SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for Microsoft Identity Manager 2016 SP1 Certificate Manager

gemalto
security to be free

Document Part Number: 007-013827-001, Rev. A

Release Date: July 2017

Contents

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Microsoft Identity Manager 2016 SP1 Certificate Manager.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

Customers today are looking to desktop virtualization to transform static desktops into dynamic mobile workspaces that can be centrally and securely managed from the datacenter, and accessed across a wide range of devices and locations. Deploying desktop virtualization without strong authentication is like putting your sensitive data in a vault (the datacenter), and leaving the key (user password) under the door mat. A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

SafeNet Authentication Client (SAC) is a Public Key Infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. SafeNet's certificate-based tokens provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

SafeNet Authentication Manager (SAM) provides your organization with a comprehensive platform to manage all of your authentication requirements, across the enterprise and the cloud, in a single, integrated system. SAM enables management of the complete user authentication life cycle. SAM links tokens with users, organizational rules, and security applications to allow streamlined handling of your organization's authentication infrastructure with a flexible, extensible, and scalable management platform.

SAM is a comprehensive token management system. It is an out-of-the-box solution for Public Certificate Authorities (CA) and enterprises to ease the administration of SafeNet's hardware or software tokens devices. SAM is designed and developed based on the best practices of managing PKI devices in common PKI implementations. It offers robust yet easy to customize frameworks that meets different organizations' PKI devices management workflows and policies. Using SAM to manage tokens is not mandatory, but it is recommended for enterprise organizations.

For more information, refer to the *SafeNet Authentication Manager Administrator Guide*.

Microsoft Identity Manager (MIM) 2016 builds on the identity and access management capabilities of FIM 2010 R2 Microsoft Forefront Identity Manager (MIM) provides identity synchronization, user provisioning, certificate and password management, and policy management in a single solution that works across heterogeneous systems. Forefront Identity Manager Certificate Management (MIM CM) provides functionality to support certificate and smart card management

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Microsoft Identity Manager 2016 SP1 Certificate Manager using SafeNet tokens.

It is assumed that the Microsoft Identity Manager 2016 SP1 Certificate Manager environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

Microsoft Identity Manager 2016 SP1 Certificate Manager can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with SafeNet products.

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC), Typical installation mode -** SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto's tokens and smart cards.
- **SafeNet Authentication Client (SAC), IDGo800 Compatible mode** - IDGo800 Minidriver based package, using Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards. For more details about different SAC installation modes, refer to the SafeNet Authentication Client Administration Guide.

Environment

The integration environment that was used in this document is based on the following software versions:

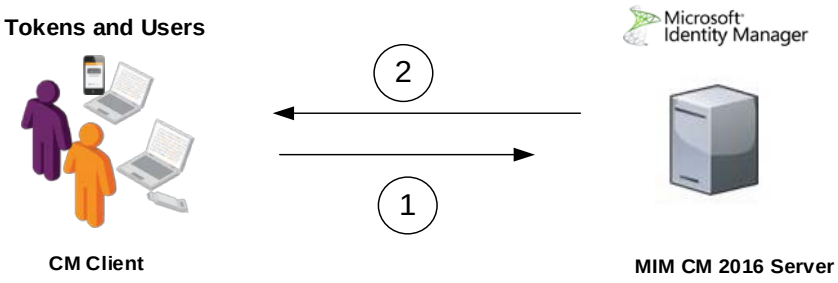
  - **SafeNet Authentication Client (SAC) Typical installation mode** - 10.3
  - **SafeNet Authentication Client (SAC) IDGo800 Compatible mode -** Created By SAC customization tool 10.3 - Binaries version 8.5.0.5
  - **Gemalto.SafeNet.Minidriver – 9.0.44**
  - **Microsoft DC and CA -** installed in Windows Server 2008R2
- **Microsoft Identity Manager 2016 SP1 Certificate Manager Server SP** 1 version 4.4.1237.0 - installed in Windows Server 2008R2
- **Microsoft Identity Manager 2016 SP1 Certificate Manager Client SP** 1 version 4.4.1237.0 - Installed on Win 7 x32 with IE 11

Audience

This document is intended for system administrators who are familiar with Microsoft Identity Manager 2016 SP1 Certificate Manager, and are interested in adding certificate-based authentication capabilities using SafeNet tokens or smart cards.

Enrollment Flow using SafeNet Authentication Client

The diagram below illustrates the flow of enrollment using SafeNet Authentication Client:



1. A user connects to the Microsoft Identity Manager 2016 SP1 Certificate Manager server from a client with the Microsoft Identity Manager 2016 SP1 Certificate Manager client application. The user inserts the SafeNet token and performs “request of permanent smart card”, and when prompted, enters a new user PIN in the **New PIN** and **Confirm PIN** fields, then clicks **OK** to continue.
2. After successful authentication, the user certificate is enrolled to token/smart card.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for Microsoft Identity Manager 2016 SP1 Certificate Manager using SafeNet tokens:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, Token Policy Object (TPO) should be configured with MS CA Connector. For further details, refer to the section “Connector for Microsoft CA” in the *SafeNet Authentication Manager Administrator’s Guide*.
- Users must have a SafeNet token with an appropriate certificate enrolled on it.
- SafeNet Authentication Client (10.3) should be installed on all client machines.
- According to https://docs.microsoft.com/en-us/microsoft-identity-manager/deploy-use/microsoft-identity-manager-deploy, Microsoft Identity Manager 2016 follows a process very similar to its predecessor, FIM 2010 R2. In this guide, Certificate Management 2016 installed and configured on the Windows server. According to http://technet.microsoft.com/en-us/library/ee534914(v=ws.10).aspx.
- Microsoft Identity Manager Certificate Management Client must be installed on all the client machines. Refer to http://technet.microsoft.com/en-us/library/ee534899(v=ws.10).aspx.
- For using SafeNet smart cards with MIM CM through SAC, SAC must be installed on the client machine
- Copy of “Smart Card User Certificate” template is configured and attached to each MIM profile template.

Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client (10.3) supports the following tokens and smart cards:

Certificate-based USB tokens

- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 CC

Smart Cards

- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840

For all supported devices please refer to SafeNet Authentication Client Customer Release Notes.

Secure Key Injection

This feature is not implemented in MIM CM for “Microsoft smart card base CSP” provider
For other PKCS11 Provider not supported at the moment.

Password quality

MIM CM does not support Customizing cards policy.

Supported Tokens/Smart Cards in Microsoft Identity Manager 2016 SP1 Certificate Manager

Token\Smart card	MIM Provider Name Configuration	Installation Mode
*IDPrime MD 840 B	Aladdin eToken	SafeNet Authentication client 10.3
	Microsoft Smart Card Base CSP	IDGo BC Compatible 10.3
IDPrime MD 830 B L3	Aladdin eToken	SafeNet Authentication client 10.3
	Microsoft Smart Card Base CSP	IDGo BC Compatible 10.3
IDPrime MD 830 B L2	Aladdin eToken	SafeNet Authentication client 10.3
	Microsoft Smart Card Base CSP	IDGo BC Compatible 10.3
** eToken 5110 FIPS	Aladdin eToken	SafeNet Authentication client 10.3
*** eToken 5110 GA	Aladdin eToken	SafeNet Authentication client 10.3
	Microsoft Smart Card Base CSP	Gemalto.Safenet.Minidriver
* eToken 5110 CC	Aladdin eToken	SafeNet Authentication client 10.3

* IDPrime MD840 and eToken 5110 CC - Enrollment of “Signature only” Certificate with “Aladdin eToken” Profile supported only when card is initialized in Linked Mode.

** eToken 5110 FIPS Token Supported only on “Aladdin eToken Provider” with SAC installed.
eToken 5110 FIPS is not supported with “MS Base” Profile with MD SafeNet Gemalto Minidriver 9.0.44 installed, will be supported with minidriver package in future release.

*** eToken 5110 GA - Supported only with Gemalto.safeNet.Minidriver on “FIPS Compatible mode”

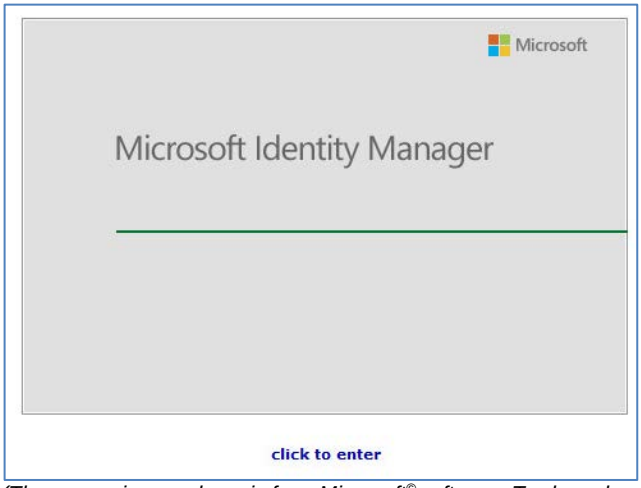
Configuring Microsoft Identity Manager 2016 SP1 Certificate Manager

Template for SAC

The CM profile template needs to be configured with the information necessary to manage the smart card.

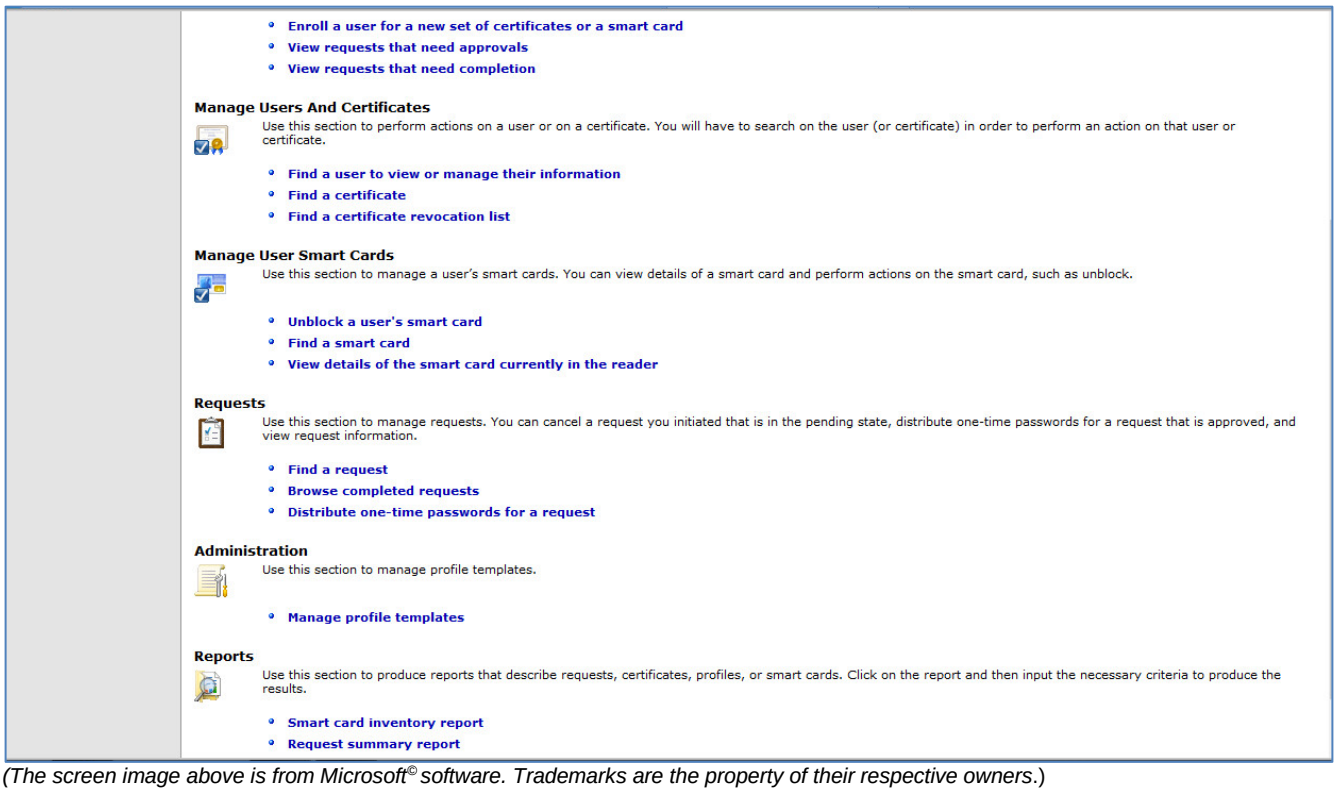
NOTE: To create a new Profile Template, copy an existing template and modify as required. Two sample templates are provided with MIM CM, for this purpose in this example “FIM CM Sample Smart Card Logon Profile Template” was copied.

1. Open **MIM CM Portal** and log in as a user with permissions to create a Profile Template.



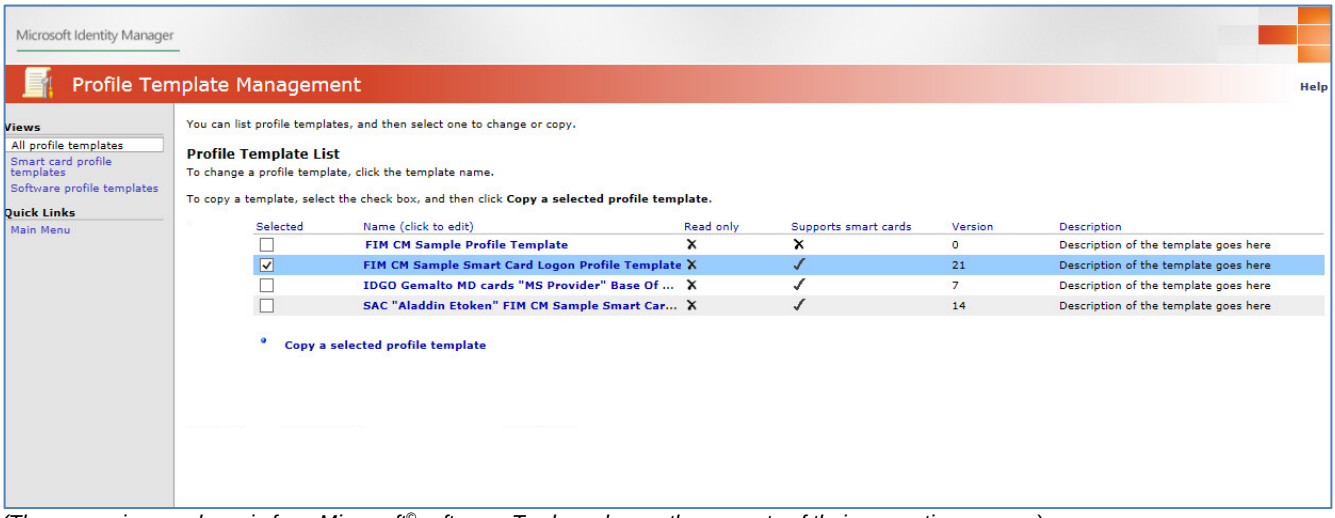
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

2. Under **Administration**, click **Manage profile templates**.



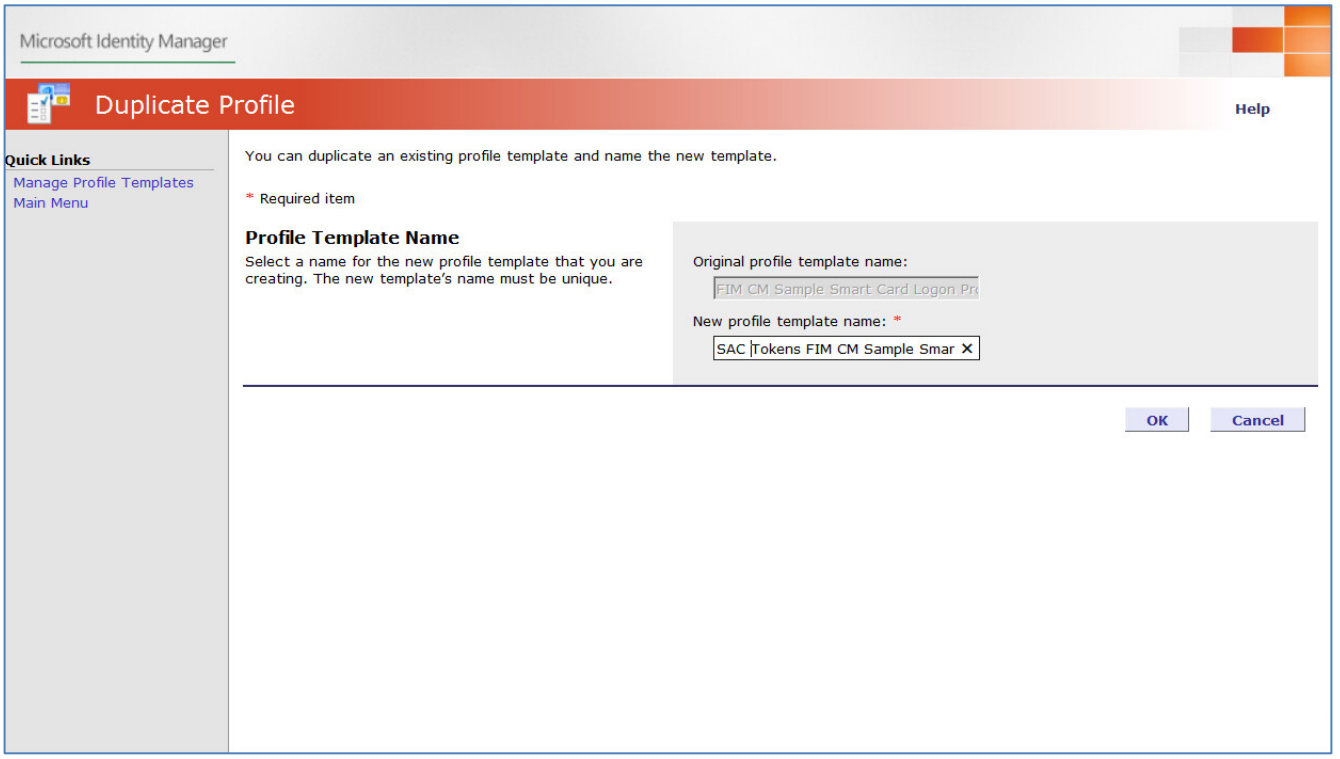
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

3. Select **FIM CM Sample Smart Card Logon Profile Template**, and then click **Copy a selected profile template**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

4. In the **New profile template name** field, enter the name of the template (Example: “SAC Tokens FIM CM Sample Smart Card User Profile”) and then click **OK**.

