SafeSign Identity Client User Guide

Microsoft Windows 2003

A.E.T. Europe B.V.

IJsselburcht 3

NL - 6825 BS Arnhem

The Netherlands

Warning Notice

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

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

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

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

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

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

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

Credit information:

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

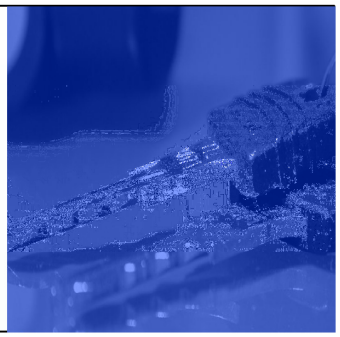
This product includes software written by Tim J. Hudson (tjh@cryptsoft.com).

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

IJsselburcht 3
NL-6825 BS
P.O. Box 5486
NL-6802 EL Arnhem
The Netherlands
Tel. +31-26-365 33 50
Tel. Support +31-26-365 35 43
Fax +31-26-365 33 51

info@aeteurope.nl / support@aeteurope.nl
http://www.aeteurope.com/

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



Document Information

Filename: **SafeSign Identity Client User Guide Microsoft Windows 2003**

Document ID: **Windows2003_SafeSign-IC_v2.1**

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

Document revision history

Version	Date	Author	Changes
1.0	14-12-2005	Drs C.M. van Houten	First edition for SafeSign Identity Client Version 2.2 for Windows (release 2.2.0)
1.1	25-04-2006	Drs C.M. van Houten	Edited for SafeSign Identity Client Version 2.2 for Windows (release 2.2.2)
2.0	27-07-2006	Drs C.M. van Houten	Edited for SafeSign Identity Client Version 2.3 for Windows (release 2.3.0)
2.1	03-01-2007	Drs C.M. van Houten	Edited for SafeSign Identity Client Version 2.3 for Windows (release 2.3.2)

WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE

Table of contents

List of Figures

About the Product

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

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

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

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

SafeSign Identity Client Version 2.3 for Windows supports the following tokens (as described in the product description):

- STARCOS® smart cards developed by Giesecke & Devrient GmbH (G&D): SPK2.3, SPK2.3 RawRSA, SPK2.4, SPK2.4 FIPS, SPK2.5 Dual Interface (DI), STARCOS 3.0;
- The G&D StarKey100 (M) and StarKey200 USB token with the completed STARCOS SPK 2.3 / 2.4 operating system;
- The G&D StarKey220 HID token with the completed STARCOS SPK 2.3 operating system;
- The G&D StarKey400 and StarKey400 M (with flash memory) USB token with Sm@rtCafé Expert 64k;
- The Eutron CryptoIdentity / CryptoCombo ITSEC-P with the completed STARCOS SPK 2.3 operating system, and the CryptoIdentity / CryptoCombo FIPS USB token with the completed STARCOS SPK 2.4 operating system;
- The SafeNet iKey 3000 USB token with the completed STARCOS SPK 2.3 operating system;
- The KeyCorp Multos v4.2 48K card and the KeyCorp Multos v4.2 64K card;
- Java Card v2.1.1 / Open Platform 2.0.1 compliant Java smart cards:
- Aspects OS755 v2.8, Axalto e-gate, Axalto Cyberflex Access Developer 32K, Axalto Cyberflex 64Kv1 and 64Kv2, Axalto Cyberflex Palmera, G&D Sm@rtCafé Expert 2.0, G&D STARSIM Java, Gemplus GemXpresso 211pk/Pro R3, IBM JCOP 20/21/30/31, MartSoft Java card, Oberthur CosmopolIC v4 and Orga JCOP 20/30.
- Java Card v2.2+ / GlobalPlatform 2.1.1 compliant Java smart cards:

  Aspects OS755 (Java Card 2.2), Atmel ATOP36 (Java Card 2.2), G&D Sm@rtCafé Expert 64, G&D Sm@rtCafé Expert 3.0, G&D Sm@rtCafé Expert 3.1, IBM JCOP21 (Java Card 2.2), IBM JCOP31 (Java Card 2.2), IBM JCOP41, Oberthur IDone Cosmo64 v5.2, Oberthur ID-One Cosmo 64 RSA D/T v5.4 and Oberthur ID-One Cosmo 32 RSA v3.6.

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

- Windows 2000, Windows XP (Professional), Windows 2003 Server, Windows Vista Ultimate.

In principle, SafeSign Identity Client 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.

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

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

About the Manual

This manual is specifically designed for users of Microsoft Windows 2003, who wish to use their SafeSign Identity Client Token to enhance the security of their communications via the Internet.

The manual how to work with your SafeSign Identity Client Token in Windows 2003, from installing Microsoft Certificate Services and enrolling for a smart card user or smart card logon certificate.

In order to set up your SafeSign Identity Client Token for use with Microsoft Windows secure log-on, follow the instructions in the manual, which describe such activities as obtaining a smart card user / logon certificate.

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

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

Go through these steps and the actions you are required to take, in order to perform the desired activity, taking into account the notes in **black** with:  and the larger ones in **blue** with: 

Note that this manual assumes you have installed SafeSign Identity Client and have initialised the token with the SafeSign Identity Client Token Management Utility / Token Administration Utility, thus making it ready to use with Internet Explorer and Microsoft applications. See for instructions on installing SafeSign Identity Client the *SafeSign Identity Client User Guide for Installation* and for configuring and managing your SafeSign Identity Client Token, either the *SafeSign Identity Client Token Management Utility Guide* or *SafeSign Identity Client Token Administration Utility Guide*.

Note

Not all activities described in this manual will be performed by the user, e.g. in order to set up Certificate Services, you will need to be logged on as administrator of the domain / have administrator's rights.

Note

Note that the description of setting up Microsoft Certificate Services in this guide is meant as guidance only and that A.E.T. Europe B.V. can never be held liable for any malfunctioning and/or other consequences from setting up Microsoft Certificate Services as described in this manual.

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

1 Windows 2003

1.1 Windows 2003 Security Features

Microsoft Windows 2003 integrates smart card capabilities in the Operating System. The Microsoft Windows 2003 operating system includes a native Public Key Infrastructure (with its own Certificate Server) and introduces smart card authentication as an alternative to passwords to achieve strong network authentication.

The primary components of the Windows PKI are:

Certificate Services, a core operating system that allows businesses to act as their own CA and issue and manage digital certificates;

Active Directory directory service, a core operating system service that provides a single place to find network resources; it serves as the publication service in the PKI;

PKI-enabled applications like Internet Explorer, Outlook and Outlook Express.

Windows 2003 offers secure e-mail, secure web access (client authentication) and secure logon. Please refer to the application User Guides how to use your Internet (mail) application for secure e-mail and web access.

This manual will describe how to obtain a certificate and how to log on to Windows 2000, Windows XP and Windows 2003 with your SafeSign Identity Client Token.

In order to use your SafeSign Identity Client Token for secure logon, you must use a *smart card user* or *smart card logon* certificate, which can be obtained from the Microsoft Certificate Server.

Chapter 2 will describe how to set up Microsoft Certificate Services.

Chapter 3 will describe how to enroll a smart card user.

Chapter 4 will describe how the secure logon procedure works for Windows 2000 / XP / 2003.

Note

Note that the description of setting up Microsoft Certificate Services in this guide is meant as guidance only. For a complete description of setting up Microsoft Certificate Services, please refer to the ***Technical Resources for Windows Server 2003*** *at:*

http://www.microsoft.com/windowsserver2003/techinfo/default.mspx

A description of the installation and functioning of Active Directory is outside the scope of this manual.

Note that A.E.T. Europe B.V. can never be held liable for any malfunctioning and/or other consequences from setting up Microsoft Certificate Services as described in this manual.

2 Microsoft Certificate Services

This paragraph will describe how to install and set up Microsoft Windows 2003 Certificate Services, comprising the following aspects:

Installing Certificate Services: paragraph 2.2

Configuring the Windows CA: paragrah 2.3

Creating a Microsoft CA RA station: paragrah 2.4

2.1 Prerequisites

This manual assumes that you have the following components installed, before setting up Microsoft Windows 2003 Certificate Services

- Windows 2003 Server installed and configured as a Primary Domain Controller.
- Active Directory configured to store users and computers.
- DNS Server configured with your domain name.
- Internet Information Services (IIS) installed (to be able to request a certificate through the Smart Card Enrolment Station, as described in Chapter 3).

2.2 Installing Certificate Services

Note

In order to install and configure Certificate Services, you need to be logged on as an administrator of the domain.

1 In Windows 2003, click **Start** > **Settings** > **Control Panel** to open the *Control Panel* dialog box:

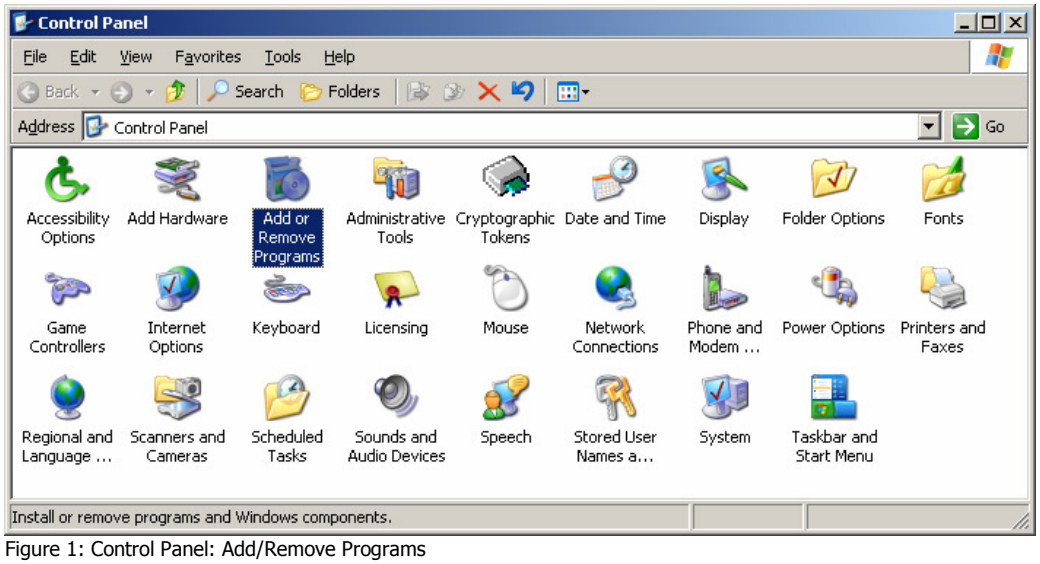


Figure 1: Control Panel: Add/Remove Programs

➔ Select and double-click **Add or Remove Programs**

2 The *Add or Remove Programs* dialog box opens:

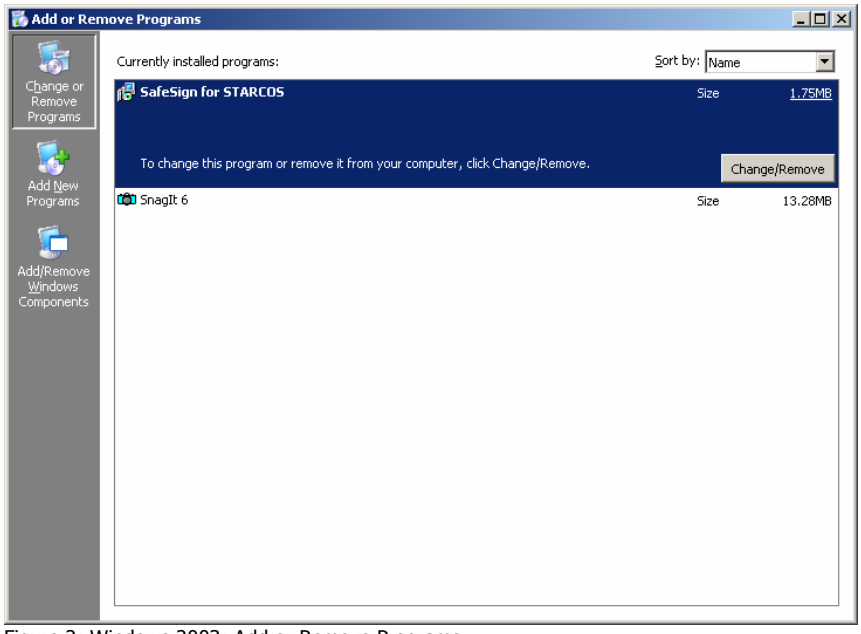


Figure 2: Windows 2003: Add or Remove Programs

➔ Click the **Add/Remove Windows Components** button: 

3 The *Windows Components Wizard* will open:

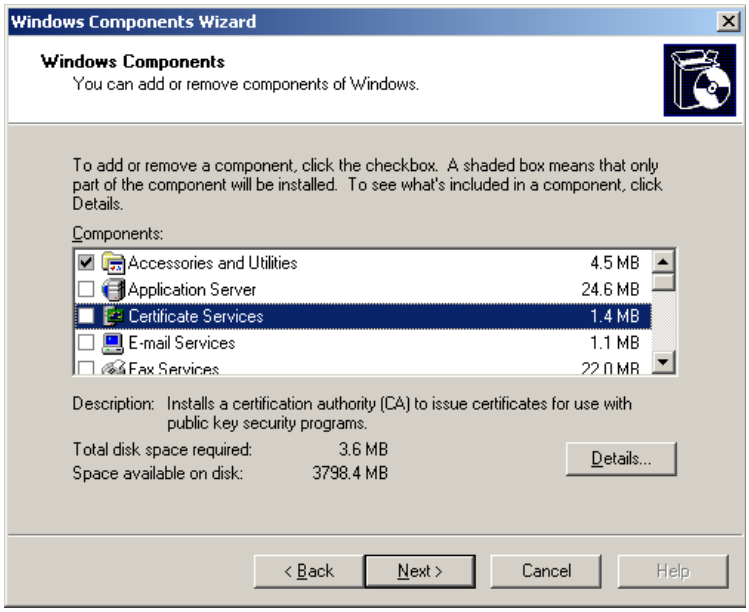


Figure 3: Windows Components Wizard: Windows Components

In the *Windows Components* dialog you can add or remove components of Windows 2003.

As the checkbox in front of **Application Server** is not checked, the Application Server is not yet installed.

As the checkbox in front of **Certificate Services** is not checked, Certificate Services are not yet installed.

➔ Check the checkbox for **Application Server**

➔ Check the checkbox for **Certificate Services**

4 Upon selecting **Certificate Services**, you will be informed that after installing Certificate Services, the computer cannot be renamed and cannot join or be removed from a domain:

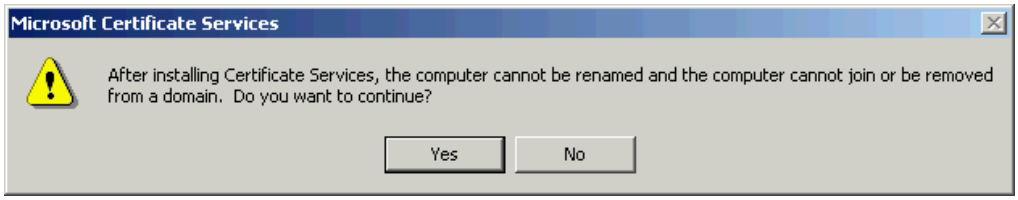


Figure 4: Microsoft Certificate Services: Do you want to continue?

