HID

15370 Barranca Parkway
Irvine, CA 92618
USA

CRESCENDO™

# Microsoft® Windows Server 2003

# Integration Guide

## 47A3-905, A.1

### C200 and C700

December 1, 2008

# Contents

**About this Guide** .... **3**

Purpose .... 3

Audience .... 3

Conventions .... 3

References .... 3

Contacts .... 4

**1 Windows 2003 Security Features** .... **5**

**2 Microsoft Certificate Services** .... **6**

2.1 Prerequisites .... 6

2.2 Installing Certificate Services .... 6

2.3 Configuring the Microsoft CA .... 15

2.4 Creating a Microsoft CA Enrollment station .... 18

**3 Enrolling a smart card user** .... **25**

3.1 ActiveX error message during certificate requests .... 31

3.2 Troubleshooting smart card enrollment .... 34

**4 Secure Logon** .... **40**

4.1 Select Digital ID .... 41

4.2 Smart Card Removal Behavior .... 42

4.3 Require Smart Card to Logon .... 49

4.4 Troubleshooting Windows XP Logon .... 51

# About this Guide

**THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY.**

**HID GLOBAL 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 HID GLOBAL BE LIABLE, WHETHER IN CONTRACT, TORT OR OTHERWISE FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING FROM USE OF INFORMATION CONTAINED IN THIS DOCUMENT.**

**Windows is a registered trademark of Microsoft Corporation in the United States and other countries.**

## Purpose

In order to set up your HID Crescendo card with Microsoft Windows® secure log-on, follow the instructions in the manual, which describe such activities as obtaining a smart card user / logon certificate.

This manual assumes you have installed SafeSign Identity Client and have a Crescendo C200 or C700 card.

Not all activities described in this manual can be performed by a user. For example, to set up Certificate Services you need to log on as administrator of the domain and have administrator rights.

Setting up Microsoft® Certificate Services is meant as guidance only. HID Global cannot be held liable for any malfunctioning from configuring Microsoft Certificate Services.

## Audience

This manual is specifically designed for users of Microsoft Windows® Server 2003, who wish to use their HID Crescendo™ C200 or C700 card to obtain strong authentication in their Microsoft® environment

## Conventions

The following outlines conventions used in this guide.

- Every activity has a number of steps, indicated by numbers.
- Each step requiring an action is indicated by a "➪".
- Special notes of consideration are repesented by a "ⓘ".

## References

Microsoft also provides information about how to enable your Domain server for smart card logon.

- For general information on deploying a smart card program, see: The Smart Card Deployment Cookbook
- For specific information on installing and configuring the PKI with the Microsoft Certificate Authority, see: Deploying the PKI
- For information on how to enroll users and deploy smart cards, see: Deploying Smart Cards

# Contacts

### North America

15370 Barranca Parkway
Irvine, CA 92618
USA

| | |
|---|---|
| Phone: | 800-237-7769 |
| Support: | 866-607-7339 |
| Fax: | 949-732-2120 |
| Email: | tech@hidglobal.com |

### Asia Pacific

19/F 625 King's Road
NorthPoint, Island East
Hong Kong

| | |
|---|---|
| Phone: | 852 3160 9800 |
| Support: | 852 3160 9833 |
| Fax: | 852 3160 4809 |
| Email: | asiasupport@hidglobal.com |

### Europe, Middle East and Africa

Phoenix Road
Haverhill, Suffolk CB9 7AE
England

| | |
|---|---|
| Phone: | +44 (0) 1440 714 850 |
| Support: | +44 (0) 1440 711 822 |
| Fax: | +44 (0) 1440 714 840 |
| Email: | eusupport@hidglobal.com |

# 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 service that allows businesses to act as their own CA and issue and manage digital certificates;
- **Active Directoy**, 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. Refer to the application User Guide for how to use your Internet (mail) application for secure e-mail and web access.

This manual describes how to obtain a certificate and how to log on to Windows 2000, Windows XP and Windows 2003 with your HID Crescendo smart card.

In order to use your HID Crescendo card 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 describes how to set up Microsoft Certificate Services.

Chapter 3 describes how to enroll a smart card user.

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

**Note:** 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

# 2 Microsoft Certificate Services

This setion describes how to install and set up Microsoft Windows 2003 Certificate Services, comprising the following aspects:

- Installing Certificate Services: section 2.2
- Configuring the Windows CA: section 2.3
- Creating a Microsoft CA RA station: section 2.4

## 2.1 Prerequisites

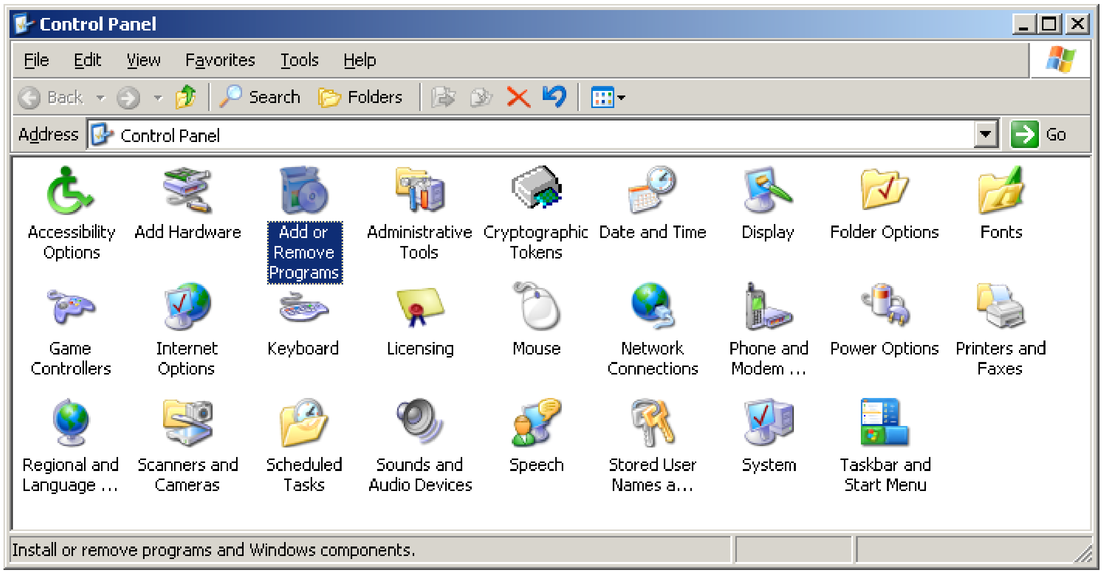
This manual assumes that you have the following components installed, before setting up Microsoft Windows 2003 Certificate Services

- 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 Enrollment 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.

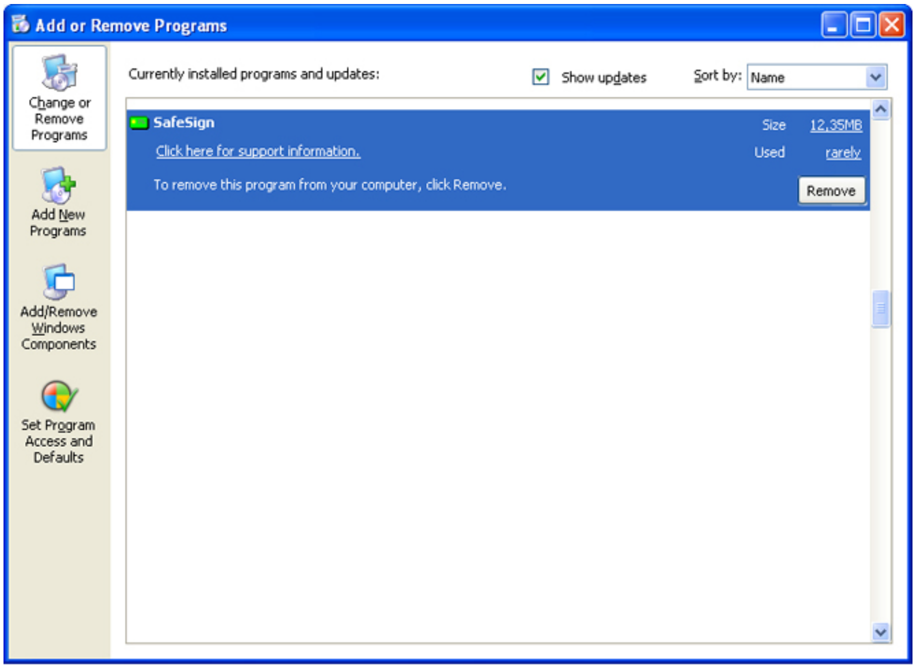


Install or remove programs and Windows components.

**Figure 1: Control Panel: Add/Remove Programs**

⇨ Double-click **Add or Remove Programs**

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


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
Remove

Currently installed programs and updates:

☑ Show updates

Sort by: Name

SafeSign

Size 12.35MB

Click here for support information.

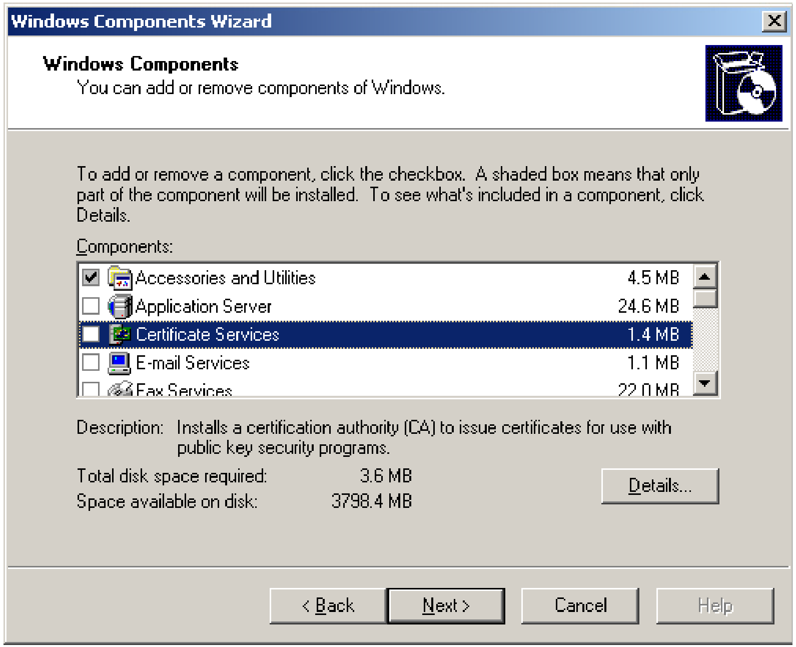
Used rarely

To remove this program from your computer, click Remove.

Figure 2: Windows 2003: Add or Remove Programs

⇨ Click **Add/Remove Windows Components**:

3. The Windows Components Wizard opens:



Windows Components Wizard

**Windows Components**

You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

| | |
|---|---|
| ☑ Accessories and Utilities | 4.5 MB |
| □ Application Server | 24.6 MB |
| □ Certificate Services | 1.4 MB |
| □ E-mail Services | 1.1 MB |
| □ Fax Services | 22.0 MB |

Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.

Total disk space required: 3.6 MB

Space available on disk: 3798.4 MB

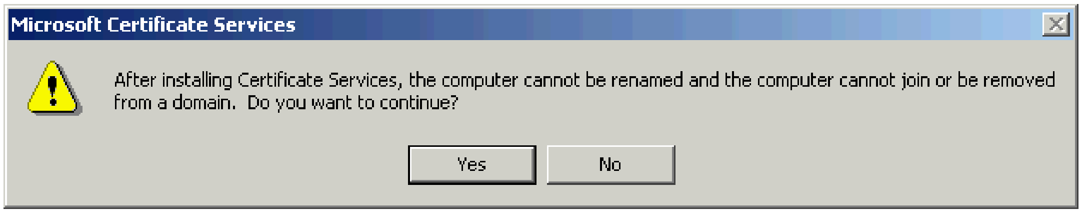
Figure 3: Windows Components Wizard: Windows Components

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

As the **Application Server** and **Certificate Services** checkboxes are not checked, these components are not yet installed.

- ➩ Check the **Application Server** checkbox
- ➩ Check the **Certificate Services** checkbox

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



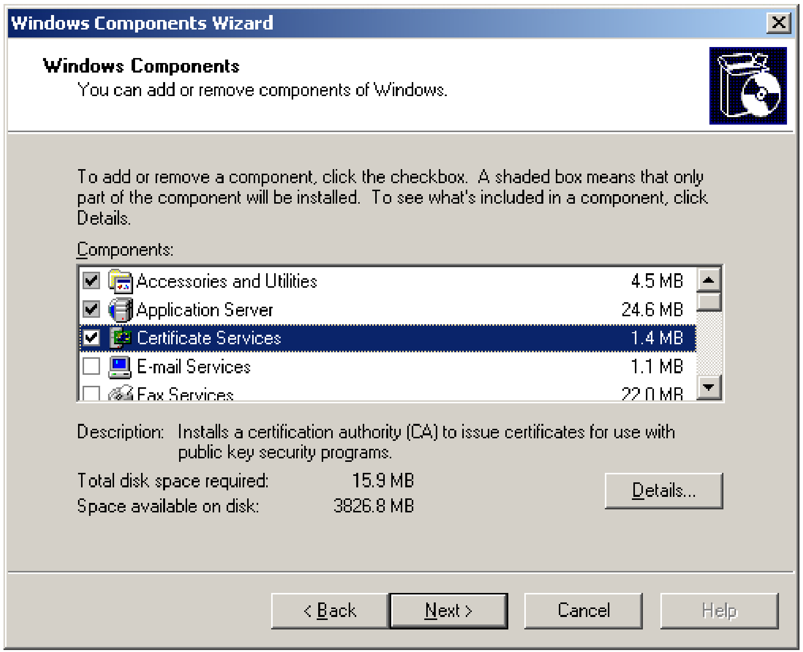
Microsoft Certificate Services

After installing Certificate Services, the computer cannot be renamed and the computer cannot join or be removed from a domain. Do you want to continue?

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

- ➩ Click **Yes** to continue

5. Upon clicking **Yes**, the Windows Components dialog displays again, now with Application Server and Certificate Services selected:



**Windows Components**

You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

| | | |
|---|---|---|
| ☑ | Accessories and Utilities | 4.5 MB |
| ☑ | Application Server | 24.6 MB |
| ☑ | Certificate Services | 1.4 MB |
| □ | E-mail Services | 1.1 MB |
| □ | Fax Services | 22.0 MB |

Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.

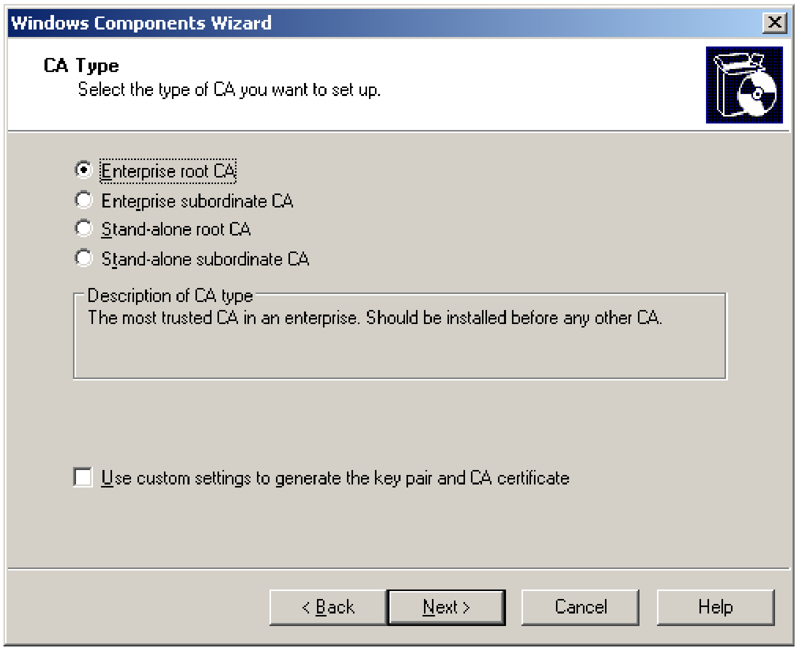
Total disk space required: 15.9 MB

Space available on disk: 3826.8 MB

**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 inquires about the Certification Authority settings:



Windows Components Wizard

CA Type
Select the type of CA you want to set up.

● Enterprise root CA
○ Enterprise subordinate CA
○ Stand-alone root CA
○ Stand-alone subordinate CA

Description of CA type
The most trusted CA in an enterprise. Should be installed before any other CA.

