SafeNet Authentication Client Integration Guide

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



All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto 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 Gemalto 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.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-013827-001, Rev. A Release Date: July 2017

Contents

Third-Party Software Acknowledgement
Description4
Applicability
Environment5
Audience
Enrollment Flow using SafeNet Authentication Client
Prerequisites
Supported Tokens and Smart Cards in SafeNet Authentication Client
Supported Tokens/Smart Cards in Microsoft Identity Manager 2016 SP1 CM8
Configuring Microsoft Identity Manager 2016 SP1 CM9
Template for SAC9
Template for IDGO 800 Mini Driver Backward compatibility16
Template for Gemalto SafeNet Minidriver23
User Policy Permissions for Profile Templates
Assigning the MIM CM Subscriber User Group Permission on the Smart Card Certificate Template35
Assigning the MIM CM Subscriber User Group Permission on the Profile Template
Client Side Configuration
Editing the Registry for SAC41
Running the Solution
Enrolling a Certificate43
Support Contacts

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

SafeNet Authentication Client: Integration Guide

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.

SafeNet Authentication Client: Integration Guide

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 certificatebased 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.

SafeNet Authentication Client: Integration Guide

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
	Aladdin eToken	SafeNet Authentication client 10.3
*** eToken 5110 GA	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 Microsoff[®] software. Trademarks are the property of their respective owners.)

2. Under Administration, click Manage profile templates.

Enroll a user for a new set of certificates or a smart card
 View requests that need approvals
• View requests that need completion
Manage Users And Certificates
Use this section to perform actions on a user or on a certificate. You will have to search on the user (or certificate) in order to perform an action on that user or certificate.
 Find a user to view or manage their information
• Find a certificate
Find a certificate revocation list
Manage User Smart Cards
Use this section to manage a user's smart cards. You can view details of a smart card and perform actions on the smart card, such as unblock.
Unblock a user's smart card
 Find a smart card
View details of the smart card currently in the reader
Requests
Use this section to manage requests. You can cancel a request you initiated that is in the pending state, distribute one-time passwords for a request that is approved, and view request information.
Find a request
Browse completed requests
Distribute one-time passwords for a request
Administration
Use this section to manage profile templates.
Manage profile templates
Reports
Use this section to produce reports that describe requests, certificates, profiles, or smart cards. Click on the report and then input the necessary criteria to produce the results.
Smart card inventory report
Request summary report

(The screen image above is from Microsoff[®] 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.

Microsoft Identity Manager	_					-	
Profile Terr	nplate Manageme	int					Help
Views All profile templates Smart card profile templates Software profile templates	You can list profile template Profile Template List To change a profile template To copy a template, select	es, and then select one to change or copy. ; te, click the template name. the check box, and then click Copy a selected profile tem	plate.				
Quick Links	Selected	Name (click to edit)	Read only	Supports smart cards	Version	Description	
		FIM CM Sample Profile Template	x	×	0	Description of the template goes here	
	 Image: A set of the set of the	FIM CM Sample Smart Card Logon Profile Template	X	1	21	Description of the template goes here	
		IDGO Gemalto MD cards "MS Provider" Base Of	x	1	7	Description of the template goes here	
		SAC "Aladdin Etoken" FIM CM Sample Smart Car	x	1	14	Description of the template goes here	
	° Сору а з	elected profile template					

(The screen image above is from Microsoff® 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**.

Microsoft Identity Manager	_		
🚰 Duplicate F	Profile		Help
Quick Links Manage Profile Templates Main Menu	You can duplicate an existing profile template and name the * Required item	e new template.	
	Profile Template Name Select a name for the new profile template that you are creating. The new template's name must be unique.	Original profile template name: FIM CM Sample Smart Card Logon Pro New profile template name: * SAC Tokens FIM CM Sample Smar X	
			OK Cancel