➔ Click **Yes** to continue

5 Upon clicking **Yes**, the *Windows Components* dialog will be displayed once again, now with Application Server and Certificate Services selected:

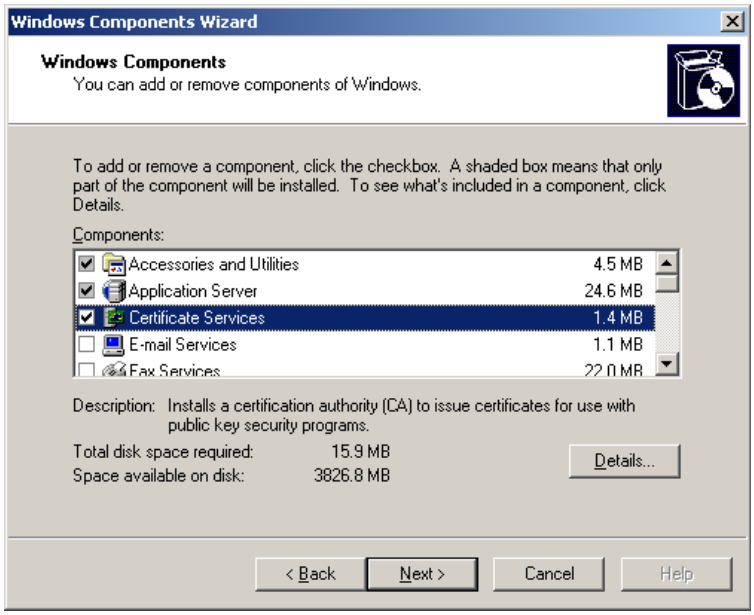


Figure 5: Windows Components Wizard: Windows Components - selected

➔ Click **Next** to install Application Server and Certificate Services

6 Upon clicking **Next**, the *Windows Components Wizard* will ask you what kind of Certification Authority you want to set up:

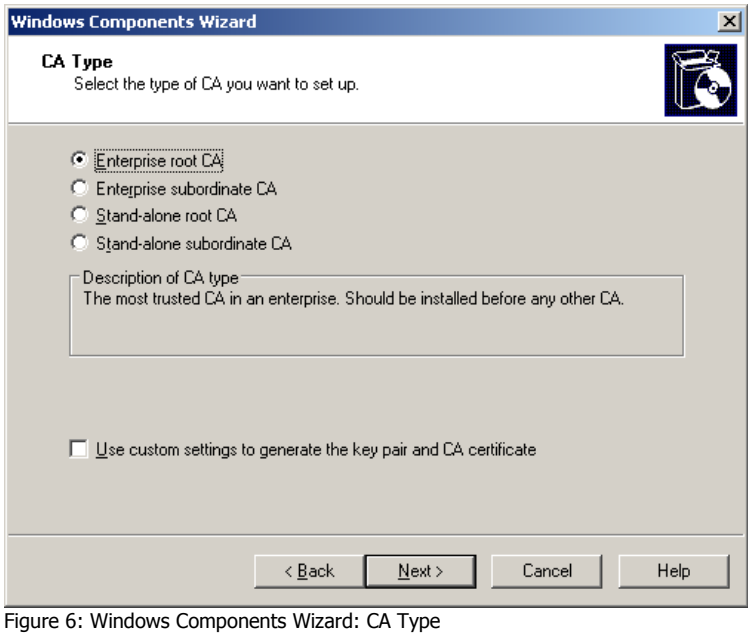


Figure 6: Windows Components Wizard: CA Type

The Enterprise root CA is the most trusted CA in an enterprise and should be installed before any other CA. If this option is not available, you may not have installed or properly configured Active Directory, as this Certification Authority type requires Active Directory.

Note

Do not check: 'Use custom settings to generate the key pair and CA certificate'. Although you may be able to select the SafeSign CSP in these settings, it is not possible to generate key pair and CA certificate on a token. This is functionality that smart card CSPs (including the SafeSign CSP) do not support.

➔ Select **Enterprise root CA** and click **Next** to continue

Note

Typically, you should install an enterprise CA if you will be issuing certificates to users or computers inside an organisation that is part of a Windows 2003 domain. An enterprise CA requires that all users requesting certificates have an entry in the Windows 2003 Server Active Directory services. An enterprise CA can issue certificates that are used to log on to a Windows 2003-based domain, and a stand-alone CA cannot.

7 Upon clicking **Next**, the *CA Identifying Information* dialog will open, allowing you to enter information to identify the Enterprise root CA you are setting up:

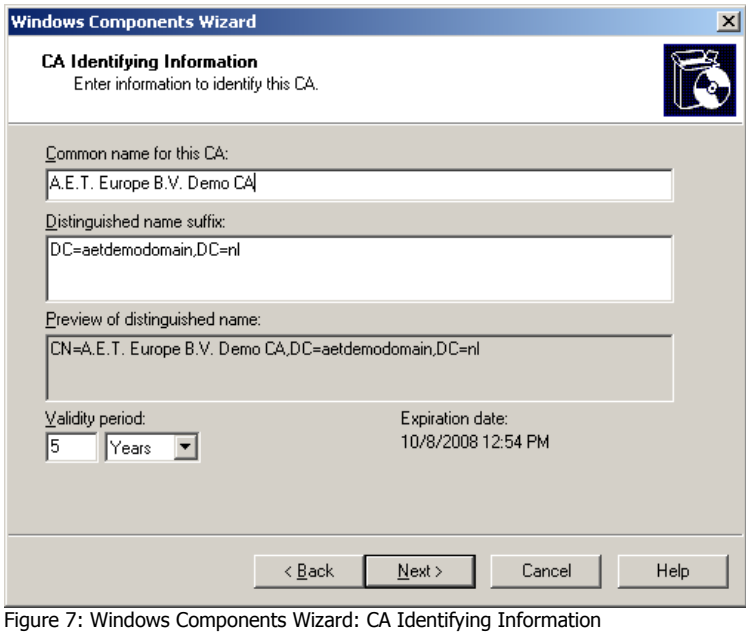


Figure 7: Windows Components Wizard: CA Identifying Information

➔ Enter a common name for the CA you are about to create (this will automatically complete the other boxes)

8 Upon clicking **Next**, the *Certificate Database Settings* dialog will open:

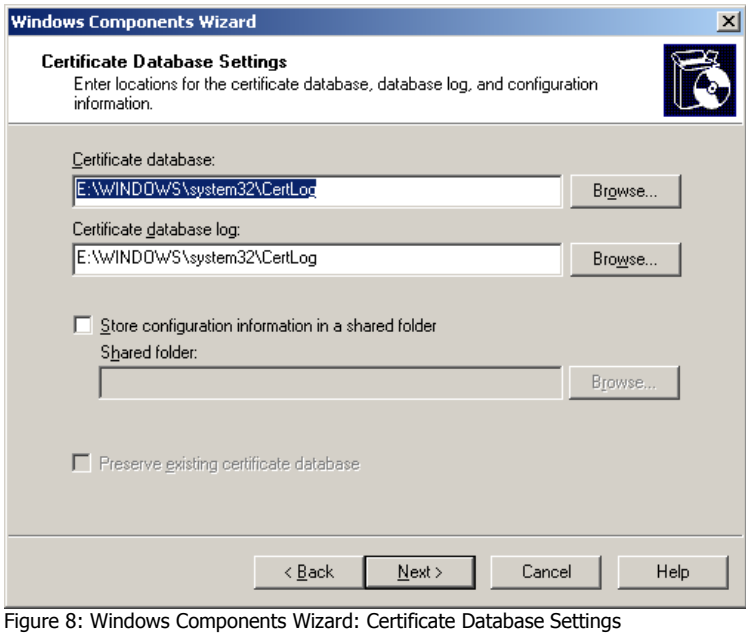


Figure 8: Windows Components Wizard: Certificate Database Settings

➔ Keep the default storage locations and click **Next** to continue

9 Active Server Pages (ASPs) must be enabled in Internet Information Services (IIS) in order to allow Certificate Services to provide web enrollment services. You will be asked if you want to enable Active Server Pages now:

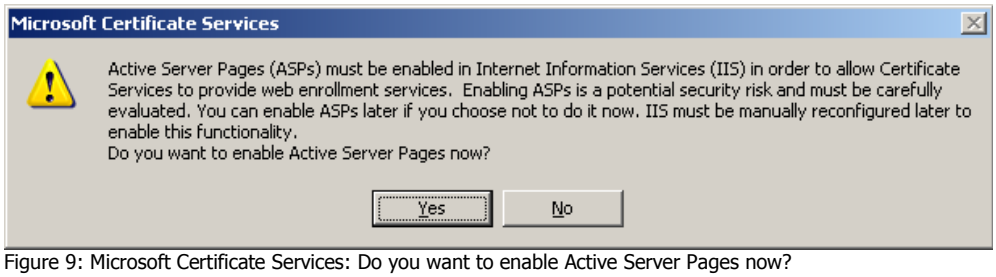


Figure 9: Microsoft Certificate Services: Do you want to enable Active Server Pages now?

➔ Click **Yes** to enable Active Server Pages

10 The *Configuration Components* dialog will inform you that setup is making the configuration changes you requested:

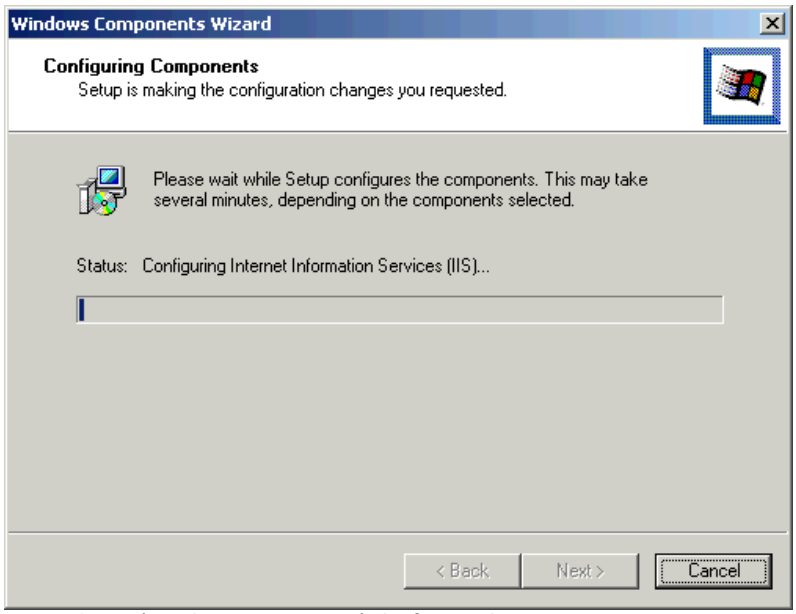


Figure 10: Windows Components Wizard: Configuring Components

➔ Insert the Windows 2003 CD-ROM and wait until setup has configured the components you selected

11 When setup is finished, the *Windows Components Wizard* will be completed:

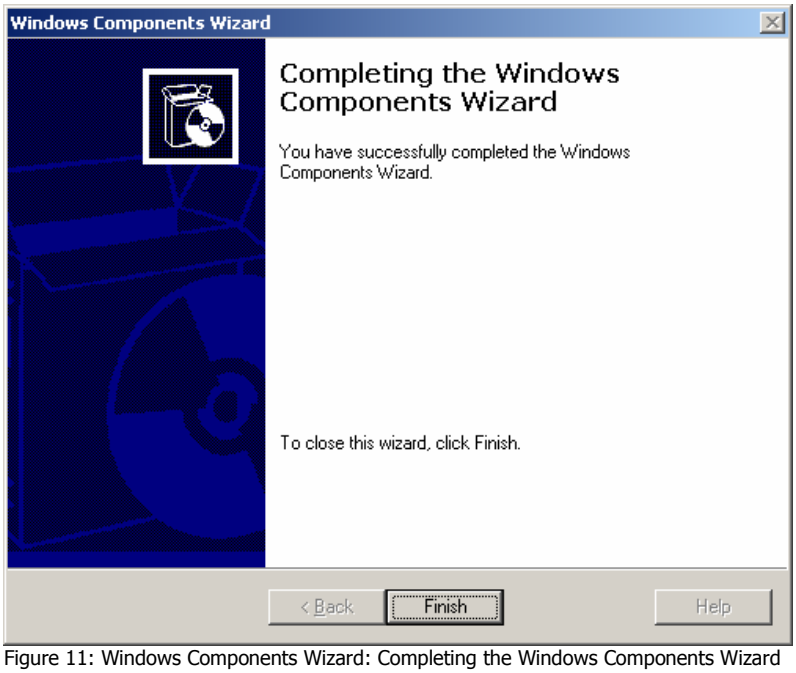


Figure 11: Windows Components Wizard: Completing the Windows Components Wizard

➔ Click **Finish**

Certificate Services are now installed. The next step is to configure the Microsoft CA, allowing you to configure the Certificate Services, to be able to issue smart card logon certificates for your domain.

2.3 Configuring the Microsoft CA

In order to enable the Microsoft CA to issue smart card certificates for your domain, you should configure it.

1 Go to **Start > Programs > Administrative Tools > Certificate Authority** to open the Microsoft Certification Authority configuration console and select the folder **Certificate Templates** to get an overview of all currently available certificate templates:

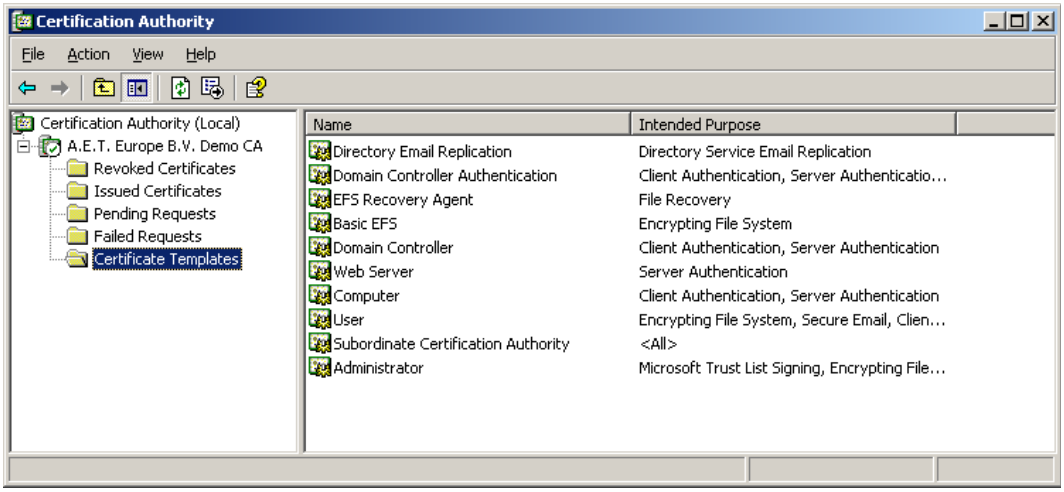


Figure 12: Certification Authority: Certificate Templates

The Microsoft CA can only issue certificates that comply to one of these certificate templates. With a default installation of the Microsoft CA (as described above), some certificate templates, such as those that are necessary for the Microsoft CA to issue smart card certificates, are not available. To make these certificate templates available to your Microsoft CA, you will have to update the list of available certificate templates.

