

# SafeSign User Guide

## Token Management Utility (TMU)

This document contains information of a proprietary nature.

No part of this manual may be reproduced or transmitted in any form or by any means electronic, mechanical or otherwise, including photocopying and recording for any purpose other than the purchaser's personal use without written permission of A.E.T. Europe B.V.

Individuals or organisations, which are authorised by A.E.T. Europe B.V. in writing to receive this information, may utilise it for the sole purpose of evaluation and guidance.

**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.

© Copyright A.E.T. Europe B.V., 1997 - 2004.

All rights reserved.

SafeSign 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 ([ey@cryptsoft.com](mailto:ey@cryptsoft.com))

This product includes software written by Tim J. Hudson ([tjh@cryptsoft.com](mailto: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](mailto:info@aeteurope.nl) / [support@aeteurope.nl](mailto:support@aeteurope.nl)  
<http://www.aeteurope.com/>

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

Copyright © 1997 - 2004 A.E.T. Europe B.V.,  
Arnhem, The Netherlands.  
All rights reserved.



## Document Information

---

**Filename:** SafeSign User Guide  
Token Management Utility (TMU)

**Document ID:** TMU\_Guide\_SafeSign\_v1.2

**Project Information:** SafeSign User Documentation

### Document revision history

Version	Date	Author	Changes
1.0	07-05-2004	Drs C.M. van Houten	First edition for SafeSign Standard 2.0 for Windows
1.1	02-08-2004	Drs C.M. van Houten	Edited for SafeSign Standard Version 2.0 for Windows (release 2.0.6)
1.2	04-10-2004	Drs C.M. van Houten	Edited for SafeSign Standard Version 2.0 for Windows (release 2.0.9)

**WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE**

## Table of contents

---

<b>Warning Notice</b> .....	<b>I</b>
<b>Document Information</b> .....	<b>II</b>
<b>Table of contents</b> .....	<b>III</b>
<b>List of Figures</b> .....	<b>IV</b>
<b>About the Product</b> .....	<b>VI</b>
<b>About the Manual</b> .....	<b>VII</b>
<b>1 SafeSign Token Management Utility</b> .....	<b>1</b>
<b>1.1 Introduction</b> .....	<b>2</b>
<b>1.2 Help menu</b> .....	<b>5</b>
1.2.1 Versions Info .....	5
1.2.2 About .....	6
1.2.3 Backwards Compatibility .....	6
<b>1.3 Multi-language</b> .....	<b>7</b>
<b>1.4 Use of pinpad</b> .....	<b>3</b>
1.4.1 G&D CashMouse .....	4
1.4.2 Omnikey CardMan Trust .....	5
1.4.3 Reiner SCT Cyberjack pinpad .....	6
<b>2 Digital IDs menu</b> .....	<b>7</b>
<b>2.1 Show Registered Digital IDs</b> .....	<b>7</b>
2.1.1 Transfer ID to token.....	10
2.1.2 Import trust chain .....	15
2.1.3 Delete Digital ID.....	17
2.1.4 View Certificate .....	19
2.1.5 Refresh.....	20
2.1.6 Check Expiration .....	20
2.1.7 Close .....	21
<b>2.2 Import Digital ID</b> .....	<b>22</b>
<b>2.3 Import Certificate</b> .....	<b>28</b>
<b>2.4 Exit</b> .....	<b>30</b>
<b>3 Token Menu</b> .....	<b>31</b>
<b>3.1 Initialise Token</b> .....	<b>31</b>
3.1.1 Initialise Token .....	31
3.1.2 Wipe Token .....	36
3.1.3 Import CA Certificates .....	39
<b>3.2 Change PIN</b> .....	<b>43</b>
3.2.1 PIN information.....	44
<b>3.3 Unlock PIN</b> .....	<b>47</b>
<b>3.4 Change PUK</b> .....	<b>48</b>
3.4.1 PUK information .....	49
<b>3.5 Show Token Info</b> .....	<b>52</b>
<b>Index of Notes</b> .....	<b>a</b>

## List of Figures

Figure 1: SafeSign menu.....	2
Figure 2: Control Panel: Cryptographic Tokens .....	2
Figure 3: Token Management Utility: Reader Name .....	3
Figure 4: Token Management Utility: Blank Token .....	3
Figure 5: Token Management Utility: Operational Token .....	4
Figure 6: Token Management Utility: Multiple operational tokens.....	4
Figure 7: Token Management Utility: Version Information .....	5
Figure 8: Token Management Utility: Version Information text file .....	5
Figure 9: Token Management Utility: About .....	6
Figure 10: Token Management Utility: Dutch .....	7
Figure 11: Token Management Utility: Chinese .....	2
Figure 12: Regional Options: General.....	2
Figure 13: Enter PIN.....	4
Figure 14: Secure PIN Entry: Please enter PIN .....	5
Figure 15: Secure PIN Entry: Action Successful .....	5
Figure 16: Secure PIN Entry: Abort.....	5
Figure 17: Secure PIN Entry: PIN wrong/barred .....	5
Figure 18: cyberJack – Sichere PIN Eingabe.....	6
Figure 19: Digital IDs: No personal Digital IDs.....	7
Figure 20: Digital IDs: Digital ID stored on token.....	8
Figure 21: Digital IDs: Token Missing.....	9
Figure 22: Digital IDs: Transfer ID to token .....	10
Figure 23: Transfer ID to token: Question.....	11
Figure 24: Transfer ID to token: Question CA certificates .....	11
Figure 25: Transfer ID to token: Enter PIN.....	11
Figure 26: Transfer ID to token: Transferring.....	11
Figure 27: Transfer ID to token: Success .....	12
Figure 28: Digital IDs: Personal Digital ID's on token .....	12
Figure 29: Transfer ID to token: Error .....	13
Figure 30: Digital IDs: no certification path .....	13
Figure 31: Digital IDs: Certification path not on token.....	14
Figure 32: Digital IDs: Certification path not on token.....	15
Figure 33: Import trust chain: Enter PIN.....	15
Figure 34: Import trust chain: Importing.....	16
Figure 35: Import trust chain: Success.....	16
Figure 36: Digital IDs: Certification path on token.....	16
Figure 37: Digital IDs: Are you sure you want to delete Digital ID .....	17
Figure 38: Delete Digital ID: Enter PIN .....	17
Figure 39: Delete Digital ID: Deleting .....	18
Figure 40: Delete Digital ID: Success .....	18
Figure 41: View Certificate: Certificate Information .....	19
Figure 42: View Certificate: Save certificate.....	20
Figure 43: Check Expiration: Information .....	20
Figure 44: Check Expiration: Certificate Expiration Warning.....	21
Figure 45: Certificate Expiration Warning .....	21
Figure 46: Token Management Utility: Import Digital ID .....	23
Figure 47: Import Digital ID .....	23
Figure 48: Import Digital ID: Select a Digital ID file .....	23
Figure 49: Import Digital ID: Digital ID file selected.....	24
Figure 50: Import Digital ID: Label on token .....	24
Figure 51: Import Digital ID: Digital ID password entered.....	25
Figure 52: Error: Digital ID needs a different password.....	25
Figure 53: Import Digital ID: Enter PIN.....	25
Figure 54: Import Digital ID: Working.....	26
Figure 55: Import Digital ID: The Digital ID has been imported successfully.....	26
Figure 56: Error: Key Size either smaller than 768 bits or larger than 1024 bits .....	26
Figure 57: Error: Token out of memory.....	27
Figure 58: Token Management Utility: Imported Digital ID.....	27
Figure 59: Token Management Utility: Import Certificate .....	28
Figure 60: Import Certificate: File name.....	29
Figure 61: Import Certificate: Enter PIN.....	29
Figure 62: Import Certificate: Your certificate is being imported .....	30
Figure 63: Token Management Utility: Certificate successfully imported .....	30
Figure 64: Token Management Utility: Initialise Token .....	31
Figure 65: Token Management Utility: Initialise Token dialog .....	32

Figure 66: Token Management Utility: Initialise Token dialog completed .....	33
Figure 67: Initialise Token: Your token is being initialised .....	33
Figure 68: Initialise Token: The operation completed successfully.....	34
Figure 69: Token Management Utility: SafeSign Token .....	34
Figure 70: Error: Device Error 0x30 .....	34
Figure 71: Token Management Utility: Initialise Token Warning.....	35
Figure 72: Token Management Utility: Wipe Token dialog .....	36
Figure 73: Token Management Utility: Wipe Token dialog completed.....	37
Figure 74: Token Management Utility: Your token is being wiped .....	37
Figure 75: Token Management Utility: The operation completed successfully .....	38
Figure 76: Token Management Utility: SafeSign Token .....	38
Figure 77: Wipe Token: Device Error .....	38
Figure 78: Token Management Utility: Initialise Token dialog .....	39
Figure 79: Browse for Folder.....	40
Figure 80: Initialise Token: Import CA Certificates .....	40
Figure 81: Token Management Utility: Token is being initialised .....	41
Figure 82: Token Management Utility: The operation completed successfully .....	41
Figure 83: Token Management Utility: Change transport PIN .....	41
Figure 84: Change transport PIN dialog .....	42
Figure 85: Change transport PIN: Your PIN was successfully changed .....	42
Figure 86: Token Management Utility: Change PIN.....	43
Figure 87: Token Management Utility: Changing the PIN .....	43
Figure 88: Token Management Utility: Your PIN was successfully changed.....	44
Figure 89: Token Information: PIN Status.....	44
Figure 90: Token Management Utility: Change PIN.....	45
Figure 91: Change PIN: PIN incorrect .....	45
Figure 92: Change PIN: You have only 1 attempt left .....	45
Figure 93: Change PIN: PIN locked.....	46
Figure 94: Change PIN: The PIN has previously been entered incorrectly.....	46
Figure 95: Token Management Utility: Unlock PIN .....	47
Figure 96: Unlock PIN: Your PIN was successfully unlocked .....	47
Figure 97: Token Management Utility: Change PUK .....	48
Figure 98: Change PUK: Your PUK was successfully changed .....	48
Figure 99: Token Information: PUK Status .....	49
Figure 100: Token Management Utility: Change PUK .....	50
Figure 101: Change PUK: PUK incorrect .....	50
Figure 102: Change PUK: You have only 1 attempt left.....	50
Figure 103: Change PUK: PUK locked .....	51
Figure 104: Change PUK: The PUK has previously been entered incorrectly.....	51
Figure 105: Token locked.....	52
Figure 106: Token Management Utility: Token Information .....	52

## About the Product

---

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

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

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

SafeSign 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 Standard Version 2.0 for Windows supports the following tokens (as described in the product description):

- STARCOS SPK smart cards developed by [Giesecke & Devrient GmbH](#) (G&D): SPK2.3, SPK2.3 RawRSA, SPK2.4, SPK2.4 FIPS, and SPK2.5 Dual Interface (DI);
- The [Rainbow Technologies](#) iKey 3000 USB token with the completed STARCOS SPK 2.3 operating system;
- The Giesecke & Devrient StarKey100 USB token with the completed STARCOS SPK 2.3 / 2.4 operating system;
- Java Card v2.1.1 / OpenPlatform 2.0 compliant Java smart cards: Aspects OS755 v2.8, Axalto e-gate, Axalto Cyberflex Access Developer 32k, Axalto Cyberflex 64Kv1 and 64Kv2, G&D Sm@rtcafé Expert v2.0, G&D Sm@rtcafé Expert 64K, G&D STARSIM Java, Gemplus GemXpresso 211pk/Pro R3, IBM JCOP 20/21/30/31, MartSoft Java card, Oberthur CosmopolIC v4, Orga JCOP 20/30.

SafeSign comes in a standard version with an installer for the following Windows environments<sup>1</sup>:

- Windows 98 SE, Windows ME
- Windows 2000, Windows XP (Professional), Windows 2003 Server

In principle, SafeSign supports any PC/SC compliant smart card reader. However, to avoid power problems, smart card readers must be capable to provide at least a current of 60mA. PC/SC driver software is available from the web site of the smart card reader manufacturer. A.E.T. Europe is constantly seeking to extend the range of PC/SC smart card readers supported by SafeSign. Please contact us if you would like to find out about certifying your smart card reader.

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

---

<sup>1</sup> Windows NT 4.0 is supported up to SafeSign 1.0.9.04, in line with Microsoft's end-of-life policy.

## About the Manual

---

This manual is specifically designed for users of SafeSign Standard Version 2.0 for Windows, who wish to use their SafeSign token to enhance the security of their communications via the Internet.

It describes the functionality provided by the SafeSign Token Management 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 Application User Guides to find out how to generate a key pair and download a certificate onto your SafeSign token and how to use it to enhance the security of your client application.

Note that the actual operations available to you by default as a user, may have been limited by the administrator, who may have set appropriate permissions and limitations with regard to the functionality included in the Token Management Utility.

In order to install SafeSign and to set up your SafeSign token for use, follow the instructions in the manual, which describe how to initialise your token and perform various operation 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. 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 **blue**.

This document is part of the user documentation for SafeSign.

# 1 SafeSign Token Management Utility

The SafeSign installation package installs the SafeSign PKCS #11 Library and Cryptographic Service Provider (CSP), allowing users to store public and private data on a personal token, either a smart card or USB token.

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

The Token Management Utility (TMU) has been specifically designed for (end-)users. It allows users to perform some basic token operations (such as initialise token, change PIN) and provides users with an easy tool for viewing, importing and transferring their Digital IDs.

The SafeSign Token Management Utility enables you to personalise your token to be part of your secure applications. To personalise your token, you will need to initialise it, which involves deleting all information that may be stored on the token and (after changing the token transport PIN, if set) set a personal PIN.

The SafeSign Token Management Utility offers three menu options:

1. **Digital IDs** menu, including such features as viewing and importing your Digital IDs and CA certificates;
2. **Token** menu, including such features as initialising your token and changing its PIN;
3. **Help** menu



## Note

---

*The actual menu items available to the user may depend on the settings your administrator has made available. For example, the administrator may have decided not to make the Change PUK item available to the user. For more details, see the SafeSign Administrator's Guide (Administrator\_Guide\_SafeSign\_v3.2).*

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

This chapter will briefly describe where to find and how to start the SafeSign Token Management Utility ([paragraph 1.1](#)) and some information with regard to:

- Version information (the **Help** menu of the SafeSign Token Management Utility) in [paragraph 1.2](#)
- The unique multi-language feature of SafeSign in [paragraph 1.3](#)
- The use of secure Class 2/3 PIN pad readers in [paragraph 1.4](#)

[Chapter 2](#) will deal with the **Digital IDs** menu of the Token Management Utility

[Chapter 3](#) will deal with the **Token** menu of the Token Management Utility



## Removal of the token

---

For all token operations such as token initialisation, change PIN etc., described in this user guide, do not remove the token from the smart card reader or USB port when performing such operations. Removal of the token may lead to damaging the data stored on the token.

When your smart card reader has an LED, do not remove your smart card from the reader as long as the LED flashes or is red.

---

## 1.1 Introduction

You will find the SafeSign Token Management Utility in the Programs menu.

Click **Start > Programs > SafeSign Standard > Token Management:**

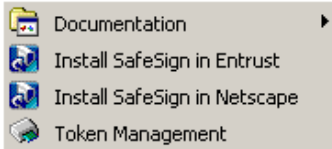


Figure 1: SafeSign menu



### Note

*Under Windows 2000, XP, and ME there will also be a shortcut to the SafeSign Token Management Utility in the Control Panel:*

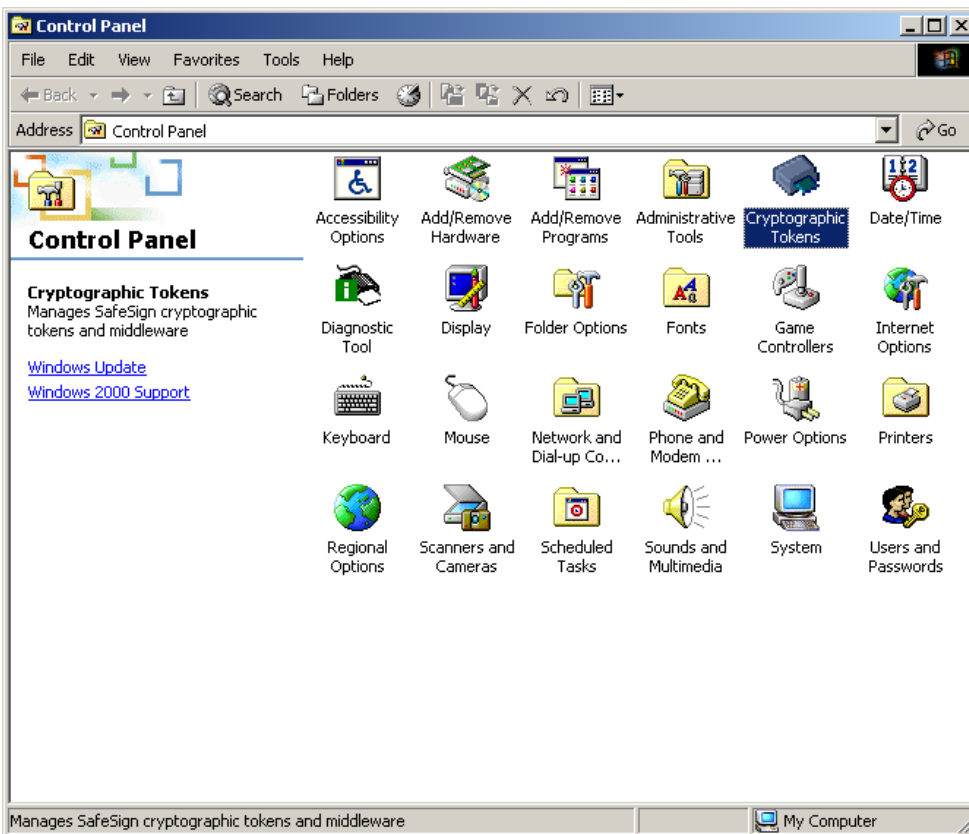


Figure 2: Control Panel: Cryptographic Tokens

Upon clicking **Token Management**, the SafeSign Token Management Utility will open:

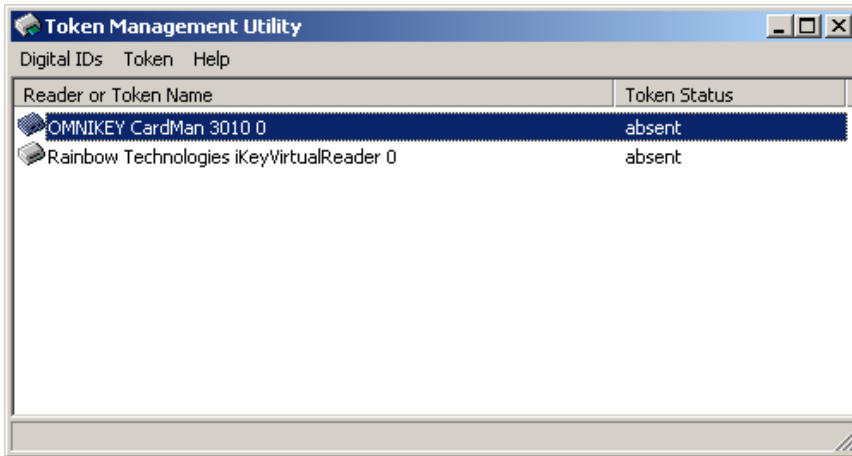


Figure 3: Token Management Utility: Reader Name

This window shows you which smart card reader(s) have been installed on your PC and the status of the token. Note that it is possible that more than one smart card reader has been installed on your PC, e.g. both a PC / SC serial reader (CardMan 3010) and a USB reader/token (iKey 3000), as [above](#).