□ Use custom settings to generate the key pair and CA certificate

**Figure 6: Windows Components Wizard: CA Type**

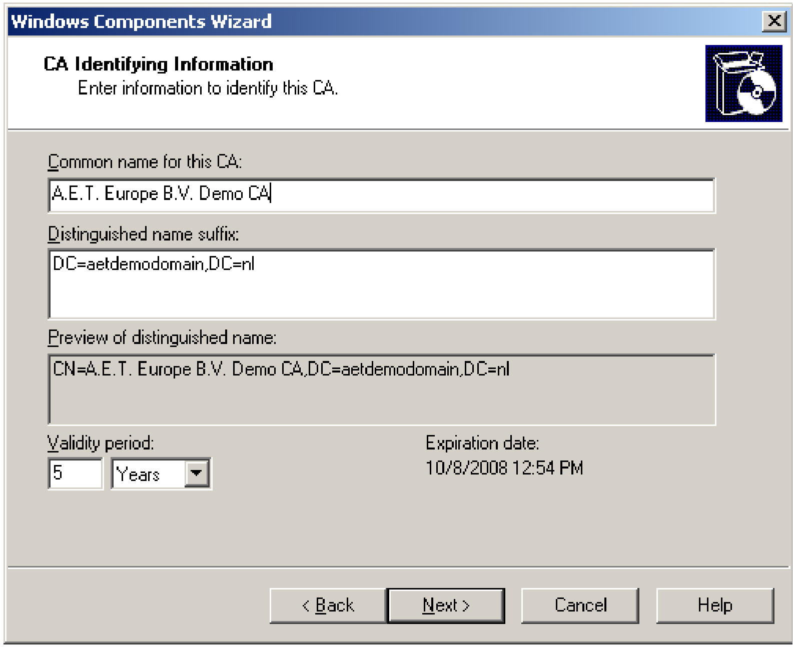
The Enterprise root CA is the most trusted CA in an enterprise and should be installed before any other CA. If this option is not available, you may not have installed or properly configured Active Directory, as this Certification Authority type requires Active Directory.

**Note:** Do not check: ‘Use custom settings to generate the key pair and CA certificate’. Although you may be able to select a smart card CSP in these settings, it is not possible to generate key pair and CA certificate on a smart card. This is functionality that smart card CSPs 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 organization 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:



Windows Components Wizard

**CA Identifying Information**

Enter information to identify this CA.

Common name for this CA: A.E.T. Europe B.V. Demo CA

Distinguished name suffix: DC=aetdemodomain,DC=nl

Preview of distinguished name: CN=A.E.T. Europe B.V. Demo CA,DC=aetdemodomain,DC=nl

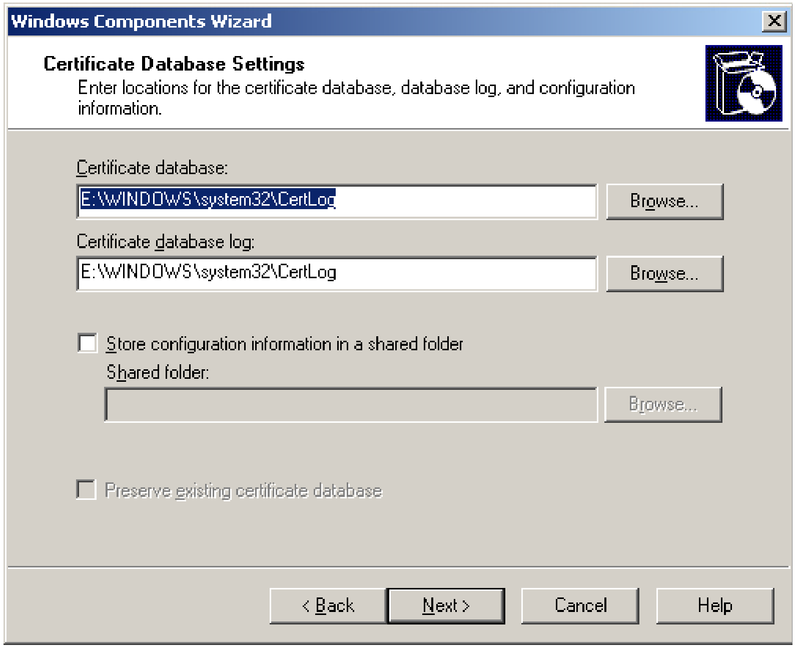
Validity period: 5 Years

Expiration date: 10/8/2008 12:54 PM

**Figure 7: Windows Components Wizard: CA Identifying Information**

- ➪ Enter a common name for the CA you are about to create (this automatically completes the other dialog fields)

8. Upon clicking **Next**, the Certificate Database Settings dialog opens:



Windows Components Wizard

Certificate Database Settings
Enter locations for the certificate database, database log, and configuration information.

Certificate database: E:\WINDOWS\system32\CertLog

Certificate database log: E:\WINDOWS\system32\CertLog

□ Store configuration information in a shared folder

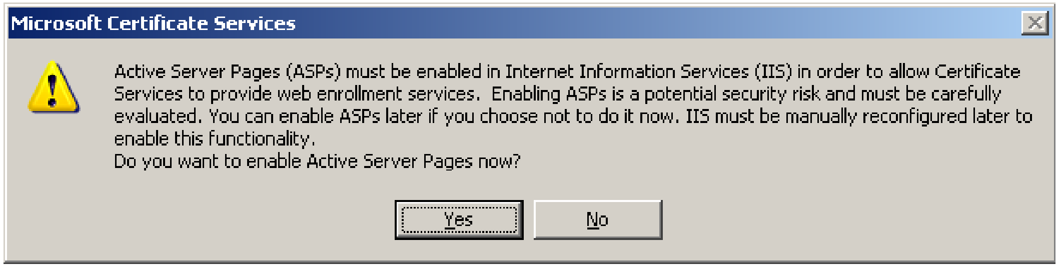
Shared folder:

□ Preserve existing certificate database

**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 to enable Active Server Pages now:



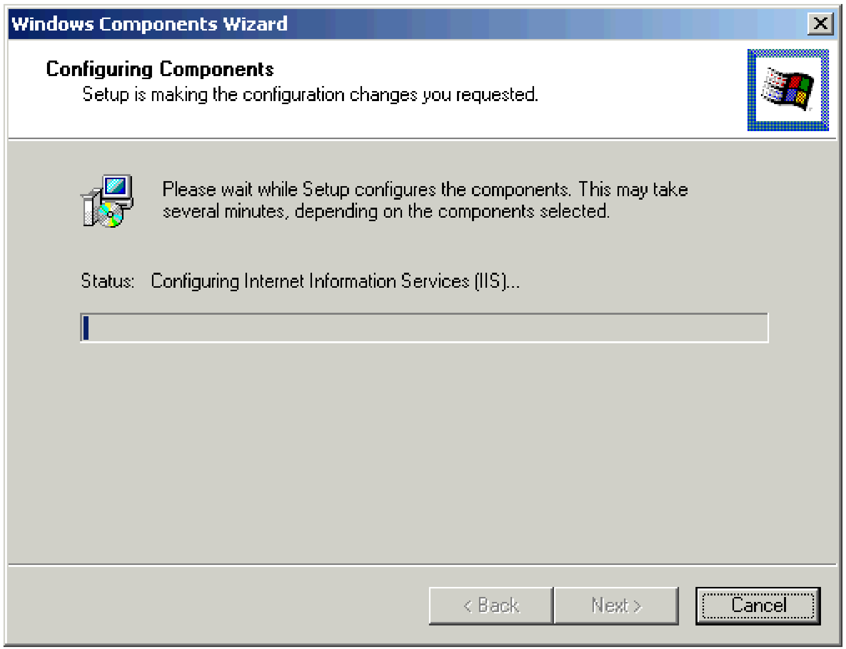
Microsoft Certificate Services

Active Server Pages (ASPs) must be enabled in Internet Information Services (IIS) in order to allow Certificate Services to provide web enrollment services. Enabling ASPs is a potential security risk and must be carefully evaluated. You can enable ASPs later if you choose not to do it now. IIS must be manually reconfigured later to enable this functionality.
Do 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 informs you that the setup is making the requested configuration changes:



Windows Components Wizard

**Configuring Components**

Setup is making the configuration changes you requested.

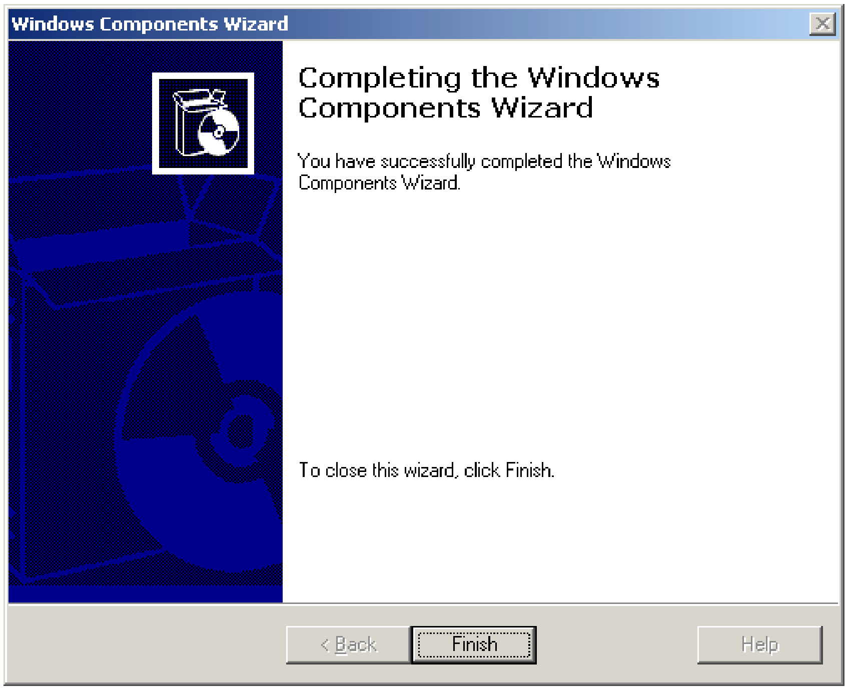
Please wait while Setup configures the components. This may take several minutes, depending on the components selected.

Status: Configuring Internet Information Services (IIS)...

**Figure 10: Windows Components Wizard: Configuring Components**

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

11. When setup is finished, the Windows Components Wizard completes:



Windows Components Wizard

Completing the Windows Components Wizard

You have successfully completed the Windows Components Wizard.

To close this wizard, click Finish.

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

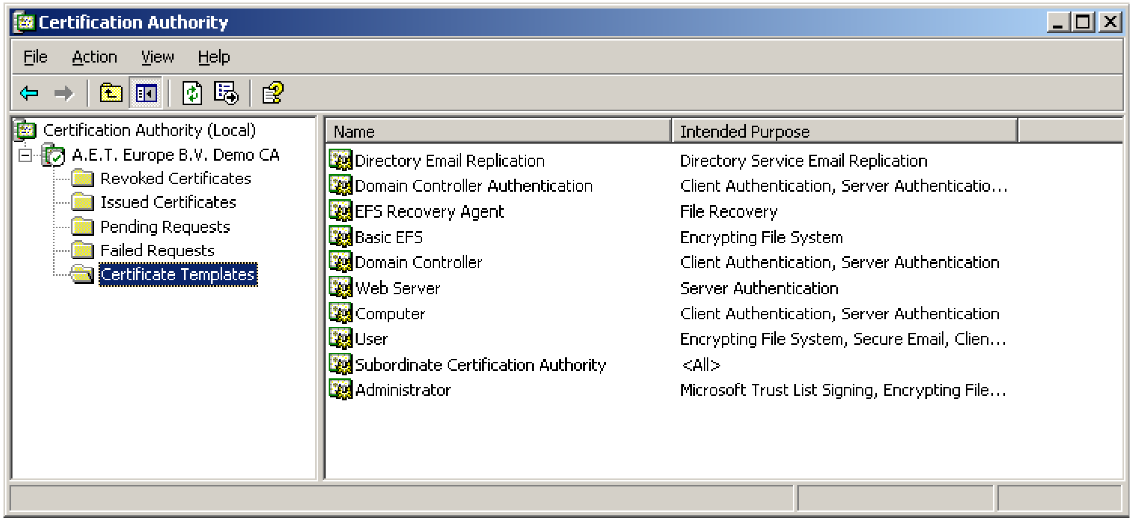
⇨ Click **Finish**

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

## 2.3 Configuring the Microsoft CA

To enable the Microsoft CA to issue your domain smart card certificates, continue with configuration.

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:

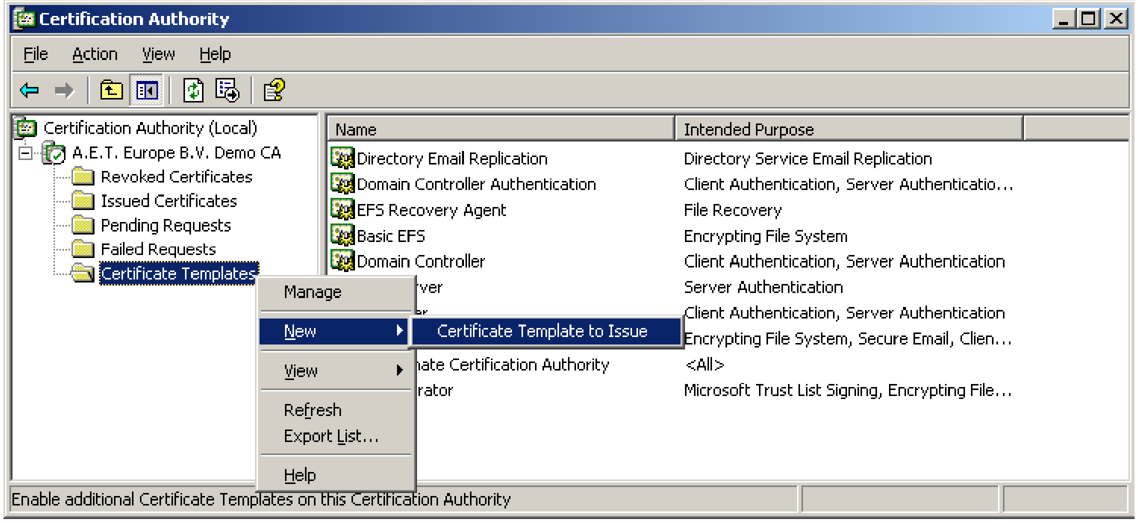


| Name | Intended Purpose |
|---|---|
| Directory Email Replication | Directory Service Email Replication |
| Domain Controller Authentication | Client Authentication, Server Authenticatio... |
| EFS Recovery Agent | File Recovery |
| Basic EFS | Encrypting File System |
| Domain Controller | Client Authentication, Server Authentication |
| Web Server | Server Authentication |
| Computer | Client Authentication, Server Authentication |
| User | Encrypting File System, Secure Email, Clien... |
| Subordinate Certification Authority | <All> |
| Administrator | Microsoft Trust List Signing, Encrypting File... |

**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, update the list of available certificate templates.

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

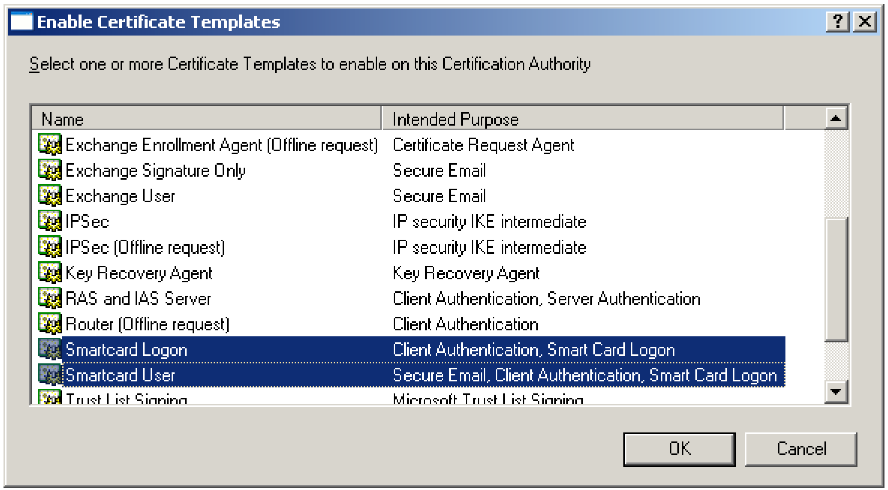


| Name | Intended Purpose |
|---|---|
| Directory Email Replication | Directory Service Email Replication |
| Domain Controller Authentication | Client Authentication, Server Authenticatio... |
| EFS Recovery Agent | File Recovery |
| Basic EFS | Encrypting File System |
| Domain Controller | Client Authentication, Server Authentication |
| ver | Server Authentication |
| r | Client Authentication, Server Authentication |
|  | Encrypting File System, Secure Email, Clien... |
| ate Certification Authority | <All> |
| rator | Microsoft Trust List Signing, Encrypting File... |

