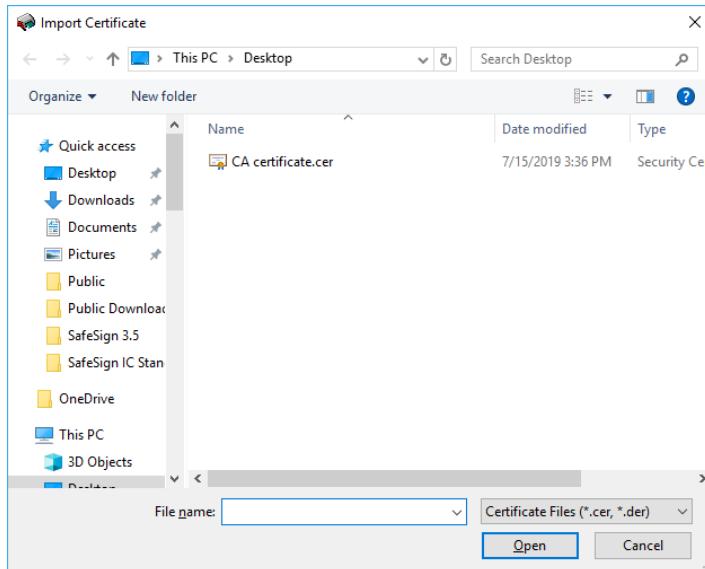


Figure 31: Import Certificate: Select Certificate

→ Select the file by clicking on it, then click Open



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

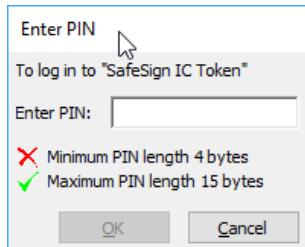


Figure 32: Enter PIN

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

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

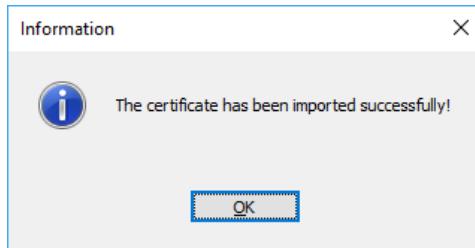


Figure 33: Import Certificate: The certificate has been imported successfully

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

### 3.4 Exit

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



## 4 Token

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

- Section 4.1: Initialise Token
- Section 4.2: Change PIN
- Section 4.3: 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

### 4.1 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 would like to emphasize that smart cards and / or USB tokens being produced for use with SafeSign IC by vendors that are not approved AET 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) are not eligible for any support by AET in case of problems, even if the user has purchased a SafeSign IC Maintenance and Support Agreement.

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.

These sections will use a NXP JCOP 2.4.1 R3 Java Card (J2A080) as an example.



#### 4.1.1 Initialise Token

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:

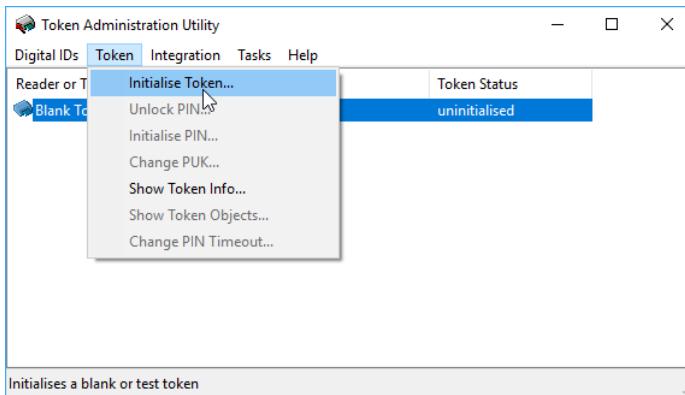


Figure 34: TAU: Initialise Token

→ 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:

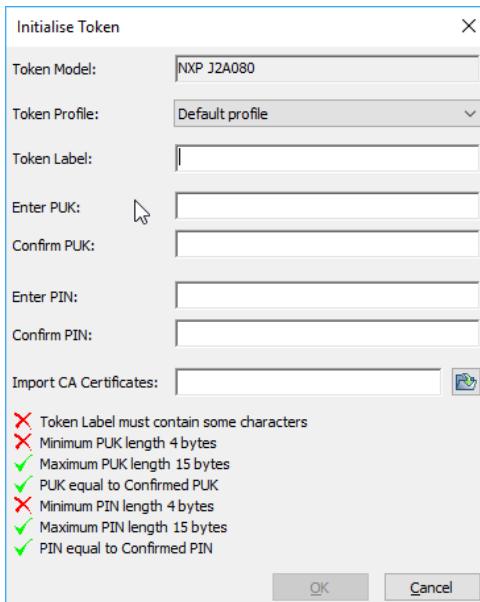


Figure 35: Initialise Token: empty

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 one (Default) profile. If greyed out, you do not have the (administrator) rights to modify it.

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	Requirement	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.
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.	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.
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".

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

The dialog box has the following fields and validation:

- Token Model: NXP J2A080
- Token Profile: Default profile
- Token Label: SafeSign IC Token
- Enter PUK: \*\*\*\*
- Confirm PUK: \*\*\*\*
- Enter PIN: \*\*\*
- Confirm PIN: \*\*\*
- Import CA Certificates: [button]
- Validation rules (all checked):
  - Token Label must contain some characters
  - Minimum PUK length 4 bytes
  - Maximum PUK length 15 bytes
  - PUK equal to Confirmed PUK
  - Minimum PIN length 4 bytes
  - Maximum PIN length 15 bytes
  - PIN equal to Confirmed PIN
- Buttons: OK, Cancel

*Figure 36: 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:

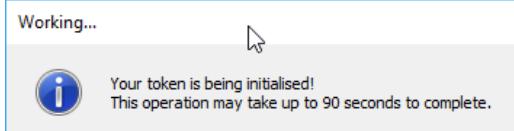


Figure 37: Initialise Token: Your token is being initialised

- ➔ 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:

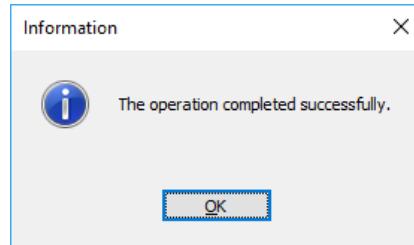


Figure 38: Initialise Token: The operation completed successfully

- ➔ Click **OK** to finish the initialisation

- 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:

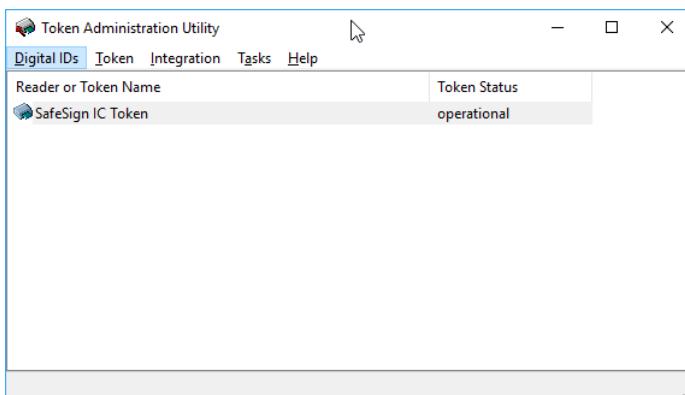


Figure 39: TAU: Token Status operational



#### 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. This error may also occur when there is not enough space left on the card.

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 local supplier or AET SafeSign Support for assistance.

#### 4.1.2 Wipe Token

When your token has been initialised (before), you will only be able to wipe the token. If you wipe a card, you will need to enter the current PUK, as it was set during initialisation, including minimum length, maximum length and retry counter. If non-default values have been used for the PUK during initialisation, the card will keep these during its lifetime.

- 1 If the token was initialised before, the **Token** menu will display the item **Wipe Token** (instead of Initialise Token, as in Figure 34):

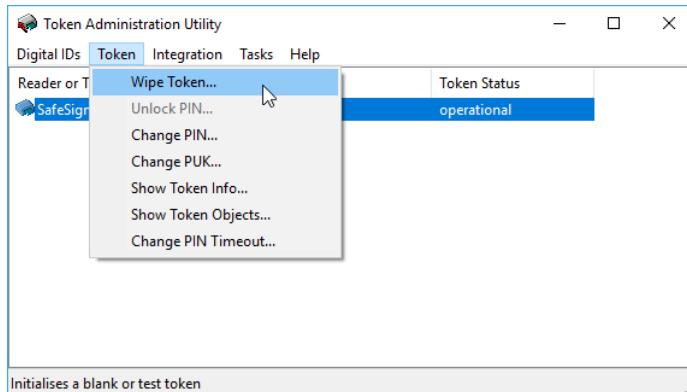


Figure 40: TAU: Wipe token

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



2 This will open the Wipe Token dialog box:

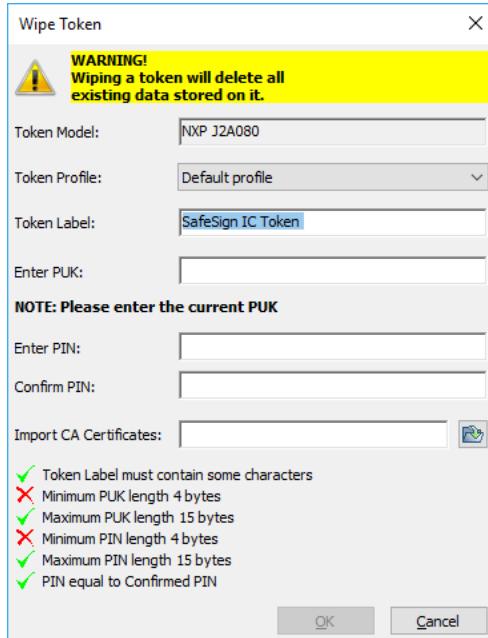


Figure 41: Wipe Token

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

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

Field	Requirement	Remarks
Token profile	The Token Profile should be set.	For Java Card v2.2+ 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.
Enter PUK	Minimum PUK length is 4 characters; maximum PUK length is 15 characters.	
Enter PIN	Minimum PIN length is 4 characters; maximum PIN length is 15 characters.	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 . Only when you enter a PIN / PUK of the required length will the PIN / PUK be accepted.
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 diacritics (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".

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

3

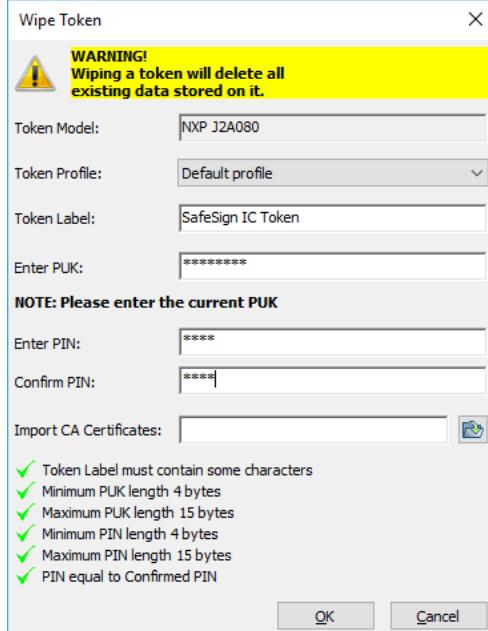


Figure 42: Wipe Token: completed

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

4

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

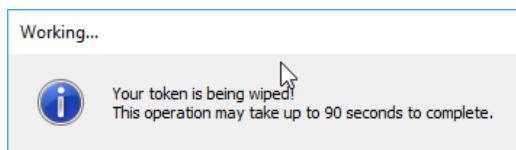


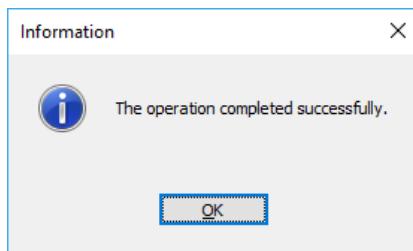
Figure 43: Your token is being wiped!

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 44: Wipe Token: The operation completed successfully*

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

#### 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. This error may also occur when there is not enough space left on the card.

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 local supplier or AET SafeSign Support for assistance.

#### 4.1.3 Recycle Token

When a special version of the 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.