2 To add new certificate templates to the list of available certificate templates, right-click on **Certificate Templates** and then select **New > Certificate Template to Issue**:

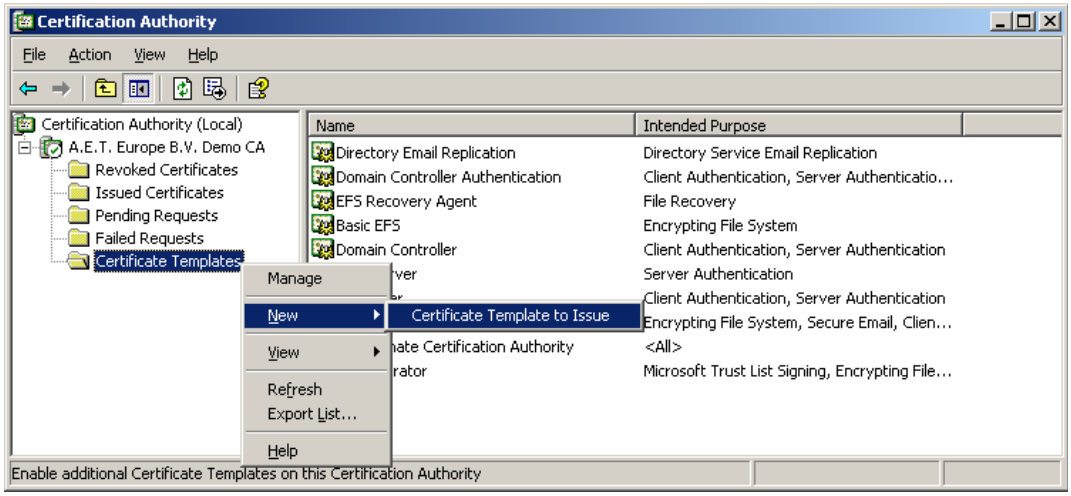


Figure 13: Certification Authority: Certificate Templates: New Certificate Template to Issue

This will open the *Enable Certificate Templates* dialog:

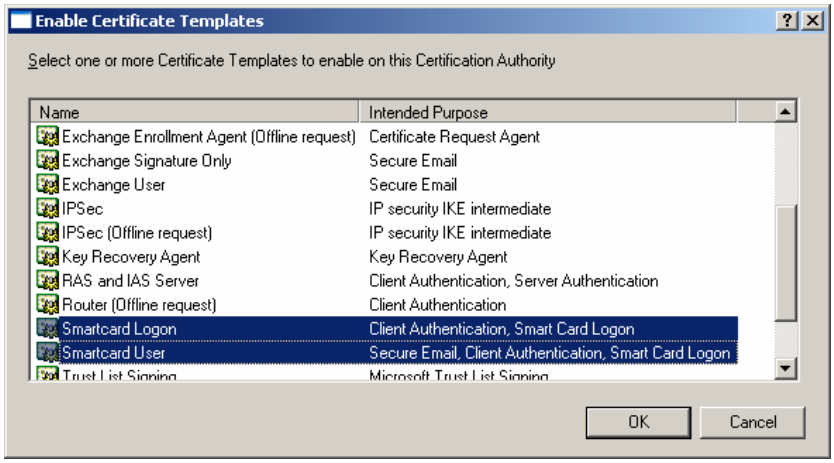


Figure 14: Enable Certificate Templates

To allow for your Microsoft CA to issue certificates for smart card logon onto the domain, you should select the following three certificate templates:

Smartcard Logon: intended for smart card logon onto the domain

Smartcard User: an all-round certificate, intended for both smart card logon and for example signing and encrypting e-mail messages and web authentication.

Enrollment Agent: a certificate intended for the entity that should be able to enrol certificates for other entities than itself. For example, when an administrator wants to deploy smart card logon certificates for the employees in his organisation, he would require an 'Enrollment Agent' certificate.

➔ Select all of the above-mentioned certificate templates press the **OK** button.

3 All the necessary certificate templates will now be included in the list, enabling the personalisation of a smart card with a smart card logon / user certificate:

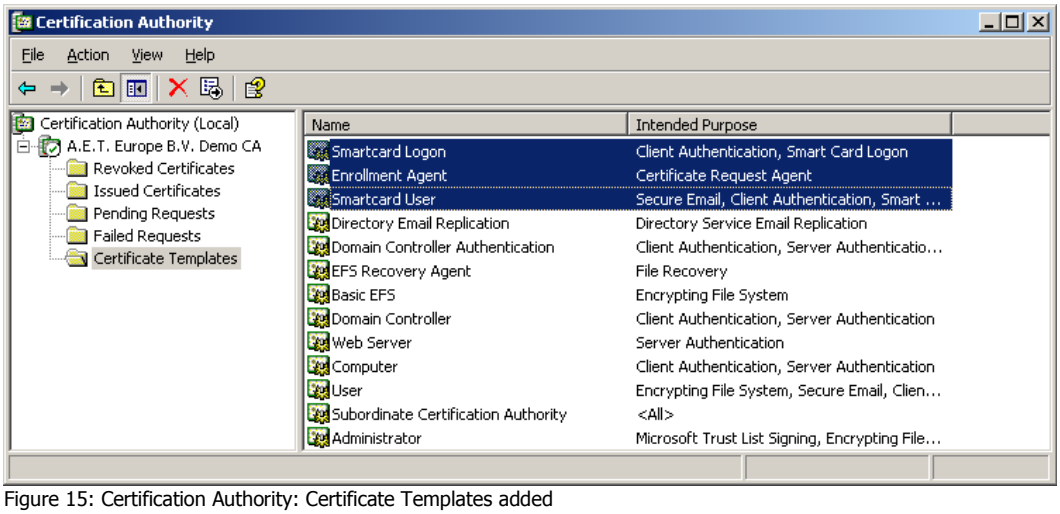


Figure 15: Certification Authority: Certificate Templates added

➔ Close the *Certification Authority* window

Important Note

Before the Microsoft CA can issue certificates to tokens that are supported by SafeSign Identity Client, you need to install SafeSign Identity Client on the same machine you have installed the Microsoft CA on, even though you do not personalise a token on this machine. By installing SafeSign Identity Client on the same machine as your Microsoft CA, you make the SafeSign Identity Client CSP selectable during token personalisation.

It is possible to create your own template, by duplicating one of the existing templates (for example, you can duplicate the Smart Card User template and then change its name and settings).

2.4 Creating a Microsoft CA RA station

In some deployment scenarios it is convenient to issue smart card certificates to entities other than yourself. A likely scenario would be that an Administrator wishes to deploy smart card certificates to all employees of a company. In this scenario an Administrator should have the possibility to issue smart card certificates to all the persons who must have a smart card.

For an Administrator to issue smart card certificates to entities other than himself, he may (have to) set up a so-called 'Registration Authority (RA) station' and obtain a so-called 'Enrollment Agent' certificate. There are several ways to retrieve an enrollment agent certificate, but in the scenario described here, an enrollment agent certificate is requested and installed via Internet Explorer.

2.4.1 Create an RA Station

These are the steps to create an RA station:

1. Install SafeSign Identity Client on the RA machine (refer to the SafeSign Identity Client Installation Guide to do so);
2. Install all the necessary smart card reader drivers;
3. Obtain an 'enrollment agent' certificate[1] (described in paragraph 2.4.2).

Note that in order to personalise a token, you will have to install on the RA machine all the necessary smart card drivers and have SafeSign Identity Client installed on the RA machine. After installation of the smart card reader and SafeSign Identity Client, the RA station is ready.

2.4.2 Request enrollment agent certificate

1 To request and retrieve an enrollment agent certificate via Internet Explorer, start the browser and go to the homepage of the Microsoft CA. This homepage can be found on http://<machine-name>/certsrv/:

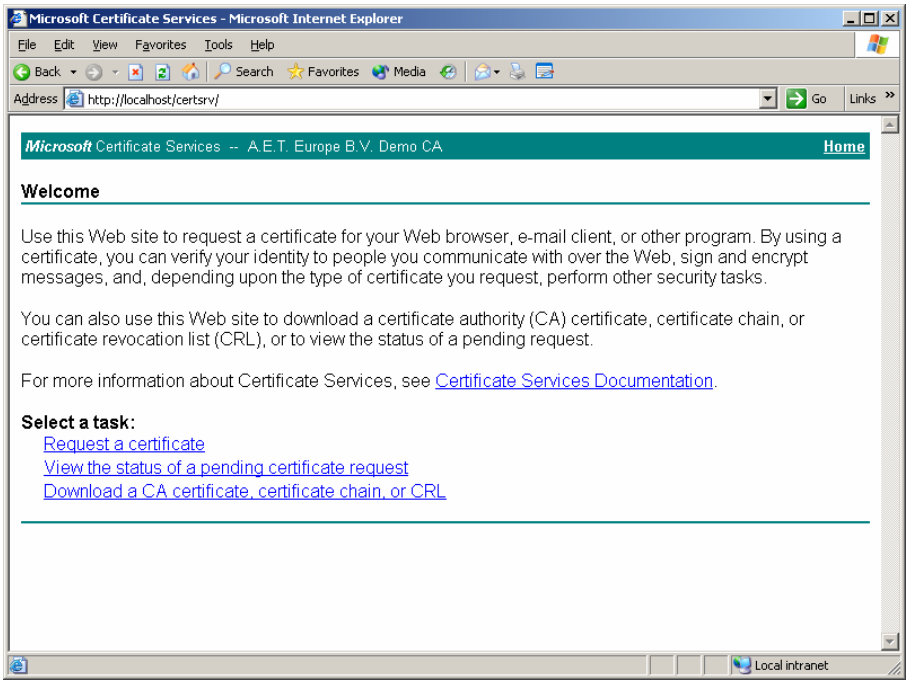


Figure 16: Microsoft Certificate Services: Welcome

➔ Select **Request a certificate**

[1] To enroll for a smart card certificate on behalf of someone, the user must have an enrollment agent certificate. The smart card enrollment agent can create smart cards on behalf of any user, including an enterprise administrator. After the smart card is created, you can use it to log on to the domain with the credentials of the user for which it was created. Thus, it is a very sensitive role. The Enrollment Agent certificate gives administrators control over which user accounts can create enroll for smart cards. This, in combination with appropriate physical security, can generate a great deal of confidence in the smart card generation process.

2 This will open the *Request a Certificate* window:

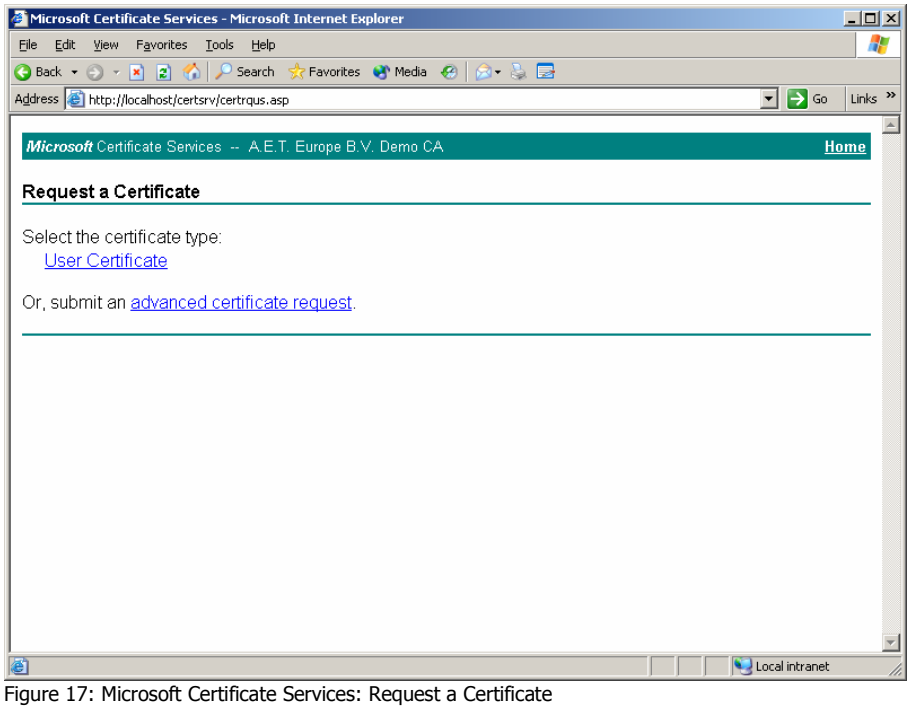


Figure 17: Microsoft Certificate Services: Request a Certificate

➔ Select **advanced certificate request**

3 This will open the *Advanced Certificate Request* window:

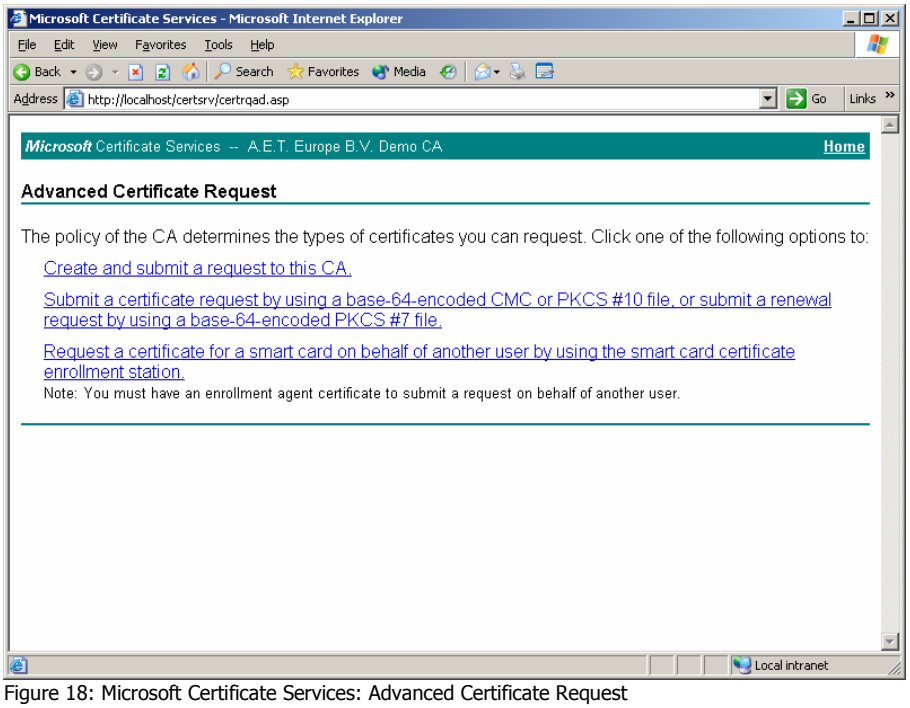


Figure 18: Microsoft Certificate Services: Advanced Certificate Request

➔ Select **Create and submit a request to this CA**

4 The *Advanced Certificate Request* window opens:

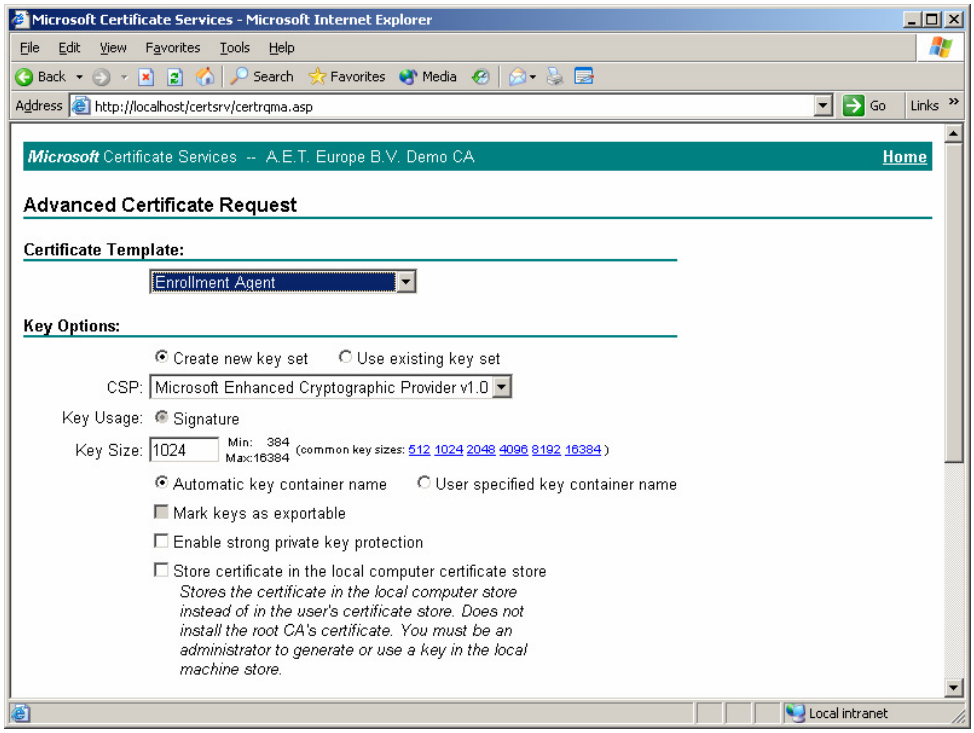


Figure 19: Microsoft Certificate Services: Advanced Certificate Requests

From the **Certificate Template** list choose **Enrollment Agent** and make sure you have selected **Microsoft Enhanced Cryptographic Provider 1.0** or similar from the CSP list under **Key Options** (as in Figure 19 above).