Enable additional Certificate Templates on this Certification Authority

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

This opens the Enable Certificate Templates dialog:



Enable Certificate Templates

Select one or more Certificate Templates to enable on this Certification Authority

| Name | Intended Purpose |
|---|---|
| Exchange Enrollment Agent (Offline request) | Certificate Request Agent |
| Exchange Signature Only | Secure Email |
| Exchange User | Secure Email |
| IPSec | IP security IKE intermediate |
| IPSec (Offline request) | IP security IKE intermediate |
| Key Recovery Agent | Key Recovery Agent |
| RAS and IAS Server | Client Authentication, Server Authentication |
| Router (Offline request) | Client Authentication |
| Smartcard Logon | Client Authentication, Smart Card Logon |
| Smartcard User | Secure Email, Client Authentication, Smart Card Logon |
| Trust List Signing | Microsoft Trust List Signing |

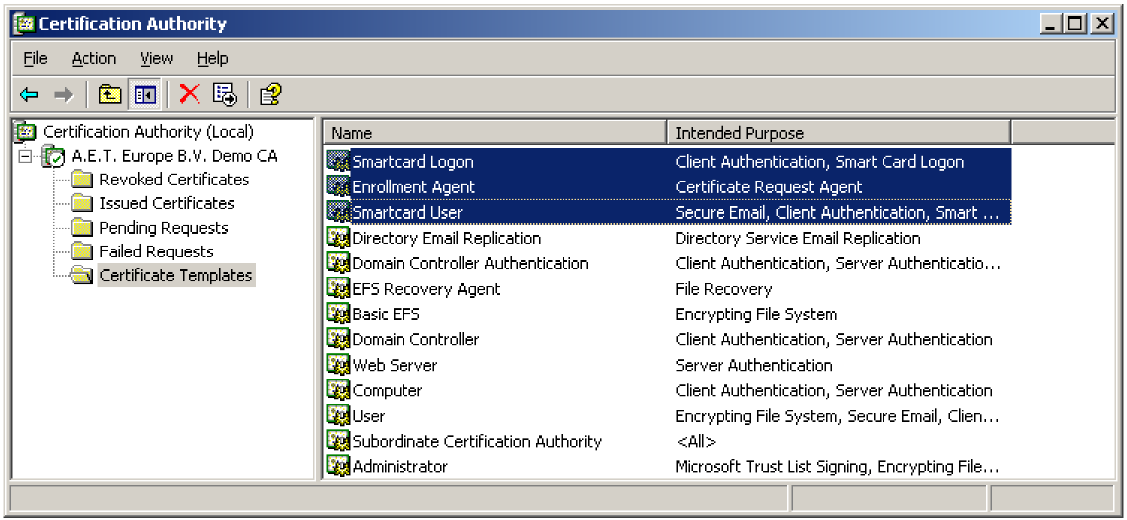
**Figure 14: Enable Certificate Templates**

To allow for your Microsoft CA to issue certificates for smart card logon onto the domain, 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 enroll certificates for other entities than itself. For example, when an administrator wants to deploy smart card logon certificates for the employees in an organization, they would require an ‘Enrollment Agent’ certificate.

⇨ Select all of the above-mentioned certificate templates, click **OK**.

2. All the necessary certificate templates are now included in the list, enabling the personalization of a smart card with a smart card logon / user certificate:



Certification Authority (Local)
- A.E.T. Europe B.V. Demo CA
  - Revoked Certificates
  - Issued Certificates
  - Pending Requests
  - Failed Requests
  - Certificate Templates

| Name | Intended Purpose |
|---|---|
| Smartcard Logon | Client Authentication, Smart Card Logon |
| Enrollment Agent | Certificate Request Agent |
| Smartcard User | Secure Email, Client Authentication, Smart ... |
| Directory Email Replication | Directory Service Email Replication |
| Domain Controller Authentication | Client Authentication, Server Authenticatio... |
| EFS Recovery Agent | File Recovery |
| Basic EFS | Encrypting File System |
| Domain Controller | Client Authentication, Server Authentication |
| Web Server | Server Authentication |
| Computer | Client Authentication, Server Authentication |
| User | Encrypting File System, Secure Email, Clien... |
| Subordinate Certification Authority | <All> |
| Administrator | Microsoft Trust List Signing, Encrypting File... |

**Figure 15: Certification Authority: Certificate Templates added**

⇨ Close the Certification Authority window

ⓘ **To use HID Crescendo smart cards, ensure that the correct drivers are installed on both the server that issues the certificates and the client computers. To use Crescendo C200 cards, perform the following two steps:**

A. Install the Microsoft Base Smart Card Crypto Provider available at http://support.microsoft.com/kb/909520

B. Install the HID Crescendo mini-driver performing a search for ‘HID Crescendo’ at http://catalog.update.microsoft.com

For Crescendo C700, install the SafeSign middleware available from HID at http://www.hidglobal.com/crescendo.

By default, the SmartCardLogon and SmartCard User templates allow the user to select the CSP. It is possible to create your own template by duplicating one of the existing templates (for example, duplicate the Smart Card User template and then change its name and settings to use a specific CSP for HID Crescendo cards).

## 2.4 Creating a Microsoft CA Enrollment station

In some deployments, it is convenient to issue smart card certificates to entities other than yourself. For instance, an Administrator deploys smart card certificates to all employees of a company. In this scenario, the Administrator should have the ability to issue smart card certificates to all persons who must have a smart card.

For Administrators issuing smart card certificates to entities other than themselves, they set up a so-called ‘Registration Authority (RA) station’ and obtain a ‘Enrollment Agent’ certificate. There are several ways to retrieve an enrollment agent certificate, one of which is an enrollment agent certificate is requested and installed through Internet Explorer.

### 2.4.1 Create an RA Station

These are the steps to create an RA station:

1. Install the drivers for your HID Crescendo card model as described in section 2.3. on the enrollment machine

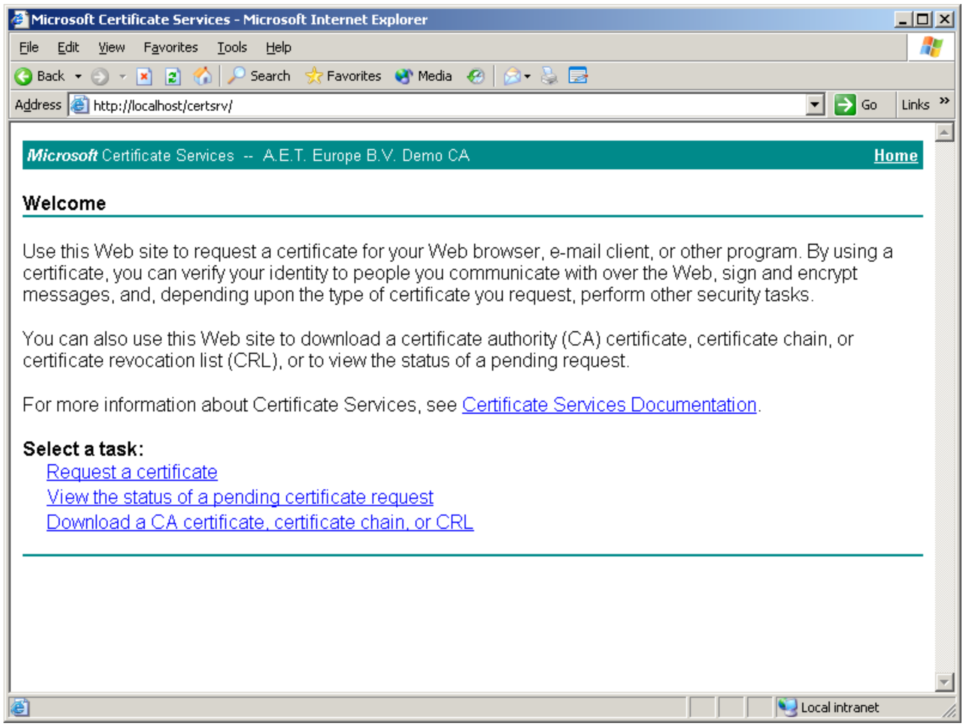
2. Install all the necessary smart card reader drivers;

3. Obtain an ‘enrollment agent’ certificate[1] (described in section 2.4.2).

[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.

### 2.4.2 Request enrollment agent certificate

1. To request and retrieve an enrollment agent certificate through Internet Explorer, start the browser and go to the Microsoft CA homepage. Find this homepage at http://<machine-name>/certsrv/:


Microsoft Certificate Services - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
http://localhost/certsrv/
Go
Links
Local intranet

*Microsoft* Certificate Services -- A.E.T. Europe B.V. Demo CA **Home**

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

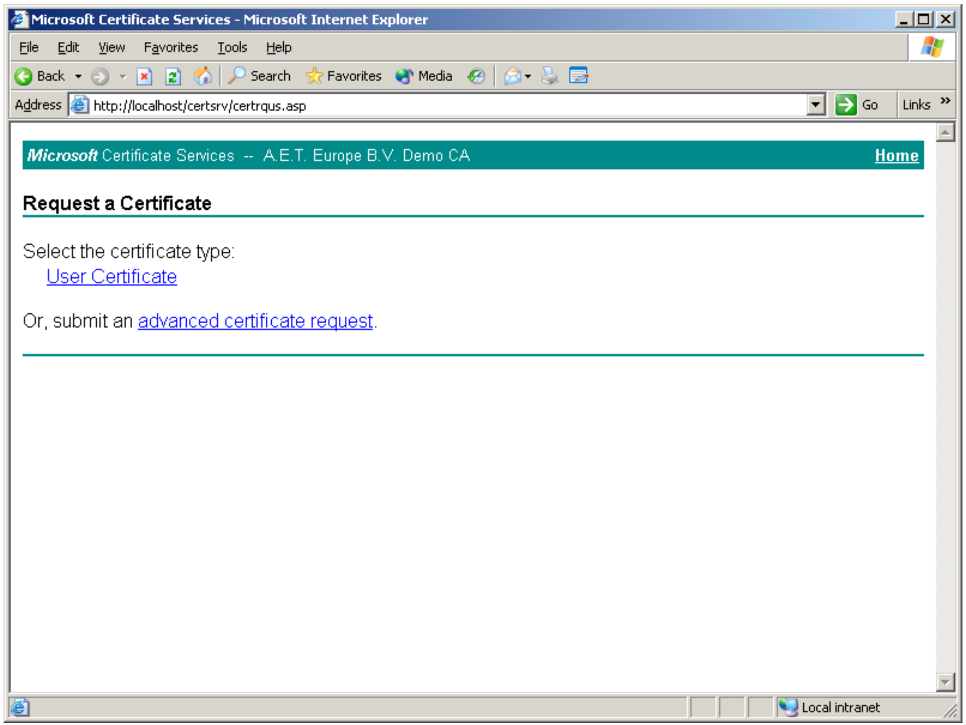
For more information about Certificate Services, see Certificate Services Documentation.

**Select a task:**
- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL

**Figure 16: Microsoft Certificate Services: Welcome**

⇨ Select **Request a certificate**

2. This opens the Request a Certificate window:


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/certsrv/certrqus.asp Go Links
Local intranet

*Microsoft* Certificate Services -- A.E.T. Europe B.V. Demo CA Home

Request a Certificate

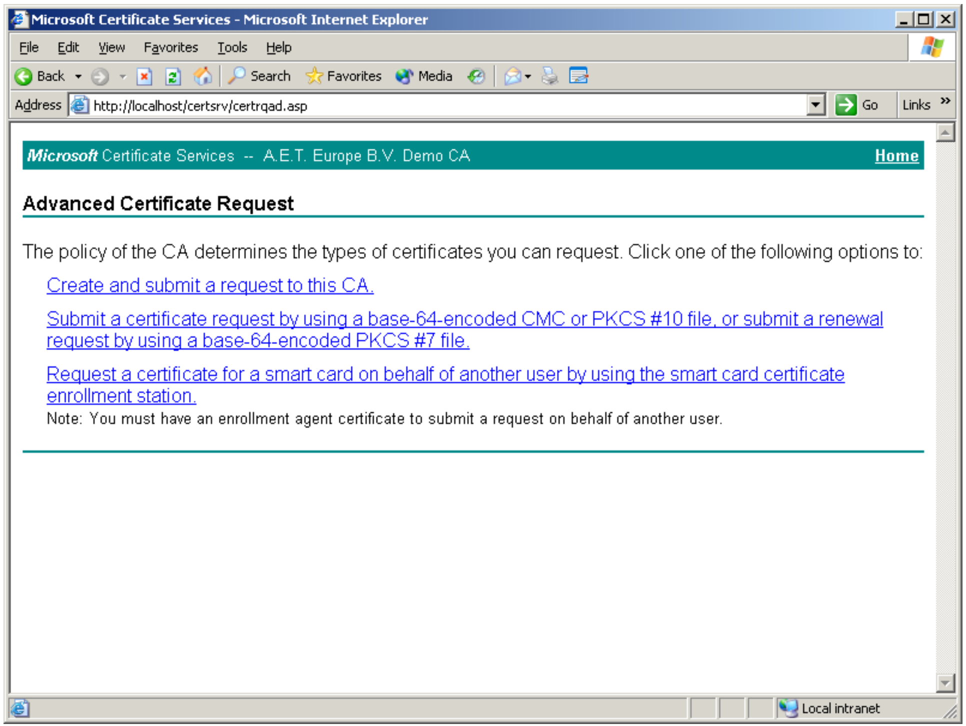
Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

Figure 17: Microsoft Certificate Services: Request a Certificate

➪ Select **advanced certificate request**

3. This opens the Advanced Certificate Request window:



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/certsrv/certrqad.asp Go Links
Microsoft Certificate Services -- A.E.T. Europe B.V. Demo CA
Home
Local intranet

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

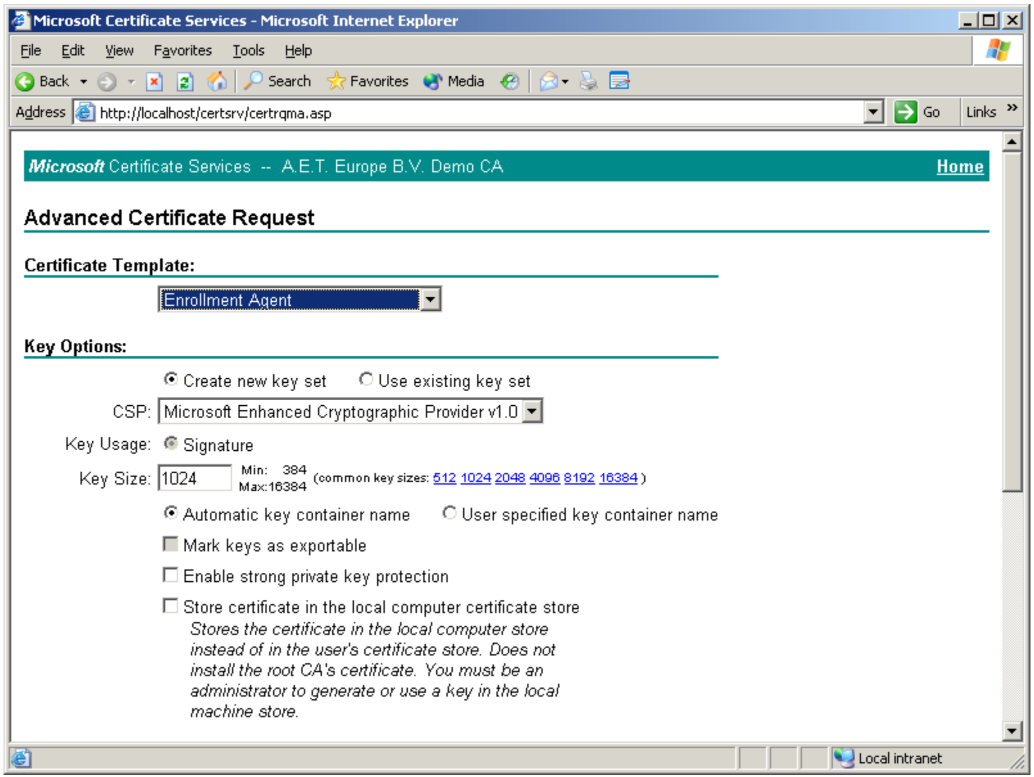
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

**Figure 18: Microsoft Certificate Services: Advanced Certificate Request**

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

4. The Advanced Certificate Request window opens:


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/certsrv/certrqma.asp
Go Links
Local intranet

*Microsoft* Certificate Services -- A.E.T. Europe B.V. Demo CA Home

Advanced Certificate Request

Certificate Template:

Enrollment Agent

Key Options:

● Create new key set ○ Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: ● Signature

Key Size: 1024 Min: 384 Max:16384 (common key sizes: 512 1024 2048 4096 8192 16384 )

