SafeSign Identity Client Standard

User Guide Token Utility

A.E.T. Europe B.V.
IJsselburcht 3
NL - 6825 BS Arnhem
The Netherlands

Warning Notice

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

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

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

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

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

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

SafeSign Identity Client 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).

Contact Information: A.E.T. Europe B.V.

*IJsselburcht 3
NL-6825 BS
P.O. Box 5486
NL-6802 EL Arnhem
The Netherlands*

Tel.	*+31-26-365 33 50*
Tel. Support	*+31-26-365 35 43*
Fax	*+31-26-365 33 51*

*info@aeteurope.nl /
safesignsupport@aeteurope.nl
http://www.aeteurope.com/*

SafeSign Identity Client is a product developed by A.E.T. Europe B.V.

Document Information

Filename: **SafeSign Identity Client Standard**
User Guide Token Utility

Document ID: **TU_Guide_SafeSign-IC-Standard_v1.1**

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

Document revision history

Version	**Date**	**Author**	**Changes**
1.0	14-05-2013	Drs C.M. van Houten	First edition for SafeSign Identity Client Standard Version 3.0 for Windows (release 3.0.87 / 3.0.87-x64)
1.1	15-07-2013	Drs C.M. van Houten	First edition for SafeSign Identity Client Standard Version 3.0 for Windows (release 3.0.88 / 3.0.88-x64)

WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE

Table of Contents

Table of Contents Token Management Utility

List of Figures

About the Product

SafeSign Identity Client is a software package that can be used to enhance the security of applications that support hardware tokens through PKCS #11 and Microsoft CryptoAPI.

The SafeSign Identity Client package provides a standards-based PKCS #11 Library as well as a Cryptographic Service Provider (CSP) and CNG Key Storage Provider (KSP) allowing users to store public and private data on a personal token, either a smart card, USB token or SIM card. It also includes the SafeSign Identity Client PKI applet, enabling end-users to utilise any Java Card 2.1.1 / Java Card 2.2 and higher compliant card with the SafeSign Identity Client middleware.

Combining full compliance with leading industry standards and protocols, with flexibility and usability, SafeSign Identity Client can be used with multiple smart cards / USB tokens, multiple Operating Systems and multiple smart card readers.

SafeSign Identity Client allows users to initialise and use the token for encryption, authentication or digital signatures and includes all functionality necessary to use hardware tokens in a variety of PKI environments.

SafeSign Identity Client comes in a standard version with an installer for the following Windows environments (with the latest Service Packs)[1]:

Windows XP (Professional), Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008 and Windows Server 2012[2].

Note that SafeSign Identity Client supports virtualization type I (or native, bare-metal hypervisors), i.e. SafeSign Identity Client installed on servers/desktops which run for example on VMware ESX or Citrix XenDesktop or Oracle/Sun VM VirtualBox directly on bare-metal hypervisors. Virtualization Type II (or hosted hypervisors), such as VMware Workstation, is not supported.

For more information, refer to the latest SafeSign Identity Client Product Description.

[1] Windows NT 4.0 is supported up to SafeSign Identity Client 1.0.9.04, in line with Microsoft's end-of-life policy.
Windows 98 and Windows ME are supported up to SafeSign Identity Client 2.3.0 (< 2.3.0), in line with Microsoft's end-of-life policy.
Windows 2000 is supported up to SafeSign Identity Client 3.0.33 (≤ 3.0.33), in line with Microsoft's end-of-life policy.

[2] Windows Server 2012 runs only on x64 processors.

About the Manual

This manual is specifically designed for administrators / advanced users of SafeSign Identity Client Standard Version 3.0.88 / 3.088-x64 for Windows, who wish to use their SafeSign Identity Client token to enhance the security of their communications via the Internet and be able to perform advanced token operations.

It describes the functionality provided by the SafeSign Identity Client Token Utility, which enable you to perform such operations as token initialisation, in order to prepare your token for key pair generation and certificate download. Please refer to the SafeSign Identity Client Application User Guides or your application's documentation to find out how to generate a key pair and download a certificate onto your SafeSign Identity Client token and how to use it to enhance the security of your client application.

In order to set up your SafeSign Identity Client token for use, follow the instructions in the manual, which describe how to initialise your token and perform various operations such as viewing the contents of your token and changing its PIN.

Every activity has a number of steps, indicated by the numbers at the left-hand side of the text: **1**

Each step will require you to take a certain action, which is indicated by a: ➔

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

taking into account the notes in **black** with: ✎ and the larger ones in **blue** with: 💡

This document is part of the user documentation for SafeSign Identity Client.

1 SafeSign Identity Client Token Utility

1.1 Introduction

SafeSign Identity Client provides a standards-based PKCS #11 and Microsoft CryptoAPI (NG) implementation (Cryptographic Service Provider and Key Storage Provider), fully compliant with leading industry standards and protocols, while being so flexible that it can be used with multiple smart cards / USB tokens, multiple Operating Systems and multiple smart card readers. Basically any application that either supports PKCS #11 and/or CSP (NG) to work with tokens on any of the supported platforms can make use of the benefits and features of SafeSign Identity Client.

In order to make your SafeSign Identity Client token work with SafeSign Identity Client in PKCS #11-supporting applications such as Mozilla Firefox, and in Microsoft CryptoAPI-supporting applications such as Outlook, you need to initialise and manage your SafeSign Identity Client token. This can be done with the SafeSign Identity Client Token Utility included in SafeSign Identity Client.

SafeSign Identity Client comes in two different versions: for users and administrators. Both packages are functionally identical, but the administrator package includes the Token Administration Utility (TAU) and the user version includes the Token Management Utility (TMU).

Although the Token Administration Utility has been specifically designed for administrators, allowing them to perform advanced token operations, it includes the same basic functionality as the Token Management Utility for end-users, i.e. it enables you to personalise and manage your token to be part of your secure applications.

To personalise your token, you will need to initialise it, which (may) involve(s) deleting all information that may be stored on the token, writing the SafeSign Identity Client PKCS #15 structure on the token and (after changing the token transport PIN, if set) setting a label and personal PIN.

1.2 Menu items

Both the Token Management Utility (TMU) and the Token Administration Utility (TAU) offer four menu items:

1. **Digital IDs**, including such features as viewing and importing your Digital IDs and CA certificates;
2. **Token**, including such features as initialising your token and changing its PIN;
3. **Integration**, allowing you to install SafeSign (PKCS#11) in Firefox and Entrust;
4. **Help**

In addition, the Token Administration Utility includes the menu option:

5. **Tasks** menu, allowing you to manage tasks;

Note

The actual menu items visible / available can be configured in the registry. For more details, see the SafeSign Identity Client Administrator's Guide.

Note that you may not always need to initialise your token yourself, as your token may have been provided to you pre-initialised and with a useable Digital ID on it already.

The following chapters will give a description of the various features of the SafeSign Identity Client Token Utility, besides that of token initialisation.

1.2.1 Help menu

This chapter 1 will briefly describe the following:

Section 1.3	:	Where to find and how to start the SafeSign Identity Client Token Utility
Section 1.4	:	Version information (the **Help** menu of the SafeSign Identity Client Token Utility)
Section 1.5	:	The unique multi-language feature of SafeSign Identity Client
Section 1.6	:	The use of secure Class 2/3 PIN pad readers

1.2.2 Digital IDs menu

Chapter 2 will deal with the **Digital IDs** menu of the Token Utility:

Section 2.1	:	Show Registered Digital IDs
Section 2.2	:	Import Digital IDs
Section 2.3	:	Import Certificate
Section 2.4	:	Exit

1.2.3 Token menu

Chapter 3 will deal with the **Token** menu of the Token Utility, where the following sections apply to both the Token Management Utility and Token Administration Utility:

Section 3.1	:	Initialise Token
Section 3.2	:	Change PIN
Section 3.3	:	Change Transport PIN
Section 3.4	:	Unlock PIN
Section 3.5	:	Change PUK
Section 3.6	:	Show Token Info

and the following sections to the Token Administration Utility only:

Section 3.7	:	Show Token Objects
Section 3.8	:	Dump Token Contents
Section 3.9	:	Query Unknown Token
Section 3.10	:	Analyse Certificate Quality
Section 3.11	:	Change PIN Timeout

1.2.4 Integration menu

Chapter 4 will deal with the **Integration** menu of the Token Utility

1.2.5 Tasks menu

Chapter 5 will deal with the **Tasks** menu of the Token Administration Utility

Note

On page V, users of the Token Management Utility will find a Table of Contents referring to those sections that apply to the Token Management Utility (only).

Note that the screenshots in this guide were taken from a computer running (32-bit) Windows 8 with the SafeSign Identity Client administrator package (with TAU) installed.

1.3 Readers and Tokens

You will find the SafeSign Identity Client Token Utility in the Programs menu (**Start > All Programs > SafeSign Standard > Token Administration** or **Start > All Programs > SafeSign Standard > Token Management**).

In Windows 8, by pinning it to the Start window, the Token Utility can be made available as a desktop app:

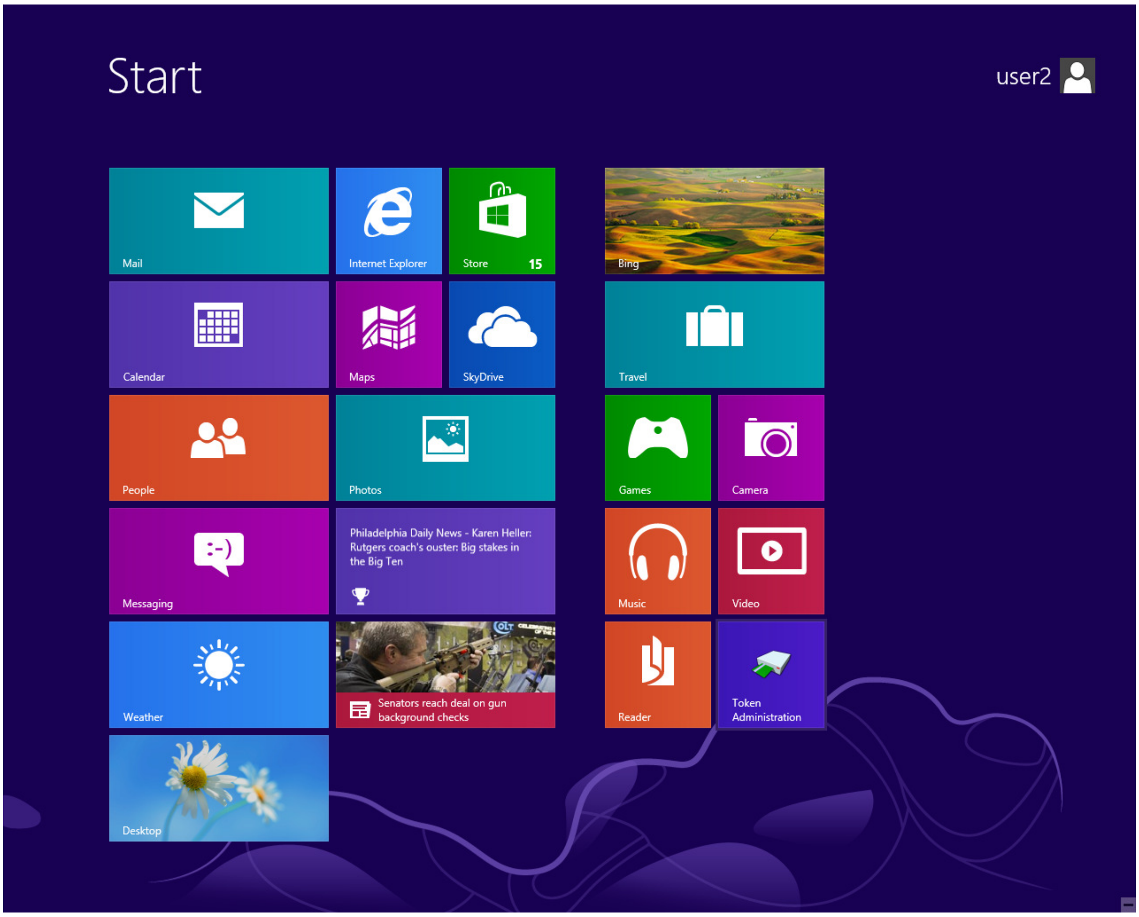
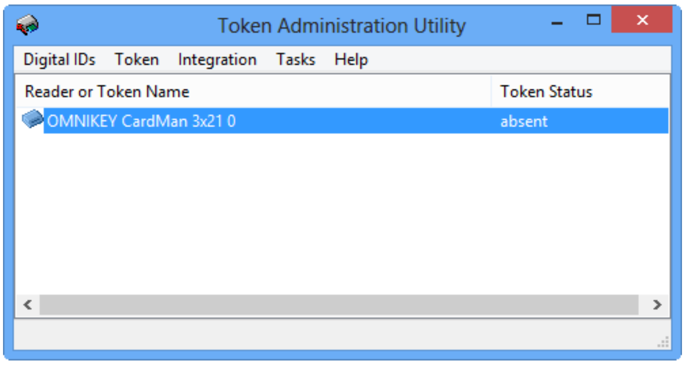


Figure 1: Windows 8 Start

Note

In Windows XP and higher there will also be a shortcut to the SafeSign Identity Client Token Administration Utility in the Control Panel, called Cryptographic Tokens. In Windows 7 and Windows 8, this shortcut is available when viewing all Control Panel items (not in Category view).

Upon clicking **Token Administration / Token Management**, the SafeSign Identity Client Token Utility will open:



Reader or Token Name	Token Status
OMNIKEY CardMan 3x21 0	absent

Figure 2: Token Utility: Reader Name

This window shows you which smart card reader(s) have been 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).

When no smart card reader is displayed, you will need to verify whether a smart card reader is installed and whether it is functioning properly. Without a functional smart card reader (and related services), SafeSign Identity Client cannot be used.

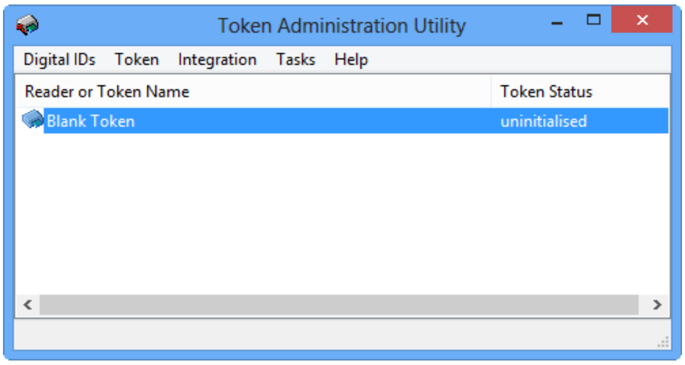
All smart card readers that are installed will be listed and allow you to initialise a token.

Note

In this manual, 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 is inserted in the smart card reader, the name of the token is displayed. In this case, there are two possibilities[1]:

Either the token is blank, not yet initialised:

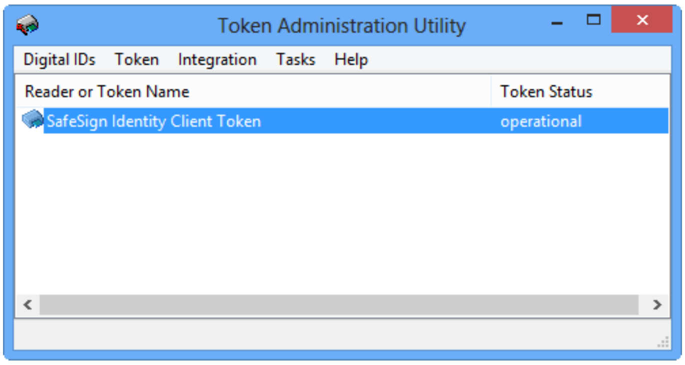


Reader or Token Name	Token Status
Blank Token	uninitialised

Figure 3: Token Utility: uninitialised Token

[1] If the token is supported and recognised. If this is not the case, your token may be identified as an unknown token (see section 3.9).

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



Reader or Token Name	Token Status
SafeSign Identity Client Token	operational

Figure 4: Token Utility: operational Token

Multiple tokens and readers

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

You may have multiple cards / tokens, e.g. one used for your personal e-mail, and the other used for your business e-mail. Both can be present on one computer, in separate readers, and you can use the features of the SafeSign Identity Client Token Utility for each of these cards / tokens.

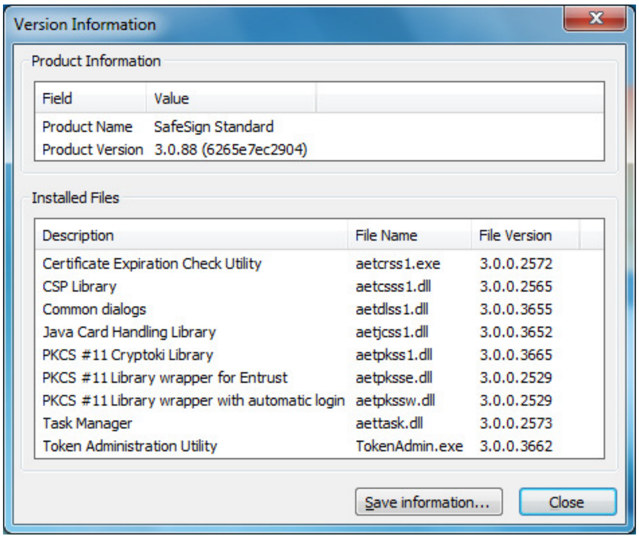
When there is one token in the reader, the Token Utility will automatically select this (highlighting it in **blue**). When there are two (or more) tokens in the readers, the last one inserted will be selected. You will need to select one of the tokens to perform such operations as *Change PIN* from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

1.4 Version Information

The **Help** menu of the SafeSign Identity Client Token Utility features two items: *Versions Info* and *About*.

1.4.1 Versions Info

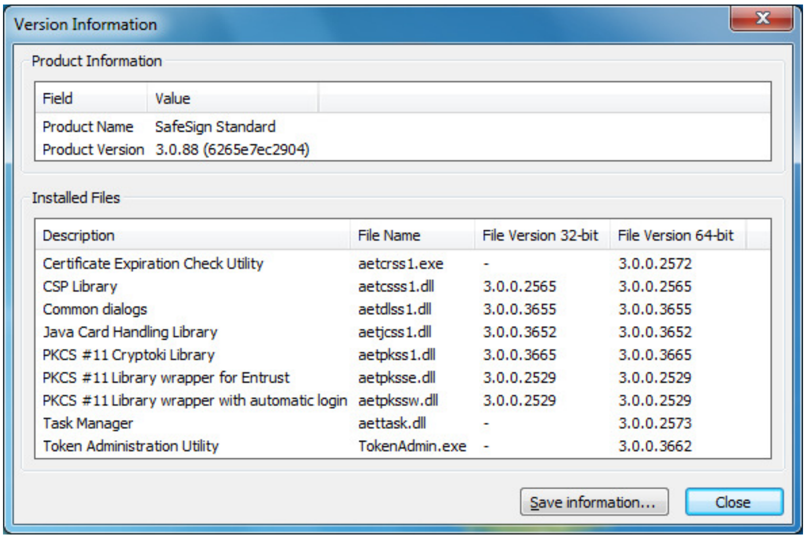
The Versions Info item opens the *Version Information* dialog:



Field	Value
Product Name	SafeSign Standard
Product Version	3.0.88 (6265e7ec2904)

Description	File Name	File Version
Certificate Expiration Check Utility	aetcrss1.exe	3.0.0.2572
CSP Library	aetcsss1.dll	3.0.0.2565
Common dialogs	aetdlss1.dll	3.0.0.3655
Java Card Handling Library	aetjcss1.dll	3.0.0.3652
PKCS #11 Cryptoki Library	aetpkss1.dll	3.0.0.3665
PKCS #11 Library wrapper for Entrust	aetpksse.dll	3.0.0.2529
PKCS #11 Library wrapper with automatic login	aetpkssw.dll	3.0.0.2529
Task Manager	aettask.dll	3.0.0.2573
Token Administration Utility	TokenAdmin.exe	3.0.0.3662

Figure 5: Token Utility: Version Information x86



Product Information

Field	Value
Product Name	SafeSign Standard
Product Version	3.0.88 (6265e7ec2904)

Installed Files

Description	File Name	File Version 32-bit	File Version 64-bit
Certificate Expiration Check Utility	aetcrss1.exe	-	3.0.0.2572
CSP Library	aetcsss1.dll	3.0.0.2565	3.0.0.2565
Common dialogs	aetdlss1.dll	3.0.0.3655	3.0.0.3655
Java Card Handling Library	aetjcss1.dll	3.0.0.3652	3.0.0.3652
PKCS #11 Cryptoki Library	aetpkss1.dll	3.0.0.3665	3.0.0.3665
PKCS #11 Library wrapper for Entrust	aetpksse.dll	3.0.0.2529	3.0.0.2529
PKCS #11 Library wrapper with automatic login	aetpkssw.dll	3.0.0.2529	3.0.0.2529
Task Manager	aettask.dll	-	3.0.0.2573
Token Administration Utility	TokenAdmin.exe	-	3.0.0.3662

Figure 6: Token Utility: Version Information x64

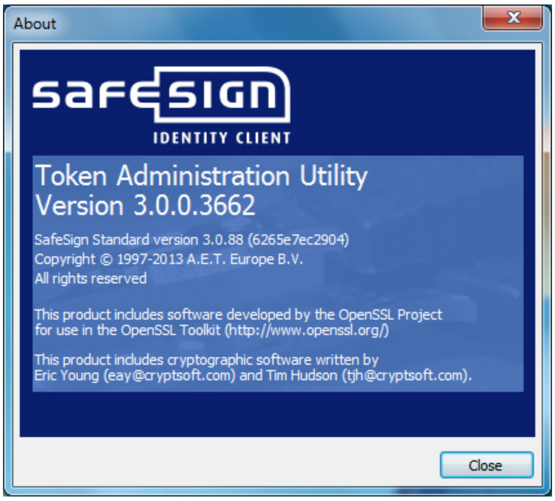
This will inform you of the version of SafeSign Identity Client you are running and the file versions of the components installed by your SafeSign Identity Client version.

This dialog is particularly useful for support issues, enabling AET SafeSign Support to quickly identify the version you are running.

For that purpose, you can also 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.

1.4.2 About

The *About* item opens the following dialog:



Token Administration Utility
Version 3.0.0.3662

SafeSign Standard version 3.0.88 (6265e7ec2904)
Copyright © 1997-2013 A.E.T. Europe B.V.
All rights reserved

This product includes software developed by the OpenSSL Project
for use in the OpenSSL Toolkit (http://www.openssl.org/)

This product includes cryptographic software written by
Eric Young (eay@cryptsoft.com) and Tim Hudson (tjh@cryptsoft.com).

Figure 7: Token Utility: About

1.5 Multi-language

Multi-language support has been implemented such, to create utmost flexibility for both administrator and user. This is shown by the fact that that the language of the InstallShield Wizard on the one hand and the Token Utility on the other hand, are separate.

For example, it may be imagined that an administrator, and not the user himself / herself, is installing SafeSign Identity Client (on a user PC or on a central PC) and that he chooses a particular language to do so in.

The language of the then installed SafeSign Identity Client (Token Utility and dialogs) may not be the same language, as it will default to the language set in the Region and Language settings of the user's computer, without the need for the user to change any settings. The user will then always be free to change the preferred language of SafeSign Identity Client.

Note

The language of the InstallShield Wizard and the SafeSign Identity Client items in the Start menu, though this language can be selected upon installation of SafeSign Identity Client, is static and cannot be changed once selected (without de-installing SafeSign Identity Client) due to limitations of Windows. The language of SafeSign Identity Client and its utilities is dynamic and can be changed to any of the languages supported.

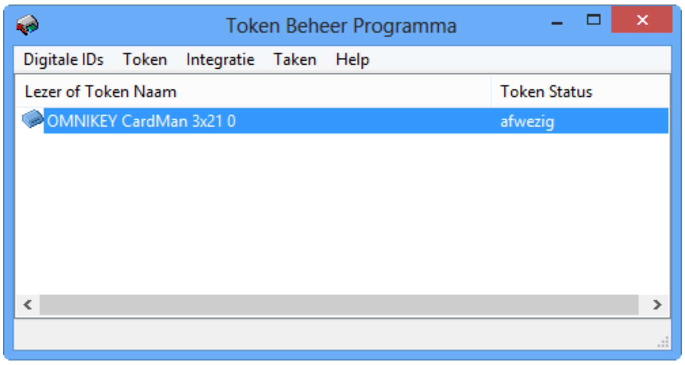
SafeSign Identity Client Standard Version 3.0.88 for Windows contains support for the following languages (apart from the default language, English):

- Basque
- Catalan
- Chinese: Simplified
- Chinese: Traditional
- Croatian
- Czech
- Dutch
- Finnish
- German
- Hungarian
- Italian
- Japanese
- Korean
- Lithuanian
- Portuguese: Portugal
- Portuguese: Brazil
- Russian
- Serbian (Latin and Cyrillic)
- Spanish
- Thai
- Turkish
- Ukrainian

Note

Editing of the language files is not allowed under any circumstances. Doing so, will forfeit any rights to support and will make all warranties void. Only upon formal request and after written approval from A.E.T. Europe B.V. may such editing be allowed, where modifications suggested are deemed to improve or facilitate the use and understanding of SafeSign Identity Client and its operations. A.E.T. Europe B.V. will maintain sole discretion in deciding to allow editing and the right to include it in (a) future release(s).

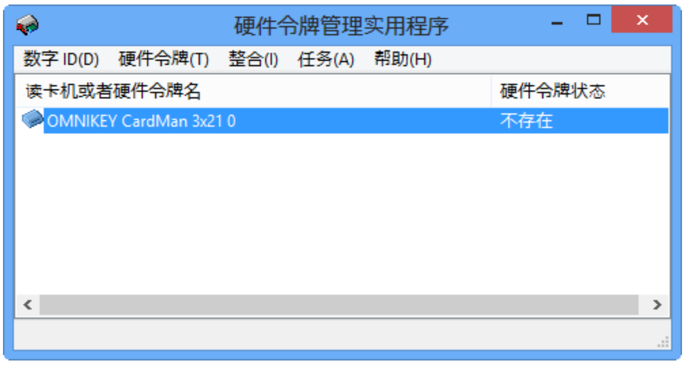
Here is an example of how the Token Utility looks in Dutch:



Lezer of Token Naam	Token Status
OMNIKEY CardMan 3x21 0	afwezig

Figure 8: Token Utility: Dutch

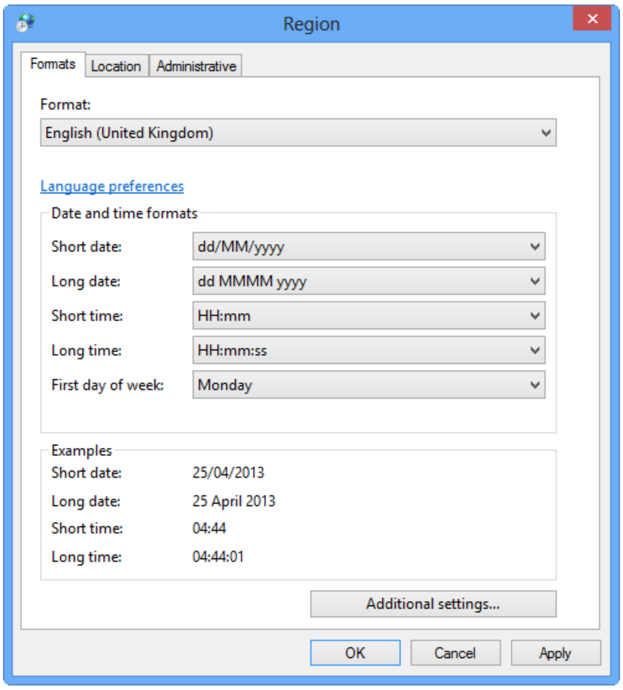
Here is an example of how the Token Utility looks in Chinese (PRC):



读卡机或者硬件令牌名	硬件令牌状态
OMNIKEY CardMan 3x21 0	不存在

Figure 9: Token Utility: Chinese

The user can set the language of the Token Utility to the language he prefers to work with, in **Region** under **Start > Control Panel** by setting the Format to the preferred language:



Format: English (United Kingdom)

Date and time formats

Short date: dd/MM/yyyy

Long date: dd MMMM yyyy

Short time: HH:mm

Long time: HH:mm:ss

First day of week: Monday

Examples

Short date: 25/04/2013

Long date: 25 April 2013

Short time: 04:44

Long time: 04:44:01

Figure 10: Region: Format

In order to set the system locale (for non-Unicode programs) that will apply to all users logging on, you need to set / change the system locale (in the tab **Administrative**).

Note that when no specific language is set or when the selected language is not supported by SafeSign Identity Client, the default language of SafeSign Identity Client will be English.

You may also need to select the input language / keyboard layout combination.

Note that though SafeSign Identity Client 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, such as Microsoft VPN, SafeSign Identity Client cannot influence the language of the Windows VPN dialogs. Microsoft VPN dialogs will appear in the language of the Operating System installed.

1.6 Use of protected authentication path devices

1.6.1 Secure pinpad reader

SafeSign Identity Client supports a number of Class 2 and Class 3 PC/SC 2.01 pinpad readers. Please refer to the latest *SafeSign Identity Client Product Description* for a full overview.

When using a secure pinpad, please note the following important guidelines:

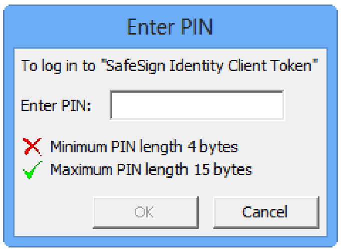
- In the Token Utility, all functions apart from **Initialise Token** and **Change PUK** have been "pinpad-enabled"[1].
- When using a secure pinpad reader with a display (Class 3), no PIN dialog will appear on-screen, but on the reader's display. When using a secure pinpad reader without a display (Class 2), a PIN dialog will appear on-screen. For both readers, you should enter the PIN on your reader's pinpad.
- In Mozilla Firefox and Thunderbird the *Password Required* dialog will appear, asking you for the 'master password' of your token. Do not enter the PIN on your computer's keyboard, but click **OK** and then enter the PIN on the reader's pinpad.
- For smart card logon with Class 2 secure pinpad readers on Windows XP, whether you have installed the SafeSign Identity Client GINA or not, the *PinPad* dialog (Figure 12) will appear.
- Note that on Windows Vista and higher, the Microsoft GINA (msgina.dll) has been removed, and custom GINAs will not be loaded. For those Operating Systems, the SafeSign Credential Provider is available, as of SafeSign Identity Client version 3.0.40 (≥ 3.0.40).
- For Microsoft VPN, the *Connect [Name of Virtual Private Connection]* dialog ("Smart card PIN") will appear upon inserting a token in the reader. Do not enter the PIN on your computer's keyboard, but click **OK** and then enter the PIN on the reader's pinpad.
- If you enter a wrong PIN, either the display of the reader will indicate this, or the SafeSign Identity Client Token Utility will display a wrong PIN error on screen. Note that upon entering an incorrect PIN in an application (for example Internet Explorer), the PIN dialog will not indicate this or allow you to enter a correct PIN. This is due to the fact that for so-called protected authentication path authentication (as with the use of a pinpad reader) the verification of the PIN is outside of the control of the CSP.

For other possible issues, refer to the latest *SafeSign Identity Client Release Notes*.

[1] The reason for this being that it cannot be communicated to the end user which code an end user must enter during initialisation. If implemented, a secure pinpad reader would just prompt the user to enter a code for about 6 times in total, without the ability to distinguish / indicate the PIN or PUK is requested.

PIN entry

In accordance with the above, in this manual and any other SafeSign Identity Client manuals, where the entry of a PIN is required, for example in the *Enter PIN* dialog in the Token Utility or applications:



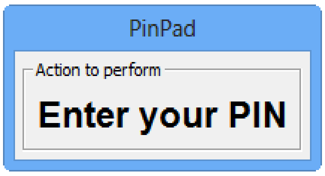
To log in to "SafeSign Identity Client Token"

Enter PIN:

✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes

Figure 11: Enter PIN

This may also refer to the entry of a PIN on the pinpad reader's keypad, either instructed by the reader's display (Class 3 secure pinpad reader) or by an on-screen dialog (Class 2 secure pinpad reader), which looks like this:



Enter your PIN

Figure 12: PinPad: Enter your PIN

Note that this dialog does not give you any information on the minimum PIN and PUK length, nor on the number of retries remaining (when you have entered an incorrect PIN), as this dialog only provides what information the reader (driver) provides.

Note also that SafeSign Identity Client 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[1]. Only when you enter a PIN / PUK of the required length will the PIN / PUK be accepted. Note that both the minimum and the maximum PIN / PUK length may have been set to different values (than the default values supported by the card) by the administrator.

[1] When the maximum PUK / PIN length exceeds the maximum length required, the **OK** button will be greyed out.

2 Digital IDs menu

The **Digital IDs** menu in both the Token Management Utility and the Token Administration Utility includes the following functionality:

Section 2.1 : Show Registered Digital IDs
Section 2.2 : Import Digital ID
Section 2.3 : Import Certificate
Section 2.4 : Exit

2.1 Show Registered Digital IDs

The SafeSign Identity Client Token Utility allows users to identify the Digital IDs on the token. The term Digital ID signifies a key pair (private and public key) and a certificate, which can be used for such operations as signing and decrypting.