➔ At the bottom of the page click **Submit**

5 When the request has been made and approved, the *Certificate Issued* window will open:

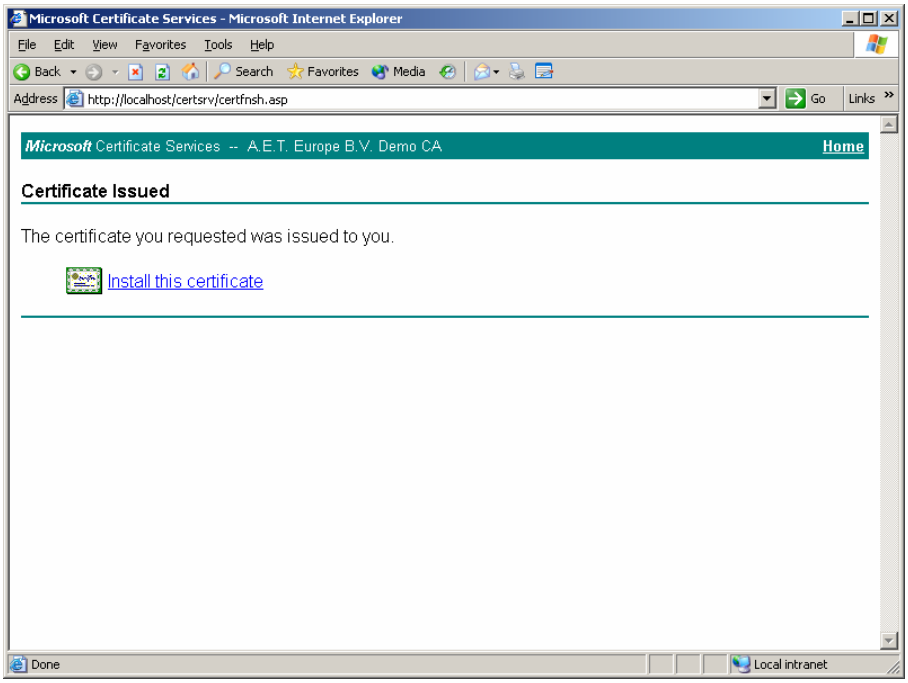


Figure 20: Microsoft Certificate Services: Certificate Issued

➔ Download the enrollment agent certificate onto the RA station by clicking **Install this certificate**

6 You will be informed when the certificate is installed:

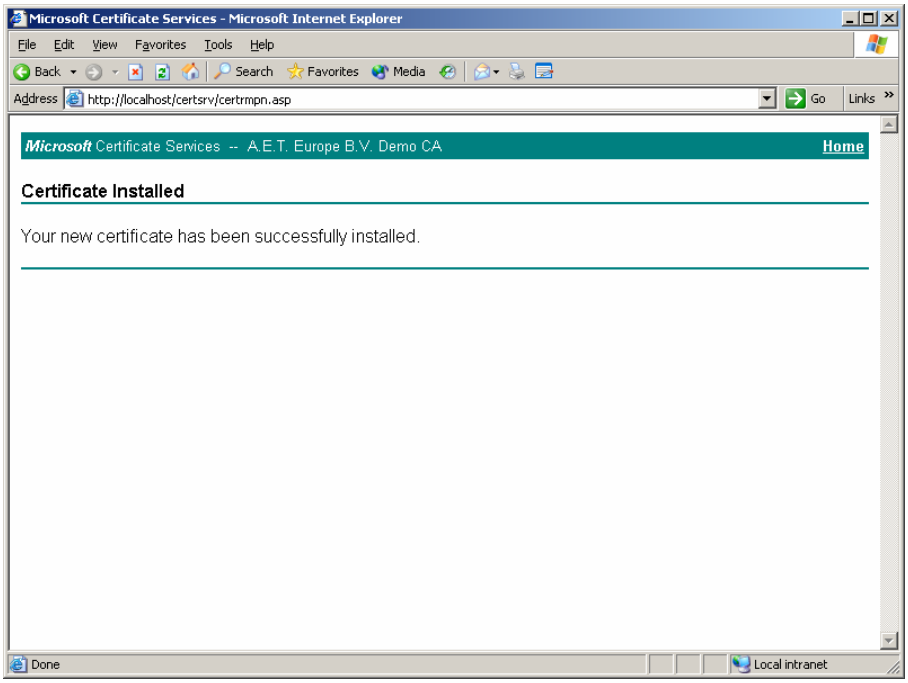


Figure 21: Microsoft Certificate Services: Certificate Installed

Now that you have installed the enrollment agent certificate, you can issue smart card certificates for other entities on the machine and account you have an enrollment agent Digital ID for.

3 Enrolling a smart card user

After you have created an RA station, as described in paragraph 2.4, you are ready to enroll smart card certificates for entities other than yourself.

Note

Enrollment for a smart card certificate must be a controlled procedure, in the same manner that employee badges are controlled for purposes of identification and physical access.

The recommended method for enrolling users for smart card-based certificates and keys is through the Smart Card Enrollment station that is integrated with Certificate Services in Windows 2003.

Therefore, we describe in this chapter the process how to enrol for a smart card user or smart card logon certificate through the Smart Card Enrolment Station, which is a process that is most likely done for you by your system administrator. As a user, you will most likely request your own certificate through the Microsoft Certificate Services interface on your local workstation. Note that in this case, a domain user cannot enroll for a Smart Card Logon certificate (which provides authentication) or a Smart Card User certificate (which provides authentication plus the capability to secure e-mail) unless a system administrator has granted the user access rights to the certificate template stored in Active Directory.

From the RA station you should connect to the 'Smart card Certificate Enrollment Station' web page of the CA.

1 This smart card enrollment web page can be found at http://<machine-name>/certsrv/ where the <machine-name> is the name of the machine where you have installed the CA:

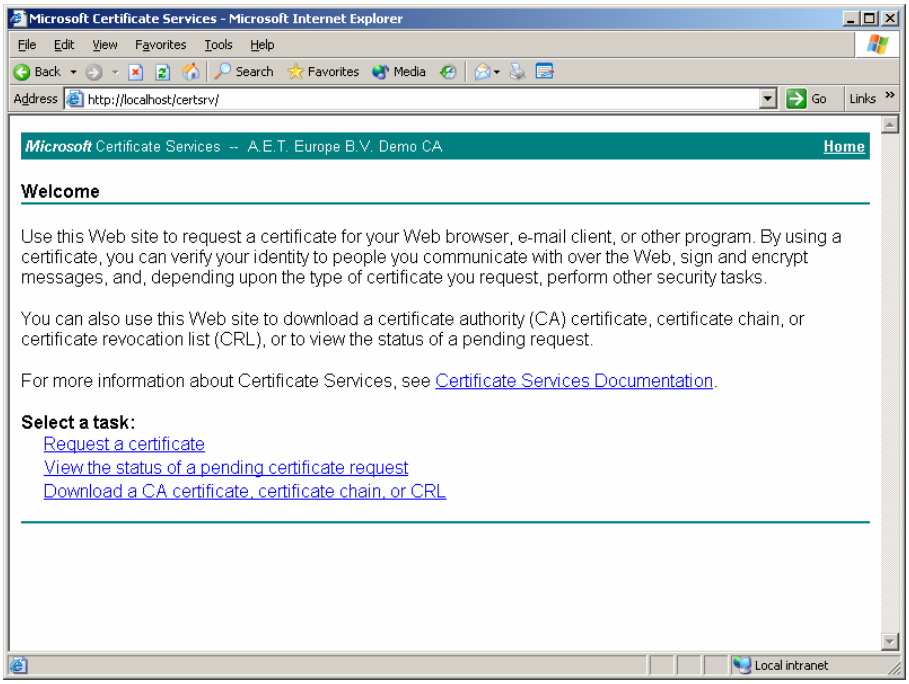


Figure 22: Microsoft Certificate Services: Welcome

➔ Select **Request a certificate**

2 This will open the *Request a Certificate* window:

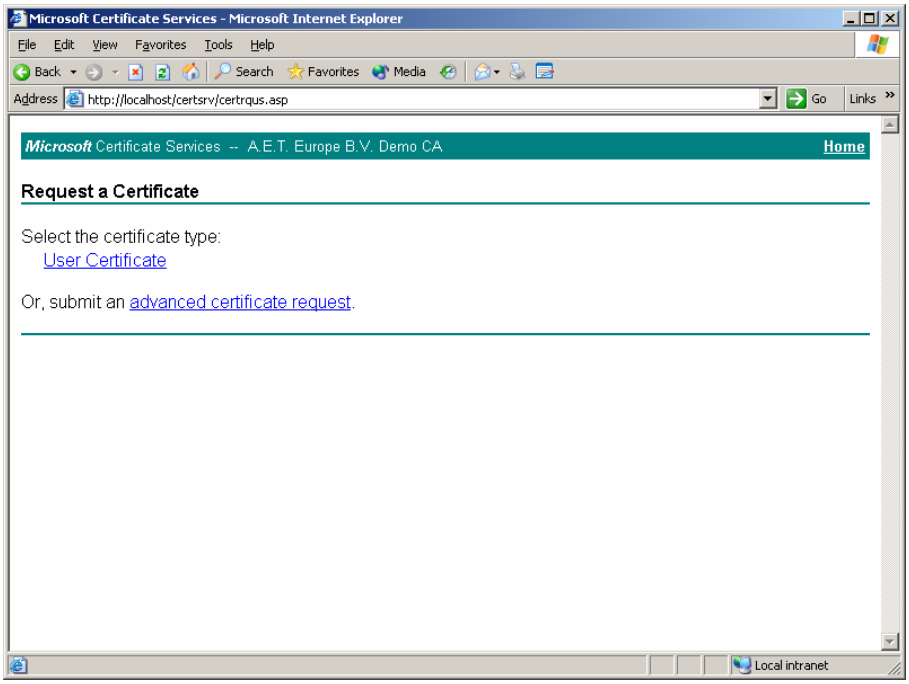


Figure 23: Microsoft Certificate Services: Request a Certificate

➔ Select **advanced certificate request**

3 This will open the *Advanced Certificate Request* window:

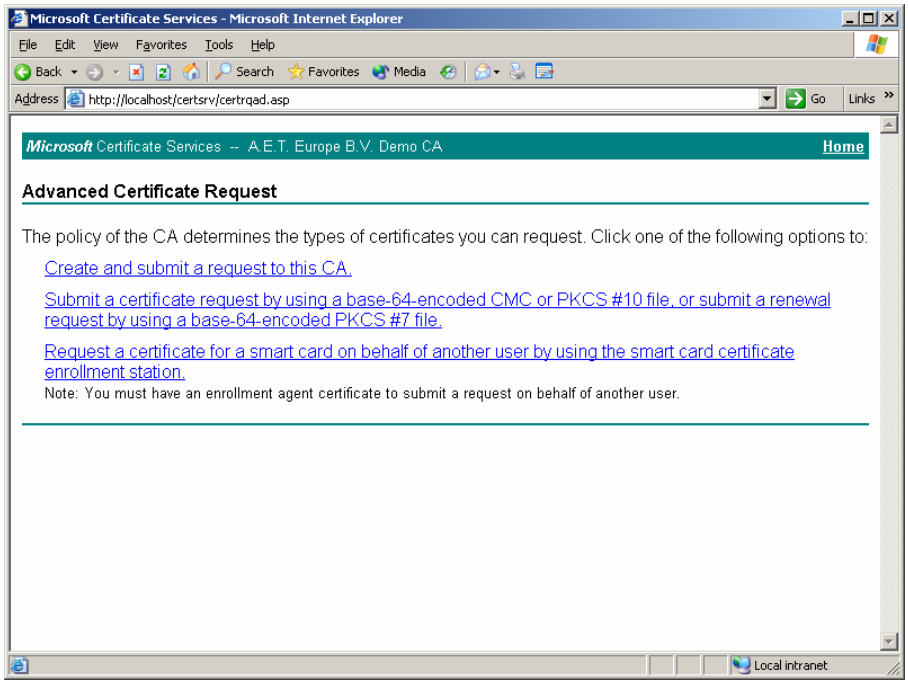


Figure 24: Microsoft Certificate Services: Advanced Certificate Request

➔ Select **Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station**

4 The *Smart Cart Certificate Enrollment Station* window opens:

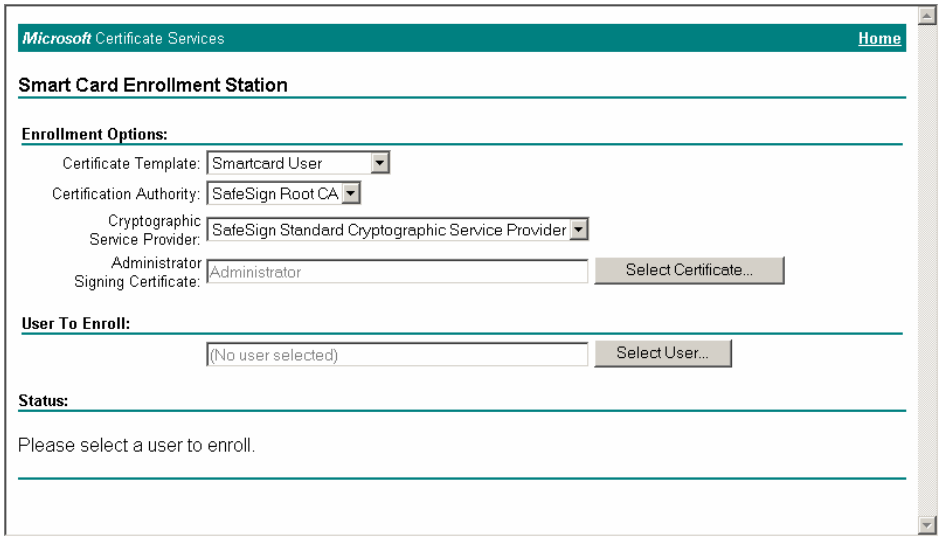


Figure 25: Microsoft Certificate Services: Smart Card Certificate Enrollment Station

Note

If you encounter an 'ActiveX' error upon connecting to this page, refer to paragraph 3.1 for more details on how to resolve this.

Under **Enrollment Options**:

From the **Certificate Template** drop-down list, choose **Smartcard User**

From the **Cryptographic Service Provider** drop-down list, select **SafeSign Identity Client Standard Cryptographic Service Provider**

Make sure that the correct Enrollment Agent certificate is selected in the **Administrator Signing Certificate** box

➔ You should now select a **User To Enroll** by clicking the button **Select User**

5 Clicking on **Select User** will open the *Select User* dialog:

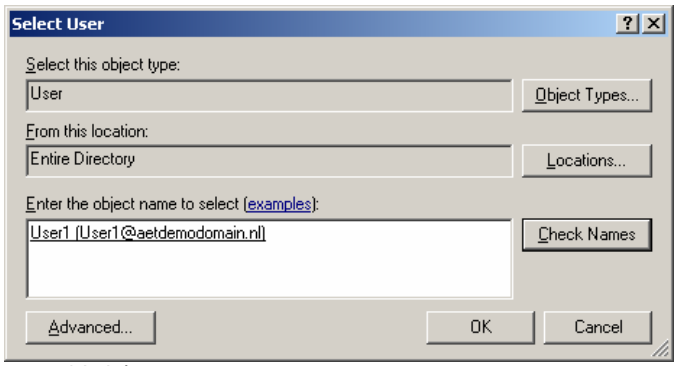


Figure 26: Select User

➔ Enter the name of the user you want to enroll a certificate for in the *Enter the object name to select* box and click **Check Names** to verify that you have entered the object name correctly. If this is the case the username is highlighted. After you have verified that this is the user you want to enrol a certificate for, press the **OK** button.