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

When no token is inserted in the smart card reader, the name of the smart card reader will be listed.



**Note**

*The iKey 3000 token in a USB port is identified by the token label when present (e.g. 'SafeSign Token') and as 'Rainbow Technologies iKeyVirtualReader' when not present.*

*In this manual, the phrase "a token in a smart card reader", may refer to a smart card in a smart card reader or a USB token in a USB port.*

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

Either the token is blank, not yet initialised:

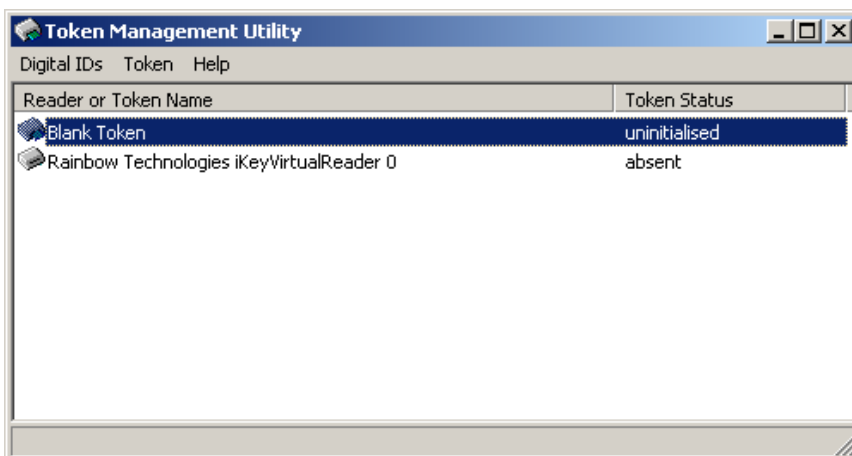


Figure 4: Token Management Utility: Blank Token

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

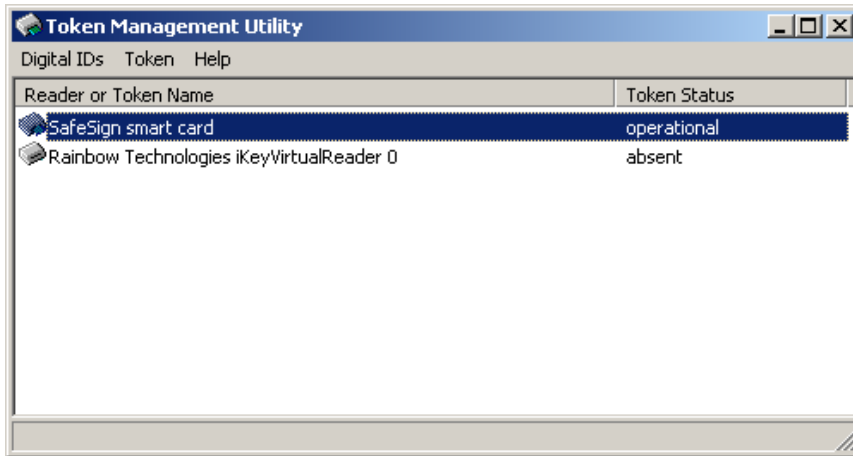


Figure 5: Token Management Utility: Operational Token



### Multiple tokens and readers

You may have multiple smart card readers installed, e.g. a serial smart card reader and a USB smart card reader (as in the examples above).

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

The following image is an example of how the SafeSign Token Management Utility looks when two smart card readers have been installed and two tokens are inserted:

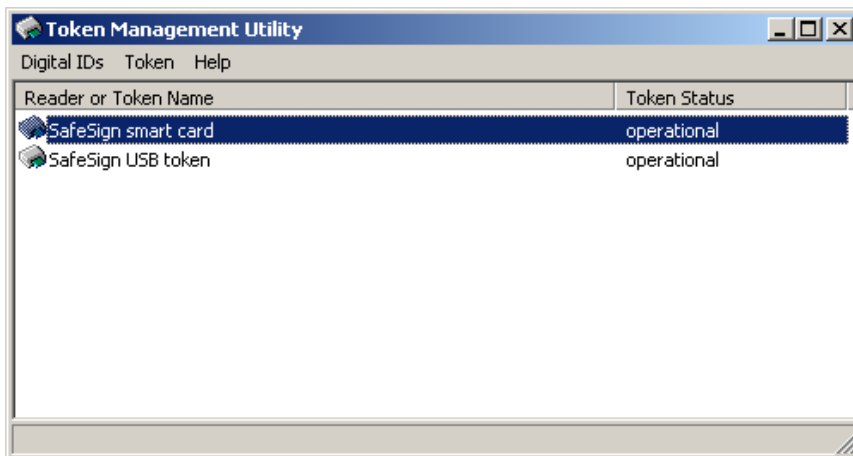


Figure 6: Token Management Utility: Multiple operational tokens



### Token availability

When there is one token in the reader, the Token Management 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.

## 1.2 Help menu

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

### 1.2.1 Versions Info

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

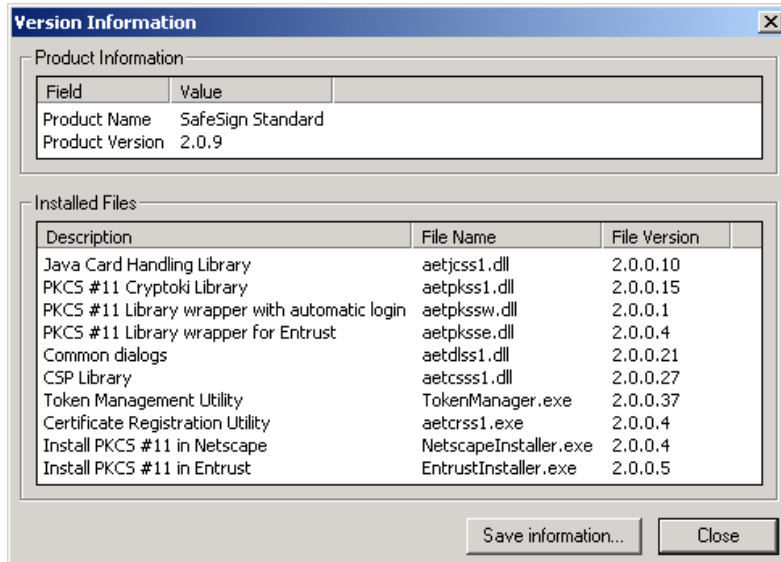


Figure 7: Token Management Utility: Version Information

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

This is particularly useful for support issues, where AET Support will be able to quickly identify the version you are running. Click *Save information* to save the versions in a text file (and name it accordingly) and include it when submitting a support request:

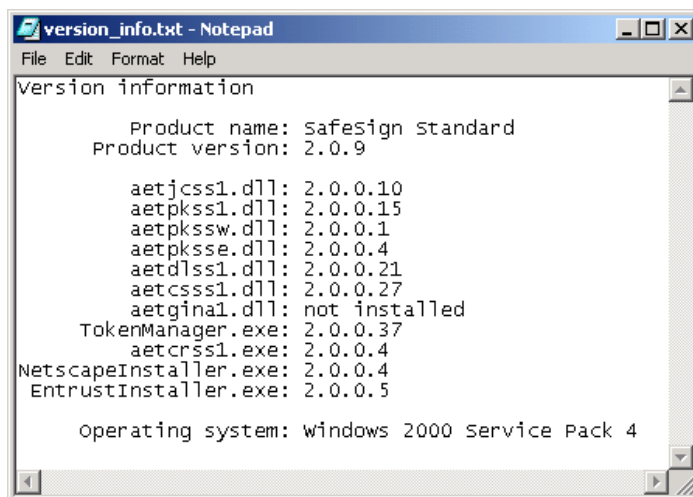


Figure 8: Token Management Utility: Version Information text file

## 1.2.2 About

The *About* item opens the following dialog:



Figure 9: Token Management Utility: About

## 1.2.3 Backwards Compatibility

### 1.2.3.1 SafeSign 1.0.8.xx

Tokens that have been initialised and used (i.e. generated a Digital ID on) with a 1.0.8.xx version of SafeSign can still be used with SafeSign Standard Version 2.0 for Windows, however, they can not be re-initialised as tokens, which were initialised with SafeSign Standard Version 2.0.

A test<sup>1</sup> completion G&D STARCOS SPK 2.3 and SPK 2.4 token that has been initialised with SafeSign version 1.0.8.xx can be re-initialised with a new token label, PUK and PIN code (*Initialise Token*), but the PKCS #15 card structure will be updated to the SafeSign Standard Version 2.0 PKCS #15 structure. A series completion G&D STARCOS SPK 2.3 and SPK 2.4 token that has been initialised with SafeSign version 1.0.8.xx cannot be re-initialised.

Moreover, such tokens (initialised with SafeSign 1.0.8.xx versions), cannot display the total / free amount of bytes in SafeSign Standard Version 2.0. This information cannot be read from the token, as the (old) file structure does not support this computation.

Note that it is not possible to use tokens, initialised with SafeSign Standard Version 2.0 with SafeSign versions 1.0.8.xx. Doing so may cause malfunction and may lead to irreparable damage to the token.

### 1.2.3.2 SafeSign 1.0.9.0x

Tokens that have been initialised and used (i.e. generated a Digital ID on) with a 1.0.9.0x version of SafeSign can still be used with SafeSign Standard Version 2.0 for Windows, however, tokens can only be re-initialised when the token has a test completion (see [above](#)).

Java cards initialised with SafeSign version 1.0.9.0x will be handled as legacy/ series cards, and cannot be re-initialised, but their contents may be wiped.

Note that it is not possible to use tokens, initialised with SafeSign Standard Version 2.0 with SafeSign versions 1.0.9.0x. Doing so may cause malfunction and may lead to irreparable damage to the token.

<sup>1</sup> Completed tokens are completed with a 'series' or 'test' completion. Test completed tokens are intended to be used for evaluation / by developers, series completed tokens are intended to be used by customers / end-users. SafeSign supports both test completed and series ('production') completed tokens.

## 1.3 Multi-language

SafeSign Standard Version 2.0 for Windows contains support for the following languages (apart from the default language, English):

- Basque
- Catalan
- Chinese: Simplified
- Chinese: Traditional
- Croatian
- Czech
- Dutch
- French
- German
- Hungarian
- Italian
- Japanese
- Portuguese
- Russian ( $\geq$  version 2.0.6)
- Spanish
- Thai
- Turkish



### 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 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).*

Multi-language support has been implemented such, to create utmost flexibility for both administrator and user. It may be imagined that an administrator, and not the user himself / herself, is installing SafeSign on a user PC or on a central PC, for which he chooses a particular language. The user will then always be free to change the preferred language of SafeSign. In practice, the language of SafeSign will default to the language set in the locale settings of the user's computer, without the need for the user to change any settings.



### Note

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

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

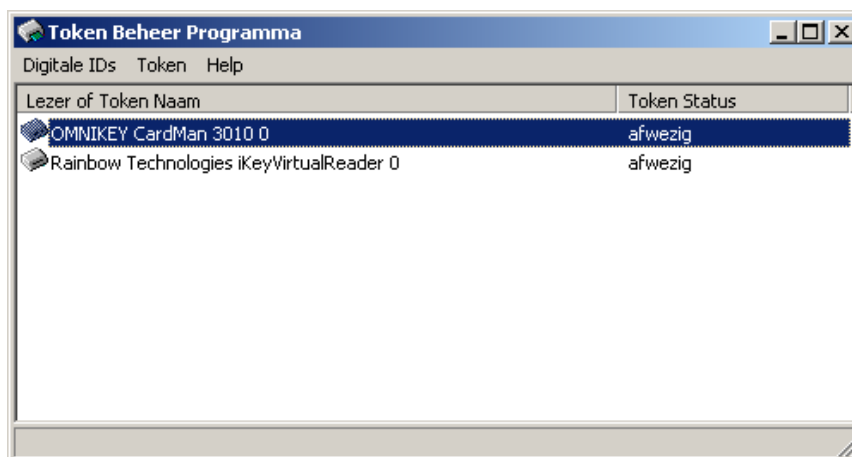


Figure 10: Token Management Utility: Dutch

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

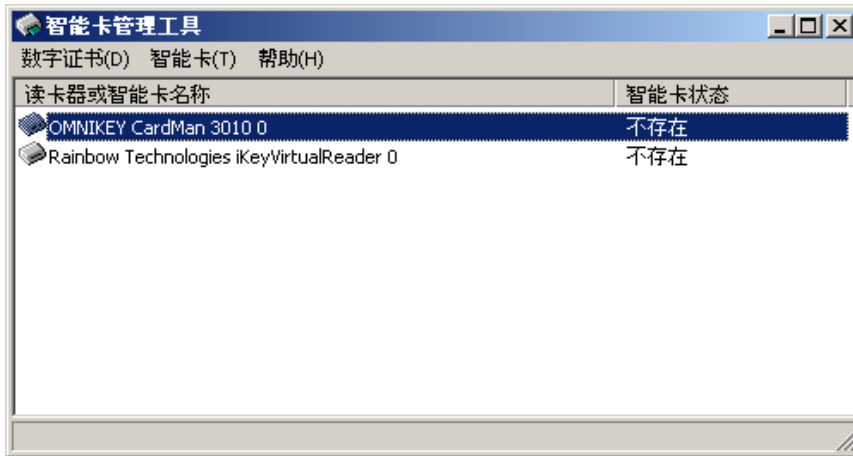


Figure 11: Token Management Utility: Chinese

The user can set the language of SafeSign and its Token Management Utility to the language he prefers to work with, in the **General** tab under **Start > Settings > Control Panel > Regional Options**, by setting the locale (location) to the preferred language:

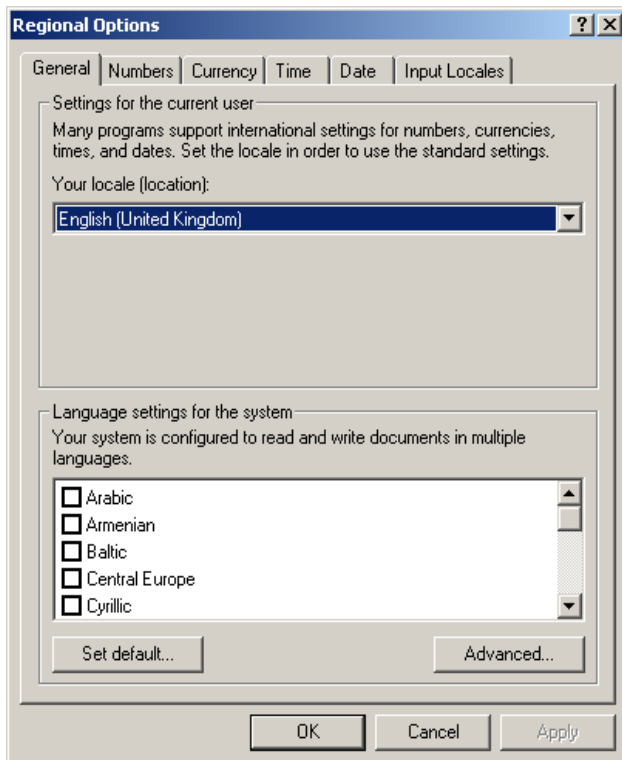


Figure 12: Regional Options: General

If the preferred locale is not present, it can be added, by going to the **Input Locales** tab and adding the preferred locale (for example Basque or Catalan). Note that when no specific locale is set, the default language of SafeSign will be English.

In order to set the locale to any of the languages under **Language settings for the system** (e.g. Thai), you will need to make this language setting the default, by selecting it and clicking **Set default**.

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

**Note**

*Changing the locale will have no effect on the language of the Operating System, or on any other applications. It does provide optimum flexibility, as the user can choose (and change) the language of SafeSign independent of the language of his Operating System. In practice, the language of SafeSign will default to the language set on the user's computer, without the need for the user to make any modifications.*

Note that though SafeSign has been tested for its Installer and utilities to correctly display language-specific characters, locale settings 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. Windows 98 for example, cannot load multiple code pages at the same time, which may lead to problems displaying special characters. In general, selecting the Czech language for SafeSign on a Czech Windows version will not lead to any difficulties, however, selecting the Czech language for SafeSign on an English Windows version (though the locale is set to Czech), may not correctly display some characters (for example the š).

Note that for some applications, such as Microsoft VPN, SafeSign cannot influence the language of the Windows dialogs. These dialogs will appear in the language of the Operating System installed.

## 1.4 Use of pinpad

SafeSign supports a number of Class 2/3 pinpad readers:

1. G&D CashMouse (Class 3, identical to SCM STR 391)
2. Omnikey CardMan Trust (Class 2)
3. Reiner SCT Cyberjack pinpad (Class 2)

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

- In the Token Management Utility, all functions apart from **Initialise Token** have been "pinpad-enabled"<sup>1</sup>.
- 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 Netscape and Mozilla, the *Password Entry Dialog* (Netscape 4.7x) or *Prompt* (Netscape 7.x, Mozilla) will appear. Do not enter the PIN on your computer's keyboard, but click **OK** and then enter the PIN on the reader's pinpad.
- For Windows smart card logon, when you have installed the SafeSign GINA, the Microsoft *Log On to Windows* dialog ("PIN:") will be replaced by the display of a screen that instructs you to enter your PIN on the secure pinpad reader (when prompted).
- 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 Token Management Utility will display a wrong PIN error on screen. Note that upon entering an incorrect PIN in an application, there will be an indication that the PIN is wrong, but no possibility to enter a correct PIN (except in the case of the CashMouse). This is due to the fact that for so-called alternative authentication (as with the use of a pinpad reader) the verification of the PIN is outside of the control of the CSP.