● Automatic key container name ○ User specified key container name

□ Mark keys as exportable

□ Enable strong private key protection

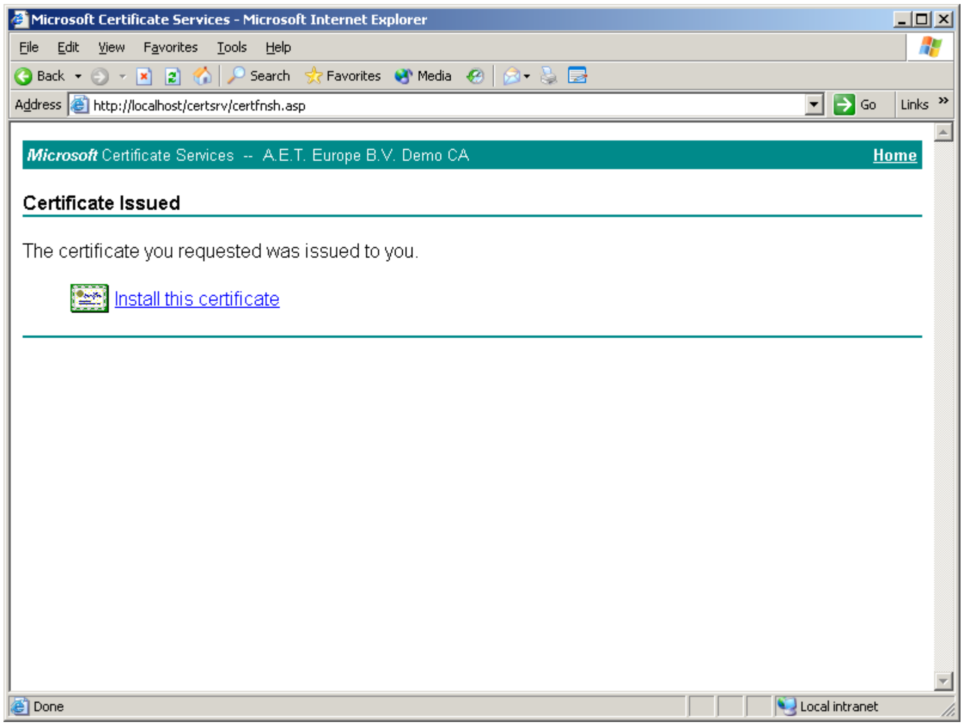
□ Store certificate in the local computer certificate store
*Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.*

**Figure 19: Microsoft Certificate Services: Advanced Certificate Requests**

From the **Certificate Template** list choose **Enrollment Agent** and ensure selecting **Microsoft Enhanced Cryptographic Provider 1.0** or similar from the CSP list under **Key Options** (as shown in Figure 19).

⇨ Click **Submit**

5. When the request is approved, the Certificate Issued window opens:


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/certsrv/certfnsh.asp
Go Links
Microsoft Certificate Services -- A.E.T. Europe B.V. Demo CA
Home
Done
Local intranet

Certificate Issued

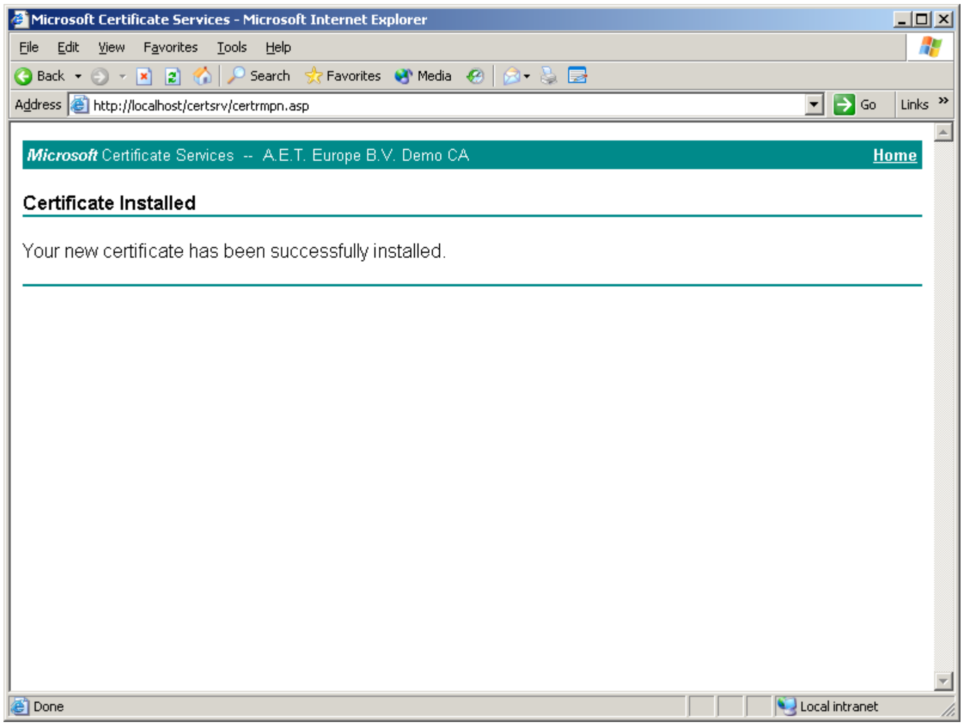
The certificate you requested was issued to you.

Install this certificate

**Figure 20: Microsoft Certificate Services: Certificate Issued**

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

6. You are informed when the certificate is successfully installed:


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/certsrv/certrmpn.asp
Go Links
Microsoft Certificate Services -- A.E.T. Europe B.V. Demo CA
Home
Done
Local intranet

Certificate Installed

Your new certificate has been successfully installed.

**Figure 21: Microsoft Certificate Services: Certificate Installed**

Now that the enrollment agent certificate is installed, issue smart card certificates on this machine and account in which you have an enrollment agent Digital ID.

# 3 Enrolling a smart card user

After creating the RA station, as described in section 2.4, you are ready to enroll smart card certificates for domain users other than yourself.

**Notes:**

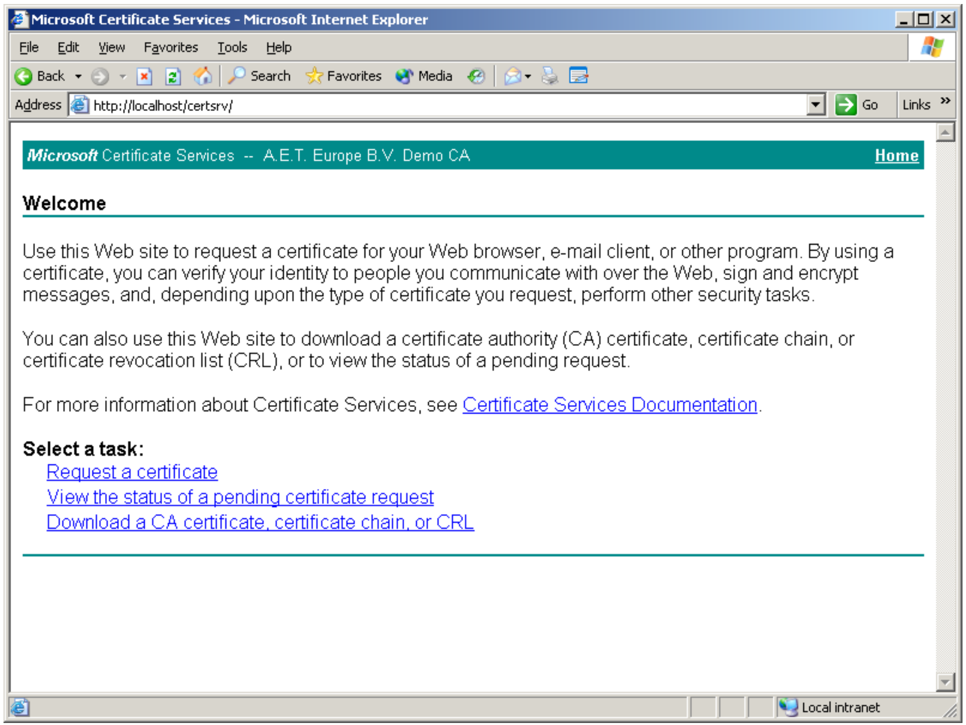
Enrollment for a smart card certificate must be a controlled procedure, in the same manner that employee badges are controlled for purposes of identification and physical access.

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, this chapter describes the process of how to enroll for a smart card user or smart card logon certificate through the Smart Card Enrollment Station. This process is likely completed  by your system administrator. As a user, request your own certificate through the Microsoft Certificate Services interface on your local workstation. 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 enrollment station 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> enter the machine name where you have installed the CA:


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/certsrv/
Go Links
Local intranet

*Microsoft* Certificate Services -- A.E.T. Europe B.V. Demo CA **Home**

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

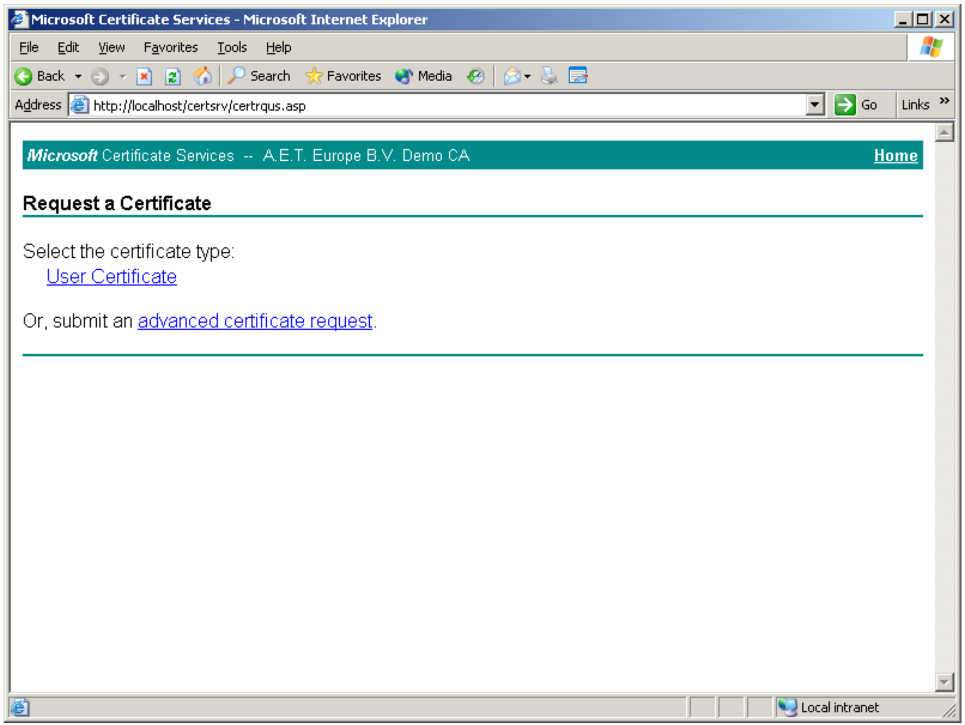
For more information about Certificate Services, see Certificate Services Documentation.

**Select a task:**
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

**Figure 22: Microsoft Certificate Services: Welcome**

⇨ Select **Request a certificate**

2. This will open the Request a Certificate window:


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/certsrv/certrqus.asp
Go Links
Local intranet

*Microsoft* Certificate Services -- A.E.T. Europe B.V. Demo CA **Home**

**Request a Certificate**

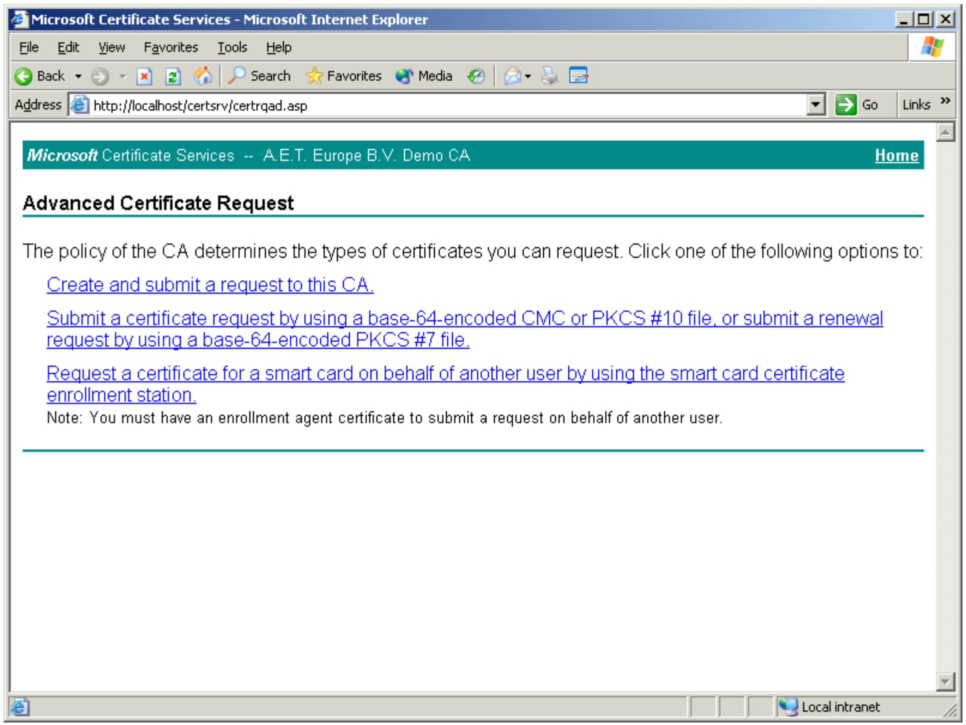
Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

**Figure 23: Microsoft Certificate Services: Request a Certificate**

➪ Select **advanced certificate request**

3. This will open the Advanced Certificate Request window:



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/certsrv/certrqad.asp
Go Links
Local intranet

*Microsoft* Certificate Services -- A.E.T. Europe B.V. Demo CA **Home**

**Advanced Certificate Request**

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

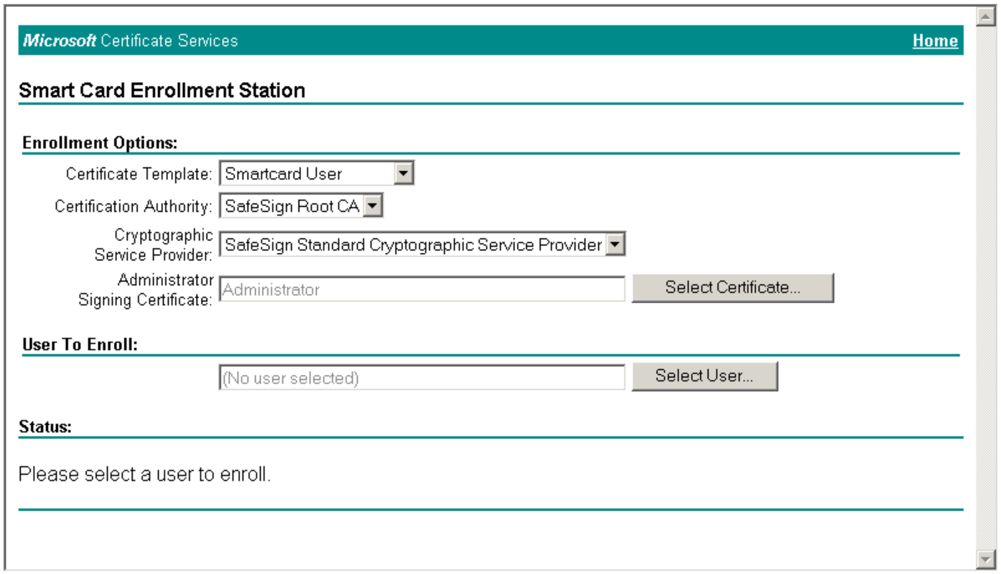
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.

Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

**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 Card Certificate Enrollment Station window opens:



*Microsoft* Certificate Services **Home**

**Smart Card Enrollment Station**

**Enrollment Options:**

Certificate Template: Smartcard User

Certification Authority: SafeSign Root CA

Cryptographic Service Provider: SafeSign Standard Cryptographic Service Provider

Administrator Signing Certificate: Administrator

**User To Enroll:**

(No user selected)

**Status:**

Please select a user to enroll.

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

**Note:** If you encounter an 'ActiveX' error upon connecting to this page, refer to section 3.1 for how to resolve this error.