6 Upon clicking **OK** in the *Select User* dialog, you will return to the **Smart Card Certificate Enrollment Station** window (Figure 25), where the user is selected and ready to be enrolled:

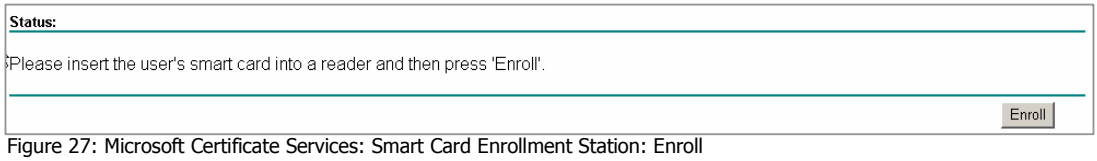


Figure 27: Microsoft Certificate Services: Smart Card Enrollment Station: Enroll

➔ Click **Enroll** to enroll a smartcard user certificate for the user

Please verify that the user's token is inserted in the smart card reader prior to pressing the enroll button.

No token inserted

If there is no smart card in the smart card reader you are prompted to do so[1]:

Figure 28: Please insert the user's smart card

➔ Click **OK**

[1] This dialog will also appear when you have inserted a smart card that is not recognized / supported by SafeSign Identity Client.

7 During the enrollment process, you are prompted that there could be a potential scripting violation:

Figure 29: Potential Scripting Violation: Do you wish to request a certificate now?

➔ When you encounter this prompt, click **Yes**

8 During the enrollment process, you are prompted to enter the PIN of the token:

Figure 30: SafeSign Identity Client Login

➔ After entering to PIN, click **OK** to continue

Protected authentication path

When you are using a protected authentication path device, you should not enter the PIN in the *Enter PIN* box above, but click **OK** or **Enter** to be allowed to use your protected authentication path device.

When you are using a secure pinpad reader, you will be asked (either through a secure PIN entry dialog on-screen or on the secure pinpad reader's display) to enter the PIN for your token on the keypad of the secure pinpad reader. Note that in addition, when you are using SafeSign Identity Client Bio, the *Authentication* dialog will be displayed, showing a picture of the secure pinpad you are using.

Though it would be possible to use a biometric sensor (only in combination with SafeSign Identity Client Bio and a token initialised with a multi-factor profile), this is not a very likely scenario, as this requires the token's user to be present to authenticate with his fingerprint. However, it is possible for some scenario's, where PIN or finger(s) are involved.

This user guide will assume that you have initialised a token with the default profile (with PIN).

For more information on the different authentication methods, please refer to the SafeSign Identity Client User Guide for Authentication.

9 After the certificate request has been made, the CA will sign the request and return a certificate. This certificate is automatically placed on the token. You may be prompted about a potential scripting violation:

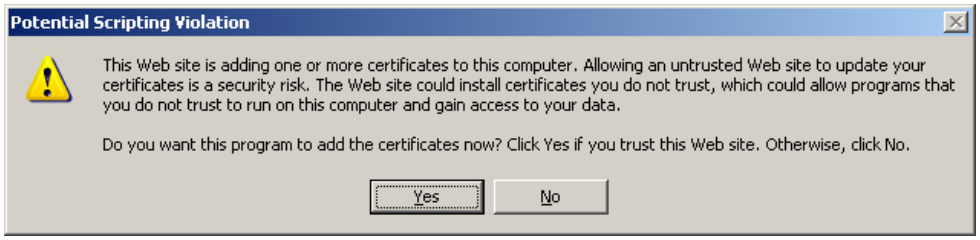


Figure 31: Potential Scripting Violation: Do you want this program to add the certificates now?

➔ Click **Yes** to continue

10 At the end of the smart card enrollment process you are informed about the fact the smart card is ready for use:

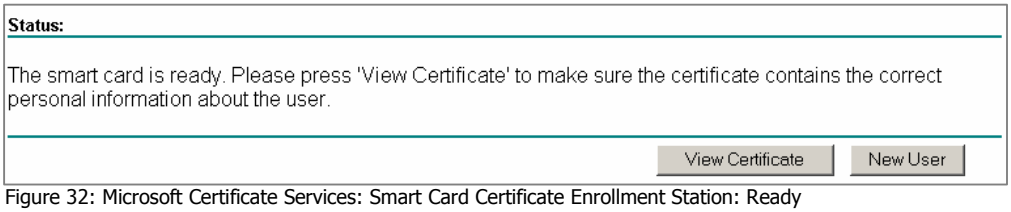


Figure 32: Microsoft Certificate Services: Smart Card Certificate Enrollment Station: Ready

You can verify if the certificate contains the correct personal information about the user, by clicking **View Certificate** to view it. You also have the opportunity to enroll a new user, by clicking **New User**.

3.1 ActiveX error message during certificate requests

When visiting some CA web pages, you may encounter a so-called 'ActiveX' error This error is caused by the fact that some ActiveX controls are not trusted within the Internet Explorer browser. As a result, you cannot view the page as it was intended, hence you cannot enroll a certificate from that page.

When visiting the web page of the **Smart Card Certificate Enrollment Station**, you may encounter such an 'ActiveX' error:

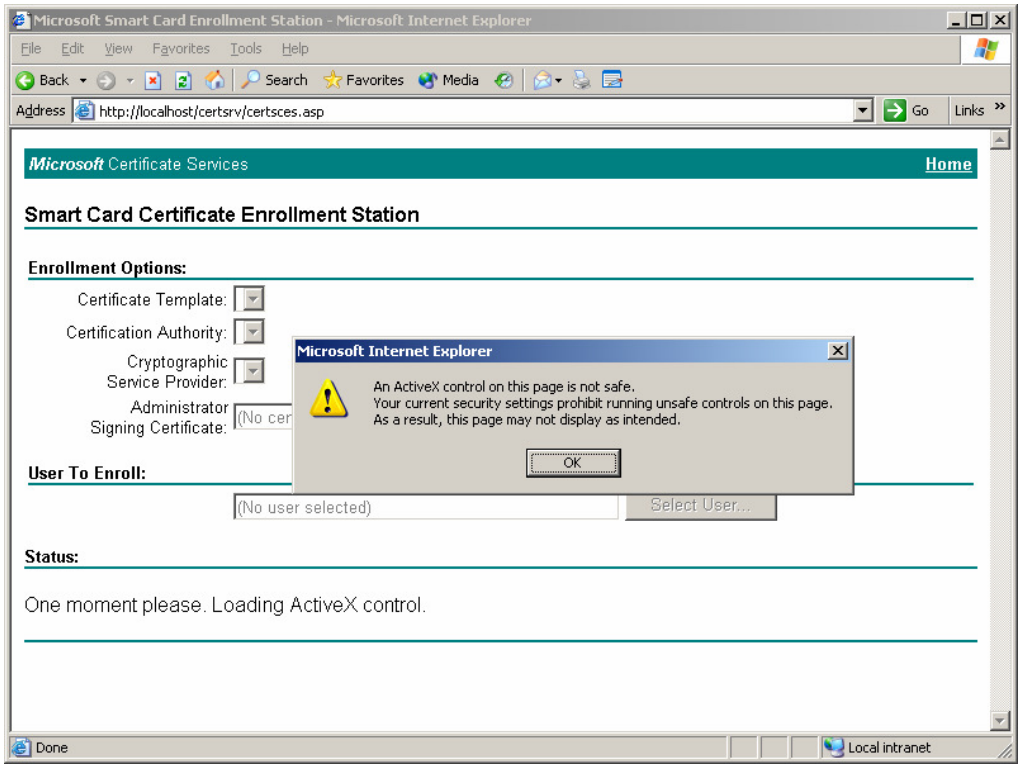


Figure 33: Microsoft Certificate Services: An ActiveX control on this page is not safe

There are several ways to resolve this issue. Thus guide will describe a scenario that configures the security of the Internet Explorer browser in such a way that it will accept the ActiveX control components. This implies that you do not have to follow the scenario we describe (as this entails bringing down the security of the Internet Explorer browser). A different solution may be better suited for your situation[1]..

Note that adding the **Smart Card Certificate Enrollment Station** page to the list of Trusted Sites does not work, as it does under Windows 2000.

➔ Go to **Tools > Internet Options...** to open the *Internet Options* dialog

[1] For other ActiveX control issues, see Knowledge Base article: 'ActiveX Error Messages Using Certificate Enrollment Web Pages to Enroll a Smart Card in Internet Explorer', http://support.microsoft.com/default.aspx?scid=kb;en-us;330211 and Configuring and Troubleshooting Windows 2000 and Windows Server 2003 Certificate Services Web Enrolment, http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/webenroll.mspx

In the *Internet Options* dialog, open the tab **Security** and select **Local intranet** (as below):

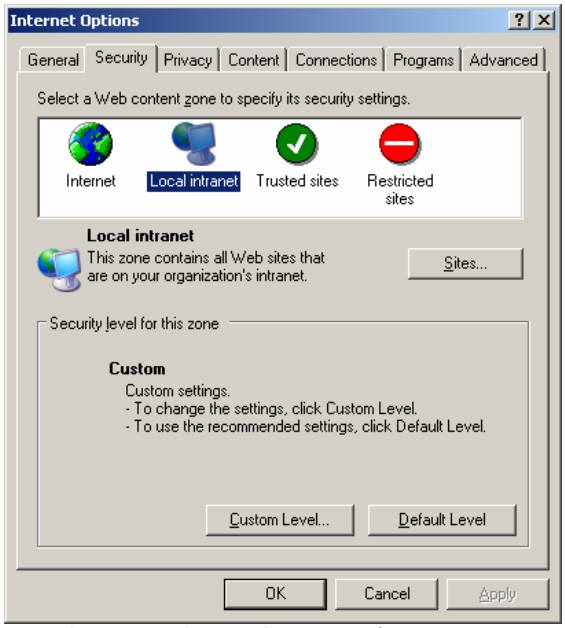


Figure 34: Internet Options: Security Local intranet

➔ Click on **Default Level**

Bring down the slider to **Low** to decrease the security level:

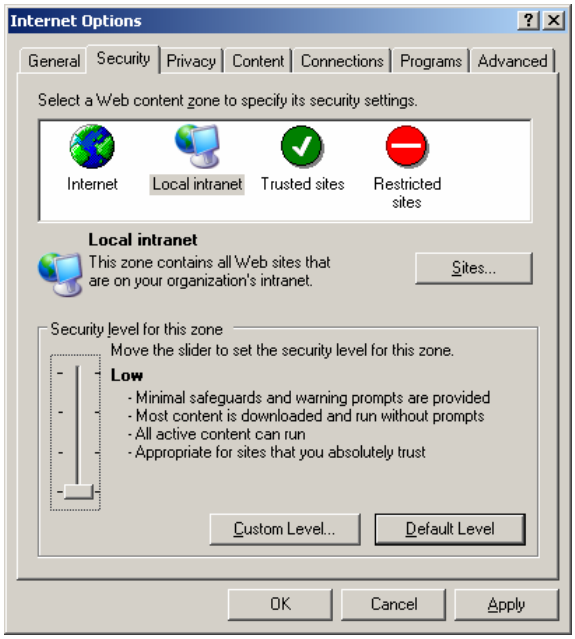


Figure 35: Internet Options: Security Local intranet: Low

➔ Close this dialog by clicking **OK**

Reload the page where you encountered the ActiveX issue. You will be prompted to allow interaction with an ActiveX control:

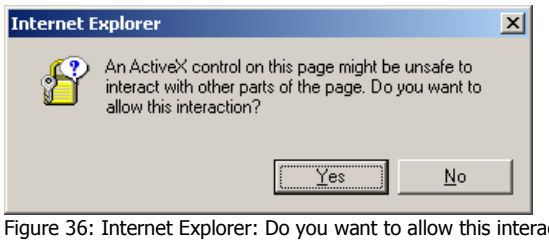


Figure 36: Internet Explorer: Do you want to allow this interaction?

➔ Click **Yes**

The **Smart Card Certificate Enrollment Station** page will now be correctly displayed.

3.2 Troubleshooting smart card enrolment

There are a number of causes why smart card enrolment may fail. We will list a few of the most common errors that may occur and their probable cause.

3.2.1 Token is blank / uninitialised

When the token is blank, has not been initialised, the following error will be displayed:

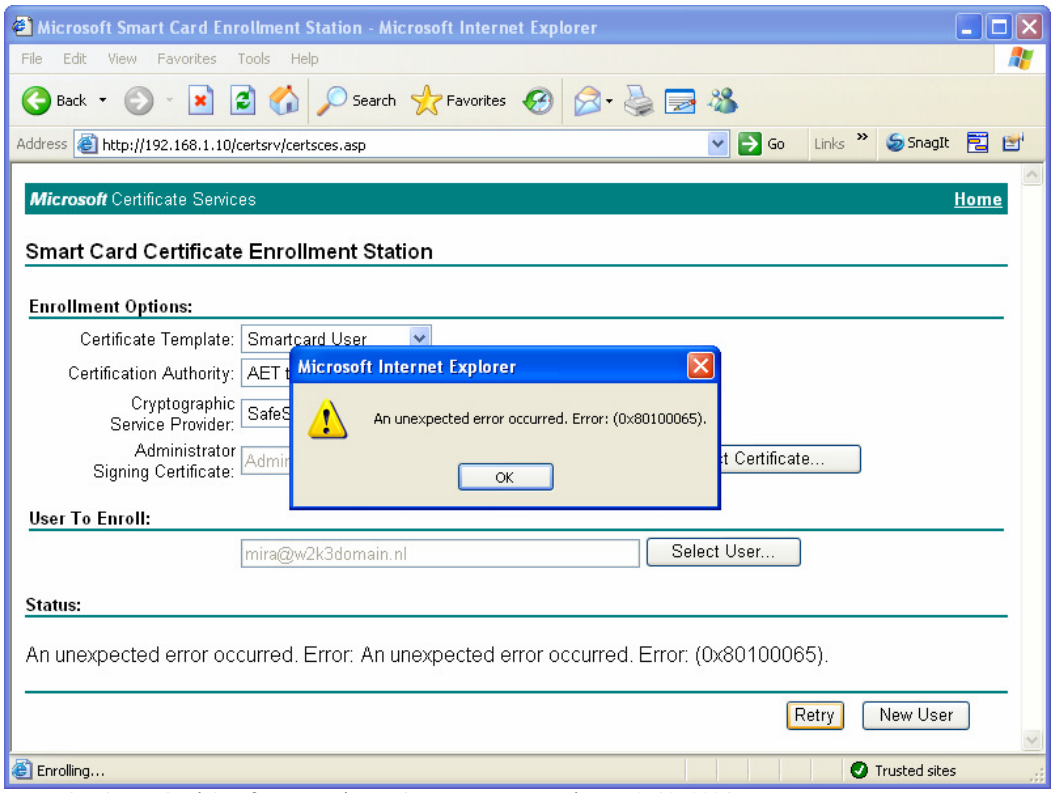


Figure 37: Smart Card Certificate Enrolment Station: Unexpected error 0x80100065

➔ Check the status of the token with the Token Management Utility / Token Administration Utility. If the token is not initialised, you should do so, setting a token label, PIN and PUK.