(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 second se	
	 Enroll a user for a new set of certificates or a smart card
	View requests that need approvals
	View requests that need completion
	Manage Users And Certificates
	Use this section to perform actions on a user or on a certificate. You will have to search on the user (or certificate) in order to perform an action on that user or certificate.
	• Find a user to view or manage their information
	Find a certificate
	Find a certificate revocation list
	Manage User Smart Cards
	Use this section to manage a user's smart cards. You can view details of a smart card and perform actions on the smart card, such as unblock.
	Unblock a user's smart card
	Find a smart card
	• View details of the smart card currently in the reader
	Requests
	Use this section to manage requests. You can cancel a request you initiated that is in the pending state, distribute one-time passwords for a request that is approved, and view request information.
	Find a request
	Browse completed requests
	Distribute one-time passwords for a request
	Administration
	Use this section to manage profile templates.
	Manage profile templates
	Para de
	Reports
	results.
	• Smart caro inventory report
	* Request summary report
/	

(The screen image above is from Microsoff[®] 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.

📔 Profile Ter	nplate Manage	ment				н
iews	You can list profile te	mplates, and then select one to change or	copy.			
All profile templates	Drofile Template	List				
Smart card profile	To change a profile t	emplate, click the template name.				
Software profile templates	To copy a template	select the check box, and then click Conv a	selected n	rofile template		
uick Links	To copy a complate,	select the check box, and then elick copy t	- Sciected pi	rome template.		
lain Menu	Selected	Name (click to edit)	Read only	Supports smart ca	. Version	Description
		SAC Tokens FIM CM Sample Smart Car	X	1	35	Description of the template goes
		FIM CM Sample Profile Template	x	x	0	Description of the template goes
		FIM CM Sample Smart Card Logon Pr	x	1	0	Description of the template goes.
		MS SC Base CSP Of FIM CM Sample S	x	1	11	Description of the template goes.
	° Copy	a selected profile template				

ıy property of

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.

	Server key generator data:
External Certificates	
In a profile template, you can specify the following:	Maximum number of external certificates:
 The number of external certificates to place in a profile or smart card 	0
Self-Registration (Self-RA)	
When you enable self RA for a policy, by default, any certificate with key usage "digital signature" found within	Enable Self RA (Require that the request is signed using a user certificate)
a smart card can be used to sign requests. Use this setting to enable Self-RA and to optionally constrain valid certificates for self RA.	Extended key usage contains OID:
 Self RA requires the following to be true: Provider is Microsoft Base Smart Card CSP. Self-service is enabled for Enroll, Duplication, Replace and Renew EA is disabled for Enroll, Duplication, Replace and Renew 	Extended key usage does not contain OID:
Smart Card Support You can use a smart card-enabled profile template to store certificates on a smart card.	Supports smart cards
Note After you enable support, you can configure additional policies related only to smart card profile templates.	
	OK Cancel

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

6. Under Smart Card Configuration, click Change Settings.

Smart Card Configuration This section displays smart card settings including	information about the care	provider and certificate authority (C	A) certificates	
Provider name:		Microsoft Smart Card Base CSP		
Provider id:		MSBaseCSP		
Create/Destroy virtual smart card:		×		
Initialize new card prior to use:		×		
Reuse retired card:		×		
Use secure key injection:		×		
Install CA Certificate(s):		1		
Certificate label text: Maximum number of certificates:		{Template!cn} Unlimited		
Diversify Admin Key:		×		
Card Initialization Provider Type: Card Initialization Provider Data: Admin Key initial value:		Default		
Admin PIN rollover:		×		
Admin PIN length:		Not Applicable		
Admin PIN character set:		Not Applicable		
Admin PIN initial value:		Not Applicable		
User PIN policy:		Server Distributed		
User PIN character set:		Ascii		
Print card:		x		
^e Change settings				

(The screen image above is from Microsoff[®] 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.