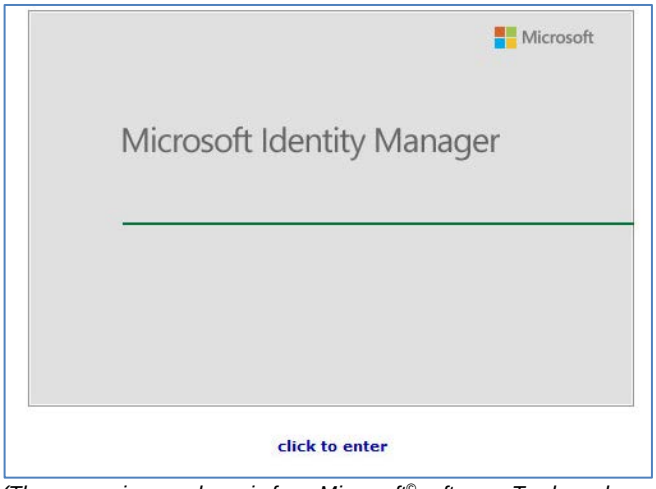


(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

Configuring a Profile Template for SAC

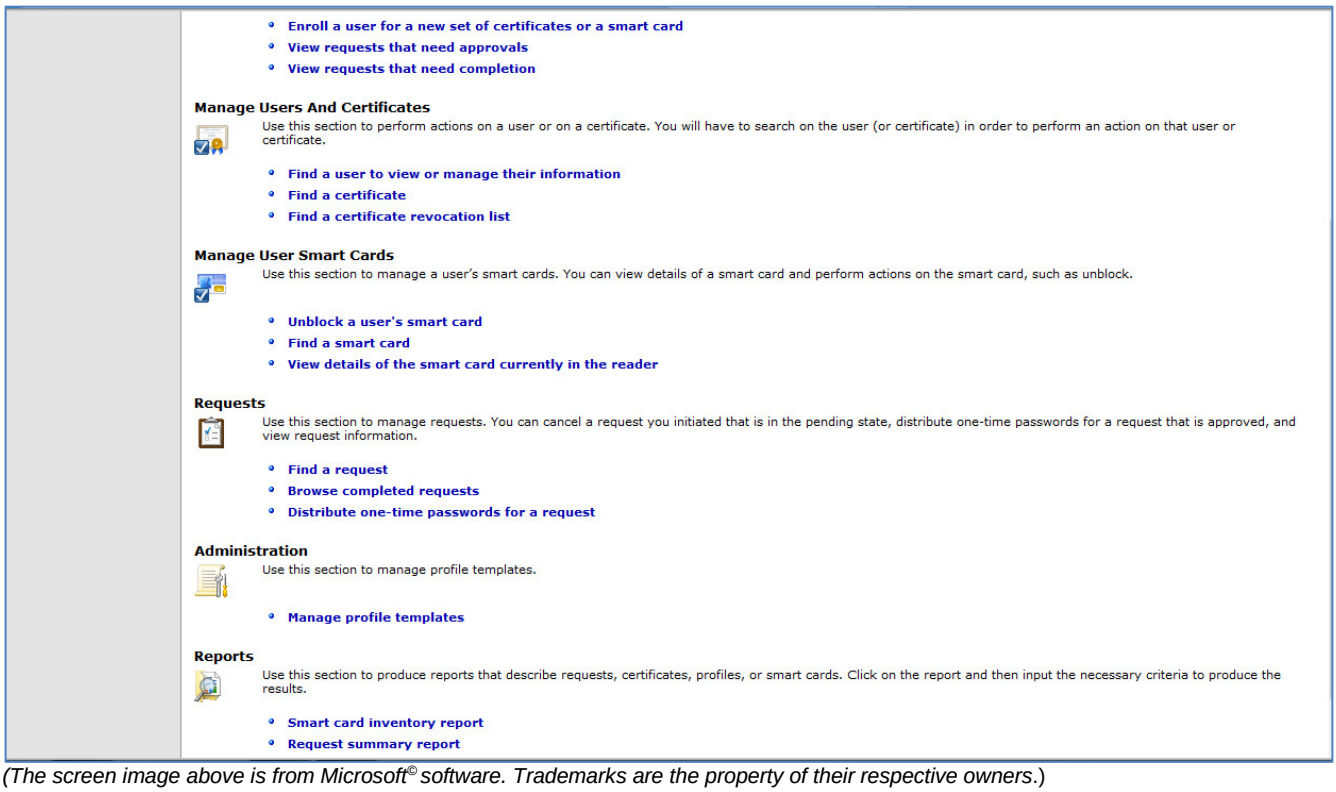
For each profile template, configure the general settings and the certificate template settings that will be used by the profile template.

1. Open **MIM CM Portal** and log in as a user with administrative privileges.



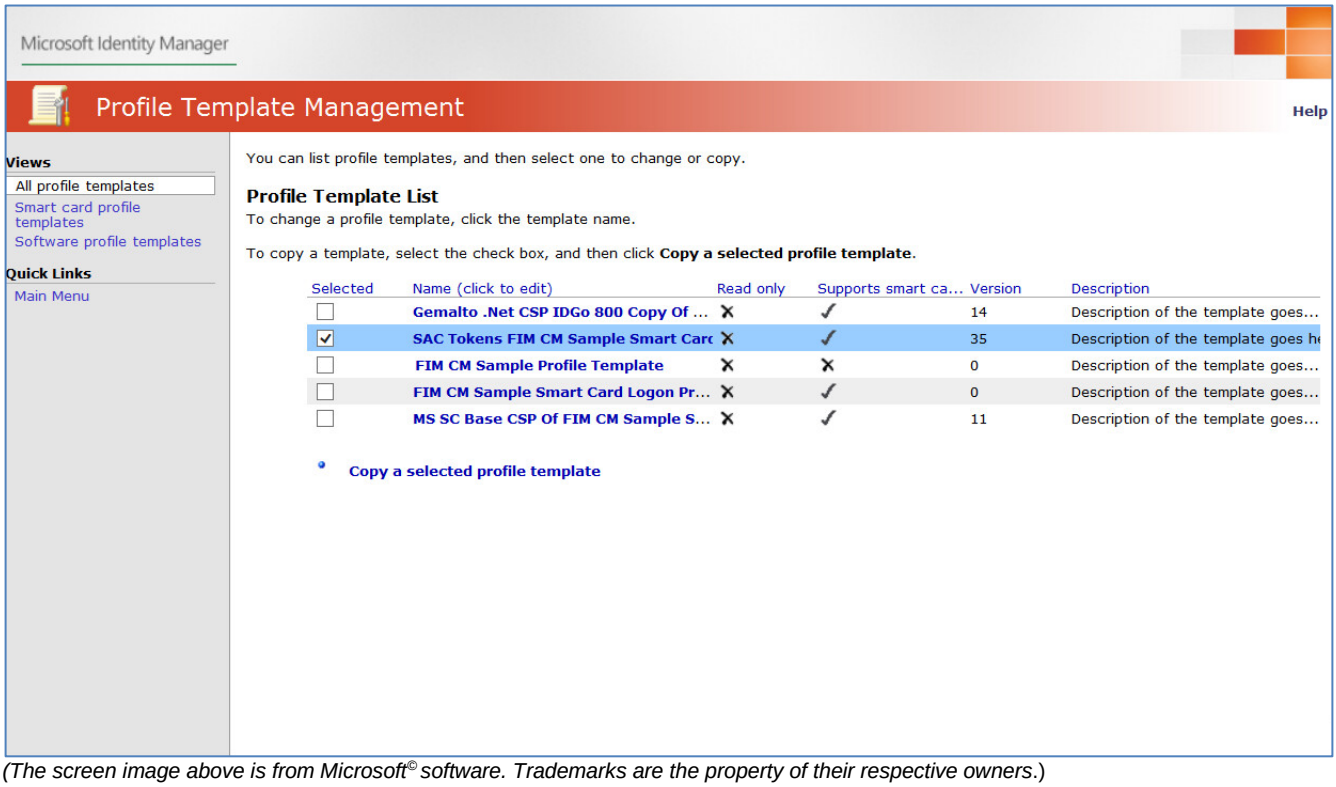
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

2. Under **Administration**, click **Manage profile templates**.



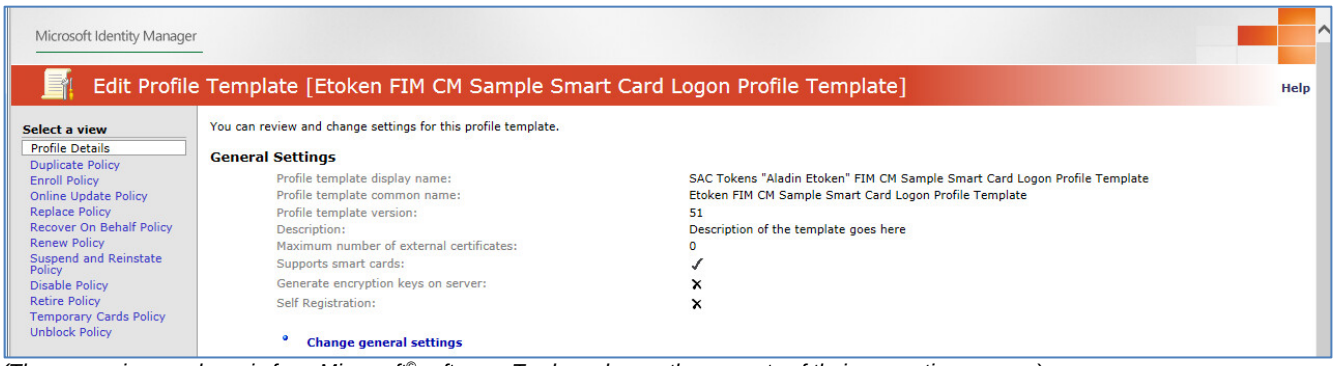
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

3. In the **Profile Template List**, select a template (Example: "SAC Tokens..."), and click on the profile template name to edit it.



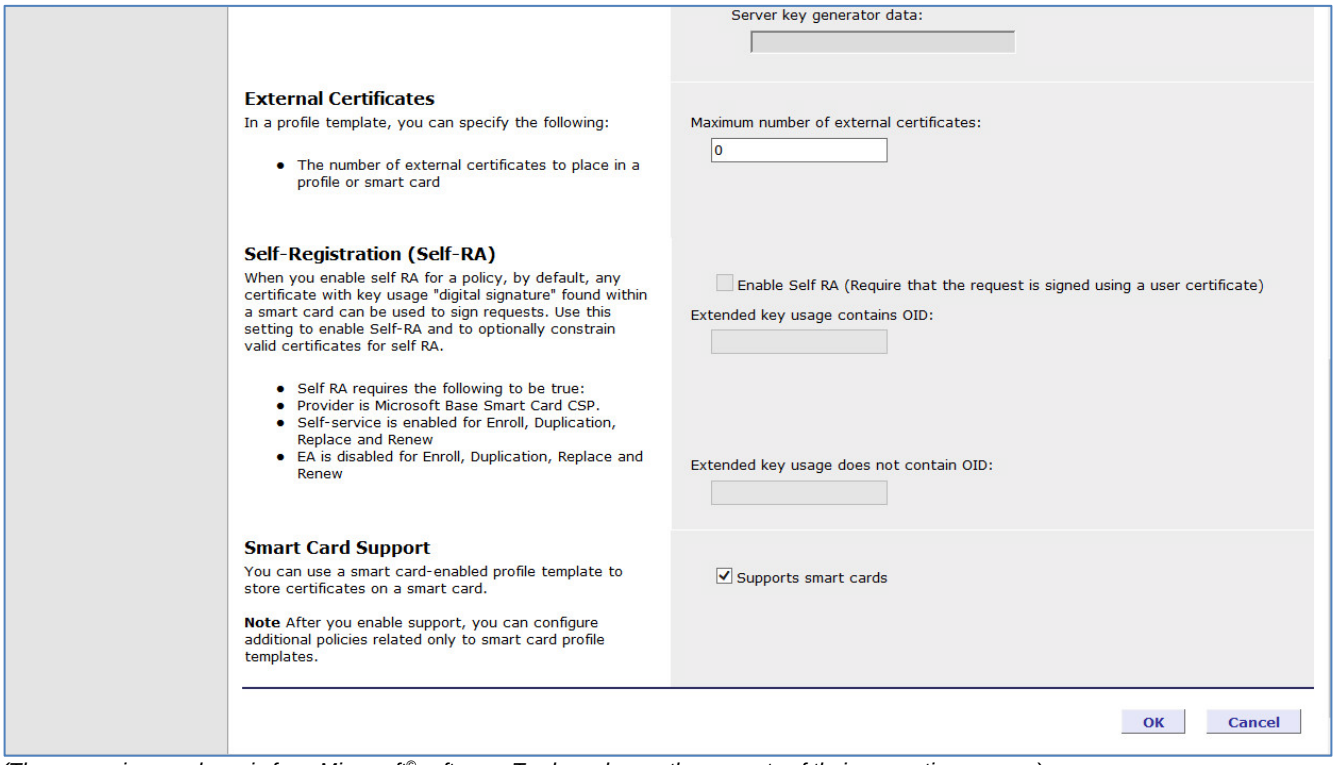
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

4. Under **General Settings**, click **Change General Settings**.



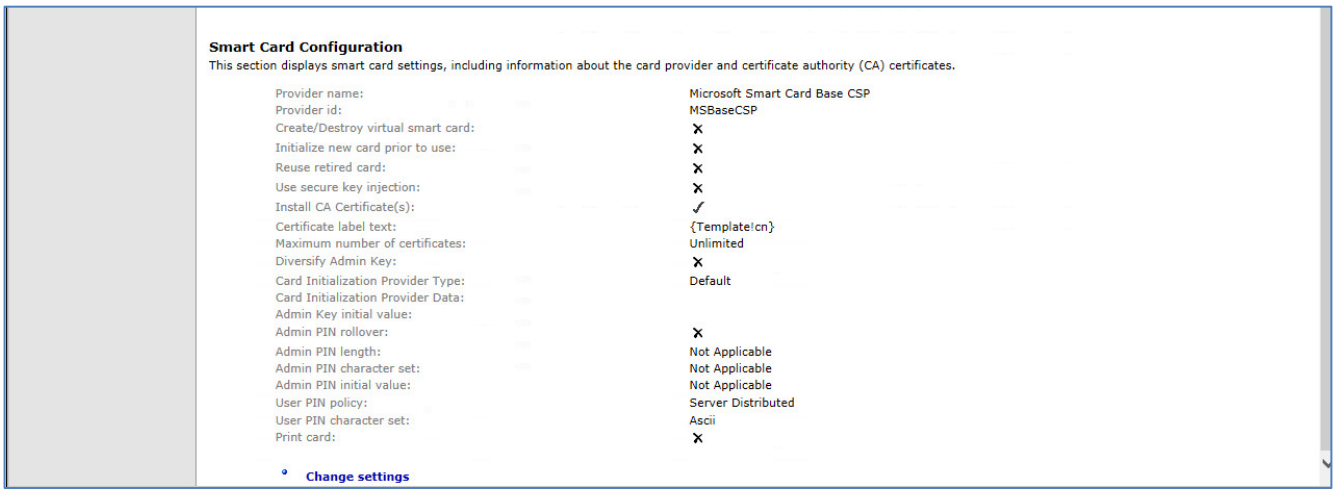
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

5. Ensure that **Supports smart cards** is selected, and then click **OK**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

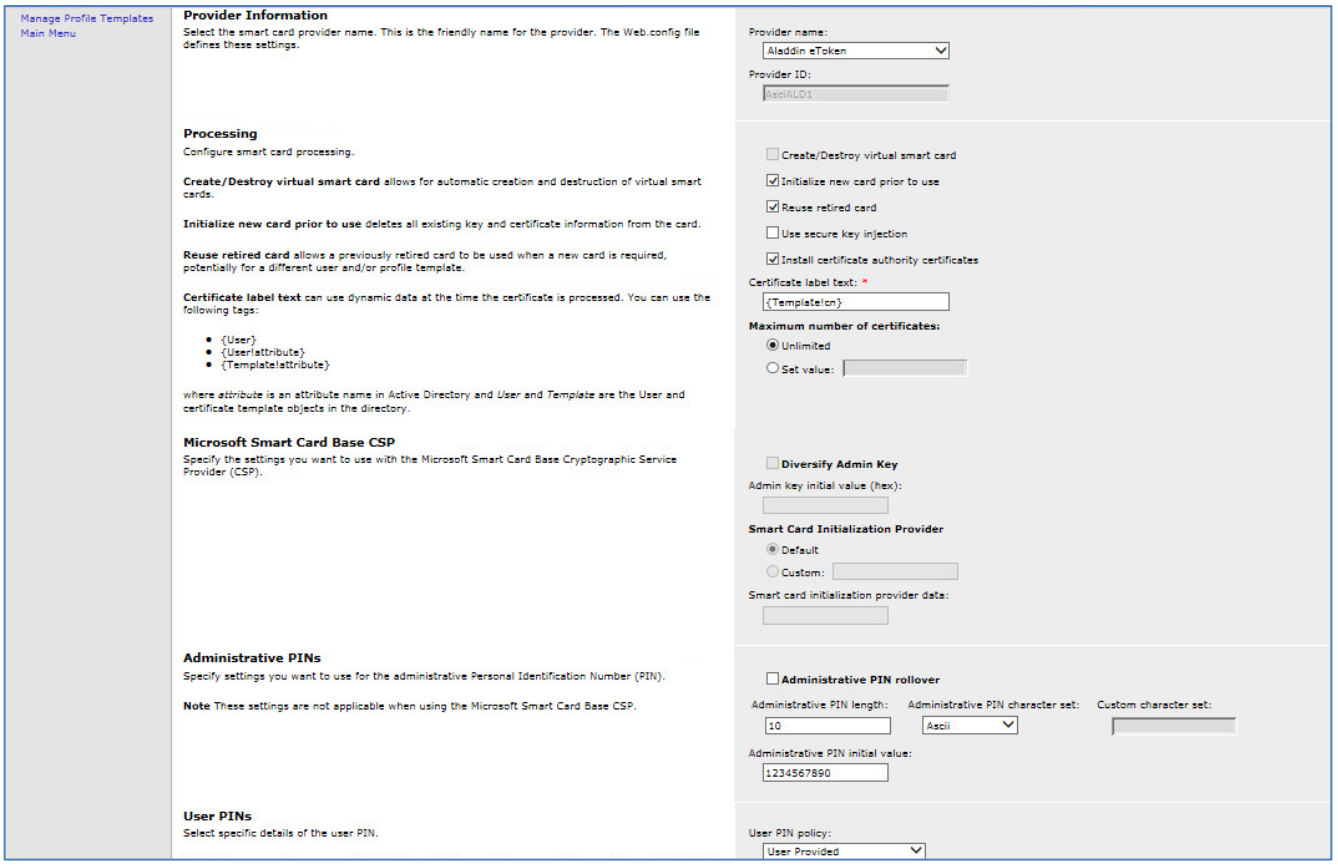
6. Under **Smart Card Configuration**, click **Change Settings**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

7. Complete the details as specified in the table below and then click **OK**.

Provider name	Select **Aladdin eToken**
Initialize new card prior to use	Select this option
Reuse retired card	Select this option.
Install certificate authority certificates	Select this option.
Administrative PIN length	Enter the Smart Card Admin PIN length. (Pay attention to differences between MD Cards (Used 48 length for example) / eTokens (Used 10 length in this example)
Administrative PIN initial value	Enter the Smart Card Admin PIN initial value. (Pay attention to differences between MD Cards (Used Admin Pin 48's zero for example) / eTokens (used Admin Pin 1-0 in this example))
User PIN policy	Select **User Provided**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

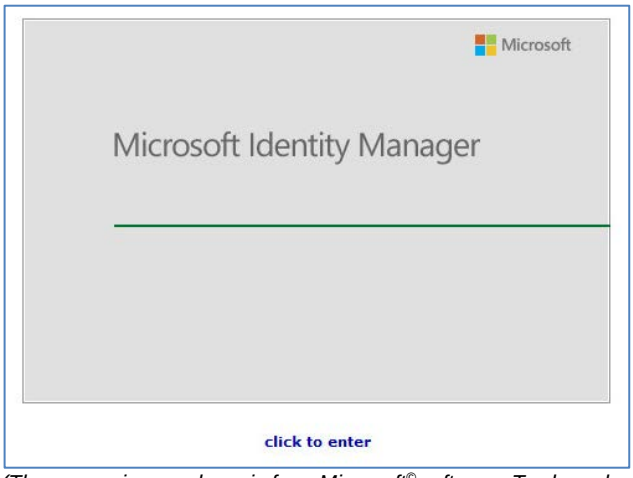
Template for IDGo800 Mini Driver Backward compatibility

The CM profile template needs to be configured with the information necessary to manage the smart card.

NOTE: To create a new profile template, copy an existing template and modify as required. Two sample templates are provided with MIM CM, for this purpose. In this example “FIM CM Sample Smart Card Logon Profile Template” was copied.