<sup>1</sup> 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.



## Secure PIN entry

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

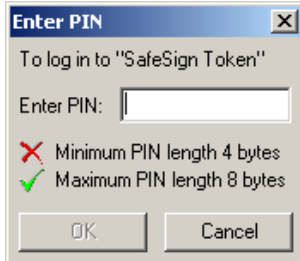


Figure 13: Enter PIN

This may also refer to the entry of a PIN on the pinpad reader's keypad, either instructed by the reader's display or by an on-screen dialog, for users with a secure pinpad reader.

### 1.4.1 G&D CashMouse

In addition to a pinpad, the CashMouse (identical to SCM [STR391](#)) also has a display. Instructions on entering the PIN will be given on the display of the reader, not on your computer screen.

Using the G&D CashMouse and the German drivers from <http://www.scm-support.com/cashmouse/>, the following applies:

When entry of a PIN is required, the reader will instruct you "**Bitte Geheimzahl eingeben**". As soon as you have entered the PIN on the pinpad, you have to click "**Bestätigung**" (OK / Confirm) on the pinpad.

To abort a PIN entry, click "**Abbruch**" (Cancel / Abort)

To correct the PIN entry (when you have entered a wrong PIN), click "**Korrektur**" (Correct / Clear)

When you have entered an incorrect PIN or when the token is locked, the following message will be displayed in the reader's display: "**Geheimzahl falsch/gesperrt**".

## 1.4.2 Omnikey CardMan Trust

When using the [Omnikey](#) CardMan Trust, you will be instructed through on-screen dialogs to enter the PIN for the token on the pinpad (*Secure PIN Entry*):



Figure 14: Secure PIN Entry: Please enter PIN

After entering the PIN on the reader's pinpad, click the **green** button with the ✓ mark, confirming the PIN entry:

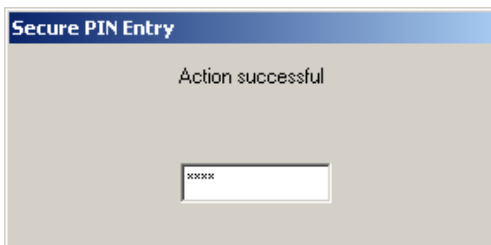


Figure 15: Secure PIN Entry: Action Successful

To correct the PIN entry (when you have entered a wrong PIN), click the **yellow** button with the ← mark.

To abort a PIN entry, click the **red** button with the X mark:



Figure 16: Secure PIN Entry: Abort

When you have entered a wrong PIN or when the token is locked, the following dialog will appear on-screen:



Figure 17: Secure PIN Entry: PIN wrong/barred

### 1.4.3 Reiner SCT Cyberjack pinpad

When using the [Reiner SCT](#) Cyberjack pinpad, you will be instructed through on-screen dialogs to enter the PIN for the token on the pinpad (*Sichere PIN Eingabe*):

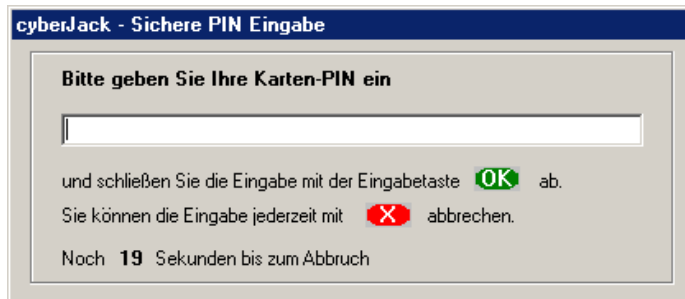


Figure 18: cyberJack – Sichere PIN Eingabe

After entering the PIN on the reader's pinpad, click the **green OK** button, confirming the PIN entry.

To abort a PIN entry, click the **red** button with the **X** mark.

Note that after you have entered the first PIN character, you will have 5 seconds to enter each following PIN character, which is not something controlled by the middleware, but by the reader (drivers) and is according to Internet banking standards.

When you have entered a wrong PIN or when the token is locked, no further feedback from the reader will be displayed on-screen, but the Token Management Utility will display an error message and applications such as Internet Explorer will not perform the operation requested (for example, in case of web authentication, "the page cannot be displayed").

## 2 Digital IDs menu

The **Digital IDs** menu contains the following items:

[Show Registered Digital IDs](#)

[Import Digital ID](#)

[Import Certificate](#)

[Exit](#)

### 2.1 Show Registered Digital IDs

The SafeSign Token Management Utility allows (end-) 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* shows the Digital IDs that are stored on the token and/or have been registered in the local certificate store.

**Note** that it may take some time for Digital IDs to be registered and displayed in the *Digital IDs* dialog, depending on the amount of objects on the token and the (speed of the) token reader used.

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

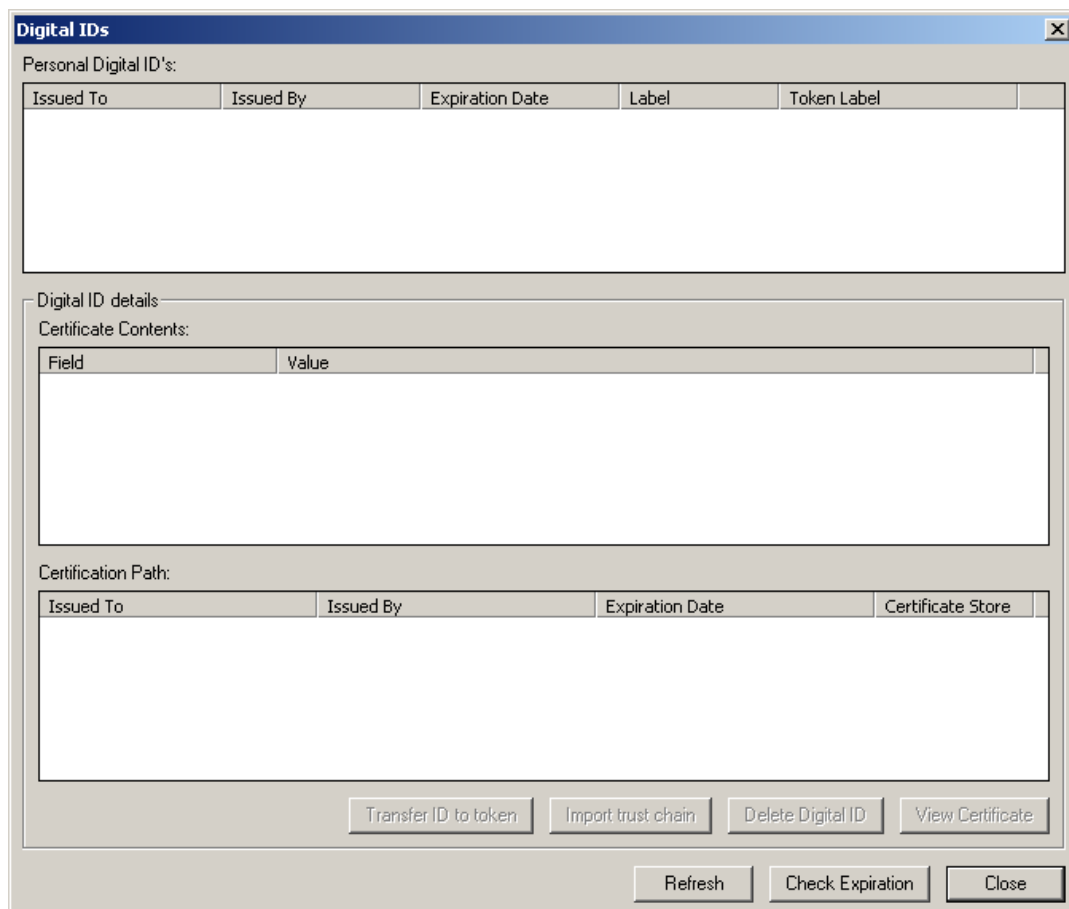


Figure 19: Digital IDs: No personal Digital IDs

When a Digital ID has been generated or imported on the token, the *Digital IDs* dialog will look like this (if the Digital ID is selected as below):

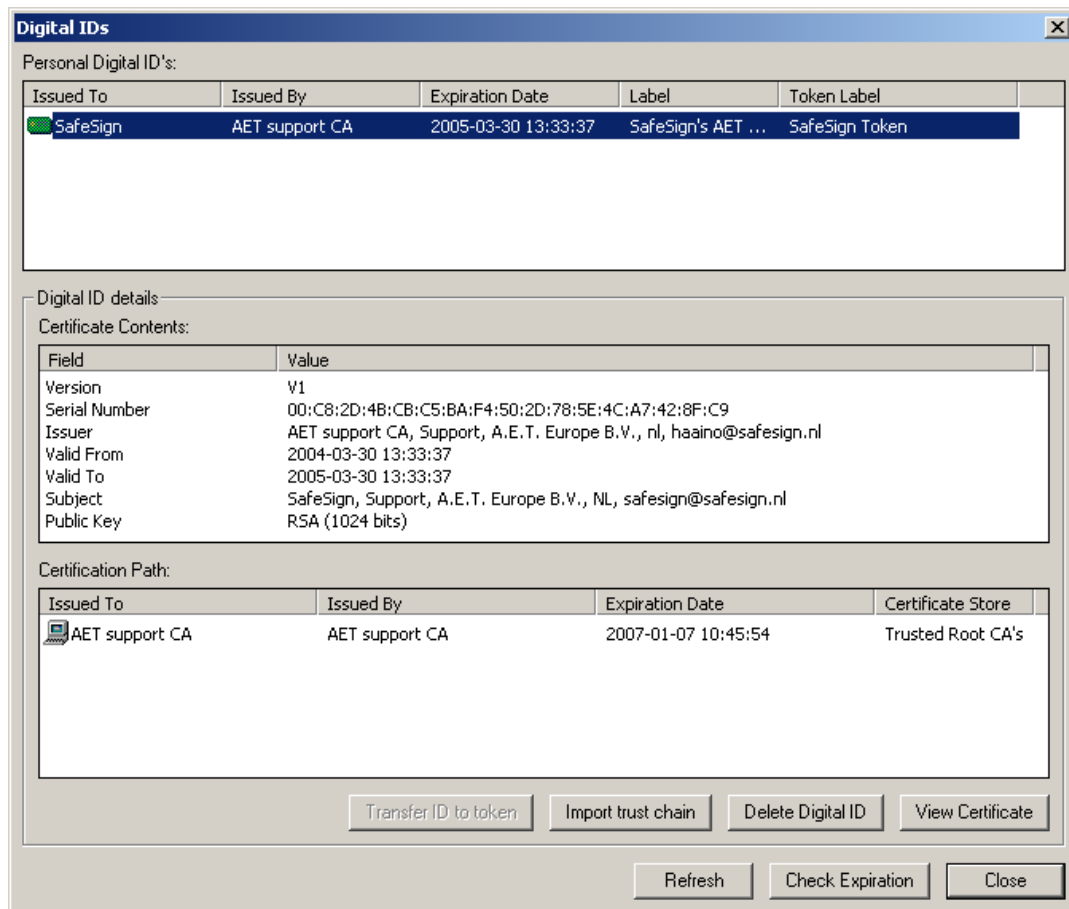


Figure 20: Digital IDs: Digital ID stored on token

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

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

To transfer a Digital ID to a token: refer to [paragraph 2.1.1](#)

To import the trust chain to a token: refer to [paragraph 2.1.1](#)

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):

- [Transfer ID to token](#)
- [Import trust chain](#)
- [Delete Digital ID](#)
- [View Certificate](#)
- [Refresh](#)
- [Check Expiration](#)
- [Close](#)

These functions will be described in the next paragraphs.



## Token missing

When the token that contains the Digital ID is not in the smart card reader, while the certificate is registered, the *Digital IDs* dialog will look like this:

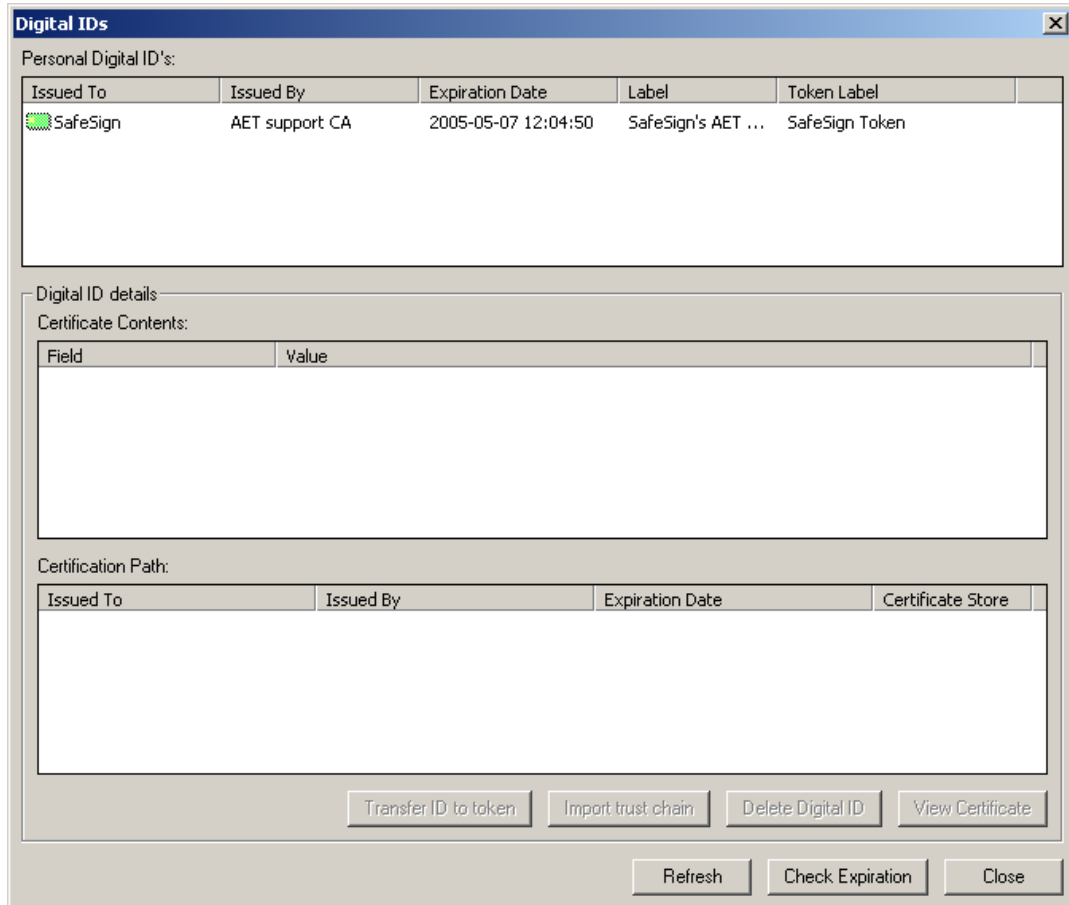


Figure 21: Digital IDs: Token Missing

The token icon is now transparent.

This situation may / will most likely occur if a user has left the token in the reader while shutting down his computer and then restarted the computer without the token inserted.

Certificate registration does not deregister certificates when shutting down the computer (or logging off).

### 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 that you wish to transfer to your token. 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.

Note that 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.

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:

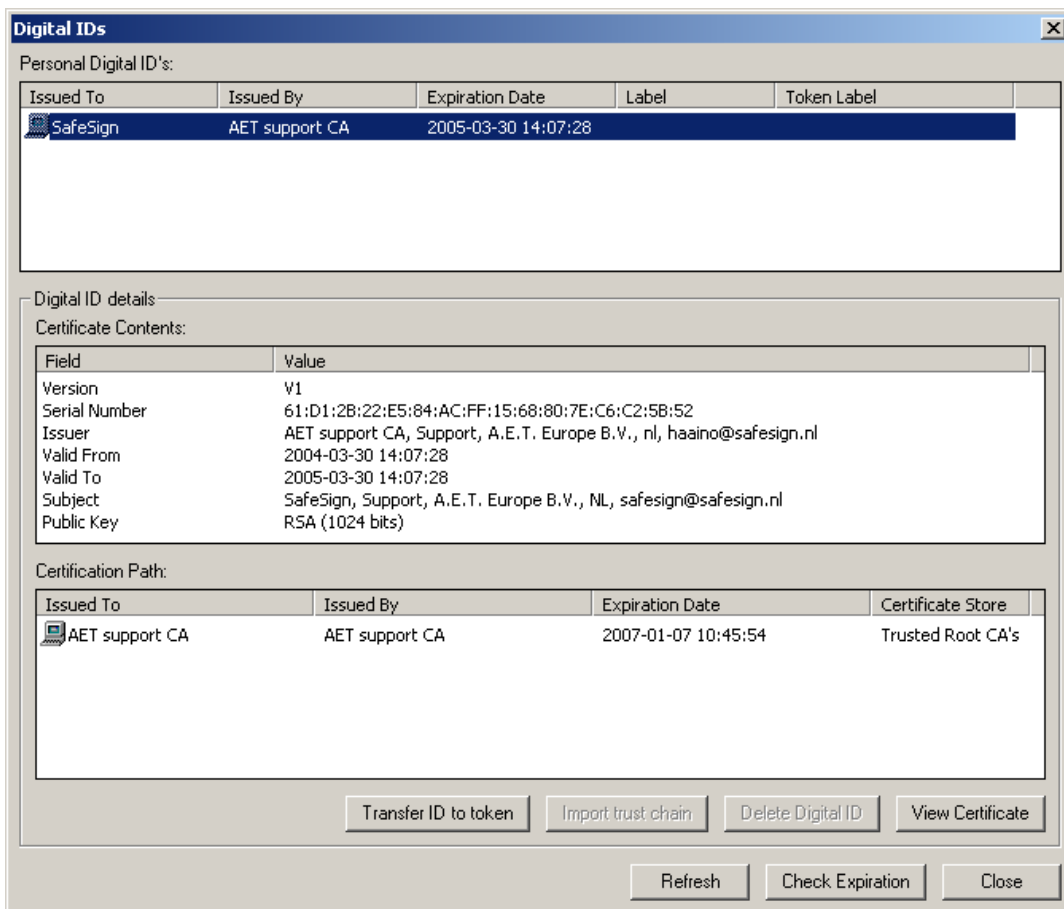


Figure 22: Digital IDs: Transfer ID to token

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

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

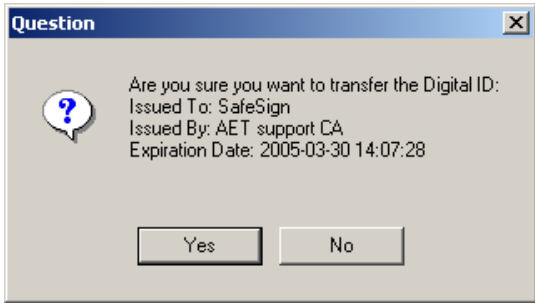


Figure 23: Transfer ID to token: Question

➔ Click **Yes** to transfer the Digital ID specified to the token

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

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

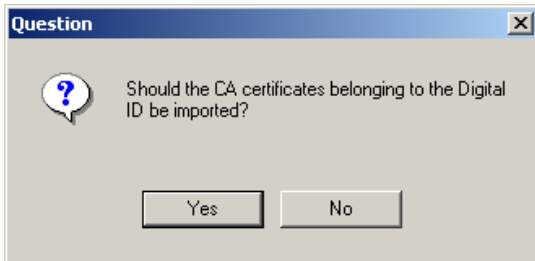


Figure 24: Transfer ID to token: Question CA certificates

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

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

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

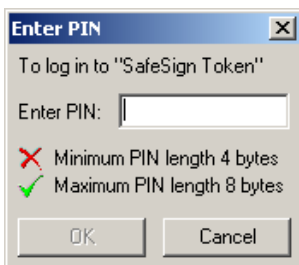


Figure 25: Transfer ID to token: Enter PIN

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

**5** The Digital ID will now be imported:

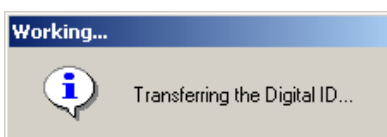


Figure 26: Transfer ID to token: Transferring

6

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

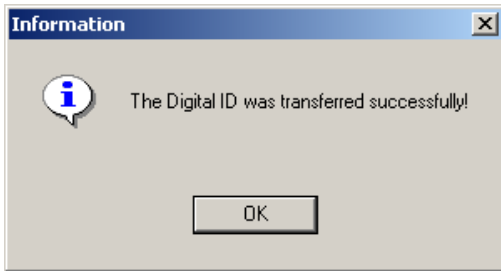


Figure 27: Transfer ID to token: Success

➔ Click **OK**

The Digital ID will now be on the token:

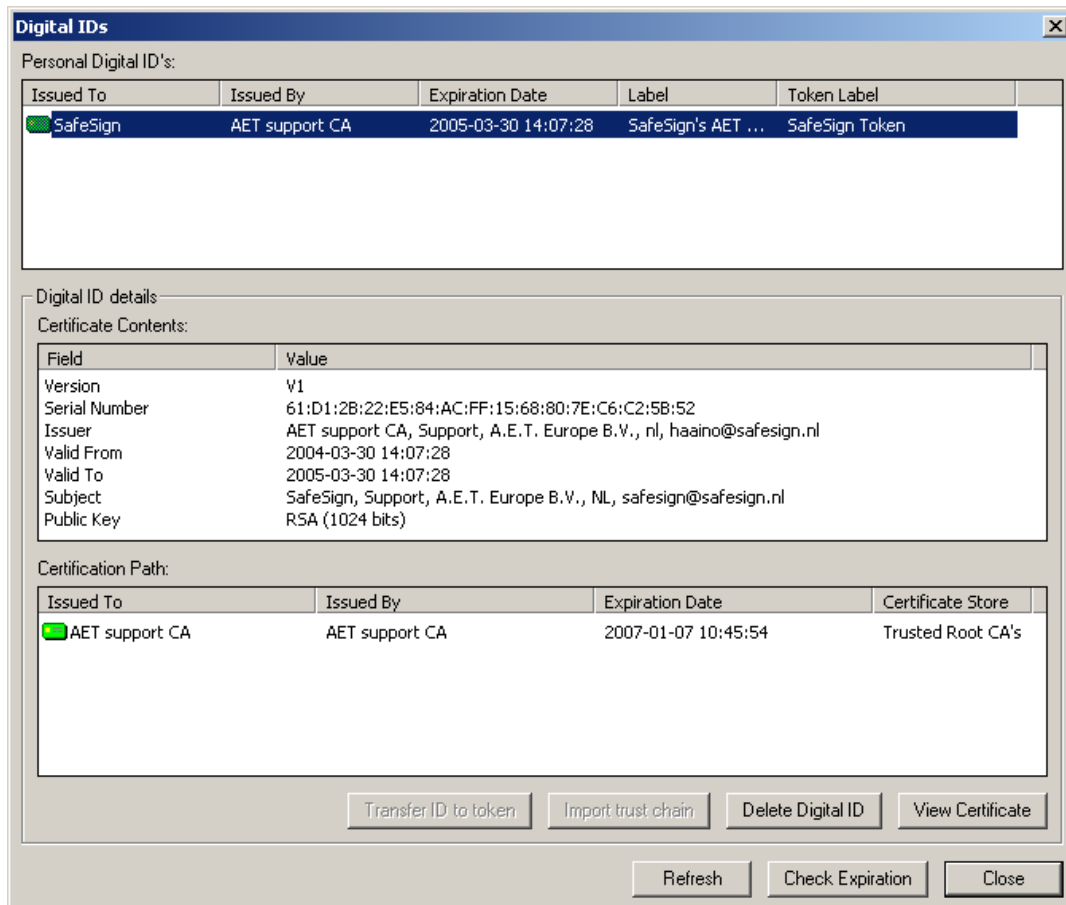


Figure 28: Digital IDs: Personal Digital ID's on token

When you have clicked **Yes** at the prompt to import CA certificates belonging to the Digital ID to the token (Figure 24), the CA certificates for the Digital IDs will also be on the token (as under **Certification Path** in the picture above).



### 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:

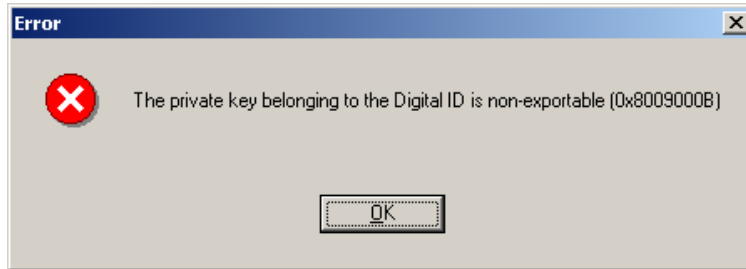


Figure 29: Transfer ID to token: Error

➔ Click **OK** to close this dialog



### Certification Path

When the CA certificate is not available (neither on the token or in the appropriate Microsoft Certificate Store), the *Digital IDs* dialog will look like this:

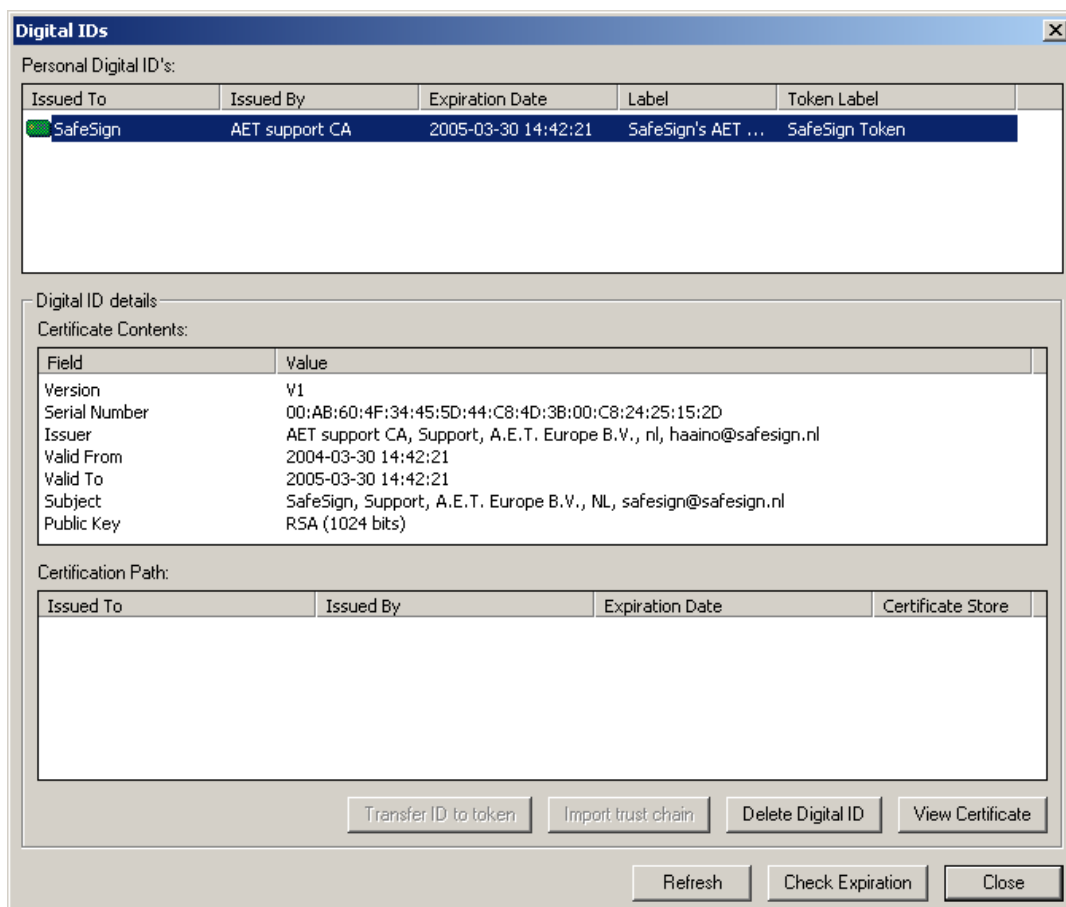


Figure 30: Digital IDs: no certification path

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

When the CA certificate is not on the token (for example when you chose not to import the certificate chain during transferral, see [Figure 24](#)), but it is in the appropriate Microsoft (Trusted Root Certification Authorities) Store, the *Digital IDs* dialog will look like this:

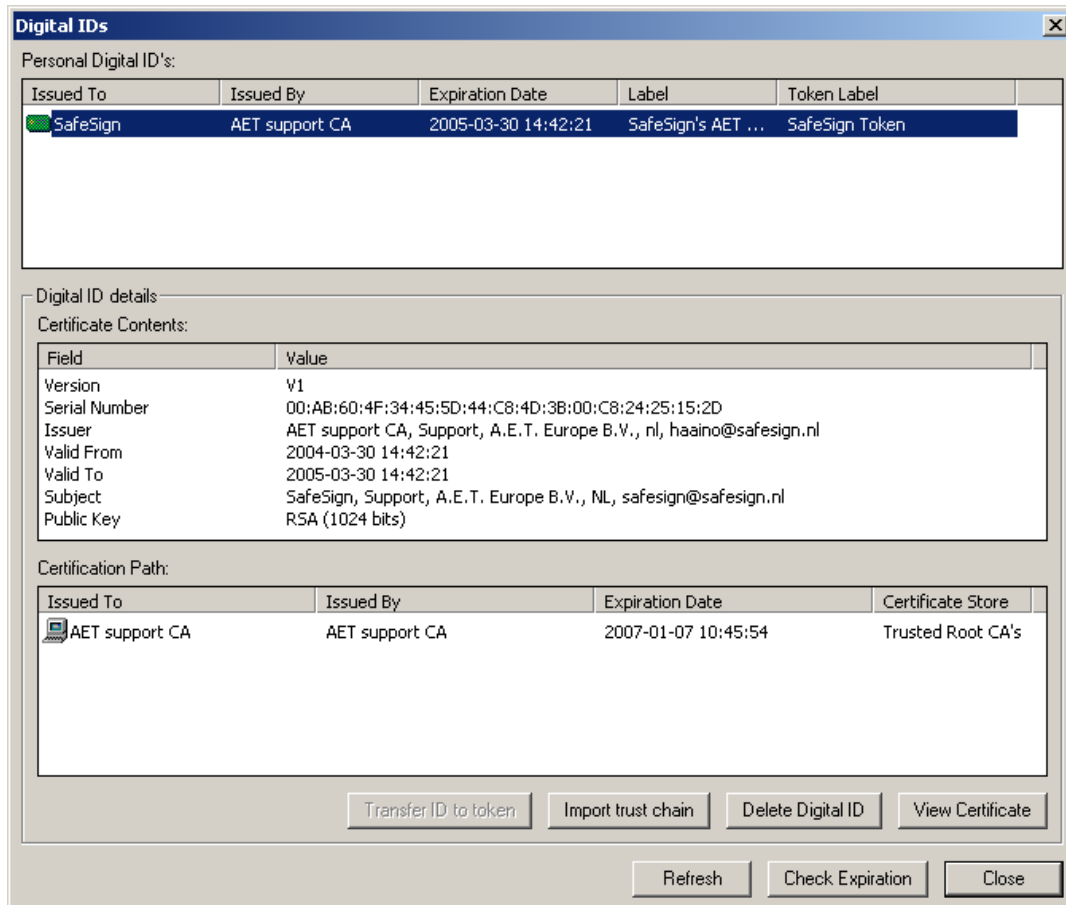


Figure 31: Digital IDs: Certification path not on token

In this case, you may want to import the trust chain onto the token. This is described in [paragraph 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 [paragraph 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:

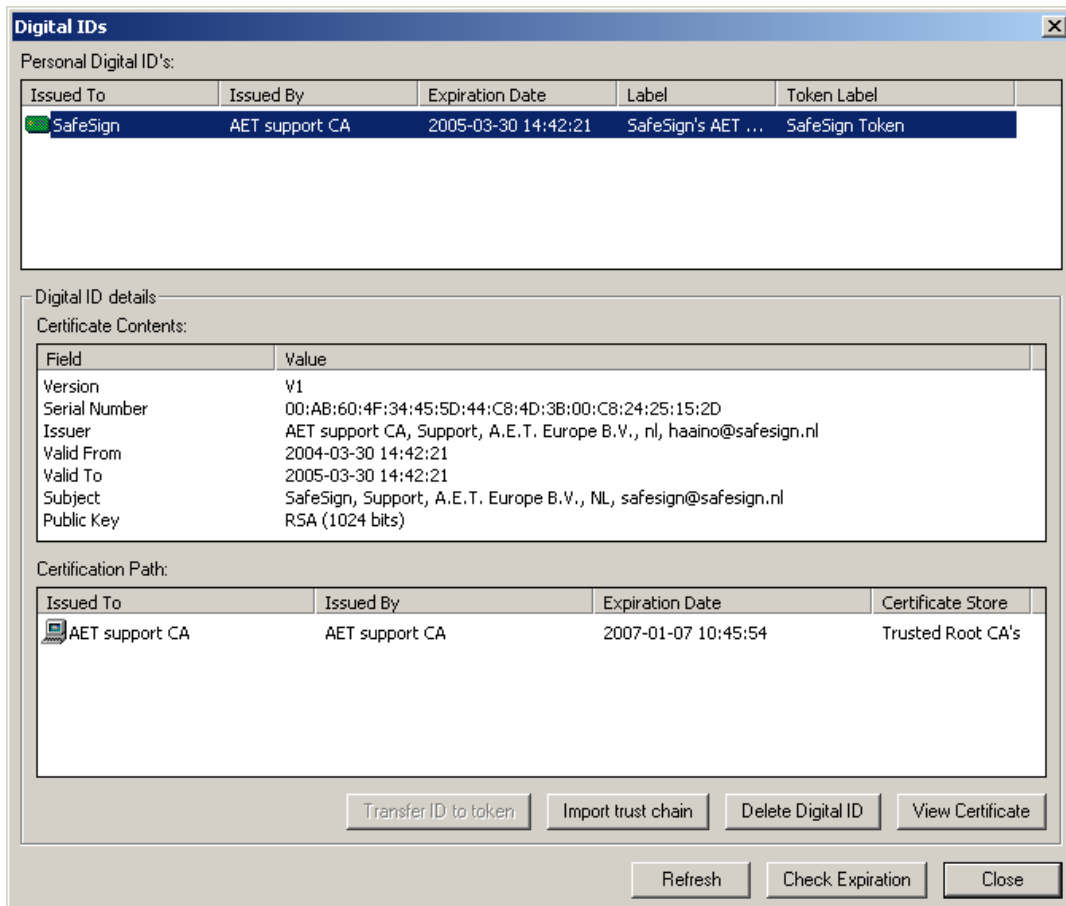


Figure 32: Digital IDs: Certification path not on token

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

2

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



Figure 33: Import trust chain: Enter PIN

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

3 The certificate chain will now be imported:

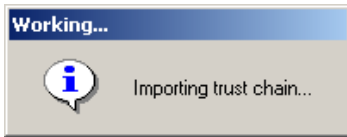


Figure 34: Import trust chain: Importing

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

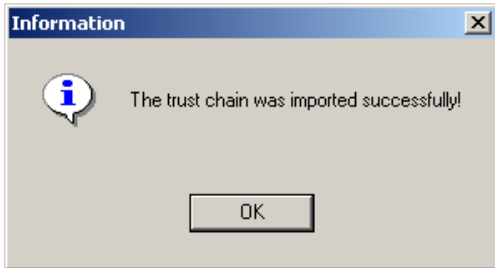


Figure 35: Import trust chain: Success

➔ Click **OK** to close this dialog

The certificate chain will now be on the token:

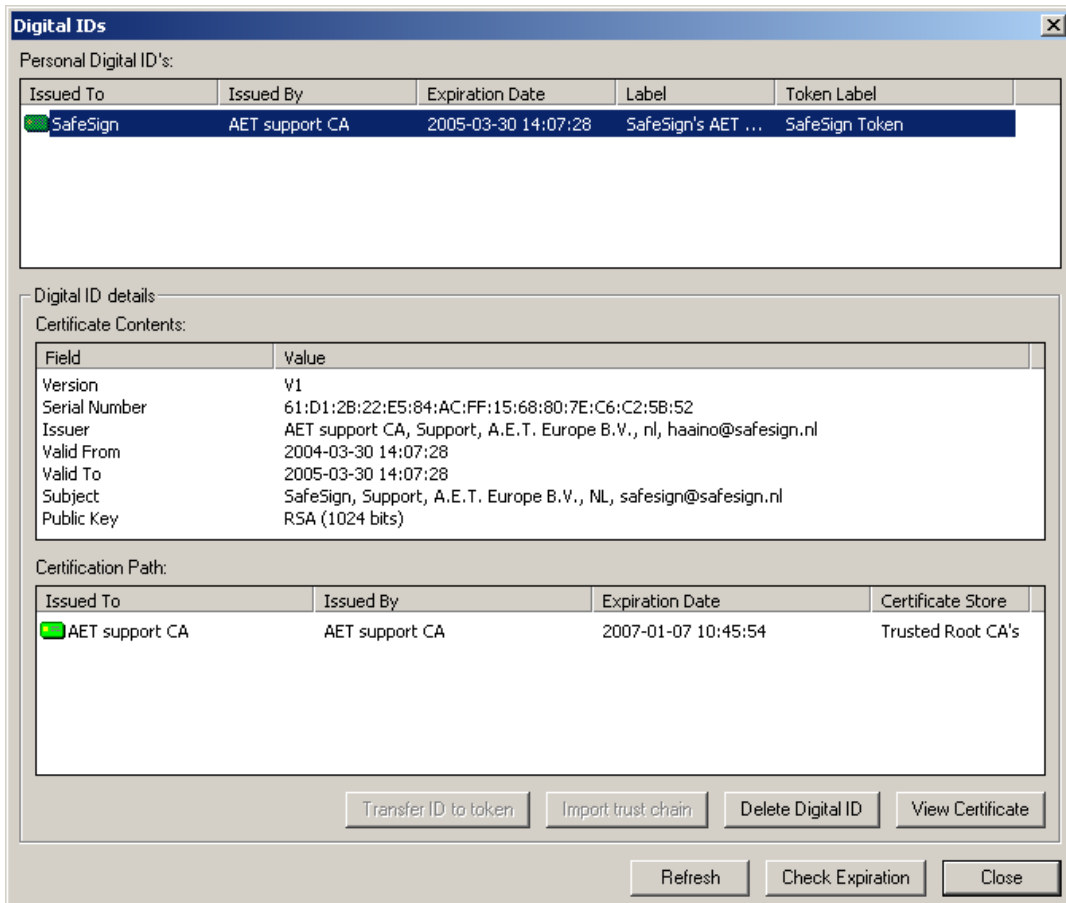


Figure 36: Digital IDs: Certification path on token

### 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 20). Note that you can only delete Digital IDs on the token by means of the Token Management Utility; you can not delete Digital IDs displayed in the *Digital IDs* dialog that are in the Certificate Store (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:

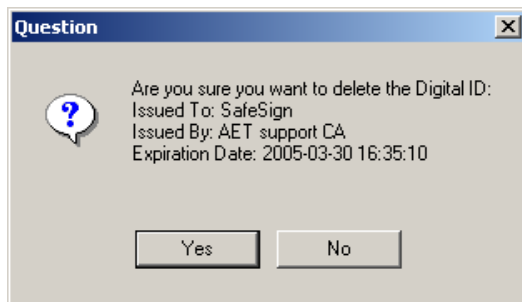


Figure 37: Digital IDs: Are you sure you want to delete Digital ID

→ 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** (Figure 37), you will be asked to enter the PIN for your token:



Figure 38: Delete Digital ID: Enter PIN

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



## PIN / PUK length

SafeSign enforces a minimum and maximum PIN / PUK length. If you enter a PIN / PUK of less than 4 characters or more than 8 characters, you will not be able to click the **OK** button in such instances where the PIN / PUK is required. Only when you enter a PIN / PUK of minimally 4 and maximally 8 characters, will the PIN / PUK be accepted. Note that the minimum / maximum PIN / PUK length may have been set to different values by the administrator.

### 3

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

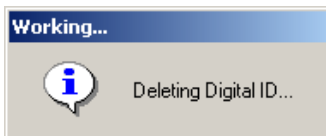


Figure 39: Delete Digital ID: Deleting

### 4

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

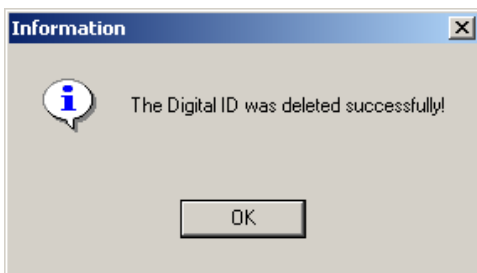


Figure 40: Delete Digital ID: Success

→ Click **OK** to close this dialog

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

### 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:

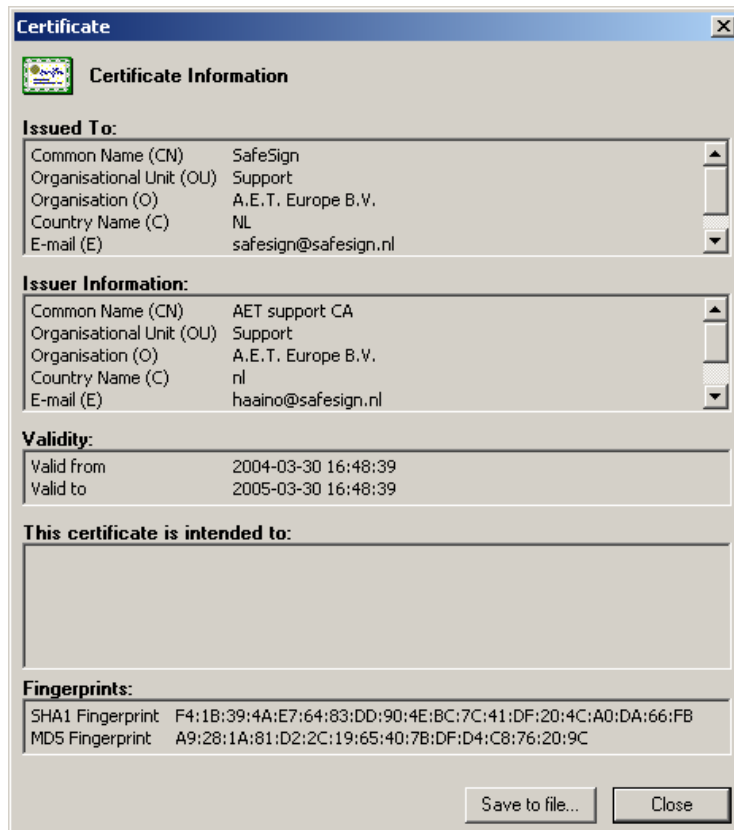


Figure 41: View Certificate: Certificate Information

This dialog will display the available certificate information.

➔ 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):

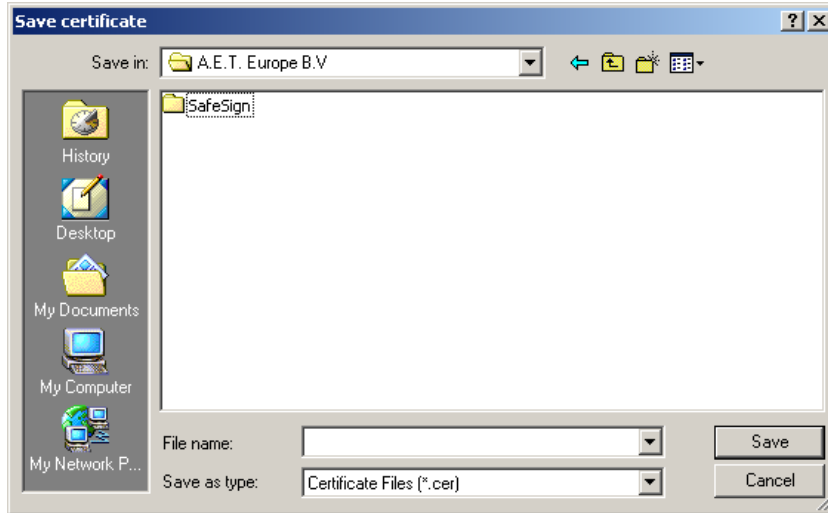


Figure 42: View Certificate: Save certificate

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

### 2.1.5 Refresh

The **Refresh** button allows you to refresh the *Digital IDs* dialog and its contents.

### 2.1.6 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:

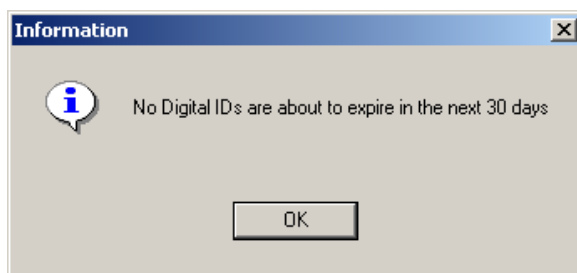


Figure 43: Check Expiration: Information

➔ Click **OK** to close this dialog.

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

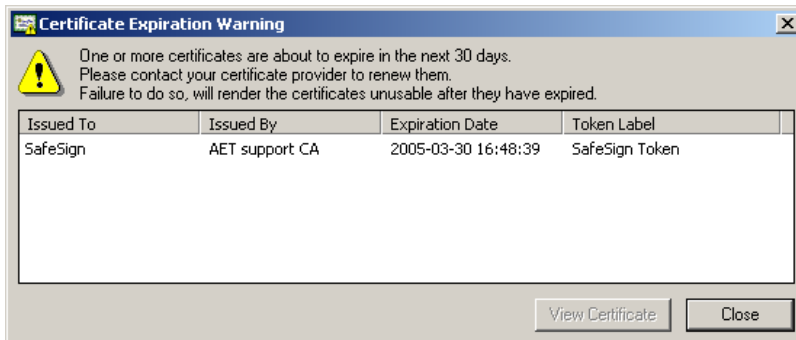


Figure 44: Check Expiration: Certificate Expiration Warning

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<sup>1</sup>.

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



**Note for Administrators**

Refer to the *SafeSign Administrators Guide* for details on how to set and customize the *Certificate Expiration Warning*.



**Certificate Expiration Warning**

The *Certificate Expiration Warning* dialog will also appear by default every time a token is inserted, which contains certificates that are about to expire in the time period specified. In that case, the following dialog will appear (note that the SafeSign Token Management Utility does not have to be open(ed) for this dialog to appear):

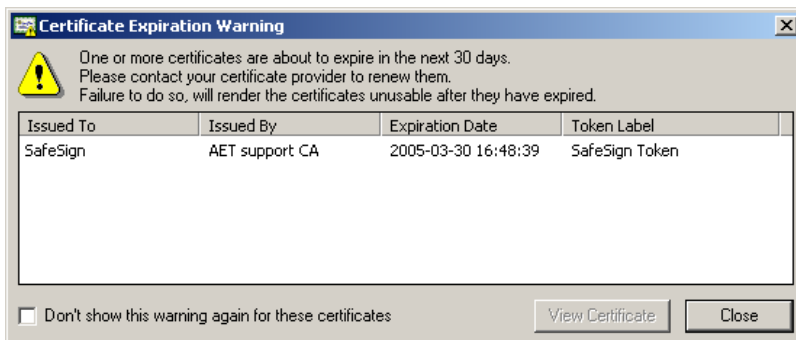


Figure 45: Certificate Expiration Warning

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

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

**2.1.7 Close**

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

<sup>1</sup> Just as Microsoft will keep certificates that are expired in its Certificate Store.

## 2.2 Import Digital ID

The SafeSign Token Management Utility allows you to import a Digital ID on your SafeSign 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.

Note that this procedure can be used to import Digital ID files stored in PKCS #12 or PFX format on your hard disk (or removable media, such as a diskette), whereas the function [Transfer ID to token](#) (as available under **Show Registered Digital IDs**) can be used for Digital IDs present 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 and does not necessarily refer to a certificate issued by Verisign.*

This Digital ID should be stored as a PKCS#12 (.p12) file (Netscape) or a Personal Information Exchange (.pfx) file (Microsoft), which are both formats that contain your private key, on a diskette or on your hard disk.

A file of this format can be obtained either by exporting the keys and certificates from your Netscape Communicator Database (.p12) or by exporting the keys and certificates 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 token.



---

**Note**

*Note that the application (and its version) used determines how the format of a Digital ID looks.*

*For example, when generating a key pair and downloading a certificate on the token in Internet Explorer, Show Token Objects may display a private key + public key + certificate. When generating a key pair and downloading a certificate in Netscape, Show Token Objects may display only a private key + certificate.*

*When SafeSign 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).*

*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**:

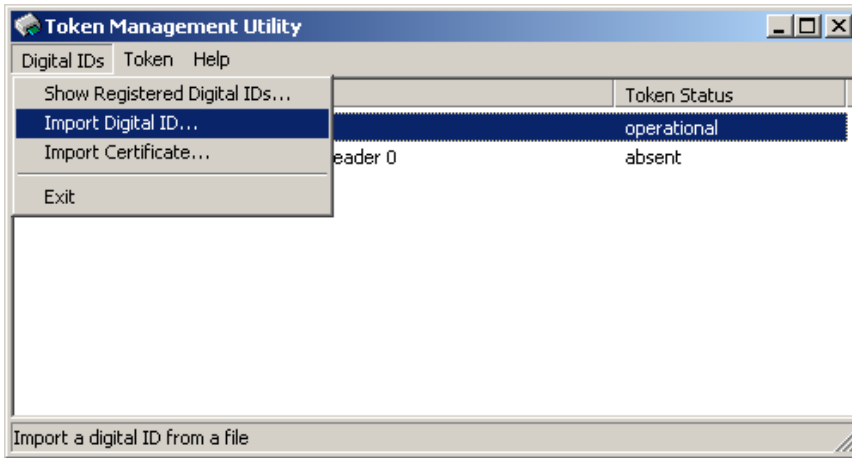


Figure 46: Token Management Utility: Import Digital ID

2 The following dialog will appear:

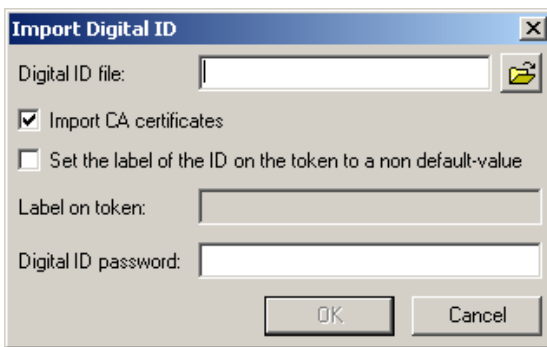



Figure 47: Import Digital ID

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 a diskette. Click on the  symbol to select the location:

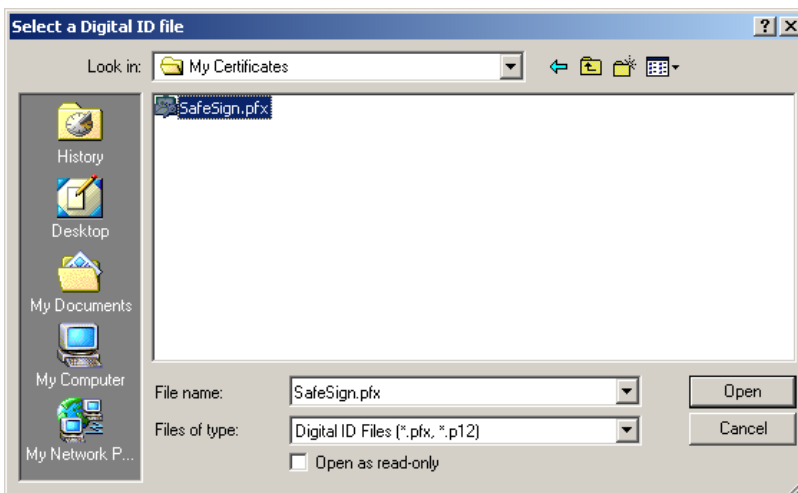


Figure 48: Import Digital ID: Select a Digital ID file

In the above example, the file was stored in: *C:/My Certificates*

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

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

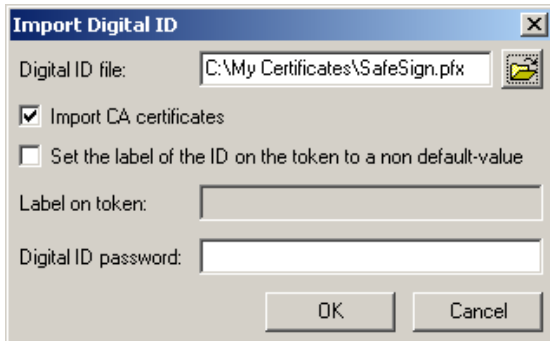


Figure 49: Import Digital ID: Digital ID file selected

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

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 Digital ID, 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, as illustrated below:



Figure 50: Import Digital ID: Label on token

**3** Enter the password for the Digital ID file:

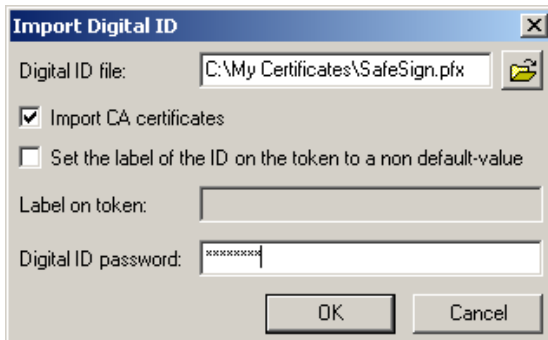


Figure 51: Import Digital ID: Digital ID password entered

➔ 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:

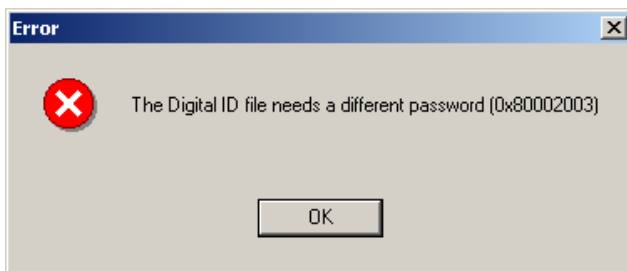


Figure 52: Error: Digital ID needs a different password

➔ 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 51](#)), you will be asked to enter the PIN for the token:

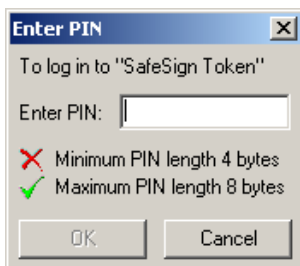


Figure 53: Import Digital ID: Enter PIN

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



## PIN / PUK length

SafeSign enforces a minimum and maximum PIN / PUK length. If you enter a PIN / PUK of less than 4 characters or more than 8 characters, you will not be able to click the **OK** button in such instances where the PIN / PUK is required. Only when you enter a PIN / PUK of minimally 4 and maximally 8 characters, will the PIN / PUK be accepted. Note that the minimum / maximum PIN / PUK length may have been set to different values by the administrator.