SafeNet Authentication Client: Integration Guide

Manage Profile Templates	Provider Information	
Main Menu	Select the smart card provider name. This is the friendly name for the provider. The Web.config file	Provider name:
	defines these settings.	Aladdin eToken 🗸
		Previden ID:
		AsciALD1
	Processing	
	Configure smart card procession	
		Create/Destroy Virtual smart card
	Create/Destroy virtual smart card allows for automatic creation and destruction of virtual smart	✓ Initialize new card prior to use
	cards.	
		✓ Reuse retired card
	Initialize new card prior to use deletes all existing key and certificate information from the card.	Use serve key intertion
	Reuse retired card allows a previously retired card to be used when a new card is required,	✓ Install certificate authority certificates
	potentially for a different user and/or profile template.	Cartificate label taxt: 8
	Certificate label text can use dynamic data at the time the certificate is processed. You can use the	
	following tags:	{lemplate:cn}
		Maximum number of certificates:
	• {User}	Unlimited
	{Useristtribute} {Tampletelettribute}	
	- (Templace accordece)	O Set value:
	where attribute is an attribute name in Active Directory and User and Template are the User and cartificate template physics in the directory	
	certificate template objects in the directory.	
	Missesoft Emart Card Page CED	
	Search the arthur way want to use with the Missearth Court Cout Base Courtersonkie Search	
	Provider (CSP).	Diversify Admin Key
		Admin key initial value (hex):
		Smart Card Initialization Provider
		Default
		Custom:
		Smart card initialization provider data:
	Administrative DINs	
	Considerant times were the use for the administration Deserved Identification Number (DIN)	
	specity settings you want to use for the administrative Personal Identification Number (PIN).	Administrative PIN rollover
	Note These settings are not applicable when using the Microsoft Smart Card Base CSP	Administrative PIN length: Administrative PIN character set: Custom character set:
	······	10 Ascii V
		Administrative DIN (a)Net values
		Administrative PIN Initial Value:
		1234567890
	Liser DINS	
	Calact energies details of the uses DIN	Line DTM and and
	annes aprente desena el UIE USEI FIII.	the state state state
		User Provided Y

(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.

Enroll a user for a new set of certificates or a smart card
 View requests that need approvals
 View requests that need completion
Manage Users And Certificates
Use this section to perform actions on a user or on a certificate. You will have to search on the user (or certificate) in order to perform an action on that user or certificate.
Find a user to view or manage their information
 Find a certificate
Find a certificate revocation list
Manage User Smart Cards
Use this section to manage a user's smart cards. You can view details of a smart card and perform actions on the smart card, such as unblock.
Unblock a user's smart card
 Find a smart card
View details of the smart card currently in the reader
Requests
Use this section to manage requests. You can cancel a request you initiated that is in the pending state, distribute one-time passwords for a request that is approved, and view request information.
Find a request
 Browse completed requests
 Distribute one-time passwords for a request
Administration
Use this section to manage profile templates.
Manage profile templates
Reports
Use this section to produce reports that describe requests, certificates, profiles, or smart cards. Click on the report and then input the necessary criteria to produce the results.
Smart card inventory report
Request summary report

(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.

Microsoft Identity Manager	r						
📑 Profile Ten	nplate Manageme	ent					Help
Views All profile templates Smart card profile templates Software profile templates Duick Links	You can list profile templat Profile Template Lis To change a profile templa To copy a template, select	tes, and then select one to change or copy. t te, click the template name. the check box, and then click Copy a selected profile tem	plate.				
Main Menu	Selected	Name (click to edit)	Read only	Supports smart cards	Version	Description	
		FIM CM Sample Profile Template	x	x	0	Description of the template goes here	
	✓	FIM CM Sample Smart Card Logon Profile Template	×	1	21	Description of the template goes here	
		IDGO Gemalto MD cards "MS Provider" Base Of	x	1	7	Description of the template goes here	
		SAC "Aladdin Etoken" FIM CM Sample Smart Car	x	1	14	Description of the template goes here	
	° Соруа:	elected profile template					

(The screen image above is from Microsoff® 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**.