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

When there are no Digital IDs, the Digital IDs dialog (Digital IDs > Show Registered Digital IDs) will be empty and look like this:

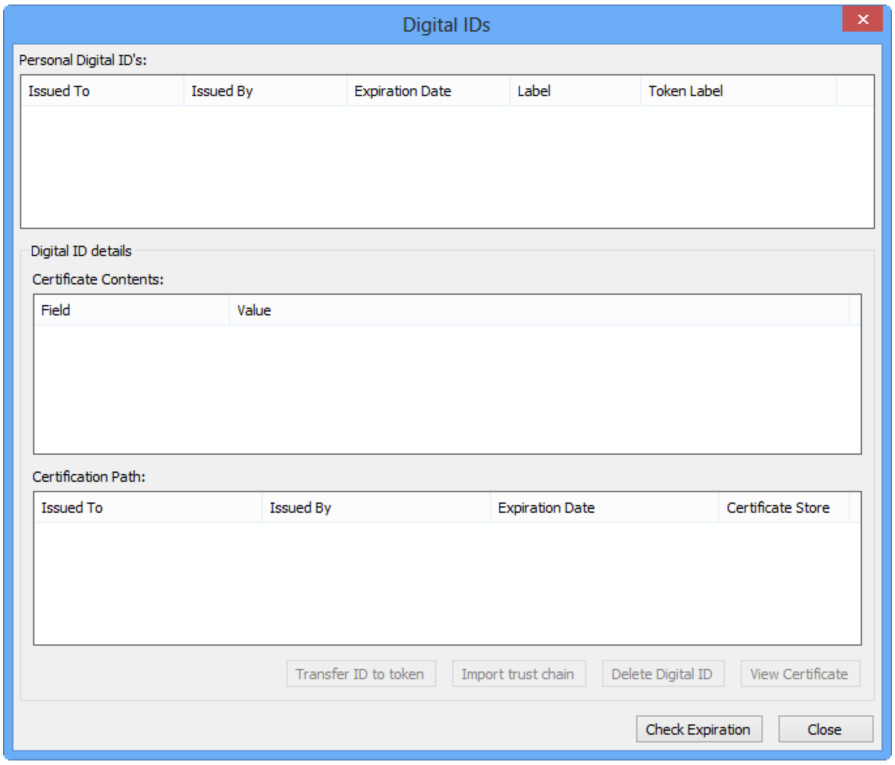
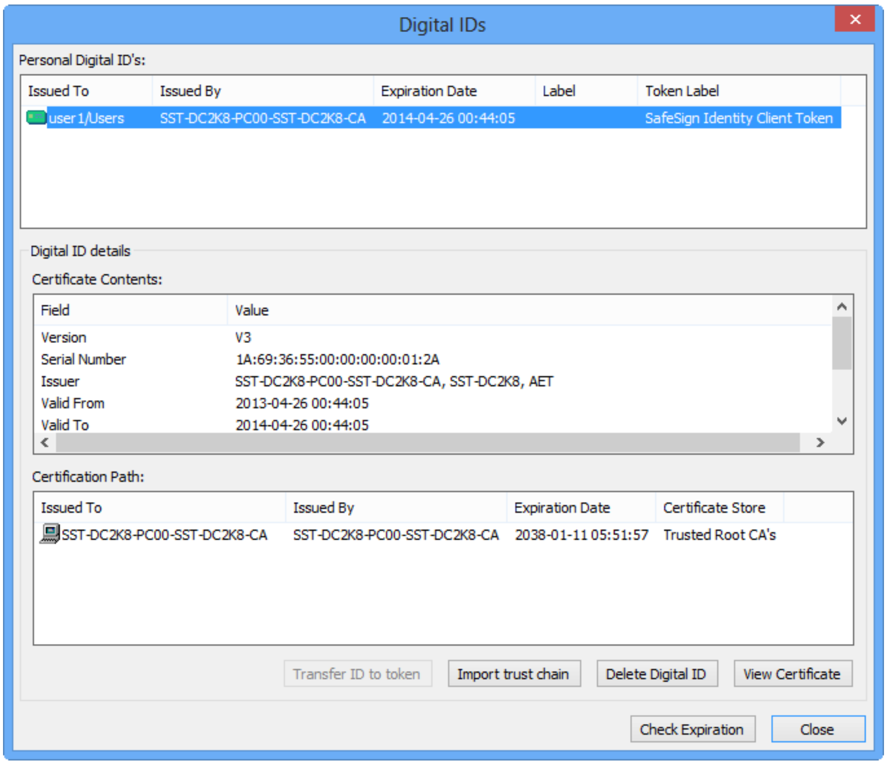


Figure 13: Digital IDs: No personal Digital IDs

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



Personal Digital ID's:

Issued To	Issued By	Expiration Date	Label	Token Label
🟩 user1/Users	SST-DC2K8-PC00-SST-DC2K8-CA	2014-04-26 00:44:05		SafeSign Identity Client Token

Digital ID details

Certificate Contents:

Field	Value
Version	V3
Serial Number	1A:69:36:55:00:00:00:00:01:2A
Issuer	SST-DC2K8-PC00-SST-DC2K8-CA, SST-DC2K8, AET
Valid From	2013-04-26 00:44:05
Valid To	2014-04-26 00:44:05

Certification Path:

Issued To	Issued By	Expiration Date	Certificate Store
🖥 SST-DC2K8-PC00-SST-DC2K8-CA	SST-DC2K8-PC00-SST-DC2K8-CA	2038-01-11 05:51:57	Trusted Root CA's

Figure 14: Digital IDs: Personal Digital ID stored on token

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

When a Digital ID (displayed under **Personal Digital ID's**) or CA certificate (displayed under **Certification Path**) is on token, this will be identified by the following symbol: 🟩

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

Certificate Registration

In SafeSign Identity Client versions up to 3.0.45 (< 3.0.45), certificate registration and de-registration was performed by the SafeSign Identity Client Store Provider. However, as a result of changed functionality in Windows Vista and higher, changes have been made to the way certificates are registered / propagated. Certificates are now registered by the appropriate Microsoft services and processes, i.e. through the Microsoft Certificate Propagation service[1].

The Microsoft Certificate Propagation Service does not deregister certificates upon token removal, therefore when the token is removed, the certificates will remain visible in the certificate store (though they will not be usable without key pair).

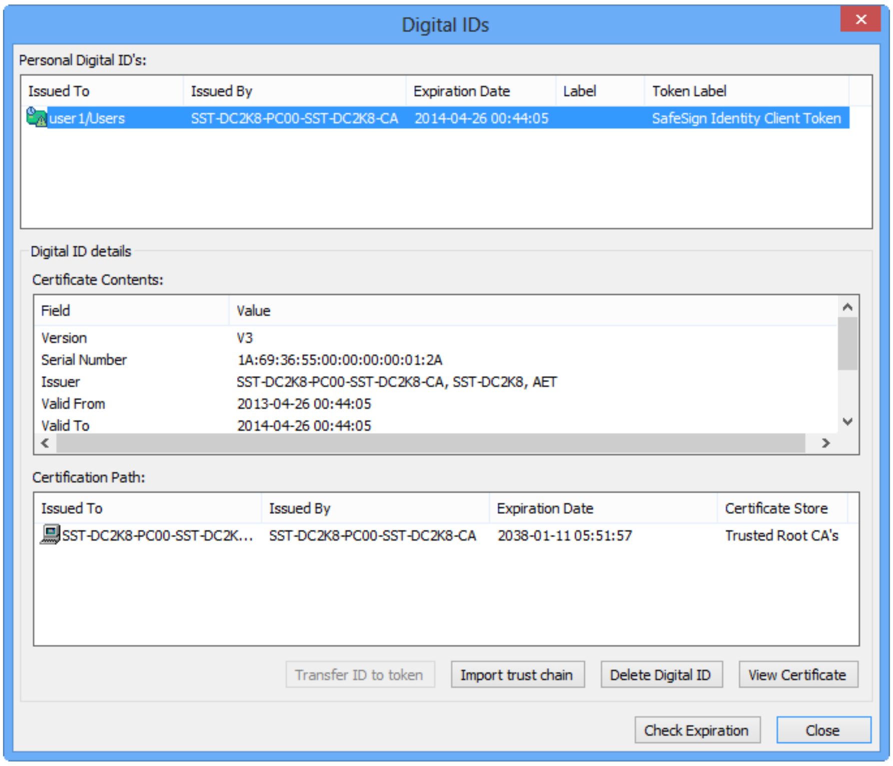
Consequently, the computer icon in the *Digital IDs* dialog may refer to either a certificate on a token that has been removed or a certificate on the local hard disk, both of which have been registered in the Microsoft personal Certificate Store.

[1] In Windows XP, the Windows Smart Card Service takes care of certificate registration as part of winlogon.exe.

The *Digital IDs* dialog will also indicate if a certificate is about to expire or already expired.

In this case, the symbol indicating a Digital ID is on the token: 🟩 is replaced by
the symbol indicating the certificate is about to expire: ⚠
or the symbol indicating the certificate is expired: 🟥

When a certificate is about to expire, the *Digital IDs* dialog will look like this:



Issued To	Issued By	Expiration Date	Label	Token Label
user 1/Users	SST-DC2K8-PC00-SST-DC2K8-CA	2014-04-26 00:44:05		SafeSign Identity Client Token

Field	Value
Version	V3
Serial Number	1A:69:36:55:00:00:00:00:01:2A
Issuer	SST-DC2K8-PC00-SST-DC2K8-CA, SST-DC2K8, AET
Valid From	2013-04-26 00:44:05
Valid To	2014-04-26 00:44:05

Issued To	Issued By	Expiration Date	Certificate Store
SST-DC2K8-PC00-SST-DC2K...	SST-DC2K8-PC00-SST-DC2K8-CA	2038-01-11 05:51:57	Trusted Root CA's

Figure 15: Digital IDs: Personal Digital ID about to expire

For more information regarding certificate expiration, refer to section 2.1.5.

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 2.1.1	:	Transfer ID to token
Section 2.1.2	:	Import trust chain
Section 2.1.3	:	Delete Digital ID
Section 2.1.4	:	View Certificate
Section 2.1.5	:	Check Expiration
Section 2.1.6	:	Close

2.1.1 Transfer ID to token

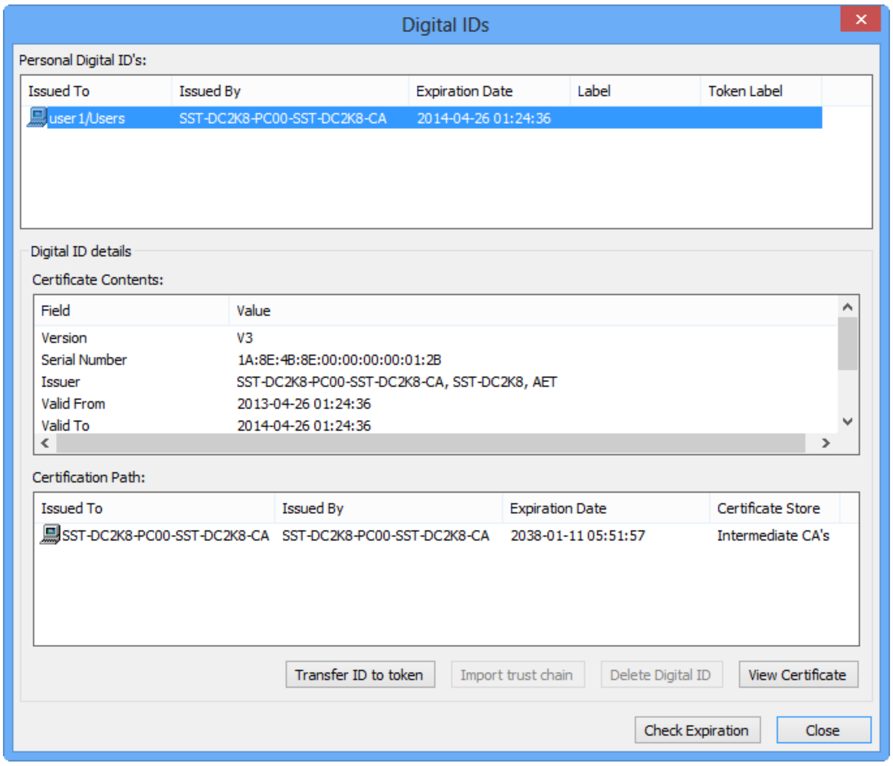
It is possible to transfer (move) a Digital ID to a token, for example when you have a personal certificate (with a private key corresponding to this certificate) in the Microsoft Certificate Store[1]. When transferring a Digital ID to the token, the private key will be moved to the token and will no 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;
2. You can only transfer the Digital ID when the private key is (marked as) exportable, which may depend on the certificate template[2], otherwise you will get an error (see **Private key non-exportable**).

When a Digital ID (in **Personal Digital ID's**) is not on token (but in the Microsoft Certificate Store), this will be identified by the symbol: 💻

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



Personal Digital ID's:

Issued To	Issued By	Expiration Date	Label	Token Label
💻 user1/Users	SST-DC2K8-PC00-SST-DC2K8-CA	2014-04-26 01:24:36		

Digital ID details

Certificate Contents:

Field	Value
Version	V3
Serial Number	1A:8E:4B:8E:00:00:00:00:01:2B
Issuer	SST-DC2K8-PC00-SST-DC2K8-CA, SST-DC2K8, AET
Valid From	2013-04-26 01:24:36
Valid To	2014-04-26 01:24:36

Certification Path:

Issued To	Issued By	Expiration Date	Certificate Store
💻 SST-DC2K8-PC00-SST-DC2K8-CA	SST-DC2K8-PC00-SST-DC2K8-CA	2038-01-11 05:51:57	Intermediate CA's

Figure 16: Digital IDs: Transfer ID to token

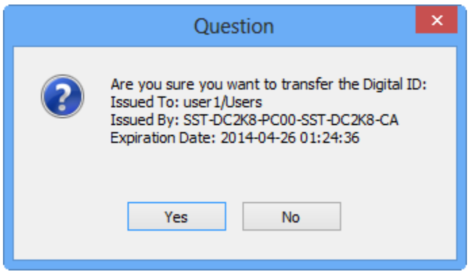
➔ Click **Transfer ID to token** to move the Digital ID from its original location to the token

[1] For example, when you have requested a certificate through the Microsoft Enhanced Cryptographic Service Provider.

[2] On Windows Server 2003, it is not possible to mark the private key as exportable for the Smart Card User template, when the certificate purpose is "signature and smartcard logon".

2

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



Question

Are you sure you want to transfer the Digital ID:
Issued To: user1/Users
Issued By: SST-DC2K8-PC00-SST-DC2K8-CA
Expiration Date: 2014-04-26 01:24:36

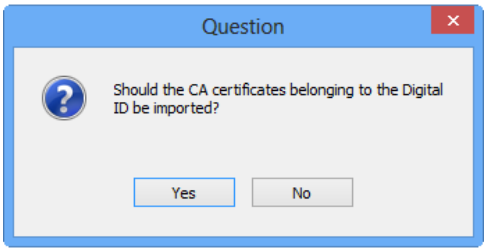
Figure 17: Transfer ID to token: Are you sure you want to transfer the Digital ID

➔ 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:



Question

Should the CA certificates belonging to the Digital ID be imported?

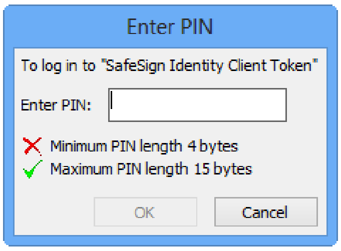
Figure 18: Transfer ID to token: Should the CA certificates belonging to the Digital ID be imported

➔ 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:



Enter PIN

To log in to "SafeSign Identity Client Token"

Enter PIN:

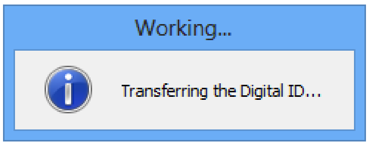
☒ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes

Figure 19: Transfer ID to token: Enter PIN

➔ Enter the correct PIN for the token and click **OK**

5

The Digital ID will now be transferred:

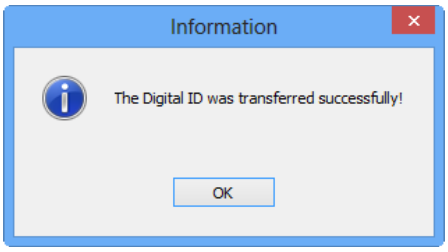


Working...

Transferring the Digital ID...

Figure 20: Transfer ID to token: Transferring the Digital ID

6 When the Digital ID has been successfully transferred to the token, you will be notified:



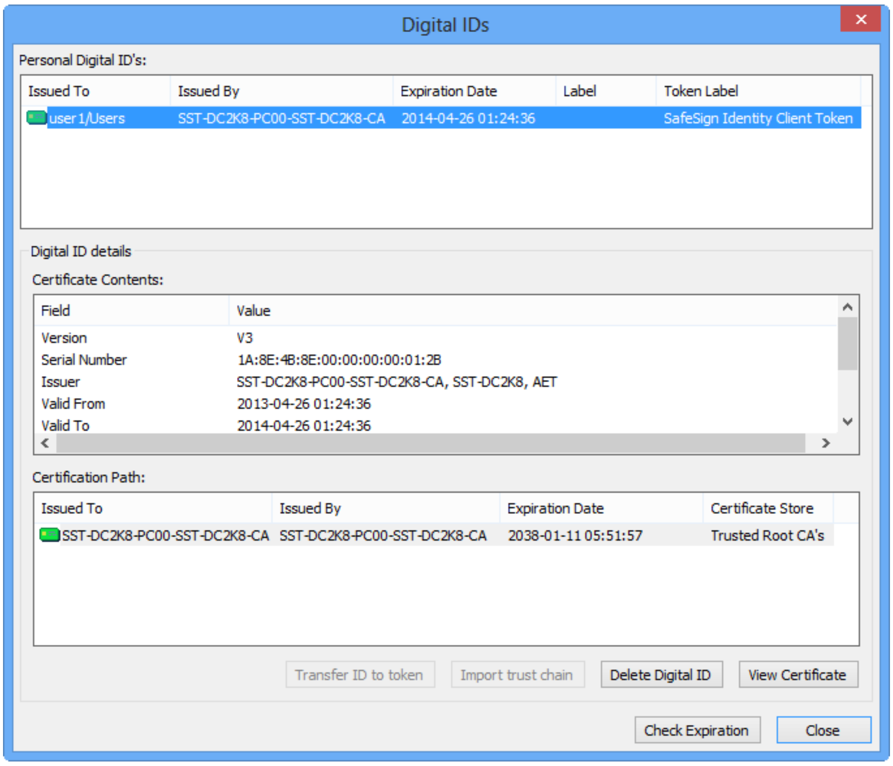
Information

The Digital ID was transferred successfully!

Figure 21: Transfer ID to token: The Digital ID was transferred successfully

➔ Click **OK**

The Digital ID will now be on the token:



Digital IDs

Personal Digital ID's:

Issued To	Issued By	Expiration Date	Label	Token Label
user1/Users	SST-DC2K8-PC00-SST-DC2K8-CA	2014-04-26 01:24:36		SafeSign Identity Client Token

Digital ID details

Certificate Contents:

Field	Value
Version	V3
Serial Number	1A:8E:4B:8E:00:00:00:00:01:2B
Issuer	SST-DC2K8-PC00-SST-DC2K8-CA, SST-DC2K8, AET
Valid From	2013-04-26 01:24:36
Valid To	2014-04-26 01:24:36

Certification Path:

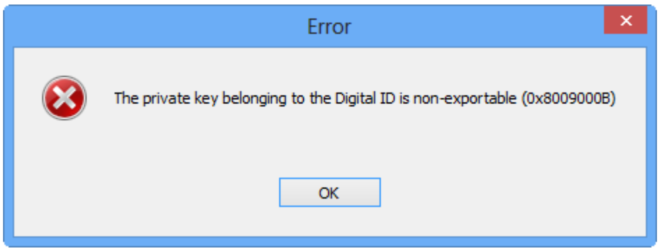
Issued To	Issued By	Expiration Date	Certificate Store
SST-DC2K8-PC00-SST-DC2K8-CA	SST-DC2K8-PC00-SST-DC2K8-CA	2038-01-11 05:51:57	Trusted Root CA's

Figure 22: Digital IDs: Personal 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 18), the CA certificates for the Digital IDs will also be on the token (as indicated in the picture above, under **Certification Path**).

Private key non-exportable

When the private key belonging to the Digital ID is non-exportable, the transfer fails and the following error message will be displayed:



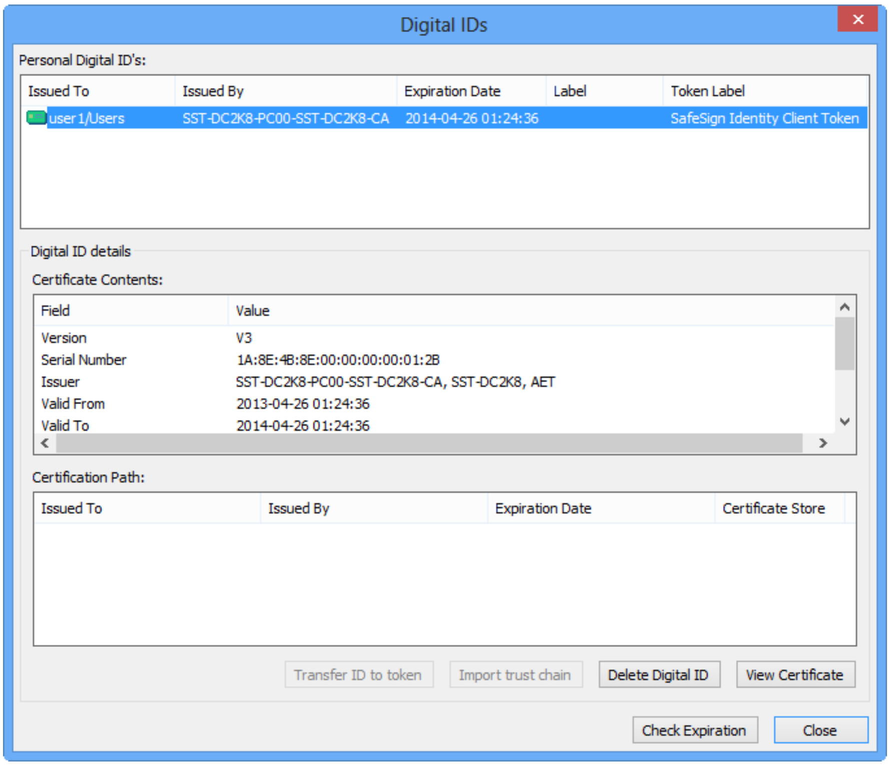
The private key belonging to the Digital ID is non-exportable (0x8009000B)

Figure 23: Transfer ID to token: The private key belonging to the Digital ID is non-exportable

➔ Click **OK** to close this dialog

2.1.1.1 Certification Path

When the CA certificate is not available (either on the token or in the appropriate Microsoft Certificate Store), the *Digital IDs* dialog will look like this:



Issued To	Issued By	Expiration Date	Label	Token Label
user1/Users	SST-DC2K8-PC00-SST-DC2K8-CA	2014-04-26 01:24:36		SafeSign Identity Client Token

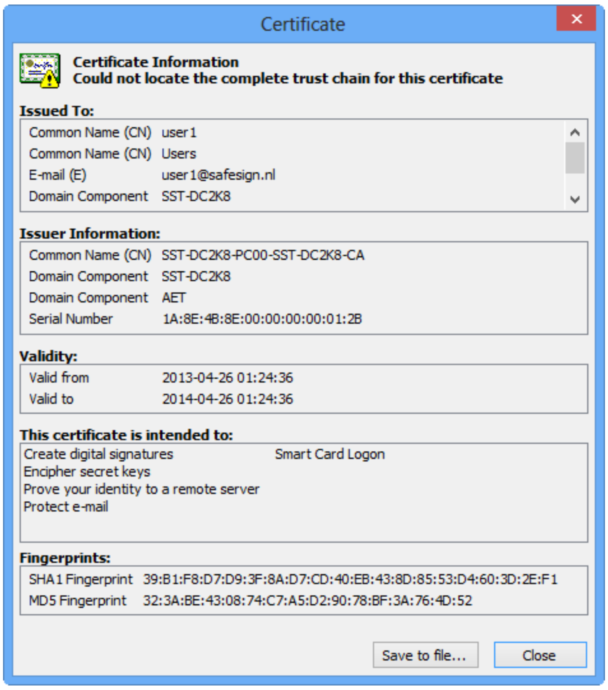
Field	Value
Version	V3
Serial Number	1A:8E:4B:8E:00:00:00:00:01:2B
Issuer	SST-DC2K8-PC00-SST-DC2K8-CA, SST-DC2K8, AET
Valid From	2013-04-26 01:24:36
Valid To	2014-04-26 01:24:36

Issued To	Issued By	Expiration Date	Certificate Store

Figure 24: Digital IDs: Certification Path empty

There is no CA certificate listed under **Certification Path**.

When you double-click to view the certificate, the *Certificate* dialog will inform you:



Certificate Information
Could not locate the complete trust chain for this certificate

Issued To:

Common Name (CN)	user1
Common Name (CN)	Users
E-mail (E)	user1@safesign.nl
Domain Component	SST-DC2K8

Issuer Information:

Common Name (CN)	SST-DC2K8-PC00-SST-DC2K8-CA
Domain Component	SST-DC2K8
Domain Component	AET
Serial Number	1A:8E:4B:8E:00:00:00:00:01:2B

Validity:

Valid from	2013-04-26 01:24:36
Valid to	2014-04-26 01:24:36

This certificate is intended to:

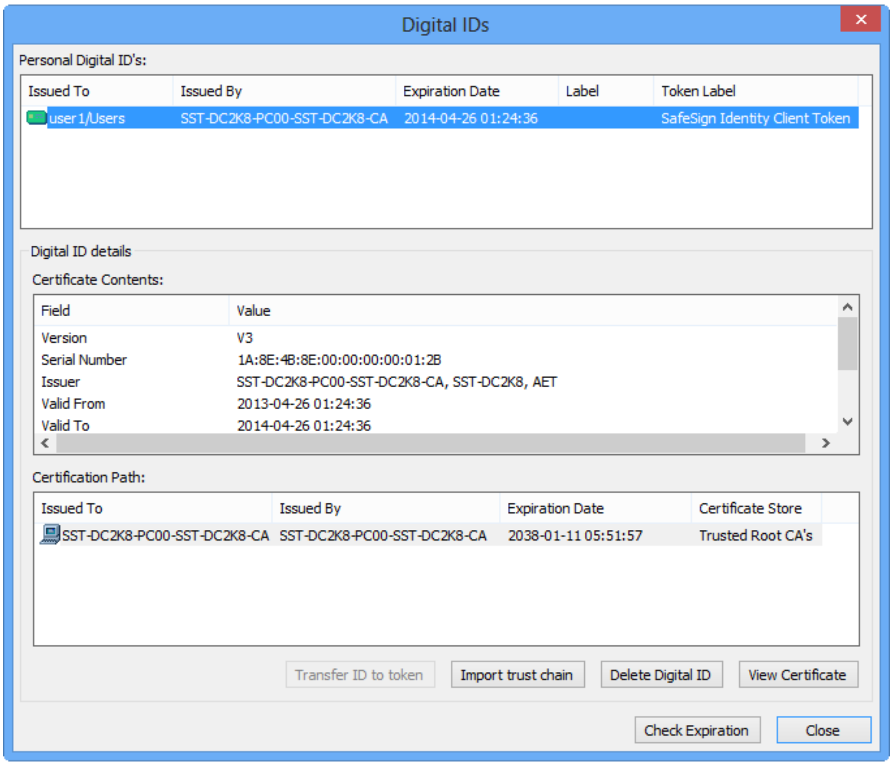
Create digital signatures
Encipher secret keys
Prove your identity to a remote server
Protect e-mail
Smart Card Logon

Fingerprints:

SHA1 Fingerprint	39:B1:F8:D7:D9:3F:8A:D7:CD:40:EB:43:8D:85:53:D4:60:3D:2E:F1
MD5 Fingerprint	32:3A:BE:43:08:74:C7:A5:D2:90:78:BF:3A:76:4D:52

Figure 25: View Certificate: Could not locate the complete trust chain for this certificate

When the CA certificate is not on the token (for example when you chose not to import the certificate chain during transferral, see Figure 18), but it is in the appropriate Microsoft (Trusted Root Certification Authorities) Store, the *Digital IDs* dialog will look like this:



Personal Digital ID's:

Issued To	Issued By	Expiration Date	Label	Token Label
user1/Users	SST-DC2K8-PC00-SST-DC2K8-CA	2014-04-26 01:24:36		SafeSign Identity Client Token

Digital ID details

Certificate Contents:

Field	Value
Version	V3
Serial Number	1A:8E:4B:8E:00:00:00:00:01:2B
Issuer	SST-DC2K8-PC00-SST-DC2K8-CA, SST-DC2K8, AET
Valid From	2013-04-26 01:24:36
Valid To	2014-04-26 01:24:36

Certification Path:

Issued To	Issued By	Expiration Date	Certificate Store
SST-DC2K8-PC00-SST-DC2K8-CA	SST-DC2K8-PC00-SST-DC2K8-CA	2038-01-11 05:51:57	Trusted Root CA's

Figure 26: Digital IDs: Certification path not on token

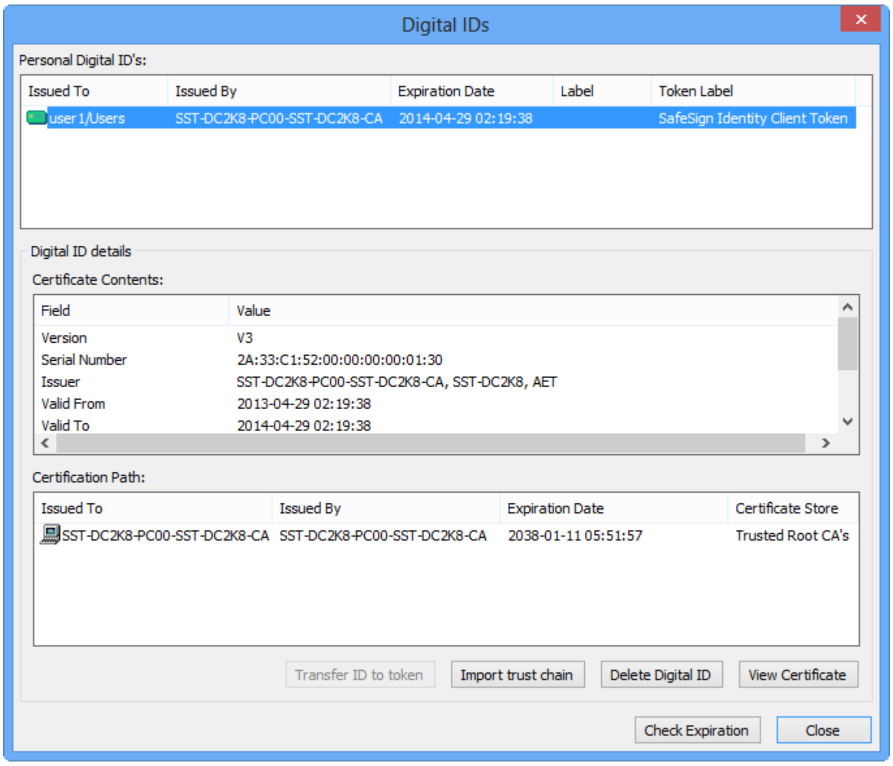
In this case, you may want to import the trust chain onto the token. This is described in section 2.1.2.

2.1.2 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), you always have all certificates with you and can register them.

You can use this functionality 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 2.1.1) 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:



Digital IDs

Personal Digital ID's:

Issued To	Issued By	Expiration Date	Label	Token Label
user1/Users	SST-DC2K8-PC00-SST-DC2K8-CA	2014-04-29 02:19:38		SafeSign Identity Client Token

Digital ID details

Certificate Contents:

Field	Value
Version	V3
Serial Number	2A:33:C1:52:00:00:00:00:01:30
Issuer	SST-DC2K8-PC00-SST-DC2K8-CA, SST-DC2K8, AET
Valid From	2013-04-29 02:19:38
Valid To	2014-04-29 02:19:38

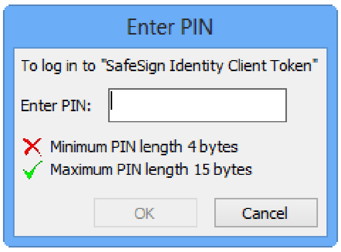
Certification Path:

Issued To	Issued By	Expiration Date	Certificate Store
SST-DC2K8-PC00-SST-DC2K8-CA	SST-DC2K8-PC00-SST-DC2K8-CA	2038-01-11 05:51:57	Trusted Root CA's

Figure 27: Digital IDs: Certification path not on token

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

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



Enter PIN

To log in to "SafeSign Identity Client Token"

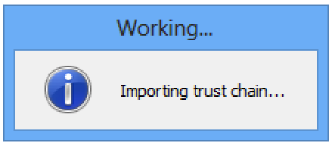
Enter PIN:

✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes

Figure 28: Import trust chain: Enter PIN

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

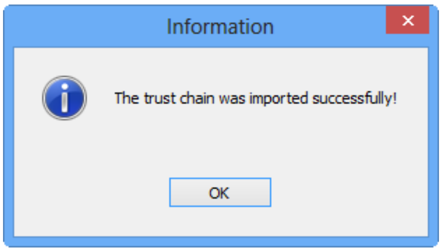
The certificate chain will now be imported:



Importing trust chain...

Figure 29: Import trust chain: Importing trust chain

3 When the certificate chain has been successfully imported, you will be informed:

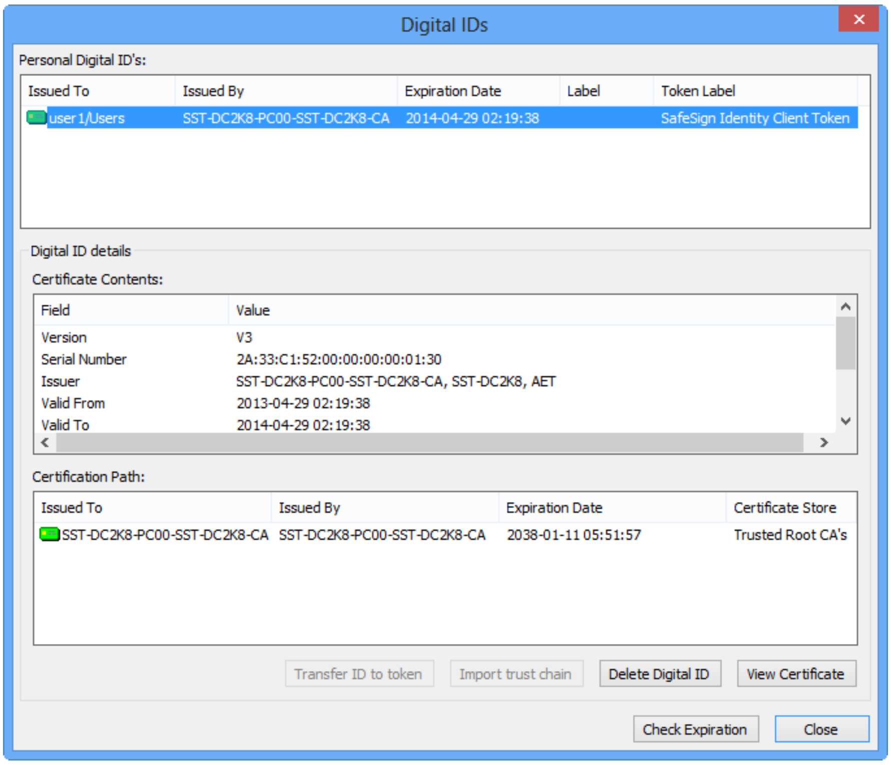


The trust chain was imported successfully!