5

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

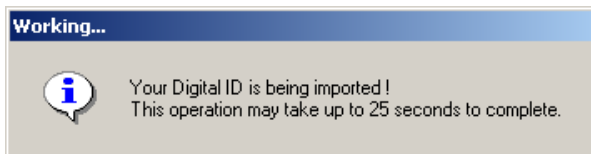


Figure 54: Import Digital ID: Working

→ Your Digital ID is being imported

6

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

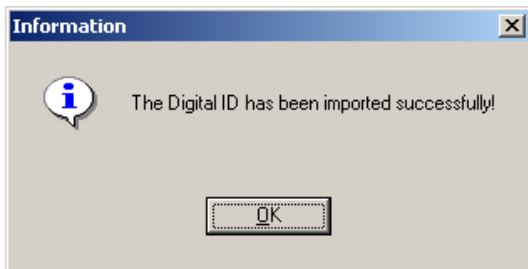


Figure 55: Import Digital ID: The Digital ID has been imported successfully

→ 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 tokens, the following dialog will be displayed:

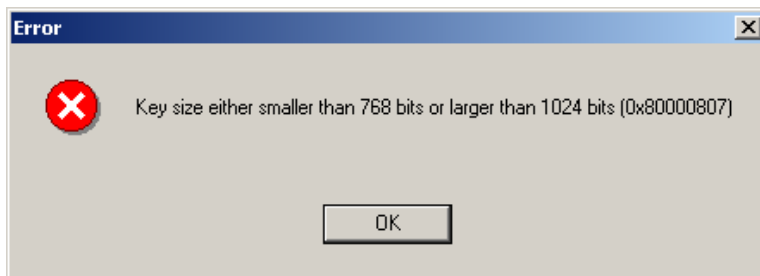


Figure 56: Error: Key Size either smaller than 768 bits or larger than 1024 bits

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:

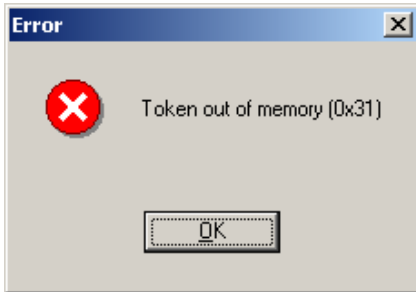


Figure 57: Error: Token out of memory

Click **OK** to close this dialog.

You may check in the *Token Information* dialog (**Token > Show Token Info**) how much space is left on the token. Note that the token may contain parts of the Digital ID file imported (e.g. when it contains multiple certificates).

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:

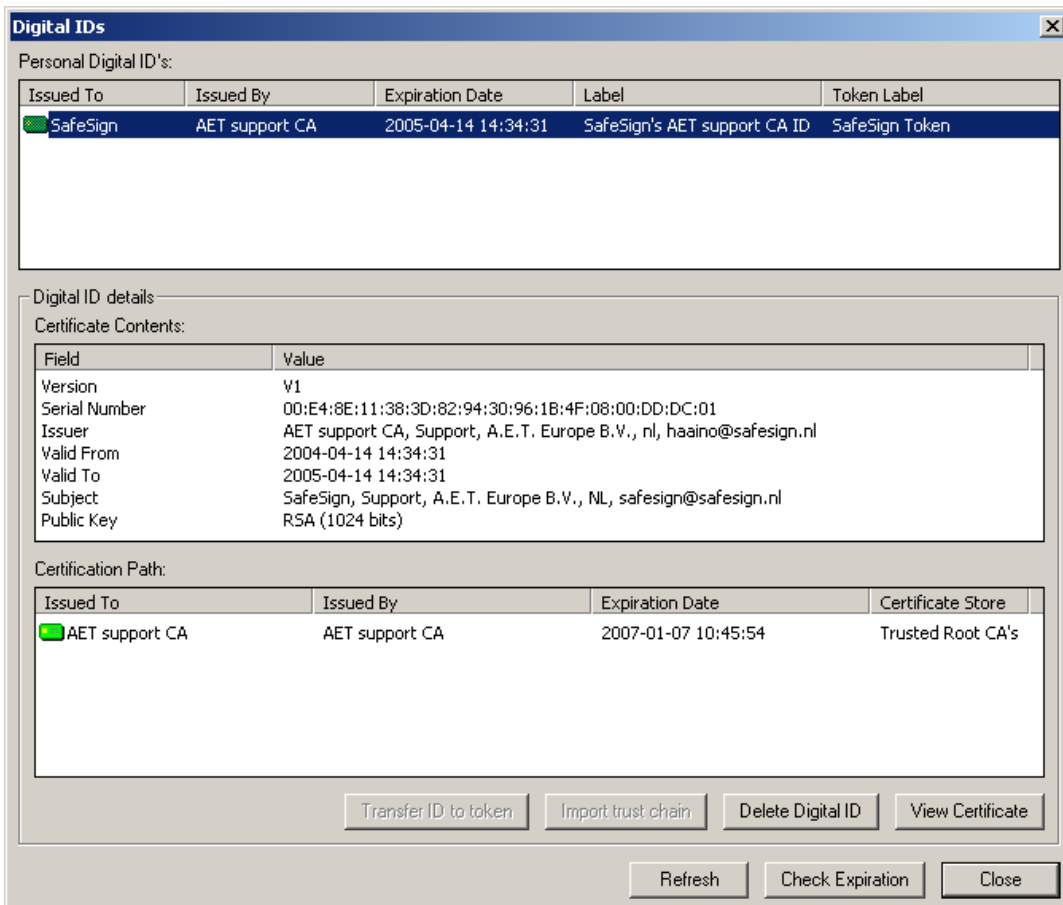


Figure 58: Token Management Utility: Imported Digital ID

## 2.3 Import Certificate

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

Upon using your SafeSign token on another computer, where the CA (root) certificate is not installed, SafeSign will enable you to install the CA certificate, creating a trusted chain for your personal Digital ID (which would not be trusted without the CA certificate that issued it being installed, as in that case "Windows does not have enough information to verify this certificate" because "the issuer of this certificate could not be found").

SafeSign 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 [paragraph 3.1.3](#)

**1**

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

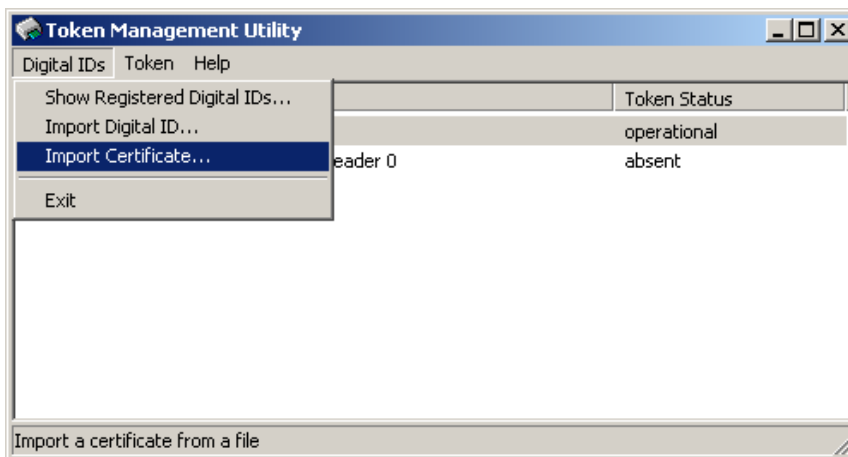


Figure 59: Token Management Utility: Import Certificate

2

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

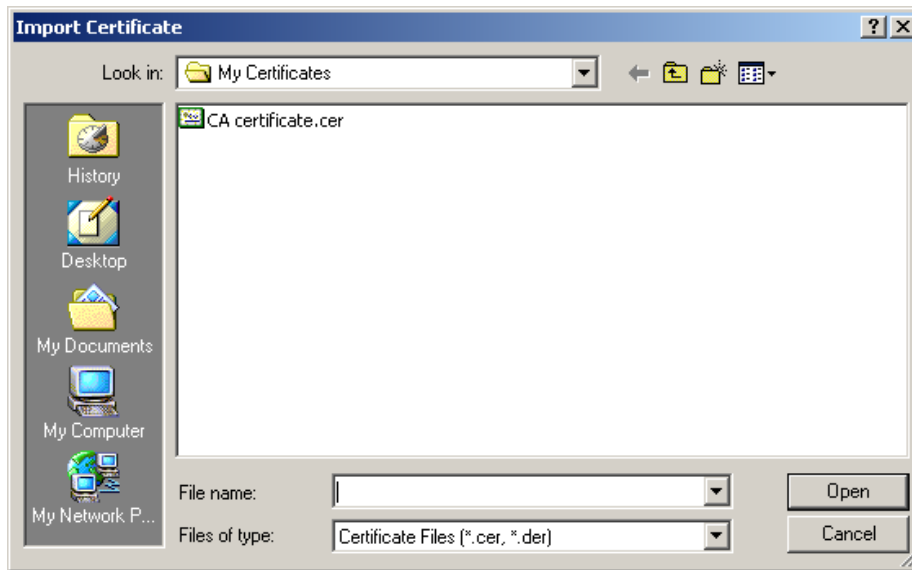


Figure 60: Import Certificate: File name

Specify the location where the Certificate File is stored. The Certificate File can be stored anywhere, either on a hard disk or on a diskette.

In the above example, the file was stored in: *C:/My Certificates*

➔ 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 Token:

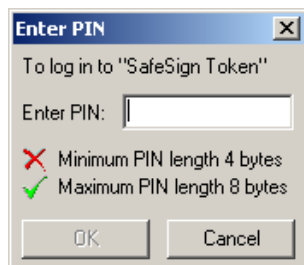


Figure 61: Import Certificate: Enter PIN

➔ Enter the PIN and click **OK**



**PIN / PUK length**

SafeSign enforces a minimum and maximum PIN / PUK length. If you enter a PIN / PUK of less than 4 characters or more than 8 characters, you will not be able to click the **OK** button in such instances where the PIN / PUK is required. Only when you enter a PIN / PUK of minimally 4 and maximally 8 characters, will the PIN / PUK be accepted. Note that the minimum / maximum PIN / PUK length may have been set to different values by the administrator.

**4** Upon clicking **OK**, the Certificate File will be imported:

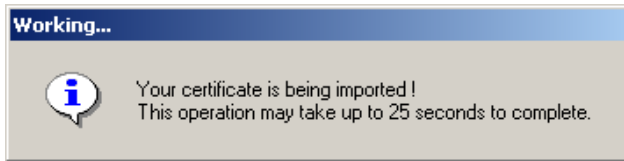


Figure 62: Import Certificate: Your certificate is being imported

This may take up some time to complete, depending on your reader, type of port, operating system, etc.

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

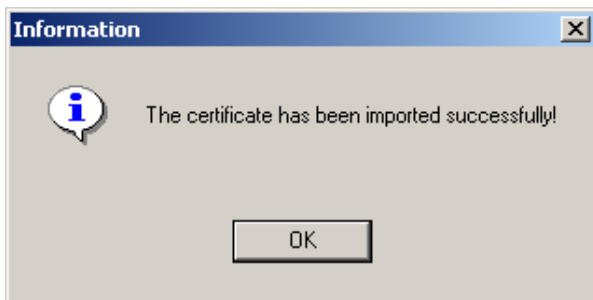


Figure 63: Token Management Utility: Certificate successfully imported

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

## 2.4 Exit

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

### 3 Token Menu

#### 3.1 Initialise Token

The first step after installing SafeSign is to initialise your token (if not yet initialised).

The values written on the token during initialisation cannot be changed during the lifetime of the token. This means that during the lifetime of the token, the token keeps the so-called 'profile' that has been created during the initialisation.

Note however, the distinction between G&D STARCOS SPK test-completed tokens and series-completed tokens. For test-completed 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 PKCS#15 structure). For series completed tokens (so-called 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.

Java cards with a test keyset can be re-initialised. Java cards with a production key set cannot be re-initialised again and will be treated as a legacy / series completed token.

When initialising a token, SafeSign will detect the token model you have inserted and will determine the best (possible) profile(s) to initialise the token with. Before initialising a token, please consider carefully that the availability of profiles depends on the type of token used. 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 profile is available (the token profile line is greyed out), this will probably mean you are dealing with an already initialised series completion token. Note that end-users are recommended to select the default profile, unless otherwise instructed by their administrator.

[Paragraph 3.1.1](#) will describe how to initialise a blank / uninitialised test or series token: follow these instructions to initialise your token for the first time. Note that these instructions also apply to already initialised test completed tokens.

[Paragraph 3.1.2](#) will describe how to wipe a series token.

[Paragraph 3.1.3](#) will describe how to import a CA Certificate during token initialisation / wiping.

These paragraphs will use the STARCOS SPK 2.3 card as an example.

##### 3.1.1 Initialise Token

### 1

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

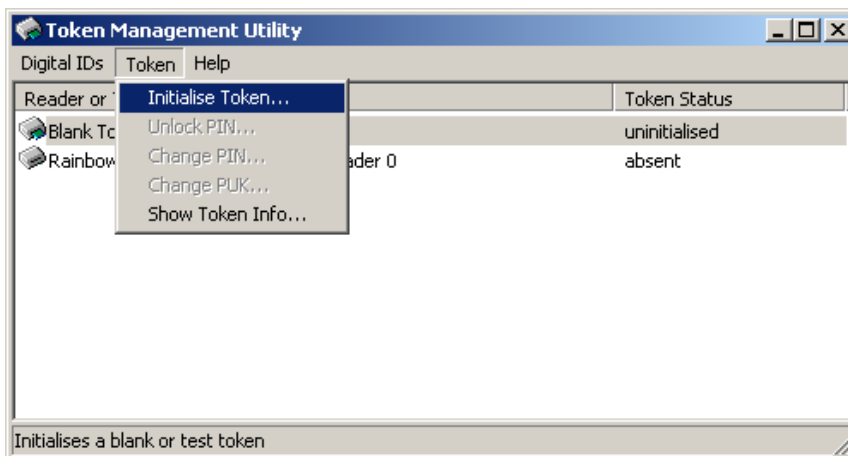


Figure 64: Token Management Utility: Initialise Token

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



**Note**

When your test-completed token has already been initialised with a token label, PUK and PIN, you may re-initialise the token. See the [Re-initialise Token](#) note.

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

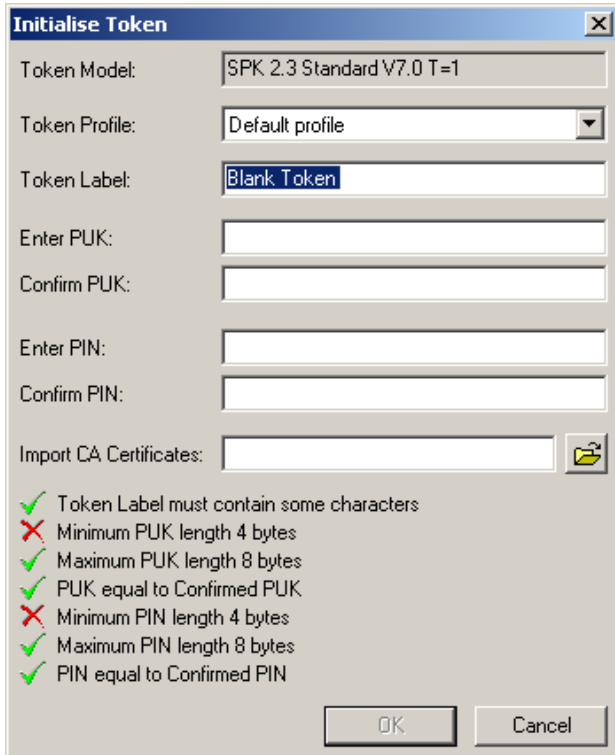


Figure 65: Token Management Utility: Initialise Token dialog

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.

**2**

In order to initialise your token, you must meet a number of requirements in doing so. 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
<i>Token Profile</i>	Different token profiles may be available, depending on the type of token you have inserted. Choose the profile that suits your needs.
<i>Token Label</i>	The token label must contain some characters, it cannot be empty; Maximum number of characters is 32
<i>Enter PUK</i>	Minimum PUK length is 4 characters, maximum PUK length is 8 characters
<i>Confirm PUK</i>	Confirmed new PUK should be equal to the new PUK
<i>Enter PIN</i>	Minimum PIN length is 4 characters, maximum PIN length is 8 characters
<i>Confirm PIN</i>	Confirmed new PIN should be equal to new PIN

Table 1: Token Management Utility: 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.

SafeSign enforces a minimum and maximum PIN / PUK length. If you enter a PIN / PUK of less than 4 characters or more than 8 characters, you will not be able to click the **OK** button in such instances where the PIN / PUK is required. Only when you enter a PIN / PUK of minimally 4 and maximally 8 characters, will the PIN / PUK be accepted. Note that the minimum / maximum PIN / PUK length may have been set to different values by the administrator.