Under **Enrollment Options**:

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

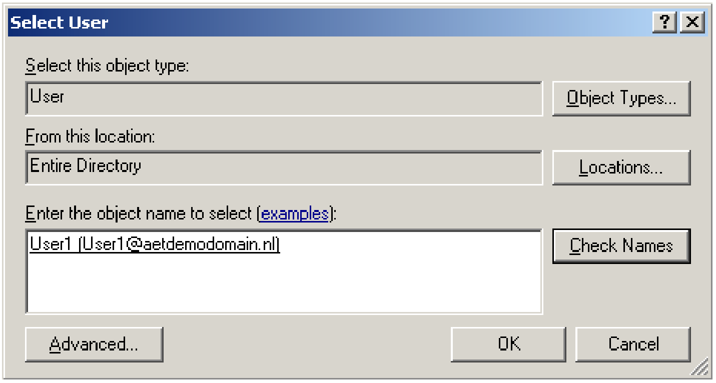
From the **Cryptographic Service Provider** drop-down list, select the CSP depending on your card model:

- For HID Crescendo C200, select Microsoft Base Smart Card Crypto Provider
- For HID Crescendo C700, select SafeSign Identity Client Standard Cryptographic Service Provider

Ensure the correct Enrollment Agent certificate is selected in the **Administrator Signing Certificate** box.

⇨ Select a **User to Enroll** by clicking the **Select User** button

5. Clicking on **Select User** opens the Select User dialog:



Select User

Select this object type:
User

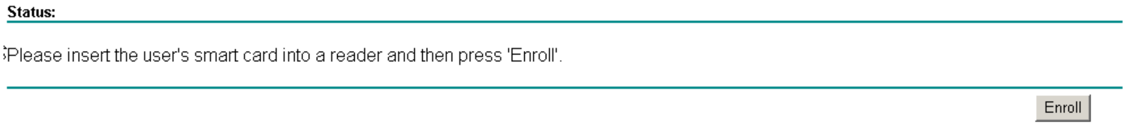
From this location:
Entire Directory

Enter the object name to select (examples):
User1 (User1@aetdemodomain.nl)

**Figure 26: Select User**

⇨ Enter the user name in which you are enrolling a certificate in the **Enter the object name to select** field. Click **Check Names** verifying the entry. If valid, the username is highlighted. After you have verified that this is the user you want to enroll a certificate, click **OK**.

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:



**Status:**

Please insert the user's smart card into a reader and then press 'Enroll'.

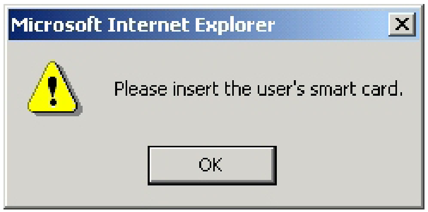
**Figure 27: Microsoft Certificate Services: Smart Card Enrollment Station: Enroll**

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

Prior to clicking **Enroll,** verify the user's token is inserted into the smart card reader.

### ⓘ No token inserted

If no smart card is in the smart card reader, a dialog requests that the smart card be inserted[2]:



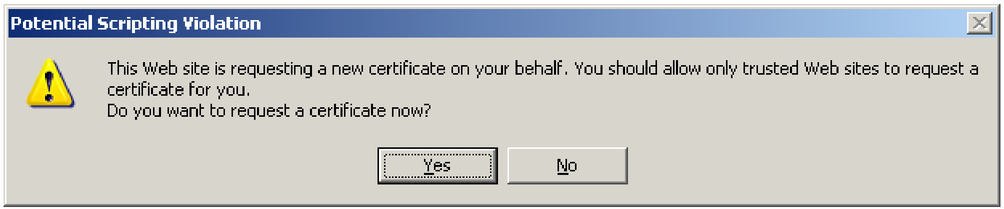
Microsoft Internet Explorer

Please insert the user's smart card.

**Figure 28: Please insert the user's smart card**

⇨ Click **OK**

7. During the enrollment process, you are prompted of a potential scripting violation:



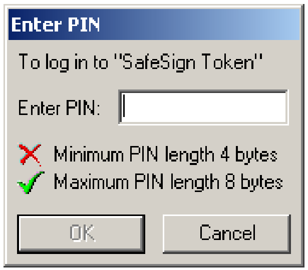
Potential Scripting Violation

This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you.
Do you want to request a certificate now?

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

⇨ Click **Yes**

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



Enter PIN

To log in to "SafeSign Token"

Enter PIN:

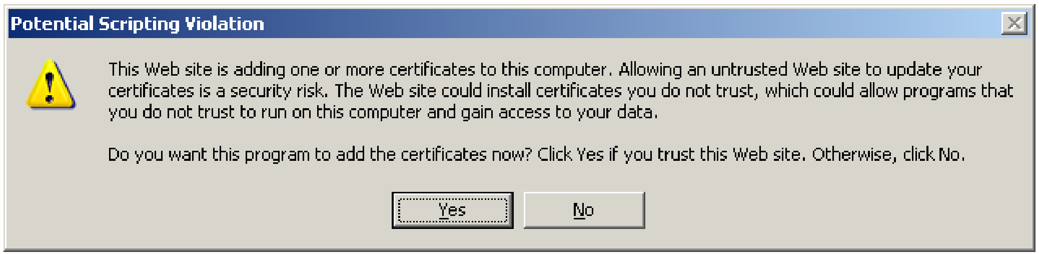
Minimum PIN length 4 bytes
Maximum PIN length 8 bytes

**Figure 30 Enter card PIN dialog**

⇨ After entering the PIN, click **OK** to continue.

[2] This dialog also appears when you have inserted a smart card that is not supported by SafeSign Identity Client.

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:



Potential Scripting Violation

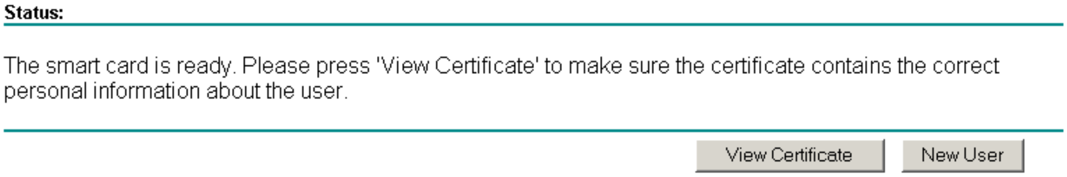
This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.

Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.

**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:



**Status:**

The smart card is ready. Please press 'View Certificate' to make sure the certificate contains the correct personal information about the user.

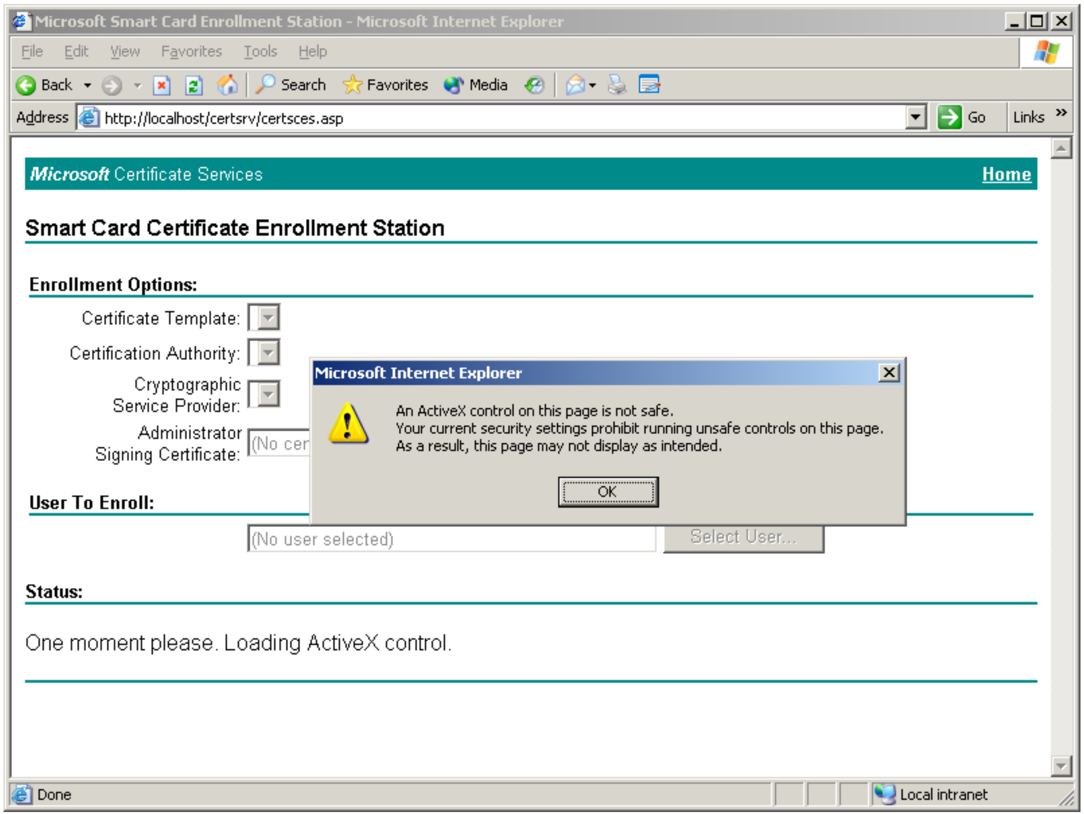
**Figure 32: Microsoft Certificate Services: Smart Card Certificate Enrollment Station: Ready**

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:


Microsoft Smart Card Enrollment Station - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
Go
Links
Microsoft Certificate Services
Home
Done
Local intranet

http://localhost/certsrv/certsces.asp

Smart Card Certificate Enrollment Station

Enrollment Options:

Certificate Template:

Certification Authority:

Cryptographic Service Provider:

Administrator Signing Certificate: (No cer

User To Enroll:

(No user selected) Select User...

Status:

One moment please. Loading ActiveX control.

Microsoft Internet Explorer

An ActiveX control on this page is not safe.
Your current security settings prohibit running unsafe controls on this page.
As a result, this page may not display as intended.

OK

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

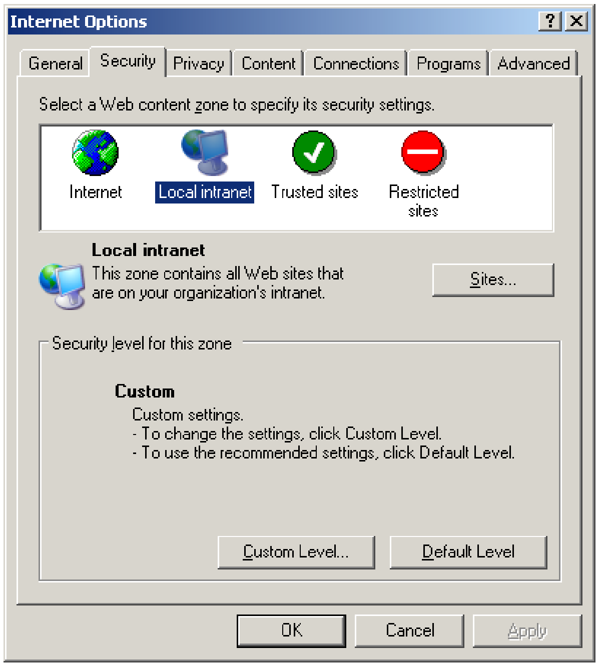
There are several ways to resolve this issue. Thus guide will describe a scenario that configures the security of the Internet Explorer browser in such a way that it will accept the ActiveX control components. This implies that you do not have to follow the scenario we describe (as this entails bringing down the security of the Internet Explorer browser). A different solution may be better suited for your situation[3]..

**Note:** 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

[3] 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 Enrollment, http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/webenroll.mspx

1. In the Internet Options dialog, select the **Security** tab and **Local intranet**:



Select a Web content zone to specify its security settings.

**Local intranet**
This zone contains all Web sites that are on your organization's intranet.

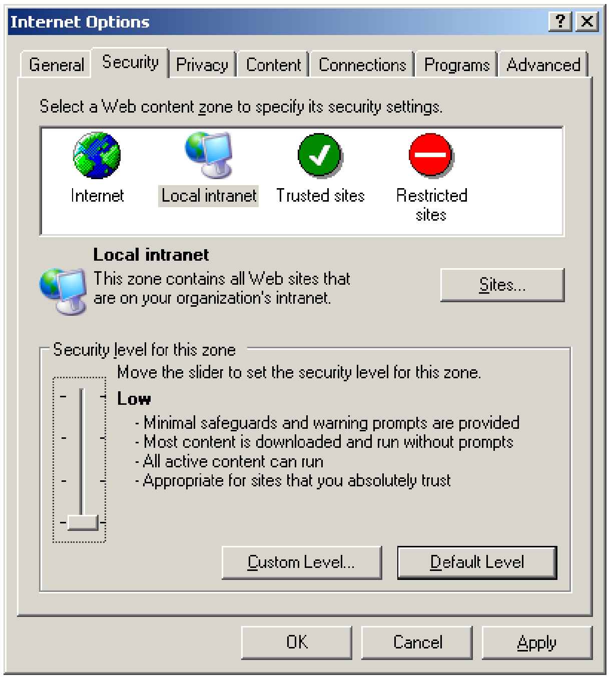
Security level for this zone

**Custom**
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

**Figure 34: Internet Options: Security Local intranet**

➪ Click **Default Level**

2. Drag the slider to **Low** decreasing the security level:



Select a Web content zone to specify its security settings.

**Local intranet**
This zone contains all Web sites that are on your organization's intranet.

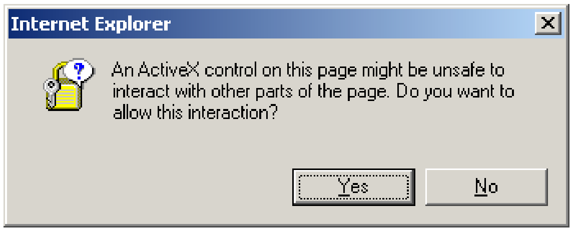
Security level for this zone
Move the slider to set the security level for this zone.

**Low**
- Minimal safeguards and warning prompts are provided
- Most content is downloaded and run without prompts
- All active content can run
- Appropriate for sites that you absolutely trust

**Figure 35: Internet Options: Security Local intranet: Low**

➪ Close this dialog by clicking **OK**

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



An ActiveX control on this page might be unsafe to interact with other parts of the page. Do you want to allow this interaction?

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

⇨ Click **Yes**

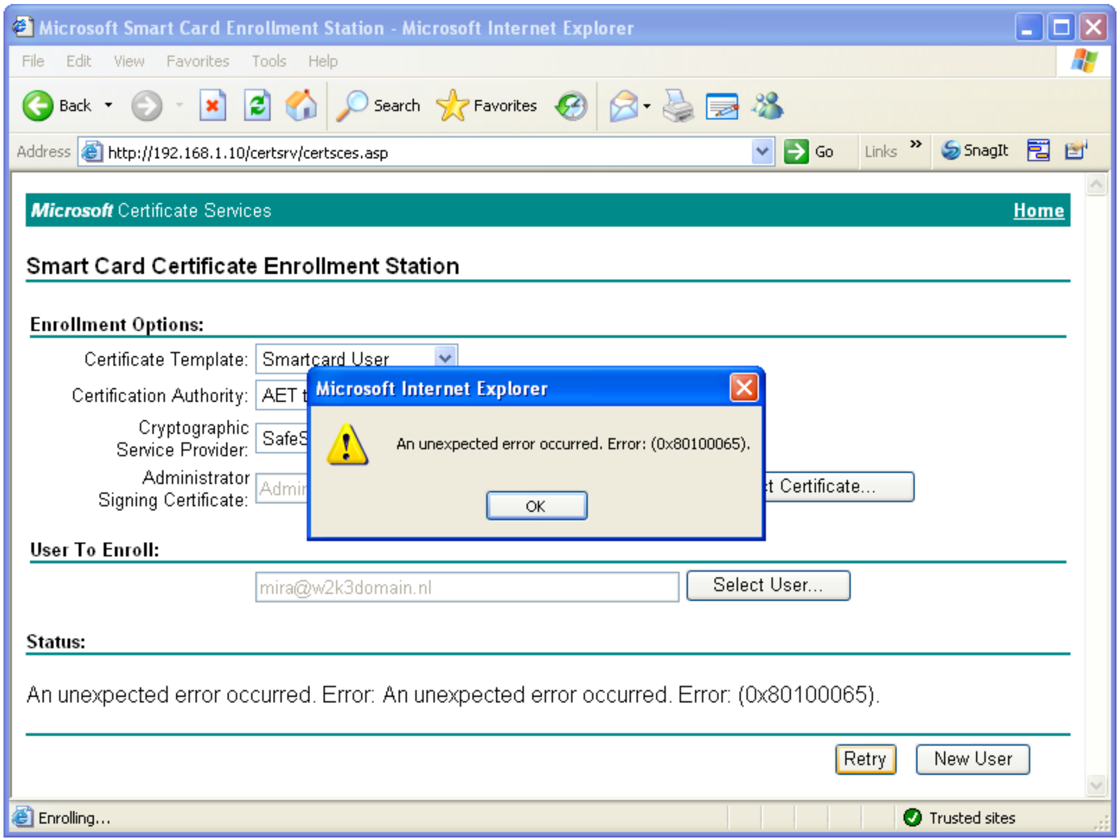
The **Smart Card Certificate Enrollment Station** page correctly displays.