Figure 30: Import trust chain: The trust chain was imported successfully

➔ Click **OK** to close this dialog

The certificate chain will now be on the token:



Personal Digital ID's:

Issued To	Issued By	Expiration Date	Label	Token Label
🟩 user1/Users	SST-DC2K8-PC00-SST-DC2K8-CA	2014-04-29 02:19:38		SafeSign Identity Client Token

Digital ID details

Certificate Contents:

Field	Value
Version	V3
Serial Number	2A:33:C1:52:00:00:00:00:01:30
Issuer	SST-DC2K8-PC00-SST-DC2K8-CA, SST-DC2K8, AET
Valid From	2013-04-29 02:19:38
Valid To	2014-04-29 02:19:38

Certification Path:

Issued To	Issued By	Expiration Date	Certificate Store
🟩 SST-DC2K8-PC00-SST-DC2K8-CA	SST-DC2K8-PC00-SST-DC2K8-CA	2038-01-11 05:51:57	Trusted Root CA's

Figure 31: Digital IDs: Certification path on token

2.1.3 Delete Digital ID

It is possible to delete a Digital ID stored on the token by means of the **Delete Digital ID** button (Figure 14).

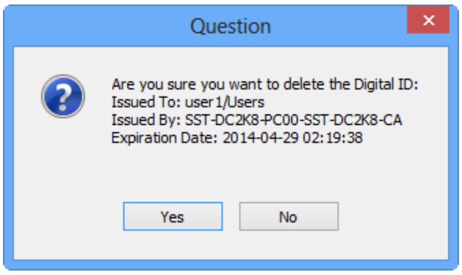
With the Token Utility, you can only delete Personal Digital IDs that are on the token; you can not delete Digital IDs that are in the Certificate Store, as indicated in the *Digital IDs* dialog by the symbol (in which case the **Delete Digital ID** button will be greyed out): 💻

Note

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:



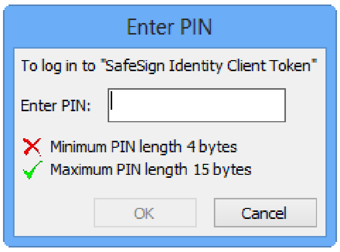
Are you sure you want to delete the Digital ID:
Issued To: user1/Users
Issued By: SST-DC2K8-PC00-SST-DC2K8-CA
Expiration Date: 2014-04-29 02:19:38

Figure 32: Delete Digital ID: Are you sure you want to delete Digital ID

➔ Click **Yes** to delete the Digital ID, upon which you will be asked to enter the PIN for your token

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:



To log in to "SafeSign Identity Client Token"

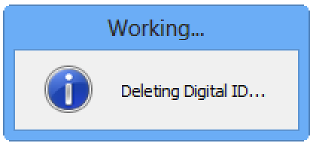
Enter PIN:

✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes

Figure 33: Delete Digital ID: Enter PIN

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

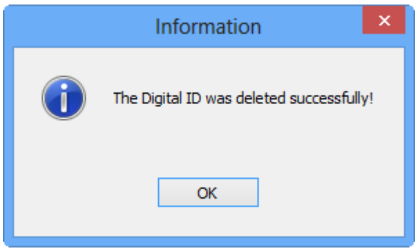
3 Upon entering the correct PIN, the Digital ID will be deleted:



Deleting Digital ID...

Figure 34: Delete Digital ID: Deleting Digital ID

4 When the Digital ID has been successfully deleted, you will be informed:



Information

The Digital ID was deleted successfully!

Figure 35: Delete Digital ID: The Digital ID was deleted successfully

➔ Click **OK** to close this dialog

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

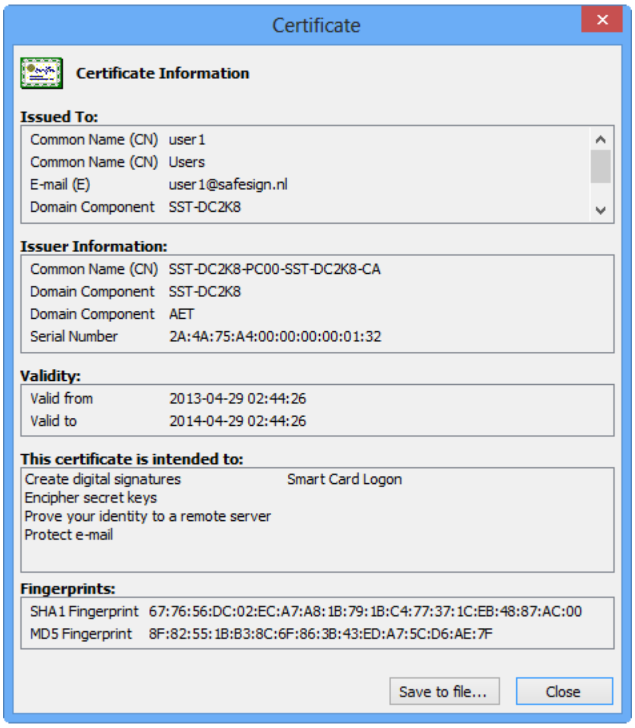
Note that the certificate will remain registered in the certificate store, as the Microsoft Certificate Propagation service does not deregister certificates (once they are registered).

2.1.4 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:



Certificate

Certificate Information

Issued To:

Common Name (CN) user1
Common Name (CN) Users
E-mail (E) user1@safesign.nl
Domain Component SST-DC2K8

Issuer Information:

Common Name (CN) SST-DC2K8-PC00-SST-DC2K8-CA
Domain Component SST-DC2K8
Domain Component AET
Serial Number 2A:4A:75:A4:00:00:00:00:01:32

Validity:

Valid from 2013-04-29 02:44:26
Valid to 2014-04-29 02:44:26

This certificate is intended to:

Create digital signatures
Encipher secret keys
Prove your identity to a remote server
Protect e-mail
Smart Card Logon

Fingerprints:

SHA1 Fingerprint 67:76:56:DC:02:EC:A7:A8:1B:79:1B:C4:77:37:1C:EB:48:87:AC:00
MD5 Fingerprint 8F:82:55:1B:B3:8C:6F:86:3B:43:ED:A7:5C:D6:AE:7F

Figure 36: View Certificate: Certificate Information

This dialog will display the available certificate information.

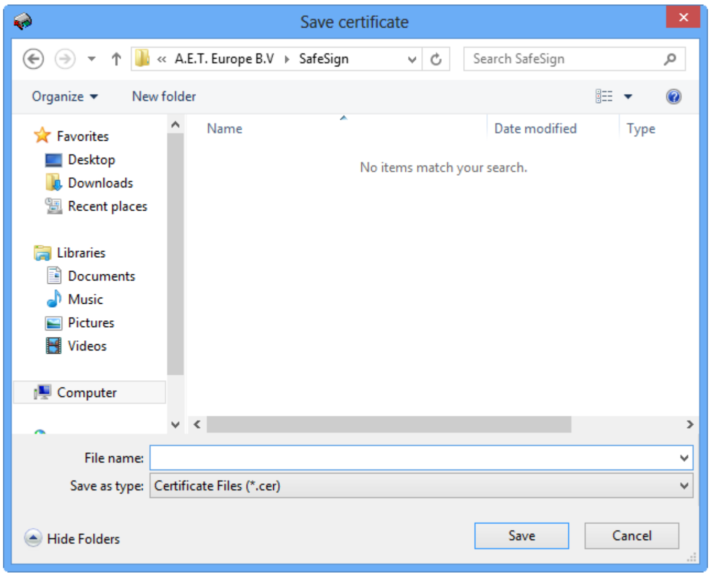
It will also give additional information when appropriate, such as when the certificate is about to expire (Figure 15) or expired, when the complete trust chain of the certificate cannot be located (Figure 25) or a combination of these.

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

Save to file

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):



No items match your search.

File name:

Save as type: Certificate Files (*.cer)

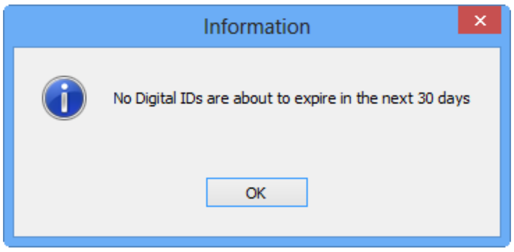
Figure 37: View Certificate: Save certificate

➔ Select a location for the file to be saved in and a name to save it under, then click **Save**

2.1.5 Check Expiration

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

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

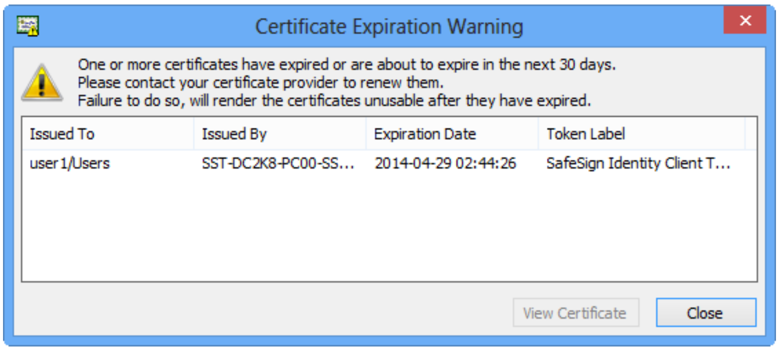


No Digital IDs are about to expire in the next 30 days

Figure 38: Check Expiration: 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:



Certificate Expiration Warning

One or more certificates have expired or are about to expire in the next 30 days.
Please contact your certificate provider to renew them.
Failure to do so, will render the certificates unusable after they have expired.

Issued To	Issued By	Expiration Date	Token Label
user1/Users	SST-DC2K8-PC00-SS...	2014-04-29 02:44:26	SafeSign Identity Client T...

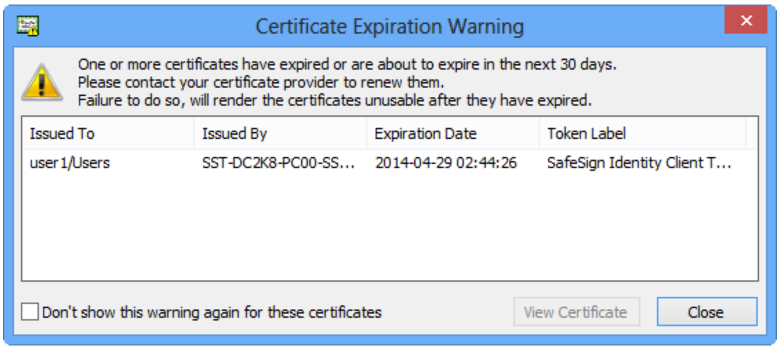
Figure 39: Check Expiration: Certificate Expiration Warning

This dialog will display both the certificate(s) that will expire in the next [x] days (30 days in our example) and the certificates that have already expired[1].

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

Certificate Expiration Warning

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



Certificate Expiration Warning

One or more certificates have expired or are about to expire in the next 30 days.
Please contact your certificate provider to renew them.
Failure to do so, will render the certificates unusable after they have expired.

Issued To	Issued By	Expiration Date	Token Label
user1/Users	SST-DC2K8-PC00-SS...	2014-04-29 02:44:26	SafeSign Identity Client T...

☐ Don't show this warning again for these certificates

Figure 40: Certificate Expiration Warning

Only in the Token Administration Utility, in the Task Manager (see section 5), you can enable / disable this task.

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**.

2.1.6 Close

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

[1] Just as Microsoft will keep certificates that are expired in its Certificate Store.

2.2 Import Digital ID

The SafeSign Identity Client Token Utility allows you to import a Digital ID on your SafeSign Identity Client 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

The term 'Digital ID (file)' is used to refer to the combination of a certificate (including a public key) and a private key (PKCS #12 format) usually protected by a password.

A file of this format can be obtained for example by exporting the keys and certificates from your Firefox (.p12) or from your Microsoft Certificate Store (.pfx). Note that during this process, you will be asked to enter a password to protect your file. This password is required when importing a Digital ID on your SafeSign Identity Client token.

When SafeSign Identity Client 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).

Even so, the user will at all times be able to view the Digital IDs available to him in the Digital IDs dialog (**Digital IDs > Show Registered Digital IDs**), which will correctly display the Digital ID(s) that can be used for cryptographic operations.

1 To import a Digital ID, click **Digital IDs** > **Import Digital ID**:

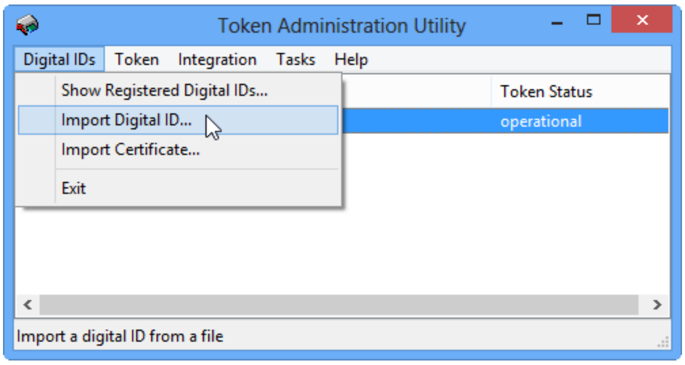
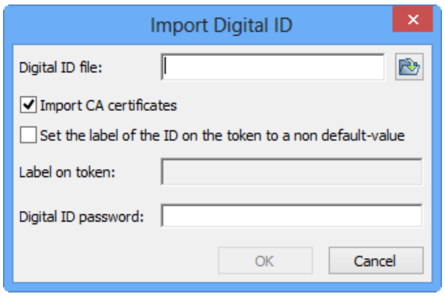


Figure 41: Token Utility: Import Digital ID

2 The following dialog will appear:



Import Digital ID

Digital ID file:

☑ Import CA certificates

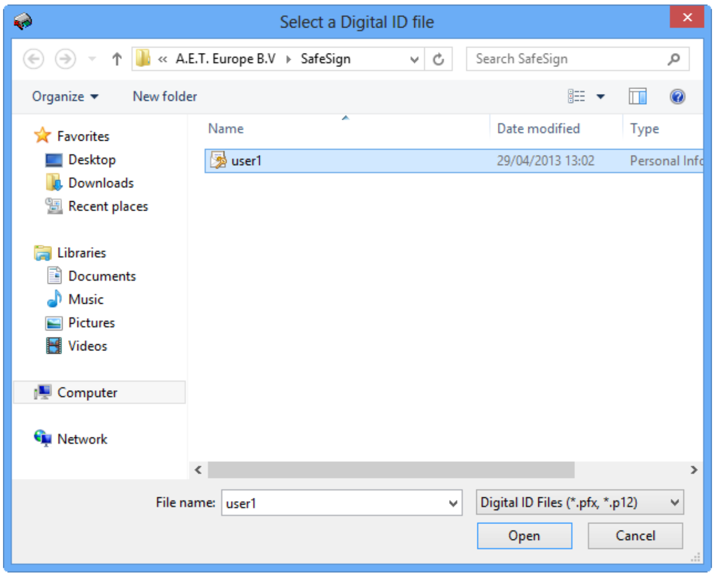
□ Set the label of the ID on the token to a non default-value

Label on token:

Digital ID password:

Figure 42: Import Digital ID

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:



Select a Digital ID file

« A.E.T. Europe B.V › SafeSign

Name	Date modified	Type
user1	29/04/2013 13:02	Personal Info

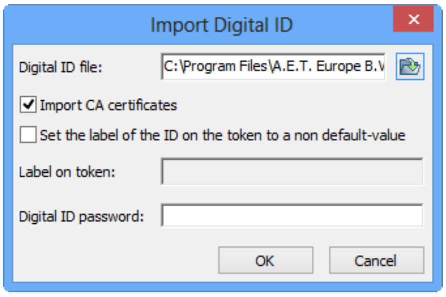
File name: user1

Digital ID Files (*.pfx, *.p12)

Figure 43: Import Digital ID: Select a Digital ID file

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

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



Import Digital ID

Digital ID file: C:\Program Files\A.E.T. Europe B.V

☑ Import CA certificates

□ Set the label of the ID on the token to a non default-value

Label on token:

Digital ID password:

Figure 44: Import Digital ID: Digital ID file

➔ The next step is to enter the Digital ID password

Import CA certificates

When importing a Digital ID, you may choose whether you want to import the CA certificates as well. Doing so will ensure maximum flexibility and interoperability. When taking your token to another computer (where the appropriate trust chain may not be installed), the CA certificate will be registered.

By default, the option **Import CA certificates** is selected.

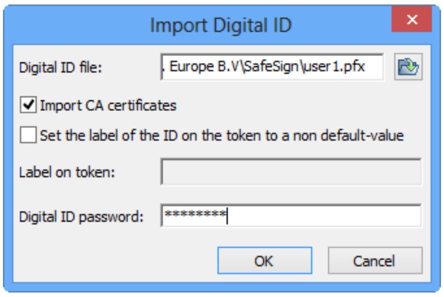
If you do not wish to import the CA certificates on the token, deselect the checkbox.

Set the label of the ID on the token to a non default-value

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.

3 Enter the password for the Digital ID file:


Import Digital ID

Digital ID file: Europe B.V\SafeSign\user1.pfx

☑ Import CA certificates

□ Set the label of the ID on the token to a non default-value

Label on token:

Digital ID password: *********

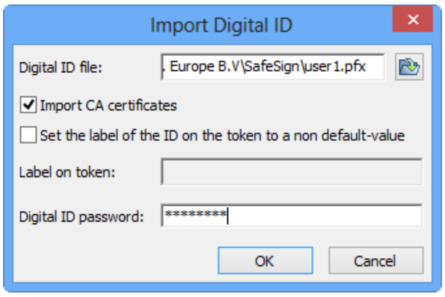
Figure 45: Import Digital ID: Digital ID password

- Click **OK** to import the Digital ID

Wrong Password

The 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, the following prompt will be displayed:


Import Digital ID

Digital ID file: Europe B.V\SafeSign\user1.pfx

☑ Import CA certificates

□ Set the label of the ID on the token to a non default-value

Label on token:

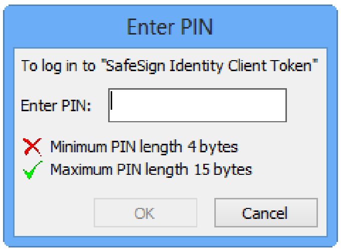
Digital ID password: *********

Figure 46: Error: Digital ID needs a different password

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

You will have to start the import a Digital ID procedure again by clicking **Digital IDs > Import Digital ID**

4 When you have clicked **OK** after entering the correct password for the Digital ID file (Figure 45), you will be asked to enter the PIN for the token:



Enter PIN

To log in to "SafeSign Identity Client Token"

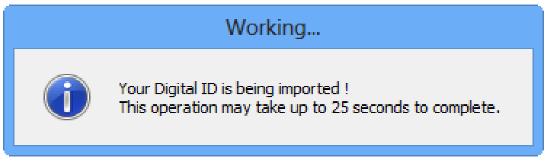
Enter PIN:

✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes

Figure 47: Import Digital ID: Enter PIN

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

5 Upon clicking **OK** after entering the correct PIN, the Digital ID will be imported:



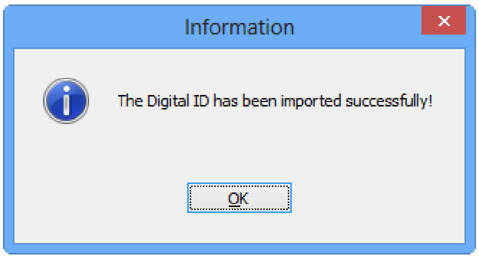
Working...

Your Digital ID is being imported !
This operation may take up to 25 seconds to complete.

Figure 48: Import Digital ID: Your Digital ID is being imported

➔ Your Digital ID is being imported

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



Information

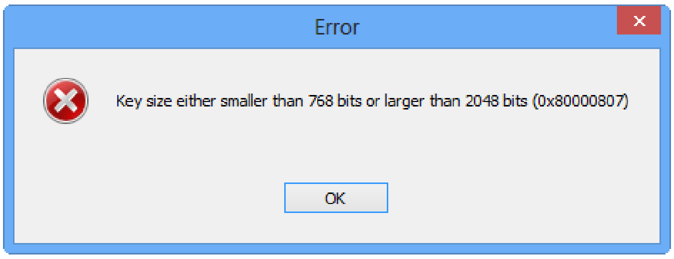
The Digital ID has been imported successfully!

Figure 49: Import Digital ID: The Digital ID has been imported successfully

➔ Click **OK** to close this dialog

Key Size Error

When you try to import a Digital ID that does not comply with the key length constraints of the supported token, the following dialog will be displayed:



Error

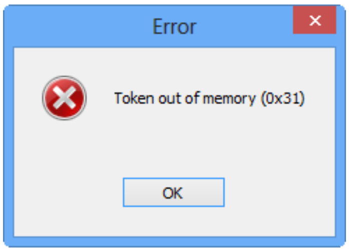
Key size either smaller than 768 bits or larger than 2048 bits (0x80000807)

Figure 50: Error: Key Size either smaller than 768 bits or larger than 2048 bits

Click **OK** to close this dialog

Token out of Memory

When the token is full, i.e. does not have enough memory to import a / another Digital ID, the following dialog will be displayed:



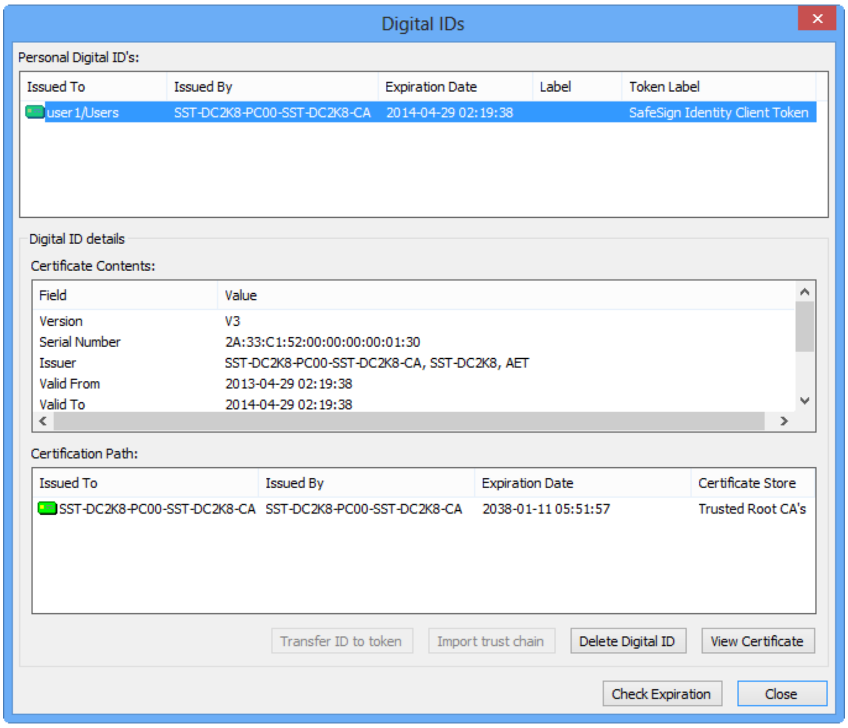
Token out of memory (0x31)

Figure 51: Error: Token out of memory

Click **OK** to close this dialog.

Note that you may not always be able to see why the token is out of memory, for example, when the amount of public space still seems to be sufficient.

After importing a Digital ID, you may check in the *Digital IDs* dialog (**Digital IDs > Show Registered Digital IDs**) if the Digital ID has been correctly imported:



Personal Digital ID's:

Issued To	Issued By	Expiration Date	Label	Token Label
user1/Users	SST-DC2K8-PC00-SST-DC2K8-CA	2014-04-29 02:19:38		SafeSign Identity Client Token

Digital ID details

Certificate Contents:

Field	Value
Version	V3
Serial Number	2A:33:C1:52:00:00:00:00:01:30
Issuer	SST-DC2K8-PC00-SST-DC2K8-CA, SST-DC2K8, AET
Valid From	2013-04-29 02:19:38
Valid To	2014-04-29 02:19:38

Certification Path:

Issued To	Issued By	Expiration Date	Certificate Store
SST-DC2K8-PC00-SST-DC2K8-CA	SST-DC2K8-PC00-SST-DC2K8-CA	2038-01-11 05:51:57	Trusted Root CA's

Figure 52: Token Utility: Personal Digital ID imported

2.3 Import Certificate

The SafeSign Identity Client Token Utility allows you to import a Certificate Authority (CA) certificate on your SafeSign Identity Client token. By importing the file, the CA certificate is securely stored on your token, greatly enhancing the mobility and flexibility of your SafeSign Identity Client token.

Upon using your SafeSign Identity Client token on another computer, where the CA (root) certificate is not installed, SafeSign Identity Client will enable you to install the CA certificate, creating a trusted chain for your personal Digital ID.

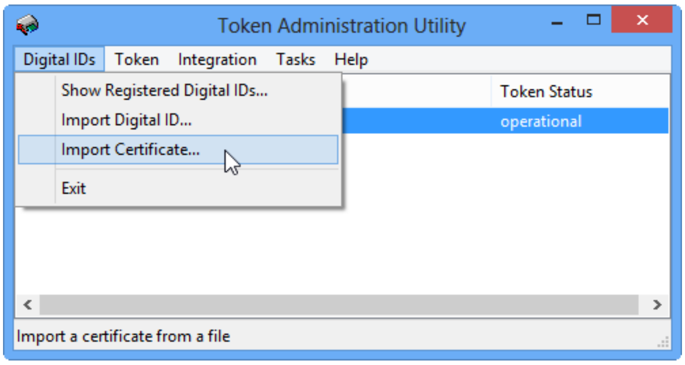
SafeSign Identity Client supports the import of:

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

Note

CA certificates may also be imported during token initialisation, please refer to section 3.1.4

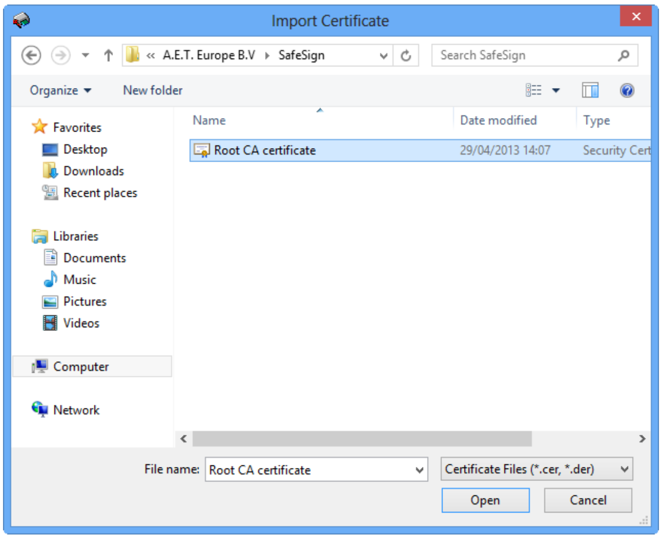
1 To import a CA Certificate, click **Digital IDs** > **Import Certificate**:



Import a certificate from a file

Figure 53: Token Utility: Import Certificate

2 You will be asked to specify the location where the Certificate File is stored:



Name	Date modified	Type
Root CA certificate	29/04/2013 14:07	Security Cert

File name: Root CA certificate

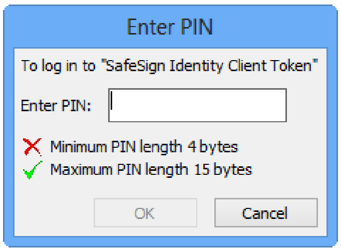
Certificate Files (*.cer, *.der)

Figure 54: Import Certificate: Import Certificate

Specify the location where the Certificate File is stored. The Certificate File can be stored anywhere, either on a hard disk or on removable media (such as a USB memory stick).

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

3 After selecting the Certificate File to import, you will be asked to enter the PIN of your SafeSign Identity Client Token:



Enter PIN

To log in to "SafeSign Identity Client Token"

Enter PIN:

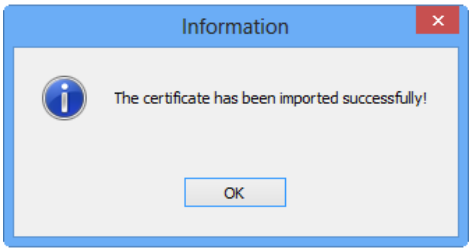
✗ Minimum PIN length 4 bytes

✓ Maximum PIN length 15 bytes

Figure 55: Import Certificate: Enter PIN

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

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



Information

The certificate has been imported successfully!

Figure 56: Import Certificate: The certificate has been imported successfully

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

2.4 Exit

The *Exit* item of the **Digital IDs** menu will close the SafeSign Identity Client Token Utility.

3 Token Menu

The **Token** menu in both the Token Management Utility and the Token Administration Utility includes the following functionality:

Section 3.1	:	Initialise Token
Section 3.2	:	Change PIN
Section 3.3	:	Change Transport PIN
Section 3.4	:	Unlock PIN
Section 3.5	:	Change PUK
Section 3.6	:	Show Token Info

The following functionality is only included in the **Token** menu of the Token Administration Utility:

Section 3.7	:	Show Token Objects
Section 3.8	:	Dump Token Contents
Section 3.9	:	Query Unknown Token
Section 3.10	:	Analyse Certificate Quality
Section 3.11	:	Change PIN Timeout

3.1 Initialising your Token

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

When initialising a token, SafeSign Identity Client will detect the token model you have inserted and will determine the best (possible) profile(s) to initialise the token with (as the availability of profiles depends on the type of token used[1]). For Java Cards v2.2 cards, there is only one profile (Default) available.

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. This includes for example the maximum number of PIN and/or PUK retries and the length of the PIN and/or PUK.

Note however, the distinction between test (completed) tokens and series / production (completed) tokens:

- For test tokens, it is possible to change the profile of the token during a re-initialisation of the token (i.e. replace the existing PKCS#15 structure with a new or updated PKCS#15 structure).
- For production tokens, it is not possible to change a profile once it has been set during initialisation. You may only wipe its contents, while maintaining the PKCS#15 structure written on it during initialisation.

You can view the completion of the token under **Token > Show Token Info** (section 3.6).

Note

Test (completed) tokens are normally used for testing and evaluation only.

Users will generally be provided with series (completed) tokens that (in case of Java cards) have the SafeSign Identity Client applet installed and that may even be initialised. Also, for Java cards, the default GlobalPlatform key set is usually changed to a (customer) specific key set, so the applet(s) cannot be removed (without knowledge of this keyset).

[1] If a particular profile is not available, this will probably mean that the profile is not available for the token (because it does not have enough room for the public and private space settings of that profile). If no selectable profile is available (the token profile line is greyed out), this will probably mean that you do not have enough rights to select a profile. Depending on your user rights, you may only be able to select the profile set by the administrator. Note that end-users are recommended to select the default profile, unless otherwise instructed by their administrator.

Note

As the correct functioning of SafeSign Identity Client is depending 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 Identity Client by vendors that are not approved AET production sites and not in accordance with our QA policies (which require i.a. the 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 Identity Client Maintenance and Support Agreement.

The following sections will describe the different scenarios involved:

Section 3.1.1	:	How to initialise an uninitialised token (whether test or series-completed).
Section 3.1.2	:	How to re-initialise an initialised token (test-completed only).
Section 3.1.3	:	How to wipe a token (series-completed only).
Section 3.1.4	:	How to recycle a token.
Section 3.1.5	:	How to initialise an uninitialised token with PIN Policy.
Section 3.1.6	:	How to import a CA Certificate during token initialisation / wiping.

These sections will use a Java Card v2.2 token as an example[1].

3.1.1 Initialise Token

1 When you have not yet initialised your token (whether the SafeSign Identity Client applet is installed or not), your token will be identified in the Token Utility, as a "*Blank Token – uninitialised*" and only the *Initialise Token* item (and the *Show Token Info* item) will be available:

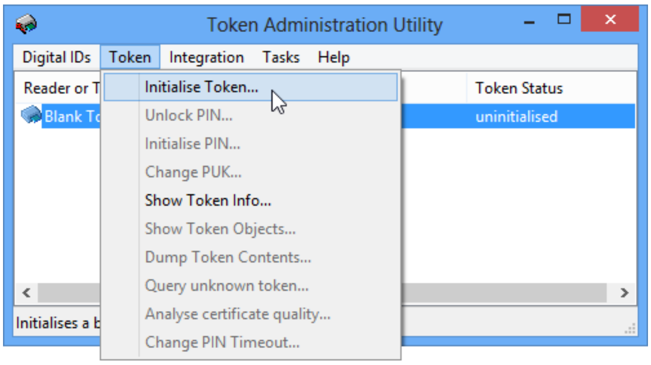
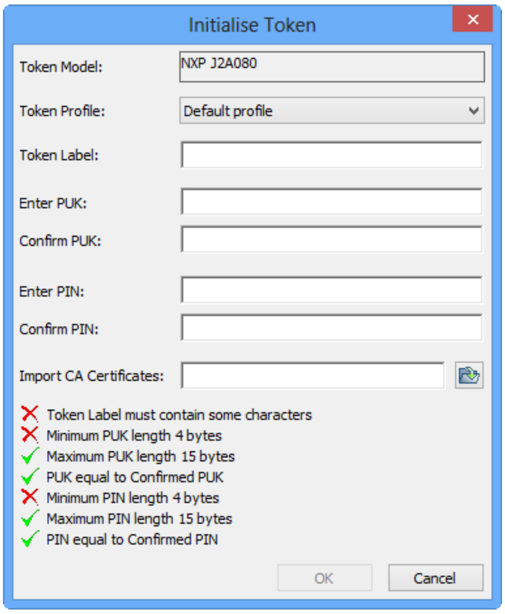


Figure 57: Token Utility: Initialise Token

➔ In order to initialise your token, click **Token** > **Initialise Token** (as above)

[1] The token used is an NXP J2A080 smart card.