#### 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:

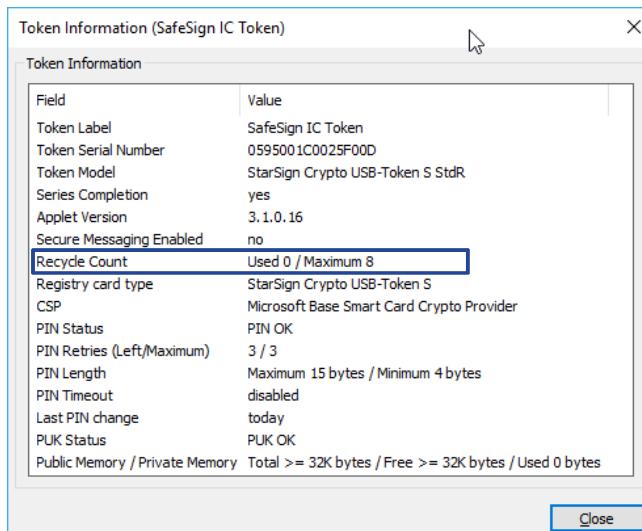


Figure 45: Token Information: Recycle Count

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 this token is 8.

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

#### 4.1.3.2 Recycle Process

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

1

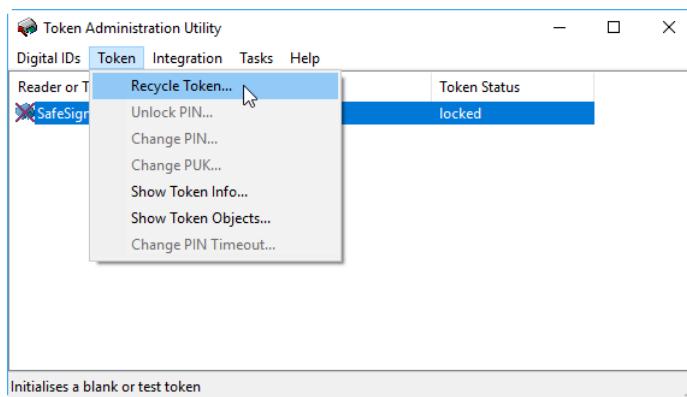


Figure 46: TAU: Recycle Token

- Click Recycle Token



2

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

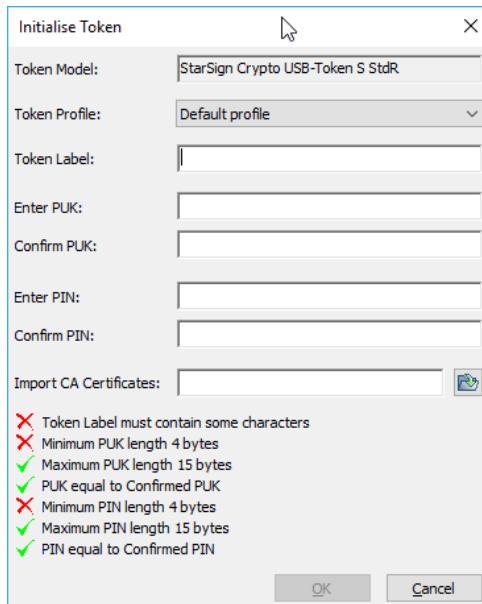


Figure 47: Initialise Token

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

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, by selecting **Initialise Token** from the **Token** menu.



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

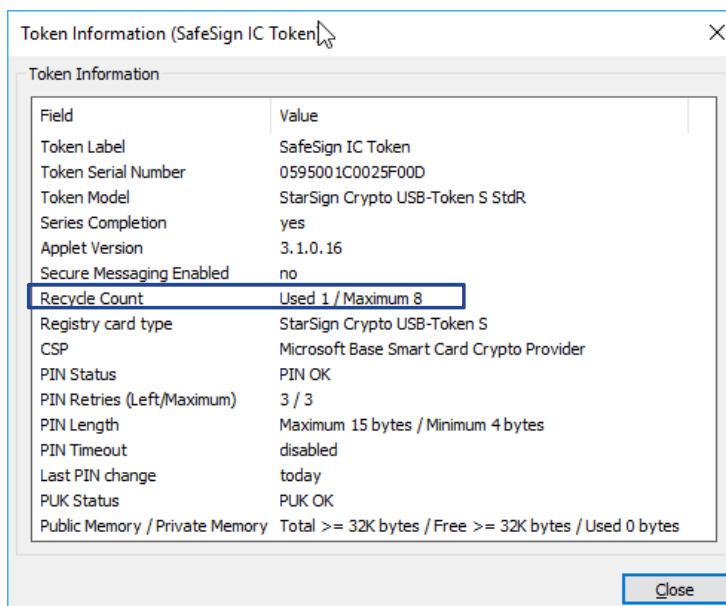


Figure 48: Recycle Count decreased



#### 4.1.3.3 Recycle Count exceeded

When the maximum recycle count has been reached ('Used 8 / Maximum 8' in our example), 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:

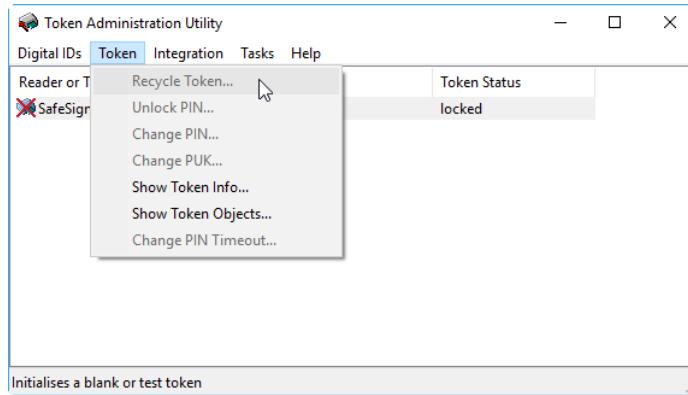


Figure 49: TAU: Token locked

#### 4.1.4 Initialise a Token with PIN Policy

When a special version of the 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 (see section 4.1.3).

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.;



#### 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:

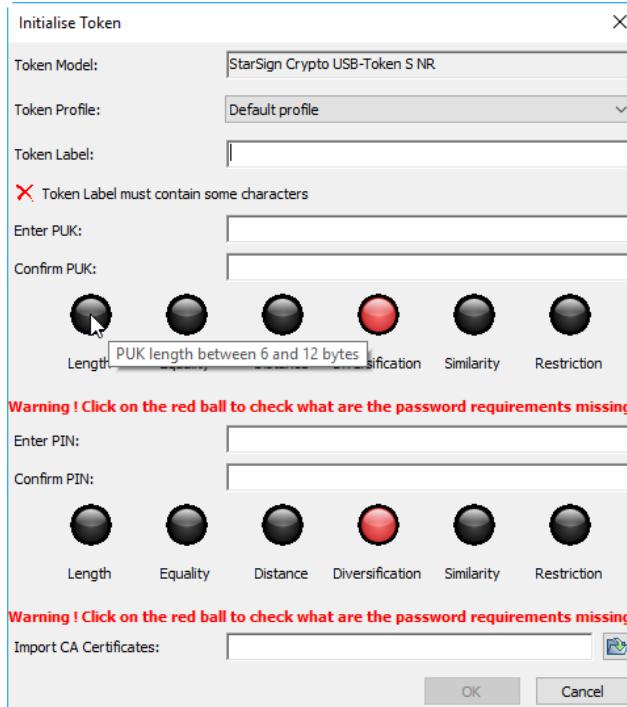


Figure 50: Initialise NR Token

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

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 downcase letters, numbers. It is missing upcase letters.”



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

The screenshot shows the 'Initialise Token' dialog box. In the 'Token Model' field, 'StarSign Crypto USB-Token S NR' is selected. The 'Token Profile' dropdown is set to 'Default profile'. The 'Token Label' field contains 'SafeSign IC Token', with a note below it stating 'Token Label must contain some characters'. The 'Enter PUK' and 'Confirm PUK' fields both show '\*\*\*\*\*'. Below these fields are six circular indicators representing password policies: Length (green), Equality (green), Distance (black), Diversification (green), Similarity (black), and Restriction (black). A green message at the top of the dialog box reads 'The informed password is correct and fulfilled all the password policy requirements!'. Below this message are fields for 'Enter PIN' and 'Confirm PIN', both showing '\*\*\*\*\*'. Underneath these are the same six policy indicators. Another green message appears above the 'Import CA Certificates' button. At the bottom right of the dialog box are 'OK' and 'Cancel' buttons.

Figure 51: Initialise NR Token: completed

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:

The screenshot shows the 'Initialise Token' dialog for a StarSign Crypto USB-Token S NR. It includes fields for Token Model (StarSign Crypto USB-Token S NR), Token Profile (Default profile), and Token Label (SafeSign IC Token). A note says 'Token Label must contain some characters'. Below are fields for Enter PUK and Confirm PUK, both containing '\*\*\*\*\*'. Underneath are six green circular progress indicators labeled Length, Equality, Distance, Diversification, Similarity, and Restriction.

**The informed password is correct and fulfilled all the password policy requirements !**

Enter PIN: \*\*\*\*\*

Confirm PIN: \*\*\*\*\*

Length      Equality      Distance      Diversification      Similarity      Restriction

**Warning ! Click on the red ball to check what are the password requirements missing !**

Import CA Certificates: [button]

Ok Cancel

Figure 52: 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.

#### 4.1.4.2 Change PIN

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

The screenshot shows the 'Change PIN' dialog for a 'SafeSign IC Token'. It has fields for Enter old PIN, Enter new PIN, and Confirm new PIN. Below are six circular progress indicators labeled Length, Equality, Distance, Diversification, Similarity, and Restriction. The first (Length) and last (Restriction) are red, while the others are green.

**Changing the PIN for "SafeSign IC Token":**

Enter old PIN:

Enter new PIN:

Confirm new PIN:

Length      Equality      Distance      Diversification      Similarity      Restriction

**Warning ! Click on the red ball to check what are the password requirements missing !**

Ok Cancel

Figure 53: 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:

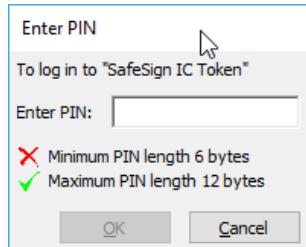


Figure 54: Enter PIN

#### 4.1.5 Import CA Certificates

The SafeSign IC TAU enables the import of:

- DER encoded .CER (CA) certificates
- DER encoded .CRT (A) 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 3.2;
- 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:

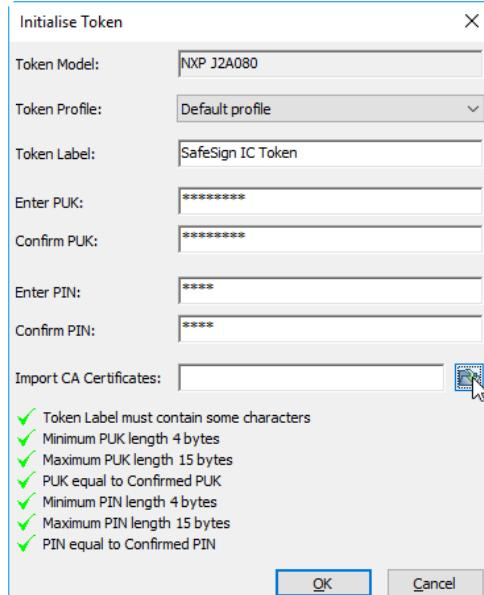


Figure 55: Initialise Token

- ➔ Click on the **Browse** icon



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

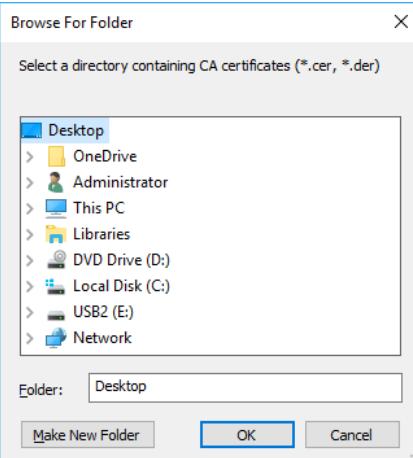


Figure 56: Import CA certificates: Browse For Folder

- Select a directory and click **OK**

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

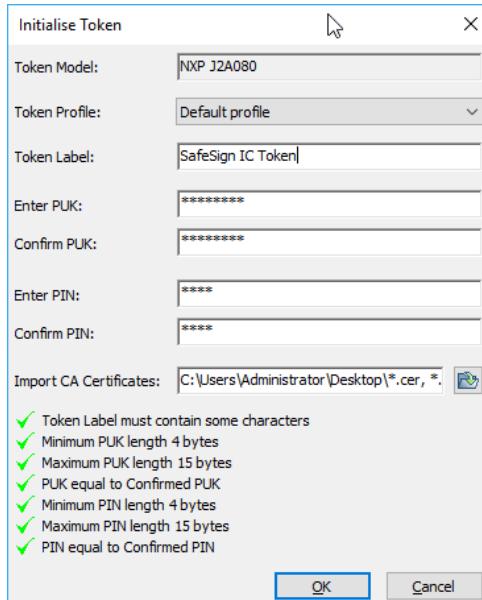


Figure 57: Initialise Token: Import CA certificates

- >Note that all CA certificates present in the directory will be imported.
- Click **OK** to initialise the token