## 3.2 Troubleshooting smart card enrollment

There are a number of causes for when a smart card Enrollment fails. The most common errors and their possible cause are described.

### 3.2.1 Token is blank / uninitialized

When the token is blank and is not initialized, the following error displays:



Microsoft Smart Card Enrollment Station - Microsoft Internet Explorer

Address http://192.168.1.10/certsrv/certsces.asp

Microsoft Certificate Services

Smart Card Certificate Enrollment Station

Enrollment Options:

Certificate Template: Smartcard User

Certification Authority: AET t

Cryptographic Service Provider: SafeS

Administrator Signing Certificate: Admir

User To Enroll:

mira@w2k3domain.nl

Status:

An unexpected error occurred. Error: An unexpected error occurred. Error: (0x80100065).

Microsoft Internet Explorer

An unexpected error occurred. Error: (0x80100065).

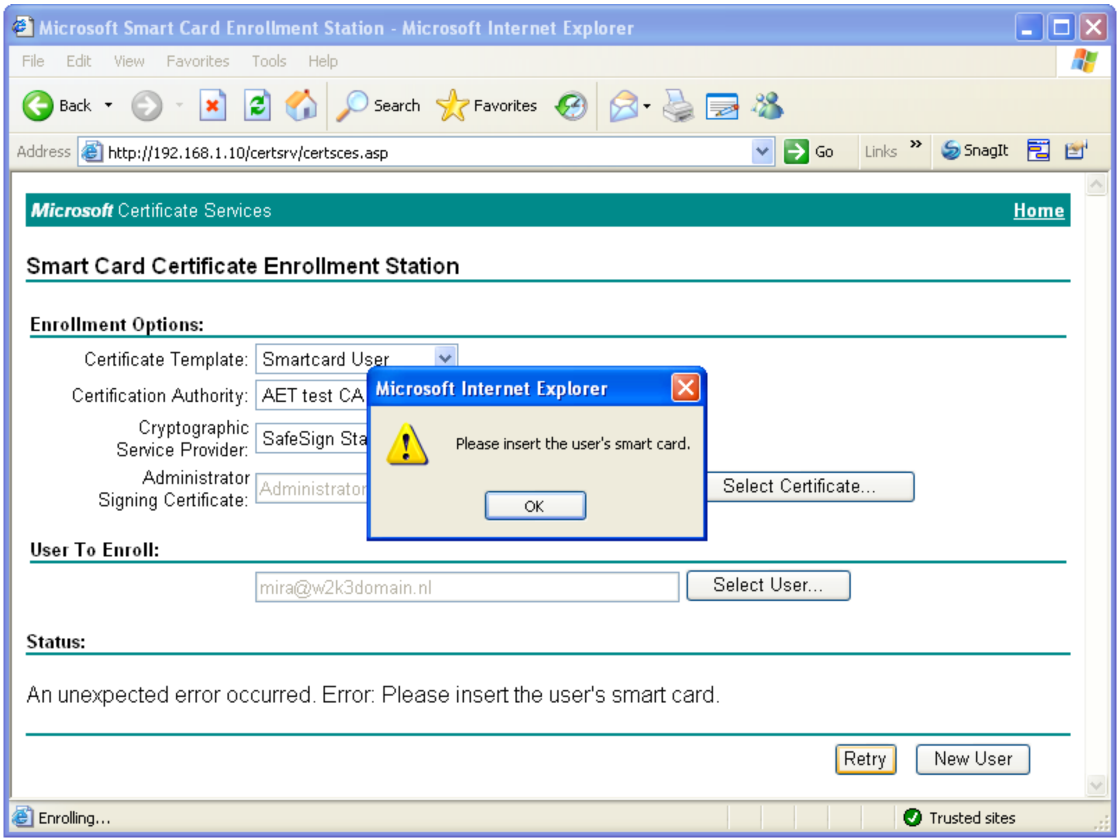
Enrolling...

**Figure 37: Smart Card Certificate Enrollment Station: Unexpected error 0x80100065**

- ➪ Check the status of the token with the Token Management Utility / Token Administration Utility. If the token is not initialized, you should initialize the token, setting a token label, PIN and PUK.

### 3.2.2 Token is unknown

When the token is not recognized, the following error displays:


Microsoft Smart Card Enrollment Station - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
SnagIt
Microsoft Certificate Services
Home

Address: http://192.168.1.10/certsrv/certsces.asp

Smart Card Certificate Enrollment Station

Enrollment Options:

Certificate Template: Smartcard User

Certification Authority: AET test CA

Cryptographic Service Provider: SafeSign Sta

Administrator Signing Certificate: Administrator

Microsoft Internet Explorer

Please insert the user's smart card.

User To Enroll:

mira@w2k3domain.nl

Status:

An unexpected error occurred. Error: Please insert the user's smart card.

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

⇨ Check the status of the token with the Token Management Utility / Token Administration Utility.

If 'Unknown token' displays, verify:

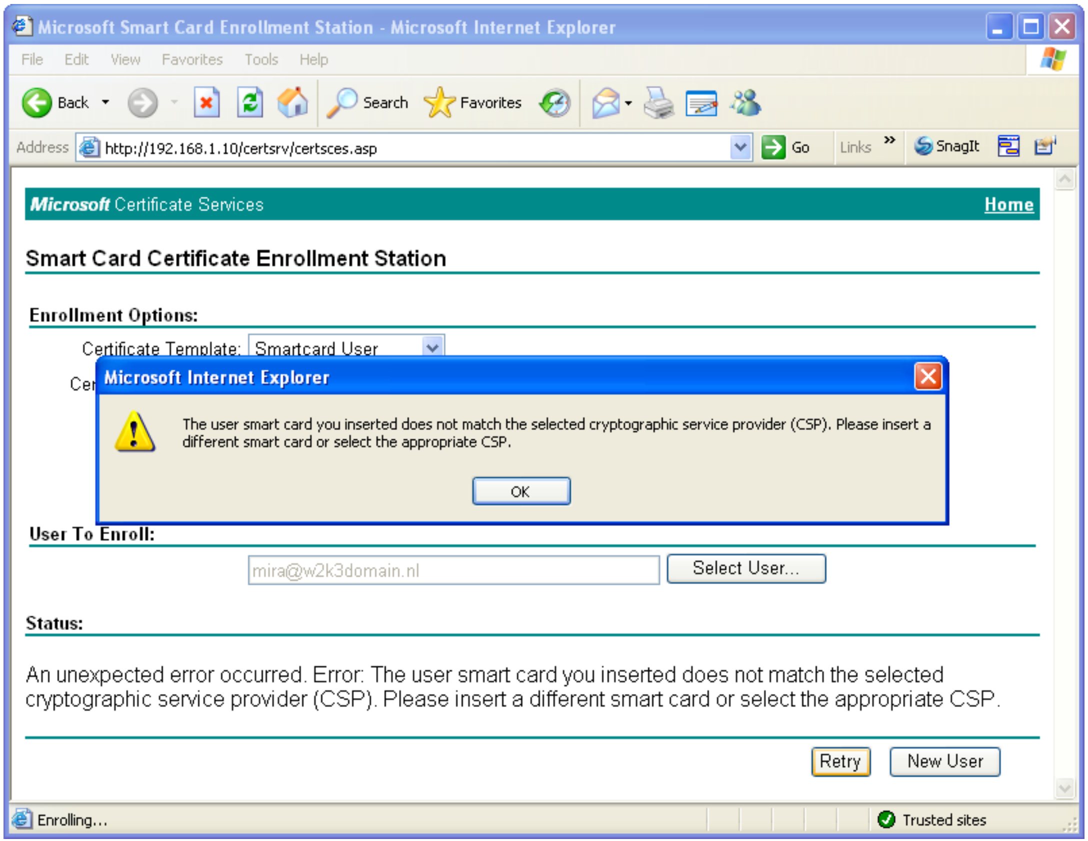
a) the token type is supported by SafeSign in the first place and

b) if the token may not be recognized yet, in which case you can use the option 'Query unknown token' to add its data to the registry.

**Note:** 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:



Address: http://192.168.1.10/certsrv/certsces.asp

Smart Card Certificate Enrollment Station

Enrollment Options:

Certificate Template: Smartcard User

The user smart card you inserted does not match the selected cryptographic service provider (CSP). Please insert a different smart card or select the appropriate CSP.

User To Enroll:

mira@w2k3domain.nl

Status:

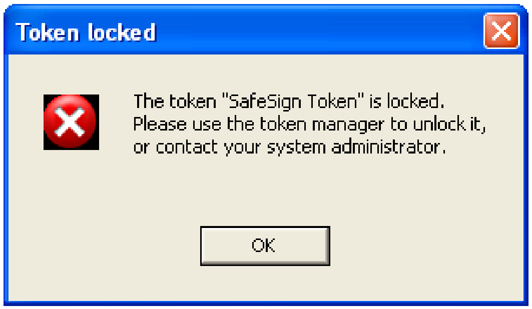
An unexpected error occurred. Error: The user smart card you inserted does not match the selected cryptographic service provider (CSP). Please insert a different smart card or select the appropriate CSP.

**Figure 39: Smart Card Certificate Enrollment Station: 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 corresponds to your card model:
- ➪ For HID Crescendo C200, select Microsoft Base Smart Card Crypto Provider
- ➪ For HID Crescendo C700, select 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:

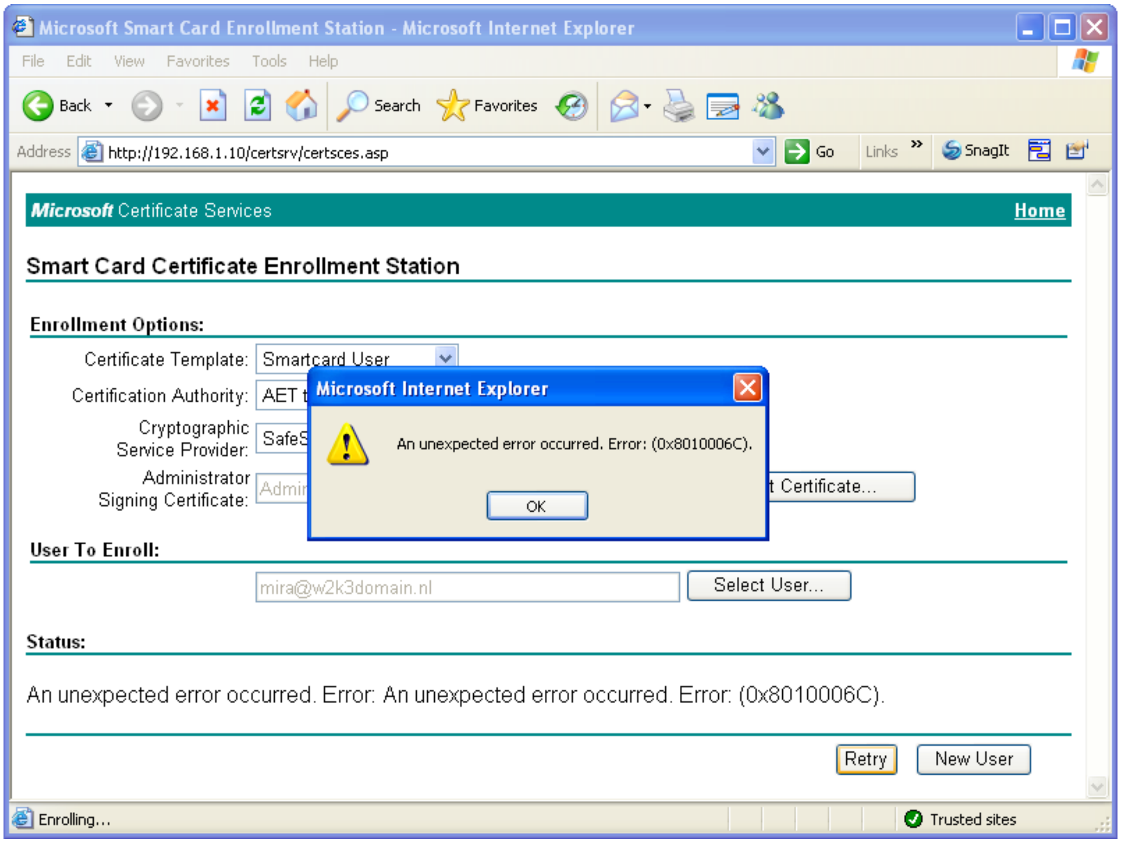


Token locked

The token "SafeSign Token" is locked.
Please use the token manager to unlock it,
or contact your system administrator.

**Figure 40: Token locked: The token is locked**

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



Microsoft Smart Card Enrollment Station - Microsoft Internet Explorer

http://192.168.1.10/certsrv/certsces.asp

Microsoft Certificate Services — Home

Smart Card Certificate Enrollment Station

Enrollment Options:

Certificate Template: Smartcard User

Certification Authority: AET t

Cryptographic Service Provider: SafeS

Administrator Signing Certificate: Admin

Microsoft Internet Explorer

An unexpected error occurred. Error: (0x8010006C).

User To Enroll:

mira@w2k3domain.nl

Status:

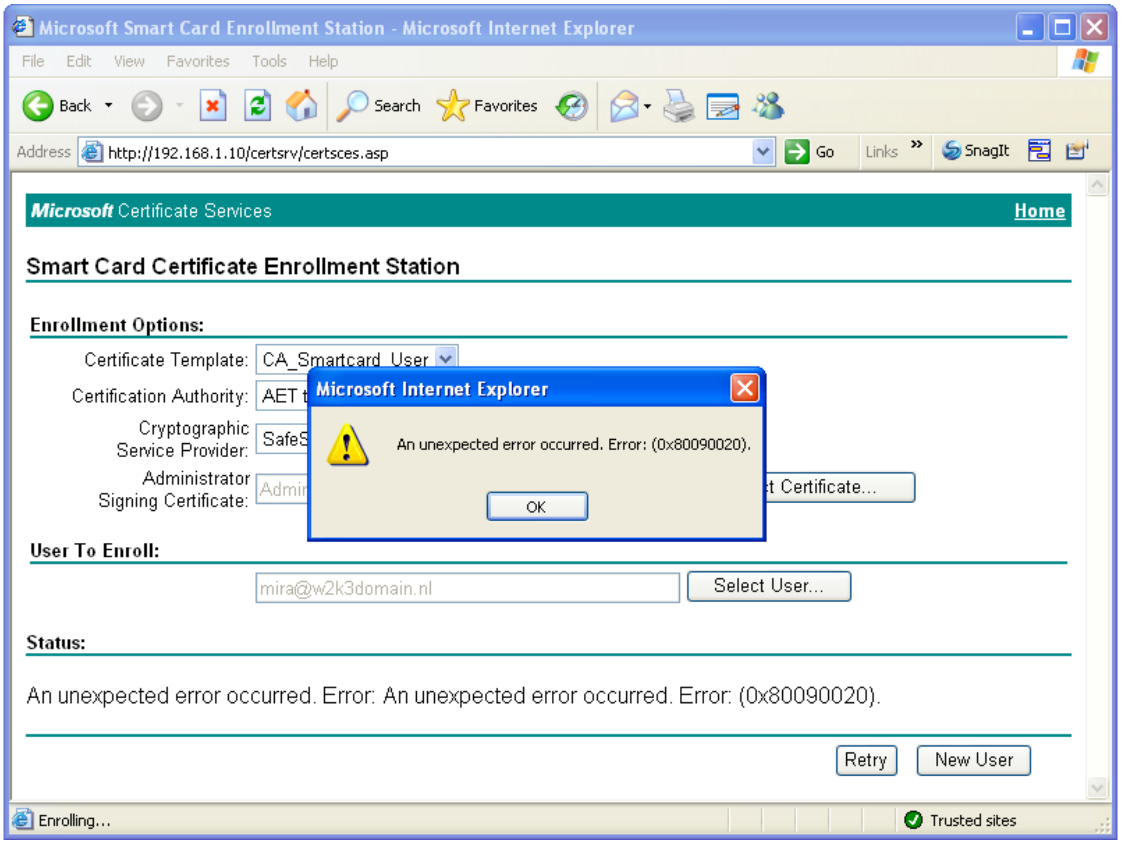
An unexpected error occurred. Error: An unexpected error occurred. Error: (0x8010006C).

**Figure 41: Smart Card Certificate Enrollment 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[4], the software will nevertheless try to generate a key pair of this size and fail. The following error may be displayed:


Microsoft Smart Card Enrollment Station - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links SnagIt
Microsoft Certificate Services
Home
Select User...
Retry
New User
Enrolling...
Trusted sites

Address: http://192.168.1.10/certsrv/certsces.asp

Smart Card Certificate Enrollment Station

Enrollment Options:

Certificate Template: CA_Smartcard_User

Certification Authority: AET t

Cryptographic Service Provider: SafeS

Administrator Signing Certificate: Admir

User To Enroll:

mira@w2k3domain.nl

Status:

An unexpected error occurred. Error: An unexpected error occurred. Error: (0x80090020).