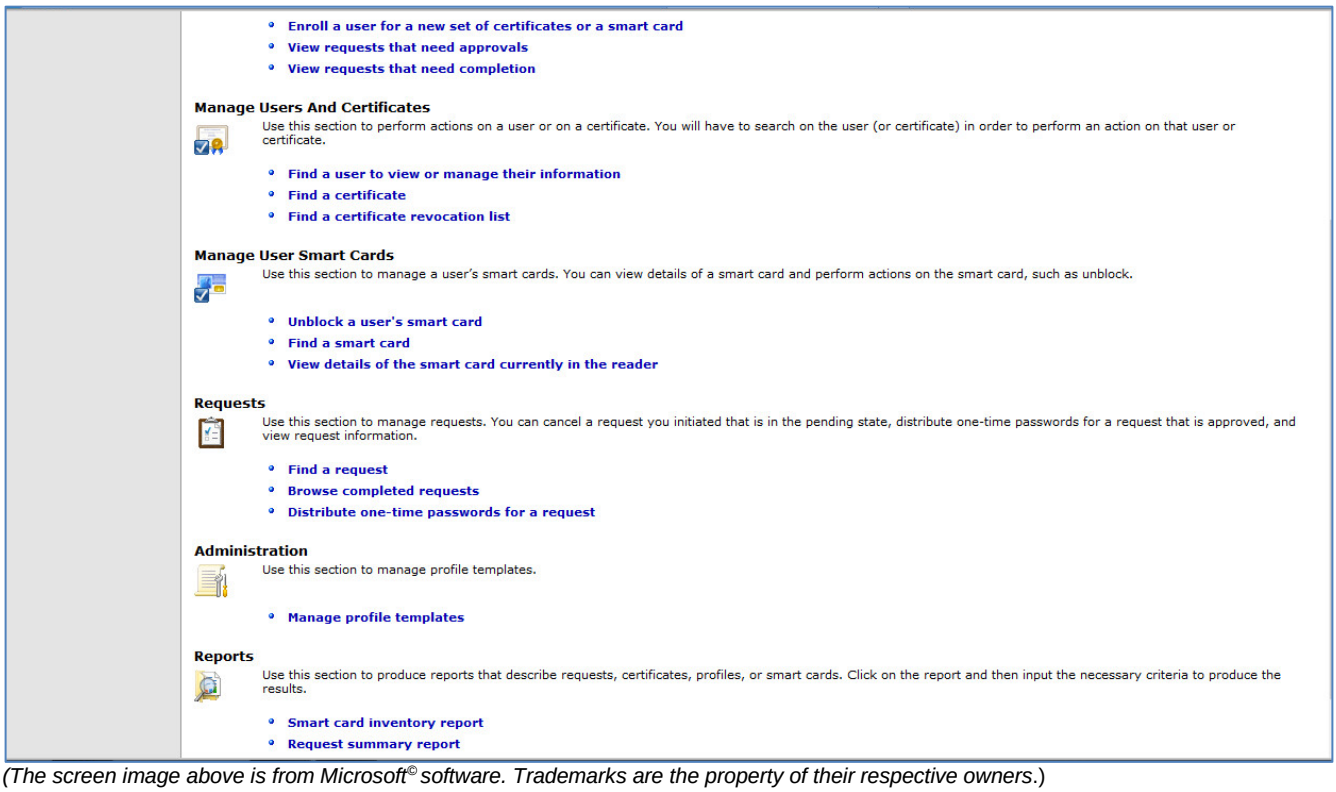
For each profile template, configure the general settings and the certificate template settings that will be used by the profile template.

1. Open **MIM CM Portal** and log in as a user with administrative privileges.



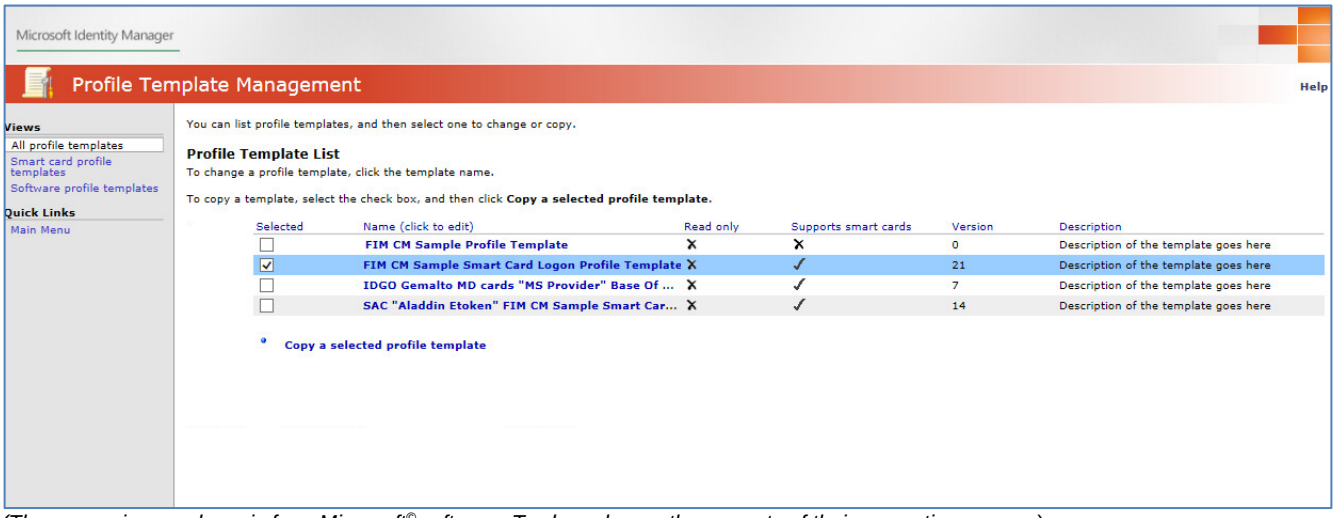
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

2. Under **Administration**, click **Manage profile templates**.



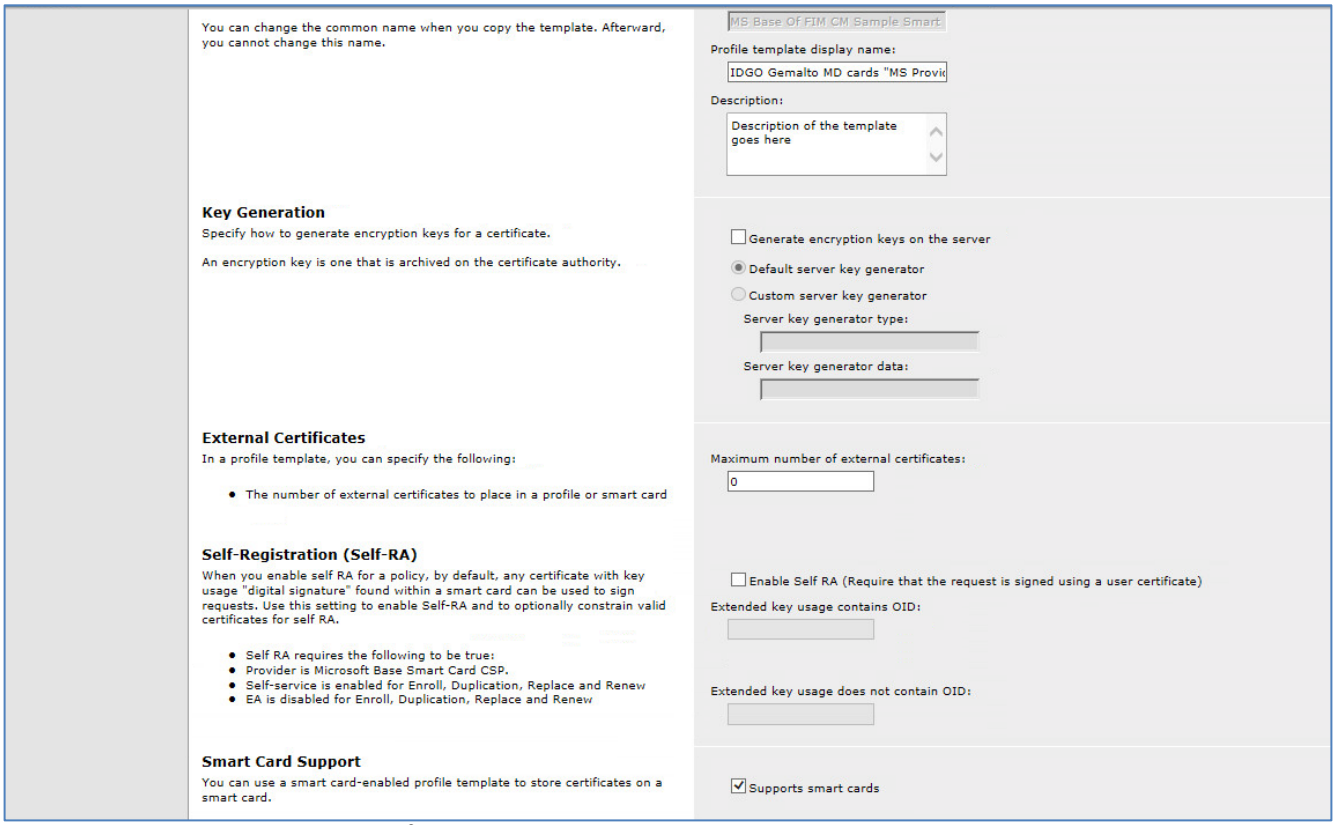
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

3. Select "**FIM CM Sample Smart Card Logon Profile Template**", and then click **Copy a selected profile template**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

4. In the **New profile template name** field, enter the name of the template (**Example: "IDGo Gemalto MD …"**) and then click **OK**.

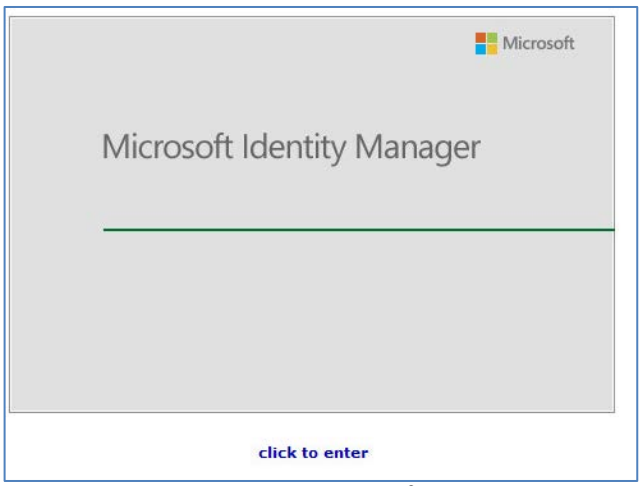


(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

Configuring a Profile Template for IDGo800 MD Backward compatibility

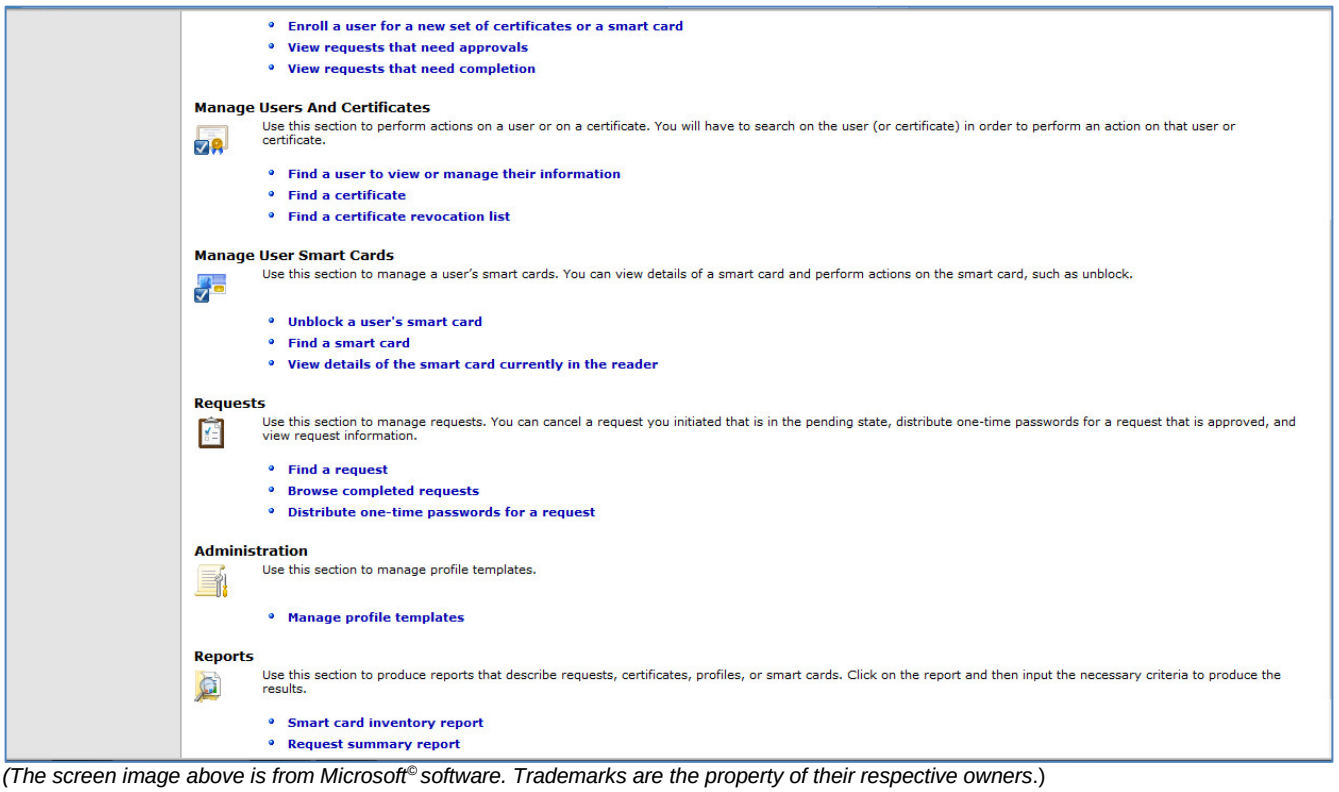
For each profile template, configure the general settings and the certificate template settings that will be used by the profile template.

1. Open **MIM CM Portal** and log in as a user with administrative privileges.



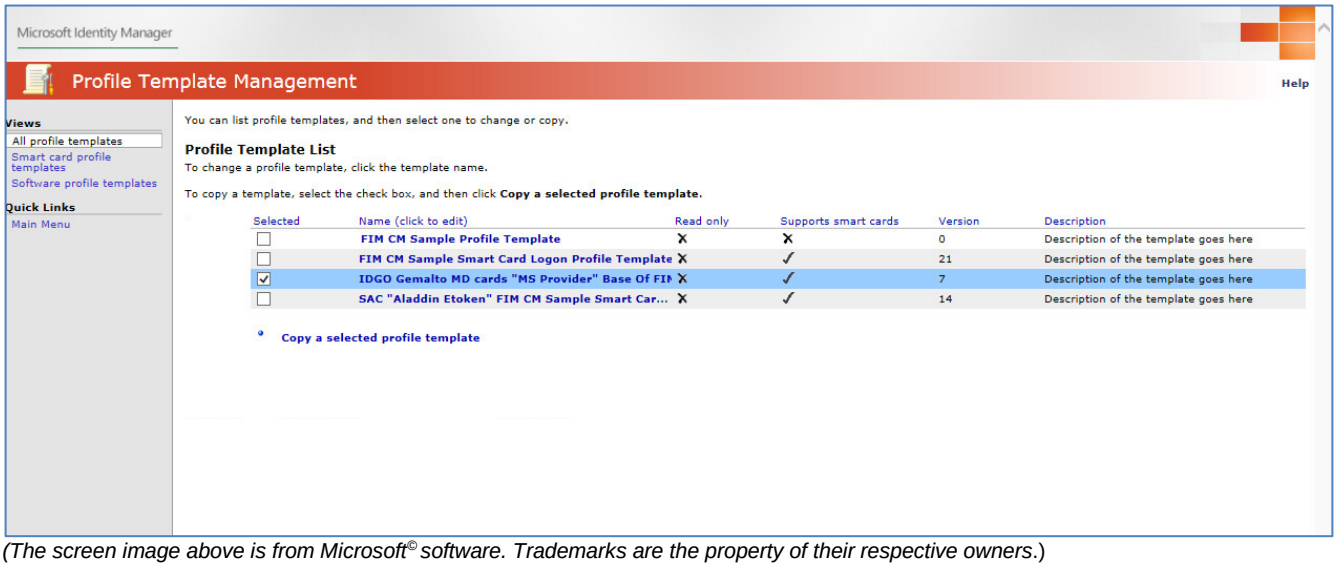
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

2. Under **Administration**, click **Manage profile templates**.



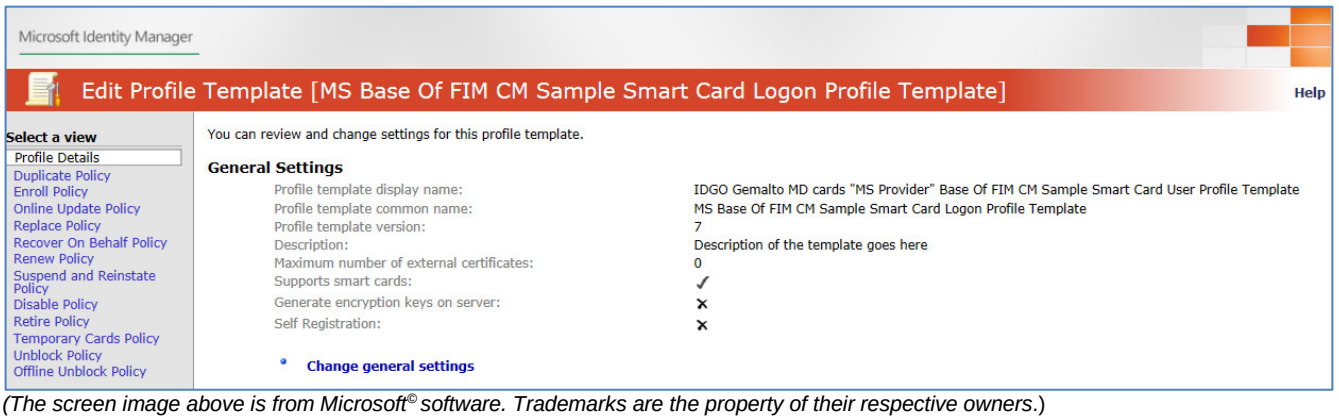
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

3. In the **Profile Template List**, select the template (For example: "IDGo Gemalto MD..."), and click on the profile template name to edit it.



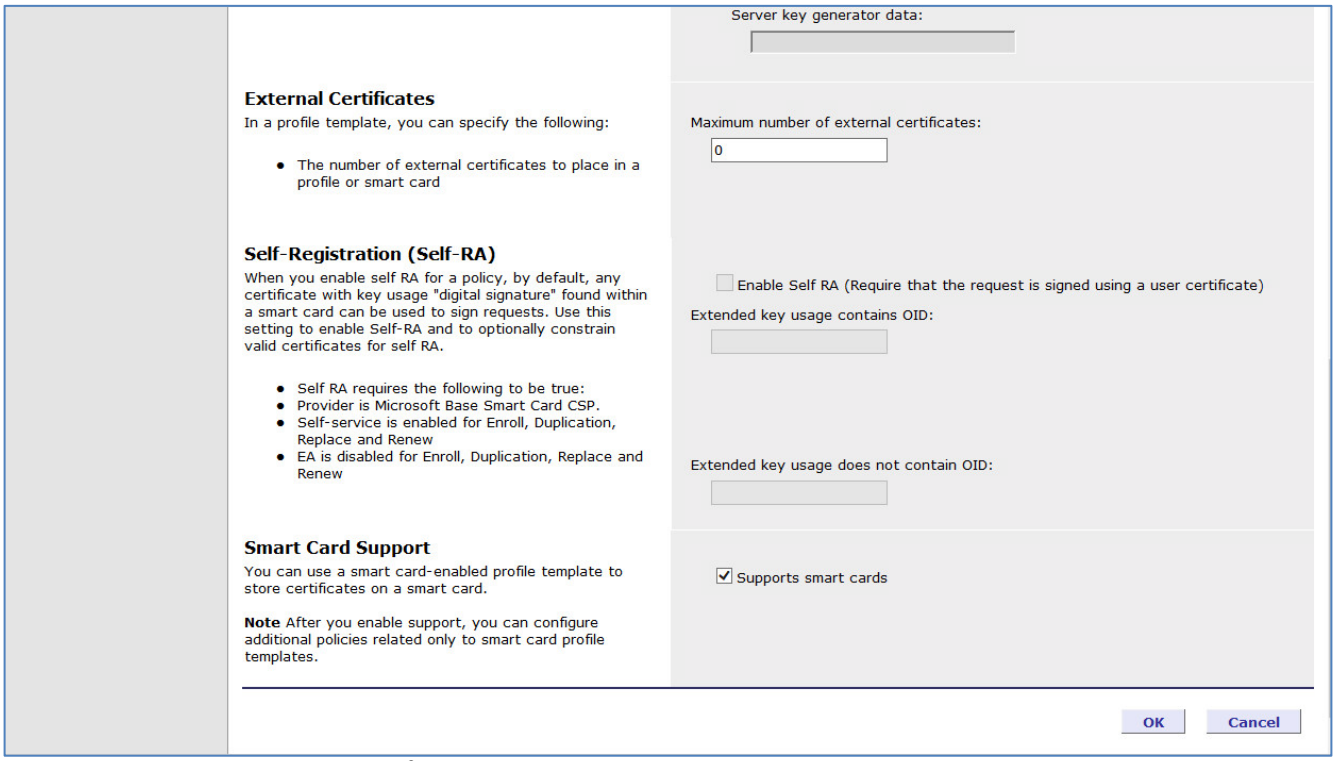
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