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



Initialise Token

Token Model: NXP J2A080

Token Profile: Default profile

Token Label:

Enter PUK:

Confirm PUK:

Enter PIN:

Confirm PIN:

Import CA Certificates:

- ✗ 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

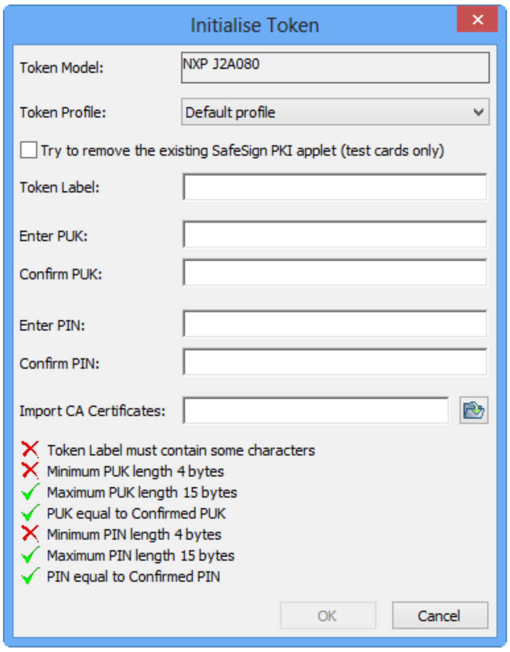
Figure 58: Initialise Token: Initialise Token

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

The *Token Profile* drop-down box will allow you to select the profile to initialise the token with. Note that this box may be greyed out, if you do not have the rights to modify it or may only contain one (Default) profile.

SafeSign applet installed in test

When the SafeSign Identity Client Java applet is installed in test, the option “Try to remove the existing SafeSign (Identity Client) PKI applet (test cards only)” will be available in the Token Administration Utility only:



Initialise Token

Token Model: NXP J2A080

Token Profile: Default profile

□ Try to remove the existing SafeSign PKI applet (test cards only)

Token Label:

Enter PUK:

Confirm PUK:

Enter PIN:

Confirm PIN:

Import CA Certificates:

- ✗ 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

Figure 59: Token Administration Utility: Try to remove the existing SafeSign PKI applet

2 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 as follows, taking into account the remarks and requirements below:

Field	**Requirements**
Token Profile	Different token profiles may be available, depending on the type of token you have inserted. Choose the profile that suits your needs. 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
Enter PUK	Minimum PUK length is 4 characters, maximum PUK length is 8 – 15 characters
Confirm PUK	Confirmed new PUK should be equal to the new PUK
Enter PIN	Minimum PIN length is 4 characters, maximum PIN length is 8 - 15 characters
Confirm PIN	Confirmed new PIN should be equal to new PIN

Table 1: Initialise Token: Initialise Token fields

Field requirements

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.[1]

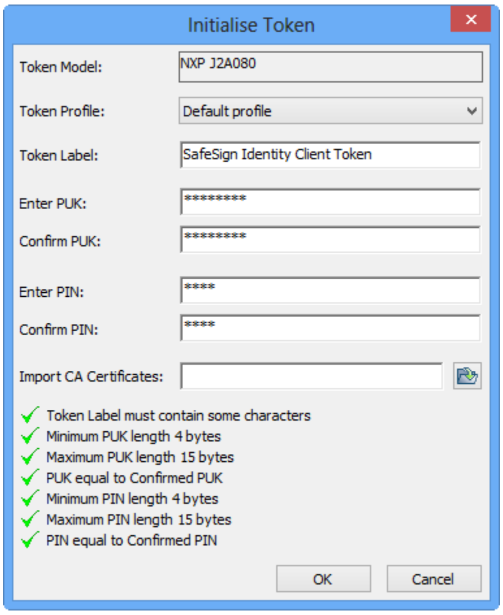
SafeSign Identity Client enforces a minimum and maximum PIN / PUK length. If you enter a PIN / PUK of less than the minimum allowed or more than the maximum allowed, you will not be able to click the **OK** button in such instances where the PIN / PUK is required[2]. Only when you enter a PIN / PUK of the required length will the PIN / PUK be accepted.

Note that both the minimum and the maximum PIN / PUK length may have been set to different values (than the default values supported by the card) by the administrator.

[1] Note that the minimum and maximum PIN/PUK length is in bytes (not characters), as according to the PKCS #11 specification, PIN is stored as UTF-8 characters (CK_UTF8CHAR). PINs that contain characters with diacrits (such as umlaut, accent grave, etc.) and such characters as ß and €, are converted into their relative UTF-8 encoding, which is at least 2 bytes long.

[2] When the maximum PUK / PIN length exceeds the maximum length required, the **OK** button will be greyed out.

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



Initialise Token

Token Model: NXP J2A080

Token Profile: Default profile

Token Label: SafeSign Identity Client Token

Enter PUK: *********

Confirm PUK: *********

Enter PIN: ****

Confirm PIN: ****

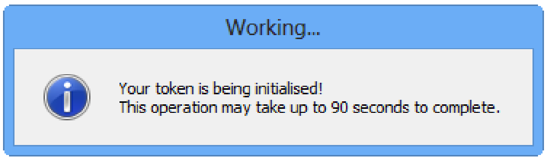
Import CA Certificates:

✓ 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

Figure 60: Initialise Token: Initialise Token completed

➔ Click **OK** to start initialising your SafeSign Identity Client Token.

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



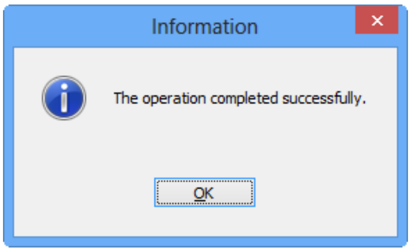
Working...

Your token is being initialised!
This operation may take up to 90 seconds to complete.

Figure 61: Initialise Token: Your token is being initialised

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

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



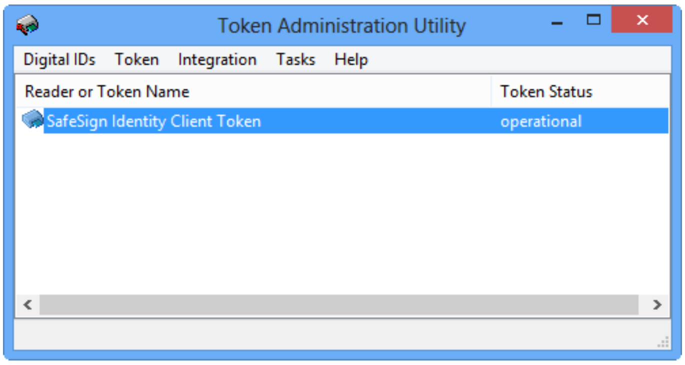
Information

The operation completed successfully.

Figure 62: Initialise Token: The operation completed successfully

➔ Click **OK** to finish the initialisation

When your token is initialised, the token name will appear in the token window:


Token Administration Utility
Digital IDs Token Integration Tasks Help
Reader or Token Name
Token Status

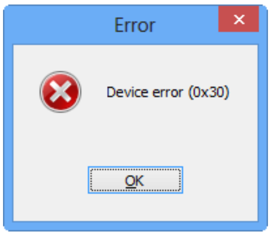
SafeSign Identity Client Token operational

Figure 63: Token Utility: Initialised token

Once your token is initialised, all operations in the **Digital IDs** and **Token** menu will be available.

Device Error

When the Initialise Token operation failed, the following warning will appear:



Device error (0x30)

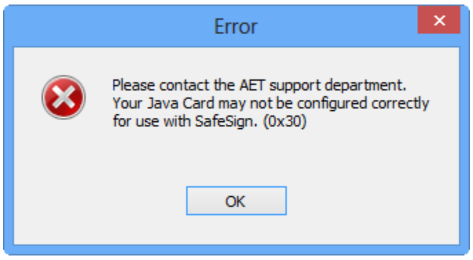
Figure 64: Initialise Token: Device Error 0x30

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 (for the profile you selected).

Click **OK** to close this dialog

Your Java Card may not be configured correctly

The following error message may be displayed when initialising a Java card:



Please contact the AET support department.
Your Java Card may not be configured correctly for use with SafeSign. (0x30)

Figure 65: Initialise Token: Your Java Card may not be configured correctly

This error may have various causes (such as the presence of other applets on the card), but one of the most common causes for this error is that the card does not have the SafeSign Identity Client applet installed and has a custom key set, in which case the Token Utility cannot load the applet (for the Token Utility can only load the SafeSign applet on tokens with a default / test keyset).

Also check that your reader is functioning properly (and satisfies the power requirements) and that you have a token supported by (the version of) SafeSign Identity Client installed.

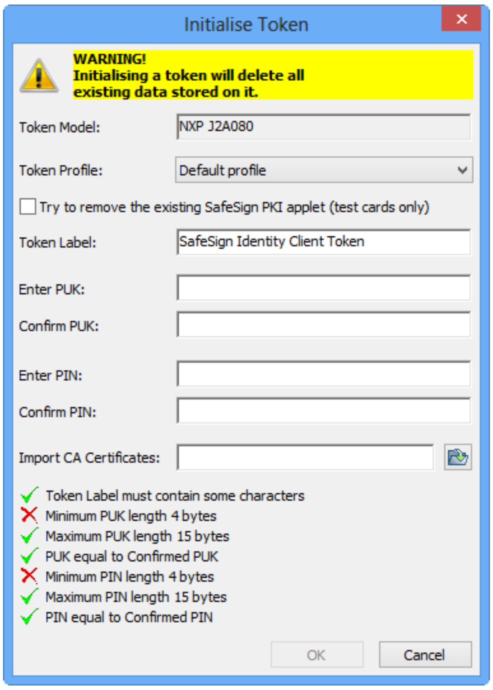
Make sure that the token is inserted in the smart card reader and click **OK** to try to initialise the token again. Otherwise, contact your local supplier or AET SafeSign Support for assistance.

Click **OK** to close this dialog.

3.1.2 Re-initialise Token

When your token has already been initialised, it may be initialised again, if the token is a test (completed) token and has a default keyset. Note that these conditions only apply to test tokens, that should be used for testing and evaluation only (and not being deployed).

Note that when you re-initialise your token, all data that may be stored on your token will be deleted. A warning to this extent will be included in the *Initialise Token* dialog box:



Initialise Token

WARNING!
Initialising a token will delete all existing data stored on it.

Token Model: NXP J2A080

Token Profile: Default profile

□ Try to remove the existing SafeSign PKI applet (test cards only)

Token Label: SafeSign Identity Client Token

Enter PUK:

Confirm PUK:

Enter PIN:

Confirm PIN:

Import CA Certificates:

✓ 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

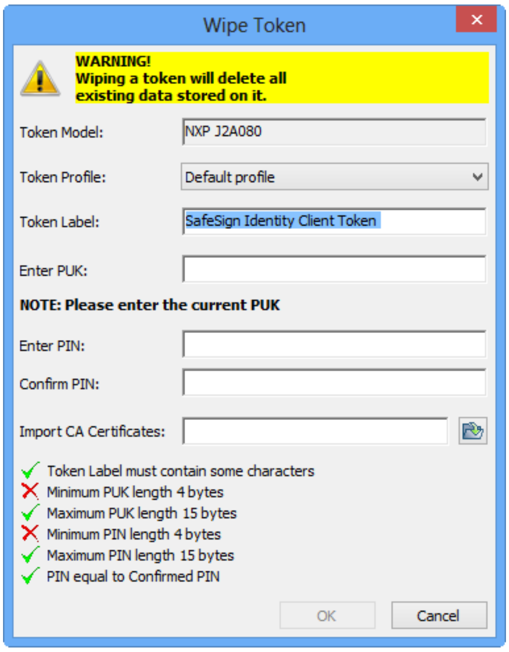
Figure 66: Token Utility: Re-Initialise Token

Upon initialising a token that is as yet uninitialised, as described in section 3.1.1, this warning will not appear, as there is no data on the token yet.

3.1.3 Wipe Token

When you have a series (completed) token that has been initialised (before), you will only be able to wipe the token (not re-initialise it). In that case, the **Token** menu will display the item *Wipe Token* (instead of *Initialise Token*, as in Figure 57).

1 Note that when you wipe your token, all data that may be stored on your token will be deleted. A warning to this extent will be included in the *Wipe Token* dialog box:



Wipe Token

WARNING!
Wiping a token will delete all existing data stored on it.

Token Model: NXP J2A080

Token Profile: Default profile

Token Label: SafeSign Identity Client Token

Enter PUK:

NOTE: Please enter the current PUK

Enter PIN:

Confirm PIN:

Import CA Certificates:

- ✓ Token Label must contain some characters
- ✗ Minimum PUK length 4 bytes
- ✓ Maximum PUK length 15 bytes
- ✗ Minimum PIN length 4 bytes
- ✓ Maximum PIN length 15 bytes
- ✓ PIN equal to Confirmed PIN

Figure 67: Token Utility: Wipe Token

Note that the token label in the dialog above is the old token label for the initialised token.

Note that the Token Profile option may not be available to you.

2 In order to wipe your token, a number of requirements should be met. When you have met a certain requirement, the ✗ will become a ✓

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

Field	**Requirements**
Token Label	The token label must contain some characters, it cannot be empty; Maximum number of characters is 32
Enter PUK	Minimum PUK length is 4 characters; maximum PUK length is 8 - 15 characters. The PUK entered should be the current / existing PUK.
Enter PIN	Minimum PIN length is 4 characters, maximum PIN length is 8 - 15 characters
Confirm PIN	Confirmed new PIN should be equal to new PIN

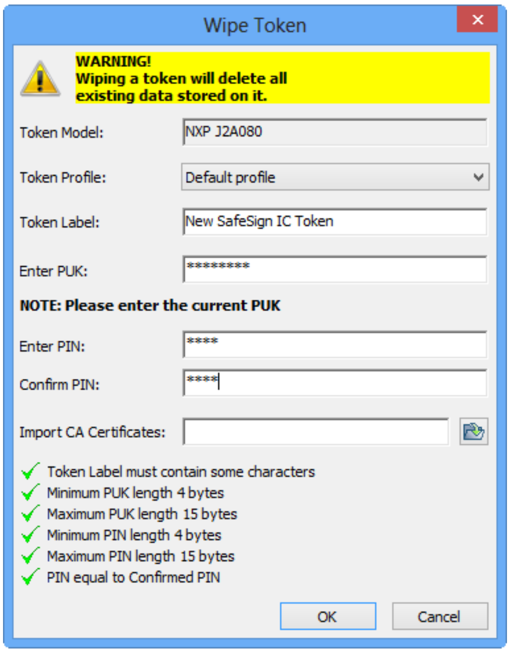
Table 2: Wipe Token: Wipe Token fields

Field requirements

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. [1]

SafeSign Identity Client 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[2]. Only when you enter a PIN / PUK of the required length will the PIN / PUK be accepted. Note that both the minimum and the maximum PIN / PUK length may have been set to different values (than the default values supported by the card) by the administrator.

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



Wipe Token

WARNING!
Wiping a token will delete all existing data stored on it.

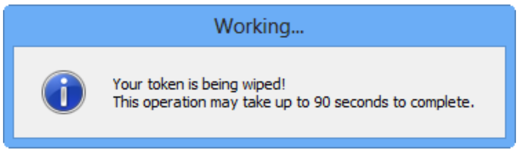
Token Model: NXP J2A080
Token Profile: Default profile
Token Label: New SafeSign IC Token
Enter PUK: ********
NOTE: Please enter the current PUK
Enter PIN: ****
Confirm PIN: ****
Import CA Certificates:

✓ Token Label must contain some characters
✓ Minimum PUK length 4 bytes
✓ Maximum PUK length 15 bytes
✓ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes
✓ PIN equal to Confirmed PIN

Figure 68: Wipe Token: Wipe Token completed

➔ Click **OK** to start wiping your SafeSign Identity Client Token.

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



Working...

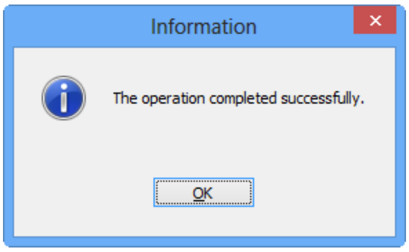
Your token is being wiped!
This operation may take up to 90 seconds to complete.

Figure 69: Wipe Token: Your token is being wiped

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

[1] Note that the minimum and maximum PIN/PUK length is in bytes (not characters), as according to the PKCS #11 specification, PIN is stored as UTF-8 characters (CK_UTF8CHAR). PINs that contain characters with diacrits (such as umlaut, accent grave, etc.) and such characters as ß and €, are converted into their relative UTF-8 encoding, which is at least 2 bytes long.
[2] When the maximum PUK / PIN length exceeds the maximum length required, the **OK** button will be greyed out.

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



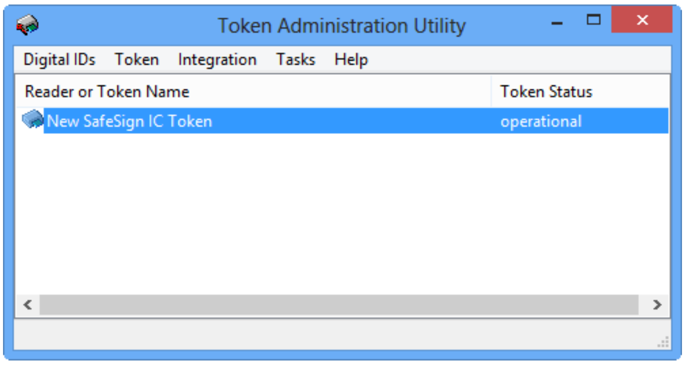
Information

The operation completed successfully.

Figure 70: Wipe Token: The operation completed successfully

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

When your token is wiped, the (new) token name will appear in the token window:



Token Administration Utility

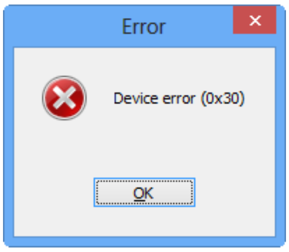
Reader or Token Name	Token Status
New SafeSign IC Token	operational

Figure 71: Token Utility: Wiped Token

Once your token is wiped, all operations in the **Digital IDs** and **Token** menu will be available.

Device Error

When the Wipe Token operation failed, the following warning will appear:



Error

Device error (0x30)

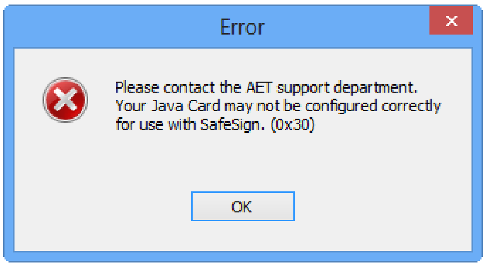
Figure 72: Wipe Token: Device Error 0x30

Check that your reader is functioning properly and whether you have a correct card. 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 (for the profile you selected).

Click **OK** to close this dialog

Your Java Card may not be configured correctly

The following error message may be displayed when initialising a Java card:



Please contact the AET support department.
Your Java Card may not be configured correctly for use with SafeSign. (0x30)

Figure 73: Wipe Token: Your Java card may not be configured correctly

Check that your reader is functioning properly (and satisfies the power requirements) and that you have a token supported by (the version of) SafeSign Identity Client 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.

Click **OK** to close this dialog.

3.1.4 Recycle Token

For certification purposes with the ICP-Brazil standard, some new functionality was implemented in SafeSign Identity Client (applet) version 3.0.80 and higher, for various cards from different vendors.

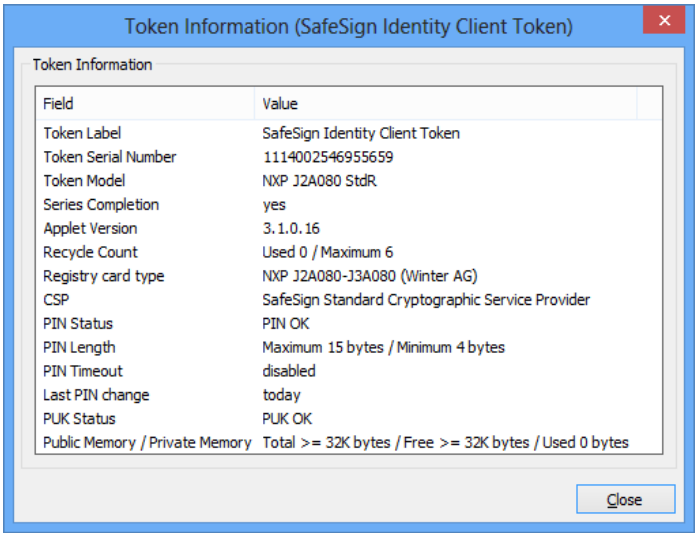
In SafeSign Identity Client version 3.0.80, it is possible to 'recycle' the token, i.e. once the PIN and PUK are blocked due to too many attempts (i.e. entering an incorrect PIN / PUK until the retry counter is exceeded), it is possible to reset the token so that it returns to its original initialized state. 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 Token Utility's Token menu, allowing you to set a new token label, PUK and PIN. The number of recycle attempt depends on the amount set during applet installation (the maximum number of recycle attempts that can be set is decimal 127 / hex 7F). The Token Utility's *Show Token Info* dialog will display the recycle count (used and maximum).

Note that for this functionality to work, a special applet is required, with special installation parameters.

3.1.4.1 Applet Version and Recycle Count

For the recycle functionality to be enabled, a special version of the applet and specific applet install parameters are required (which are outside of the scope of this document). When this applet is installed correctly, the *Token Information* dialog will display the applet version and the number of recycle attempts available:



Field	Value
Token Label	SafeSign Identity Client Token
Token Serial Number	1114002546955659
Token Model	NXP J2A080 StdR
Series Completion	yes
Applet Version	3.1.0.16
Recycle Count	Used 0 / Maximum 6
Registry card type	NXP J2A080-J3A080 (Winter AG)
CSP	SafeSign Standard Cryptographic Service Provider
PIN Status	PIN OK
PIN Length	Maximum 15 bytes / Minimum 4 bytes
PIN Timeout	disabled
Last PIN change	today
PUK Status	PUK OK
Public Memory / Private Memory	Total >= 32K bytes / Free >= 32K bytes / Used 0 bytes

Figure 74: Token Information: Recycle Count

The total number of available recycles for this token is 6.

3.1.4.2 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:

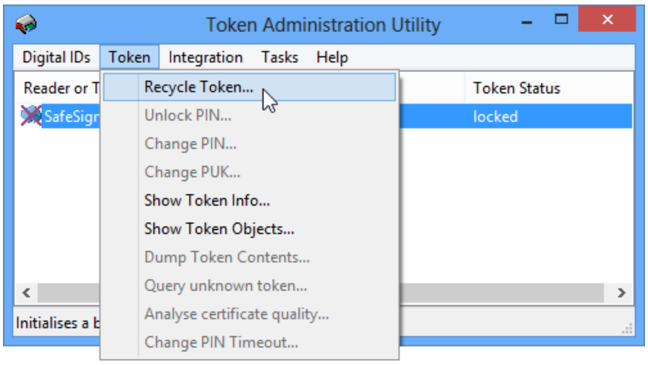
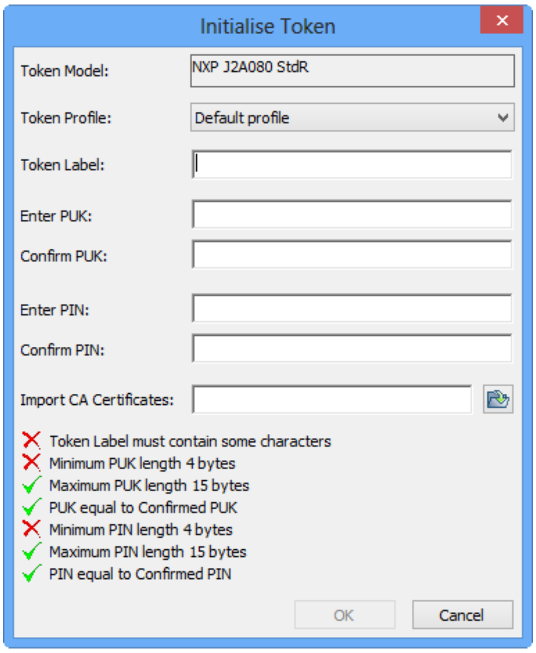


Figure 75: Token Utility: Recycle Token

➔ Click **OK** to start recycling your SafeSign Identity Client Token.

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



Token Model: NXP J2A080 StdR

Token Profile: Default profile

Token Label:

Enter PUK:

Confirm PUK:

Enter PIN:

Confirm PIN:

Import CA Certificates:

- ✗ 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

Figure 76: Initialise Token: Initialise Token

You can now initialise your token as described in section 3.1.1.

3.1.4.3 Recycle Count exceeded

When the maximum number of recycle attempts is reached, the option *Recycle Token* will not be available anymore:

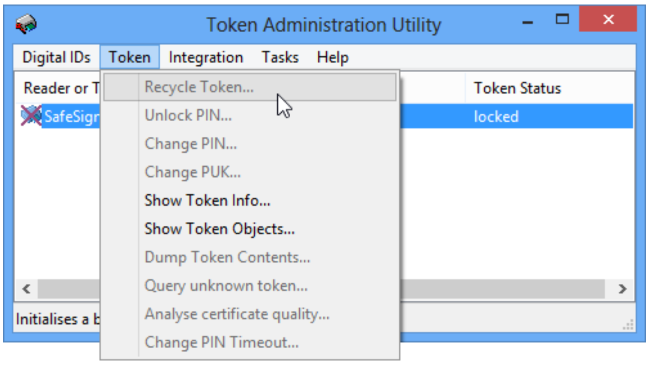
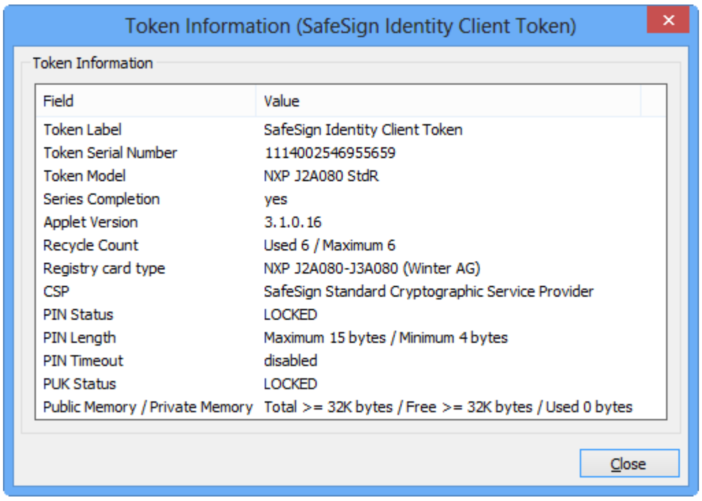


Figure 77: Token Utility: Recycle Token greyed out

The *Show Token Info* dialog will display:



Token Information (SafeSign Identity Client Token)

Token Information

Field	Value
Token Label	SafeSign Identity Client Token
Token Serial Number	1114002546955659
Token Model	NXP J2A080 StdR
Series Completion	yes
Applet Version	3.1.0.16
Recycle Count	Used 6 / Maximum 6
Registry card type	NXP J2A080-J3A080 (Winter AG)
CSP	SafeSign Standard Cryptographic Service Provider
PIN Status	LOCKED
PIN Length	Maximum 15 bytes / Minimum 4 bytes
PIN Timeout	disabled
PUK Status	LOCKED
Public Memory / Private Memory	Total >= 32K bytes / Free >= 32K bytes / Used 0 bytes

Figure 78: Token Information: Recycle Count Locked

3.1.5 Initialise a Token with PIN Policy

For certification purposes with the ICP-Brazil standard, some new functionality was implemented in SafeSign Identity Client (applet) version 3.0.80 and higher, for various cards from different vendors.

SafeSign Identity Client version 3.0.80 supports 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).

In SafeSign IC version 3.0.80, the following policy has been enabled:

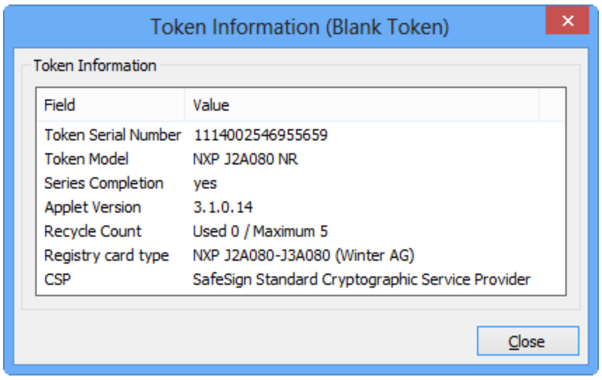
1. PIN / PUK must have at least one (01) capitalized alphabetic character (A-Z);
2. PIN / PUK must have at least one (01) lowercase alphabetic character (a-z);
3. PIN / PUK must have at least one (01) numerical character (0-9);
4. Allow the use of special characters. Example: “$”, “@”, “&” etc.;

This policy is called the Diversification policy.

Note that for this functionality to work, a special applet is required. Currently, an applet is available with support for PIN policy and recycling (see section 3.1.4).

3.1.5.1 Applet Version and Recycle Count

For the PIN Policy and recycle functionality to be enabled, a special version of the applet and specific applet install parameters are required (which are outside of the scope of this document). When this applet is installed correctly, the *Token Information* dialog will display the applet version and the number of recycle attempts available:



Token Information (Blank Token)

Token Information

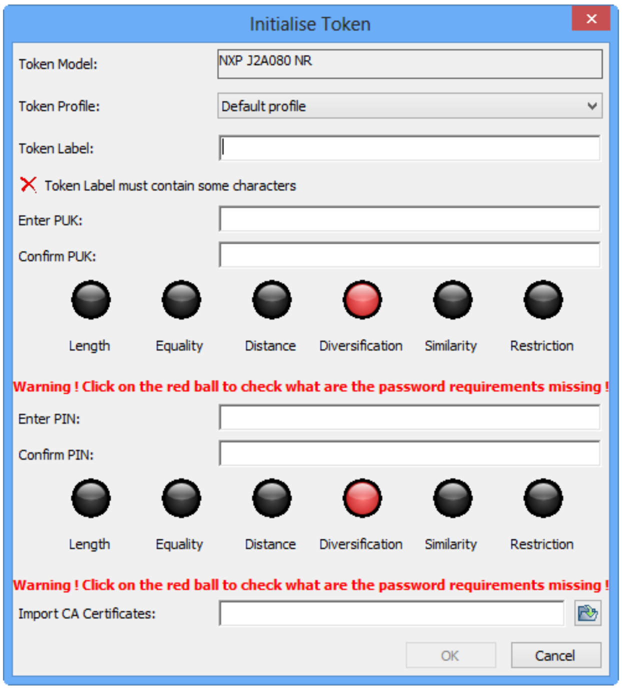
Field	Value
Token Serial Number	1114002546955659
Token Model	NXP J2A080 NR
Series Completion	yes
Applet Version	3.1.0.14
Recycle Count	Used 0 / Maximum 5
Registry card type	NXP J2A080-J3A080 (Winter AG)
CSP	SafeSign Standard Cryptographic Service Provider

Figure 79: Token Information: Recycle Count Blank Token

The total number of available recycles is 5.

3.1.5.2 Initialise Process

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



Initialise Token

Token Model: NXP J2A080 NR

Token Profile: Default profile

Token Label:

✗ Token Label must contain some characters

Enter PUK:

Confirm PUK:

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

Enter PIN:

Confirm PIN:

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

Import CA Certificates:

Figure 80: Initialise Token: Initialise Token with password requirements

When a ball is **grey**, this means that the policy is not enabled.

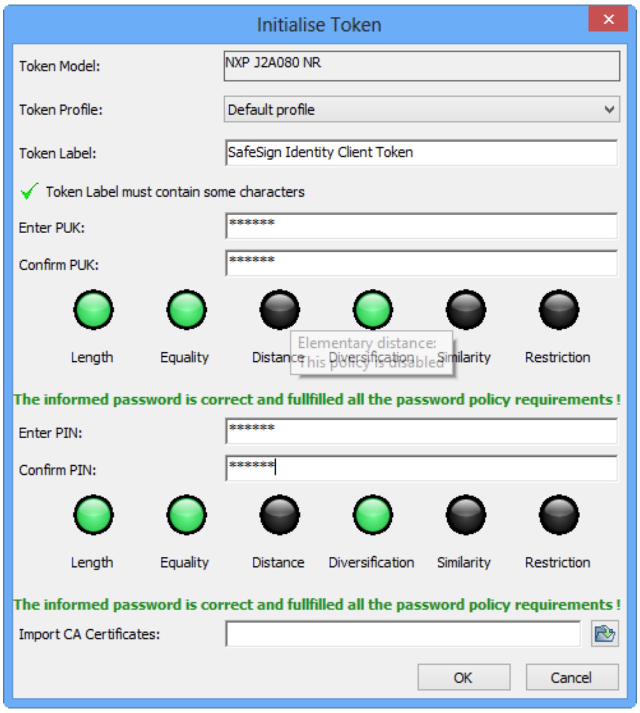
When a ball is **red**, this means that the policy is enabled, but that the entered PIN / PUK does not fulfil the policy requirements.

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

The following "balls" are active for this token:

Ball	**Label**	**Description**
Length	PIN / PUK length between 6 and 12 bytes	The length of the PIN / PUK should be at least 6 bytes, but no more than 12 bytes.
Equality	New PIN / PUK equal to confirmed new PIN / PUK	The confirmed new PIN / PUK entered should be the same as the new 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 downcase letters, upcase letters, 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."

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



Initialise Token

Token Model: NXP J2A080 NR

Token Profile: Default profile

Token Label: SafeSign Identity Client Token

✓ Token Label must contain some characters

Enter PUK: ******

Confirm PUK: ******

The informed password is correct and fullfilled all the password policy requirements !