Microsoft Internet Explorer

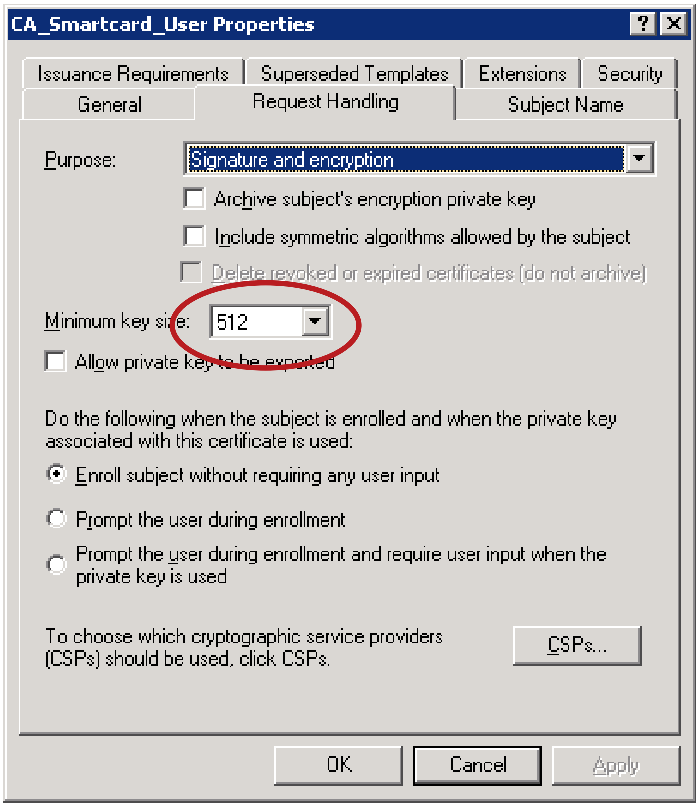
An unexpected error occurred. Error: (0x80090020).

OK

**Figure 42: Smart Card certificate Enrollment Station: Unexpected error 0x80090020**

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

Check the Certificate Template, if necessary, edit the minimum key size to 1024:



Purpose: Signature and encryption

□ Archive subject's encryption private key

□ Include symmetric algorithms allowed by the subject

□ Delete revoked or expired certificates (do not archive)

Minimum key size: 512

□ Allow private key to be exported

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

To choose which cryptographic service providers (CSPs) should be used, click CSPs. CSPs...

Figure 43: Smart Card User Template Properties: Request Handling

## 3.2.6 Enrollment rights

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

# 4 Secure Logon

You can use your HID Crescendo smart card 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 HID Crescendo smart card

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

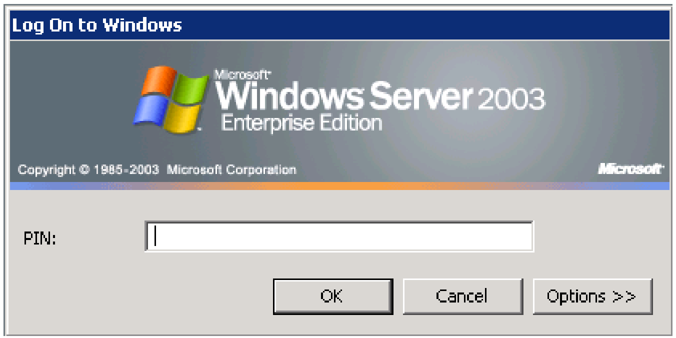

Log On to Windows
Microsoft Windows Server 2003
Enterprise Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft
PIN:
OK
Cancel
Options >>

**Figure 44: Log On to Windows: PIN**

➪ Enter the PIN of your HID Crescendo card 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 in which your computer is member.

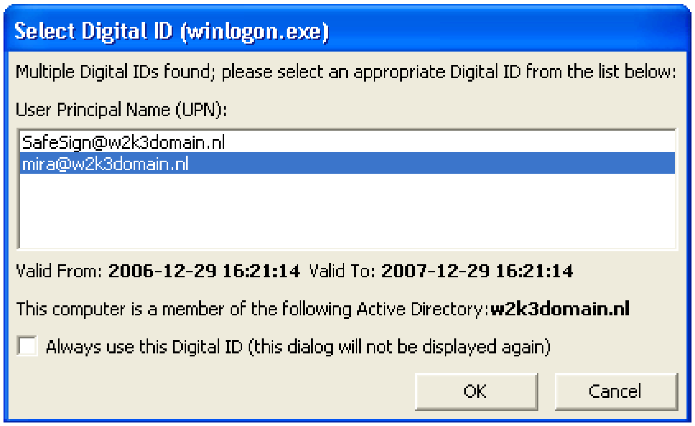
In order to perform smart card logon to a stand-alone, local (Windows 2000 or Windows XP) computer, you will need a third-party application.

## 4.1 Select Digital ID

If you are using an HID Crescendo C700 card containing more than one Digital ID suitable for smart card logon (either for the same domain or different domains), it is possible to select the Digital ID you want to use for smart card logon[5].

**Note:** To enable this dialog box, a Registry key should be modified to specify the seconds this dialog is displayed. By default, this value is zero and the dialog is not displayed. Modify the *DWORD DefaultKeyContainerSelection* value found in the key *[HKLM\Software\Microsoft\Cryptography\Defaults\Provider\SafeSign Standard Cryptographic Service Provider]* to the desired value.

When enabled, the user is prompted to select the Digital ID after entering the PIN for the token:



Select Digital ID (winlogon.exe)

Multiple Digital IDs found; please select an appropriate Digital ID from the list below:

User Principal Name (UPN):

SafeSign@w2k3domain.nl
mira@w2k3domain.nl

Valid From: **2006-12-29 16:21:14** Valid To: **2007-12-29 16:21:14**

This computer is a member of the following Active Directory:**w2k3domain.nl**

□ Always use this Digital ID (this dialog will not be displayed again)

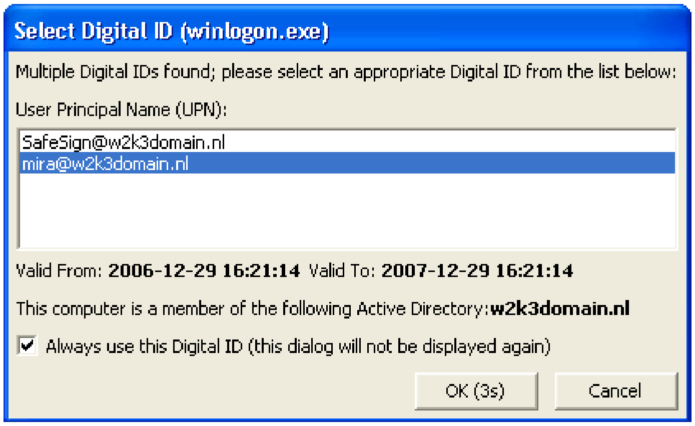
**Figure 45: Select Digital ID (winlogon.exe)**

In the example, 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 are used to logon to the same domain (called ‘w2k3domain’). Note that it is possible that the token contains two (or more) Digital IDs, suitable for smart card logon, for different domains.

Select one of the Digital IDs for logon to log on as that user.

[5] Implemented from SafeSign version 2.3.2 onwards (≥ 2.3.2).

Select ‘Always use this Digital ID’. The dialog appears at log on, and within a 5 second counter the login proceeds with the selected certificate:


Select Digital ID (winlogon.exe)

Multiple Digital IDs found; please select an appropriate Digital ID from the list below:

User Principal Name (UPN):

SafeSign@w2k3domain.nl
mira@w2k3domain.nl

Valid From: **2006-12-29 16:21:14** Valid To: **2007-12-29 16:21:14**

This computer is a member of the following Active Directory:**w2k3domain.nl**

☑ Always use this Digital ID (this dialog will not be displayed again)

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

This functionality has been included to allow users to be aware if their token contains multiple Digital IDs for log on (should they want to switch at a given time). This counter can be configured in the registry[6].

## 4.2 Smart Card Removal Behavior

For security reasons, enable smart card removal behavior. This means when a user removes their token from the smart card reader, a pre-defined policy is activated within that domain.

Smart card removal behavior is defined by a security policy. This policy determines what happens 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 Behavior

Smart card removal behavior is configured on the Domain Controller. In order to configure the smart card removal behavior for your domain, go to the **Domain Security Policy** settings. For instance, configure all computers in the domain, in addition to the Domain Controller[7].

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

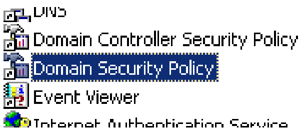
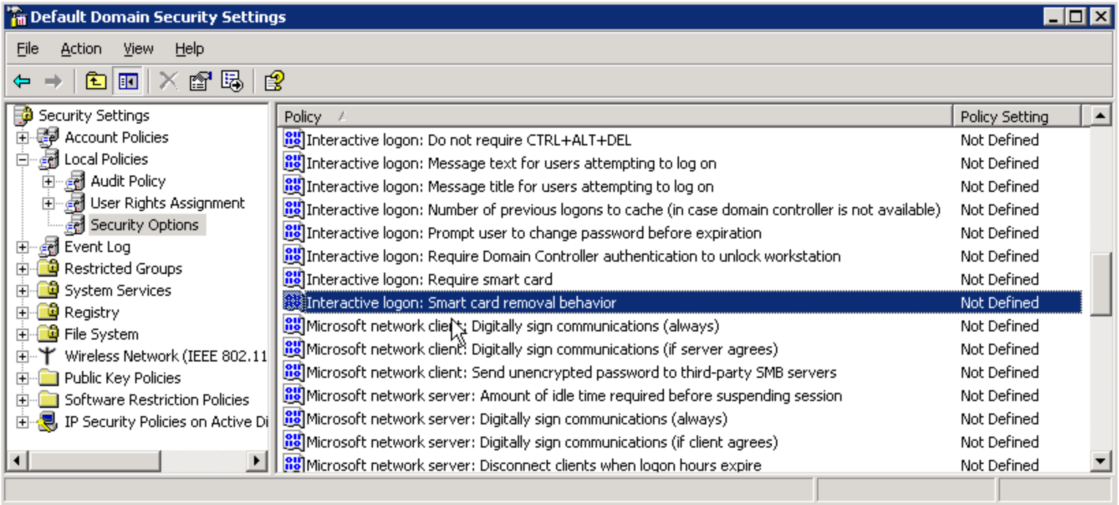

DNS
Domain Controller Security Policy
Domain Security Policy
Event Viewer
Internet Authentication Service

**Figure 47: Domain Security Policy**

[6] In order to enable and configure this functionality, you need sufficient administration rights to edit the registry.
[7] Do not confuse this with the Domain Controller Security Policy settings, where you configure the Security Policy for the Domain Controller.

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



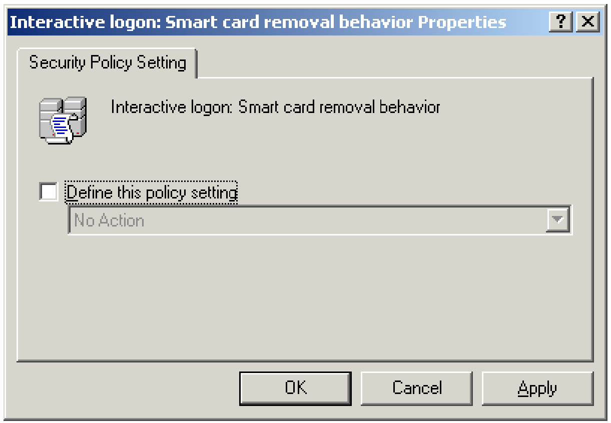
| Policy | Policy Setting |
|---|---|
| Interactive logon: Do not require CTRL+ALT+DEL | Not Defined |
| Interactive logon: Message text for users attempting to log on | Not Defined |
| Interactive logon: Message title for users attempting to log on | Not Defined |
| Interactive logon: Number of previous logons to cache (in case domain controller is not available) | Not Defined |
| Interactive logon: Prompt user to change password before expiration | Not Defined |
| Interactive logon: Require Domain Controller authentication to unlock workstation | Not Defined |
| Interactive logon: Require smart card | Not Defined |
| Interactive logon: Smart card removal behavior | Not Defined |
| Microsoft network client: Digitally sign communications (always) | Not Defined |
| Microsoft network client: Digitally sign communications (if server agrees) | Not Defined |
| Microsoft network client: Send unencrypted password to third-party SMB servers | Not Defined |
| Microsoft network server: Amount of idle time required before suspending session | Not Defined |
| Microsoft network server: Digitally sign communications (always) | Not Defined |
| Microsoft network server: Digitally sign communications (if client agrees) | Not Defined |
| Microsoft network server: Disconnect clients when logon hours expire | Not Defined |

**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'.

⇨ Double-click 'Interactive logon: Smart card removal behavior'.

The Interactive logon: Smart card removal behavior Properties dialog opens:



Interactive logon: Smart card removal behavior

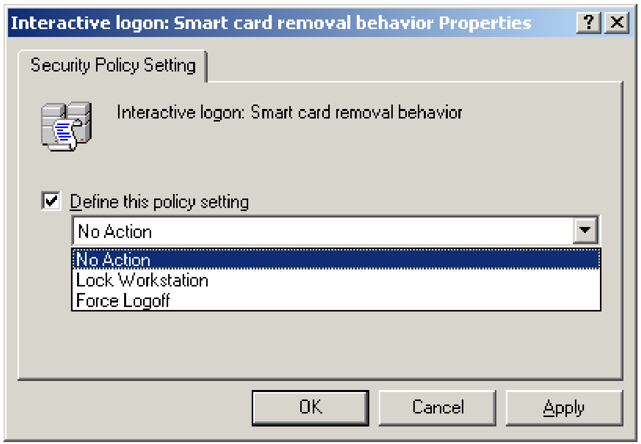
□ Define this policy setting

No Action

**Figure 49: Interactive logon: Smart card removal behavior Properties**

⇨ Check **Define this policy setting**

Define a policy setting for the behavior for when a token is removed from within your domain:



Interactive logon: Smart card removal behavior Properties

Interactive logon: Smart card removal behavior

☑ Define this policy setting

No Action ▼

- No Action
- Lock Workstation
- Force Logoff

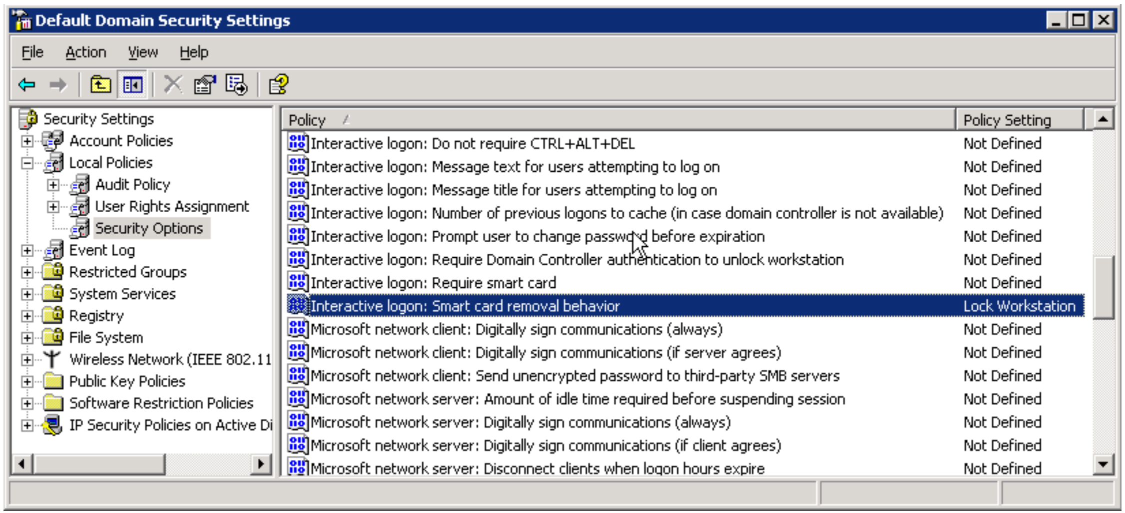
**Figure 50: Interactive logon: Smart card removal behavior Properties: Define this policy setting**

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 behavior for the domain is now set.



| Policy | Policy Setting |
|---|---|
| Interactive logon: Do not require CTRL+ALT+DEL | Not Defined |
| Interactive logon: Message text for users attempting to log on | Not Defined |
| Interactive logon: Message title for users attempting to log on | Not Defined |
| Interactive logon: Number of previous logons to cache (in case domain controller is not available) | Not Defined |
| Interactive logon: Prompt user to change password before expiration | Not Defined |
| Interactive logon: Require Domain Controller authentication to unlock workstation | Not Defined |
| Interactive logon: Require smart card | Not Defined |
| Interactive logon: Smart card removal behavior | Lock Workstation |
| Microsoft network client: Digitally sign communications (always) | Not Defined |
| Microsoft network client: Digitally sign communications (if server agrees) | Not Defined |
| Microsoft network client: Send unencrypted password to third-party SMB servers | Not Defined |
| Microsoft network server: Amount of idle time required before suspending session | Not Defined |
| Microsoft network server: Digitally sign communications (always) | Not Defined |
| Microsoft network server: Digitally sign communications (if client agrees) | Not Defined |
| Microsoft network server: Disconnect clients when logon hours expire | Not Defined |

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

Be advised that it could 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, and 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 the 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 while unlocking the machine, Windows displays the Computer Locked error dialog: “The computer is locked. Only [user name] or an administrator can unlock this computer.”