You can change the common name when you copy the template. Afterward,	MS Base OF FIM CM Sample Smart
you cannot change this name.	Profile template display name:
	IDGO Gemalto MD cards "MS Provid
	Description:
	Description of the template
	goes here
	~
Key Generation	
Specify how to generate encryption keys for a certificate.	Generate encryption keys on the server
An encryption key is one that is archived on the certificate authority.	Default server key generator
	O Custom server key generator
	Server key generator type:
	Server key generator data:
External Certificates	
In a profile template, you can specify the following:	Maximum number of external certificates:
 The number of external certificates to place in a profile or smart card 	0
Self-Registration (Self-RA)	
When you enable self RA for a policy, by default, any certificate with key usage "digital signature" found within a smart card can be used to sign	Enable Self RA (Require that the request is signed using a user certificate)
requests. Use this setting to enable Self-RA and to optionally constrain valid	Extended key usage contains OID:
Self RA requires the following to be true:	
 Provider is Microsoft Base Smart Card CSP. Self-service is enabled for Enroll, Duplication, Replace and Renew 	Extended key usage does not contain OID:
 EA is disabled for Enroll, Duplication, Replace and Renew 	
Smart Card Support	
You can use a smart card-enabled profile template to store certificates on a	Supports smart cards
smart card.	

(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.

Enroll a user for a new set of certificates or a smart card
 View requests that need approvals
• View requests that need completion
Manage Users And Certificates
Use this section to perform actions on a user or on a certificate. You will have to search on the user (or certificate) in order to perform an action on that user or certificate.
 Find a user to view or manage their information
 Find a certificate
 Find a certificate revocation list
Manage User Smart Cards
Use this section to manage a user's smart cards. You can view details of a smart card and perform actions on the smart card, such as unblock.
Unblock a user's smart card
 Find a smart card
View details of the smart card currently in the reader
Parmasts
Use this section to manage requests. You can cancel a request you initiated that is in the pending state, distribute one-time passwords for a request that is approved, and view request information.
 Find a request
 Browse completed requests
Distribute one-time passwords for a request
Administration
Use this section to manage profile templates.
Manage profile templates
Reports
Use this section to produce reports that describe requests, certificates, profiles, or smart cards. Click on the report and then input the necessary criteria to produce the results.
Smart card inventory report
Request summary report

(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.

Microsoft Identity Manage	r						
📔 Profile Ter	nplate Managem	ent					Help
Views All profile templates Smart card profile templates Software profile templates	You can list profile templa Profile Template Lis To change a profile templa To copy a template, select	tes, and then select one to change or copy. .t et e, click the template name. t the check box, and then click Copy a selected profile tem	plate.				
Quick Links	Selected	Name (click to edit)	Read only	Supports smart cards	Version	Description	
Main Menu		FIM CM Sample Profile Template	x	X	0	Description of the template goes here	
		FIM CM Sample Smart Card Logon Profile Templat	X	1	21	Description of the template goes here	
		IDGO Gemalto MD cards "MS Provider" Base Of FI	X	1	7	Description of the template goes here	
		SAC "Aladdin Etoken" FIM CM Sample Smart Car	x	1	14	Description of the template goes here	
	е Сору а	selected profile template					

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

4. Under General Settings, click Change General Settings.

Microsoft Identity Manager	-	
📑 Edit Profile	Template [MS Base Of FIM CM Sample	Smart Card Logon Profile Template]
Select a view Profile Details Duplicate Policy Enroll Policy Online Update Policy Replace Policy Replace Policy Renew Policy Suspend and Reinstate Policy Disable Policy Retire Policy Temporary Cards Policy Unblock Policy Offine Unlock Policy Offine Unlock Policy	You can review and change settings for this profile template. General Settings Profile template display name: Profile template common name: Profile template version: Description: Maximum number of external certificates: Supports smart cards: Generate encryption keys on server: Self Registration: * Change general settings	IDGO Gemalto MD cards "MS Provider" Base Of FIM CM Sample Smart Card User Profile Template MS Base Of FIM CM Sample Smart Card Logon Profile Template 7 Description of the template goes here 0 √ ★ ★

(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**.