4. Under **General Settings**, click **Change General Settings**.



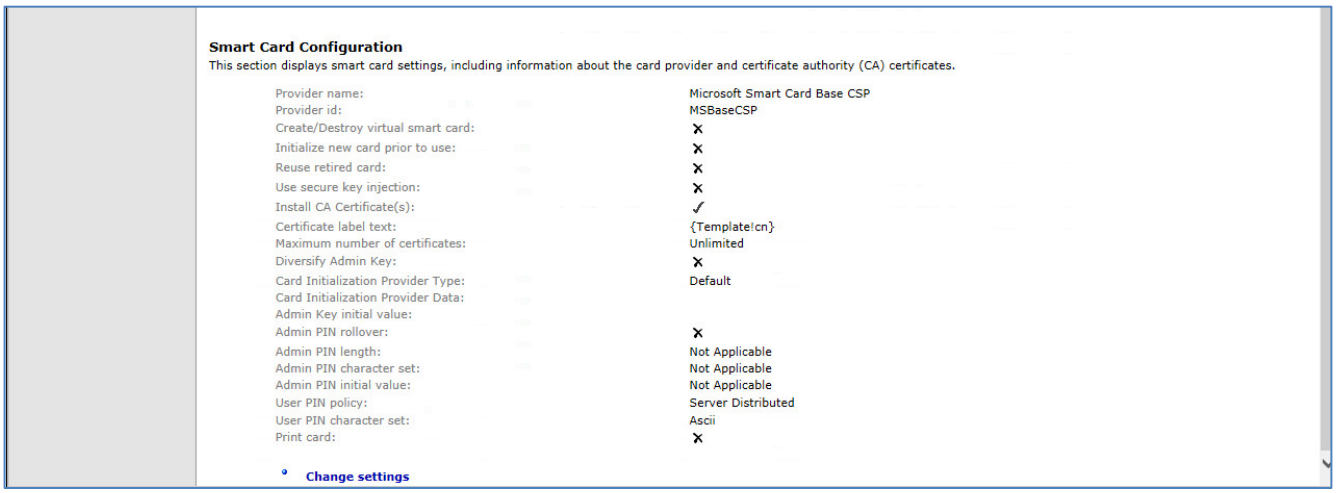
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

5. Ensure that **Supports smart cards** is selected, and then click **OK**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

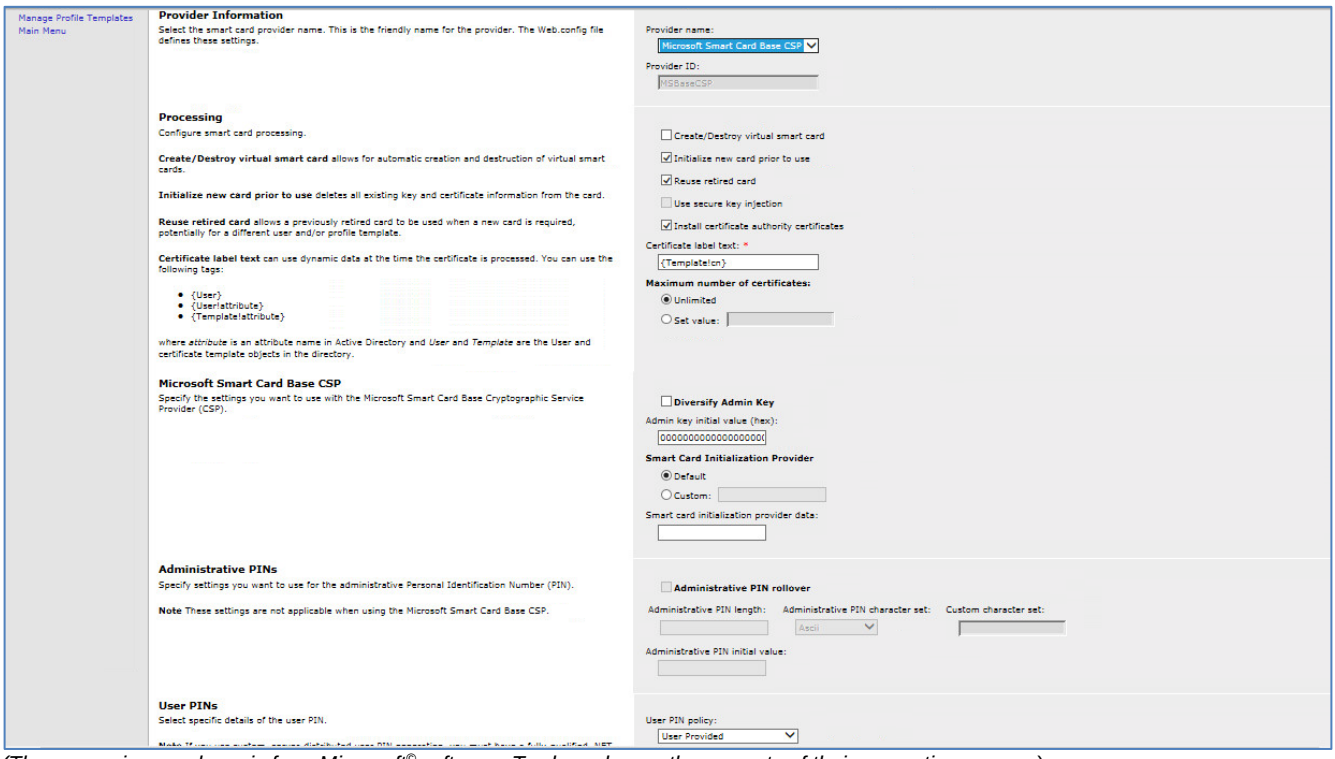
6. Under **Smart Card Configuration**, click **Change Settings**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

7. Complete the details as specified in the table below and then click **OK**.

Provider name	Select **Microsoft Smart Card Base CSP**
Initialize new card prior to use	Select this option
Reuse retired card	Select this option.
Install certificate authority certificates	Select this option.
Administrative Key initial value (HEX)	Enter the Smart Card Admin PIN initial value MD Cards (Used 48's Zero in this example.
User PIN policy	Select **User Provided**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

8. Click **OK.**

Template for Gemalto SafeNet Minidriver

The CM profile template needs to be configured with the information necessary to manage the smart card.

NOTE: To create a new profile template, copy an existing template and modify as required. Two sample templates are provided with MIM CM for this purpose. In this example “FIM CM Sample Smart Card Logon Profile Template” was copied.

Prerequisites: AdminKey.exe

The AdminKey.exe application is used to retrieve the hexadecimal-encoded value for the Admin PIN in MIM CM 2016. It generates the hexadecimal value corresponding to the value given to it. For example, if the Admin PIN of the smart card or token is 1234567890, its corresponding hexadecimal code can be obtained by running the following command:

C:\>AdminKey.exe 1234567890

Key: 1d6a4f7a652e18203e3d3b0c70451022107f7420216e611b

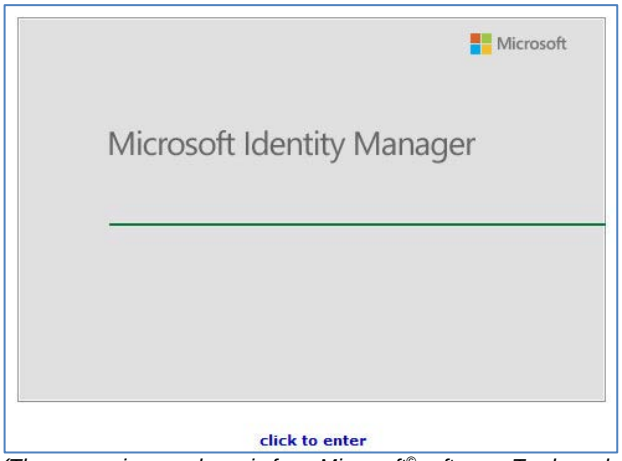
Where C:\ indicates the location of the AdminKey.exe application.

NOTE: The AdminKey.exe application is required only when you are using the FIM CM with Safenet Gemalto Minidriver, It is not required with SAC.

The AdminKey.exe application can be downloaded from the following link:

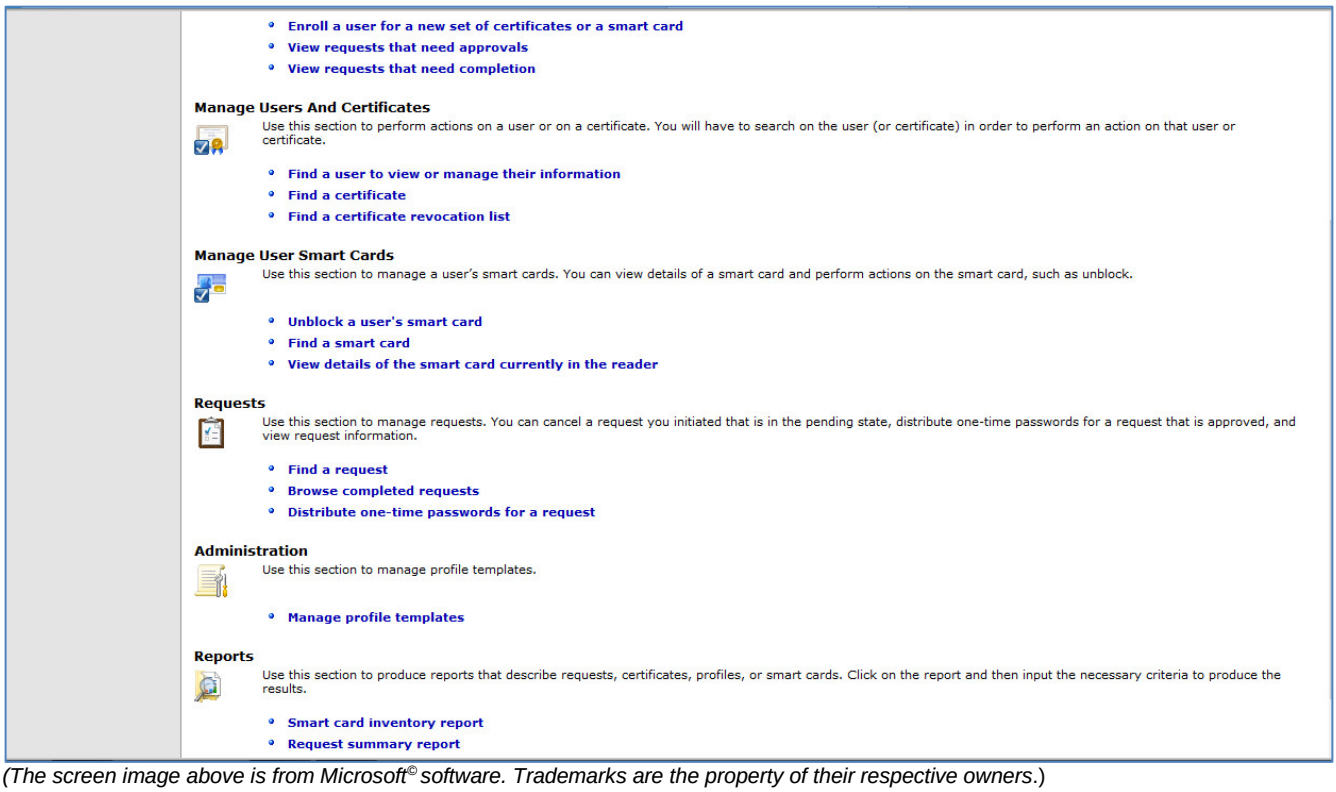
http://bel1web002:9876/Files/5207fcb449c14d078a0d66830e106a34

1. Open **MIM CM Portal** and log in as a user who has administrative privileges.



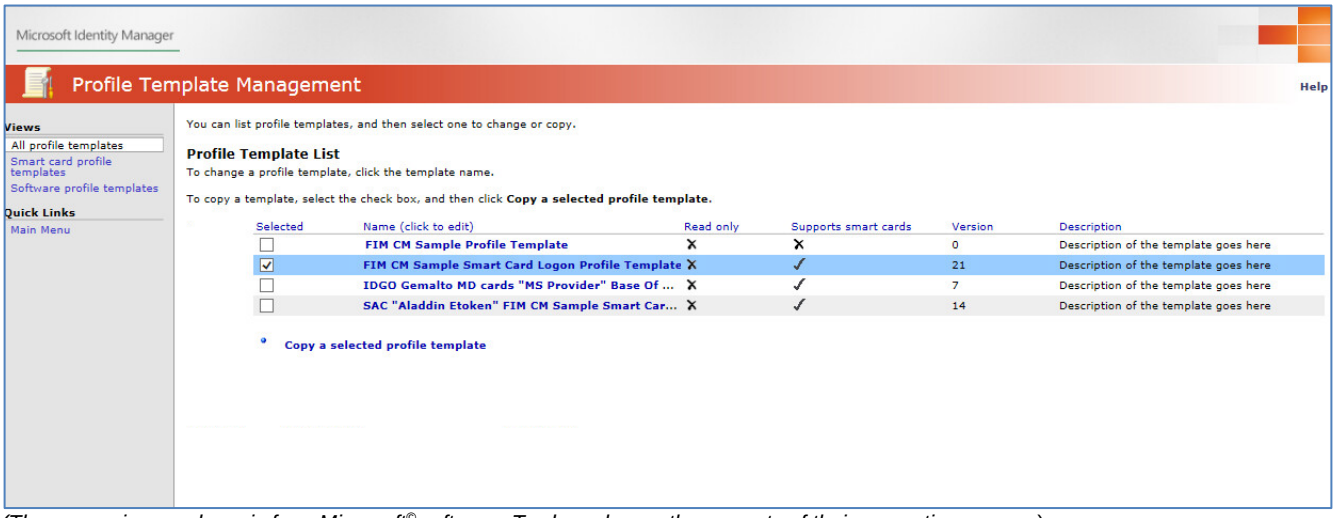
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

2. Under **Administration**, click **Manage profile templates**.



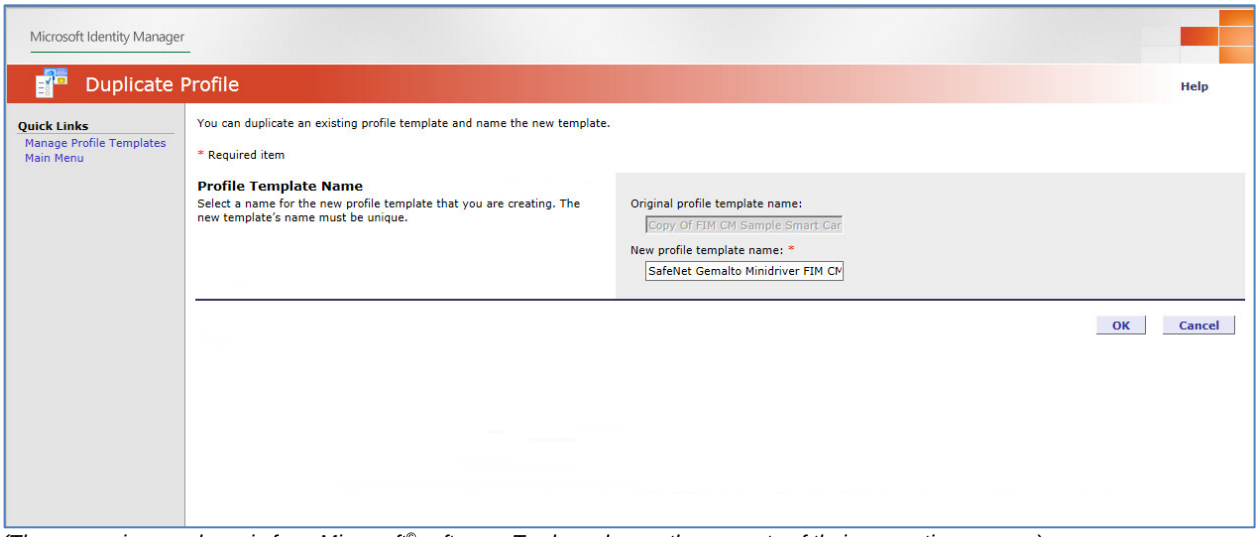
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

3. Select "FIM CM Sample Smart Card Logon Profile Template", and then click **Copy a selected profile template**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

4. In the **New profile template name** field, enter the name of the template (For example: “SafeNet Gemalto MiniDriver …”) and then click **OK**.

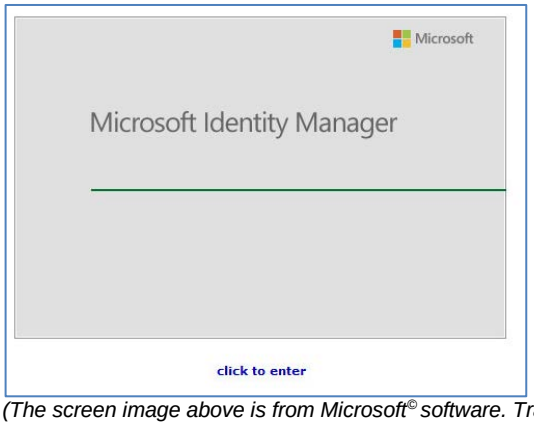


(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

Configuring a Profile Template for Gemalto SafeNet Minidriver

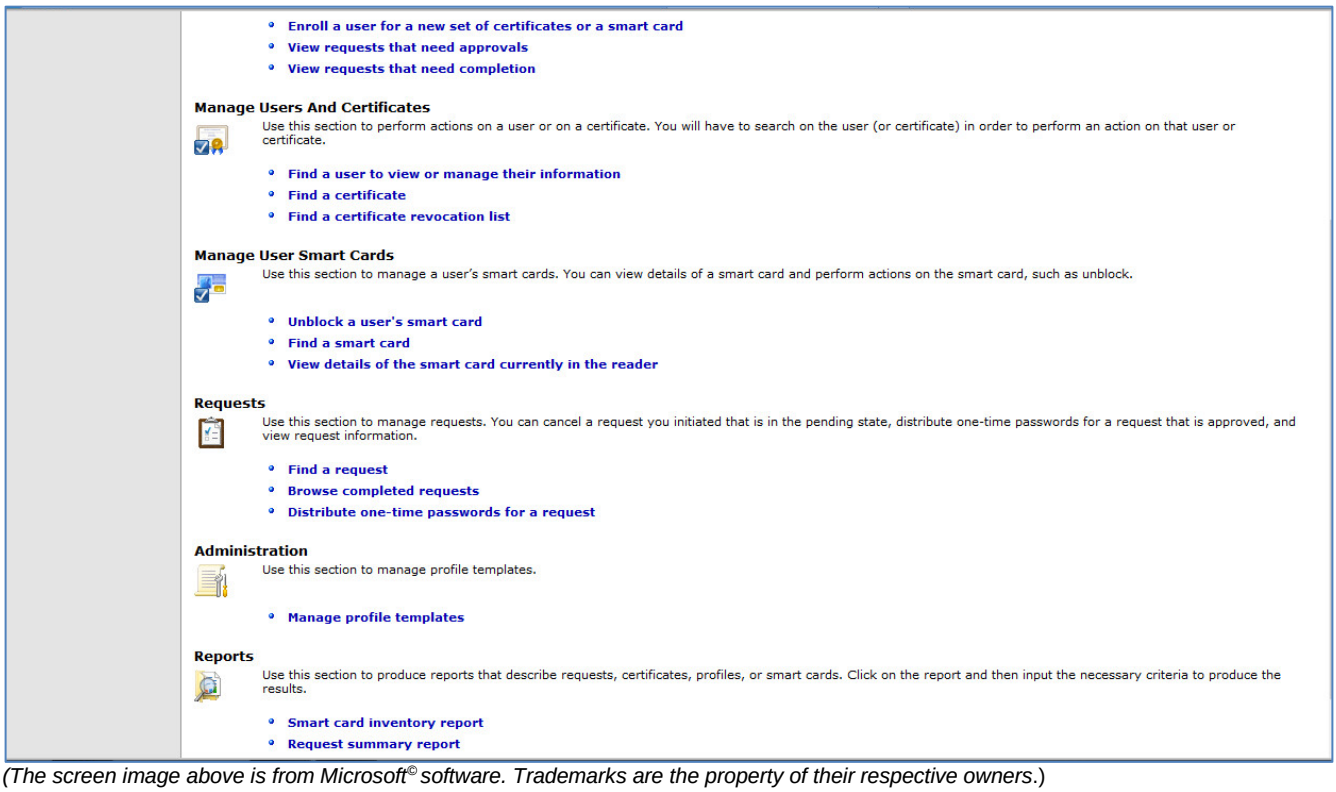
For each profile template, configure the general settings and the certificate template settings that will be used by the profile template.