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

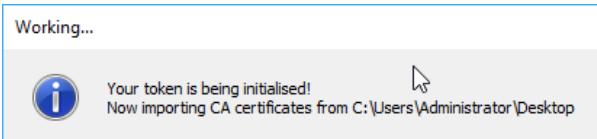


Figure 58: Initialise Token: Now importing CA certificates

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

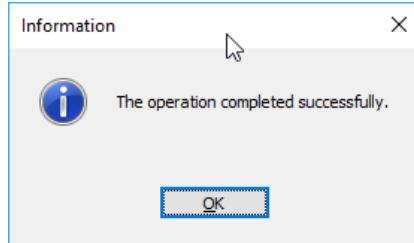


Figure 59: Initialise Token: The operation completed successfully

- Click **OK** to finish the initialisation

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

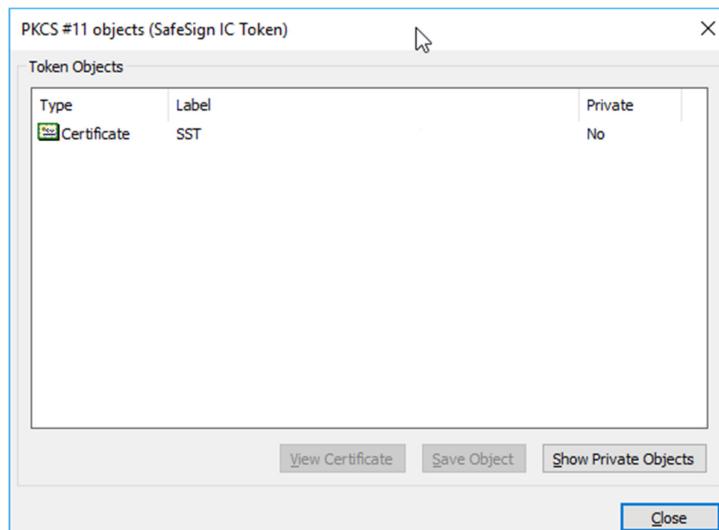


Figure 60: PKCS#11 objects: CA Certificate



## 4.2 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:

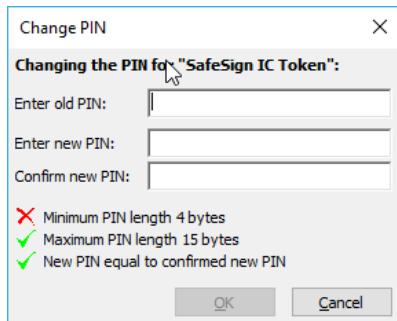


Figure 61: Change PIN

This dialog will identify the token 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:

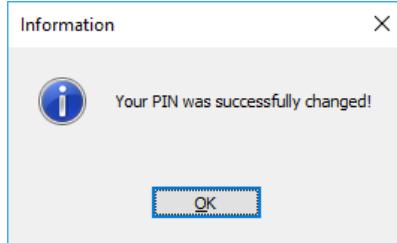


Figure 62: Change PIN: Your PIN was successfully changed

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

### 4.2.1 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):

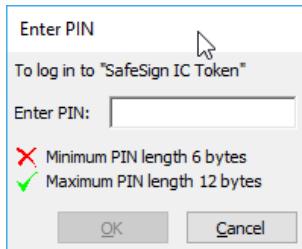


Figure 63: Enter PIN

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

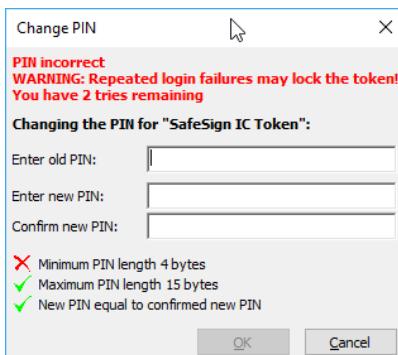


Figure 64: Enter PIN: You have 2 tries remaining

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

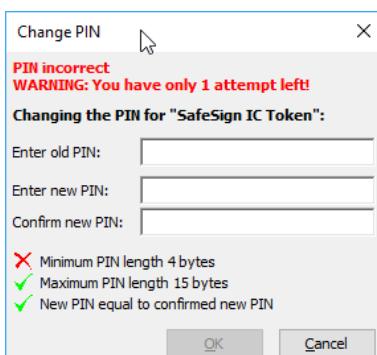


Figure 65: Enter PIN: You have only 1 attempt left



- 4 When the PIN is locked:

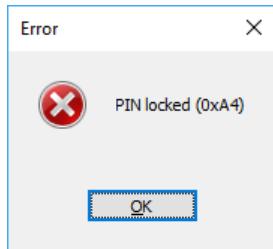


Figure 66: Enter PIN: PIN locked

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:

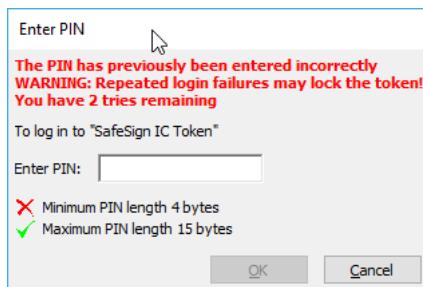


Figure 67: Enter PIN: The PIN has previously been entered incorrectly.

### 4.3 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:

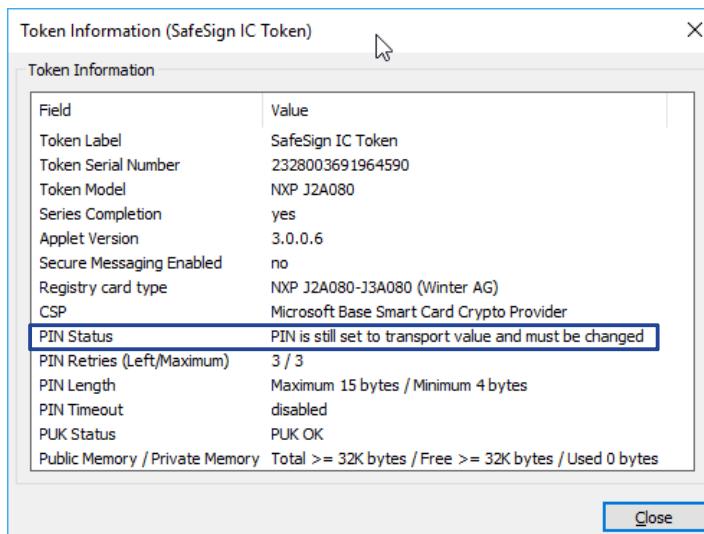


Figure 68: Token Information: PIN is still set to transport value



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

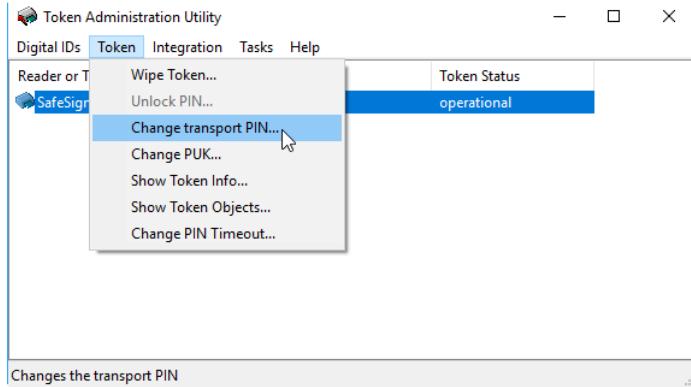


Figure 69: TAU: Change transport PIN

- Select Change transport PIN (as above)

- 2 This will open the *Change transport PIN* dialog:

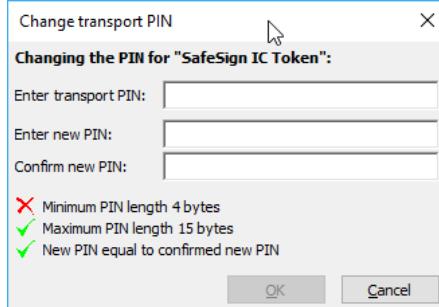


Figure 70: Change transport PIN

- 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:

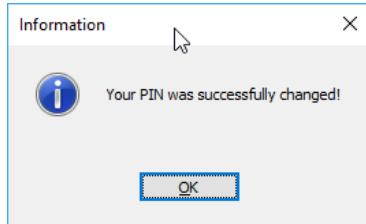


Figure 71: Change transport PIN: Your PIN was successfully changed

- Click OK

You can now use your token with your own PIN.



## 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

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

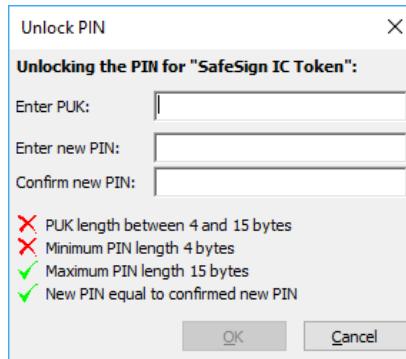


Figure 72: *Unlock PIN*

This dialog will identify the token 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

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

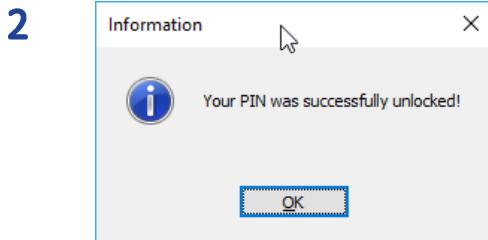


Figure 73: *Unlock PIN: Your PIN was successfully unlocked*

- 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 (such as Import Digital IDs).



#### 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 SafeSign Support.

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

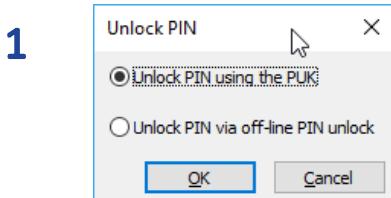


Figure 74: Unlock PIN: unlocking methods

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

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

2

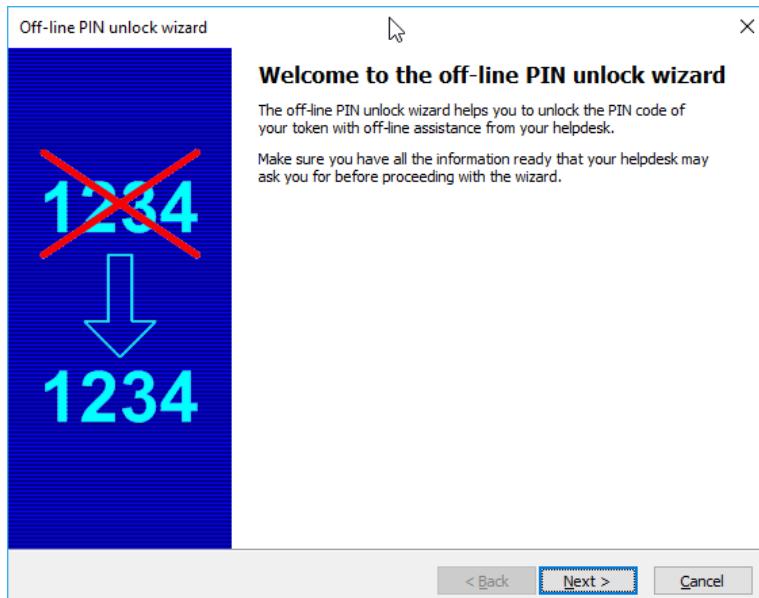


Figure 75: Off-line PIN unlock wizard: Welcome to the off-line PIN unlock wizard

- 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:

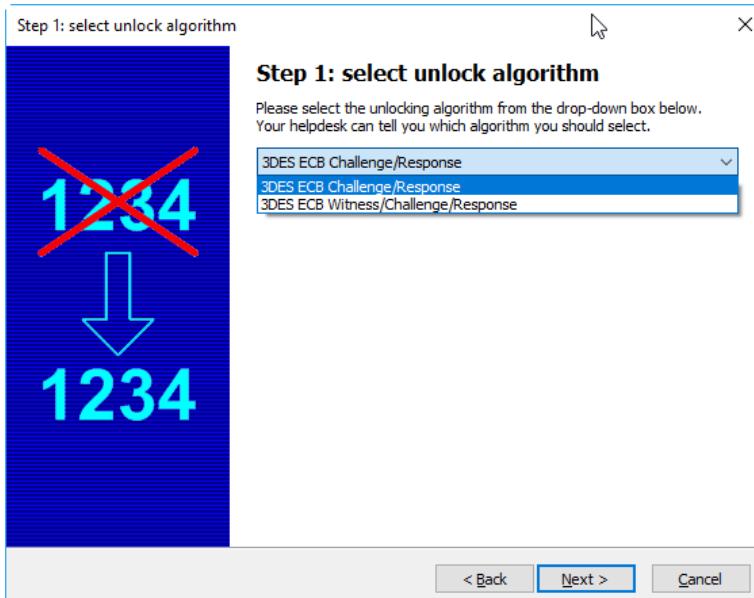


Figure 76: Off-line PIN unlock wizard: Step 1: select unlock algorithm

- Select the unlocking algorithm and click **Next** to continue
- 4** Once you have selected an algorithm, the next step is to report the challenge requested from the card:

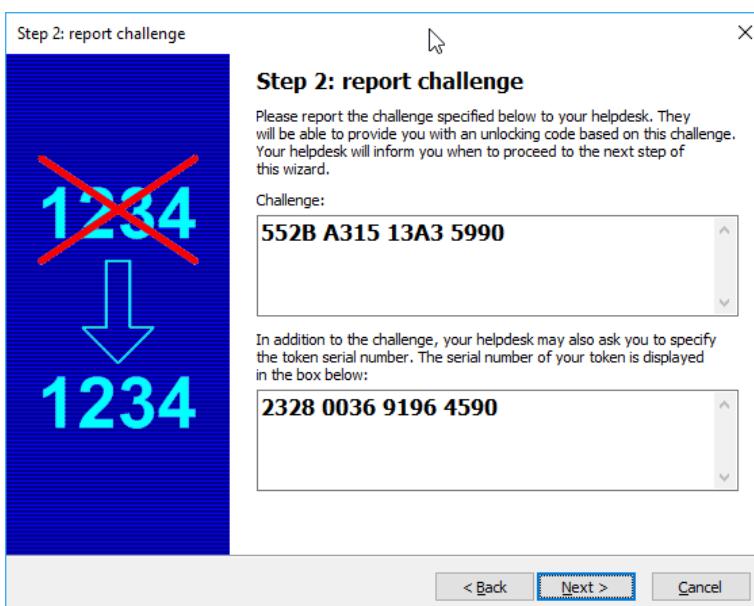


Figure 77: Off-line PIN unlock wizard: Step 2: report challenge

- 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:

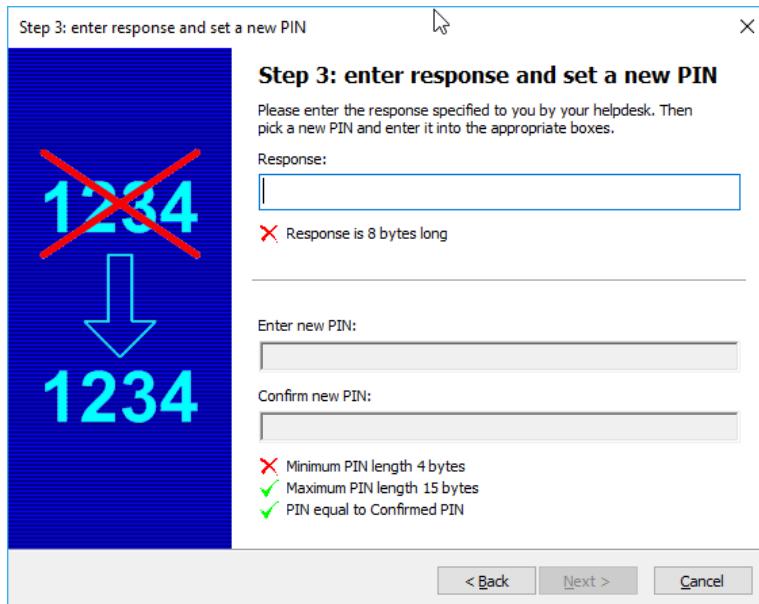


Figure 78: Off-line PIN unlock wizard: Step 3: enter response and set a new PIN

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

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

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

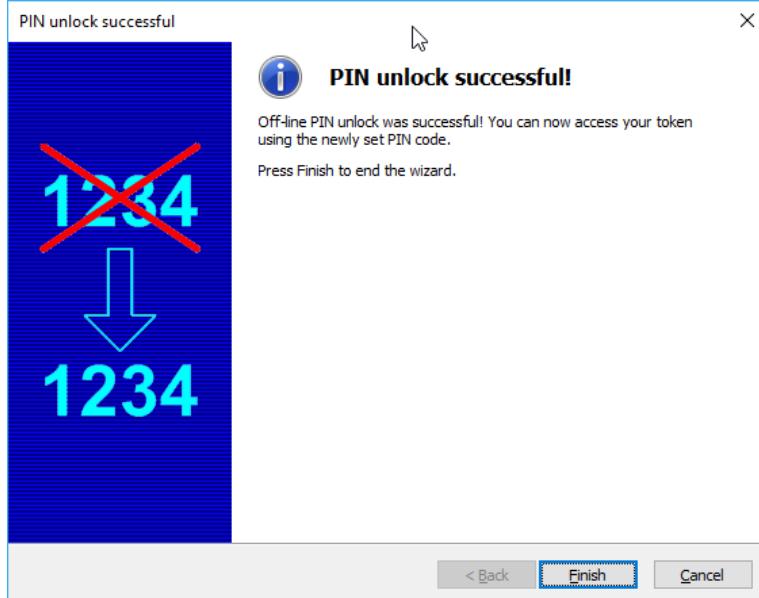


Figure 79: Off-line PIN unlock wizard: PIN unlock successful

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



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

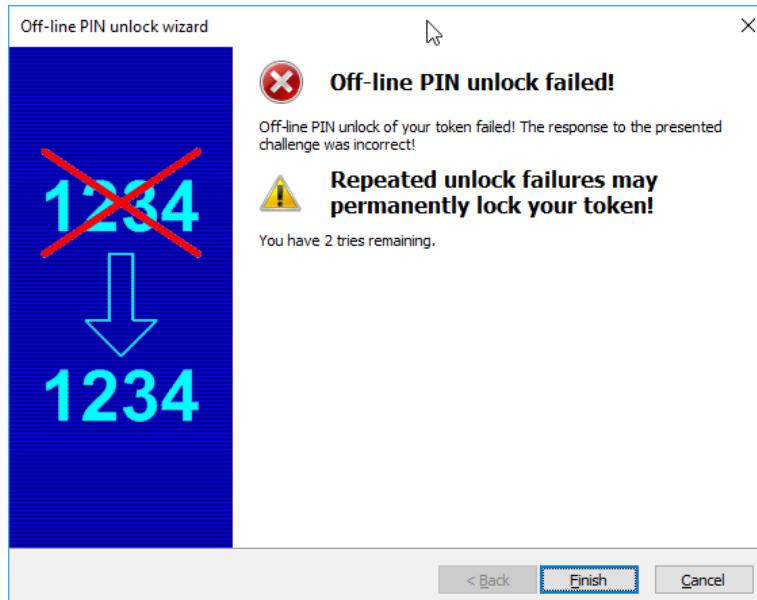


Figure 80: Off-line PIN unlock wizard: Off-line PIN unlock failed

If off-line PIN unlock fails after the two remaining tries, you can only unlock the PIN using the PUK, as described in section 4.4.1.

## 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:

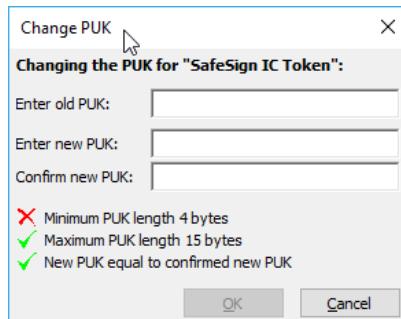


Figure 81: Change PUK

This dialog will identify the token 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 fulfil 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:

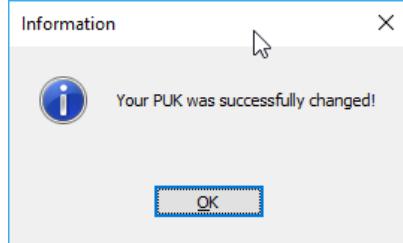


Figure 82: Change PUK: Your PUK was successfully changed

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

#### 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 cannot be used anymore:

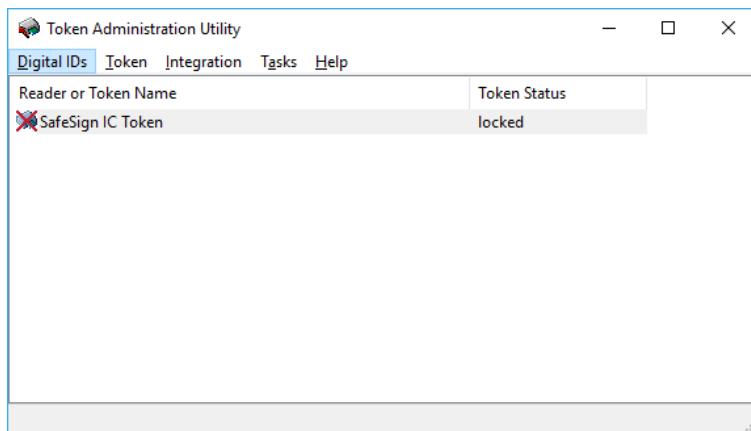


Figure 83: TAU: Token Status locked



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. Here also, four notifications are possible:

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

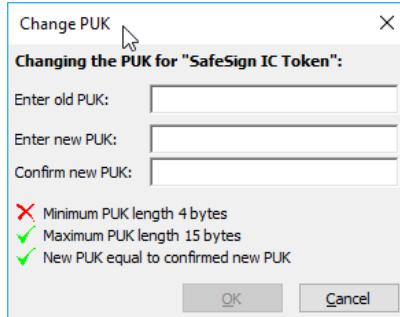


Figure 84: Change PUK

- 2 When the PUK has been entered incorrectly:

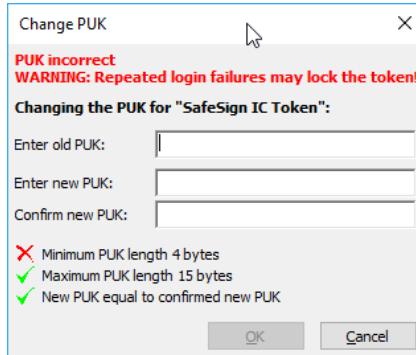


Figure 85: Change PUK: Repeated login failures may lock the token

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

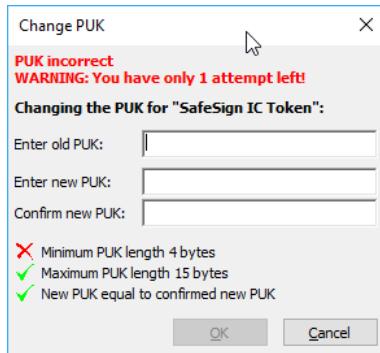


Figure 86: Change PUK: You have only 1 attempt left



- 4 When the PUK is locked:

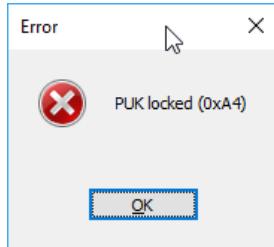


Figure 87: PUK locked

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:

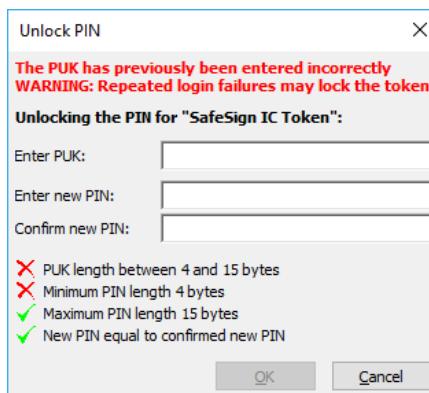


Figure 88: Change PUK: The PUK has previously been entered incorrectly

- As for the PIN, it is possible to enable a retry counter for the PUK (in the registry<sup>1</sup>). When the PUK retry counter is enabled, the dialogs that require PUK entry will also display how many attempts are left:

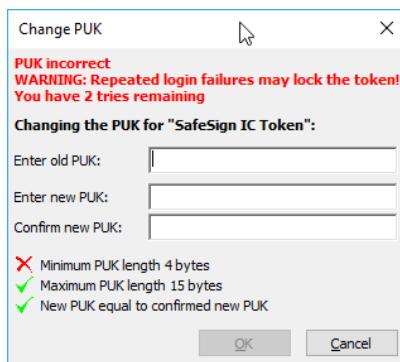


Figure 89: Change PUK: retry counter enabled

<sup>1</sup> Please refer to the Administrator's Guide.