Enter PIN: ******

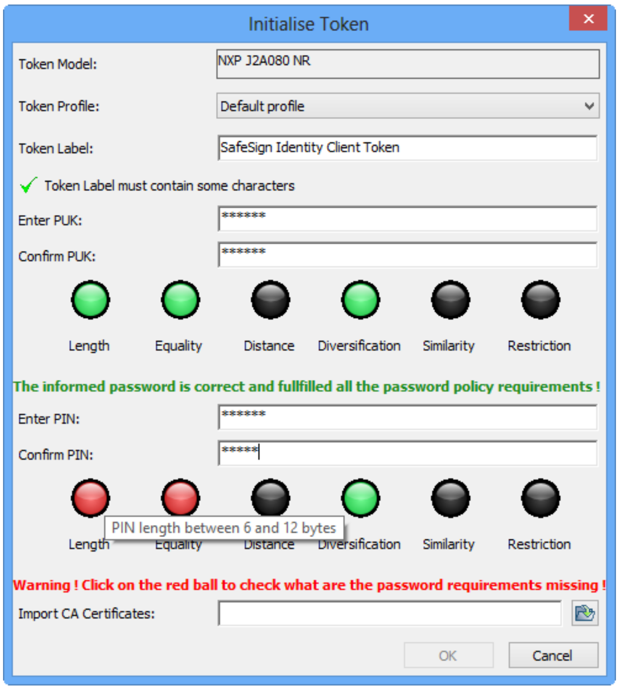
Confirm PIN: ******

The informed password is correct and fullfilled all the password policy requirements !

Import CA Certificates:

Figure 81: Initialise Token: Initialise Token completed

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



Initialise Token

Token Model: NXP J2A080 NR

Token Profile: Default profile

Token Label: SafeSign Identity Client Token

✓ Token Label must contain some characters

Enter PUK: ******

Confirm PUK: ******

The informed password is correct and fullfilled all the password policy requirements !

Enter PIN: ******

Confirm PIN: *****

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

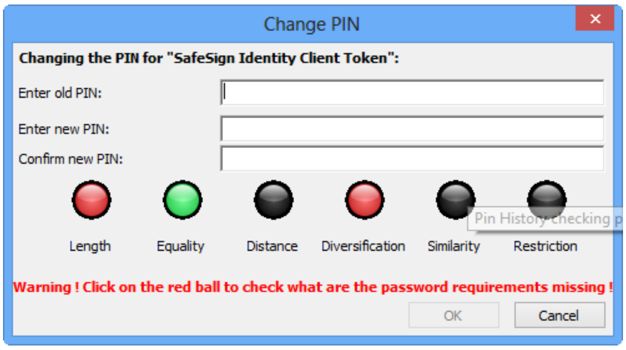
Import CA Certificates:

Figure 82: Initialise Token: Password requirements missing

In the screenshot above, the confirmed PIN does not match the entered PIN (hence the Equality ball is red); also, the length of the confirmed PIN does not match the requirement of length (hence the Length ball is red).

3.1.5.3 Change PIN

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



Change PIN

Changing the PIN for "SafeSign Identity Client Token":

Enter old PIN:

Enter new PIN:

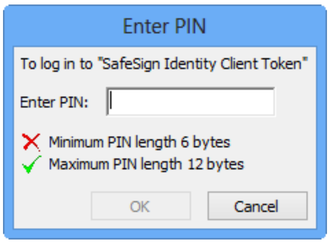
Confirm new PIN:

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

Figure 83: Change PIN: Change PIN with password requirements

3.1.5.4 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:



Enter PIN

To log in to "SafeSign Identity Client Token"

Enter PIN:

✗ Minimum PIN length 6 bytes
✓ Maximum PIN length 12 bytes

Figure 84: Enter PIN

3.1.6 Import CA Certificates

The SafeSign Identity Client Token Utility enables the import of Certificate Authority (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 2.3;
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.

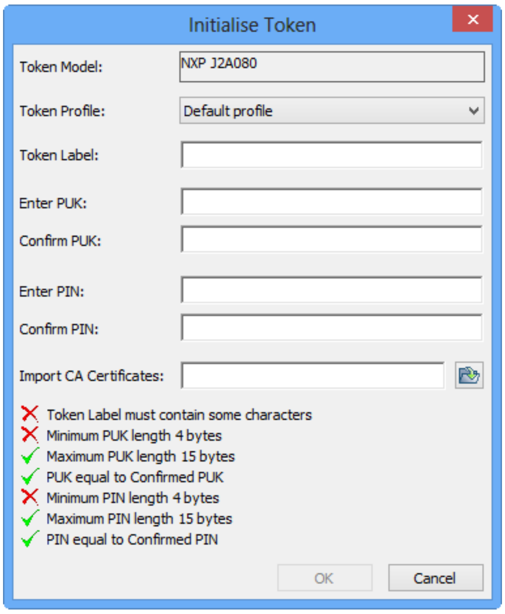
CA certificate format

SafeSign Identity Client supports the import of:

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

Select the directory where the CA certificates are located, and change the default extension from *.cer to *.crt or *.der as required.

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:



Initialise Token

Token Model: NXP J2A080

Token Profile: Default profile

Token Label:

Enter PUK:

Confirm PUK:

Enter PIN:

Confirm PIN:

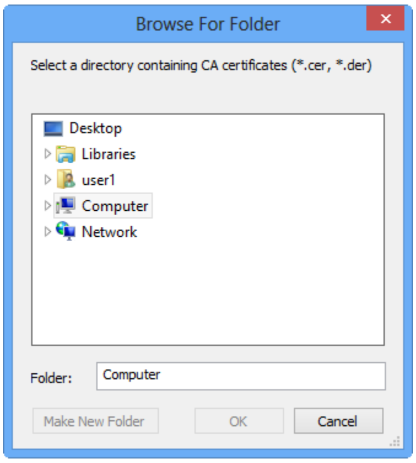
Import CA Certificates:

✗ 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

Figure 85: Initialise Token: Initialise Token

Fill in all fields according to requirements (as described in section 3.1.1) and click on the browse icon to select a directory where the CA certificates have been placed.

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



Browse For Folder

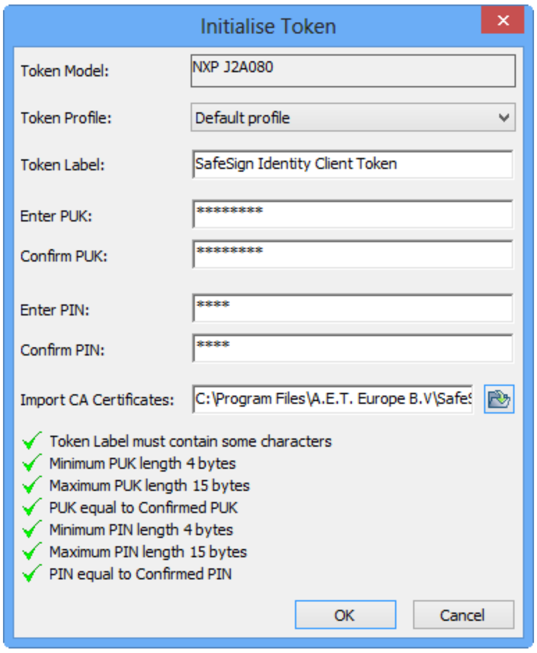
Select a directory containing CA certificates (*.cer, *.der)

Folder: Computer

Figure 86: Import CA certificates: Browse for Folder

➔ Select a directory and click **OK**

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



Initialise Token

Token Model: NXP J2A080

Token Profile: Default profile

Token Label: SafeSign Identity Client Token

Enter PUK: *********

Confirm PUK: *********

Enter PIN: ****

Confirm PIN: ****

Import CA Certificates: C:\Program Files\A.E.T. Europe B.V\SafeS

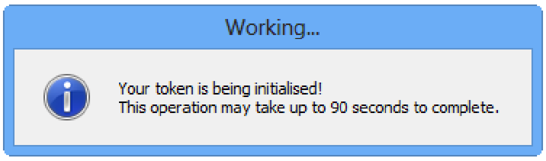
✓ Token Label must contain some characters
✓ Minimum PUK length 4 bytes
✓ Maximum PUK length 15 bytes
✓ PUK equal to Confirmed PUK
✓ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes
✓ PIN equal to Confirmed PIN

Figure 87: Initialise Token: Initialise Token completed with CA certificates

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

➔ Click **OK** to initialise the token

3 Upon clicking **OK**, you token will be initialised:



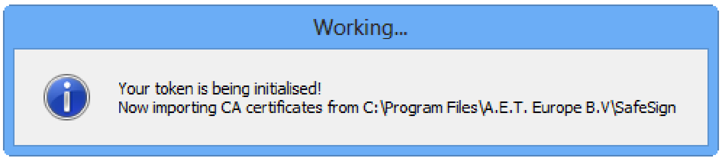
Working...

Your token is being initialised!
This operation may take up to 90 seconds to complete.

Figure 88: Initialise Token: Your token is being initialised

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

4 When the CA certificate(s) is imported as part of the initialisation process, you will see the following dialog:

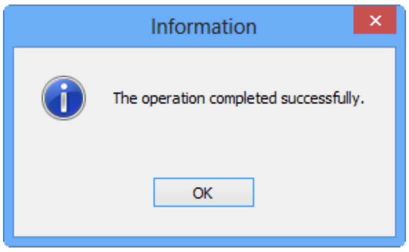


Working...

Your token is being initialised!
Now importing CA certificates from C:\Program Files\A.E.T. Europe B.V\SafeSign

Figure 89: Initialise Token: Now importing CA certificates

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



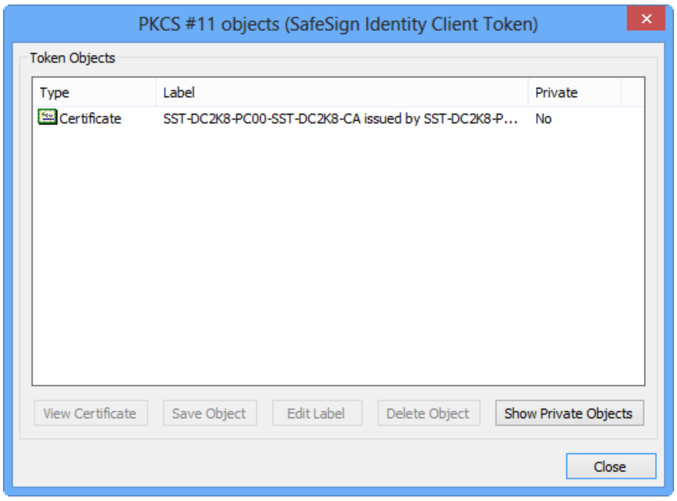
Information

The operation completed successfully.

Figure 90: Initialise Token: The operation completed successfully

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

As can be seen in the *PKCS#11 objects* dialog of the Token Administration Utility (only), the CA certificate is now imported,:



PKCS #11 objects (SafeSign Identity Client Token)

Token Objects

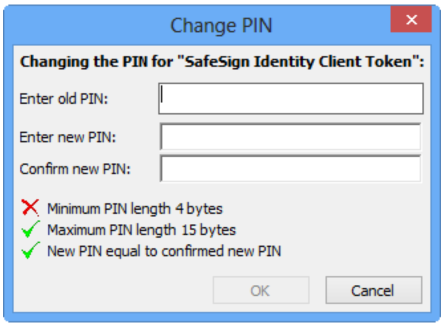
Type	Label	Private
Certificate	SST-DC2K8-PC00-SST-DC2K8-CA issued by SST-DC2K8-P...	No

Figure 91: Token Administration Utility: PKCS#11 objects

3.2 Change PIN

The SafeSign Identity Client Token Administration Utility enables you to change the PIN for your SafeSign Identity Client Token.

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



Change PIN

Changing the PIN for "SafeSign Identity Client Token":

Enter old PIN:

Enter new PIN:

Confirm new PIN:

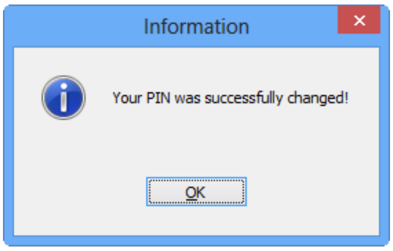
✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes
✓ New PIN equal to confirmed new PIN

Figure 92: Change PIN: Change PIN

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

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

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



Information

Your PIN was successfully changed!

Figure 93: Change PIN: Your PIN was successfully changed

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

3.2.1 PIN information

Every time you enter your PIN for the SafeSign Identity Client Token, either when asked to do so in applications (e.g. in the *Enter PIN* dialog for Microsoft applications) or within the SafeSign Identity Client Token Utility, SafeSign Identity Client will provide you with information as to the status of the PIN.

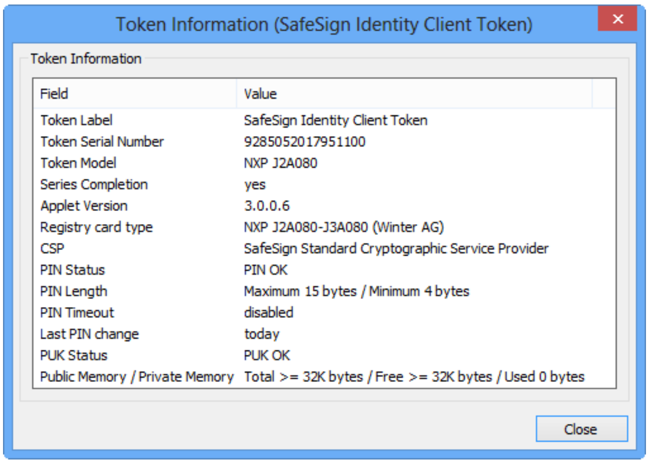
Note that by default, you have **three** attempts to enter the correct PIN[1] and that SafeSign Identity Client will register this and give you information as to the status of the PIN. When you enter an incorrect PIN three times, the token will be LOCKED and you should use the *Unlock PIN* item from the **Token** menu (as described in section 3.4).

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).

[1] Note that your administrator may have changed the maximum number of PIN retries.

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

1. PIN is "*OK*" (as in Figure 94 below):



Token Information (SafeSign Identity Client Token)

Token Information

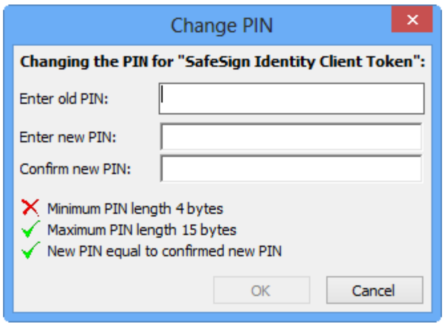
Field	Value
Token Label	SafeSign Identity Client Token
Token Serial Number	9285052017951100
Token Model	NXP J2A080
Series Completion	yes
Applet Version	3.0.0.6
Registry card type	NXP J2A080-J3A080 (Winter AG)
CSP	SafeSign Standard Cryptographic Service Provider
PIN Status	PIN OK
PIN Length	Maximum 15 bytes / Minimum 4 bytes
PIN Timeout	disabled
Last PIN change	today
PUK Status	PUK OK
Public Memory / Private Memory	Total >= 32K bytes / Free >= 32K bytes / Used 0 bytes

Figure 94: Token Information: PIN Status

2. "PIN has been entered incorrectly at least once"
3. "One final attempt left to enter the PIN correctly"
4. PIN is "*LOCKED*"

Also, when you perform an operation within the SafeSign Identity Client Token Utility, such as *Change 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):



Change PIN

Changing the PIN for "SafeSign Identity Client Token":

Enter old PIN:

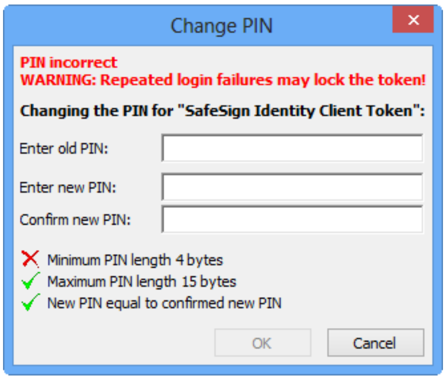
Enter new PIN:

Confirm new PIN:

✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes
✓ New PIN equal to confirmed new PIN

Figure 95: Change PIN: Change PIN

(2) When the PIN has been entered incorrectly:



Change PIN

PIN incorrect
WARNING: Repeated login failures may lock the token!

Changing the PIN for "SafeSign Identity Client Token":

Enter old PIN:

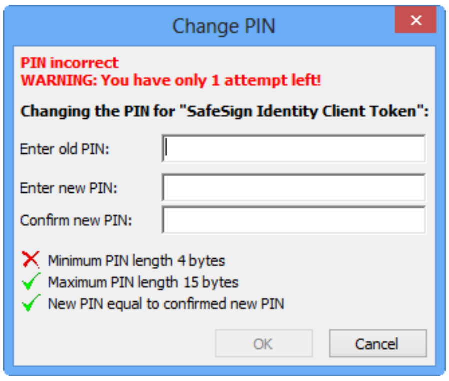
Enter new PIN:

Confirm new PIN:

✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes
✓ New PIN equal to confirmed new PIN

Figure 96: Change PIN: Repeated login failures may lock the token

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



Change PIN

PIN incorrect
WARNING: You have only 1 attempt left!

Changing the PIN for "SafeSign Identity Client Token":

Enter old PIN:

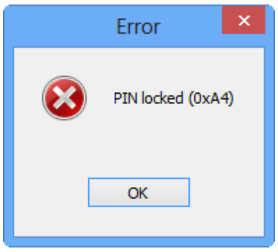
Enter new PIN:

Confirm new PIN:

✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes
✓ New PIN equal to confirmed new PIN

Figure 97: Change PIN: You have only 1 attempt left

(4) When the PIN is locked:



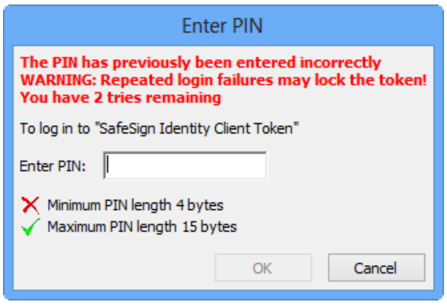
Error

PIN locked (0xA4)

Figure 98: Change PIN: PIN locked

Wrong PIN in different item

When you close one menu item in the SafeSign Identity Client Token Utility and you enter an incorrect PIN in another item, you will be notified of this ("*The PIN has previously been entered incorrectly*") and the status of incorrect PIN entries. For example, the dialog below indicates you have already entered an incorrect PIN in another item and that you have only two attempts left to enter the correct PIN:



Enter PIN

The PIN has previously been entered incorrectly
WARNING: Repeated login failures may lock the token!
You have 2 tries remaining

To log in to "SafeSign Identity Client Token"

Enter PIN:

✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes

Figure 99: Enter PIN: The PIN has previously been entered incorrectly

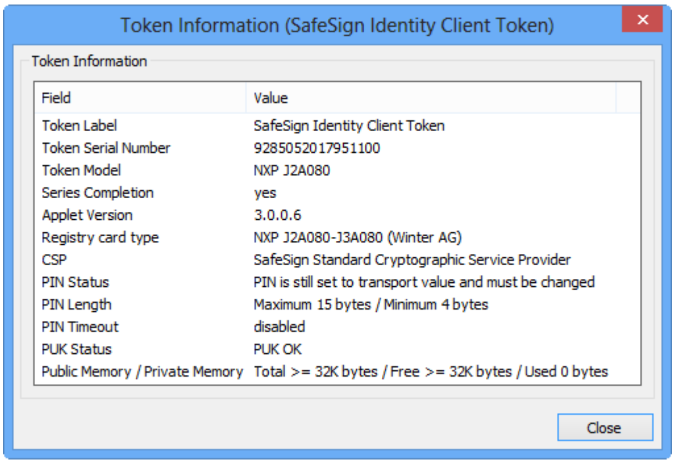
3.3 Change Transport PIN

Your SafeSign Identity Client 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 code before a token can be used. Setting a Transport PIN can be useful for security reasons, for example when you want to be certain that a user (consciously) sets his / her own PIN prior to any signature token operations.

Note that the *Change Transport PIN* item will only be available when the token has a Transport PIN. If not, the item *Change PIN* will be available.

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



Field	Value
Token Label	SafeSign Identity Client Token
Token Serial Number	9285052017951100
Token Model	NXP J2A080
Series Completion	yes
Applet Version	3.0.0.6
Registry card type	NXP J2A080-J3A080 (Winter AG)
CSP	SafeSign Standard Cryptographic Service Provider
PIN Status	PIN is still set to transport value and must be changed
PIN Length	Maximum 15 bytes / Minimum 4 bytes
PIN Timeout	disabled
PUK Status	PUK OK
Public Memory / Private Memory	Total >= 32K bytes / Free >= 32K bytes / Used 0 bytes

Figure 100: Token Information: PIN is still set to transport value

Then in the Token Utility, the item *Change PIN* is not available; instead the option *Change transport PIN* is available:

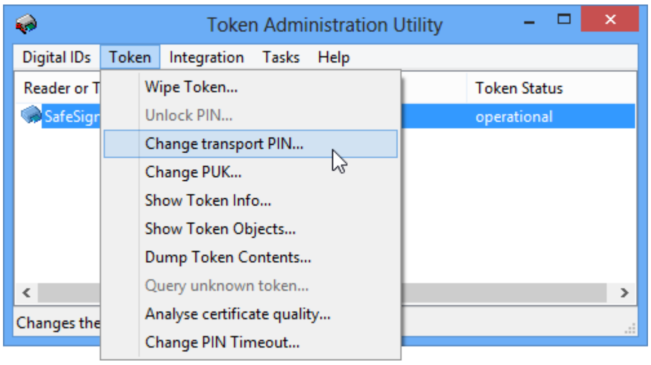
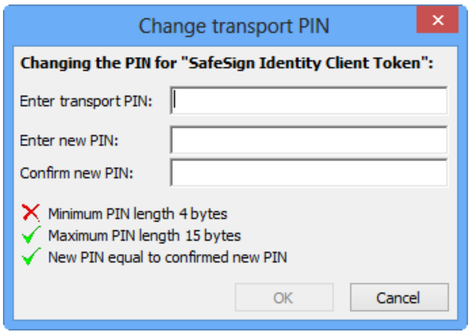


Figure 101: Token Utility: Change transport PIN

➔ Select Change Transport PIN (as above)

This will open the *Change transport PIN* dialog:



Change transport PIN

Changing the PIN for "SafeSign Identity Client Token":

Enter transport PIN:

Enter new PIN:

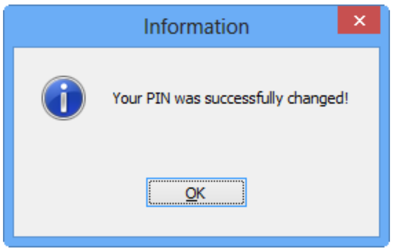
Confirm new PIN:

☒ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes
✓ New PIN equal to confirmed new PIN

Figure 102: Change transport PIN: Change Transport PIN

➔ Enter the correct transport PIN, a new (personal) PIN for the token and confirm the new PIN

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



Information

Your PIN was successfully changed!

Figure 103: Change transport PIN: Your PIN was successfully changed

➔ Click **OK**

You can now use your token with your own personal PIN.

3.4 Unlock PIN

The SafeSign Identity Client Token Utility enables you to unlock the PIN for your SafeSign Identity Client Token (when your PIN is locked, as in Figure 98).

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

There are two ways of unlocking the PIN: unlocking the PIN using the PUK or unlocking the PIN via off-line PIN unlock.

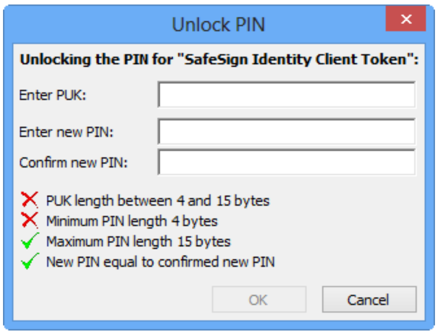
Section 3.4.1 describes the first option

section 3.4.2 describes the second option

3.4.1 Unlock using the PUK

In order to unlock the PIN, select *Unlock PIN* from the **Token** menu[1].

This will open the following dialog:



Unlock PIN

Unlocking the PIN for "SafeSign Identity Client Token":

Enter PUK:

Enter new PIN:

Confirm new PIN:

✗ PUK length between 4 and 15 bytes
✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes
✓ New PIN equal to confirmed new PIN

Figure 104: Token Utility: Unlock PIN

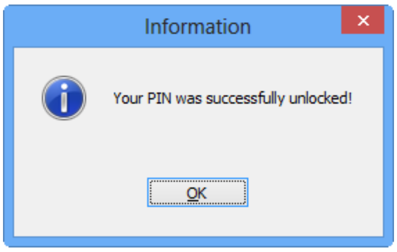
This dialog will identify the token of which you want to unlock the PIN ("SafeSign Identity Client Token" in our example).

Enter the current PUK, a new PIN and confirm the new PIN.

Only when you enter the correct PUK and a new and confirmed PIN that are the same (and fulfil the PIN length requirements), will the **OK** button be available.

➔ Click **OK** to unlock the PIN

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



Information

Your PIN was successfully unlocked!

Figure 105: Unlock PIN: Your PIN was successfully unlocked

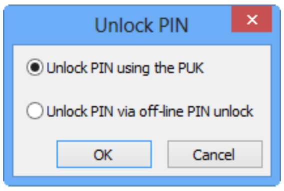
➔ Click **OK** to close this dialog box.

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*).

3.4.2 Unlock via off-line PIN unlock

The SafeSign Identity Client Token Utility has built-in support for off-line PIN unlock.

1 When enabled, the user will be allowed to choose how to unlock the PIN, upon selecting *Unlock PIN* from the **Token** menu:



Unlock PIN

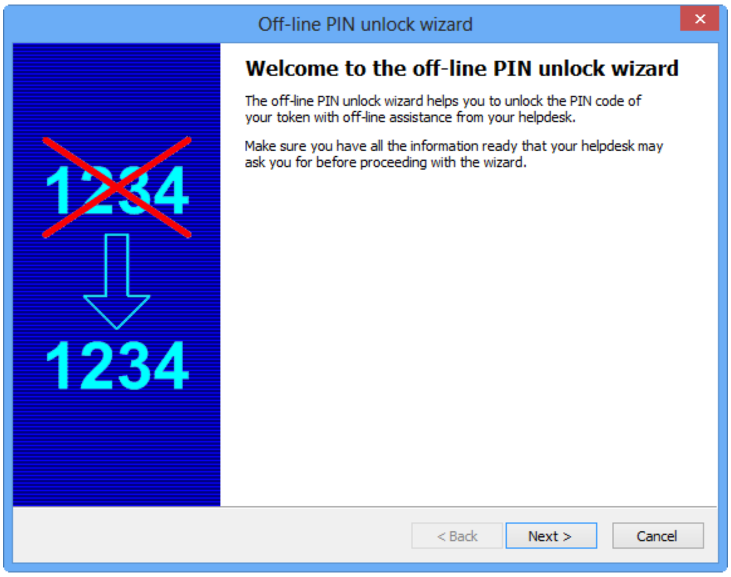
● Unlock PIN using the PUK

○ Unlock PIN via off-line PIN unlock

Figure 106: Unlock PIN

[1] When off-line PIN unlock is enabled, you will be asked to choose which method you want to use to unlock your PIN, as in Figure 106.

2 Select the option "Unlock PIN via off-line PIN unlock" to start the off-line PIN unlock wizard, which starts with the welcome page:



Off-line PIN unlock wizard

Welcome to the off-line PIN unlock wizard

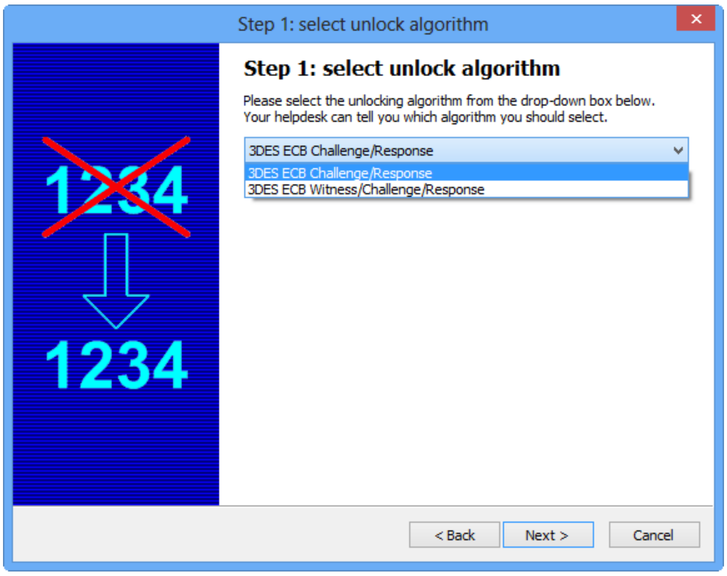
The off-line PIN unlock wizard helps you to unlock the PIN code of your token with off-line assistance from your helpdesk.

Make sure you have all the information ready that your helpdesk may ask you for before proceeding with the wizard.

Figure 107: Off-line PIN unlock wizard: Welcome to the off-line PIN unlock wizard[1]

➔ 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:



Step 1: select unlock algorithm

Step 1: select unlock algorithm

Please select the unlocking algorithm from the drop-down box below. Your helpdesk can tell you which algorithm you should select.

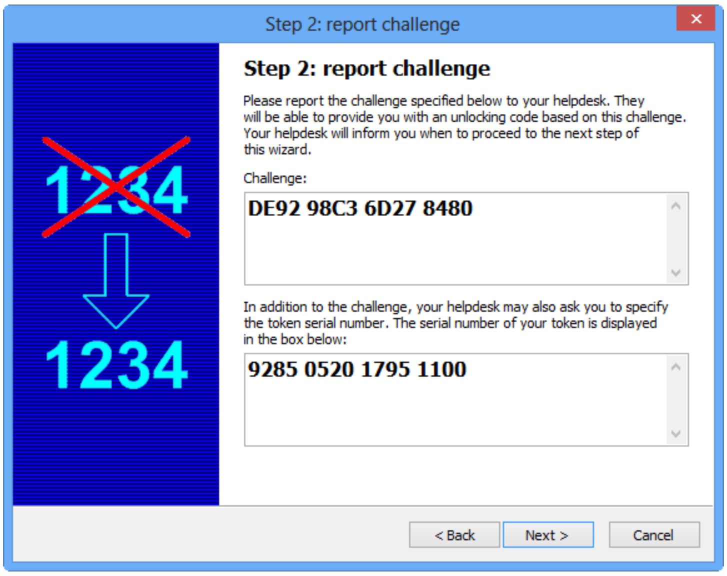
3DES ECB Challenge/Response
3DES ECB Challenge/Response
3DES ECB Witness/Challenge/Response

Figure 108: Off-line PIN unlock wizard: Step 1: select unlock algorithm

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

[1] This page contains an optional text telling the user how he/she can contact the helpdesk. The content of this text field is always "You can contact your helpdesk at %s.", where %s is replace by the string value HelpdeskContact under the [HKEY_LOCAL_MACHINE\SOFTWARE\A.E.T. Europe B.V.\SafeSign\2.0] registry key. This text field is displayed on all pages of the wizard if this registry value is set.

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



Step 2: report challenge

Please report the challenge specified below to your helpdesk. They will be able to provide you with an unlocking code based on this challenge. Your helpdesk will inform you when to proceed to the next step of this wizard.

Challenge:

DE92 98C3 6D27 8480

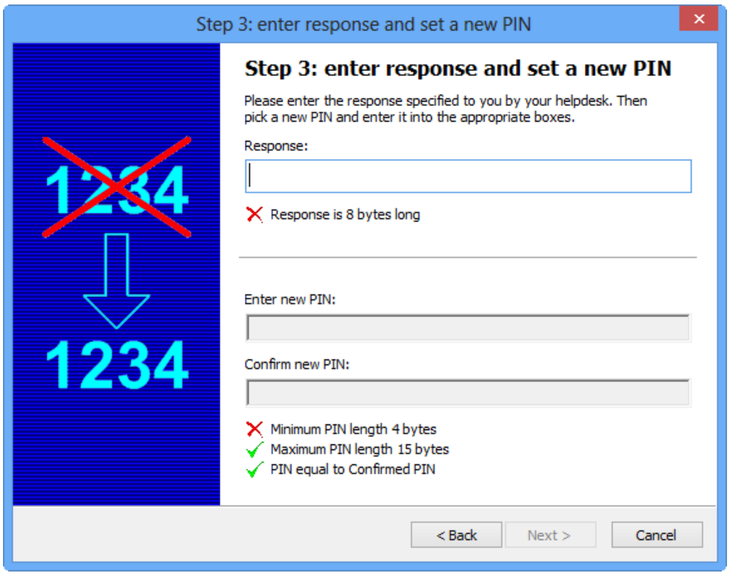
In addition to the challenge, your helpdesk may also ask you to specify the token serial number. The serial number of your token is displayed in the box below:

9285 0520 1795 1100

Figure 109: Off-line PIN unlock wizard: Step 2: report challenge

➔ Once the challenge has been reported to your helpdesk and a response given, click **Next** to continue

5 After clicking **Next**, in the next step you can enter the response you have been given by the helpdesk employee, and you are allowed to enter a new PIN code for the token:



Step 3: enter response and set a new PIN

Please enter the response specified to you by your helpdesk. Then pick a new PIN and enter it into the appropriate boxes.

Response:

✗ Response is 8 bytes long

Enter new PIN:

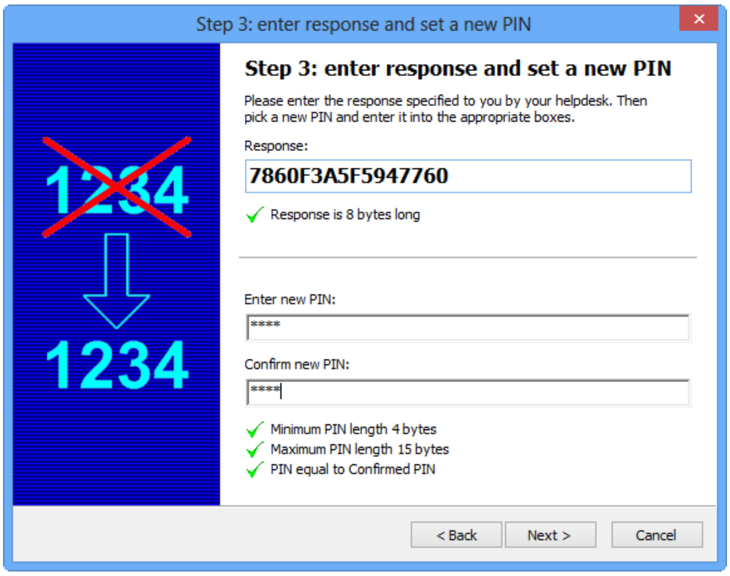
Confirm new PIN:

✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes
✓ PIN equal to Confirmed PIN

Figure 110: 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 as follows:


Step 3: enter response and set a new PIN

Step 3: enter response and set a new PIN

Please enter the response specified to you by your helpdesk. Then pick a new PIN and enter it into the appropriate boxes.