1. Open **MIM CM Portal** and log in as a user with administrative privileges.



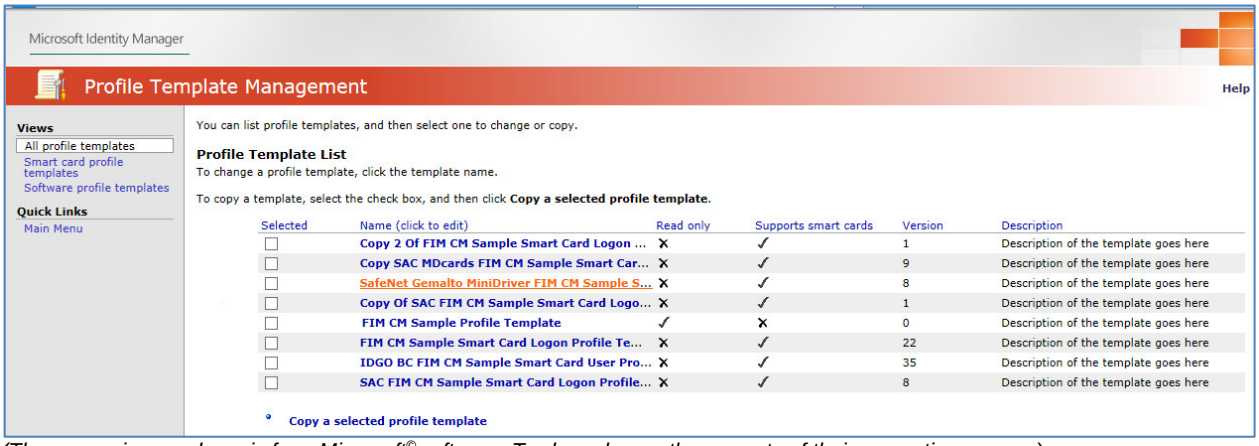
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

2. Under **Administration**, click **Manage profile templates**.



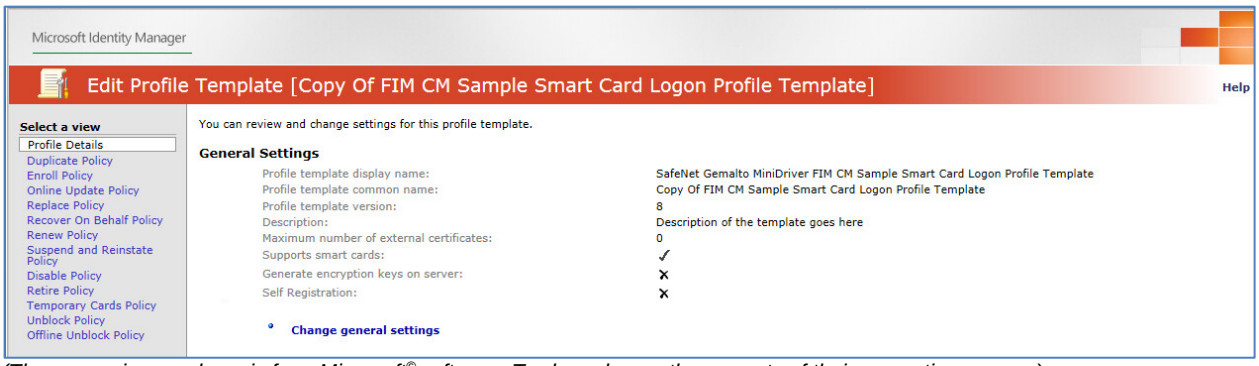
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

3. In the **Profile Template List, s**elect the template (**Example: "SafeNet Gemalto MiniDriver …"**), then click on the profile template name to edit it.



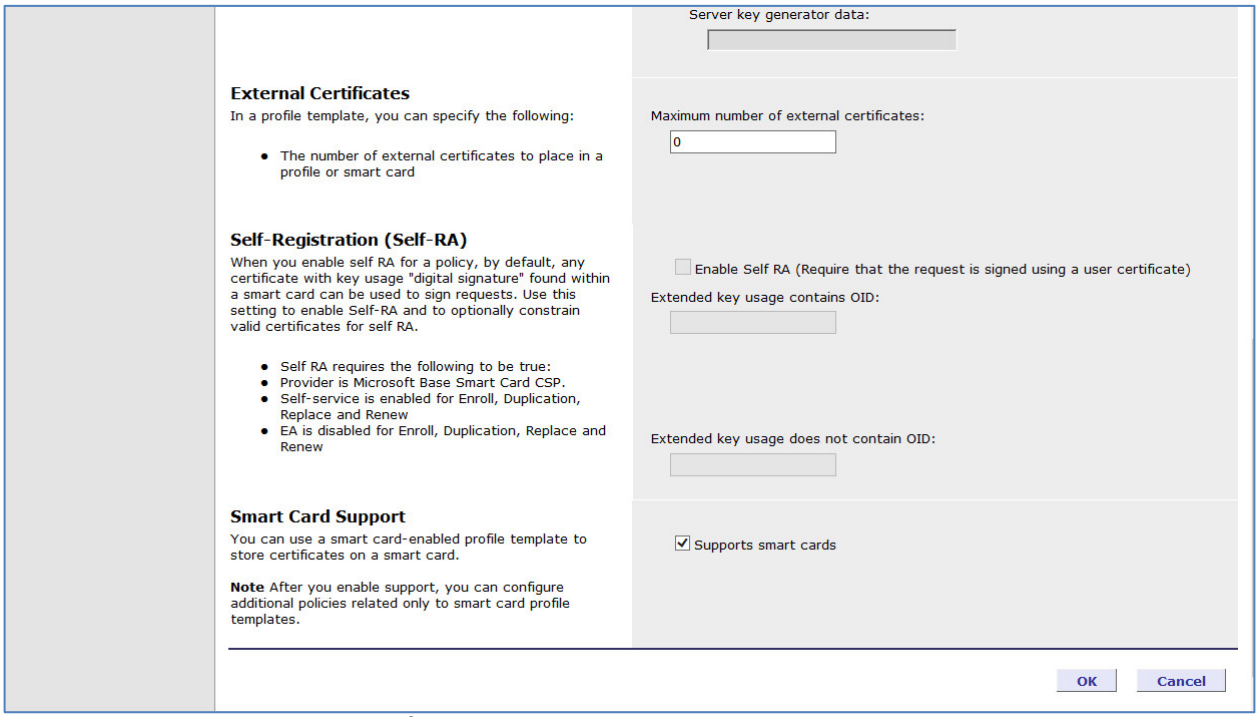
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

4. Under **General Settings**, click **Change General Settings.**



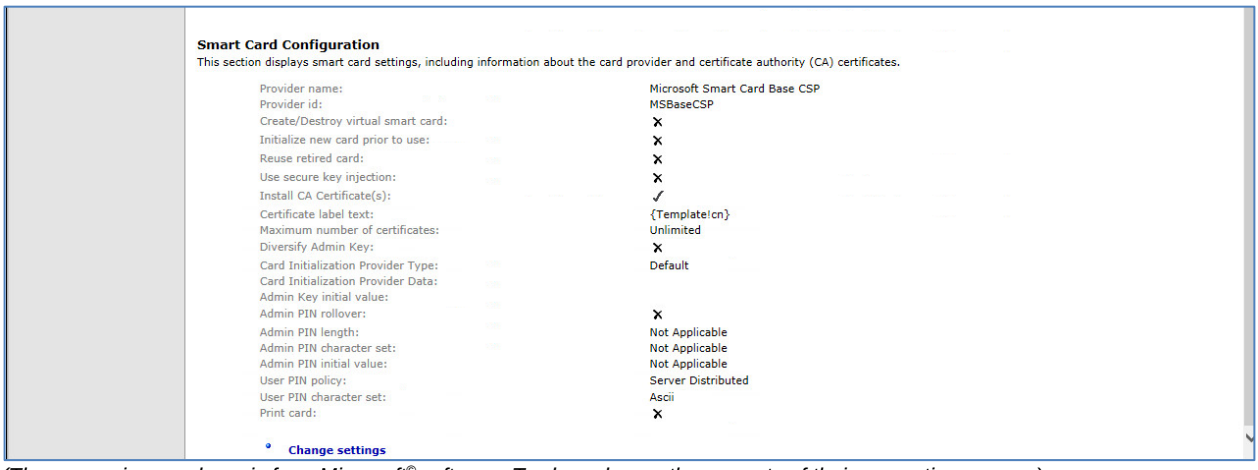
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

5. Ensure that **Supports smart cards** is selected, and then click **OK**.



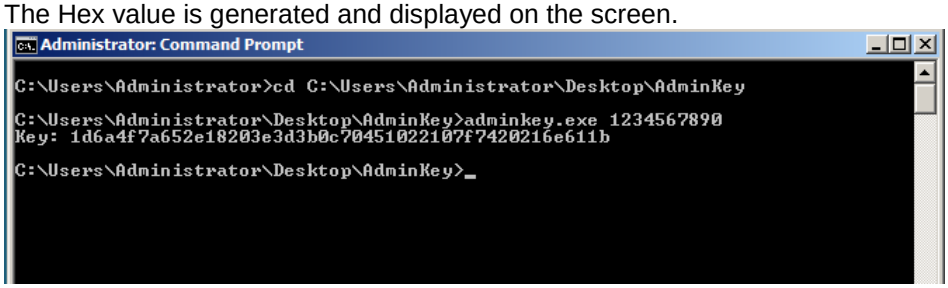
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

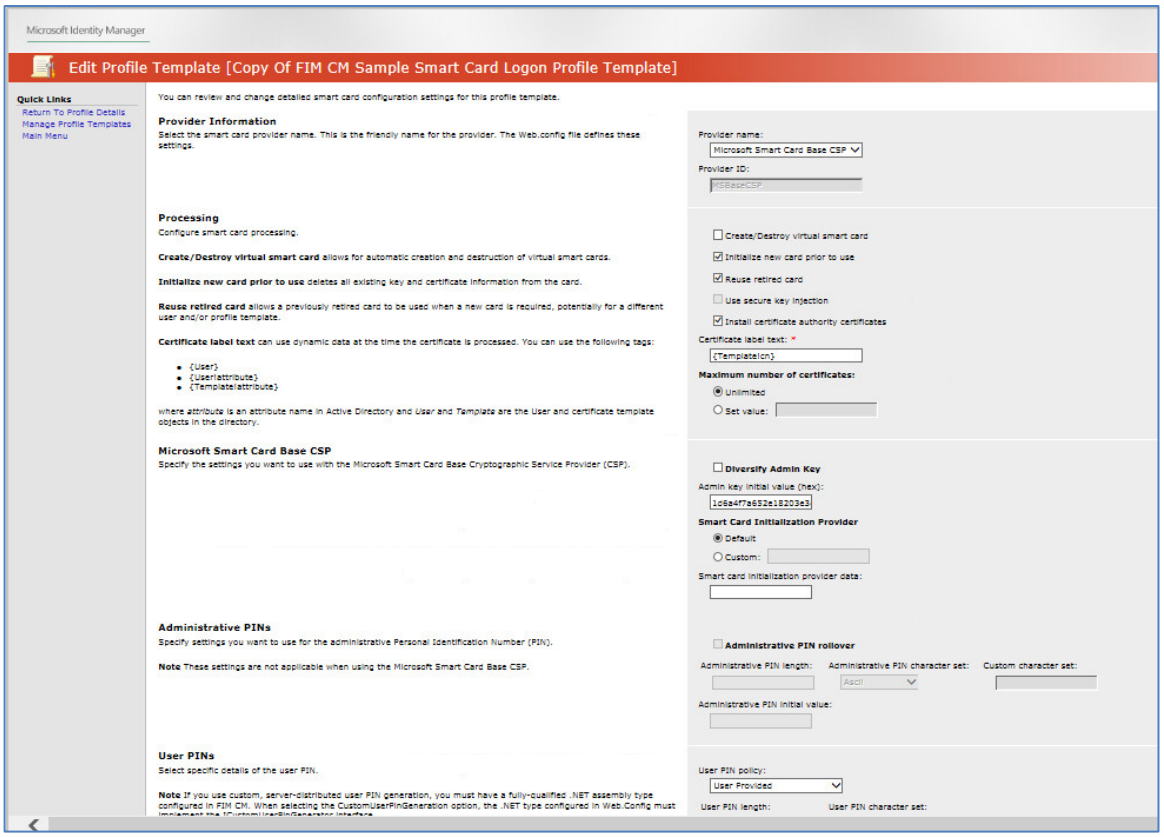
6. Under **Smart Card Configuration**, click **Change Settings**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

7. Complete the details as specified in the table below and then click **OK**.

Provider name	Select **Microsoft Smart Card Base CSP**
Initialize new card prior to use	Select this option
Reuse retired card	Select this option.
Administrative Key initial value (HEX)	Enter the hex value of Admin PIN. Follow these steps to create the Hex value: 1. Open the **Command Prompt** and browse to the location of **Adminkey.exe** application. 2. Run the **Adminkey.exe** command as below: `Adminkey.exe 1234567890` Where, 1234567890 is the Admin PIN. The Hex value is generated and displayed on the screen. 
User PIN policy	Select **User Provided**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

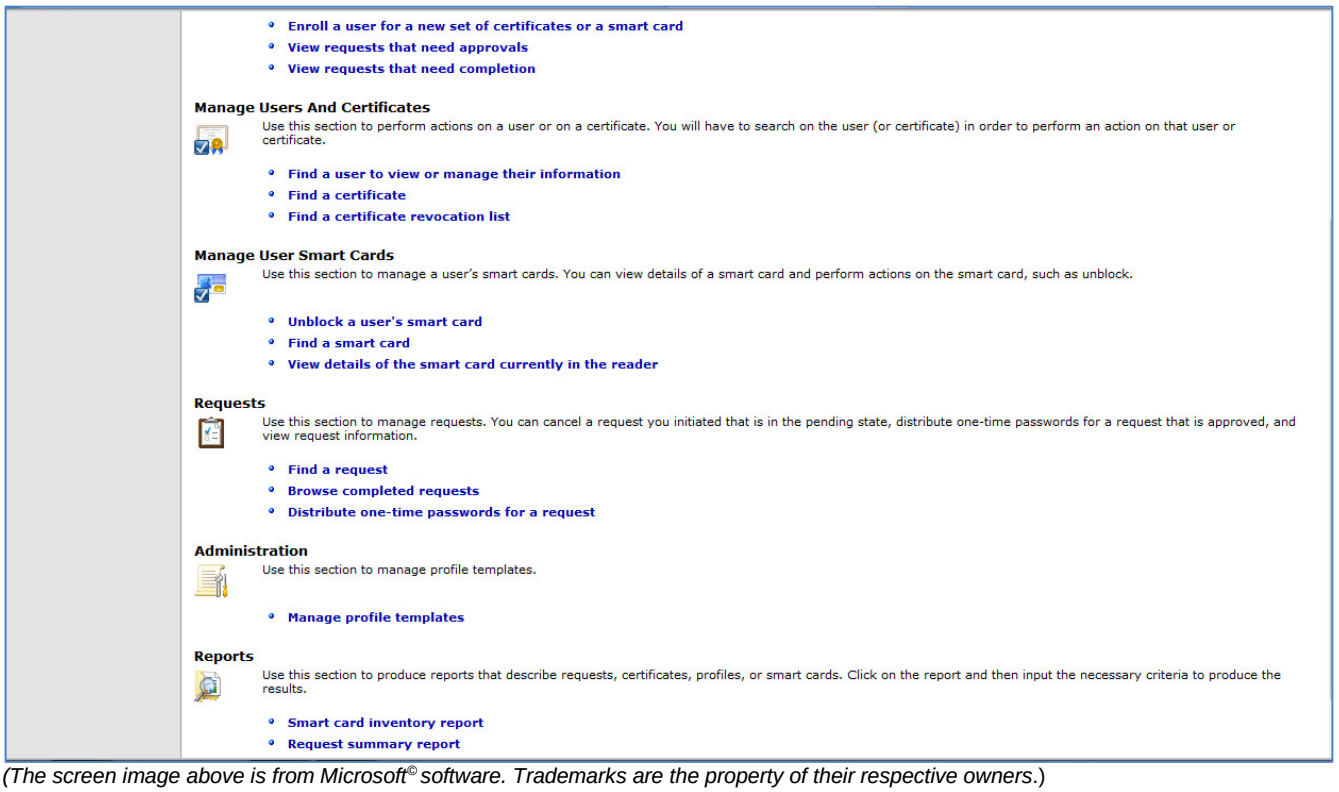
User Policy Permissions for Profile Templates

NOTE: This configuration is necessary for each policy template in order to grant the user permissions to perform operations such as Enroll, Renew, Retire, Unblock, etc. In this Example: “Enroll Policy” is demonstrated.

1. Open **MIM CM Portal** and log in as a user who has administrative privileges.

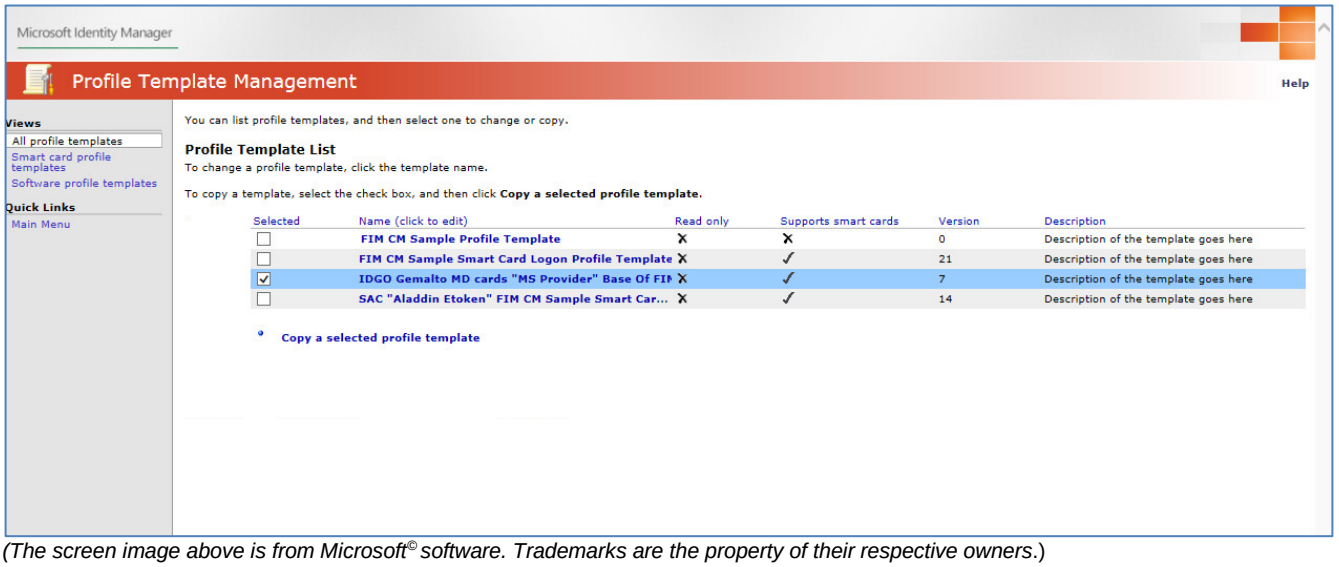
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

2. Under **Administration**, click **Manage profile templates**.



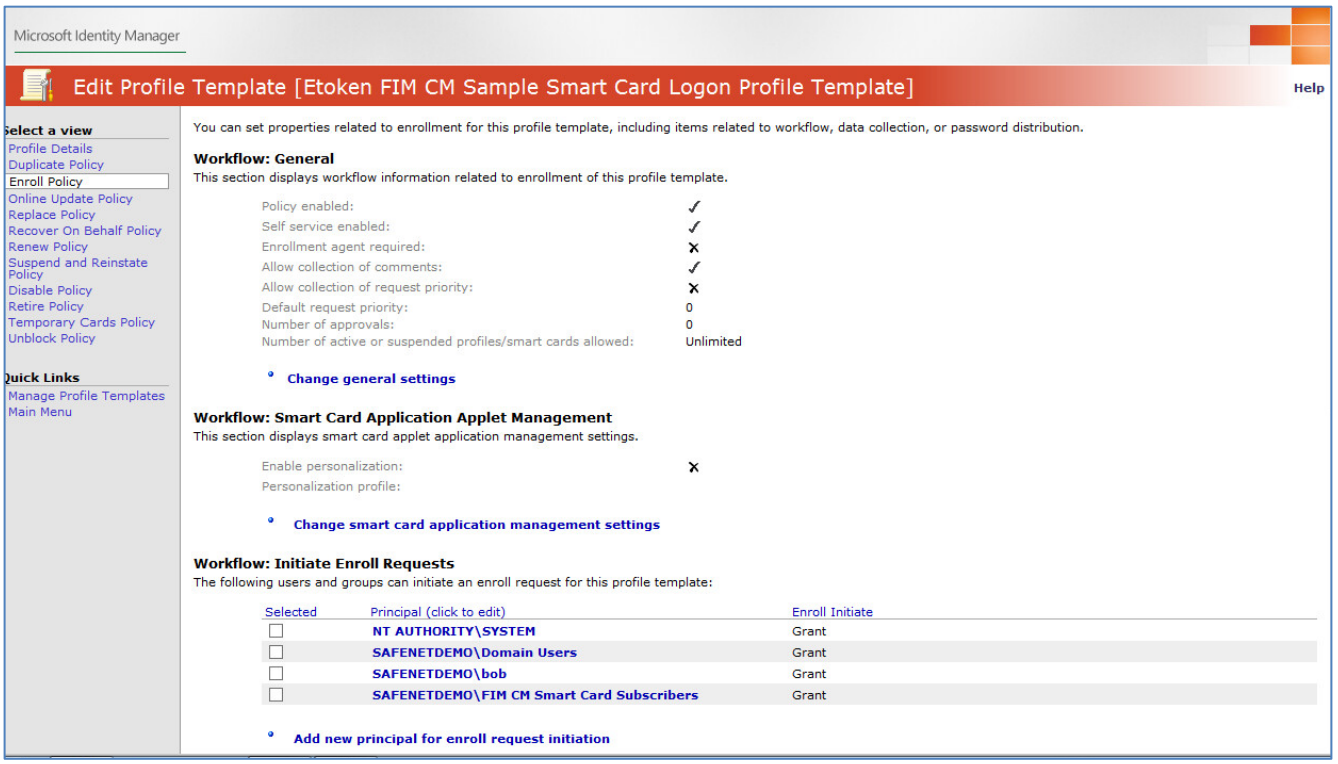
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

3. In the **Profile Template List**, select the template (example: "IDGO Gemalto MD…"), then click on the profile template name to edit it.