3.2.2 Token is unknown

When the token is not recognised, the following error may be displayed:

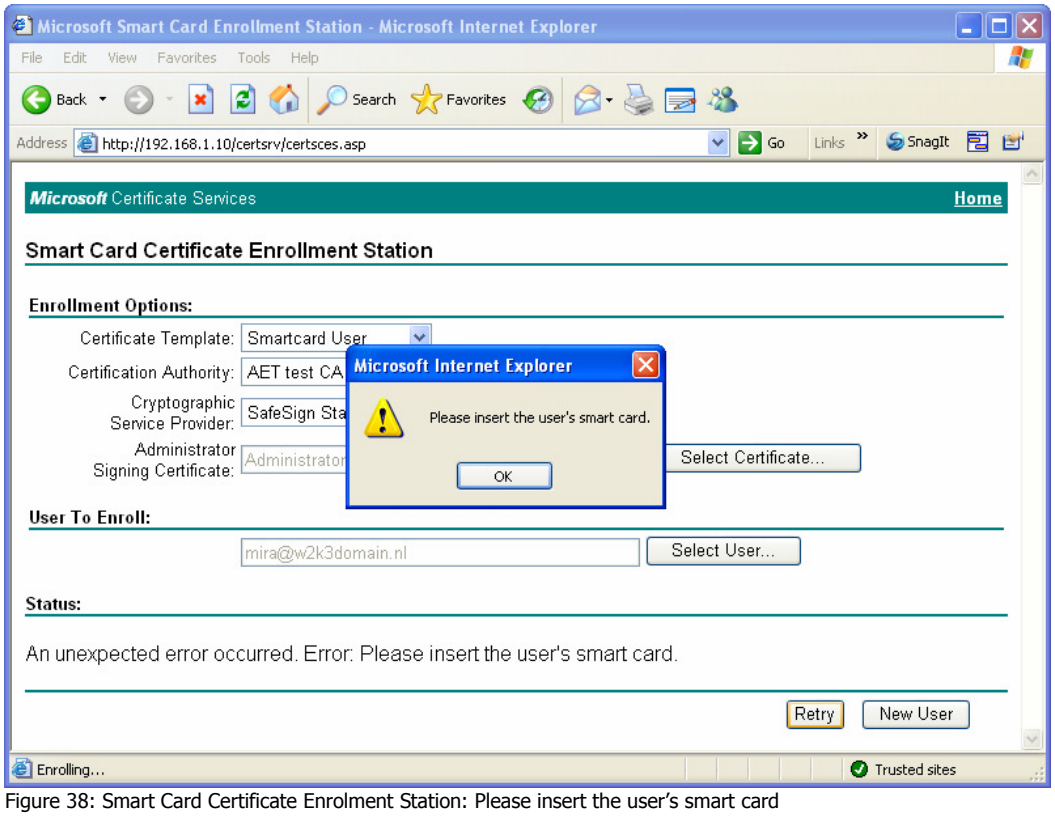


Figure 38: Smart Card Certificate Enrolment Station: Please insert the user's smart card

➔ Check the status of the token with the Token management Utility / Token Administration Utility. If it says 'Unknown token', verify if a) the token type is supported by SafeSign in the first place and b) if the token may not be recognised yet, in which case you can use the option 'Query unknown token' to add its data to the registry.

Note that this error also occurs when there is no token in the reader inserted at this point.

3.2.3 Wrong CSP

When you have selected the wrong CSP (i.e. a CSP that does not correspond to the token you have inserted), the following error will be displayed:

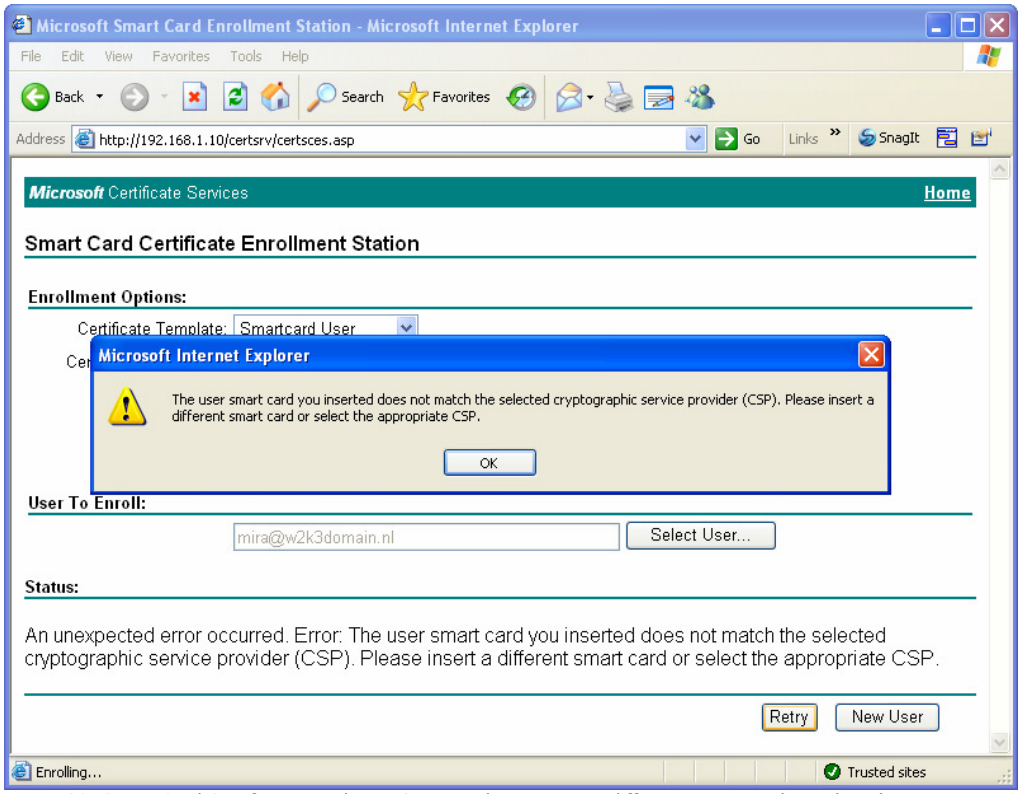


Figure 39: Smart Card Certificate Enrolment Station: Please insert a different smart card or select the appropriate CSP

➔ Verify that the CSP you have selected from the Cryptographic Service Provider drop-down list, is the 'SafeSign Standard Cryptographic Service Provider'.

3.2.4 The token PIN is locked

When the PIN of the token is locked, you will be notified by the following dialog:

Figure 40: Token locked: The token is locked

When you click **OK**, the following error will be displayed:

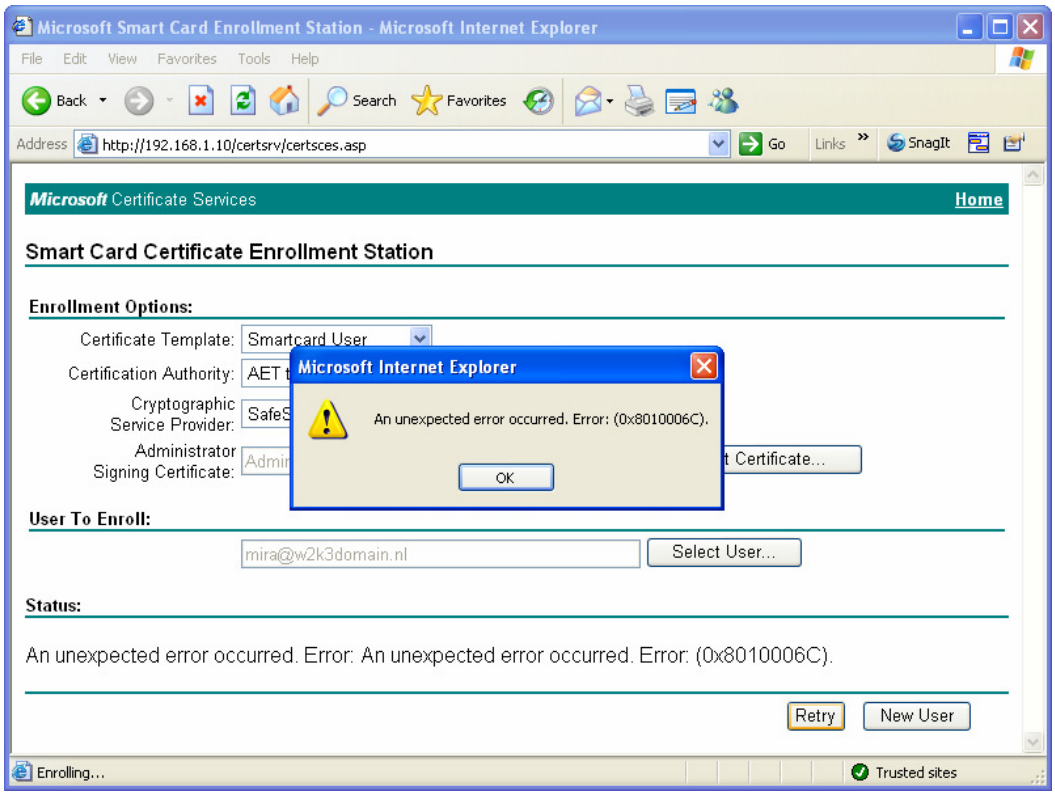


Figure 41: Smart Card Certificate Enrolment Station: Unexpected error 0x8010006C

➔ Check the status of the token with the Token Management Utility / Token Administration Utility. If the PIN is locked, you should be able to unlock it by means of the Unlock PIN feature.

3.2.5 Key length setting

When the minimum key size in the Certificate Templates (in this case, the Smart Card User, Smart Card Logon or your own custom template, based on these) has been set to a key length not supported by the token[1], the software will nevertheless try to generate a key pair of this size and fail. The following error may be displayed:

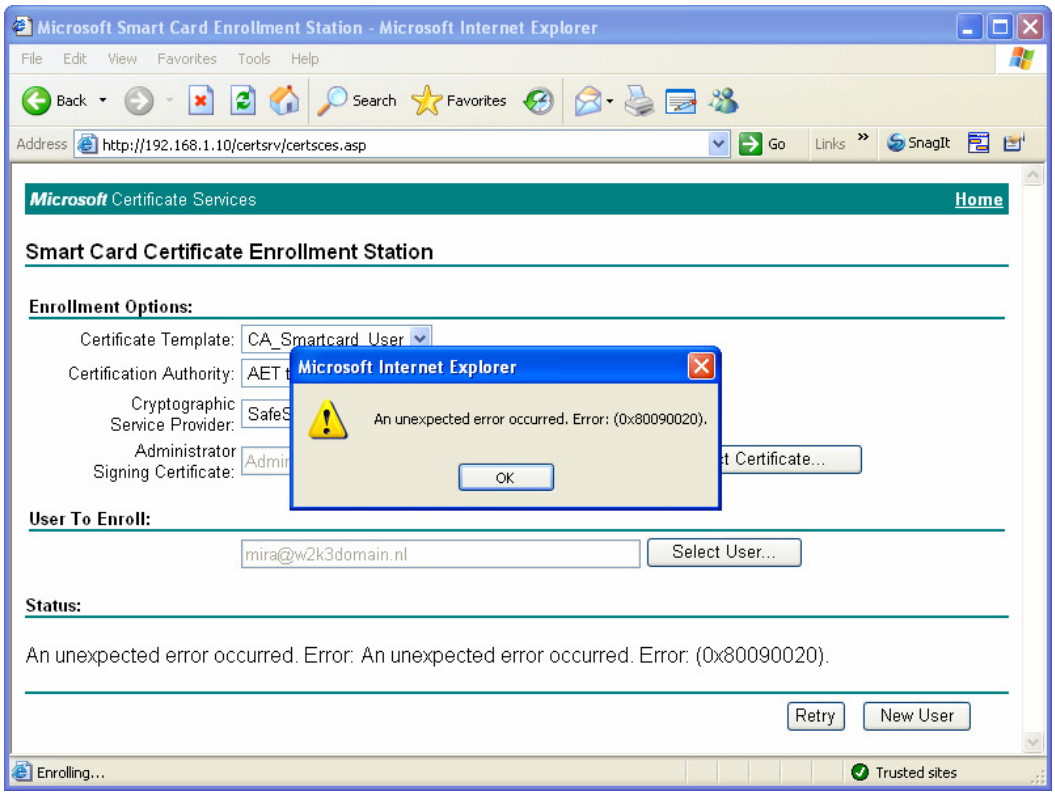


Figure 42: Smart Card certificate Enrolment Station: Unexpected error 0x80090020

[1] In particular, if you are using a Java Card 2.1.1 card (such as a JCOP20).

Check the Certificate Template that is used and if necessary, edit the minimum key size to 1024:

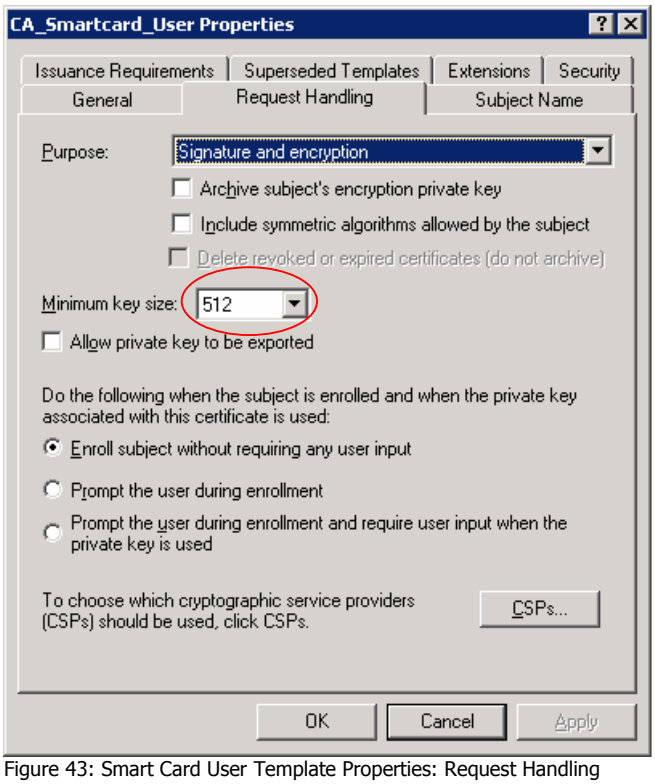


Figure 43: Smart Card User Template Properties: Request Handling

3.2.6 Enrolment rights

- When the Administrator Signing Certificate is not available, check whether the user logged in and who is acting as the enrollment agent, has an enrollment agent certificate.
- When the Certificate Template you require, is not available, verify the rights of the enrolment agent on the desired template. The enrolment agent should have read and enroll rights on the template.

4 Secure Logon

You can use your SafeSign Identity Client token to log on to a Windows domain with Windows 2000, XP and 2003.

When Windows logon via a smart card is activated and a valid PC/SC reader is found by the operating system, you will see a smart card reader icon at the logon prompt. Windows will ask you to log on, either by clicking **CTRL + ALT + DEL** and entering a username and password, or by inserting a smart card and entering a PIN ("*Insert card or press Ctrl+Alt+Delete to begin*"):

➔ When the Windows logon prompt appears, insert / re-insert your SafeSign Identity Client Token

When you insert your token, you will be asked to enter the PIN for your token:

Figure 44: Log On to Windows: PIN

➔ Enter the PIN of your SafeSign Identity Client Token and click **OK**

When your credentials have been verified, Windows will start up.

Stand-alone logon

The procedure described above is Windows domain logon: you log on to a particular domain your computer is member of.

In order to perform smart card logon to a stand-alone, local (Windows 2000 or Windows XP) computer, you will need a third-party application.

4.1 Select Digital ID

When your token contains more than one Digital ID suitable for smart card logon (either for the same domain or for different domains), it is possible to select the Digital ID you want to use for smart card logon[1].

Note that this functionality needs to have been enabled in the registry (for a detailed description of this functionality and how to activate it, refer to the Administrator's Guide)[2].

When enabled, the user will be prompted to select the Digital ID he wants to use, after he has entered the PIN for the token, by the following dialog:

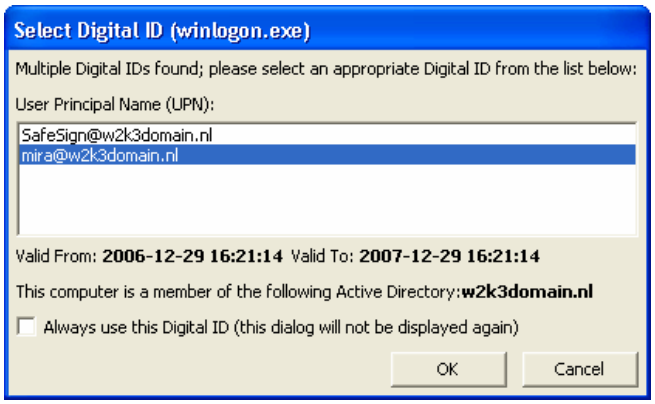


Figure 45: Select Digital ID (winlogon.exe)

In the example above, the token contains two Digital IDs suitable for smart card logon, one for a user named 'SafeSign', the other for a user named 'Mira'. Both Digital IDs can be used to logon to the same domain (called 'w2k3domain'). Note that it is also possible that the token contains two (or more) Digital IDs, suitable for smart card logon, for different domains.