Response: 7860F3A5F5947760

✓ Response is 8 bytes long

Enter new PIN: ****

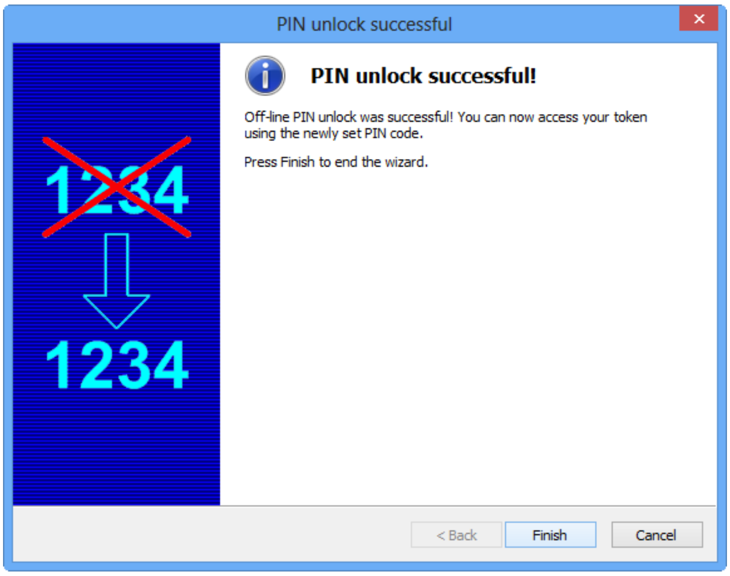
Confirm new PIN: ****

✓ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes
✓ PIN equal to Confirmed PIN

Figure 111: Off-line PIN unlock wizard: Step 3: enter response and set a new PIN completed

➔ Click **Next** to continue

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


PIN unlock successful

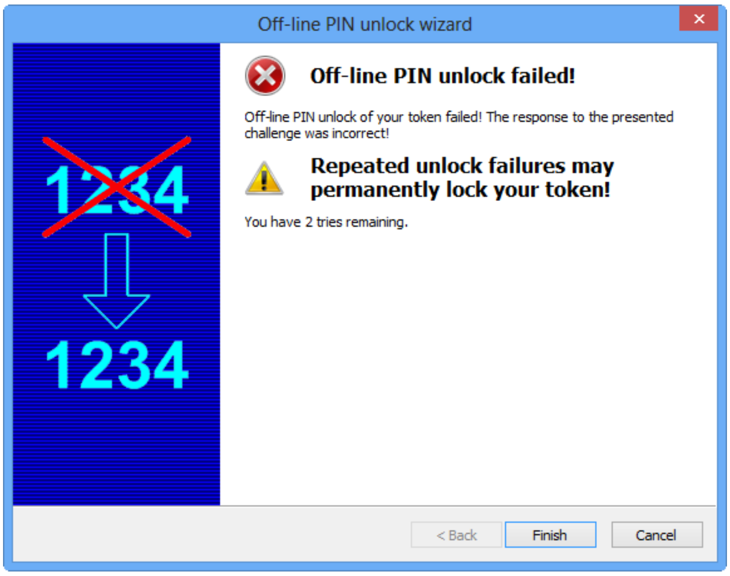
PIN unlock successful!

Off-line PIN unlock was successful! You can now access your token using the newly set PIN code.

Press Finish to end the wizard.

Figure 112: Off-line PIN unlock wizard: PIN unlock successful

Or failed:



Off-line PIN unlock wizard

Off-line PIN unlock failed!

Off-line PIN unlock of your token failed! The response to the presented challenge was incorrect!

Repeated unlock failures may permanently lock your token!

You have 2 tries remaining.

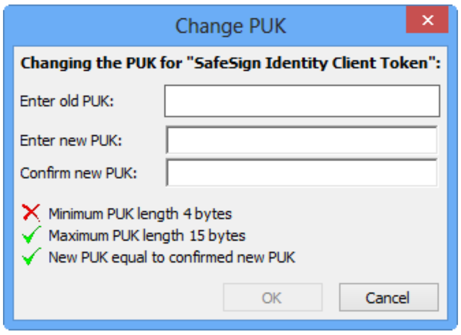
Figure 113: Off-line PIN unlock wizard: Off-line PIN unlock failed

If off-line PIN unlock fails after the two remaining tries, you can only unlock the PIN using the PUK, as described in section 3.4.1.

3.5 Change PUK

The SafeSign Identity Client Token Utility enables you to change the PUK for your SafeSign Identity Client Token.

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



Change PUK

Changing the PUK for "SafeSign Identity Client Token":

Enter old PUK:

Enter new PUK:

Confirm new PUK:

✗ Minimum PUK length 4 bytes
✓ Maximum PUK length 15 bytes
✓ New PUK equal to confirmed new PUK

Figure 114: Change PUK: Change PUK

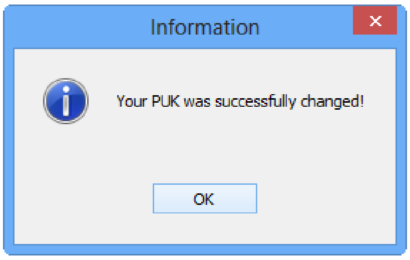
This dialog will identify the token of which you want to change the PUK ("SafeSign Identity Client Token" in our example).

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 are the same (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:



Your PUK was successfully changed!

Figure 115: Change PUK: Your PUK was successfully changed

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

Your PUK is changed.

3.5.1 PUK information

Every time you enter your PUK for the SafeSign Identity Client Token, which is mostly likely done within the SafeSign Identity Client Token Utility *Change PIN* or *Change PUK* item, SafeSign Identity Client will provide you information with regard to the status of the PUK.

Note that you have **three** attempts to enter the correct PUK[1] and that SafeSign Identity Client will register this and give you information as to the status of the PUK. When you enter an incorrect PUK three times, the PUK will be LOCKED.

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).

Note

When you enter an incorrect PUK three times, the PUK will be locked and cannot be unlocked.

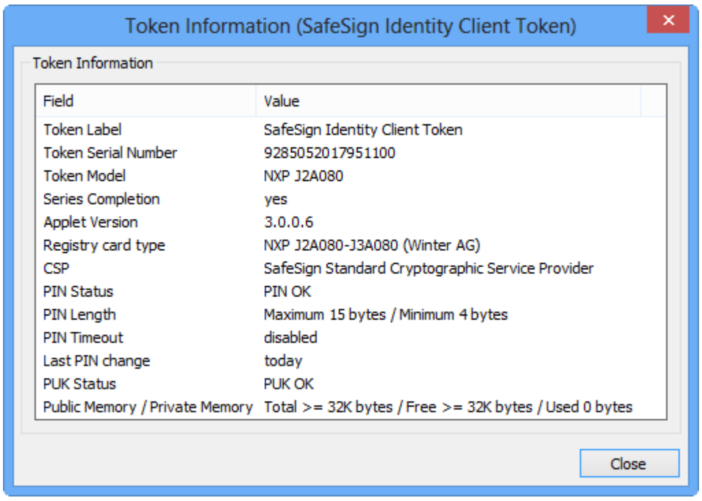
For a test completed token, this implies you will have to initialise the token again, thereupon losing all data stored on the token.

For a series completed token, your token will become unusable, as you cannot wipe the contents of your token, for in order to do so, you will need the PUK.

[1] Note that your administrator may have changed the maximum number of PUK retries.

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

1. PUK is "*OK*" (as in Figure 116 below)



Token Information (SafeSign Identity Client Token)

Token Information

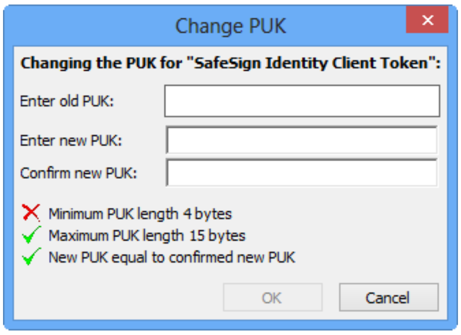
Field	Value
Token Label	SafeSign Identity Client Token
Token Serial Number	9285052017951100
Token Model	NXP J2A080
Series Completion	yes
Applet Version	3.0.0.6
Registry card type	NXP J2A080-J3A080 (Winter AG)
CSP	SafeSign Standard Cryptographic Service Provider
PIN Status	PIN OK
PIN Length	Maximum 15 bytes / Minimum 4 bytes
PIN Timeout	disabled
Last PIN change	today
PUK Status	PUK OK
Public Memory / Private Memory	Total >= 32K bytes / Free >= 32K bytes / Used 0 bytes

Figure 116: Token Information: PUK Status

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

Also, when you perform an operation within the SafeSign Identity Client Token Utility, 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 possible notifications are possible:

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



Change PUK

Changing the PUK for "SafeSign Identity Client Token":

Enter old PUK:

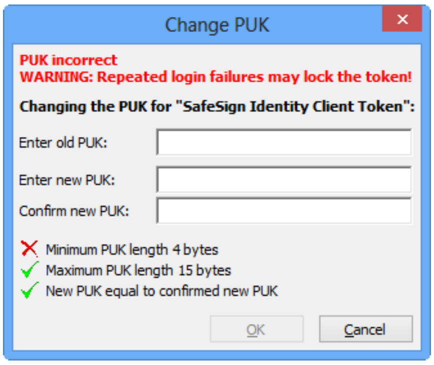
Enter new PUK:

Confirm new PUK:

✗ Minimum PUK length 4 bytes
✓ Maximum PUK length 15 bytes
✓ New PUK equal to confirmed new PUK

Figure 117: Change PUK: Change PUK

(2) When the PUK has been entered incorrectly:



Change PUK

PUK incorrect
WARNING: Repeated login failures may lock the token!

Changing the PUK for "SafeSign Identity Client Token":

Enter old PUK:

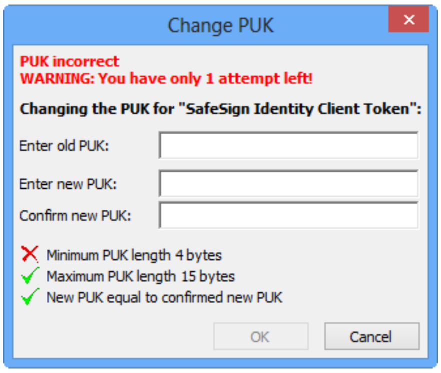
Enter new PUK:

Confirm new PUK:

✗ Minimum PUK length 4 bytes
✓ Maximum PUK length 15 bytes
✓ New PUK equal to confirmed new PUK

Figure 118: Change PUK: Repeated login failures may lock the token

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



Change PUK

PUK incorrect
WARNING: You have only 1 attempt left!

Changing the PUK for "SafeSign Identity Client Token":

Enter old PUK:

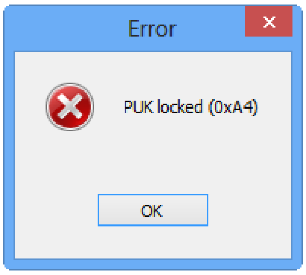
Enter new PUK:

Confirm new PUK:

✗ Minimum PUK length 4 bytes
✓ Maximum PUK length 15 bytes
✓ New PUK equal to confirmed new PUK

Figure 119: Change PUK: You have only 1 attempt left

(4) When the PUK is locked:



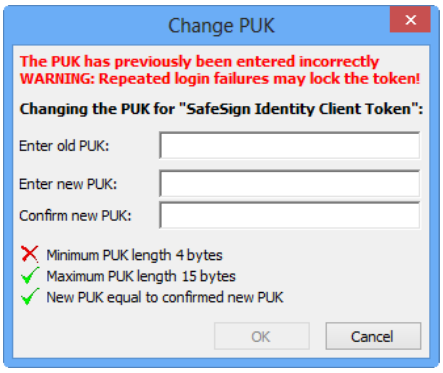
Error

PUK locked (0xA4)

Figure 120: Change PUK: PUK locked

Wrong PUK in different item

When you close one menu item in the SafeSign Identity Client Token Administration Utility and you enter an incorrect PUK in another item, you will be notified of this ("*Previous attempts to use the PUK have failed*") and the status of incorrect PUK entries. For example, the dialog below indicates you have already entered an incorrect PUK in another item and that you have only two attempts left to enter the correct PUK:



Change PUK

The PUK has previously been entered incorrectly
WARNING: Repeated login failures may lock the token!

Changing the PUK for "SafeSign Identity Client Token":

Enter old PUK:

Enter new PUK:

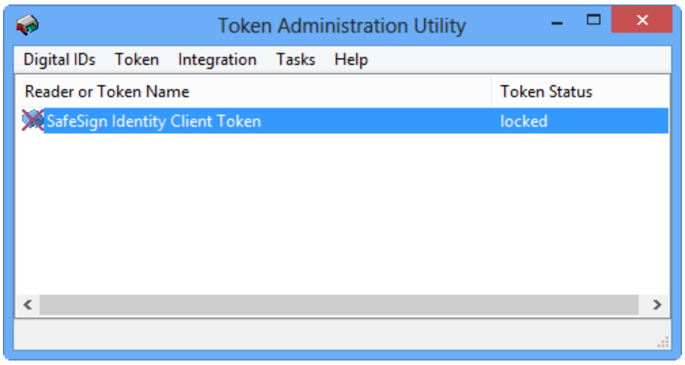
Confirm new PUK:

✗ Minimum PUK length 4 bytes
✓ Maximum PUK length 15 bytes
✓ New PUK equal to confirmed new PUK

Figure 121: Change PUK: The PUK has previously been entered incorrectly

Token Locked

When both the PIN and PUK of the token have been locked, the Token Utility will look like this:



Reader or Token Name	Token Status
SafeSign Identity Client Token	locked

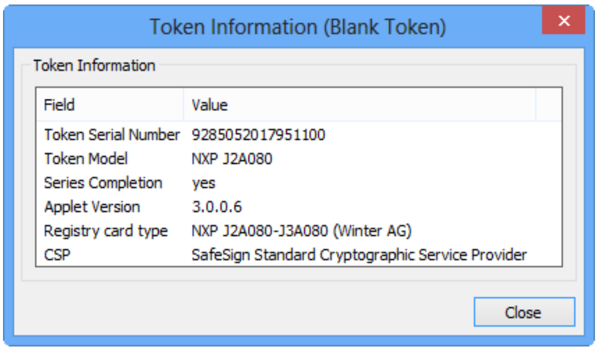
Figure 122: Token Utility: Locked token

Note that in this case, only a test completion token can be (re-)initialised (deleting all contents and rewriting the entire file structure), whereas a series completion token has become useless.

3.6 Show Token Info

The *Token Information* dialog (**Token > Show Token Info**) displays some information on the token inserted. AET SafeSign Support will usually ask for a screenshot of this dialog in case of issues.

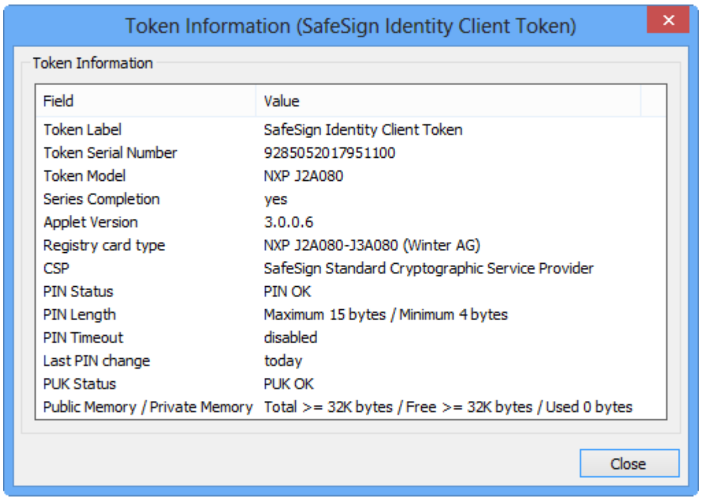
When the token is not initialised, the *Token Information* dialog will (probably) look like this[1]:



Field	Value
Token Serial Number	9285052017951100
Token Model	NXP J2A080
Series Completion	yes
Applet Version	3.0.0.6
Registry card type	NXP J2A080-J3A080 (Winter AG)
CSP	SafeSign Standard Cryptographic Service Provider

Figure 123: Token Utility: Token Information (uninitialised token)

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



Field	Value
Token Label	SafeSign Identity Client Token
Token Serial Number	9285052017951100
Token Model	NXP J2A080
Series Completion	yes
Applet Version	3.0.0.6
Registry card type	NXP J2A080-J3A080 (Winter AG)
CSP	SafeSign Standard Cryptographic Service Provider
PIN Status	PIN OK
PIN Length	Maximum 15 bytes / Minimum 4 bytes
PIN Timeout	disabled
Last PIN change	today
PUK Status	PUK OK
Public Memory / Private Memory	Total >= 32K bytes / Free >= 32K bytes / Used 0 bytes

Figure 124: Token Utility: Token Information (initialised token)

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

3.6.1 Token Label

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

3.6.2 Token Serial Number

Displays the serial number of the token (usually the chip serial number).

3.6.3 Token Model

Displays the token model and version, as recognised by the SafeSign Identity Client software.

[1] In this example, the SafeSign Identity Client applet is installed, as it usually is for production cards. When the applet is not installed, no serial number will be displayed.

3.6.4 Series Completion

Displays whether the token is a test (completed) or series/production (completed) token.

When the token is in test, it will say [No], meaning you can re-initialise the token[1].

When the token is in series/production, it will say [Yes], meaning you can only wipe the token contents.

3.6.5 Applet Version

Displays the version of the applet installed on the token.

3.6.6 Registry card type

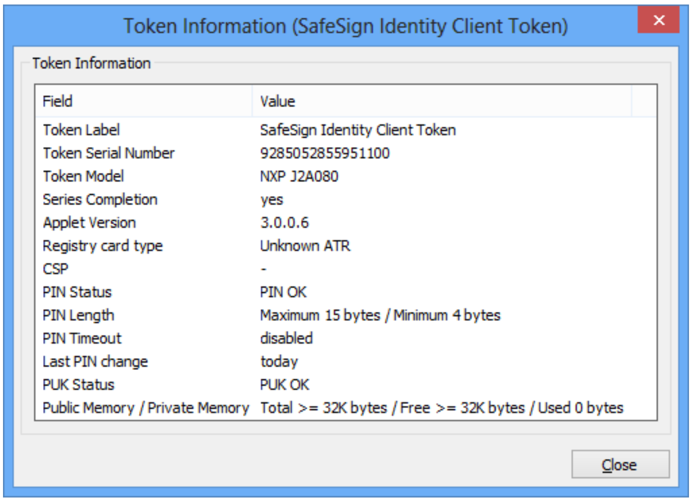
Displays the card name as it is recorded in the appropriate place in the registry[2], associating the ATR of the token with the SafeSign Cryptographic Service Provider for use with Microsoft applications.

3.6.6.1 Unknown ATR

Note that it may occur that the token is recognised (Token Model), but that the ATR is unknown. When the ATR of a token is not registered correctly for use in Microsoft CryptoAPI applications (while the token model is recognised), this could lead to problems with, for example, Windows smart card logon.

When trying to log on 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 requires drivers that are not present on this system".

If the token has an unknown ATR, the registry card type will display:



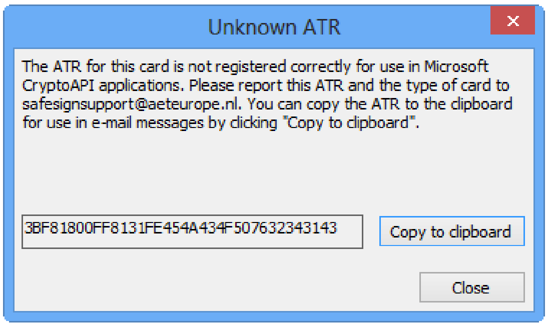
Field	Value
Token Label	SafeSign Identity Client Token
Token Serial Number	9285052855951100
Token Model	NXP J2A080
Series Completion	yes
Applet Version	3.0.0.6
Registry card type	Unknown ATR
CSP	-
PIN Status	PIN OK
PIN Length	Maximum 15 bytes / Minimum 4 bytes
PIN Timeout	disabled
Last PIN change	today
PUK Status	PUK OK
Public Memory / Private Memory	Total >= 32K bytes / Free >= 32K bytes / Used 0 bytes

Figure 125: Show Token Info: Unknown ATR

[1] Note that when you are using a Java Card with a custom keyset, you will not be able to re-initialise the token when the applet is installed in test. Re-initialisation of a Java card is only possible when the card has a test key set and the applet installed in test.

[2] HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\

In addition, the following dialog will be displayed each time you insert the token with the Token Utility opened:



Unknown ATR

The ATR for this card is not registered correctly for use in Microsoft CryptoAPI applications. Please report this ATR and the type of card to safesignsupport@aeteurope.nl. You can copy the ATR to the clipboard for use in e-mail messages by clicking "Copy to clipboard".

3BF81800FF8131FE454A434F507632343143

Figure 126: Unknown ATR: The ATR is not registered correctly

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 Identity Client and Cryptographic Service Provider) to the clipboard, so you can copy it in an e-mail message (for example).

Please contact your supplier to provide you with a SafeSign Identity Client version that does support this token or take further action towards obtaining such a version.

Note that in Windows 7, 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 http://support.microsoft.com/kb/976832 for more details.

3.6.7 CSP

Displays the configured CSP for the token, which should be the SafeSign Standard Cryptographic Service Provider.

3.6.8 PIN Status

See also section 3.2.1.

Displays the status of the PIN:

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

3.6.9 PIN Length

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

3.6.10 PIN Timeout

See also section 3.11.

Displays the status of the PIN Timeout setting, which is by default 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. For example, when using Outlook to send signed e-mail messages or using Adobe Reader to sign a document, you will be asked to enter your PIN again when the maximum amount of time has passed since the last time you logged in to the token.

The timeout value for a particular token can be set in the Token Administration Utility[1], through the menu Token > Change PIN Timeout, if the (initialised) token is inserted and the correct PIN is entered.

[1] The Token Management Utility does not include this option.

3.6.11 Last PIN change

It is possible (through the registry) to set a limit on the validity of the PIN[1]. When set, you will be notified that your PIN is invalid or will be invalid in a number of days and you will be asked to change it.

However, changing the PIN to a new value is not enforced (so you can enter the same / current PIN and it does not have to conform to any PIN policies).

Whether enabled or not, the *Token Information* dialog of the Token Utility will include an item called 'Last PIN change' and record how many days ago the PIN was set / changed.

3.6.12 PUK Status

See also section 3.5.1.

Displays the status of the PUK:

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

3.6.13 Public Memory / Private Memory

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

Note that the private memory is not the place where the private keys are stored. According to and in accordance with the PKCS#15 standard, private keys are stored in a directory, while the private memory is used to store for example secure data objects. This explains why the amount of private space does not decrease when a token is inserted that contains a (number of) private key(s).

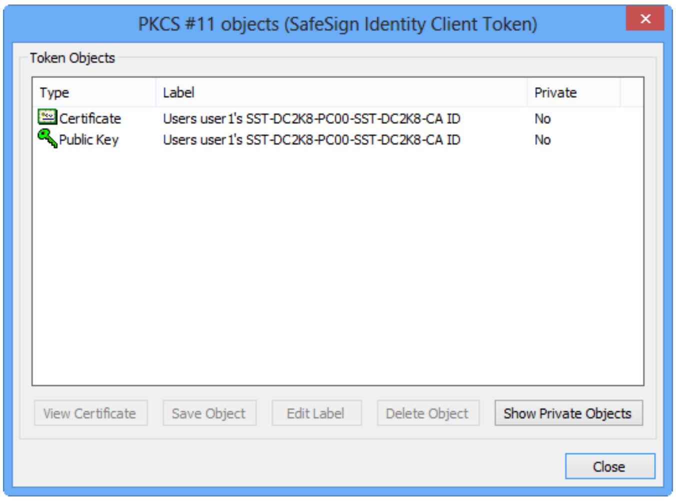
[1] PinValidityDayPeriod in HKEY_LOCAL_MACHINE\Software\ A.E.T. Europe B.V.\SafeSign\2.0\. By default it is set to 0 (zero), which means that it is not set.

3.7 Show Token Objects

This feature is only available in the Token Administration Utility.

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

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



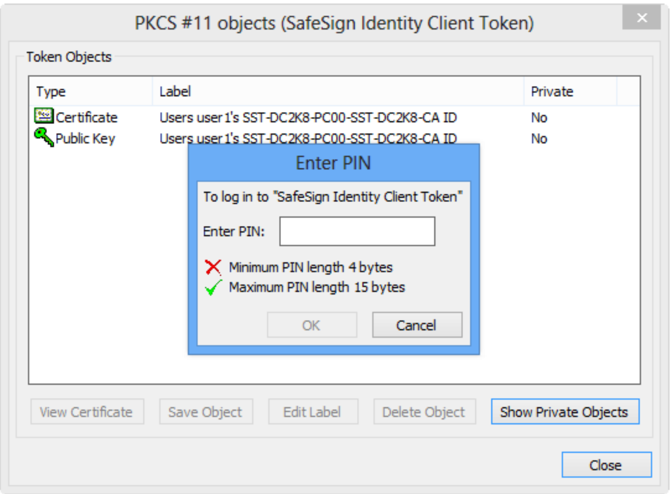
Type	Label	Private
Certificate	Users user 1's SST-DC2K8-PC00-SST-DC2K8-CA ID	No
Public Key	Users user 1's SST-DC2K8-PC00-SST-DC2K8-CA ID	No

Figure 127: PKCS #11 objects: Token Objects

This dialog will display the Public token objects.

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

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



Type	Label	Private
Certificate	Users user 1's SST-DC2K8-PC00-SST-DC2K8-CA ID	No
Public Key	Users user 1's SST-DC2K8-PC00-SST-DC2K8-CA ID	No

To log in to "SafeSign Identity Client Token"

Enter PIN:

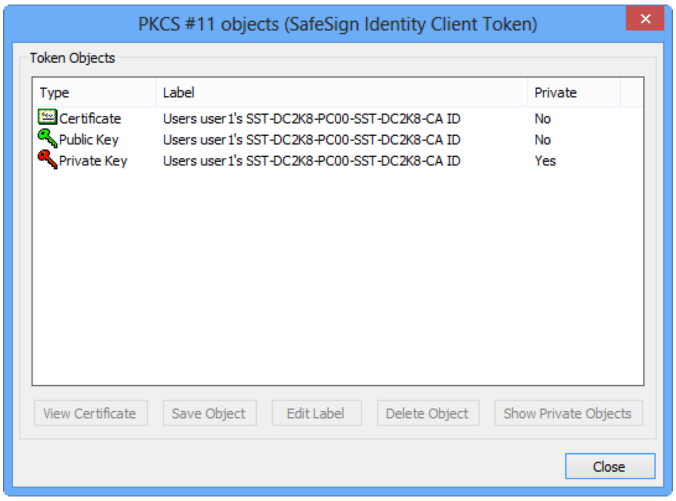
✗ Minimum PIN length 4 bytes

✓ Maximum PIN length 15 bytes

Figure 128: PKCS #11 Objects: Enter PIN

➔ Enter the correct PIN to display the private objects on the token

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



PKCS #11 objects (SafeSign Identity Client Token)

Token Objects

Type	Label	Private
Certificate	Users user1's SST-DC2K8-PC00-SST-DC2K8-CA ID	No
Public Key	Users user1's SST-DC2K8-PC00-SST-DC2K8-CA ID	No
Private Key	Users user1's SST-DC2K8-PC00-SST-DC2K8-CA ID	Yes

Figure 129: PKCS #11 Objects: All objects

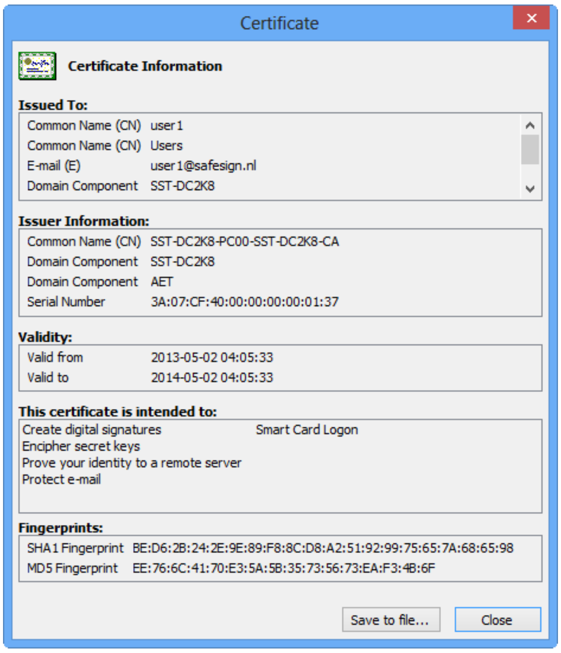
A number of operations are possible with regard to (some of) the objects on the token, which are described in the following sections:

Section 3.7.1	:	View Certificate
Section 3.7.2	:	Save Object
Section 3.7.3	:	Edit Label
Section 3.7.4	:	Delete Object

3.7.1 View Certificate

This allows you to view the certificate content.

Select the certificate on the token and click on **View Certificate** to view the contents of the certificate:



Certificate

Certificate Information

Issued To:

Common Name (CN)	user1
Common Name (CN)	Users
E-mail (E)	user1@safesign.nl
Domain Component	SST-DC2K8

Issuer Information:

Common Name (CN)	SST-DC2K8-PC00-SST-DC2K8-CA
Domain Component	SST-DC2K8
Domain Component	AET
Serial Number	3A:07:CF:40:00:00:00:00:01:37

Validity:

Valid from	2013-05-02 04:05:33
Valid to	2014-05-02 04:05:33

This certificate is intended to:

Create digital signatures
Encipher secret keys
Prove your identity to a remote server
Protect e-mail
Smart Card Logon

Fingerprints:

SHA1 Fingerprint	BE:D6:2B:24:2E:9E:89:F8:8C:D8:A2:51:92:99:75:65:7A:68:65:98
MD5 Fingerprint	EE:76:6C:41:70:E3:5A:5B:35:73:56:73:EA:F3:4B:6F

Figure 130: View Certificate: Certificate Information

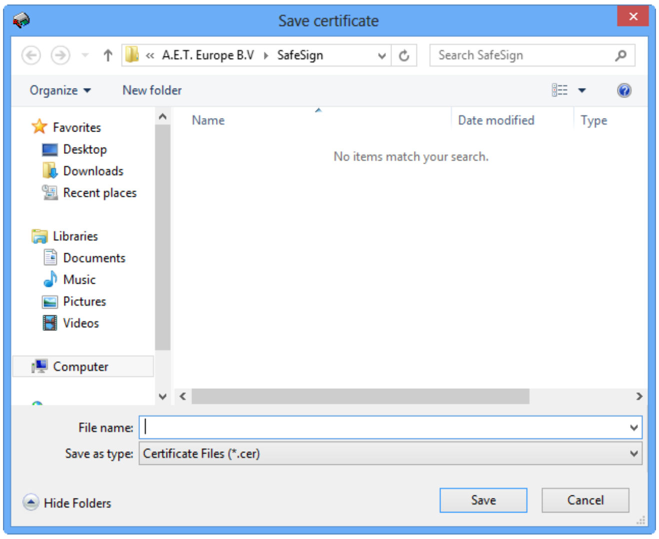
3.7.2 Save Object

This allows you to save certificates in *.cer format, as well as data objects on the token.

Note

*Note that the **Save to file** button in Figure 130 does the same for certificates.*

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



No items match your search.

File name:

Save as type: Certificate Files (*.cer)

Figure 131: Save Object: Save certificate

➔ Select a location and click **Save**

3.7.3 Edit Label

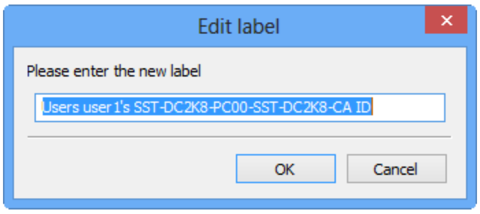
You can edit the label of both public and private keys and certificates (e.g. to be able to identify with your own label of choice which public and private key and certificate go together).

Note

Note that this will only be visible in the Token Administration Utility's PKCS#11 Objects dialog.

When requesting a key pair and certificate through the CSP, the key pair is generated before the certificate. SafeSign Identity Client matches the label of the public and private key with the label of the certificate, so as better to distinguish which public and private key and certificate go together.

Upon clicking **Edit Label**, the following dialog will be opened:



Please enter the new label

Users user1's SST-DC2K8-PC00-SST-DC2K8-CA ID

Figure 132: Edit Label

➔ Enter the new label and click **OK** to save it.

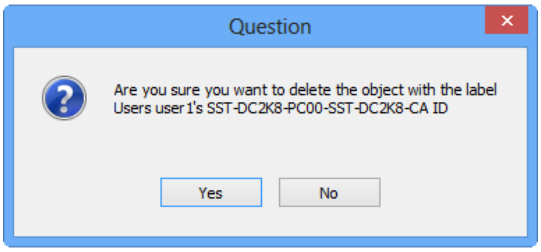
After entering the correct PIN for the token, the label will be changed.

Note that you will have to edit the label of each object separately.

3.7.4 Delete Object

This allows you to delete token objects, both public key(s), private key(s) and certificate(s).

Select an object and click on **Delete Object**. You will be asked to confirm the deletion:

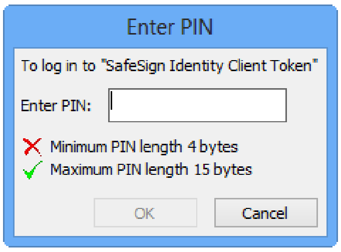


Are you sure you want to delete the object with the label
Users user1's SST-DC2K8-PC00-SST-DC2K8-CA ID

Figure 133: Delete Object: Are you sure

➔ Click **Yes** if you want to delete the object.