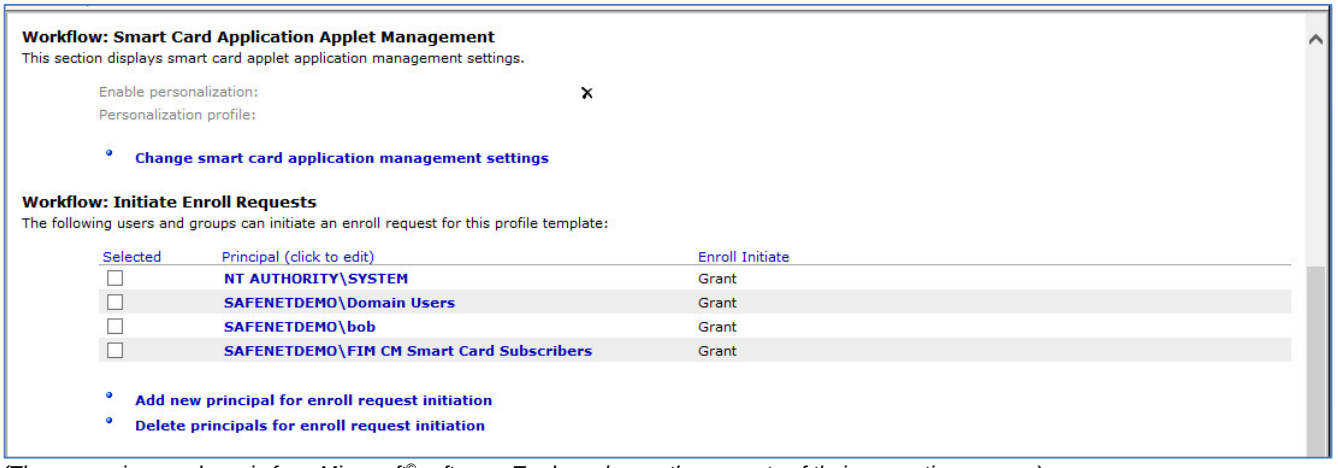
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

4. Under **Select a view** on the left pane of the **Edit Profile Template** window, click **Enroll Policy**.



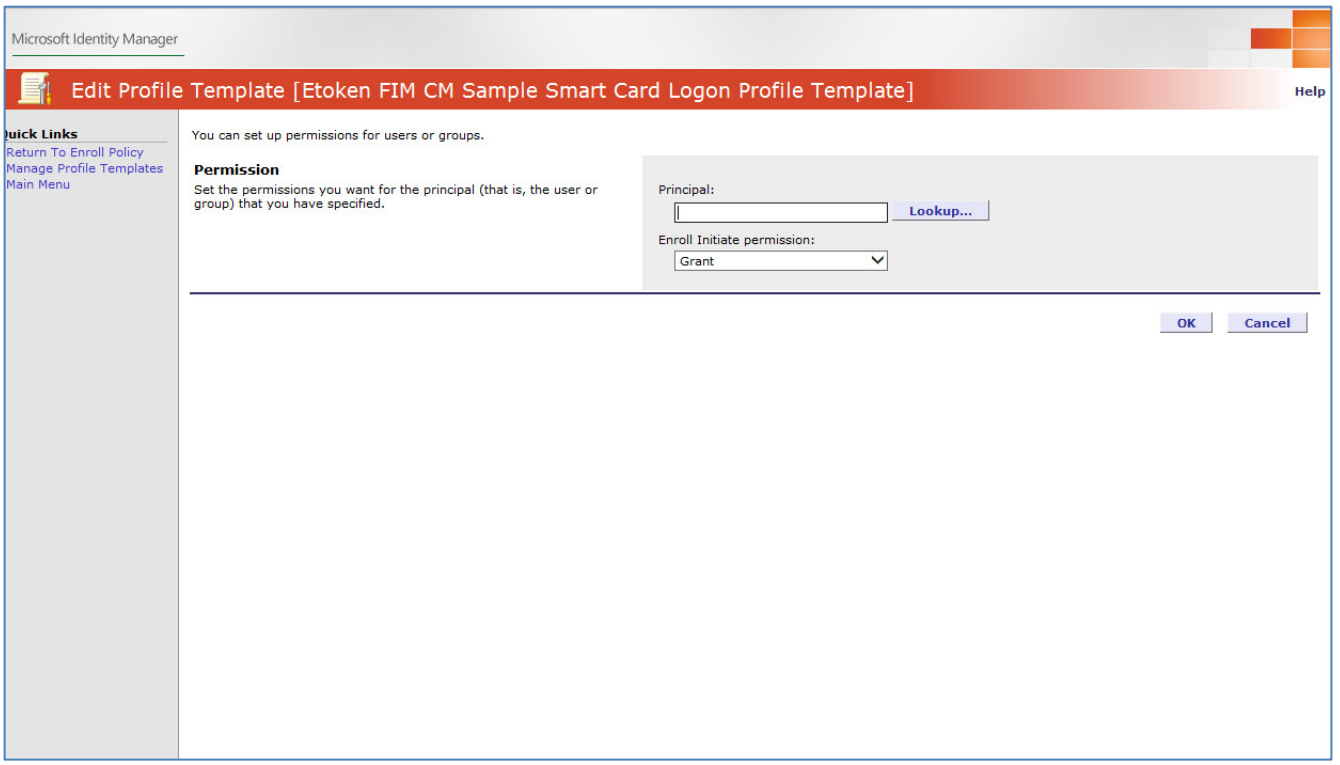
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

5. Under **Workflow: Initiate Enroll Requests**, click **Add new principal for enroll request initiation**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

6. To set permissions for the principal user or group, click **Lookup**.

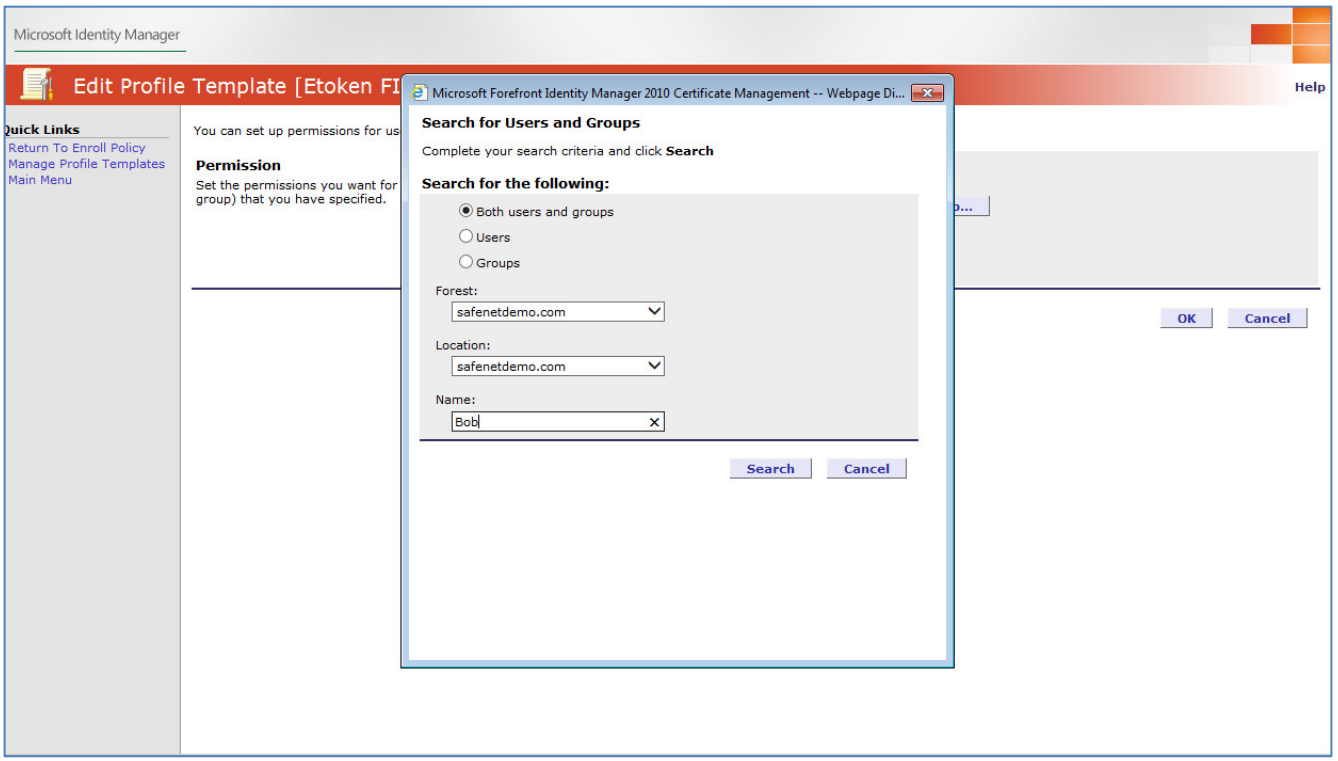


(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

7. Complete the following details:

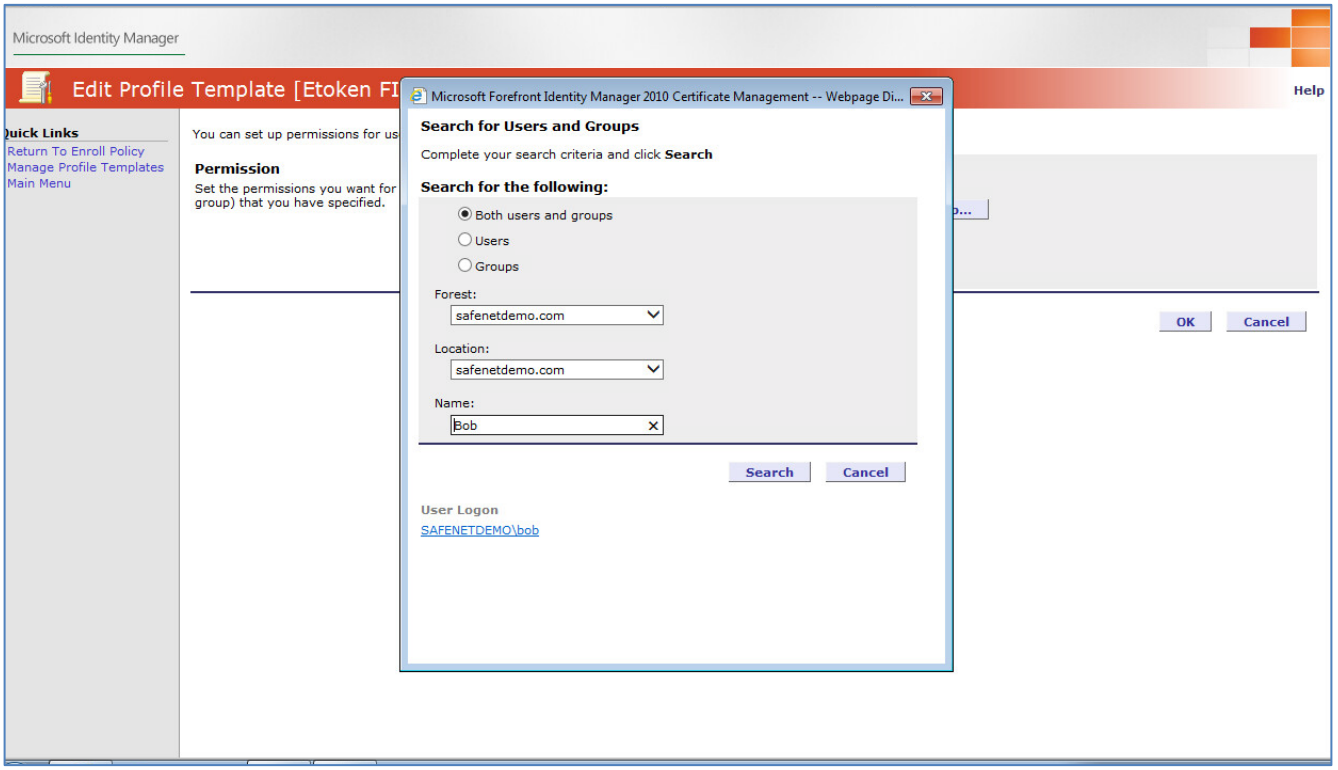
Forest	Select your domain name.
Location	Select your domain name.
Name	Enter the name of the user or group to whom you want to give permission to use the Profile Template

8. Click **Search**.



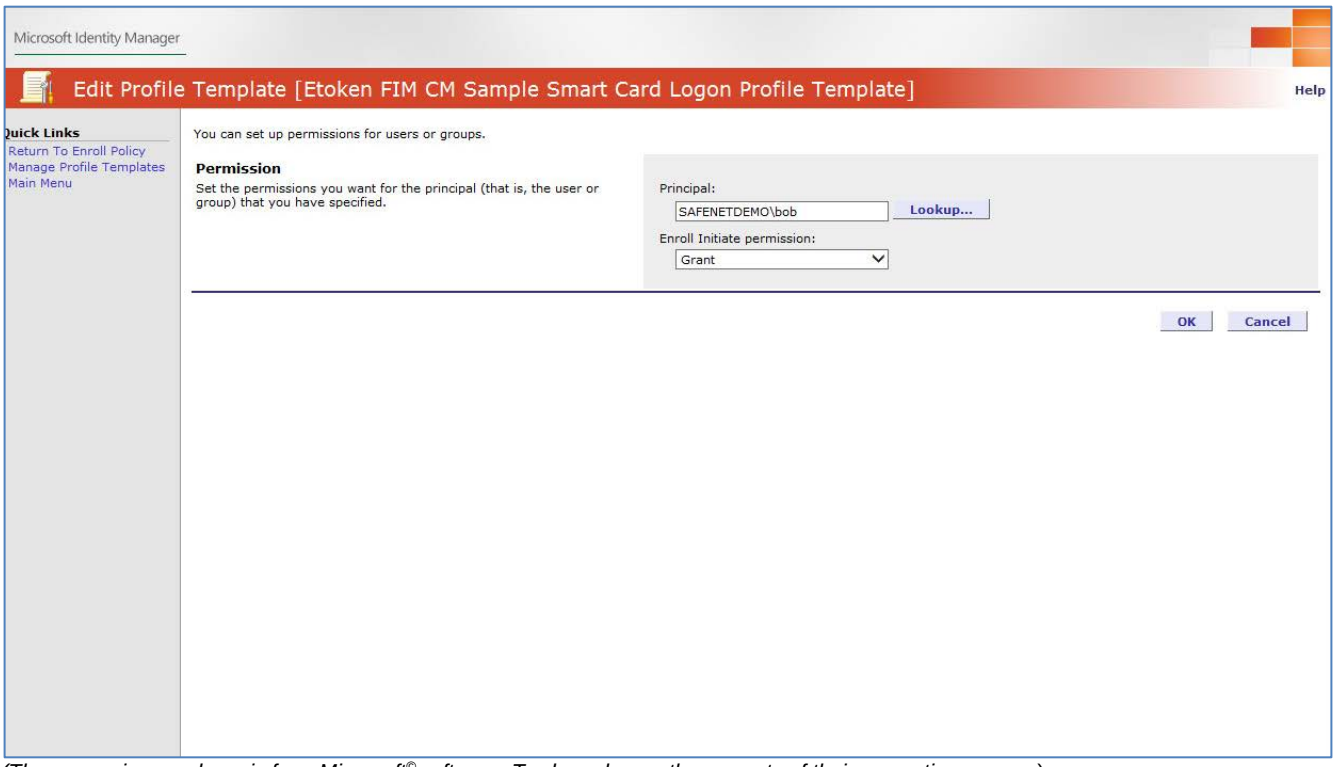
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

9. In the search result, click the user or group you want to allow.



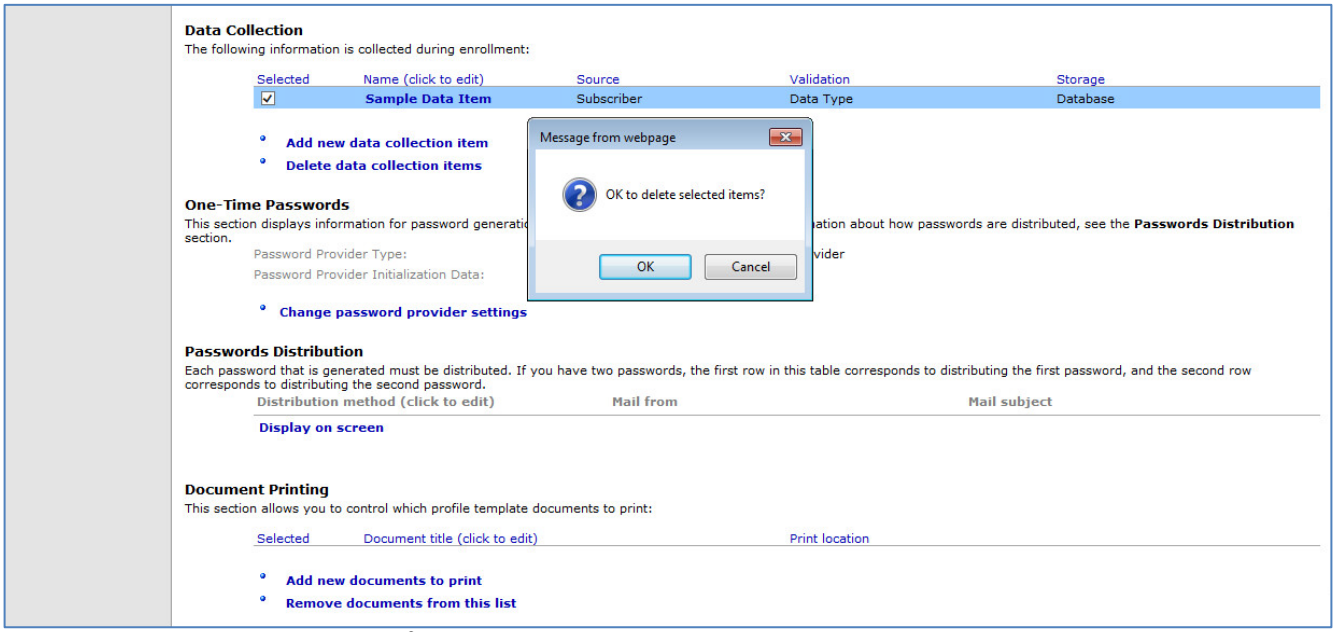
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

10. In the Enroll Initiate permission field, select **Grant** and then click **OK**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

11. In the example: "**Enroll policy"**, under "**Data Collection"**, do the following:
    a. Select the **Sample Data Item** option.
    b. Click **Delete data collection items**.
    c. Click **OK** to confirm deletion of the selected items.