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

Figure 66: Token Management Utility: Initialise Token dialog completed

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

### 3

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

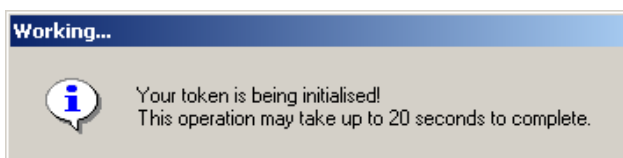


Figure 67: Initialise Token: Your token is being initialised

Do not interrupt or remove your SafeSign 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:

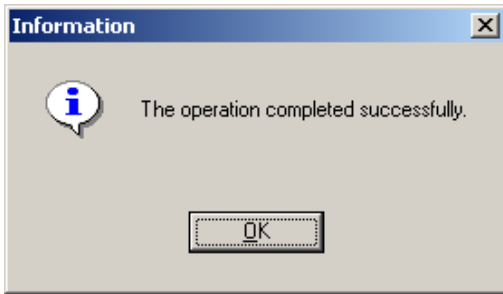


Figure 68: Initialise Token: The operation completed successfully

→ Click **OK** to finish the initialisation

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

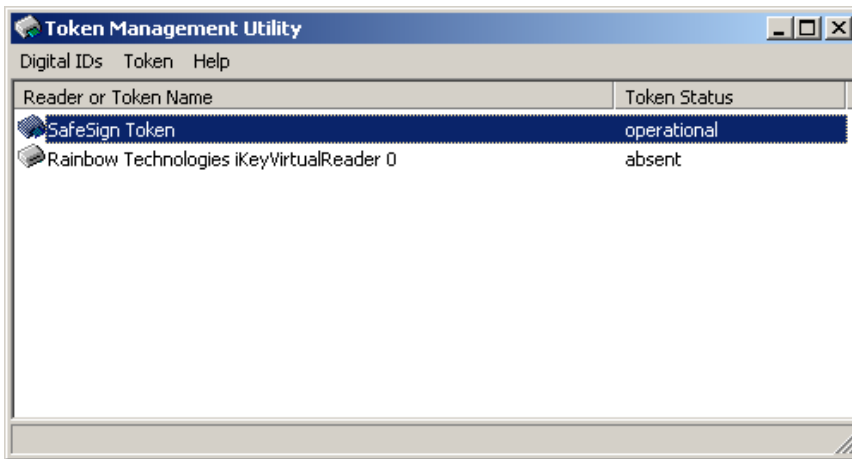


Figure 69: Token Management Utility: SafeSign Token

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:



Figure 70: Error: Device Error 0x30

Click **OK** to close this dialog

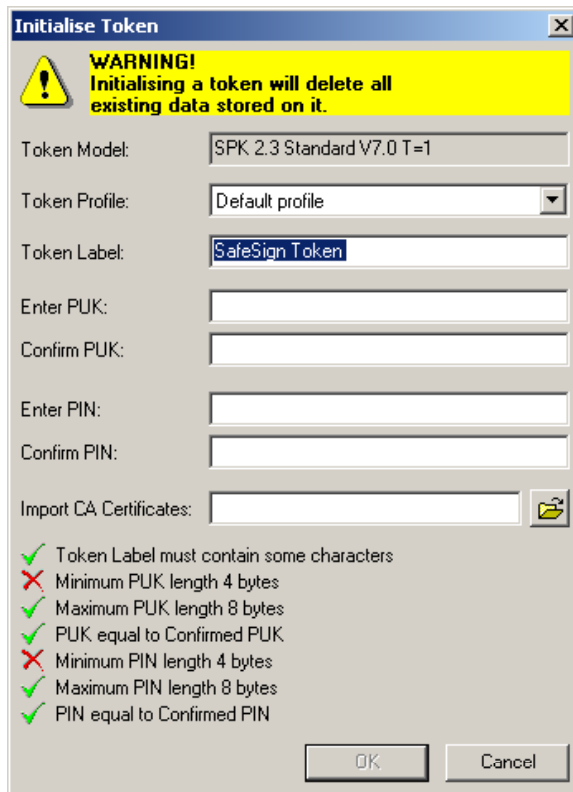
Check that your reader is functioning properly and whether you have a correct card. Make sure that the token is inserted in the smart card reader and click **OK** to try to initialise the token again. This error may also occur when there is not enough space left on the card (for the profile you selected) or because there are other applets on the card.



## Re-initialise token

When your token has already been initialised, it may be initialised again.

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:

Figure 71: Token Management Utility: Initialise Token Warning

Upon initialising a token that is as yet uninitialised, as described in [paragraph 3.1.1](#), this warning will not appear, as there is no data on the token yet.

### 3.1.2 Wipe Token

1

When you have a series completed STARCOS SPK token or a production Java card, the **Token** menu will display the item *Wipe Token* (instead of *Initialise Token*). Clicking on it will open the following window:

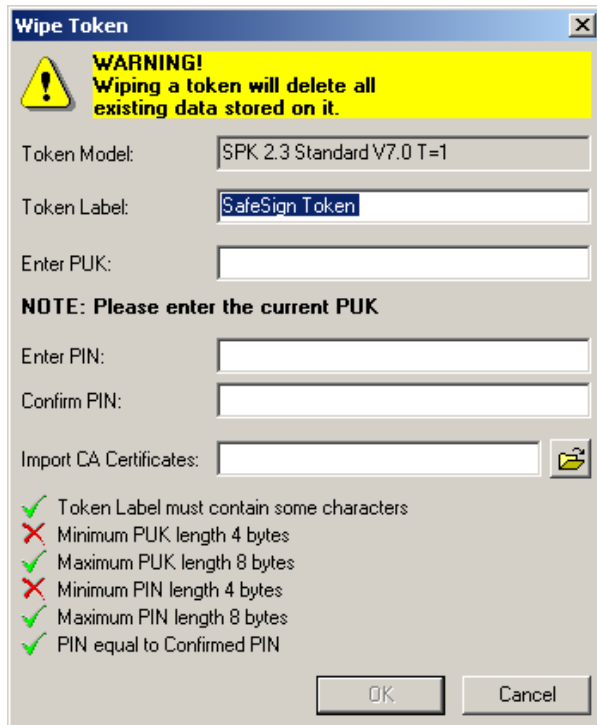


Figure 72: Token Management Utility: Wipe Token dialog

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

You will not be able to choose a token profile, as it is not possible to erase the file structure written on a series completed token.

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.

2

In order to wipe your token, a number of requirements should be met in doing so. 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
<i>Token Label</i>	The token label must contain some characters, it cannot be empty; Maximum number of characters is 32
<i>Enter PUK</i>	Minimum PUK length is 4 characters; maximum PUK length is 8 characters. The PUK entered should be the current / existing PUK.
<i>Enter PIN</i>	Minimum PIN length is 4 characters, maximum PIN length is 8 characters
<i>Confirm PIN</i>	Confirmed new PIN should be equal to new PIN

Table 2: Token Management Utility: 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.

SafeSign enforces a minimum and maximum PIN / PUK length. If you enter a PIN / PUK of less than 4 characters or more than 8 characters, you will not be able to click the **OK** button in such instances where the PIN / PUK is required. Only when you enter a PIN / PUK of minimally 4 and maximally 8 characters, will the PIN / PUK be accepted. Note that the minimum / maximum PIN / PUK length may have been set to different values by the administrator.

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

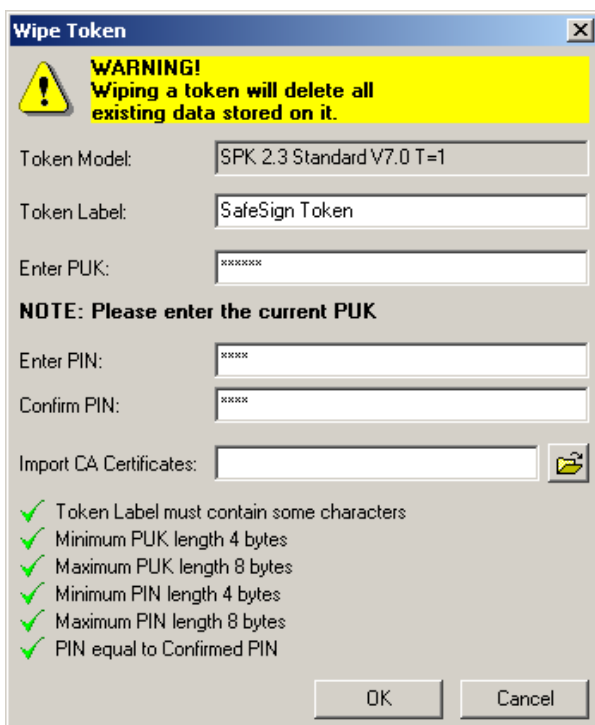


Figure 73: Token Management Utility: Wipe Token dialog completed

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

### 3

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

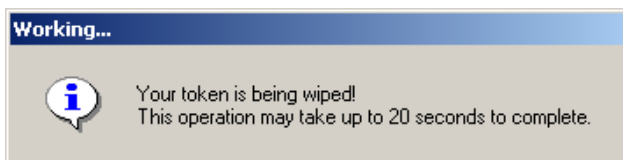


Figure 74: Token Management Utility: Your token is being wiped

Do not interrupt or remove your SafeSign 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.

4

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

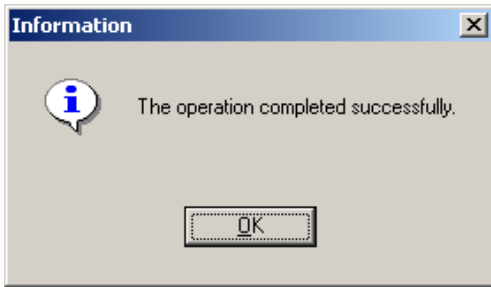


Figure 75: Token Management Utility: The operation completed successfully

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

When you token has been wiped, the token name will appear in the token window:

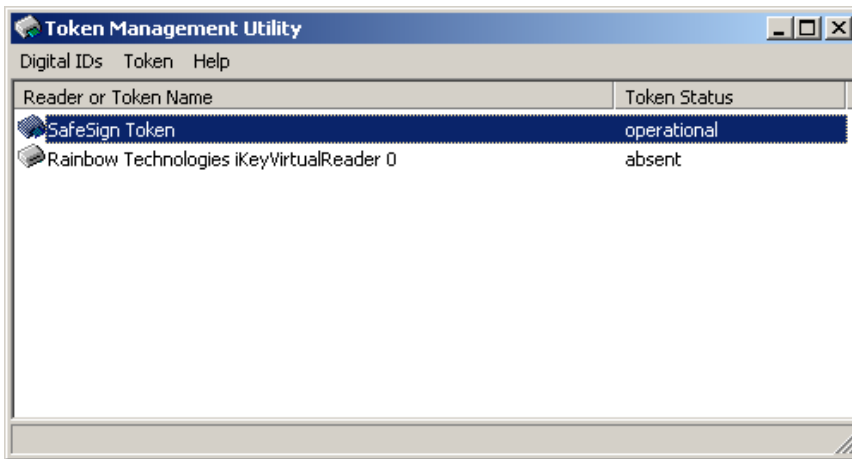


Figure 76: Token Management Utility: SafeSign Token



**Device Error**

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



Figure 77: Wipe Token: Device Error

Click **OK** to close this dialog

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) or because there are other applets on the card.

If the token is removed during the wiping process, it may be that all information on the token will be erased and that it will be uninitialised.

### 3.1.3 Import CA Certificates

The SafeSign Token Management 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 [paragraph 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 paragraph.



#### CA certificate format

SafeSign 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:

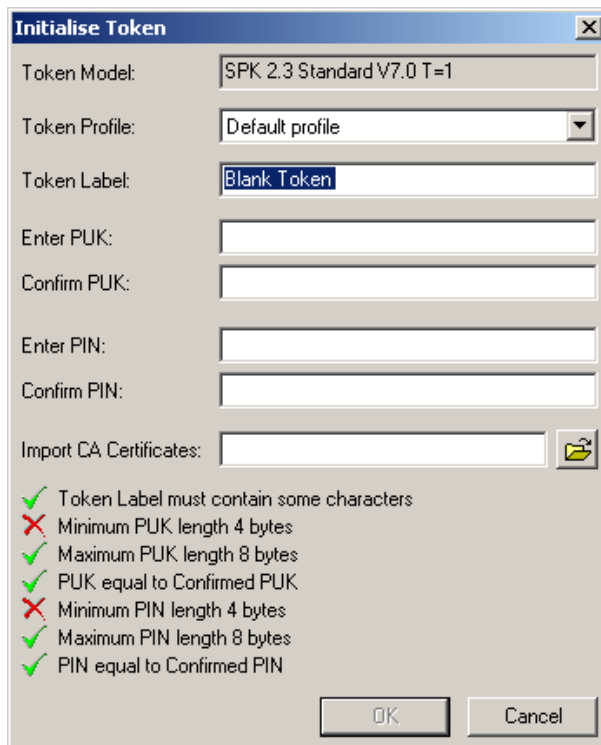


Figure 78: Token Management Utility: Initialise Token dialog

Fill in all fields according to requirements (as described in [paragraph 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:

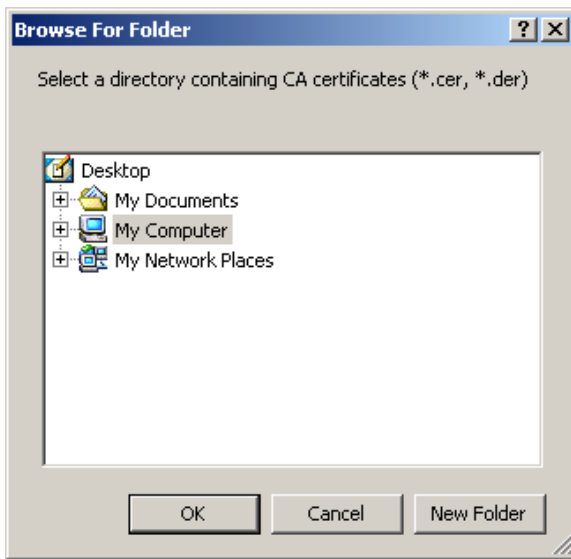


Figure 79: Browse for Folder

➔ Select a directory and click **OK**

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

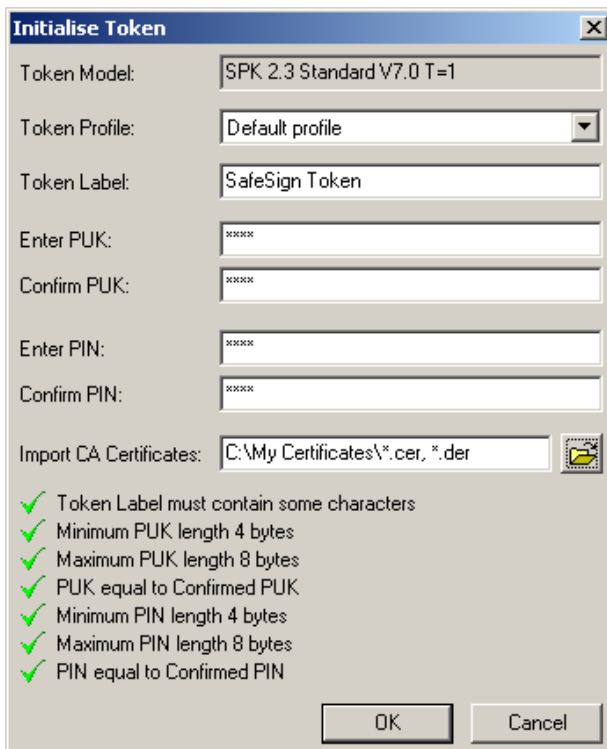


Figure 80: Initialise Token: Import CA Certificates

**Note** that **all** CA certificates present in the directory will be imported. If the certificates you want to import, have a different extension (for example .crt) change the extension displayed.

➔ Click **OK** to initialise the token

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

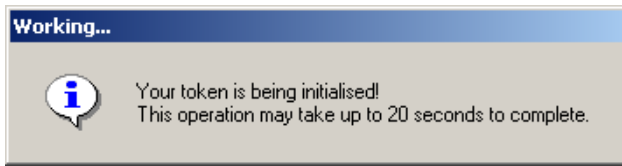


Figure 81: Token Management Utility: Token is being initialised

Do not interrupt or remove your SafeSign 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:

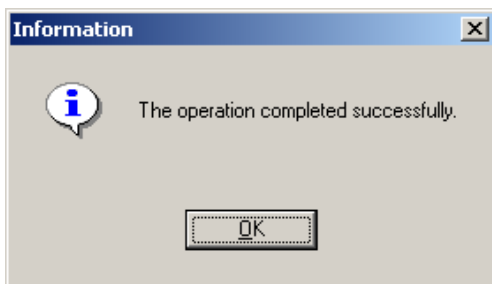


Figure 82: Token Management Utility: The operation completed successfully

➔ Click **OK** to finish the initialisation



## Change Transport PIN

The administrator may have initialised the token 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 has (consciously) sets his / her own PIN prior to any signature token operations.

For SafeSign, a Transport PIN is a PIN that contains fewer characters than a valid PIN code. For example, if a valid PIN is set to be at least 5 characters, the Transport PIN should contain no more than 4 characters.

When the administrator has set a Transport PIN, the user should first change the Transport PIN into his own personal PIN for the token. When a Transport PIN is set, the Token Administration Utility will enable you to change the Transport PIN:

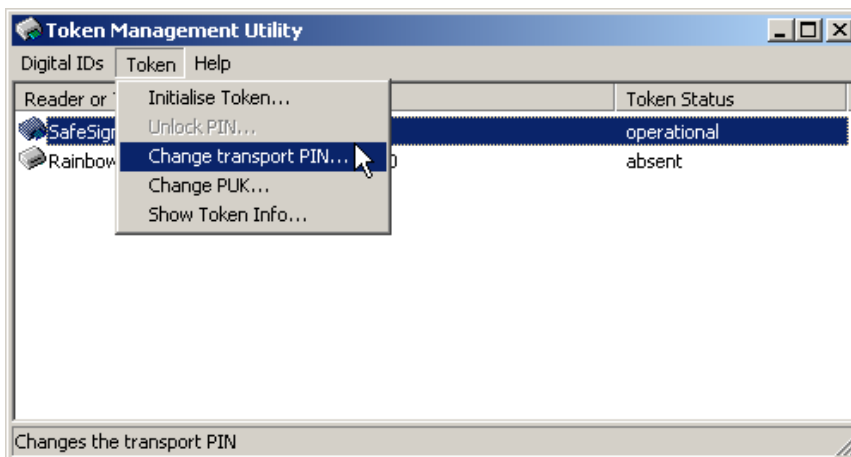


Figure 83: Token Management Utility: Change transport PIN

➔ Select **Change Transport PIN** (as above)

This will open the *Change transport PIN* dialog

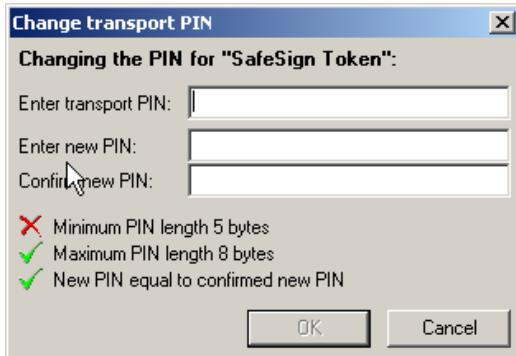


Figure 84: Change transport PIN dialog

The transport PIN should contain 4 characters, whereas the new PIN should contain at least 5 characters (in our example).