You will be asked for the PIN of the token:



To log in to "SafeSign Identity Client Token"

Enter PIN:

✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes

Figure 134: Delete Object: Enter PIN

➔ Enter the correct PIN and click **OK**, upon which the object will be deleted.

Note that if you have entered the PIN once in the *PKCS #11 Objects* dialog (e.g. to show private objects), you will not have to enter it again at this point.

3.8 Dump Token Contents

This feature is only available in the Token Administration Utility.

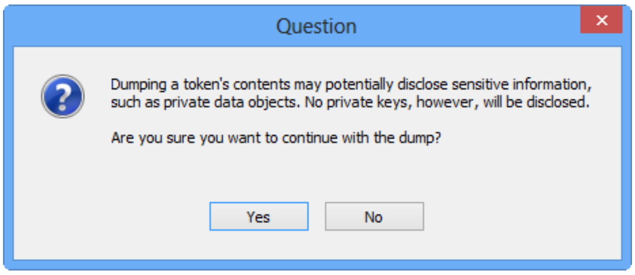
This function allows you to dump the contents of the token, identifying the PKCS #11 objects on the token and their attributes, which can then be sent to AET SafeSign Support for further analysis if errors occur that may be related to the token contents.

This dump is particularly useful 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 administrators (and AET SafeSign Support) more information on whether the attributes are set and whether they are set correctly. This is important both for certificate registration and applications trying to use the token (and the certificate it contains).

Note that the actual objects on the token will in no way be saved or placed off the card. Only the public information of the contents of the token will be exported.

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

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



Question

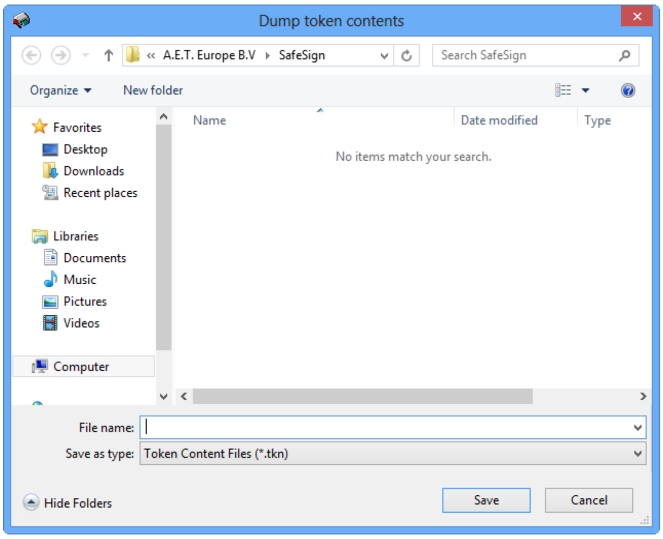
Dumping a token's contents may potentially disclose sensitive information, such as private data objects. No private keys, however, will be disclosed.

Are you sure you want to continue with the dump?

Figure 135: Dump Token Contents: Question

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

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



Dump token contents

No items match your search.

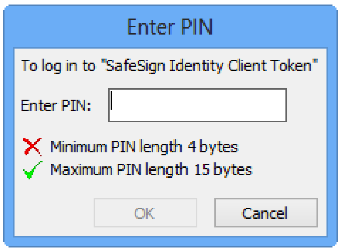
File name:

Save as type: Token Content Files (*.tkn)

Figure 136: Dump Token Contents: Save

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

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



Enter PIN

To log in to "SafeSign Identity Client Token"

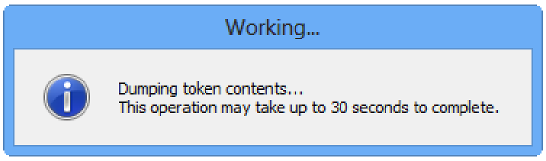
Enter PIN:

✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes

Figure 137: Dump Token Contents: Enter PIN

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

The token contents will now be written to a file in the location specified:

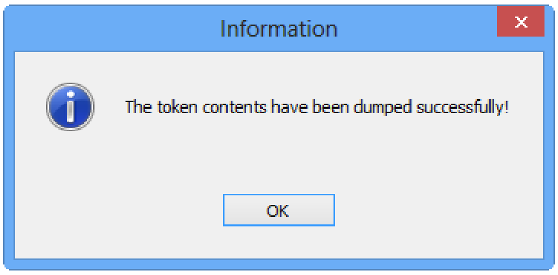


Working...

Dumping token contents...
This operation may take up to 30 seconds to complete.

Figure 138: Dump Token Contents: Dumping

When the dump is successful, you will be notified:



Information

The token contents have been dumped successfully!

Figure 139: Dump Token Contents: Dump successful

➔ Click **OK**

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

3.9 Query Unknown token

This feature is only available in the Token Administration Utility.

This function has been built into the Token Administration Utility to be able to add the appropriate registry data for as yet unrecognised versions of supported Java tokens with a default test keyset, which do not contain the SafeSign Identity Client applet.

If the token is identified as an unknown token, this may mean[1] that the CPLC data of the token[2] is not known in SafeSign Identity Client. The **Query Unknown Token** function allows you to query the CPLC data of the token and create the registry entries necessary to support it.

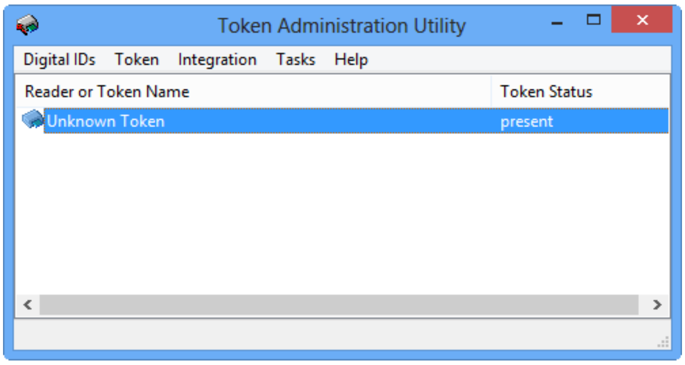
Note that the CPLC data is only used for initialising a blank token with a test key set, in order to have the right settings for installing the applet upon initialisation through the Token Utility. For production tokens that have the applet installed (and a custom key set), the CPLC data is not used.

Note that in case your token is not recognised or query unknown token does not work, it is advisable first to verify whether there is a new version of SafeSign Identity Client available (that may recognise your token) and/or to contact your supplier about the exact details of the token.

[1] Note that it may also be that the particular token is not supported by SafeSign (see the list of supported tokens in the Product Description).

[2] Actually, we use twelve bytes extracted from the Card Production Life Cycle data, but for the purposes of this document we will use the phrase "CPLC data".

When SafeSign Identity Client does not recognise a token (yet), the Token Utility will display “Unknown token – present”[1]:

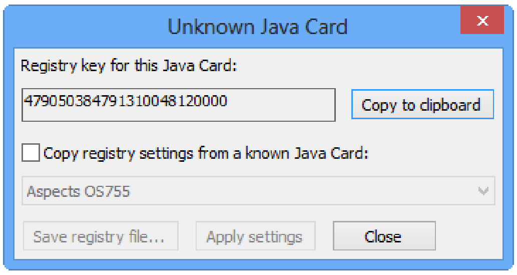


Reader or Token Name	Token Status
Unknown Token	present

Figure 140: Token Utility: Unknown Token

➔ Select **Token > Query unknown token**

Upon selecting the *Query unknown token* item of the **Token** menu, the following dialog will open:



Registry key for this Java Card:

4790503847913100481200000

□ Copy registry settings from a known Java Card:

Aspects OS755

Figure 141: Query unknown token: Unknown Java Card

This dialog identifies the registry key for the Java card inserted.

You can copy the registry settings from a known Java card, if you know which Java card (an as yet unrecognised version of an already supported Java card) you are using.

Use the drop-down box to select the Java card type you know the token to be. The drop-down box does not automatically select the token model you are using.

➔ Select **Copy registry settings from a known Java card** and select the known Java card

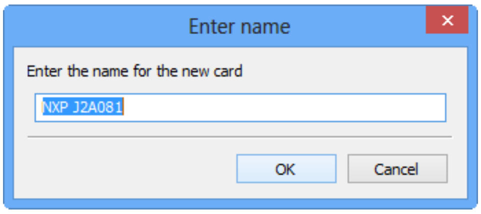
You can now either apply the registry settings to the (as yet) unknown card, or you can save the registry file to add it manually at a later time by double-clicking it[2].

[1] Note that it may also be that the particular token is not supported by SafeSign (see the list of supported tokens in the Product Description) or that something else is wrong (in which case, Query unknown token may inform you that the “token is not recognised as a Java card”.

[2] This may be convenient if one or more workstations of SafeSign end-users need to support the new version of a Java card.

3.9.1 Apply settings

Upon clicking on **Apply settings**, you will be asked to enter the name for the new card:



Enter name

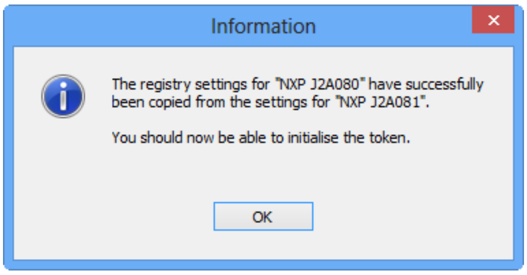
Enter the name for the new card

NXP J2A081

Figure 142: Apply settings: Enter name

➔ Enter a name for the new card (or retain the name of the known Java card) and click **OK**

Upon clicking **OK**, you will be informed that:



Information

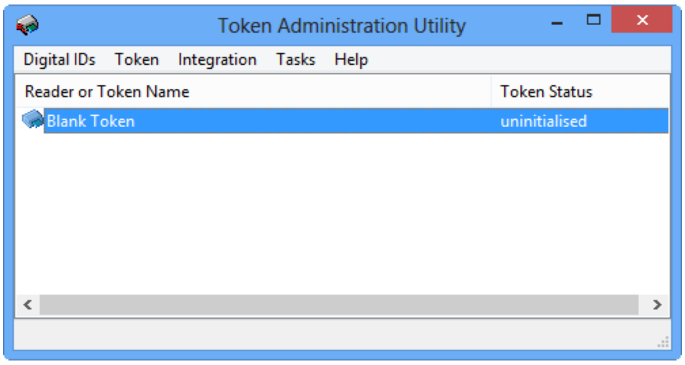
The registry settings for "NXP J2A080" have successfully been copied from the settings for "NXP J2A081".

You should now be able to initialise the token.

Figure 143: The registry settings have successfully been copied

➔ Click **OK**, then click **Close**

The token can now be initialised, as described in section 3.1.1:

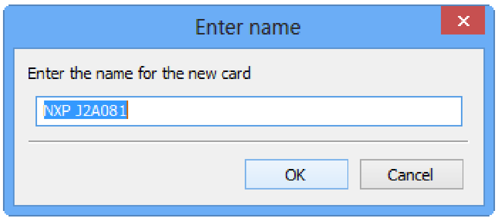


Reader or Token Name	Token Status
Blank Token	uninitialised

Figure 144: Token Administration Utility: Blank Token

3.9.2 Save registry file

Upon clicking on **Save registry file**, you will be asked to enter the name for the new card:



Enter name

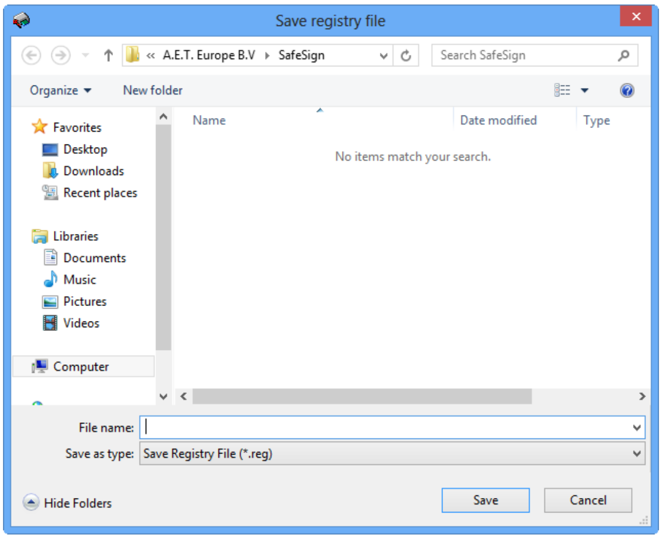
Enter the name for the new card

NXP J2A081

Figure 145: Save registry file: Enter name

➔ Enter a name for the new card (or retain the name of the known Java card) and click **OK**

You can now save the registry file to a suitable location:



No items match your search.

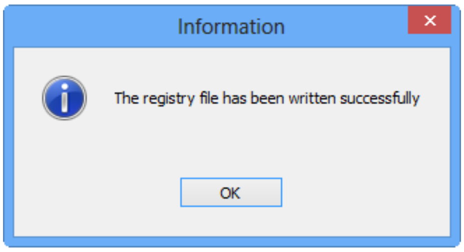
File name:

Save as type: Save Registry File (*.reg)

Figure 146: Save registry file

➔ Click **Save**

When the registry file has been saved, you will be informed that:

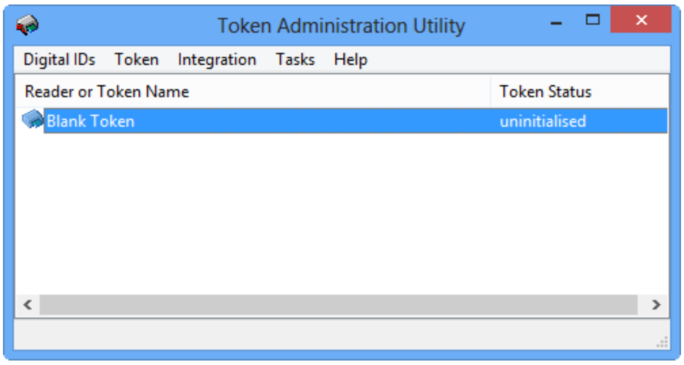


The registry file has been written successfully

Figure 147: Save registry file: The registry file has been written successfully

➔ Click **OK**, then **Close**

The registry file will now be available at the location where you saved it. Upon double-clicking it, the registry file will be saved in the registry and you will be able to initialise the (now) blank token:



Reader or Token Name	Token Status
Blank Token	uninitialised

Figure 148: Token Administration Utility: Blank Token

3.10 Analyse Certificate Quality

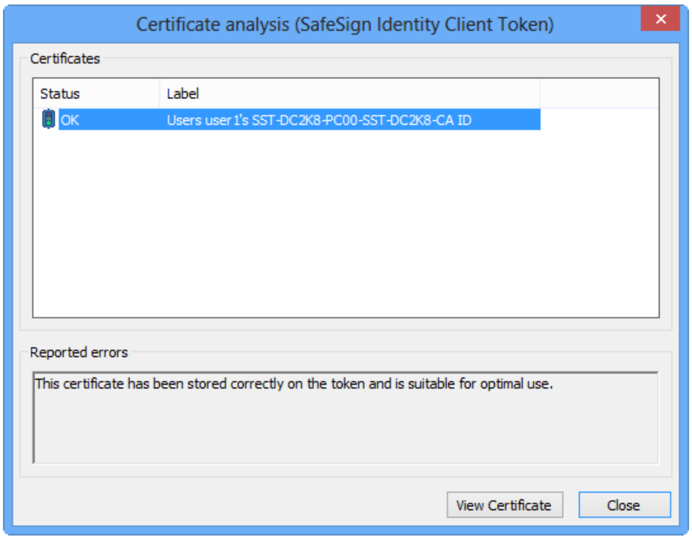
This feature is only available in the Token Administration Utility.

This function analyses the quality of the 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.

There are three possible scenarios:

3.10.1 Certificate Status OK

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



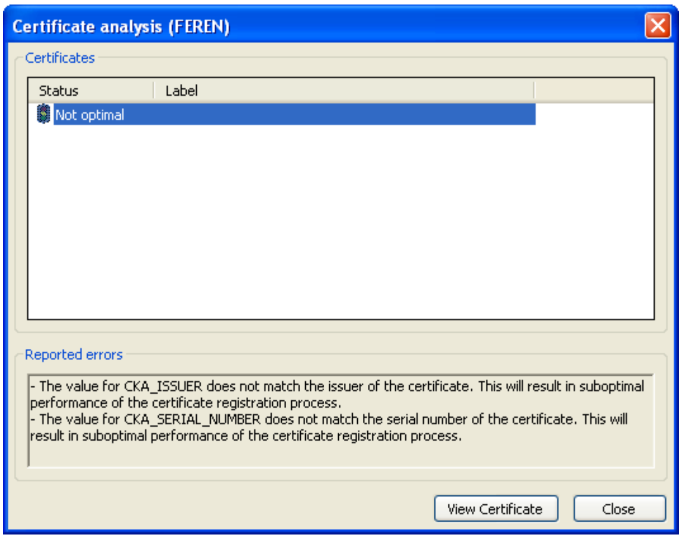
Status	Label
OK	Users user1's SST-DC2K8-PC00-SST-DC2K8-CA ID

This certificate has been stored correctly on the token and is suitable for optimal use.

Figure 149: Certificate analysis: OK

3.10.2 Certificate Status Not Optimal

The certificate status is “Not optimal”:



Certificate analysis (FEREN)

Certificates

Status	Label
Not optimal	

Reported errors

- The value for CKA_ISSUER does not match the issuer of the certificate. This will result in suboptimal performance of the certificate registration process.
- The value for CKA_SERIAL_NUMBER does not match the serial number of the certificate. This will result in suboptimal performance of the certificate registration process.

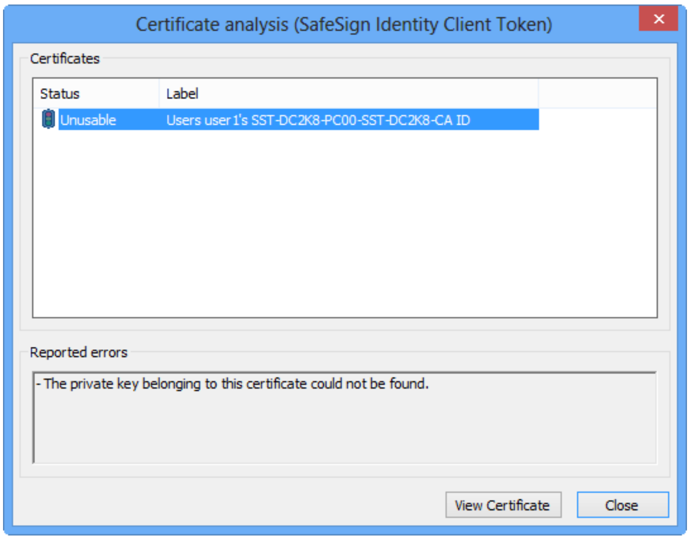
Figure 150: Certificate analysis: Not optimal

When the status of a certificate is not optimal, this may result in suboptimal performance of the certificate registration process. Therefore, the certificate analysis tool will indicate a number of causes why this could be the case (as in the example above).

These causes can be verified when making a dump of the token contents (as described in section 3.8).

3.10.3 Certificate Status Unusable

The certificate status is “Unusable”:



Certificate analysis (SafeSign Identity Client Token)

Certificates

Status	Label
Unusable	Users user1's SST-DC2K8-PC00-SST-DC2K8-CA ID

Reported errors

- The private key belonging to this certificate could not be found.

Figure 151: Certificate analysis: Unusable

This may occur when the private key could not be found on the token, or when the private key does not match the public key in the certificate.

In this case, the certificate is unusable for any application.

3.11 Change PIN Timeout

This feature is only available in the Token Administration Utility.

In SafeSign Identity Client[1], it is possible to set a PIN timeout, for both PKCS #11 and CSP applications, for Java Card v2.2+ cards.

By default, the PIN timeout is disabled, as in Figure 124. When the PIN timeout is enabled, you will be asked to (re-)login to the token, i.e. the SafeSign PIN dialog will be displayed.

In practice, this means that for example when using Outlook to send signed e-mail messages, you will be asked to enter your PIN again when the maximum amount of time has passed since the last time you logged in to the token.

The timeout value for a particular token can be set in the Token Administration Utility, 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.

Note that the PIN Timeout feature does not work with secure pinpad readers, i.e. it cannot be set and does not work within applications.

Select **Change PIN Timeout** from the **Token** menu:

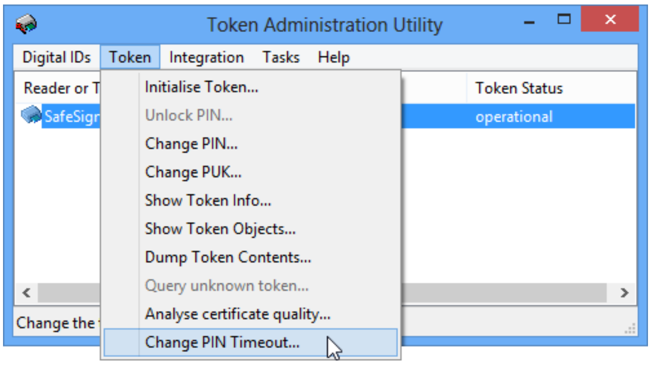
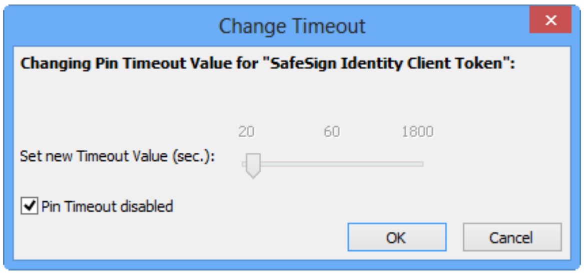


Figure 152: Token Administration Utility: Change PIN Timeout

Upon selecting **Change PIN Timeout**, the *Change Timeout* dialog will open:


Change Timeout

Changing Pin Timeout Value for "SafeSign Identity Client Token":

Set new Timeout Value (sec.):

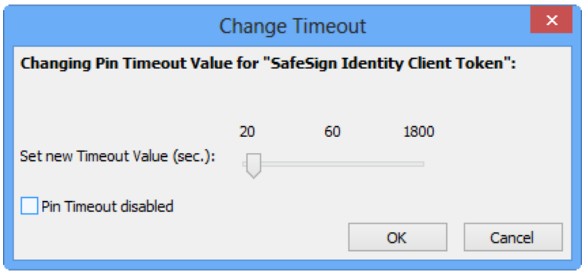
☑ Pin Timeout disabled

Figure 153: Change Timeout: Pin Timeout disabled

By default, the PIN Timeout is disabled.

[1] From SafeSign Identity Client version 3.0.33 onwards (≥ 3.0.33).

Deselect **Pin Timeout disabled**, after which you will be able to set the new Timeout Value:



Change Timeout

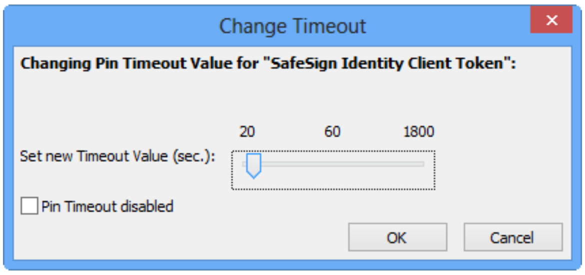
Changing Pin Timeout Value for "SafeSign Identity Client Token":

Set new Timeout Value (sec.): 20 60 1800

□ Pin Timeout disabled

Figure 154: Change Timeout: Pin Timeout enabled

Drag the slider to the desired value (in our example, 60 seconds):



Change Timeout

Changing Pin Timeout Value for "SafeSign Identity Client Token":

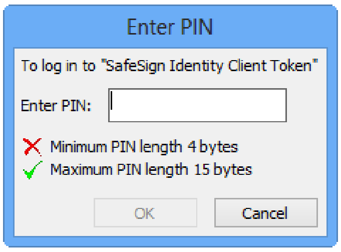
Set new Timeout Value (sec.): 20 60 1800

□ Pin Timeout disabled

Figure 155: Change Timeout: New Timeout Value

- ➔ Click **OK**

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



Enter PIN

To log in to "SafeSign Identity Client Token"

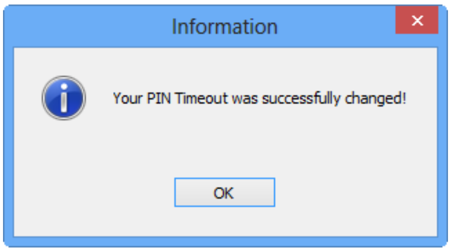
Enter PIN:

✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes

Figure 156: Enter PIN

- ➔ Enter the PIN and click **OK**

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



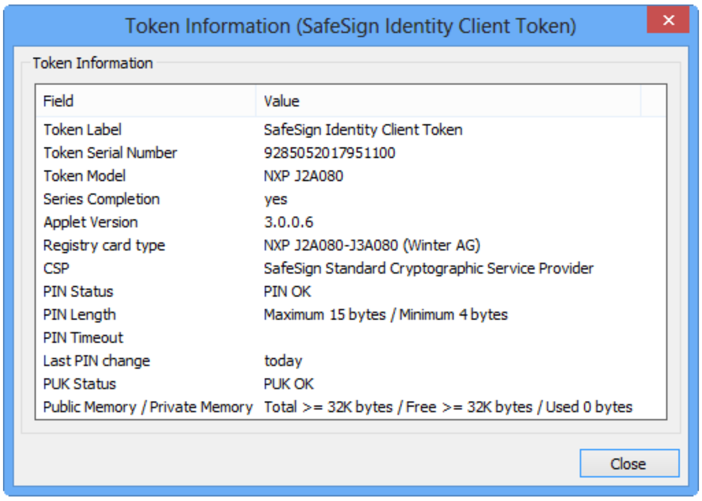
Information

Your PIN Timeout was successfully changed!

Figure 157: Your PIN Timeout was successfully changed

- ➔ Click **OK**

When the PIN Timeout is enabled, the *Token Information* will no longer display it is disabled (but it will not display the Timeout value):



Field	Value
Token Label	SafeSign Identity Client Token
Token Serial Number	9285052017951100
Token Model	NXP J2A080
Series Completion	yes
Applet Version	3.0.0.6
Registry card type	NXP J2A080-J3A080 (Winter AG)
CSP	SafeSign Standard Cryptographic Service Provider
PIN Status	PIN OK
PIN Length	Maximum 15 bytes / Minimum 4 bytes
PIN Timeout	
Last PIN change	today
PUK Status	PUK OK
Public Memory / Private Memory	Total >= 32K bytes / Free >= 32K bytes / Used 0 bytes

Figure 158: Token Information: PIN Timeout enabled

Note that this an error in the display of the PIN Timeout, which will be fixed in a future release of SafeSign Identity Client.

4 Integration menu

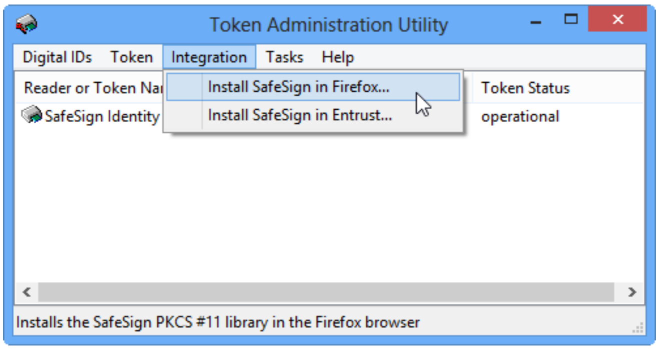
When you have Mozilla Firefox and/or Entrust 6.x installed on your computer, the SafeSign Identity Client InstallShield Wizard will allow you to install SafeSign Identity Client in Firefox / Entrust during the SafeSign Identity Client installation procedure.

In addition, it is also possible to install SafeSign Identity Client in Firefox and Entrust at a later stage, through the **Integration** menu of the Token Administration Utility, which also allows you to de-install SafeSign from Firefox / Entrust.

For more information on installing SafeSign in Firefox / Entrust during installation, refer to the *SafeSign Identity Client Installation Guide*.

4.1 Install SafeSign in Firefox

1 In the Token Administration Utility window, select **Integration > Install SafeSign in Firefox**:



Installs the SafeSign PKCS #11 library in the Firefox browser

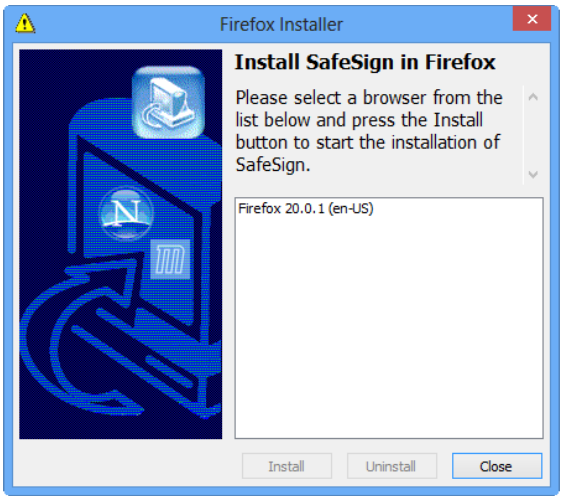
Figure 159: Token Administration Utility: Install SafeSign in Firefox

Note

Note that there was an issue with Firefox version 3.5 and the installation of the SafeSign PKCS#11 Library as a security module in Firefox, through the SafeSign Firefox Installer. As of Firefox 3.5.x, it is no longer possible to install PKCS#11 modules automatically, as described in the Firefox 3.5 release notes: "Web pages can no longer automatically install PKCS11 cryptographic tokens. Users are now required to do this manually or install an Add-on that installs them."

From SafeSign Identity Client version 3.0.40 onwards, the Firefox Installer will install the SafeSign PKCS#11 Library again in Firefox 3.5 or higher.

2 The Firefox Installer is loaded:



Firefox Installer

Install SafeSign in Firefox

Please select a browser from the list below and press the Install button to start the installation of SafeSign.

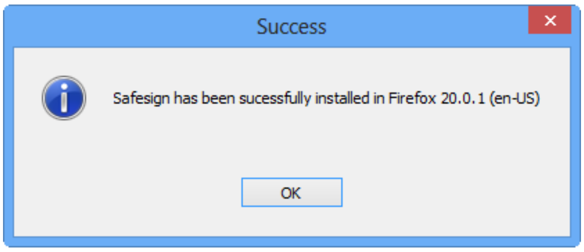
Firefox 20.0.1 (en-US)

Figure 160: Firefox Installer: Install SafeSign in Firefox

It will list the version of Firefox present on your system and allows you to install SafeSign Identity Client as a security module.

➔ Select your Firefox browser from the list and click **Install**

3 Upon selecting Firefox from the list and clicking Install, the SafeSign Identity Client PKCS #11 Library will be installed as a security module in Firefox:



Success

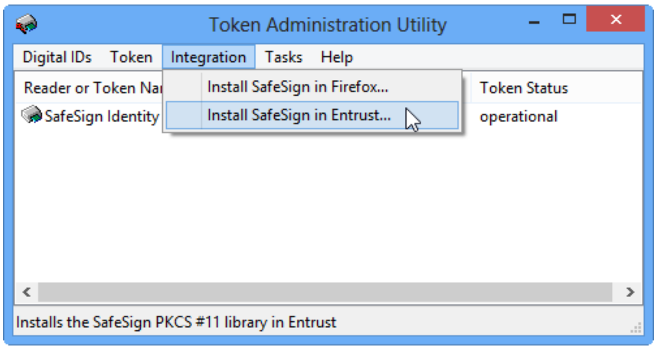
Safesign has been sucessfully installed in Firefox 20.0.1 (en-US)

Figure 161: Firefox Installer: SafeSign has been successfully installed in Firefox

➔ Click **OK**

4.2 Install SafeSign in Entrust

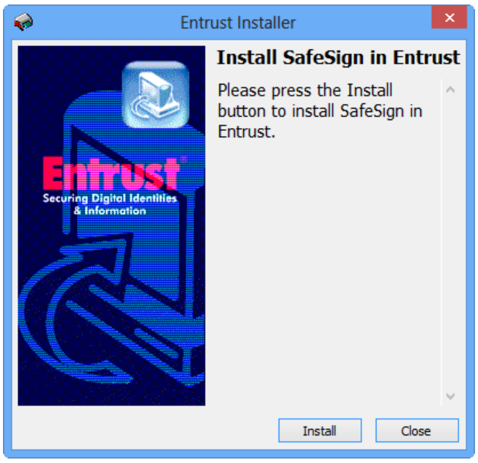
1 In the Token Administration Utility window, select **Integration > Install SafeSign in Entrust**:



Installs the SafeSign PKCS #11 library in Entrust

Figure 162: Token Administration Utility: Install SafeSign in Entrust

2 The Entrust Installer is loaded:



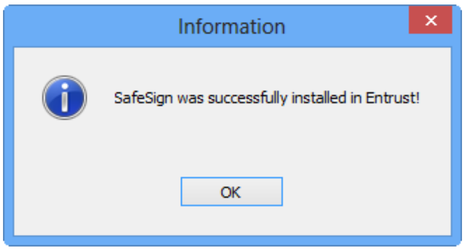
Install SafeSign in Entrust

Please press the Install button to install SafeSign in Entrust.

Figure 163: Entrust Installer: Install SafeSign in Entrust

➔ Click **Install** to install SafeSign Identity Client in Entrust

3 Upon clicking **Install** in the *Entrust Installer* window, SafeSign Identity Client will be installed in Entrust and you will be notified if this has been successful:



SafeSign was successfully installed in Entrust!