You can select one of the Digital IDs for logon to be logged on as that user.

It is also possible to select '*Always use this Digital ID (this dialog will not be displayed again*'). When this option is selected, the dialog will still appear at logon, with a 5 seconds counter (before the OK button is clicked), before login will proceed with the selected certificate:

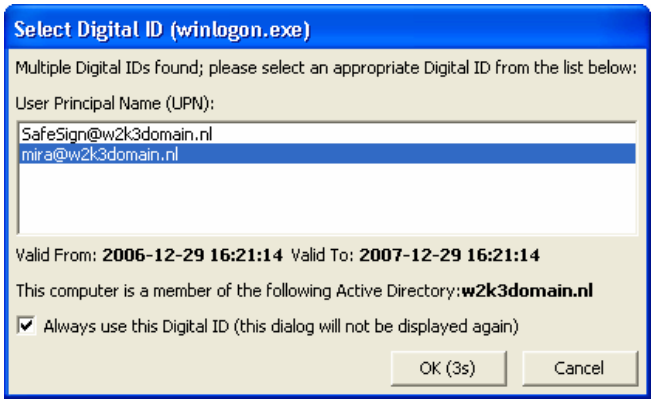


Figure 46:Select Digital ID (winlogon.exe): Always use this Digital ID

This functionality has been included to allow users to be aware / reminded of the fact that their token contains multiple Digital IDs for logon (should they want to switch at a given time). This counter can be configured in the registry[3].

[1] Implemented from SafeSign version 2.3.2 onwards (≥ 2.3.2).
[2] In order to enable and configure this functionality, you need to have sufficient rights to edit the registry.
[3] In order to enable and configure this functionality, you need to have sufficient rights to edit the registry.

4.2 Smart Card Removal Behaviour

For security reasons it could be advisable to enable smart card removal behaviour. This means when a user removes his / her token from the smart card reader a pre-defined policy will be activated within that domain.

Smart card removal behaviour is defined by a security policy. This policy determines what should happen when the token for a logged-on user is removed from the smart card reader. The options are:

- No Action
- Lock Workstation: the workstation is locked when the token is removed
- Force Logoff: the user is automatically logged off when the token is removed

If *Lock Workstation* is specified, then the workstation is locked when the token is removed, thereby allowing users to leave their workplace and take their token with them, while still maintaining a protected session. This policy setting is described below.

4.2.1 Configuration of Smart Card Removal Behaviour

Smart card removal behaviour is configured on the Domain Controller. In order to configure the smart card removal behaviour for your domain, go to the **Domain Security Policy** settings, where you can configure smart card removal behaviour for your domain (i.e. all computers in the domain, apart from the Domain Controller itself[1]).

To open the **Domain Security Policy** settings, go to **Start > Settings > Control Panel > Administrative Tools**:

Figure 47: Domain Security Policy

When you have activated the **Domain Security Policy** settings, go to **Local Policies > Security Options**:

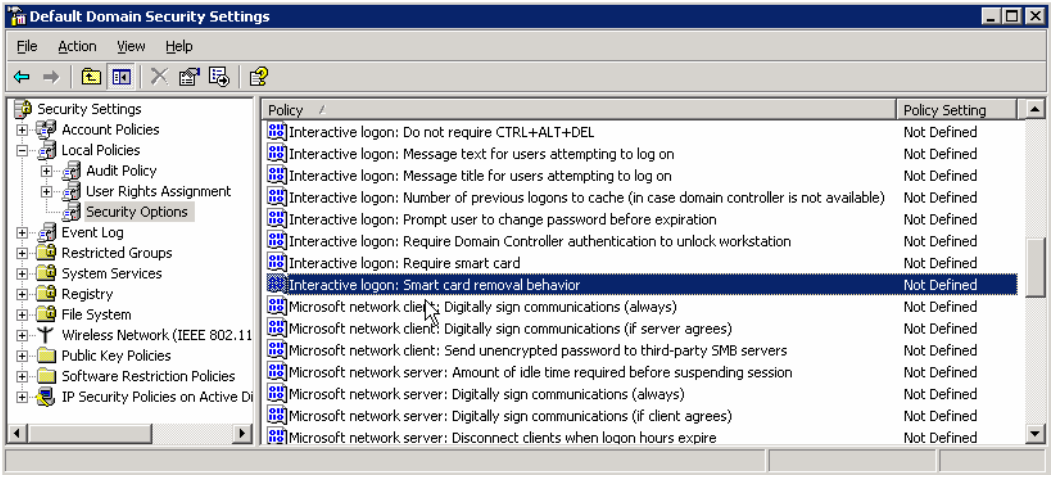


Figure 48: Default Domain Security Settings

In the right pane, you will find 'Interactive logon: Smart card removal behavior', which is be default 'Not Defined'.

➔ In the right pane, double-click 'Interactive logon: Smart card removal behavior'.

[1] Do not confuse this with the **Domain Controller Security Policy** settings, where you can configure the Security Policy for the Domain Controller itself.

The *Interactive logon: Smart card removal behaviour Properties* dialog open:

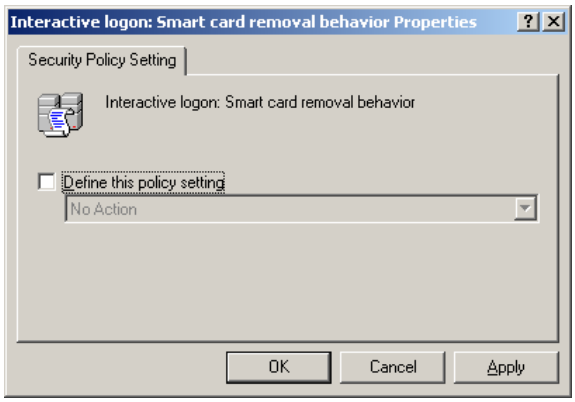


Figure 49: Interactive logon: Smart card removal behavior Properties

➔ Check **Define this policy setting**

You can now define a policy setting for the behaviour you wish to see when a token is removed from within your domain:

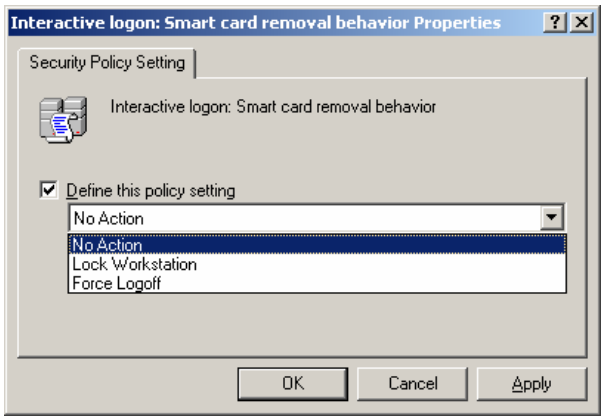


Figure 50: : Interactive logon: Smart card removal behavior Properties: Define this policy setting

There are three types of action to choose from:

- **No Action**: no action will be taken the moment a token is removed from the smart card reader;
- **Lock Workstation**: when a token is removed, the desktop will be locked until an Administrator or the user that removed the token unlocks the desktop (by inserting the token and entering the PIN);
- **Force Logoff**: when a token is removed, the user will be logged off from the current desktop.

➔ Select the desired policy and click **OK**

The smart card removal behaviour for you domain is now set.

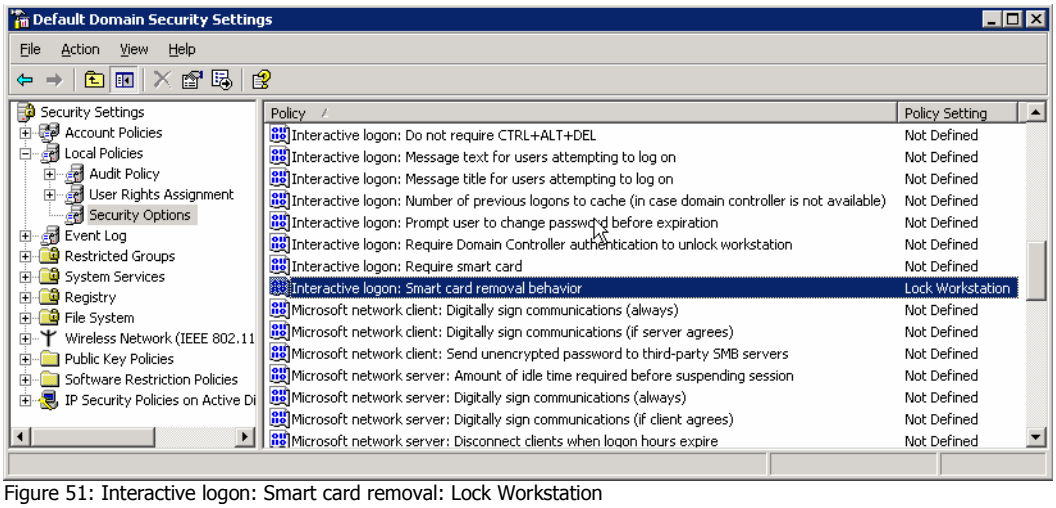


Figure 51: Interactive logon: Smart card removal: Lock Workstation

Please be advised that it could / will take until the next Active Directory update before this policy will take effect.

4.2.2 Lock your computer

In order to lock your computer with your SafeSign Identity Client Token, remove the SafeSign Identity Client Token from the smart card reader. The computer will now be locked until you re-insert the token enter the PIN.

4.2.3 Unlock your computer

In order to unlock your computer with your SafeSign Identity Client Token, insert your token in the smart card reader (while the *Computer Locked* dialog is presented).

When you insert the token, you will be asked to enter the PIN for your token

➔ Enter the PIN of your SafeSign Identity Client Token and click **OK**

When your credentials have been verified, your computer will be unlocked.

If you enter an incorrect PIN when trying to unlock the machine, Windows will display the *Computer Locked* error dialog: "*The computer is locked. Only [logged on user name] or an administrator can unlock this computer.*"

4.3 SafeSign GINA

The SafeSign GINA is primarily intended for users of protected authentication path devices, such as a secure pinpad reader. It improves usability, as it instructs the user to enter his PIN on his protected authentication path device, when prompted to do so. Section 4.4 describes the use of protected authentication path devices and smart card logon, assuming the GINA is installed.

The GINA also includes a number of other functionality, which is described in the paragraphs below.

4.3.1 Logon with Starkey 220 HID token

By the nature of HID, it is not possible to logon with an HID token. However, the SafeSign enables you to do smart card logon with a StarKey220 HID token.

4.3.2 Smart card removal

The GINA provides additional functionality with regard to smart card removal at log off / lock. When the user tries to lock the computer or log off, he will get an auditory and visual signal to remove the card from the reader. The dialog displayed is the following:

Figure 52: SafeSign GINA: Remove token

Unless the user removes his token, he will not be logged off or the computer will not lock.

This functionality can be set in the registry (only when the GINA is installed). Refer to the SafeSign Identity Client Administrator's Guide how to enable this functionality[1].

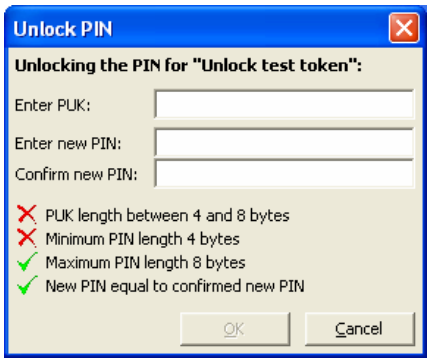
When the GINA is installed, it is possible at logon time, to unlock a token of which the PIN is blocked (paragraph 4.3.3) and to change the transport PIN of a token that has a transport PIN (paragraph 4.3.4).

[1] In order to enable and configure this functionality, you need to have sufficient rights to edit the registry.

4.3.3 Unlock PIN

When the PIN of the token you are trying to logon with is locked, you will be allowed to unlock the PIN at logon. After entering the (locked) PIN at the Windows logon prompt, a dialog will inform you that the token is locked and ask you if you want to unlock the token.

Note that the PIN may be unlocked in two ways: by means of the PUK or by means of the secure off-line PIN unlock mechanism (if this has been implemented). If the token can only be unlocked by means of the PUK, the



following dialog will appear:

Figure 53: Unlock PIN

➔ Enter the PUK for the token and a new PIN to unlock the token

If secure off-line PIN unlock is implemented, the user will be allowed to chose which method to use for unlocking the PIN, either by using the PUK or by off-line PIN unlock:

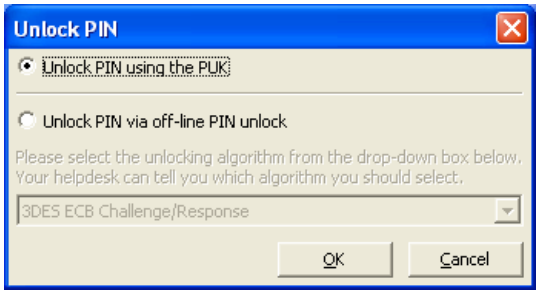


Figure 54: Unlock PIN: Select method

When selecting the option to '*Unlock PIN via off-line PIN unlock*', the user should contact the designated person or department (e.g. helpdesk) to obtain the necessary details for unlocking the PIN:

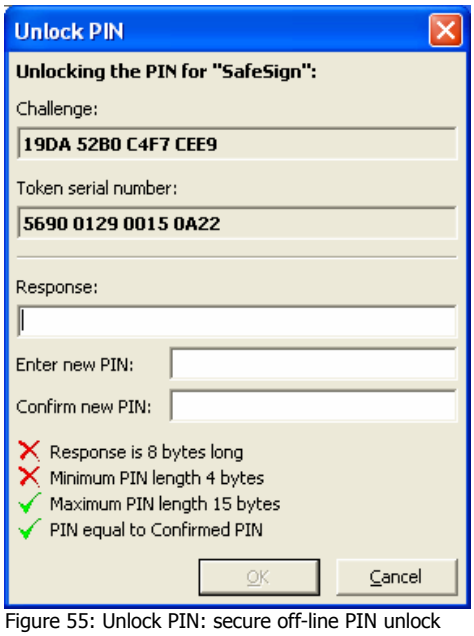


Figure 55: Unlock PIN: secure off-line PIN unlock

4.3.4 Change Transport PIN

When the token you are trying to logon with has a Transport PIN, you cannot logon with the token until the Transport PIN is changed.

At logon, a dialog will inform you that the token still has a Transport PIN and ask you if you want to change the Transport PIN. When selecting Yes, you will be allowed to change the Transport PIN:

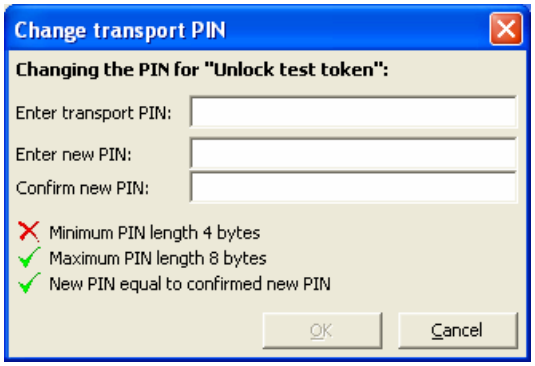


Figure 56: Change transport PIN

➔ Enter the Transport PIN for the token and then enter a new PIN

4.4 Logon with protected authentication path devices

4.4.1 Secure pinpad reader

When you have a secure pinpad reader, you should not enter the PIN of your SafeSign Identity Client token in the PIN dialog that Windows presents upon card insertion. Rather, you should use the keypad of your secure pinpad reader.