➔ 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:



Figure 85: Change transport PIN: Your PIN was successfully changed

➔ Click **OK**

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

### 3.2 Change PIN

The SafeSign Token Management Utility enables you to change the PIN for your Safesign Token.

1



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

Figure 86: Token Management Utility: Change PIN

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

Enter the old PIN, a new PIN and confirm the new PIN.

Only when you enter the correct old PIN 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 change the PIN



#### PIN / PUK length

SafeSign enforces a minimum and maximum PIN / PUK length. If you enter a PIN / PUK of less than 4 characters or more than 8 characters, you will not be able to click the **OK** button in such instances where the PIN / PUK is required. Only when you enter a PIN / PUK of minimally 4 and maximally 8 characters, will the PIN / PUK be accepted. Note that the minimum / maximum PIN / PUK length may have been set to different values by the administrator.

2

The PIN will now be changed:

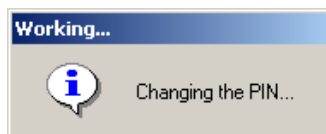


Figure 87: Token Management Utility: Changing the PIN

➔ Wait until the PIN is changed

3

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

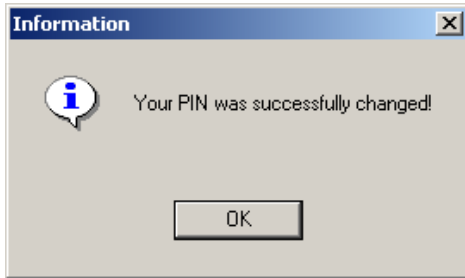


Figure 88: Token Management Utility: Your PIN was successfully changed

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

### 3.2.1 PIN information

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

Note that you have **three** attempts to enter the correct PIN<sup>1</sup> and that SafeSign 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 [paragraph 3.3](#)).

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

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

1. PIN is "OK" (as in [Figure 89](#) below)

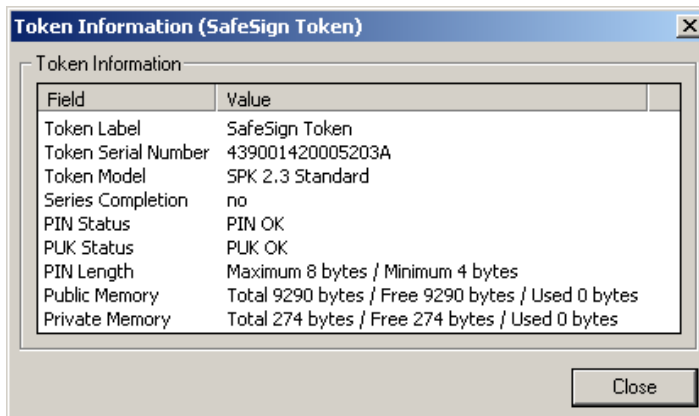


Figure 89: Token Information: PIN Status

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

<sup>1</sup> Note that your administrator may have changed the maximum number of PIN retries.

Also, when you perform an operation within the SafeSign Token Management 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):



Figure 90: Token Management Utility: Change PIN

(2) When the PIN has been entered incorrectly:

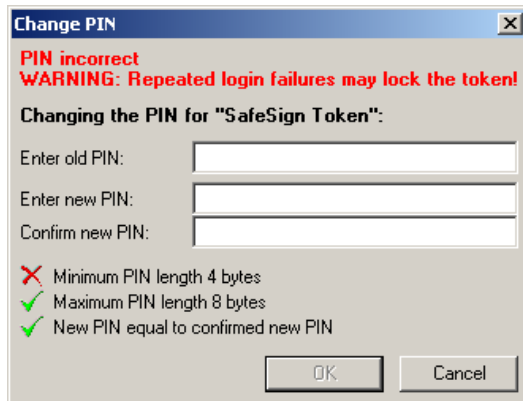


Figure 91: Change PIN: PIN incorrect

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



Figure 92: Change PIN: You have only 1 attempt left

(4) When the PIN is locked:



Figure 93: Change PIN: PIN locked



### Wrong PIN in different item

When you close one menu item in the SafeSign Token Management 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 (for example when importing a Digital ID) and that you have only one attempt left to enter the correct PIN:

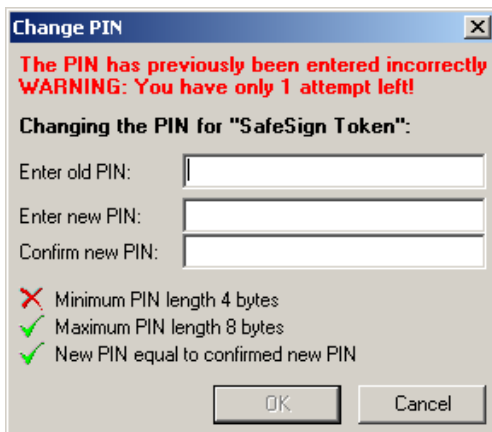


Figure 94: Change PIN: The PIN has previously been entered incorrectly

### 3.3 Unlock PIN

The SafeSign Token Management Utility enables you to unlock the PIN for your Safesign Token (when your PIN is locked, as in [Figure 93](#)).

**Note** that the *Unlock PIN* item will only be available when the PIN is actually locked. If not, the item will be greyed out. In order to unlock the PIN, you will need to know the PUK of the SafeSign token.

In order unlock the PIN, select *Unlock PIN* from the **Token** menu. This will open the following dialog:

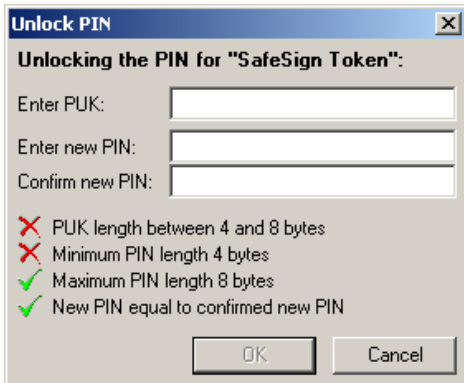


Figure 95: Token Management Utility: Unlock PIN

This dialog will identify the token of which you want to unlock the PIN (“SafeSign 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



#### PIN / PUK length

SafeSign enforces a minimum and maximum PIN / PUK length. If you enter a PIN / PUK of less than 4 characters or more than 8 characters, you will not be able to click the **OK** button in such instances where the PIN / PUK is required. Only when you enter a PIN / PUK of minimally 4 and maximally 8 characters, will the PIN / PUK be accepted. Note that the minimum / maximum PIN / PUK length may have been set to different values by the administrator.

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

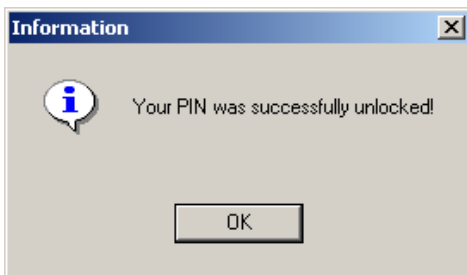


Figure 96: Unlock PIN: Your PIN was successfully unlocked

➔ 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 Change PUK

The SafeSign Token Management Utility enables you to change the PUK for your Safesign Token.

1

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

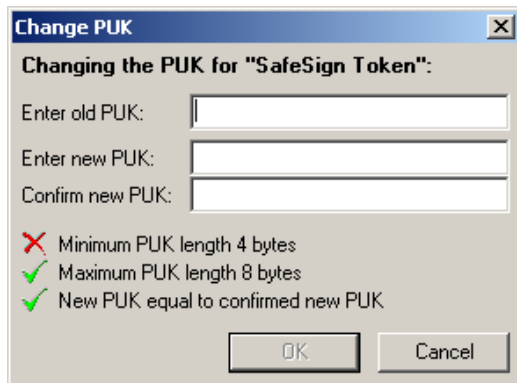


Figure 97: Token Management Utility: Change PUK

This dialog will identify the token of which you want to change the PUK ("SafeSign 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



#### PIN / PUK length

SafeSign enforces a minimum and maximum PIN / PUK length. If you enter a PIN / PUK of less than 4 characters or more than 8 characters, you will not be able to click the **OK** button in such instances where the PIN / PUK is required. Only when you enter a PIN / PUK of minimally 4 and maximally 8 characters, will the PIN / PUK be accepted. Note that the minimum / maximum PIN / PUK length may have been set to different values by the administrator.

2

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

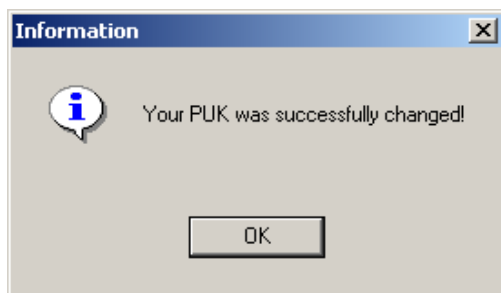


Figure 98: Change PUK: Your PUK was successfully changed

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

Your PUK is changed.

### 3.4.1 PUK information

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

Note that you have **three** attempts to enter the correct PUK<sup>1</sup> and that SafeSign 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.*

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 99](#) below)

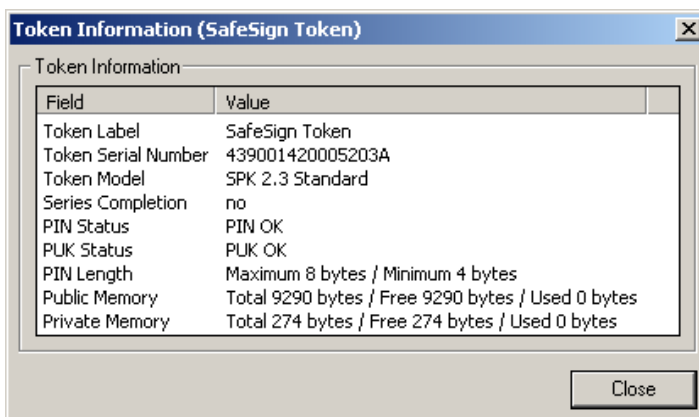


Figure 99: Token Information: PUK Status

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

<sup>1</sup> Note that your administrator may have changed the maximum number of PUK retries.

Also, when you perform an operation within the SafeSign Token Management 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):

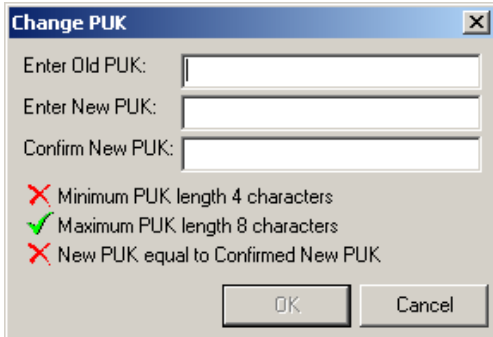


Figure 100: Token Management Utility: Change PUK

(2) When the PUK has been entered incorrectly:

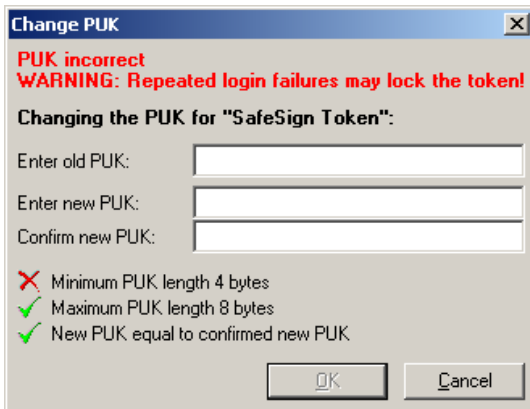
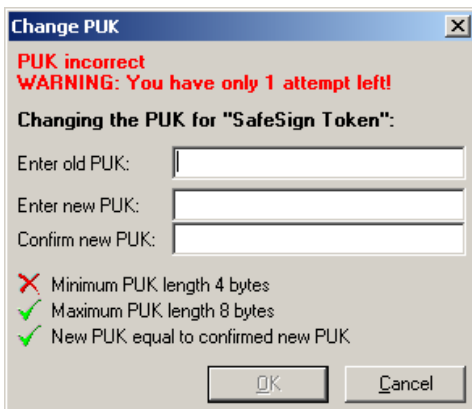


Figure 101: Change PUK: PUK incorrect



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

Figure 102: Change PUK: You have only 1 attempt left

(4) When the PUK is locked:

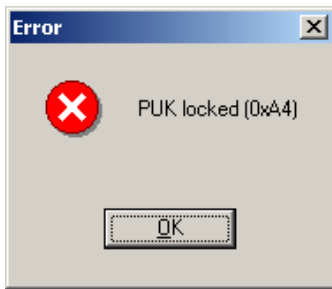
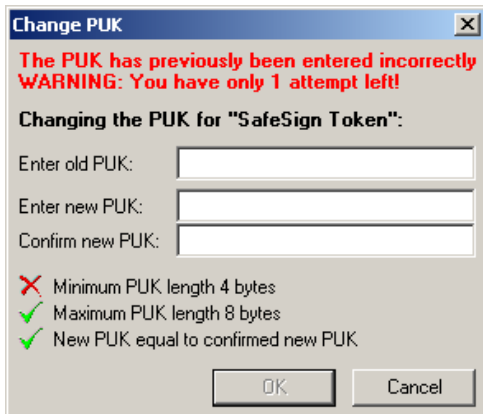


Figure 103: Change PUK: PUK locked



### Wrong PUK in different item

When you close one menu item in the SafeSign Token Management 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 one attempt left to enter the correct PUK:

Figure 104: 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 Management Utility will look like this:

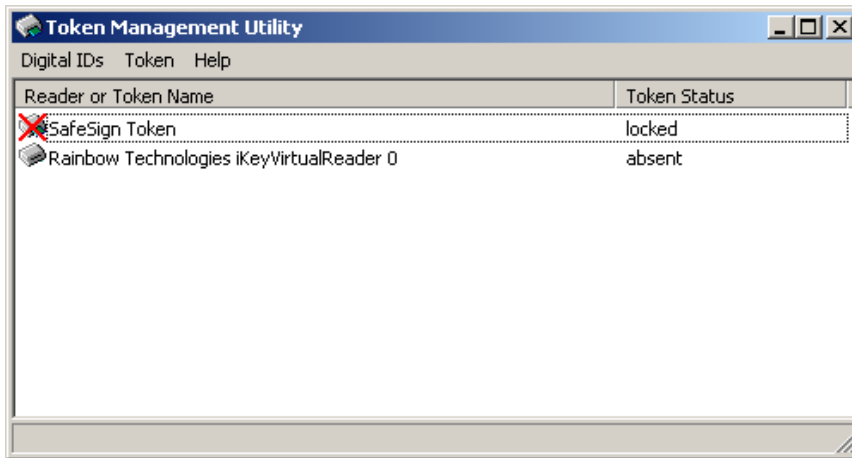


Figure 105: Token locked

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

## 3.5 Show Token Info

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

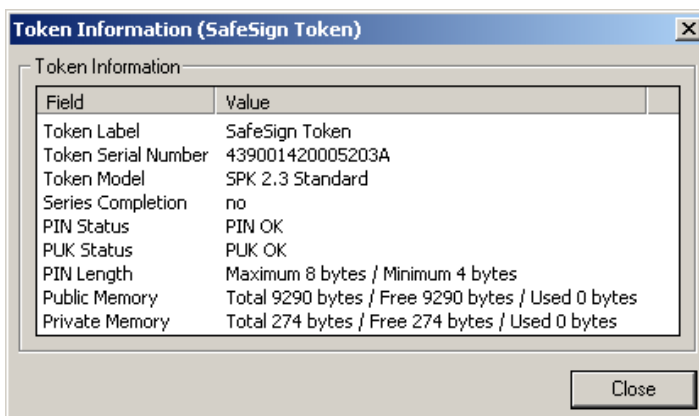


Figure 106: Token Management Utility: Token Information

The *Token Information* field displays the following information:

<b>Token Label</b>	[token label]
	Displays the label of the token, as given to it by the administrator or by the user himself.
<b>Token Serial Number</b>	[serial number]
	Displays the serial number of the token.
<b>Token Model</b>	[token model]
	Displays the token model and version.
<b>Series Completion</b>	[Yes / No]
	Displays whether the token is test completed or series completed. When the token is test completed, it will say [No], when the token is series completed, it will say [Yes].
<b>PIN Status</b>	[ <i>PIN status message</i> ]
	Displays the status of the PIN.
	<i>OK</i>
	<i>PIN has been entered incorrectly at least once</i>
	<i>One final attempt left to enter PIN incorrectly</i>
	<i>LOCKED</i>
<b>PUK Status</b>	[ <i>PUK status message</i> ]
	Displays the status of the PUK.
	<i>OK</i>
	<i>PUK has been entered incorrectly at least once</i>
	<i>One final attempt left to enter PUK incorrectly</i>
	<i>LOCKED</i>
<b>PIN Length</b>	[maximum x characters / minimum x characters]
	Displays the maximum and minimum number of characters for the PIN length, i.e. a maximum of 8 and a minimum of 4 characters.
<b>Public Memory</b>	[Total x bytes / Free x bytes / Used x bytes]
	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).
<b>Private Memory</b>	[Total x bytes / Free x bytes / Used x bytes]
	Displays the total amount of bytes, the free amount of bytes and the used amount of bytes available in the private memory on the token (after initialisation).



**Note**

*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).*

## Index of Notes

---

CA certificate format	39
Certificate Expiration Warning	21
Certification Path	13
Change Transport PIN	41
Device Error	34, 38
Field requirements	33, 37
Import CA certificates	24
Key Size Error	26
Menu availability	3
Multiple tokens and readers	4
Note	1, 2, 3, 7, 3, 17, 22, 28, 31, 32, 49, 53
Note for Administrators	21
PIN / PUK length	18, 26, 29, 43, 47, 48
Private Key non-exportable	13
Re-initialise token	35
Removal of the token	1
Save to file	20
Secure PIN entry	4
Set the label of the ID on the token to a non default-value	24
Token availability	4
Token Locked	52
Token missing	9
Token out of Memory	27
Wrong Password	25
Wrong PIN in different item	46
Wrong PUK in different item	51