### 4.2.4 Smart card removal

The GINA component (installed as part of the HID Crescendo C700 middleware) provides additional functionality with regard to smart card removal at log off / lock. When the user locks the computer or logs off, an audible and visual signal indicates to remove the card from the reader. The following dialog displays:

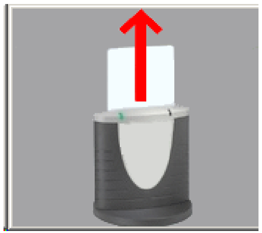


**Figure 52: SafeSign GINA: Remove token**

Unless the user removes their token, they are not logged off or the computer does not lock.

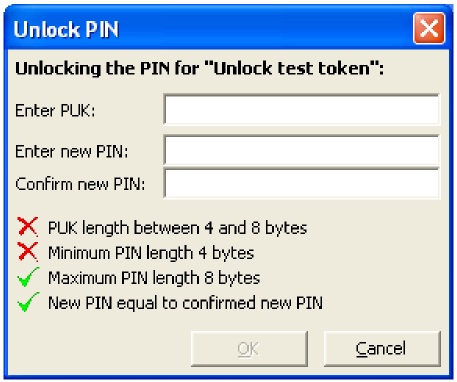
To force the user to remove the card while locking the workstation or logging off, modify the registry key with the following values. Under *DWORD DenyLockIfCardPresent / DenyLogoffIfCardPresent*, change the values to 1 in the registry key *[HKEY_LOCAL_MACHINE\SOFTWARE\A.E.T. Europe B.V.\SafeSign\2.0\GINA]*. By default, these values are zero and the user can lock the computer while leaving the card in the reader.

At logon time, unlock a token of which the PIN is blocked (section 4.2.5) and change the transport PIN of a token that has a transport PIN (section 4.2.6).

### 4.2.5 Unlock PIN

When the PIN is locked, you may unlock the PIN at logon. After entering the (locked) PIN at the Windows logon prompt, a dialog informs you that the token is locked, asking if you wish to unlock the token.

**Note:** Unlock the PIN in two ways: with PUK or secure off-line PIN unlock mechanism (if implemented). If the token can only be unlocked by the PUK, the following dialog appears:



Unlock PIN

**Unlocking the PIN for "Unlock test token":**

Enter PUK:

Enter new PIN:

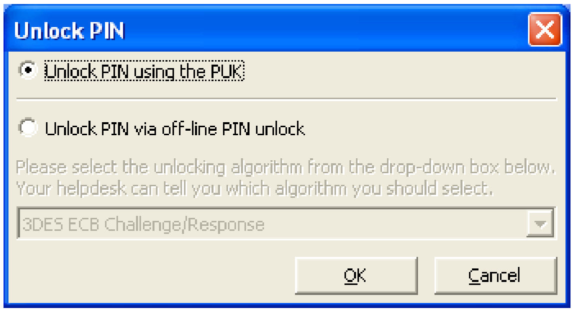
Confirm new PIN:

✗ PUK length between 4 and 8 bytes
✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 8 bytes
✓ New PIN equal to confirmed new PIN

**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 is allowed to chose which method to use for unlocking the PIN, either by using the PUK or off-line PIN unlock:



● Unlock PIN using the PUK

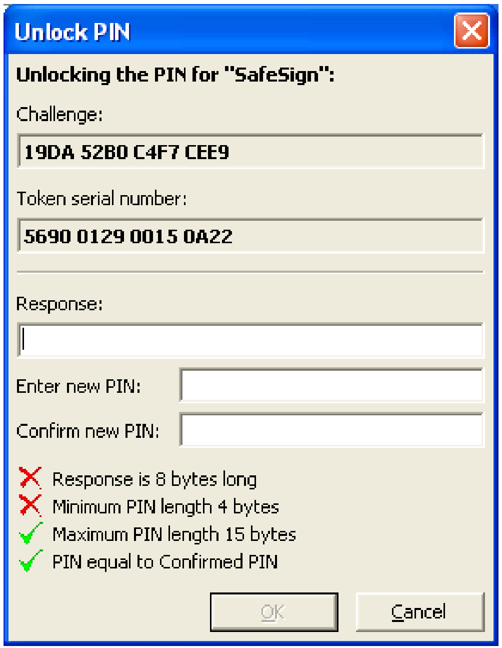
○ Unlock PIN via off-line PIN unlock

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

3DES ECB Challenge/Response

Figure 54: Unlock PIN: Select method

When selecting ‘Unlock PIN via off-line PIN unlock’, the user should contact the designated person or department (for example, helpdesk) to obtain the necessary details for unlocking the PIN:



Unlocking the PIN for "SafeSign":

Challenge: 19DA 52B0 C4F7 CEE9

Token serial number: 5690 0129 0015 0A22

Response:

Enter new PIN:

Confirm new PIN:

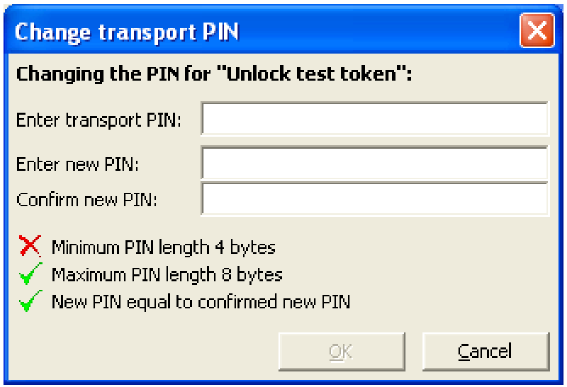
✗ Response is 8 bytes long
✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes
✓ PIN equal to Confirmed PIN

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

### 4.2.6 Change Transport PIN

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

At logon, a dialog informs you that the token has a Transport PIN, asking if you want to change the Transport PIN. Select **Yes** to change the Transport PIN:



Change transport PIN

Changing the PIN for "Unlock test token":

Enter transport PIN:

Enter new PIN:

Confirm new PIN:

✗ Minimum PIN length 4 bytes
✓ Maximum PIN length 8 bytes
✓ New PIN equal to confirmed new PIN

Figure 56: Change transport PIN

⇨ Enter the Transport PIN for the token and enter a new PIN

## 4.3 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), a user should logon to the domain with a token and PIN instead of a username and password. When two-factor authentication is enforced, a user can only log on with a token and PIN. This security feature is only configured on a per-user basis.

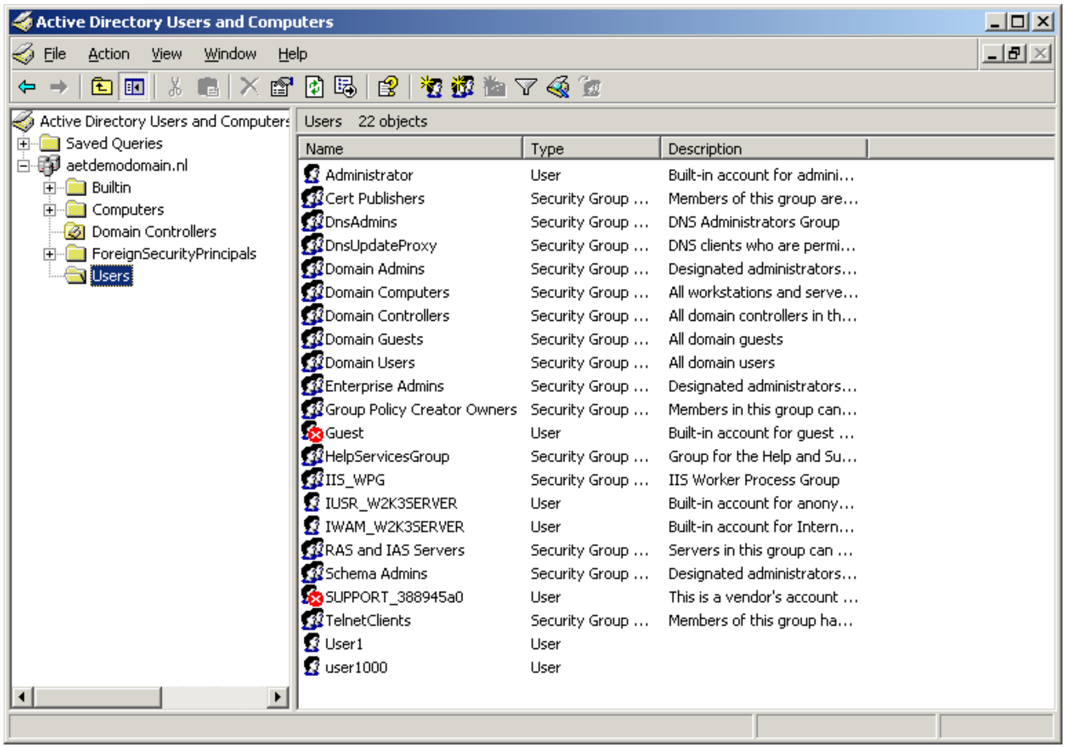
When activating this policy for (domain) administrators, remove this feature after logging on to the Windows 2003 server with the same smart card. You can also remove this feature with another smart card that contains a correct certificate for the domain administrator.

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

Active Directory Sites and Services
Active Directory Users and Computers
Authorization Manager

**Figure 57: Active Directory Users and Computers**

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

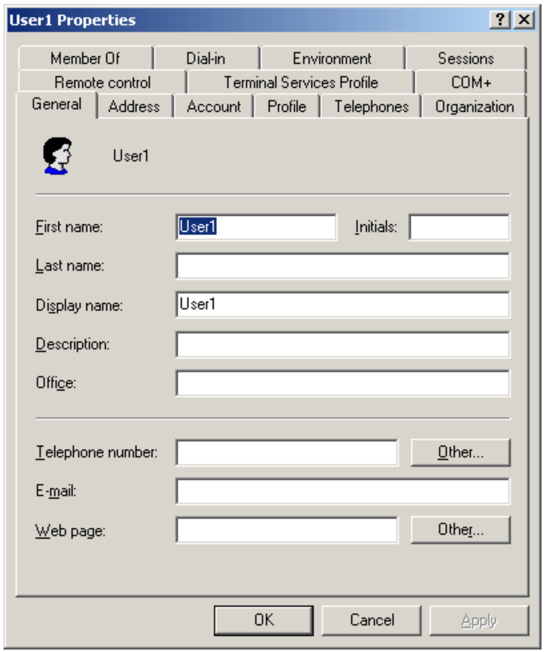

Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computers
Saved Queries
aetdemodomain.nl
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Users 22 objects

| Name | Type | Description |
|---|---|---|
| Administrator | User | Built-in account for admini... |
| Cert Publishers | Security Group ... | Members of this group are... |
| DnsAdmins | Security Group ... | DNS Administrators Group |
| DnsUpdateProxy | Security Group ... | DNS clients who are permi... |
| Domain Admins | Security Group ... | Designated administrators... |
| Domain Computers | Security Group ... | All workstations and serve... |
| Domain Controllers | Security Group ... | All domain controllers in th... |
| Domain Guests | Security Group ... | All domain guests |
| Domain Users | Security Group ... | All domain users |
| Enterprise Admins | Security Group ... | Designated administrators... |
| Group Policy Creator Owners | Security Group ... | Members in this group can... |
| Guest | User | Built-in account for guest ... |
| HelpServicesGroup | Security Group ... | Group for the Help and Su... |
| IIS_WPG | Security Group ... | IIS Worker Process Group |
| IUSR_W2K3SERVER | User | Built-in account for anony... |
| IWAM_W2K3SERVER | User | Built-in account for Intern... |
| RAS and IAS Servers | Security Group ... | Servers in this group can ... |
| Schema Admins | Security Group ... | Designated administrators... |
| SUPPORT_388945a0 | User | This is a vendor's account ... |
| TelnetClients | Security Group ... | Members of this group ha... |
| User1 | User | |
| user1000 | User | |

**Figure 58: Active Directory Users and Computers: Users**

➪ Double-click the user you wish to configure the ‘require smart card to logon’ policy.

This opens the Properties dialog for the user:



User1

First name: User1 Initials:

Last name:

Display name: User1

Description:

Office:

Telephone number:

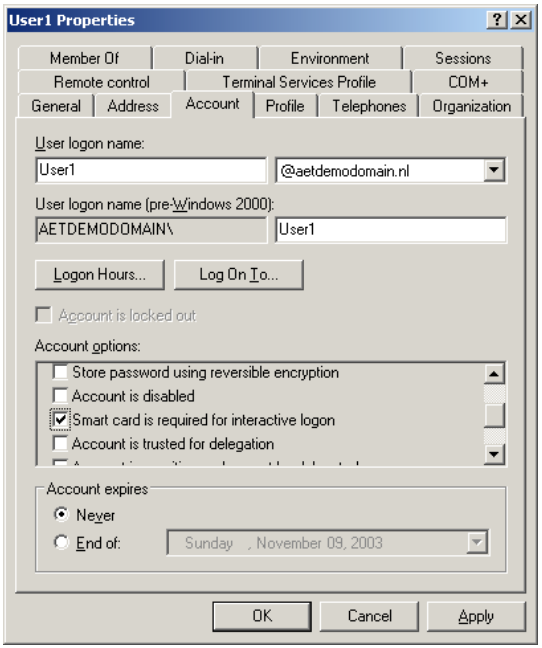
E-mail:

Web page:

Figure 59: Properties: general

➪ Open the **Account** tab

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



User logon name: User1 @aetdemodomain.nl

User logon name (pre-Windows 2000): AETDEMODOMAIN\ User1

□ Account is locked out

Account options:

□ Store password using reversible encryption
□ Account is disabled
☑ Smart card is required for interactive logon
□ Account is trusted for delegation

Account expires
● Never
○ End of: Sunday , November 09, 2003

Figure 60: Properties: Account

➪ Click **OK**

The user now only uses a token for interactive logon.

## 4.4 Troubleshooting Windows XP Logon

| Logon Message | Possible Cause | Remedy |
|---|---|---|
| The card supplied requires drivers that are not present on this system.<br>Please try another card. | No CSP is 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 initialized.<br>The token does not contain a Digital ID. | Use the Token Management Utility / Token Administration Utility to initialize the (blank) token.<br>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].<br>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. | Verify if the token contains a Digital ID that is suitable for the domain. |
| 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.<br>Enter the correct PIN. |
| The system could not you log on and 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.<br>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.<br>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:

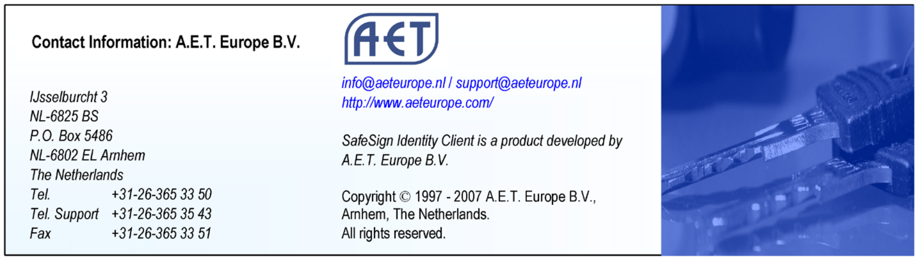
Knowledge Base article ‘Guidelines for Enabling Smart Card Logon with Third-Party Certification Authorities’: http://support.microsoft.com/default.aspx?scid=kb;en-us;281245

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.

The original version of this guide was written by A.E.T. Europe B.V and this version is based on document ID1.

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.



**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.*

Copyright © 1997 - 2007 A.E.T. Europe B.V.,
Arnhem, The Netherlands.
All rights reserved.

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.

## Access Secure Identity

**HID Global**
9292 Jeronimo Road
Irvine, CA 92618
Tel.: (949)-598-1600
Fax: (949)-598-1690
www.hidglobal.com