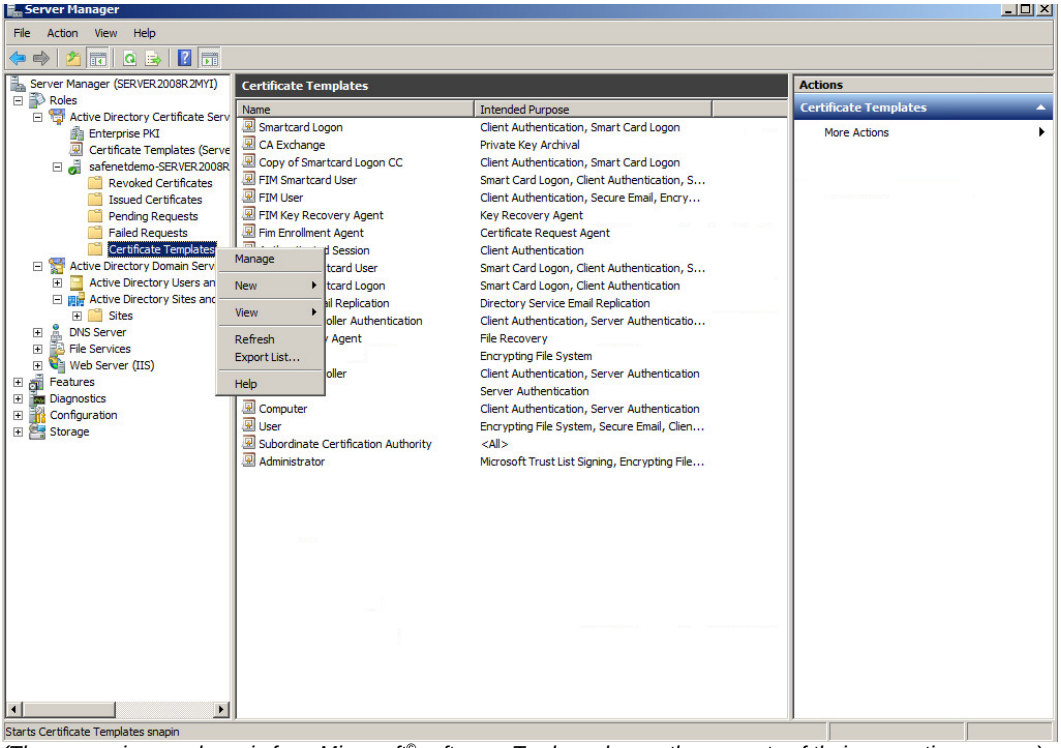


(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

Assigning the MIM CM Subscriber User Group Permission on the Smart Card Certificate Template

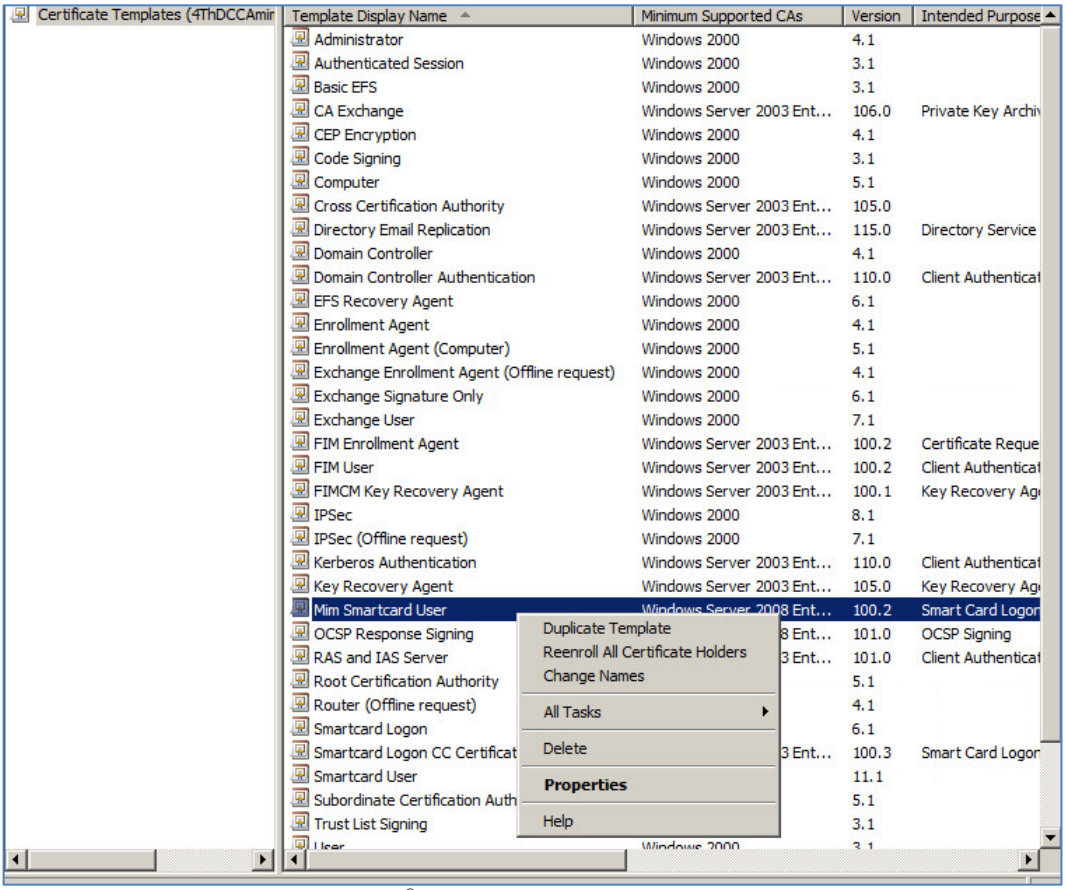
In this example, the MIM CM Subscriber group is created, containing the users that will use MIM. In the CA assign the MIM CM Subscriber group permissions on the previously created “Smart Card User Certificate Template”.

1. Click **Start > Administrative Tools > Server Manager**.
2. In the left pane, select **Roles > Active Directory Certificate Services > Certificate Templates**.
3. Right click on **Certificate Templates**, then click **Manage.**



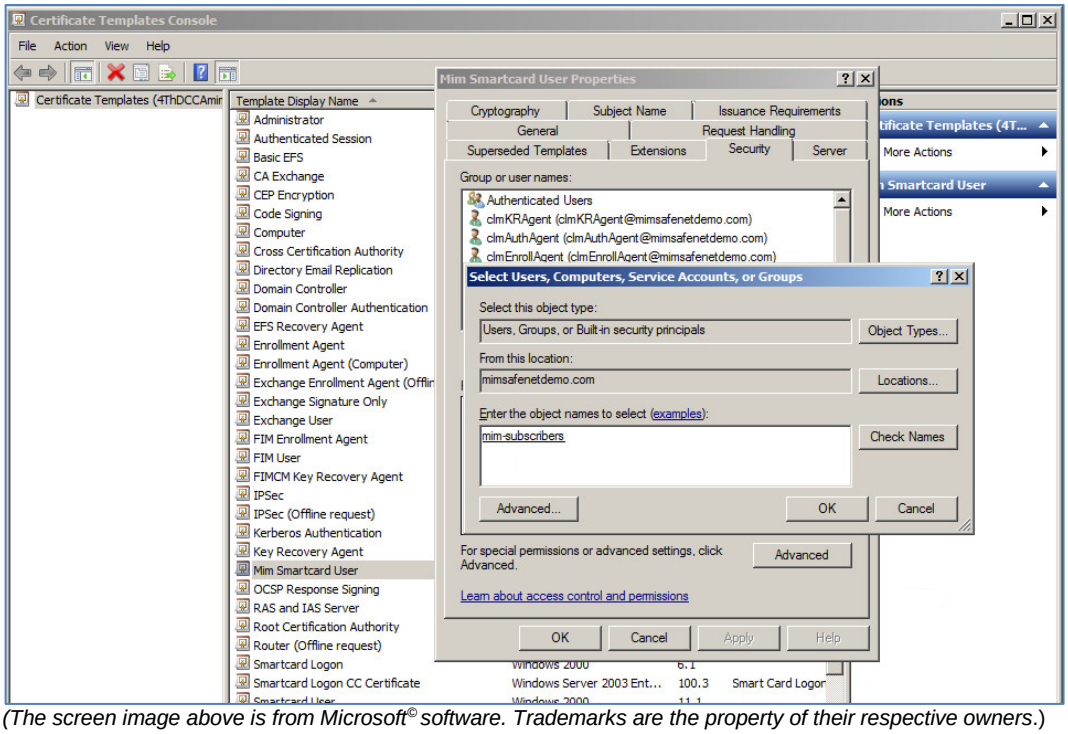
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

4. In the right pane, right-click the duplicated Smart card user template (In this example: "**Mim Smartcard User")** and select **Properties**.



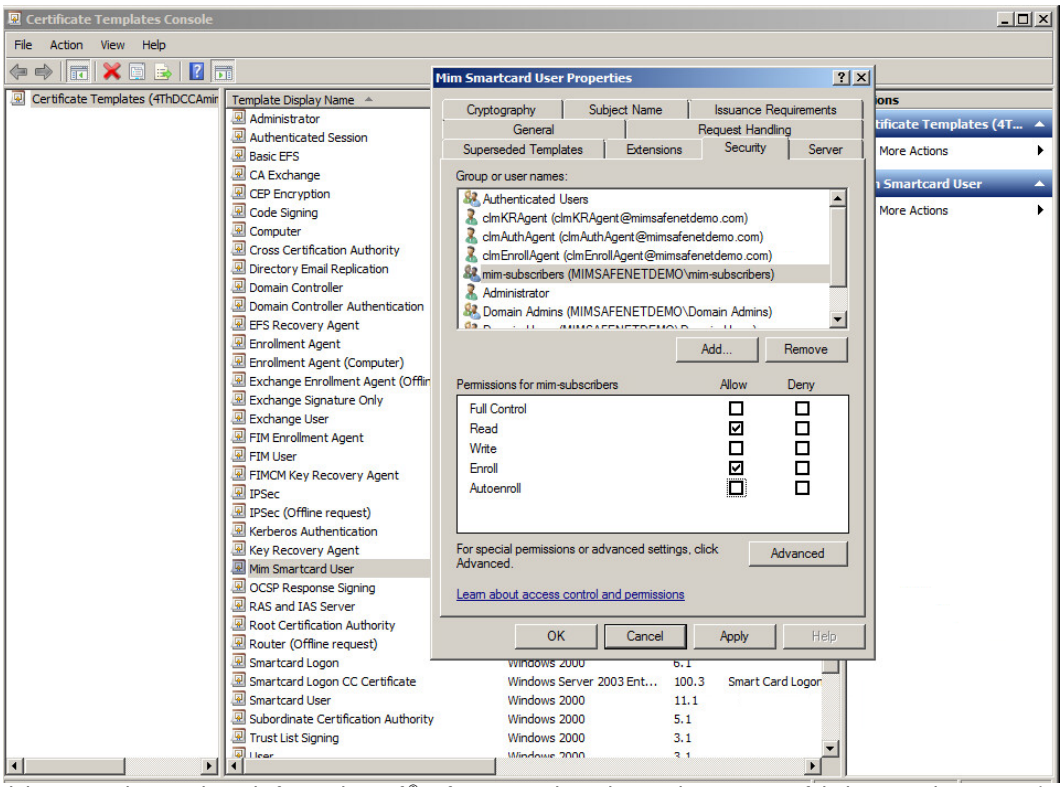
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

5. On the **Security** tab, click **Add**.
6. In the text box below **Enter the object names to select (examples)**, enter **mim-subscribers** and then click **Check Names**. This should resolve with underlined text. Click **OK**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

7. In the **Permissions for MIM CM Subscribers** list, in the **Allow** column, select **Read** and **Enroll**, then click **OK**.

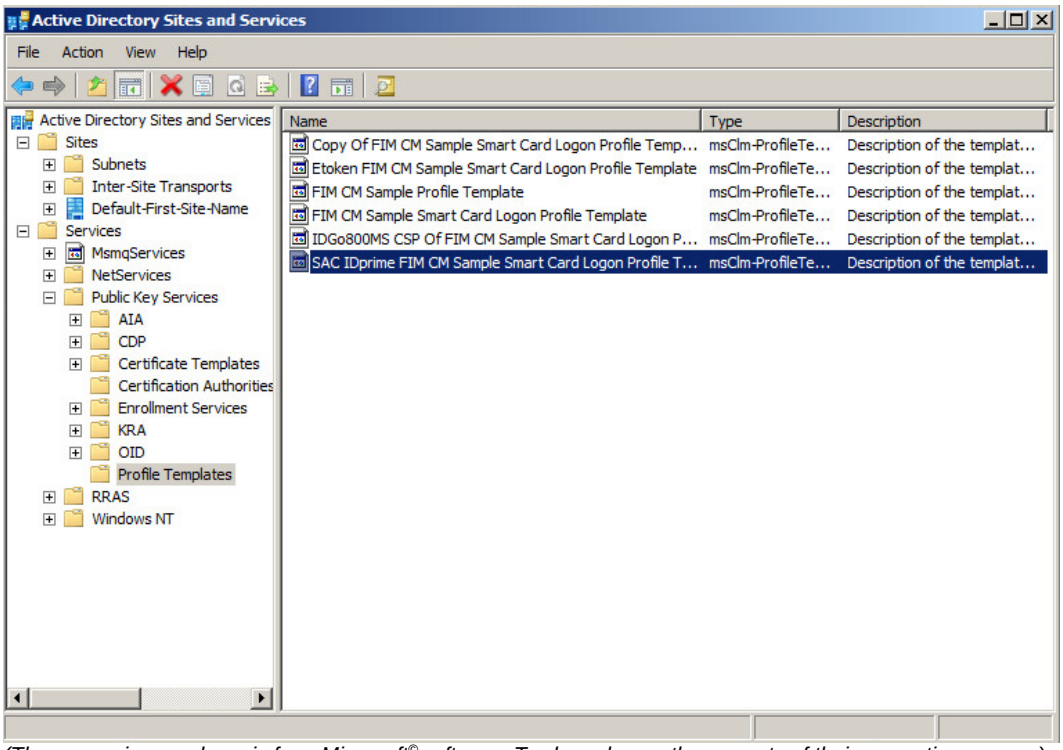


(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

Assigning the MIM CM Subscriber User Group Permission on the Profile Template

To assign the MIM CM Subscriber group permission on the Smart Card Profile Template:

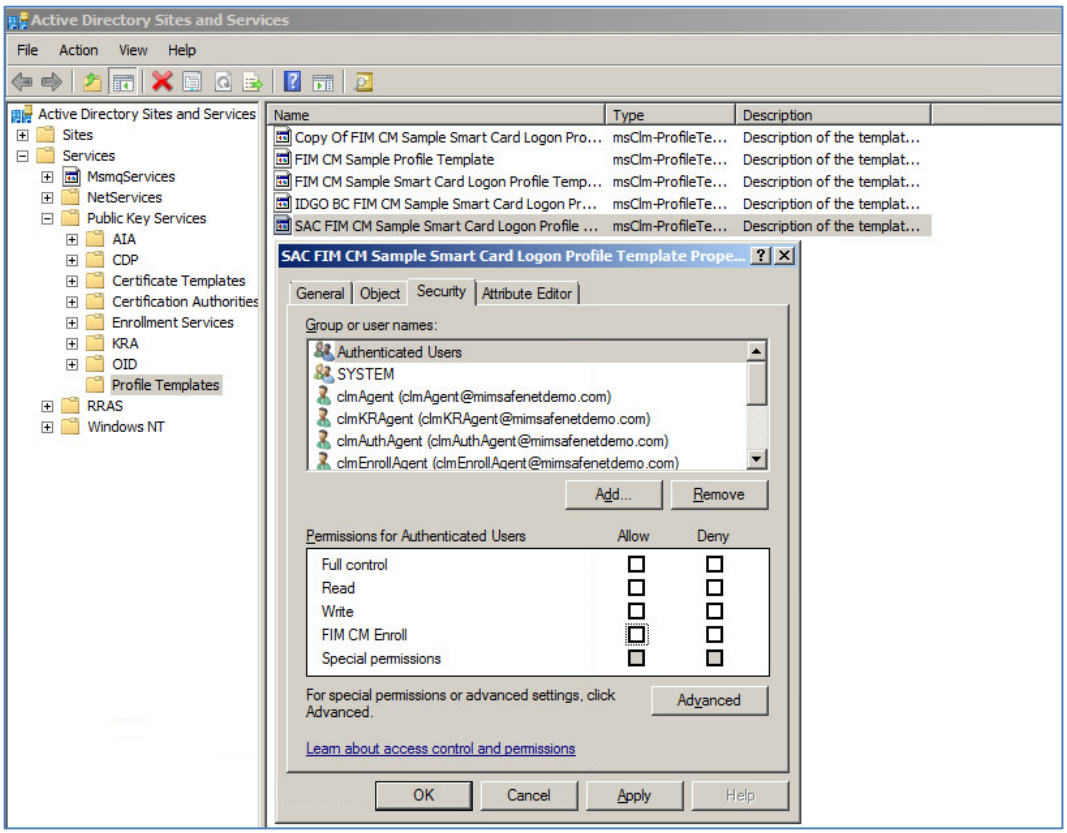
1. Click **Start > Administrative Tools > Active Directory Sites and Services**.
2. On the **View** menu, select **Show Services Node**.
3. In the left pane, click **Services > Public Key Services > Profile Templates**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

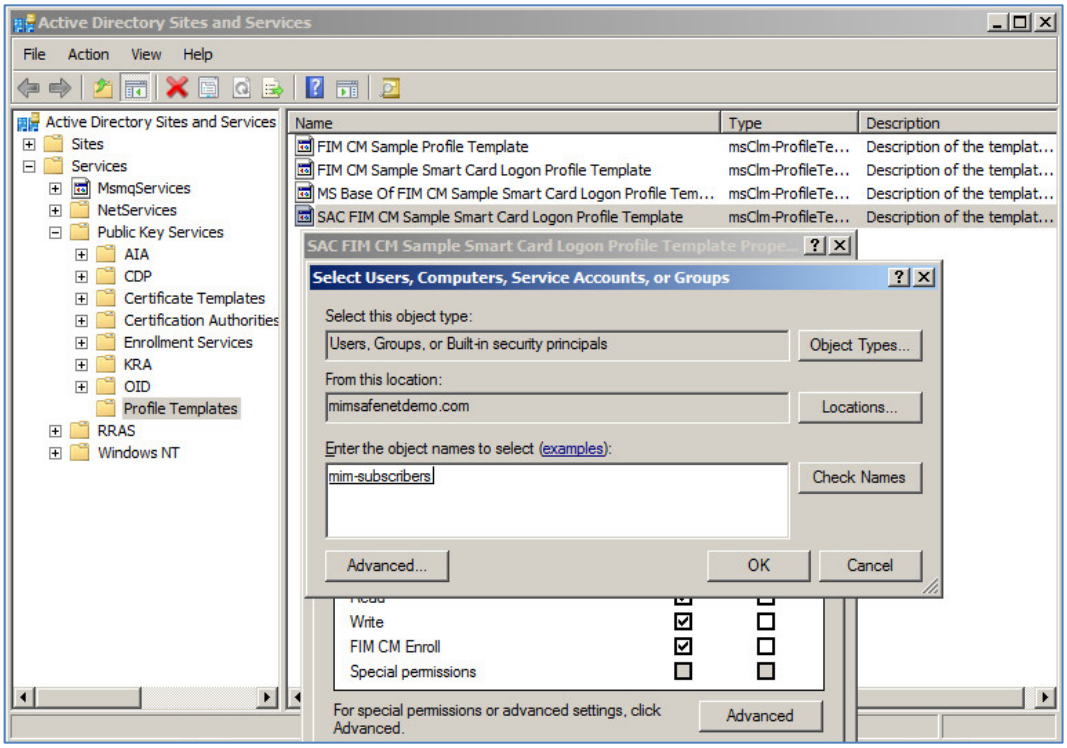
4. In the right pane, right-click the profile template you have created (in this example, SAC IDprime MIM CM Smart Card Logon Profile Template) and select **Properties**.