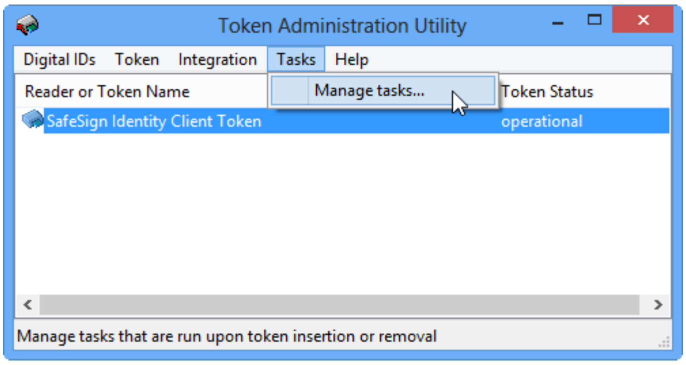
Figure 164: Entrust Installer: SafeSign was successfully installed in Entrust

➔ Click **OK** to close this dialog, upon which the *Entrust Installer* window will close

5 Tasks menu

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

The Token Administration Utility includes a **Tasks** menu:

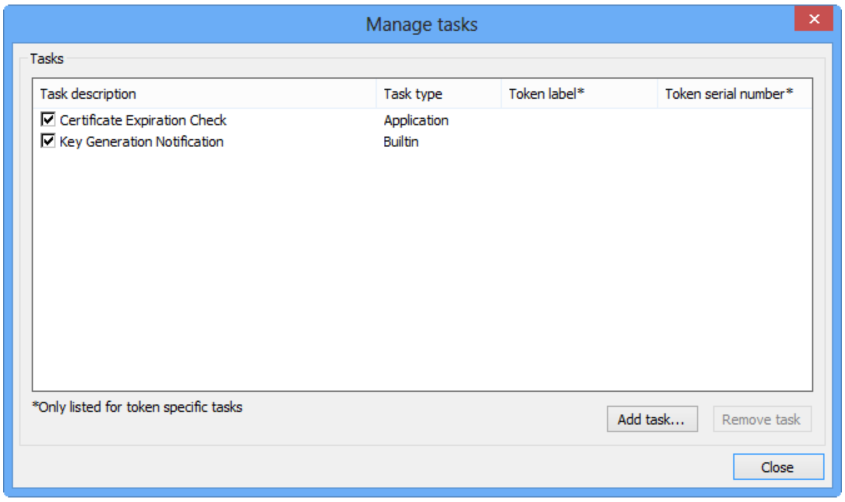


Reader or Token Name	Token Status
SafeSign Identity Client Token	operational

Manage tasks that are run upon token insertion or removal

Figure 165: Token Administration Utility: Manage tasks

Clicking on **Manage tasks** will open the *Manage tasks* dialog, which already contains two tasks by default (that apply to all cards), which is that of checking certificate expiration and displaying the key generation dialog:



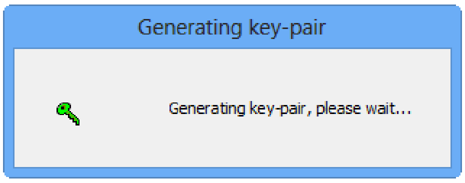
Task description	Task type	Token label*	Token serial number*
☑ Certificate Expiration Check	Application		
☑ Key Generation Notification	Builtin		

*Only listed for token specific tasks

Figure 166: Manage tasks: Tasks

The task "Certificate Expiration Check" will prompt a dialog when a certificate is expired or is about to expire. See Figure 39 and Figure 40.

The task "Key Generation Notification" will prompt a dialog during key generation:



Generating key-pair, please wait...

Figure 167: Key Generation Notification: Generating key-pair

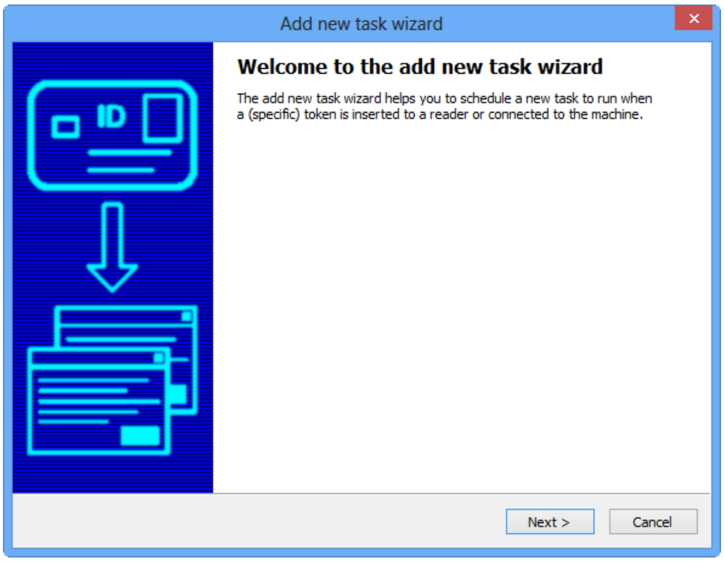
If you want to disable one of the tasks, for example certificate registration checking, you can remove the task (*Remove task*) from the Task menu of the Token Administration Utility, but we recommend deselecting the Task in the *Manage tasks* dialog (as you may want to enable it again at a later time).

When both tasks are deselected, the process ' aetcrss1.exe' (that takes care of both these tasks) will automatically be ended, so that it does not interfere with other processes.

5.1 Adding a Task

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

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



Add new task wizard

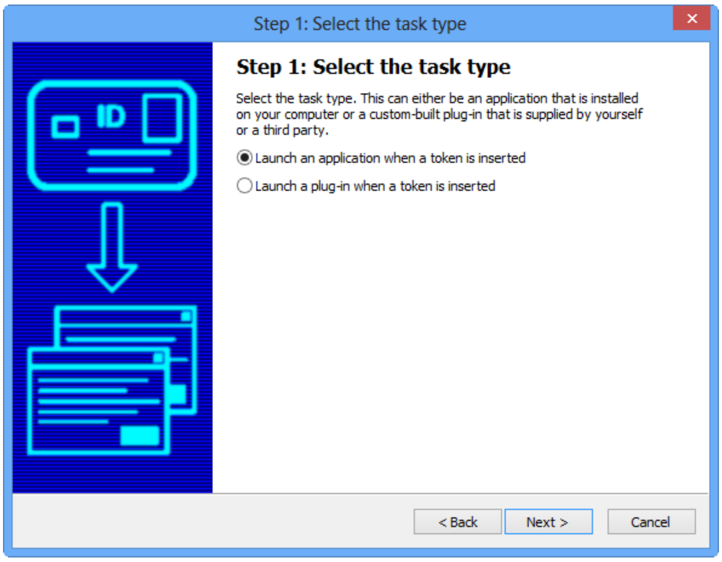
Welcome to the add new task wizard

The add new task wizard helps you to schedule a new task to run when a (specific) token is inserted to a reader or connected to the machine.

Figure 168: 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:



Step 1: Select the task type

Step 1: Select the task type

Select the task type. This can either be an application that is installed on your computer or a custom-built plug-in that is supplied by yourself or a third party.

● Launch an application when a token is inserted

○ Launch a plug-in when a token is inserted

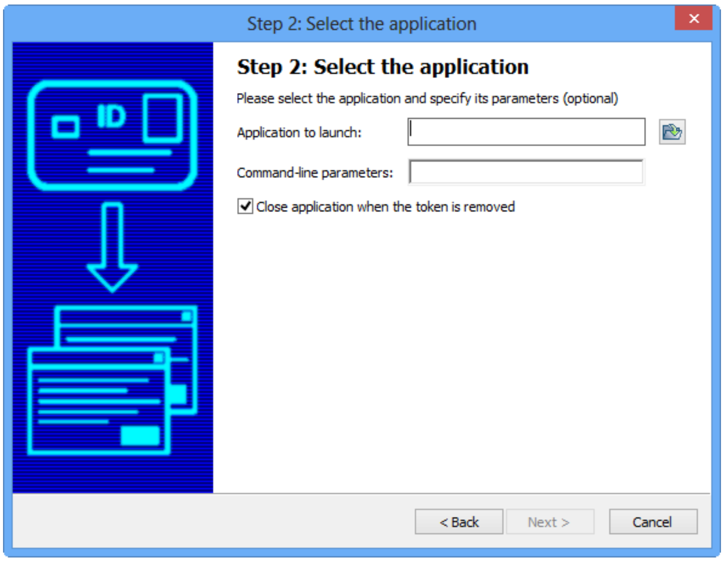
Figure 169: Add new task wizard: Select the task type

You can select two task types:

1. Launch an application when a token is inserted: for example, open Internet Explorer ((on a particular (secure) web site)) or set up a Remote Desktop Connection / Citrix connection;
2. Launch a plug-in when a token is inserted: for example, to change the Transport PIN of the token.

5.1.1 Launch an application

3 Upon selecting the option *Launch an application when a token is* inserted, Step 2 will allow you to select the application to launch and specify its parameters (if required / desired):



Step 2: Select the application

Step 2: Select the application

Please select the application and specify its parameters (optional)

Application to launch:

Command-line parameters:

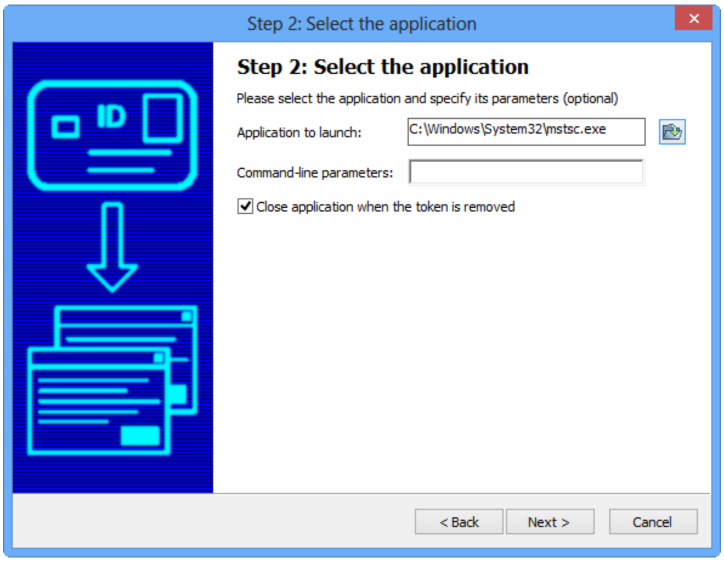
☑ Close application when the token is removed

Figure 170: Add new task wizard: Select the application

In our example, we will launch a Remote Desktop Connection, which can be found in the system32 directory and is called *mstsc.exe*.

➔ Select the application

When you have selected the application, you can specify command-line parameters for this application:



Step 2: Select the application

Step 2: Select the application

Please select the application and specify its parameters (optional)

Application to launch: C:\Windows\System32\mstsc.exe

Command-line parameters:

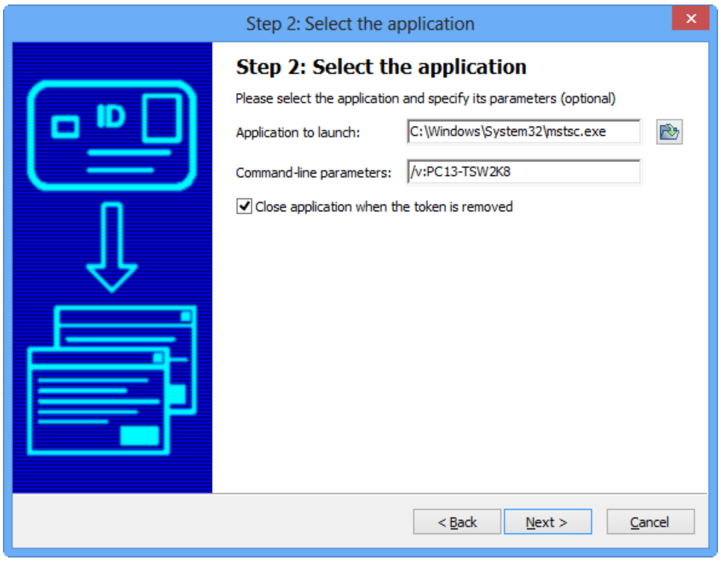
☑ Close application when the token is removed

Figure 171: Select the application: Application to launch

Note that these parameters are application-specific. For example, in order to start up a Remote Desktop Connection, you should enter: /v:<server name>.

4

Thus, in our example, step 2 is completed as follows:



Step 2: Select the application

Step 2: Select the application

Please select the application and specify its parameters (optional)

Application to launch: C:\Windows\System32\mstsc.exe

Command-line parameters: /v:PC13-TSW2K8

☑ Close application when the token is removed

Figure 172: Add new task wizard: Select the application completed

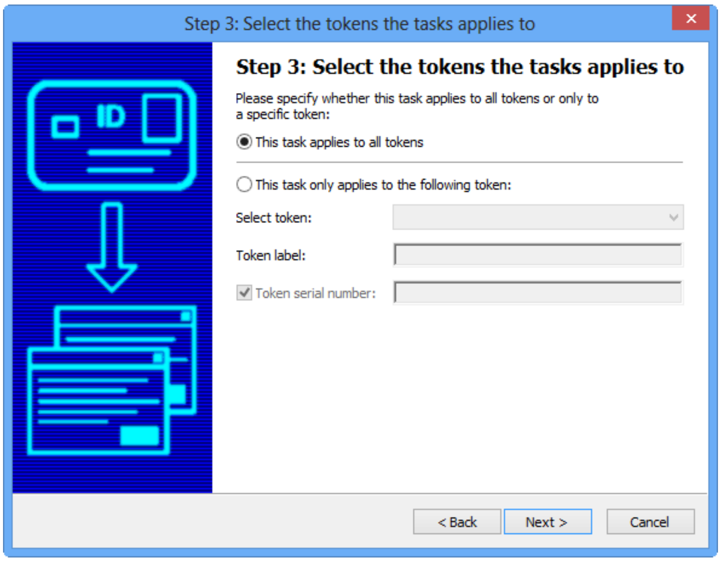
You can also select in this window, whether you want to close the task when the token is removed.

➔ Click **Next** to continue

Note

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

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



Step 3: Select the tokens the tasks applies to

Step 3: Select the tokens the tasks applies to

Please specify whether this task applies to all tokens or only to a specific token:

● This task applies to all tokens

○ This task only applies to the following token:

Select token:

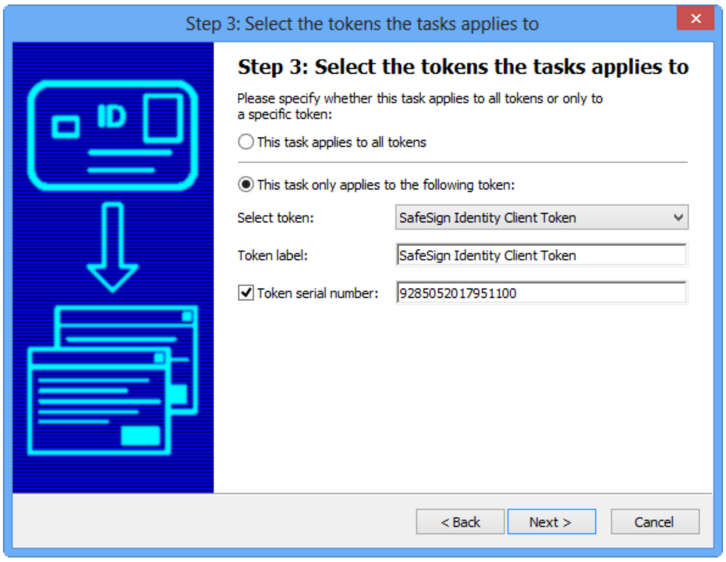
Token label:

☑ Token serial number:

Figure 173: Add new task wizard: Select the tokens the task applies to

When no token is inserted in the reader, the window above will be shown (with the option 'This *task only applies to the following token'* greyed out).

5 When a token is inserted, this option is selectable and when completed, will look as follows:



Step 3: Select the tokens the tasks applies to

Step 3: Select the tokens the tasks applies to

Please specify whether this task applies to all tokens or only to a specific token:

○ This task applies to all tokens

● This task only applies to the following token:

Select token: SafeSign Identity Client Token

Token label: SafeSign Identity Client Token

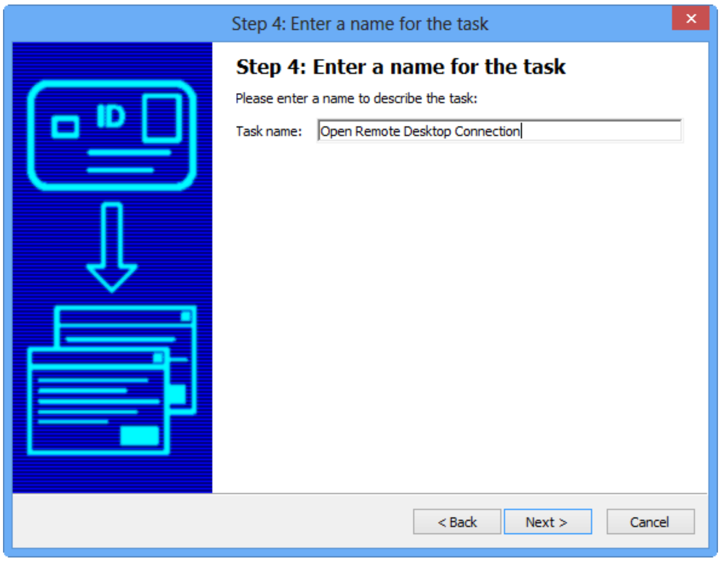
☑ Token serial number: 9285052017951100

Figure 174: Select the tokens the tasks applies to: This task only applies to the following token

Note that it is possible either to select the task to apply to a specific token with a specific serial number or to select the task to apply to any token(s) with the specified token label.

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

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



Step 4: Enter a name for the task

Step 4: Enter a name for the task

Please enter a name to describe the task:

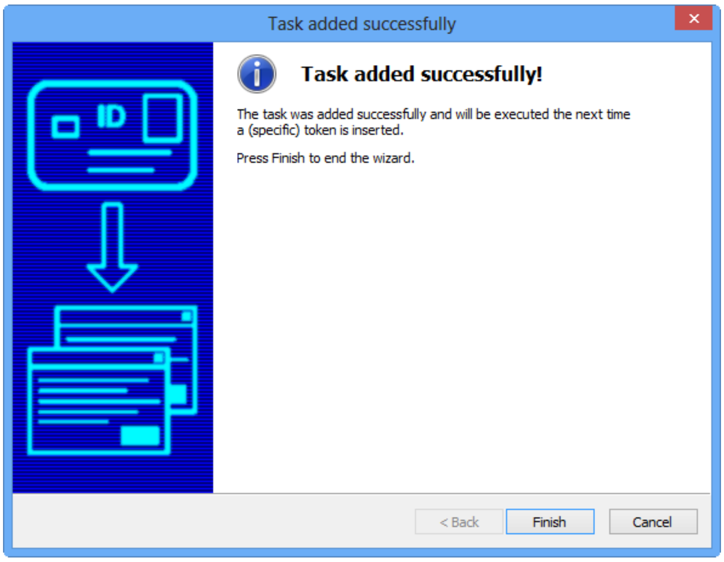
Task name: Open Remote Desktop Connection

Figure 175: Add new task wizard: Enter a name for the task

In our example, the task is called '*Open Remote Desktop Connection*'.

➔ Click **Next** to continue

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



Task added successfully

Task added successfully!

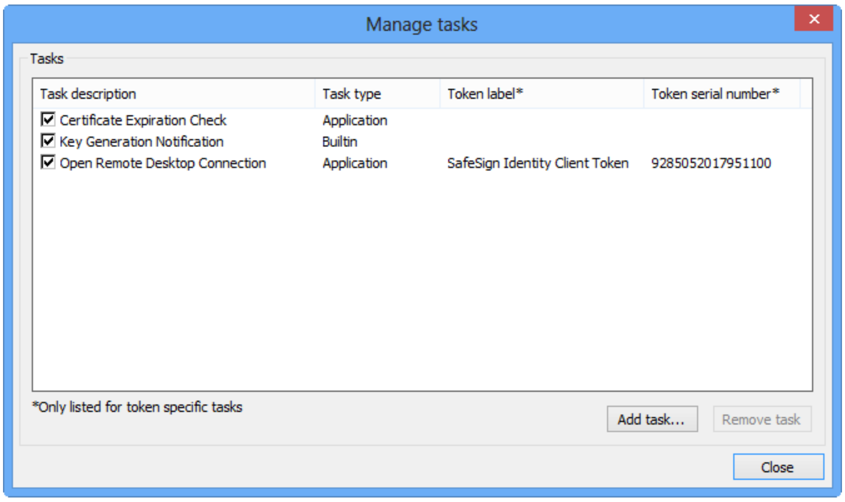
The task was added successfully and will be executed the next time a (specific) token is inserted.

Press Finish to end the wizard.

Figure 176: Add new task wizard: Task added successfully

➔ Click **Finish**

The task will now be added to the *Manage task* window in the Token Administration Utility:



Manage tasks

Tasks

Task description	Task type	Token label*	Token serial number*
☑ Certificate Expiration Check	Application		
☑ Key Generation Notification	Builtin		
☑ Open Remote Desktop Connection	Application	SafeSign Identity Client Token	9285052017951100

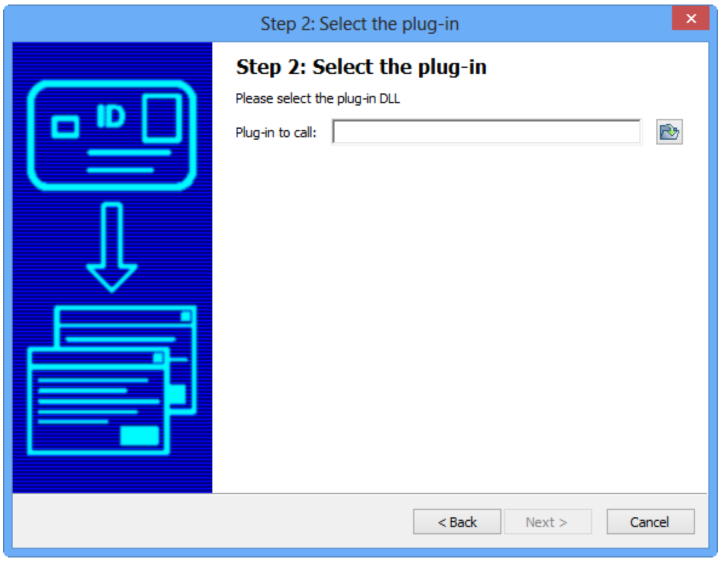
*Only listed for token specific tasks

Figure 177: Manage tasks: Remote Desktop Connection

When a token is inserted, the Remote Desktop Connection will start (due to the parameters given).

5.1.2 Launch a plug-in

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



Step 2: Select the plug-in

Step 2: Select the plug-in

Please select the plug-in DLL

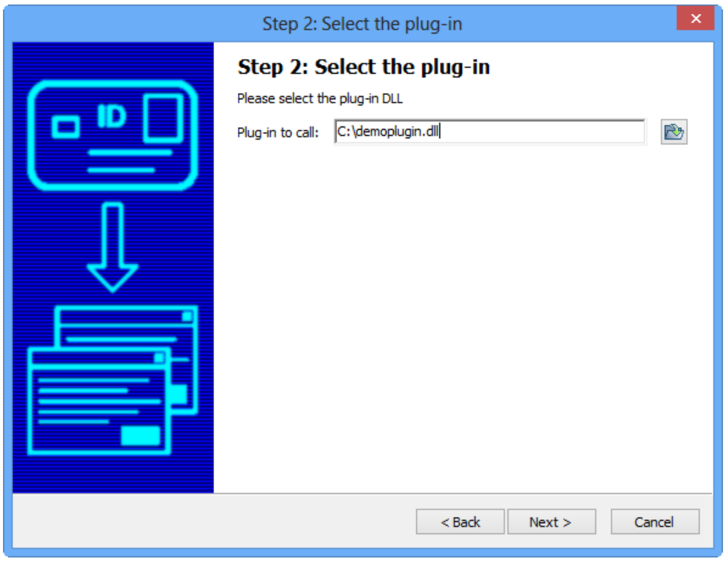
Plug-in to call:

Figure 178: Add new task wizard: Select the plug-in

In our example, we will launch a plug-in called '*demoplugin.dll*', that will allow you to change the Transport PIN of a token (when set).

➔ Select the plug-in to call

When you have selected the plug-in to call, as follows:



Step 2: Select the plug-in

Step 2: Select the plug-in

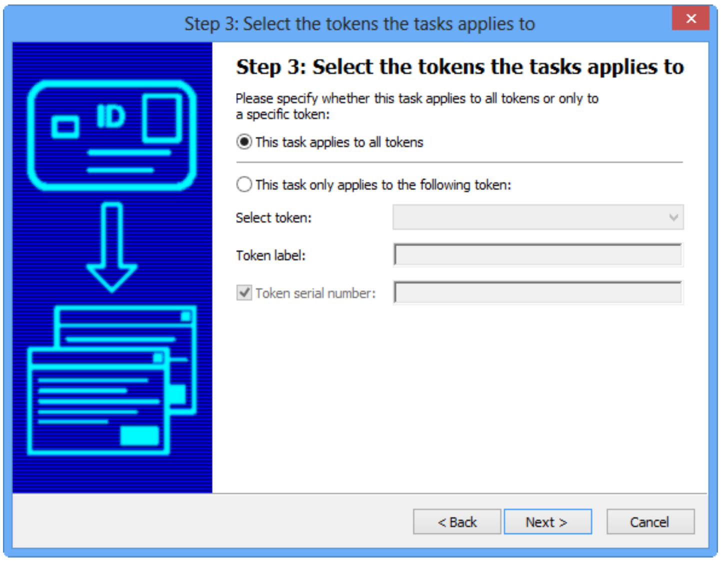
Please select the plug-in DLL

Plug-in to call: C:\demoplugin.dll

Figure 179: Select the plug-in: Plug-in to call

➔ Click **Next** to continue

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



Step 3: Select the tokens the tasks applies to

Step 3: Select the tokens the tasks applies to

Please specify whether this task applies to all tokens or only to a specific token:

● This task applies to all tokens

○ This task only applies to the following token:

Select token:

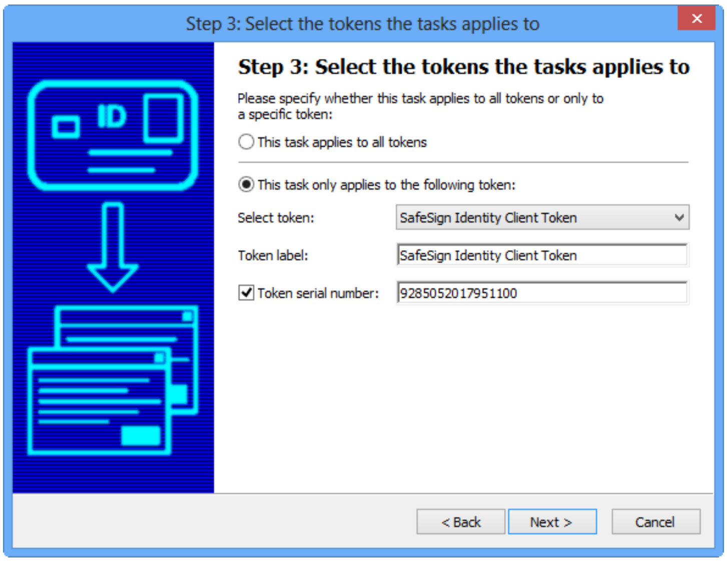
Token label:

☑ Token serial number:

Figure 180: Add new task wizard: Select the tokens the tasks applies to

When no token is inserted in the reader, the window above will be shown (with the option 'This *task only applies to the following token*' greyed out).

When a token is inserted, this option is selectable and when completed, will look as follows:



Step 3: Select the tokens the tasks applies to

Step 3: Select the tokens the tasks applies to

Please specify whether this task applies to all tokens or only to a specific token:

○ This task applies to all tokens

● This task only applies to the following token:

Select token: SafeSign Identity Client Token

Token label: SafeSign Identity Client Token

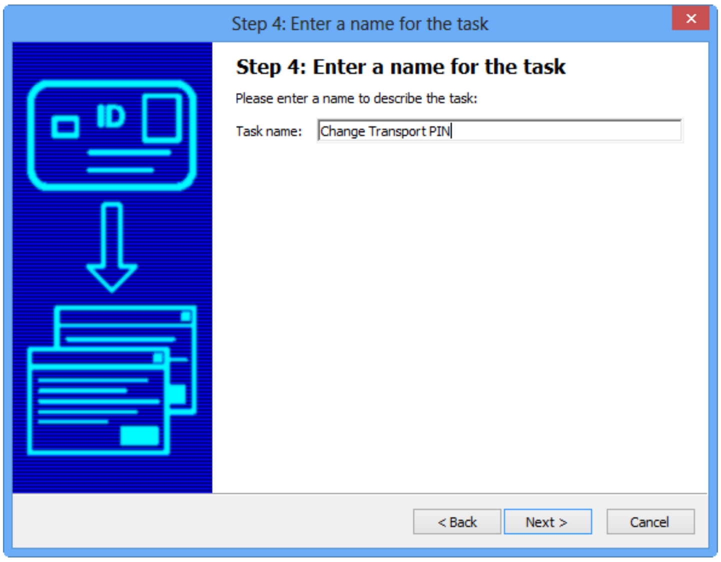
☑ Token serial number: 9285052017951100

Figure 181: Select the tokens the tasks applies to: This task only applies to the following token

Note that it is possible either to select the task to apply to a specific token with a specific serial number or to select the task to apply to any token with the specified token label.

➔ 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):



Step 4: Enter a name for the task

Please enter a name to describe the task:

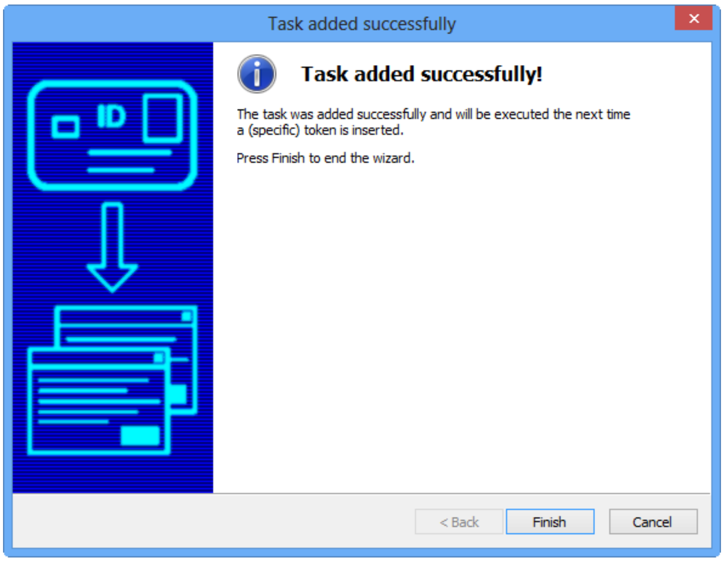
Task name: Change Transport PIN

Figure 182: Add a new task wizard: Enter a name for the task

In our example, the task is called '*Change Transport PIN*'.

➔ Click **Next** to continue

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



Task added successfully!

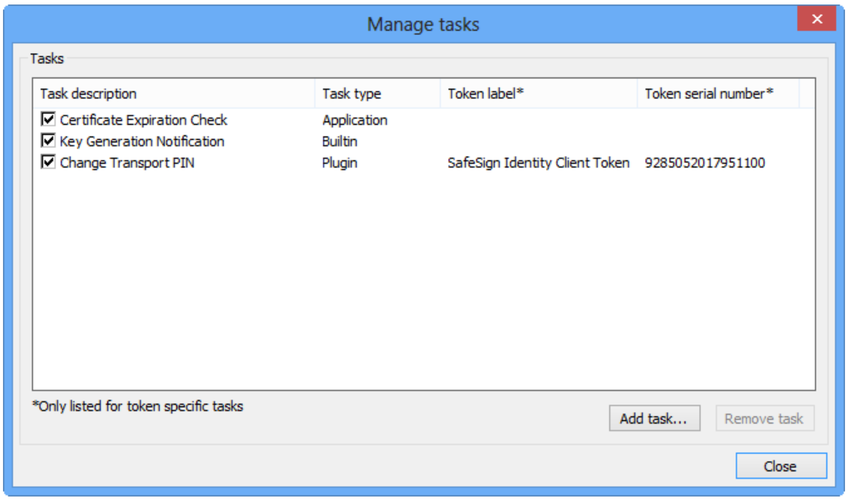
The task was added successfully and will be executed the next time a (specific) token is inserted.

Press Finish to end the wizard.

Figure 183: Add a new task wizard: Task added successfully

➔ Click **Finish**

The task will now be added to the *Manage task* window in the Token Administration Utility:



Task description	Task type	Token label*	Token serial number*
☑ Certificate Expiration Check	Application		
☑ Key Generation Notification	Builtin		
☑ Change Transport PIN	Plugin	SafeSign Identity Client Token	9285052017951100

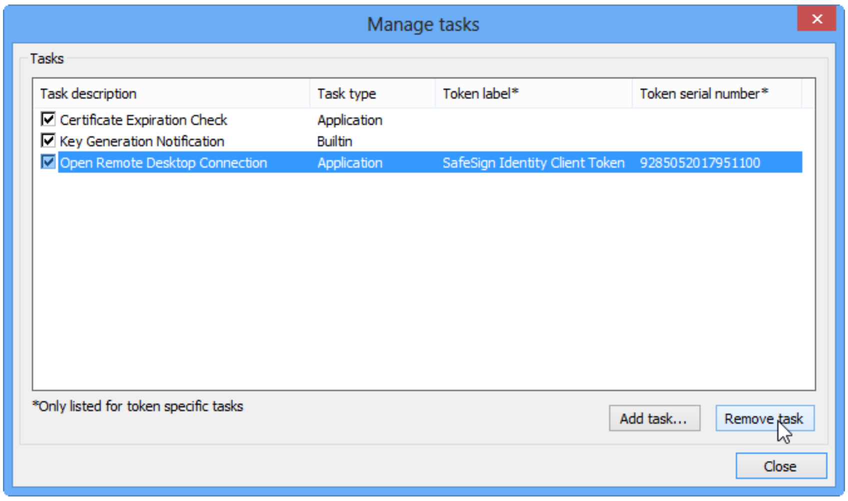
*Only listed for token specific tasks

Figure 184: Manage tasks: Change Transport PIN

5.2 Remove a task

It is not possible to edit an existing task, but it is possible to remove a task.

In the Token Administration Utility's *Manage tasks* window, select the task you want to remove:



Task description	Task type	Token label*	Token serial number*
☑ Certificate Expiration Check	Application		
☑ Key Generation Notification	Builtin		
☑ Open Remote Desktop Connection	Application	SafeSign Identity Client Token	9285052017951100

*Only listed for token specific tasks

Figure 185: Manage tasks: Remove task

➔ Click **Remove task** to remove the task.

Index of Notes