SafeSign Identity Client facilitates this for you, when you have installed the SafeSign Identity Client GINA[1]. When you insert your token at the Windows logon dialog ("*Insert card or press Ctrl+Alt+Delete to begin*") in a secure pinpad reader, the SafeSign Identity Client GINA dialog for secure pinpad readers will appear, instead of the Windows Logon PIN prompt (Figure 44). The dialog displayed looks like this:

Figure 57: SafeSign Identity Client GINA for secure pinpad readers

You will then be prompted by your secure pinpad reader when to enter the PIN on its keypad, either by a message on the display of your secure pinpad reader or by a blinking LED. Note that the way this is done, is determined by the secure pinpad reader and cannot be influenced by SafeSign Identity Client. The paragraphs below describe how this works for the different secure pinpad readers supported.

Note that if you do not install the GINA, the secure pinpad reader functionality is supported, but the above dialog (Figure 57) will not appear (but Figure 44).

4.4.1.1 G&D CashMouse (Class 3)

The G&D CashMouse[2] has a display, which will instruct you when to enter your PIN.

1. At the Windows Logon prompt, "*Insert card or press Ctrl+Alt-Delete to begin*", insert your token in the CashMouse reader;
2. The SafeSign Identity Client GINA for secure pinpad readers will be displayed (see Figure 57 above);
3. Wait until the CashMouse display asks you to enter your PIN for the token;
4. When it does ("*Bitte Geheimzahl eingeben*"), enter your PIN and then click "**Bestätigung**" (OK / Confirm) on the pinpad;
5. You will then be logged on.

4.4.1.2 Omnikey CardMan Trust (Class 2)

The Omnikey CardMan Trust[3] does not have a display[4]. This means that although the SafeSign Identity Client GINA will instruct you '*when prompted, please enter your PIN on the protected PIN entry pad of your smart card reader*', the nature of this prompt is defined by the smart card reader.

1. At the Windows Logon prompt, "*Insert card or press Ctrl+Alt-Delete to begin*", insert your token in the CardMan reader;
2. The SafeSign Identity Client GINA for secure pinpad readers will be displayed (see Figure 57 above);
3. Wait until the LED on the right side of the reader starts blinking **red** to enter your PIN for the token;
4. When it does, enter your PIN and then click the **green** button with the √ mark on the pinpad;
5. You will then be logged on.

[1] For the installation of the GINA, refer to the installation guide. It will be not installed by default. If you want to install the GINA, you will need to select it during installation.
[2] Note that the G&D CashMouse is identical to SCM STR 391.
[3] Omnikey CardMan 3610, 3620, 3621 (≥ version 2.1.6) and 3821 (≥ version 2.1.6).
[4] Note that the Omnikey CardMan 3821 Trust does have a display.

4.4.1.3 Reiner SCT Cyberjack pinpad (Class 2)

The Reiner SCT Cyberjack pinpad does not have a display. This means that although the SafeSign Identity Client GINA will instruct you '*when prompted, please enter your PIN on the protected PIN entry pad of your smart card reader*', the nature of this prompt is defined by the smart card reader.

1. At the Windows Logon prompt, "*Insert card or press Ctrl+Alt-Delete to begin*", insert your token in the Reiner reader;
2. The SafeSign Identity Client GINA for secure pinpad readers will be displayed (see Figure 57 above);
3. Wait until one of the LEDs starts blinking **orange** to enter your PIN for the token;
4. When it does, enter your PIN and then click the **green** **OK** button on the pinpad;
5. You will then be logged on.

SafeSign Identity Client GINA not installed

When the SafeSign Identity Client GINA is not installed (i.e. during SafeSign Identity Client installation, you did not select the GINA), the Windows Logon prompt to enter the PIN will be displayed, instead of the SafeSign Identity Client GINA dialog for secure pinpad readers (Figure 57).

In order to log on with your secure pinpad reader, you can click **OK** or press **Enter** to have the secure pinpad reader prompt you for the PIN of your SafeSign Identity Client Token (i.e. step 3 above).

4.4.2 SafeSign Identity Client Bio

When you have SafeSign Identity Client Bio installed, the same applies with regard to the use of a secure pinpad reader (i.e. you should enter the PIN on the keypad of the secure pinpad reader) as described in paragraph 4.4.1. Moreover, the *Authentication* dialog will be displayed, showing a picture of the secure pinpad you are using.

As SafeSign Identity Client Bio supports biometrics (i.e. you can initialise you token with a multi-factor profile, to use a combination of PIN and / or finger(s) with particular tokens), you can also log on with your fingerprint (in combination with one of the biometric sensors supported). The *Authentication* dialog will be displayed, showing a picture of the biometric sensor you are using and asking you to place your finger(s) on the sensor to authenticate.

For more information on the different authentication scenarios, please refer to the *SafeSign Identity Client User Guide for Authentication*.

4.5 Require Smart Card to Logon

Since the use of a username and password is inherently weaker than the use of a token with a PIN (two-factor authentication), it could be advisable to force a user to logon to the domain with a token and PIN instead of a username and password. When this is enforced, a particular user can only log on with a token and PIN and not with a username and password anymore. This security feature can only be configured on a per-user basis.

Please note that when activating this policy for (domain) administrators, it can only be undone after logging on to the Windows 2003 server with the same smart card or with another smart card that contains a correct certificate for the domain administrator.

To configure a user in Active Directory in such a way that this user can only log on to the domain with a token, go to **Start > Settings > Control Panel > Active Directory Users and Computers**:

Figure 58: Active Directory Users and Computers

In the **Active Directory Users and Computers** console, go to **[your domain name] > Users**:

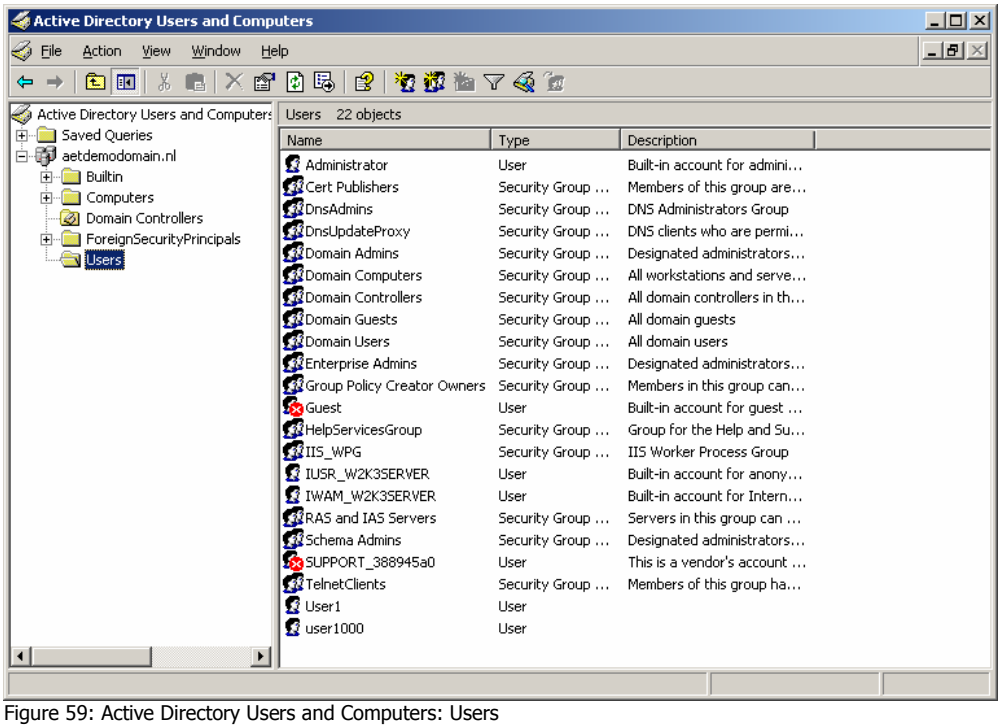


Figure 59: Active Directory Users and Computers: Users

➔ In the right pane, find and double-click the user you wish to configure the 'require smart card to logon' policy for.

This will open the *Properties* dialog for the user:

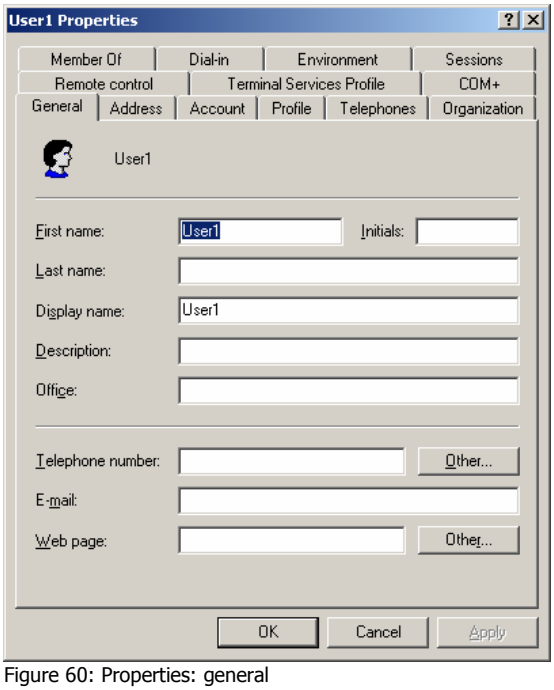


Figure 60: Properties: general

➔ Open the **Account** tab

In the **Account** tab, select the option **Smart card is required for interactive logon**:

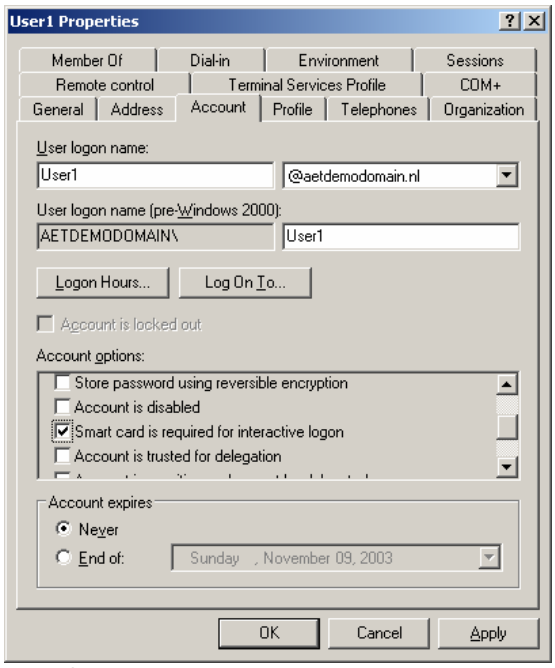


Figure 61: Properties: Account

➔ Click **OK**

The user can now only use a token for interactive logon.

4.6 Troubleshooting Windows 2000 Logon

Logon Message	Possible Cause(s)	Remedy
The card supplied requires drivers that are not present on this system. *Please try another card.*	No CSP can be found corresponding to the ATR of the inserted card.	Verify if SafeSign Identity Client is (properly) installed and if SafeSign Identity Client supports the token. Use the Token Management Utility / Token Administration Utility to check if the token is recognized[1].
The reader cannot communicate with the smart card, due to ATR configuration conflicts.	The token is not initialised.	Use the Token Management Utility / Token Administration Utility to initialize the (blank) token.
Your credentials could not be read from the smart card. Verify the card is valid, and that it is seated properly in the reader.	The token you inserted does not contain a Digital ID.	Use the Token Management Utility / Token Administration Utility to check if the token contains a Digital ID.
The system can not log you on. Your credentials could not be verified[2].	The token inserted does not contain a Digital ID valid for the domain you try to log on to.	Verify if the token contains a Digital ID that is suitable for the domain you try to log on to.
The system can not log you on due to the following error: The card cannot be accessed because the wrong PIN was presented.	The PIN for the token you inserted, is not correct.	Use the Token Management Utility / Token Administration Utility to check the status of the PIN. Token > Show Token Objects will show the status of the PIN. Enter the correct PIN.
The system cannot log you on due toe the following error: an internal error has been detected, but the source is unknown.	The PIN for the token you inserted in the pinpad reader is not correct.	Use the Token Management Utility / Token Administration Utility to check the status of the PIN. Token > Show Token Objects will show the status of the PIN. Enter the correct PIN.
The system can not you log on due to the following error: The card cannot be accessed because the maximum number of PIN entry attempts has been reached.	The PIN for the token you inserted, is locked.	Use the Token Management Utility to check the status of the PIN. Token > Show Token Objects will show the status of the PIN. Unlock the PIN.
The system can not log you on due to the following error: A certificate chain processed correctly, but terminated in a root certificate which is not trusted by the trust provider.	The root certificate for the Digital ID presented cannot be verified.	Verify if the root certificate is available and registered in the Trusted Root Certificate Authorities certificate store. Obtain the root certificate (chain).

[1] Note that it is possible that although a token is properly recognised in the Token Management Utility / Token Administration Utility on one machine (and the smart card logon / user certificate present and registered), trying to log on with the token may fail with this error on another machine. This is most likely caused by the fact that you are using a "new" Java card that has not been added to the particular machine you are logging on to. Although the card will be recognised on other machines (i.e. its details and contents can be viewed in the Token Utility), the logon will fail, because the ATR is different from that in the registry. In this case, the Token Utility may report that the card has an unknown ATR (which you can send to AET). Refer to the Token Administration Guide for more details and how to do this.

[2] This is a generic error message and may have various causes (such as the domain controller has no domain controller certificate, the smart card contains an untrusted certificate, invalid CRL).

4.7 Troubleshooting Windows XP Logon

Logon Message	Possible Cause	Remedy
The card supplied requires drivers that are not present on this system. *Please try another card.*	No CSP can be found corresponding to the ATR of the inserted card.	Verify if SafeSign Identity Client is (properly) installed and if SafeSign Identity Client supports the token. Use the Token Management Utility / Token Administration Utility to check if the token is recognized.
The system could not log you on. The requested keyset does not exist on the smart card.	The token is not initialised. The token does not contain a Digital ID.	Use the Token Management Utility / Token Administration Utility to initialize the (blank) token. Use the Token Management Utility / Token Administration Utility to check if the token contains a Digital ID.
The system could not log you on. The smartcard certificate used for authentication was not trusted.	Revocation checking has failed[1]. The token inserted does not contain a Digital ID valid for log on purposes.	Verify if the token contains a Digital ID that is suitable for Windows logon.
The system cannot log you on due to the following error: The parameter is incorrect.	The token inserted does not contain a Digital ID valid for the domain you try to log on to.	Verify if the token contains a Digital ID that is suitable for the domain you try to log on to.
The system could not log you on. An incorrect PIN was presented to the smartcard.	The PIN for the token you inserted, is not correct.	Use the Token Management Utility / Token Administration Utility to check the status of the PIN. Token > Show Token Objects will show the status of the PIN. Enter the correct PIN.
The system could not you log on. The smartcard is blocked[2].	The PIN for the token you inserted, is locked.	Use the Token Management Utility / Token Administration Utility to check the status of the PIN. Token > Show Token Objects will show the status of the PIN. Unlock the PIN.
The system could not log you on. Your credentials could not be verified.	The root certificate for the Digital ID presented cannot be verified.	Verify if the root certificate is available and registered in the Trusted Root Certificate Authorities certificate store. Obtain the root certificate (chain).

[1] Failing to find and download the Certificate Revocation List (CRL), an invalid CRL, a revoked certificate, and a revocation status of "unknown" are all considered revocation failures.
[2] The SafeSign 'Token is locked" dialog will also appear".

Smart card logon errors

Also refer to:

Knowledge Base article 'Guidelines for Enabling Smart Card Logon with Third-Party Certification Authorities':
http://support.microsoft.com/default.aspx?scid=kb;en-us;281245

Checklist 'Deploying smart cards for logging on to Windows':
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/17a1f58e-b176-4389-ab45-6aa3a314b5ef.mspx

Or search for 'smart card logon' on the http://www.microsoft.com web site.

Index of Notes