5. On the Security tab, click **Add**.



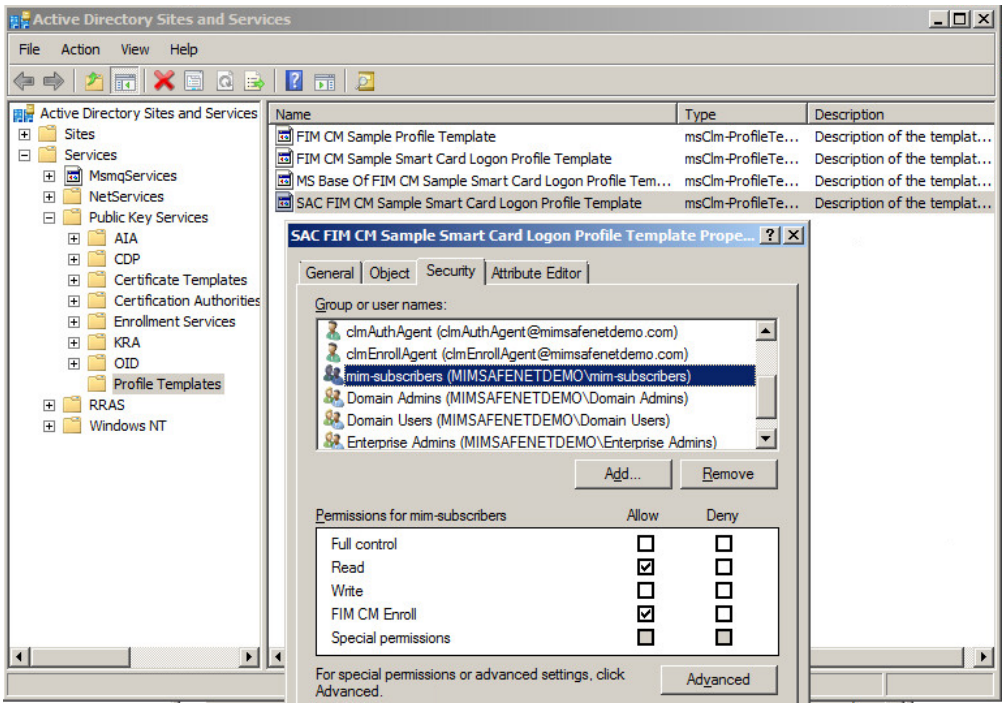
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

6. In the text box below **Enter the object names to select (examples)**, enter mim-subscribers and then click **Check Names**. This should resolve with an underlined text. Click **OK**.

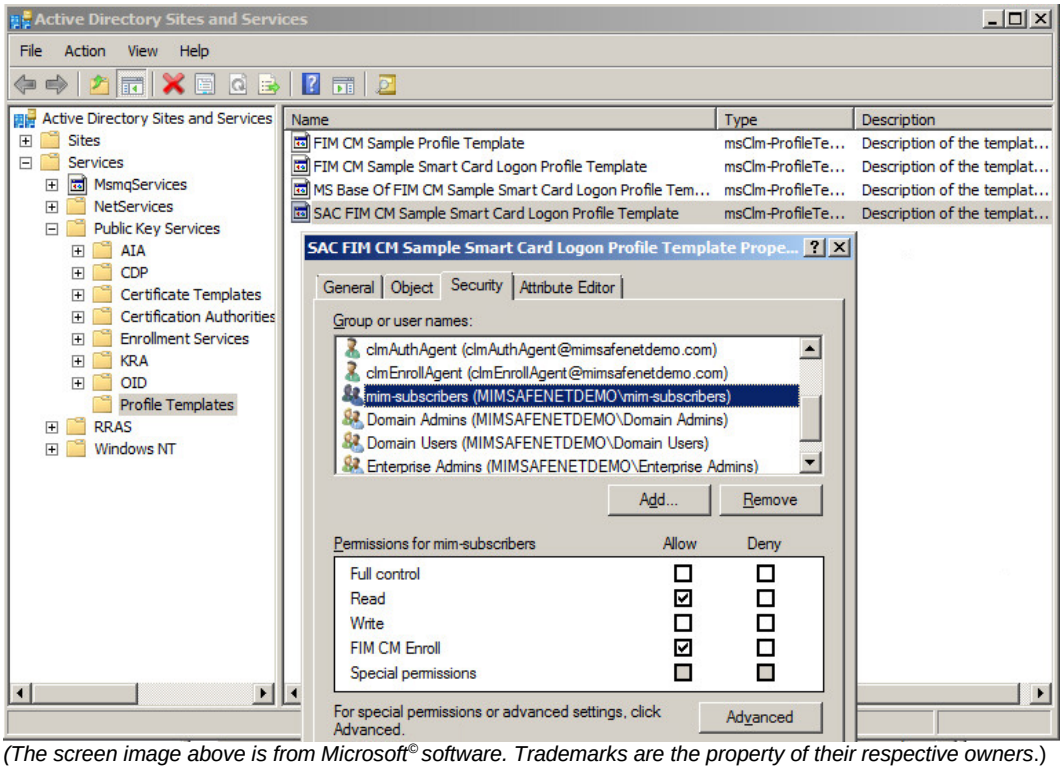


(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

7. Under group or user names, select **MIM CM Subscribers**.



8. Under **Permissions for mim-subscribers**, in the **Allow** column, select **Read** and **FIM CM Enroll**. Click **OK**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

Client Side Configuration

Editing the Registry for SAC

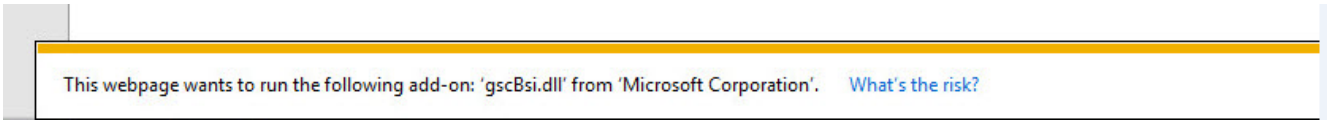
When using SAC as a middleware application, some changes are required in the Windows Registry on the client side.

1. Run regedit.exe.
2. Click **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > SafeNet > SAC**.
3. Right-click **SAC** and then click **New > Key**.
4. In the **Name** field, enter init.
5. Right-click init and then click **New > DWORD (32-bit) Value**.
6. Specify **ignoreopensessions** as a name and **1** as its value.
7. Close the Registry Editor.

Important Notes

Enable ActiveX

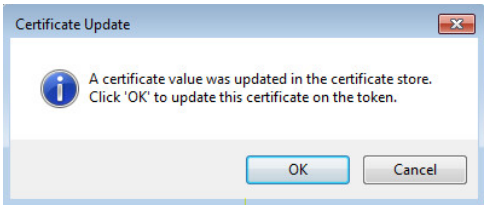
In this example, Internet Explorer 11 was demonstrated. ActiveX must be enabled for the MS dll installation



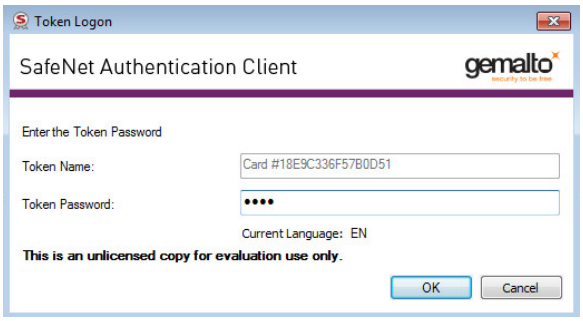
MIM "Renew this Smart Card" Option - Update Certificate Status from Valid to Archived State

When performing renew smart card with IDPrime MD cards with SAC installed, and when using the MIM Profile template **Aladdin eToken Provider**, to ensure that the certificate updates certificate status from **Valid** to **Archived** state, perform the following step during renew flow:

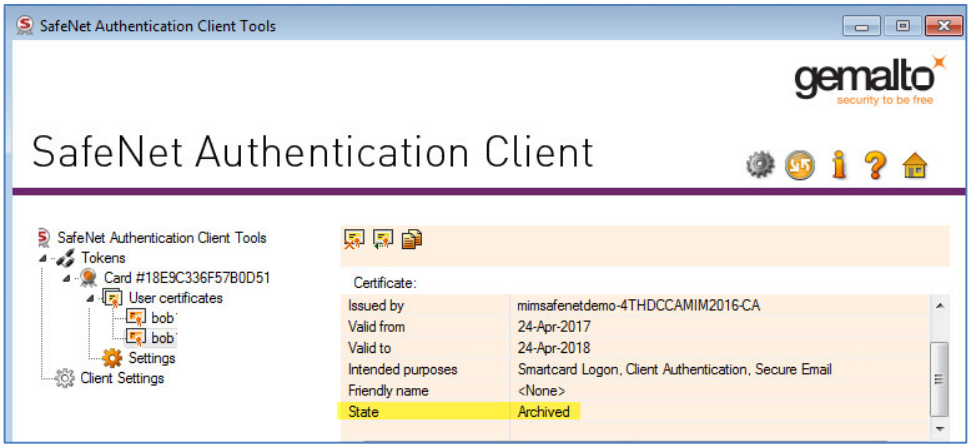
1. Click OK on Certificate update



2. In the **Token Logon** window, in the **Token Password** field, enter the smart card PIN and click **OK**.



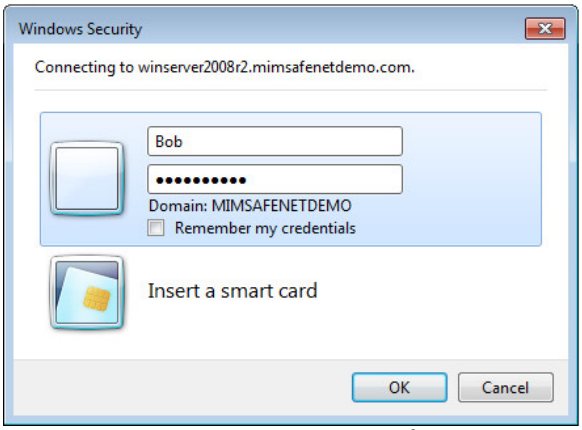
The certificate state is updated from **Valid** to **Archived**.



Running the Solution

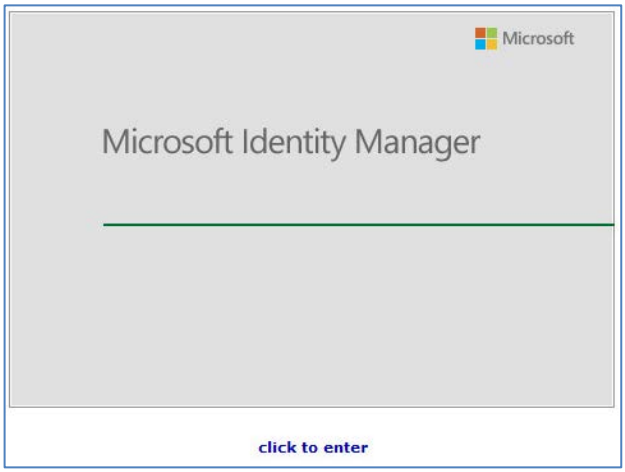
Enrolling a Certificate

1. Open Internet Explorer and enter the MIM CM Portal url https://Server/certificatemanagement
2. Enter the user name and domain password, and then click **OK**.



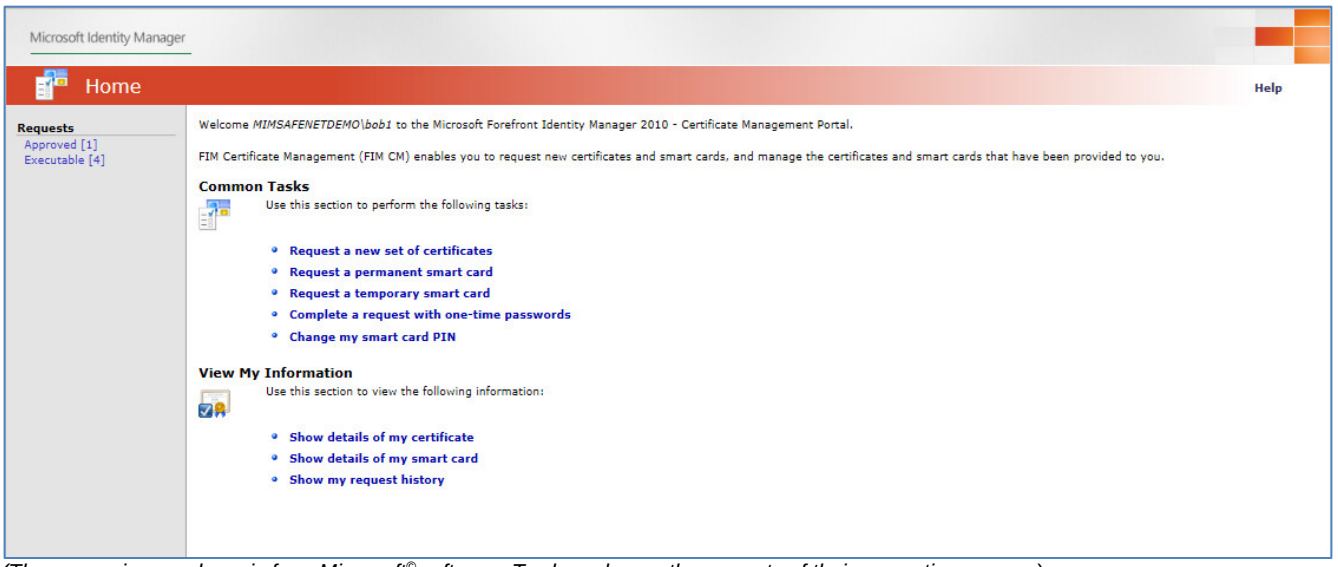
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

3. Click **click to enter**.



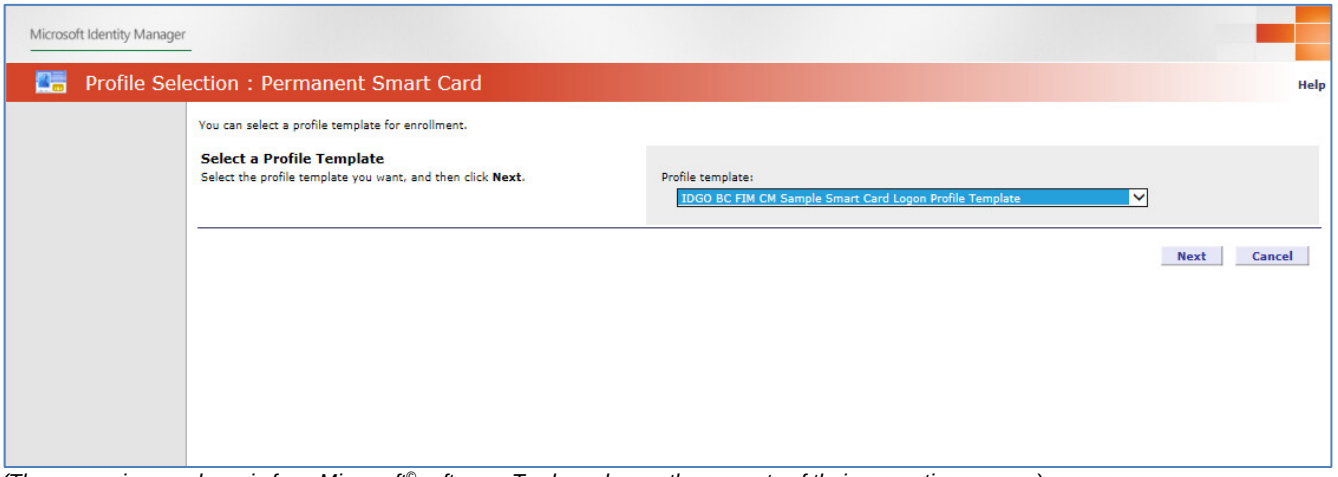
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

4. Select **Request a permanent smart card**



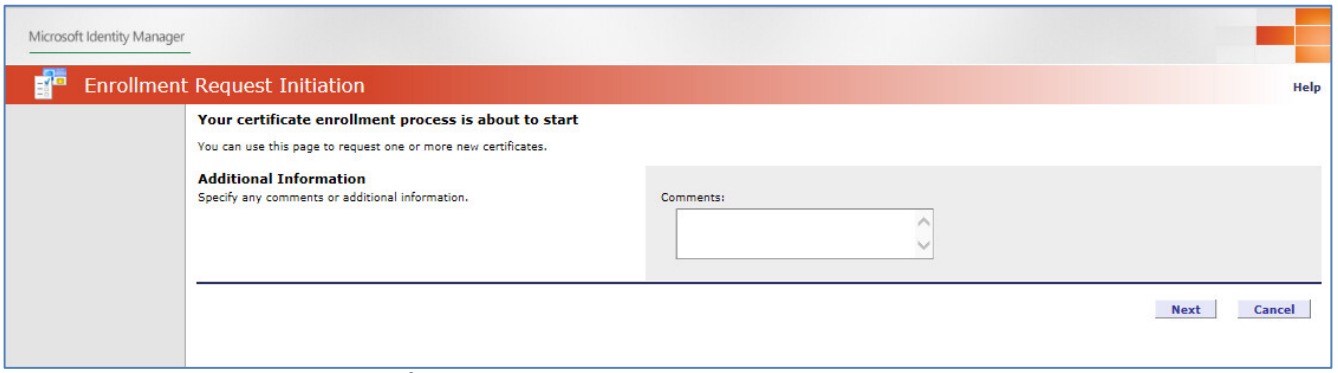
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

5. In the **Profile template** field, select your profile template (**IDgo Bc** in this example) and then click **Next**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

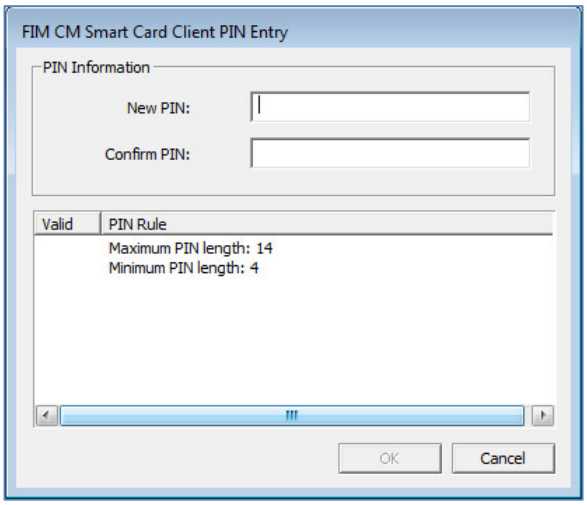
6. Insert the smart card on which you want to enroll the certificate, and on the **Enrollment Request Initiation** page, click **Next**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

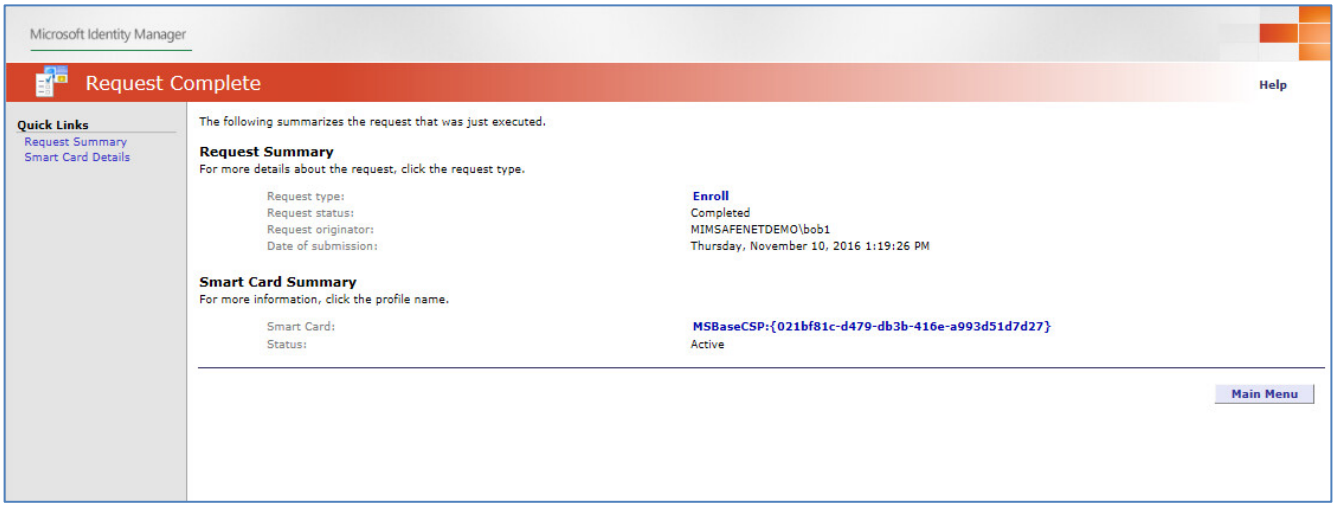
7. On the Creating certificate request window, enter a **new user PIN** in the **New PIN** and **Confirm PIN** fields. Click **OK** to continue.

> **NOTE:** The minimum or maximum password length of the Token or Smart Card is aligned to MIM CM.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

8. On successful completion of the certificate request, the **Request Complete** window is displayed



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

9. The certificate is now enrolled to the token/Smart Card.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information
Customer Support Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.
Technical Support contact email	technical.support@gemalto.com