## 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:

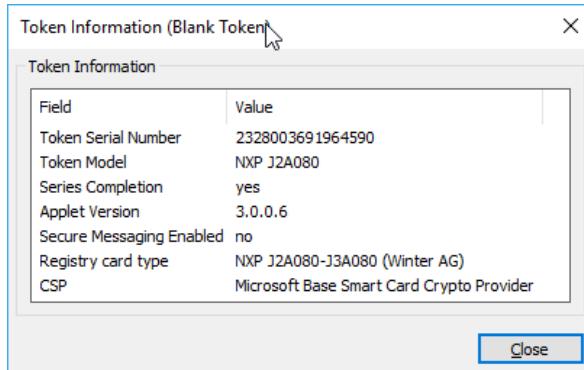


Figure 90: Token Information: Blank Token

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

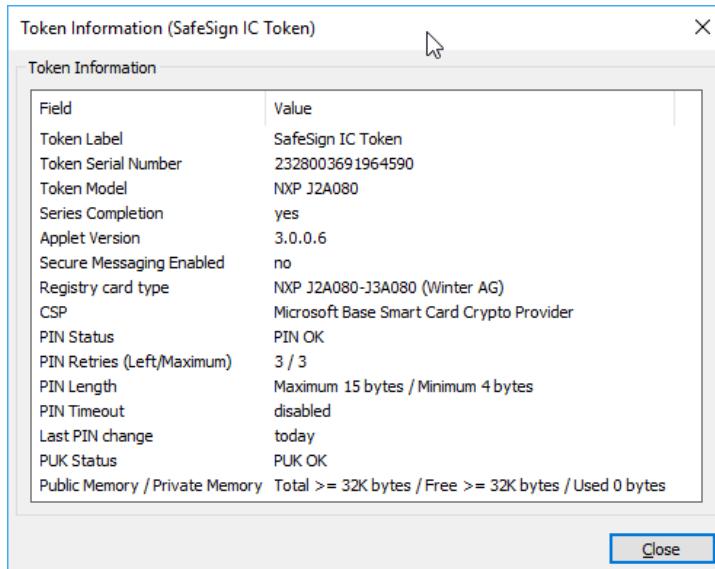


Figure 91: Token Information: SafeSign IC Token

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

### 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.

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

Note that (the use of) a test token is not secure and that the 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.

#### 4.6.6 Secure messaging enabled

For certification purposes with the ICP-Brazil standard, some new functionality was implemented in the SafeSign IC applet, for various cards from different vendors. For these cards, secure messaging may be enabled.

The Secure Messaging Enabled field indicates whether the card you are using has secure messaging enabled (in addition to 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.

On 32-bit Windows Operating Systems, the card ATRs are stored in:

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards]

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".



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

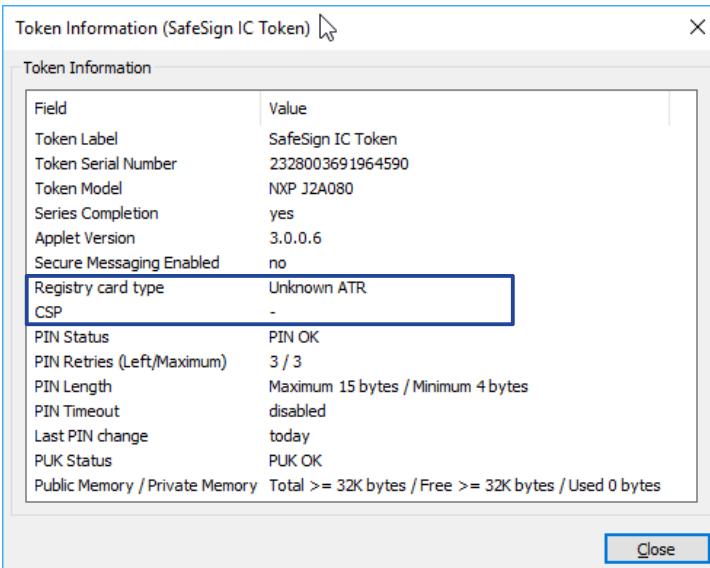


Figure 92: Token Information: Unknown ATR

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:

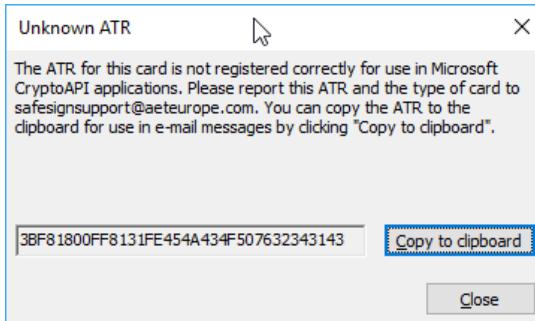


Figure 93: Unknown ATR

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:

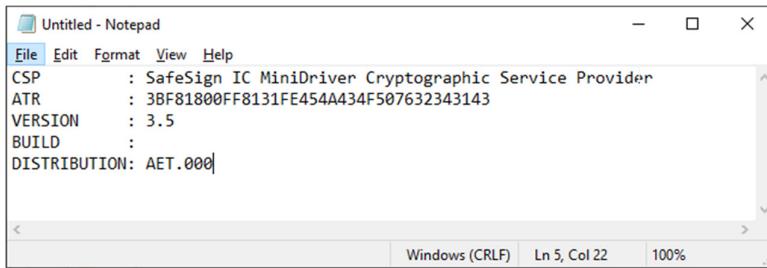


Figure 94: Unknown ATR: Copy to clipboard

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.



- >Note that in Windows 7, with SafeSign IC Standard installed, when the ATR of a token is not recognised, Windows will start looking for drivers for the Smart Card. This is because Windows tries to download and install the smart card minidrivers for the card through Plug and Play services. See <https://support.microsoft.com/en-us/kb/976832> for more details.

#### 4.6.8 CSP

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

With SafeSign IC Standard installed, the CSP is: *SafeSign IC Standard Cryptographic Service Provider*.

With SafeSign IC Minidriver installed, the CSP is: *Microsoft Base Smart Card Crypto Provider*.

#### 4.6.9 PIN Status

See also section 4.2.1.

Displays the status of the PIN:

- OK
- PIN has been entered incorrectly at least once
- One final attempt left to enter PIN incorrectly
- 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.

#### 4.6.12 PIN Timeout

Displays the status of the PIN Timeout setting.

The PIN Timeout is by default disabled. 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.

The PIN Timeout functionality is only supported in SafeSign IC Standard, for applications using SafeSign IC PKCS #11 and SafeSign IC CSP/KSP.

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).

#### 4.6.14 PUK Status

Displays the status of the PUK:

- OK
- PUK has been entered incorrectly at least once
- One final attempt left to enter PUK incorrectly
- LOCKED

See also section 4.5.1.

#### 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).<sup>2</sup>

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.

---

<sup>2</sup> Using the method described in the 'Application Programming Interface Java Card™ Platform, Version 2.2.2'.



## 4.7 Show Token Objects

The option Show Token Objects provides a more detailed and technical view of the contents of the token, displaying all the separate objects on the token, than the option Show Registered Digital IDs. It is not designed to give a detailed and correlated structure between the objects on the token though (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.

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

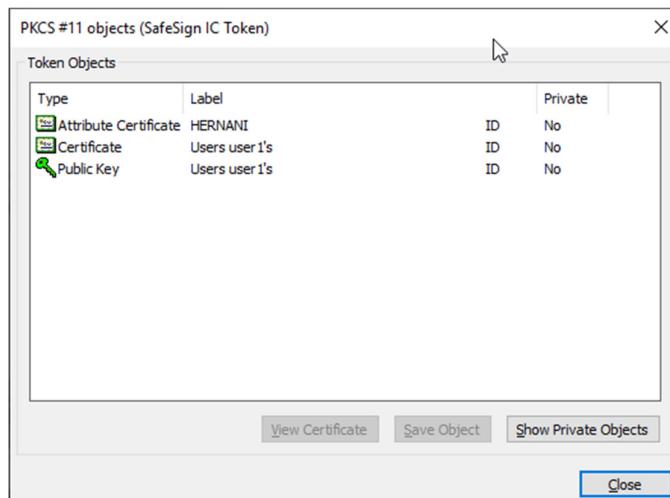


Figure 95: TAU: PKCS #11 objects

This dialog will display the Public token objects, including Public Keys, (PKI) Certificates and 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:

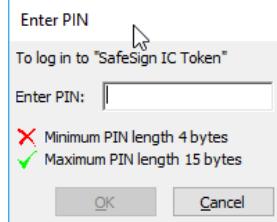


Figure 96: PKCS #11 objects: Enter PIN

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



3

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

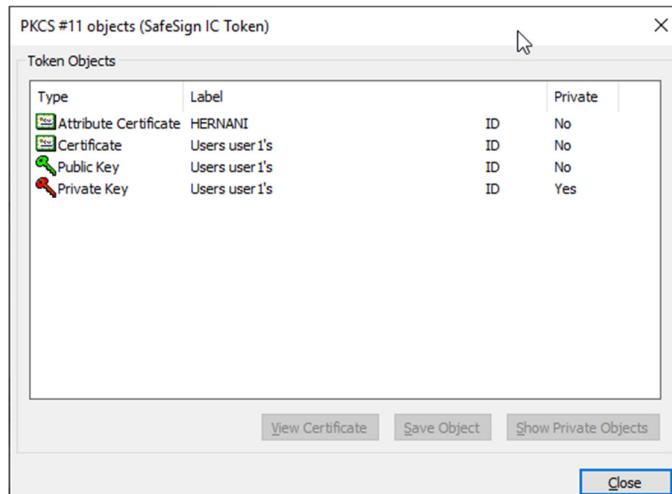


Figure 97: PKCS #11 Objects: All objects

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

#### 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.

##### 4.7.1.1 PKI Certificate

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

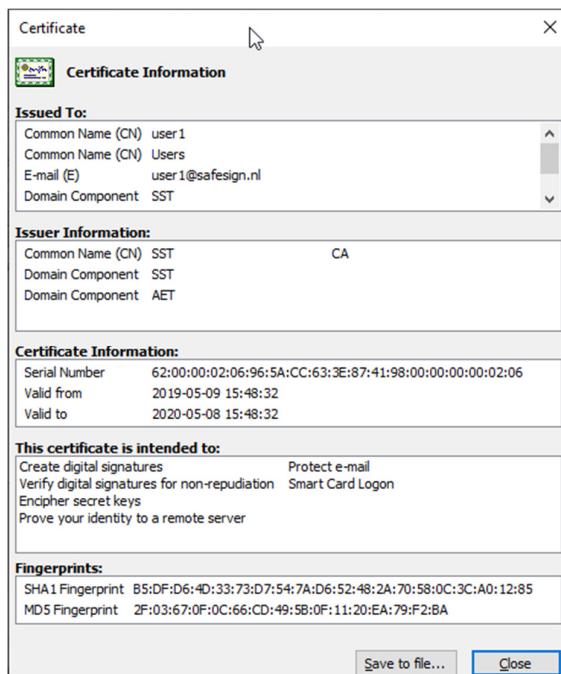


Figure 98: Certificate Information



#### 4.7.1.2 Attribute Certificate

In case of an Attribute Certificate, the following information will be displayed:

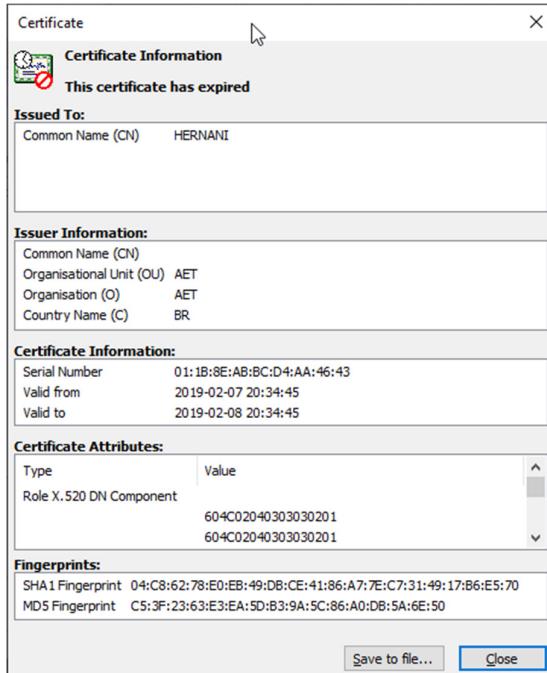


Figure 99: Certificate Information

#### 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:

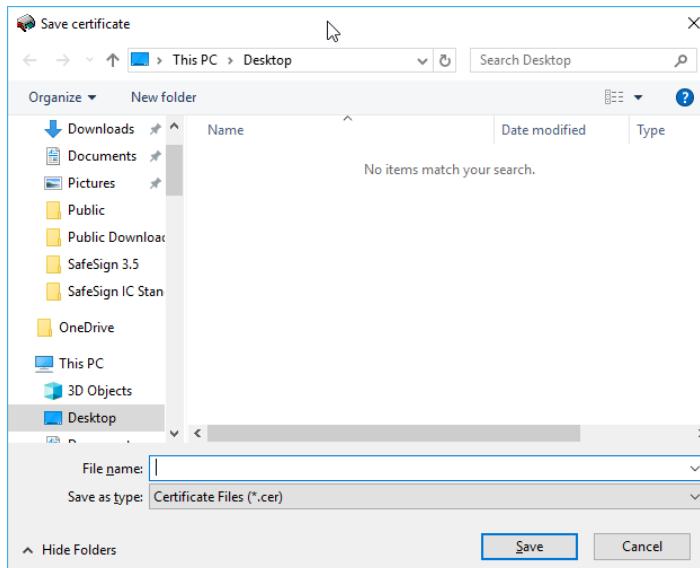


Figure 100: Save certificate

→ Select a location and click **Save**



## 4.8 Change PIN Timeout

The PIN Timeout functionality is only supported in SafeSign IC Standard for the SafeSign IC PKCS #11 and SafeSign IC CSP/KSP. With SafeSign IC Minidriver installed, the PIN Timeout functionality will work for the SafeSign IC PKCS #11, but not for the Microsoft Base Smart Card Crypto Provider.

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.

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



Figure 101: 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 (30 seconds in our example):

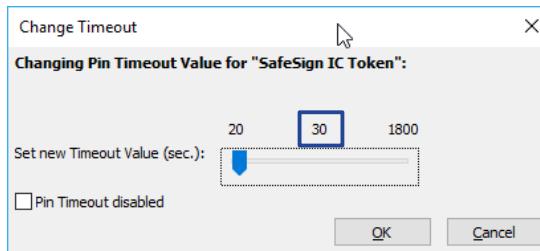


Figure 102: Change Timeout: PIN Timeout enabled

- Click OK



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

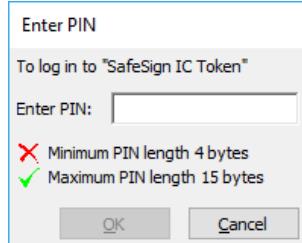


Figure 103: Enter PIN

- Enter the PIN and click OK

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

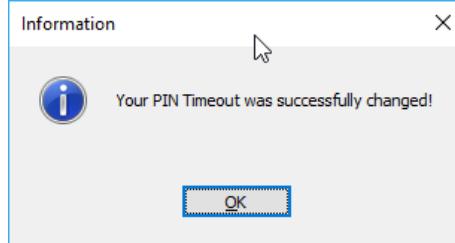


Figure 104: Change Timeout: Your PIN Timeout was successfully changed

- Click OK

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

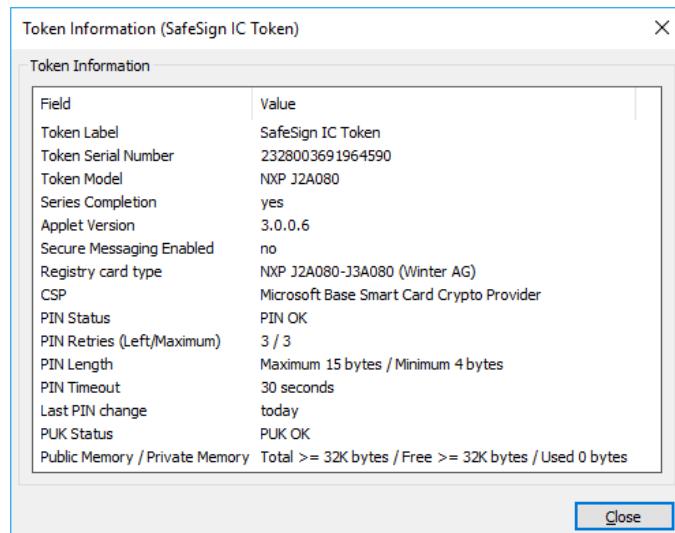


Figure 105: Token Information: PIN Timeout value



## 5 Integration

When you have Mozilla Firefox installed on your computer, the SafeSign IC InstallShield Wizard will allow you to install SafeSign IC in Firefox during the SafeSign IC installation procedure. For more information on how to do this, refer to the SafeSign IC Installation Guide.

In addition, it is also possible to install SafeSign IC in Firefox at a later stage, through the *Integration* menu of the TAU, which also allows you to de-install SafeSign IC from Firefox.

### 5.1 Install SafeSign in Firefox

- 1 In the TAU, select **Integration > Install SafeSign in Firefox** to open the *SafeSign IC for Firefox Installer*:

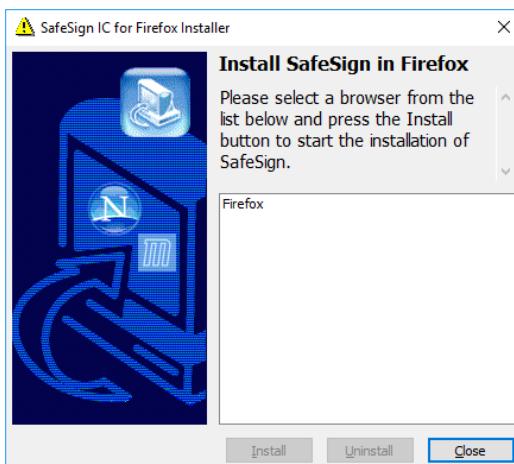


Figure 106: Firefox Installer: Install SafeSign in Firefox

This dialog will display whether Firefox is present on your system and allows you to install SafeSign IC as a security module.

- ➔ Select the Firefox browser from the list and click **Install**
  
- 2 Upon selecting Firefox from the list and clicking **Install**, the SafeSign IC PKCS #11 Library will be installed as a security module in Firefox:

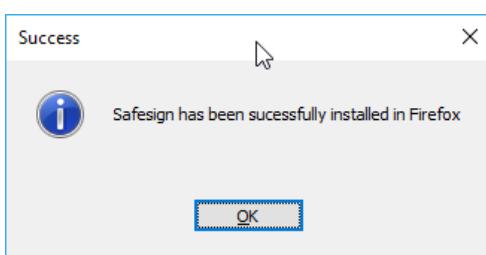


Figure 107: Firefox Installer: SafeSign has been successfully installed in Firefox

- ➔ Click **OK**



## 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 two tasks by default (that apply to all cards):

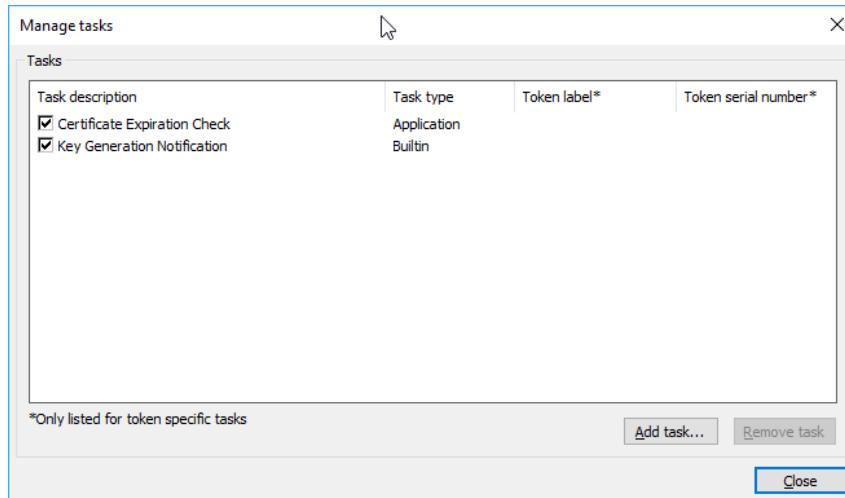


Figure 108: Manage tasks

- The task “Certificate Expiration Check” will prompt a dialog when a certificate is expired or is about to expire.
- The task “Key Generation Notification” will prompt a dialog during key generation (only) when SafeSign Standard (SafeSign CSP) installed.

If you want to disable one of the tasks, for example certificate expiration checking, 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 both tasks are deselected, the process ‘aetcrss1.exe’ will be ended automatically, so that it does not interfere with other processes.



## 6.1 Adding a Task

You can add a task by clicking **Add task**.

You can select two task types:

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

### 6.1.1 Launch an application

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

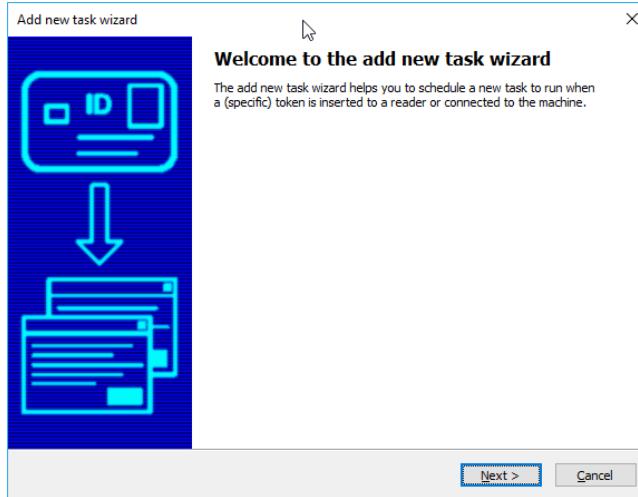


Figure 109: Add new task wizard: Welcome to the add new task wizard

→ Click **Next**

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

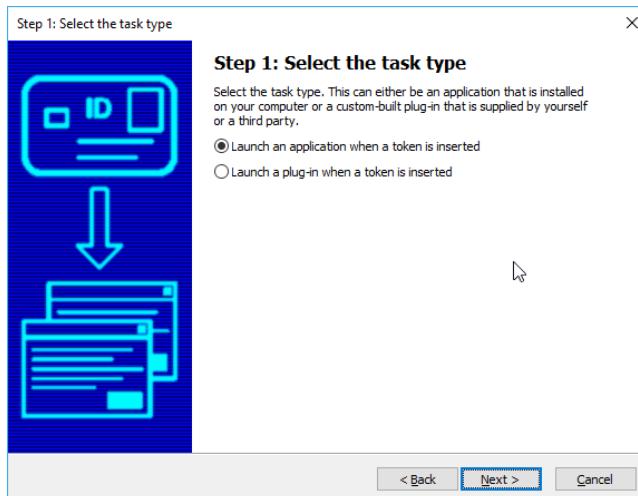
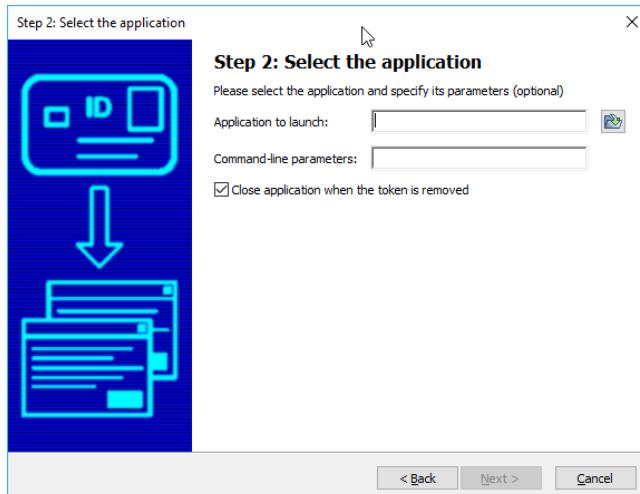


Figure 110: Add new task wizard: Step 1: Select the task type

→ 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 111: 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.

- ☞ 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.
  - ➔ When you have completed the fields, click **Next** to continue
  - ☞ Note that when selecting the option to “Close the application when the token is removed”, the Task Manager 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:

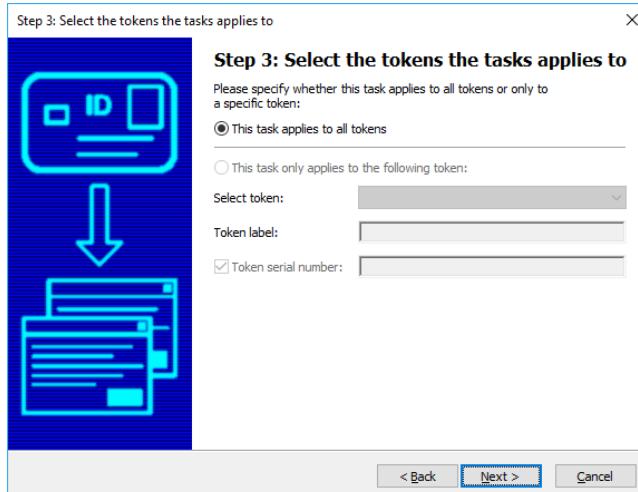


Figure 112: Add new task wizard: Step 3: Select the tokens the task applies to

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

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

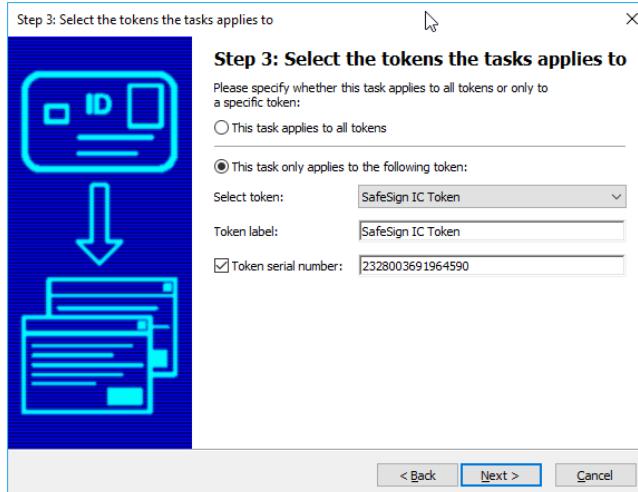


Figure 113: Step 3: This task only applies to the following token

- 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**



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

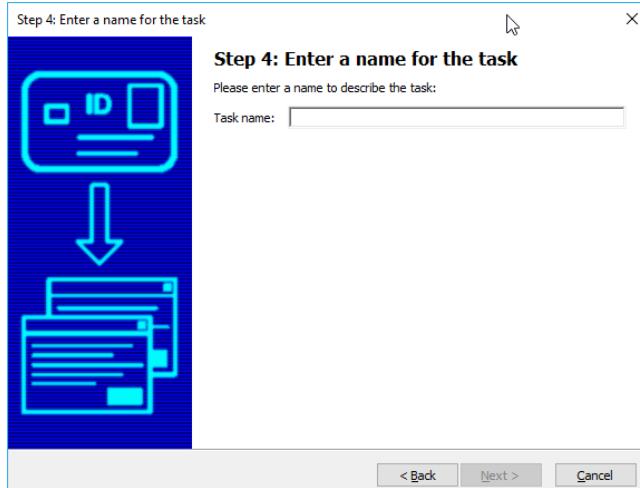


Figure 114: Add new task wizard: Step 4: Enter a name for the task

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

- 6 These four steps conclude the Add a new task wizard:

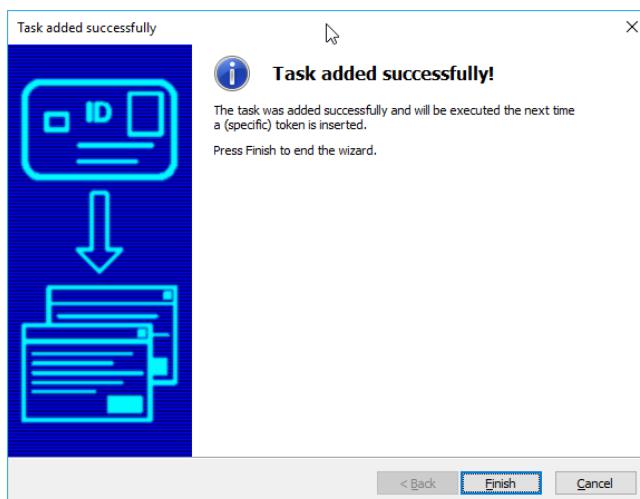


Figure 115: Add new task wizard: Task added successfully

- Click **Finish**



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

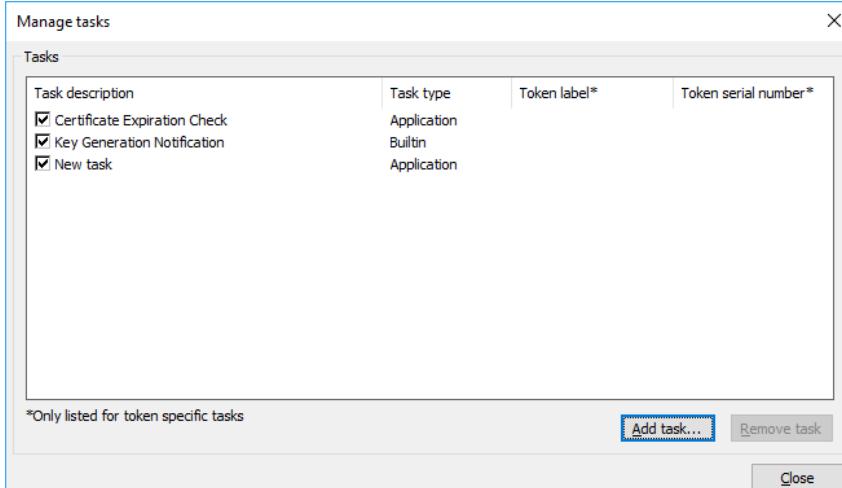


Figure 116: Manage tasks: New task

When a token is inserted, the application will start.

#### 6.1.2 Launch a plug-in

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

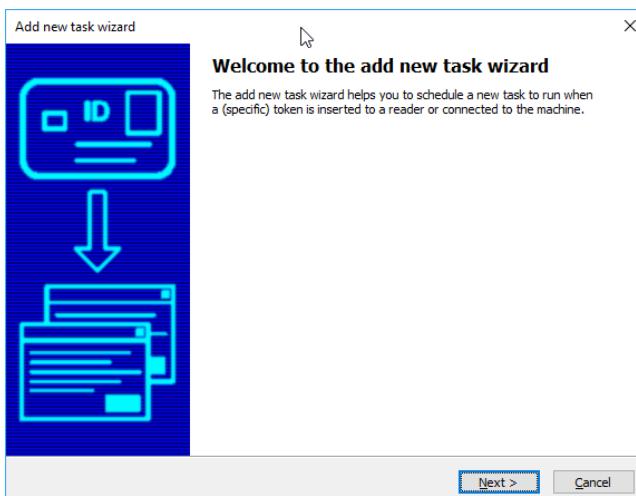


Figure 117: Add new task wizard: Welcome to the add new task wizard

- Click **Next**



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

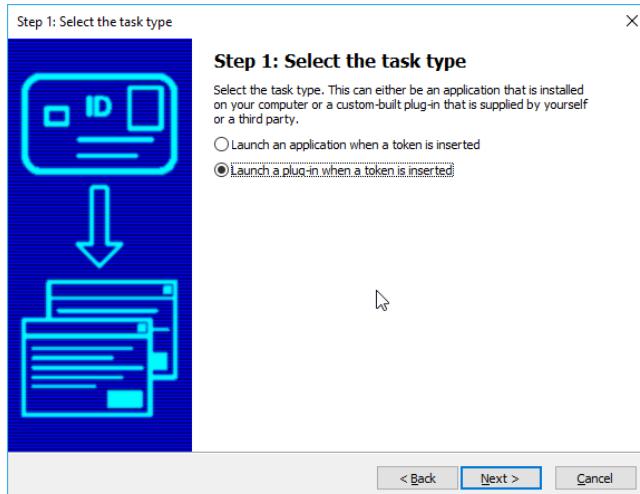


Figure 118: Add new task wizard: Step 1: Select the plug-in

- ➔ Select the plug-in to call and click **Next**

- 3** Upon selecting the option “Launch a plug-in when a token is inserted”, Step 2 will allow you to specify the plug-in to call:

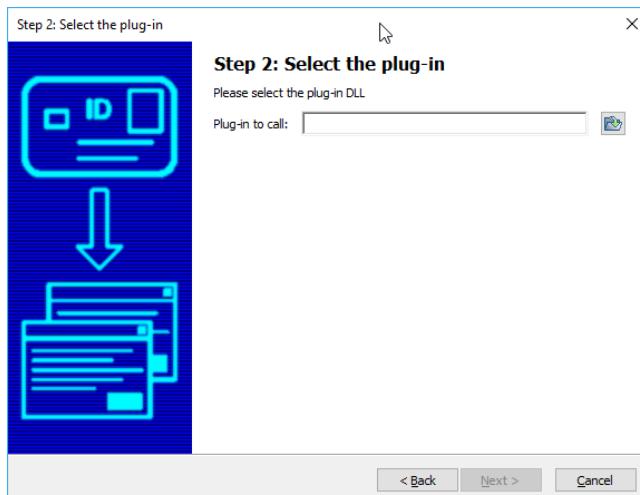


Figure 119: Add a new task wizard: Step 2: Select the plug-in

- ➔ Select the plug-in and click **Next**



- 4 The next step in the process is to select if the task applies to all tokens, or only to a specific token:

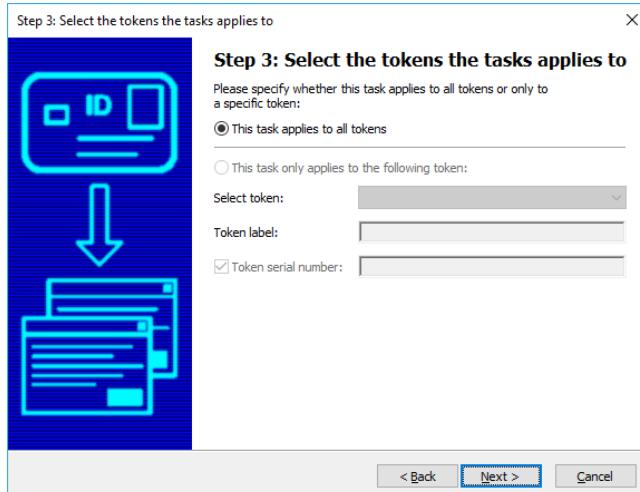


Figure 120: Add new task wizard: Step 3: Select the tokens the task applies to

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

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

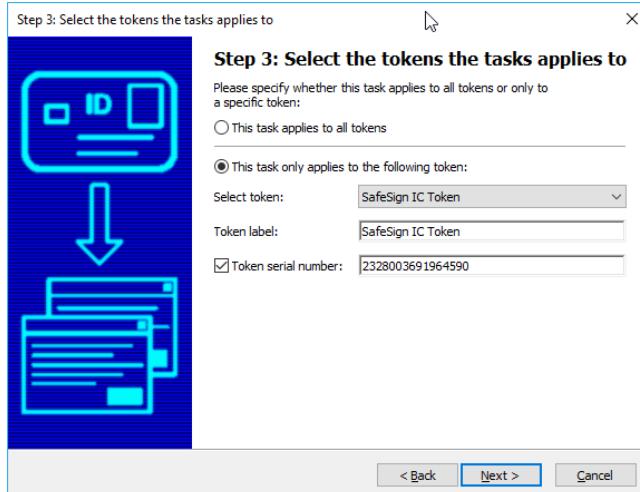


Figure 121: Step 3: This task only applies to the following token

In addition, 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**



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

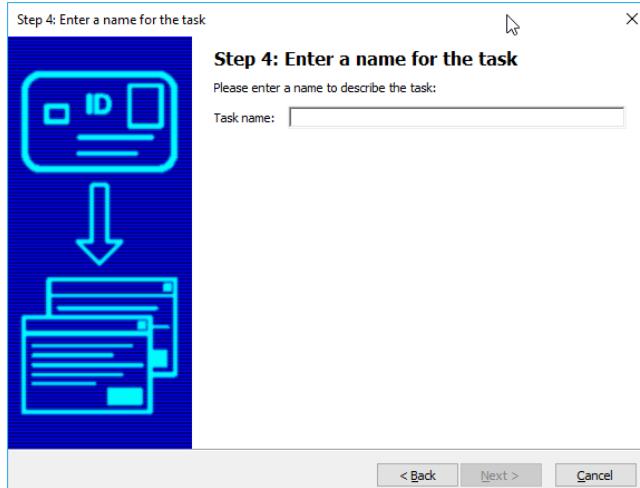


Figure 122: Add new task wizard: Step 4: Enter a name for the task

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

- 6 These four steps conclude the Add a new task wizard:

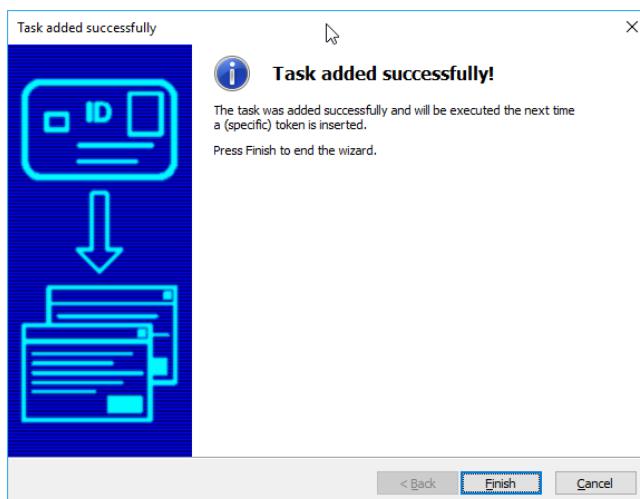


Figure 123: Add new task wizard: Task added successfully

- Click **Finish**



7

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

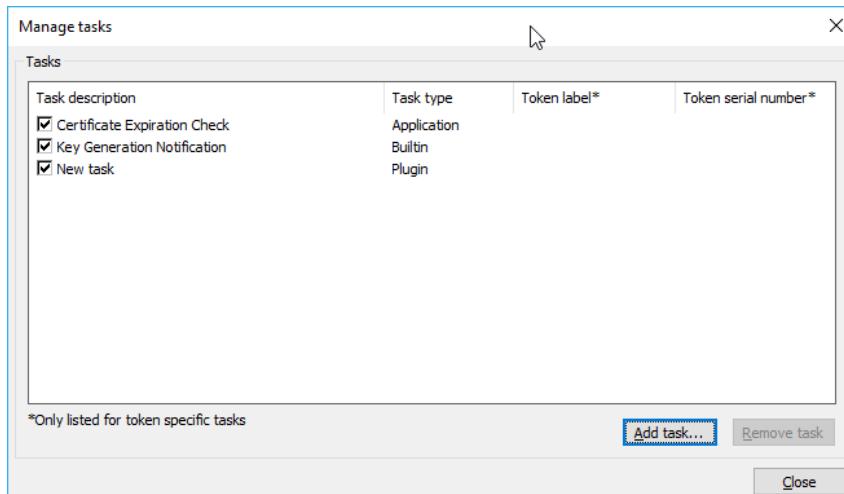


Figure 124: Manage tasks: New task



## 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 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 SafeSign Support.

#### 7.1.1 Windows 32-bit and 64-bit

SafeSign IC (Standard and Minidriver) for Windows comes in a 32-bit and 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).

The difference between SafeSign IC Standard and SafeSign IC Minidriver on Windows lies in the fact that SafeSign IC Standard includes the SafeSign IC CSP Library (*aetcsss1.dll*), whereas SafeSign IC Minidriver includes the SafeSign Read Write Card Module / Minidriver (*aetrwcm1.dll*) to interface with the Microsoft Base Smart Card CSP / KSP.

#### 7.1.2 Linux 64-bit

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

#### 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.



## 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:

- Section 8.1: Analyse certificate quality
- Section 8.2: Dump token contents
- 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:

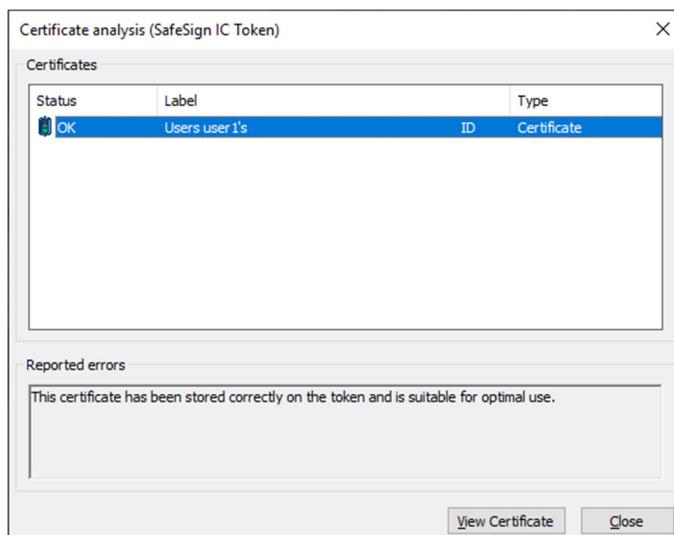


Figure 125: Certificate analysis: OK



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:

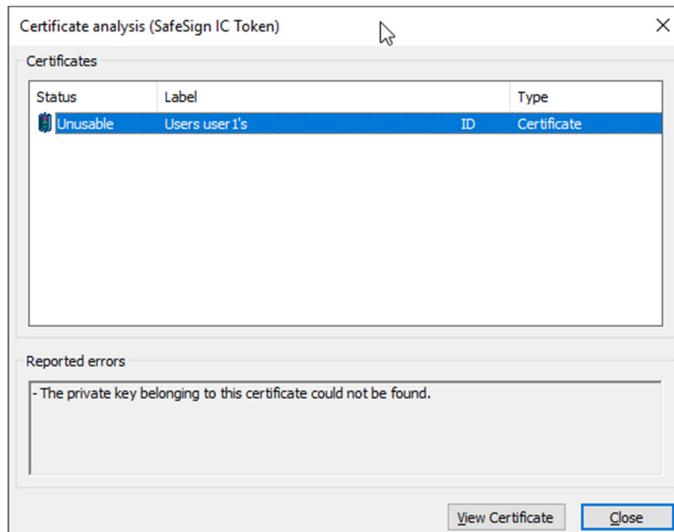


Figure 126: Certificate analysis: Unusable

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 **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.



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

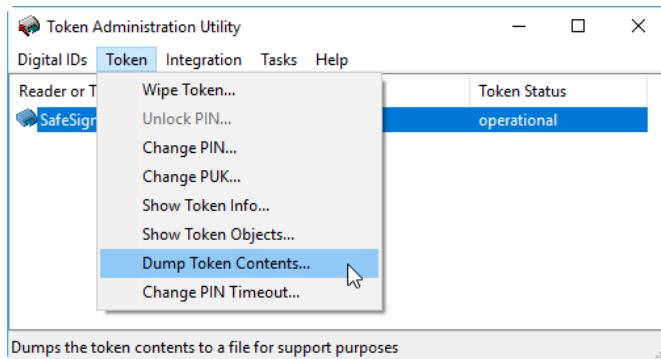


Figure 127: TAU: Dump Token Contents

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

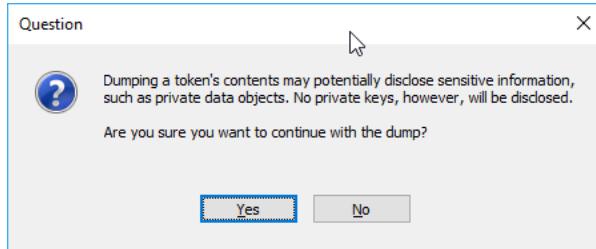


Figure 128: Dump token contents: Question

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

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

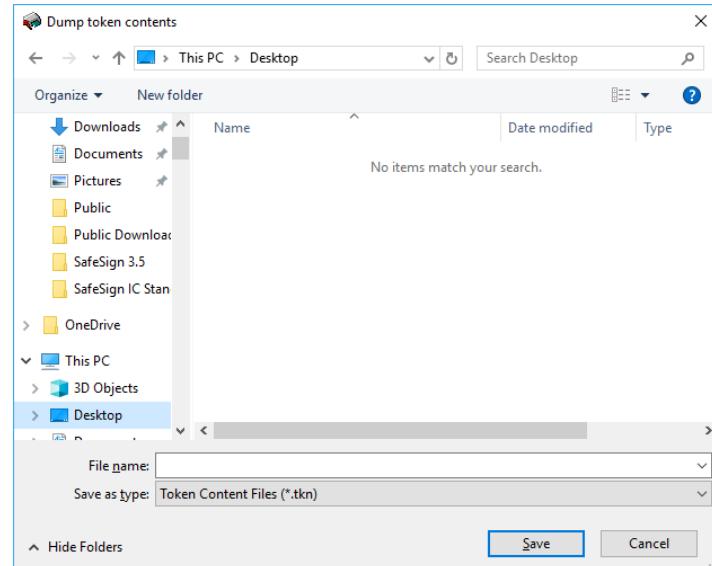


Figure 129: Dump Token Contents: Save

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



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

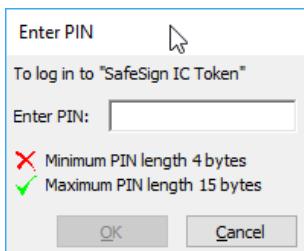


Figure 130: Enter PIN

- 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:

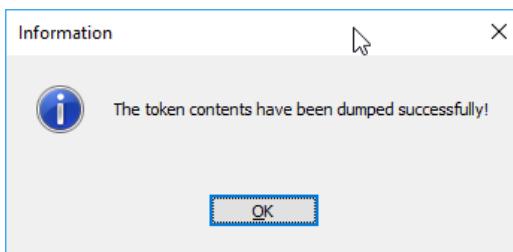


Figure 131: Dump Token Contents: Information

- Click **OK**

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

### 8.3 Show PUK retry counter

From SafeSign IC Standard and Minidriver version 3.5 onwards, 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:

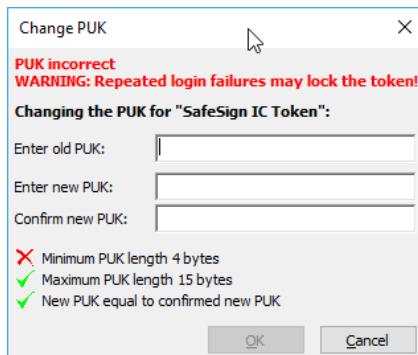


Figure 132: Change PUK



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:

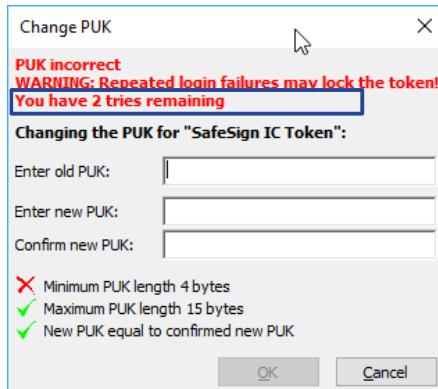


Figure 133: Change PUK with retry counter