	Server key generator data:
External Certificates In a profile template, you can specify the following: • The number of external certificates to place in a profile or smart card	Maximum number of external certificates:
Self-Registration (Self-RA) When you enable self RA for a policy, by default, any certificate with key usage "digital signature" found within a smart card can be used to sign requests. Use this setting to enable Self-RA and to optionally constrain valid certificates for self RA.	Enable Self RA (Require that the request is signed using a user certificate) Extended key usage contains OID:
 Self RA requires the following to be true: Provider is Microsoft Base Smart Card CSP. Self-service is enabled for Enroll, Duplication, Replace and Renew EA is disabled for Enroll, Duplication, Replace and Renew 	Extended key usage does not contain OID:
Smart Card Support You can use a smart card-enabled profile template to store certificates on a smart card.	☑ Supports smart cards
Note After you enable support, you can configure additional policies related only to smart card profile templates.	
	OK Cancel

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

6. Under Smart Card Configuration, click Change Settings.

Smart Card Configuration This section displays smart card settings, including	information about the card	provider and certificate authority (CA	A) certificates.		
Provider name: Provider id:		Microsoft Smart Card Base CSP MSBaseCSP			
Create/Destroy virtual smart card:		×			
Initialize new card prior to use:		×			
Reuse retired card:		×			
Use secure key injection:		×			
Install CA Certificate(s):		1			
Certificate label text: Maximum number of certificates:		{Template!cn} Unlimited			
Diversify Admin Key:		×			
Card Initialization Provider Type: Card Initialization Provider Data: Admin Key initial value:		Default			
Admin PIN rollover:		×			
Admin PIN length: Admin PIN character set:		Not Applicable Not Applicable			
Admin PIN initial value:		Not Applicable			
User PIN policy:		Server Distributed			
User PIN character set:		Ascii			
Print card:		×			
^e Change settings					`



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.

Managa Profile Templates	Provider Information	
Main Menu	Select the smart card provider name. This is the friendly name for the provider. The Web.config file	Provider name:
	defines these settings.	Microsoft Smart Card Base CSP 🗸
		Provider ID:
		MS8#seCSP
	Descarsion	
	Processing	
	compare smart card processing.	□ Create/Destroy virtual smart card
	Create/Destroy virtual smart card allows for automatic creation and destruction of virtual smart	✓ Initialize new card prior to use
		Reuse retired card
	Initialize new card prior to use deletes all existing key and certificate information from the card.	Use secure key injection
	Reuse retired card allows a previously retired card to be used when a new card is required,	✓ Install certificate authority certificates
	potentially for a different user and/or profile template.	Certificate label text: *
	Certificate label text can use dynamic data at the time the certificate is processed. You can use the	(Templateicn)
	ionowing tags:	Maximum number of certificates:
	• {User}	Unlimited
	(Useriattribute) (Templatelattribute)	
	where attribute is an attribute name in Active Directory and //ser and Template are the User and	
	certificate template objects in the directory.	
	Microsoft Smart Card Base CSP	
	Specify the settings you want to use with the Microsoft Smart Card Base Cryptographic Service	Diversify Admin Key
	Provider (CSP).	Admin key initial value (hex):
		000000000000000000000000000000000000000
		Smart Card Initialization Provider
		Default
		Queter
	Administrative PINs	
	Specify settings you want to use for the administrative Personal Identification Number (PIN).	Administrative PIN rollover
	Note These settings are not applicable when using the Microsoft Smart Card Base CSP.	Administrative PIN length: Administrative PIN character set: Custom character set:
		Ascii 🗸
		Administrative PIN initial value:
	User PINs	
	Select specific details of the user PIN.	User PIN policy:
	Make 17	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.

Enroll a user for a new set of certificates or a smart card
 View requests that need approvals
View requests that need completion
Manage Users And Certificates
Use this section to perform actions on a user or on a certificate. You will have to search on the user (or certificate) in order to perform an action on that user or certificate.
 Find a user to view or manage their information
• Find a certificate
 Find a certificate revocation list
Manage Licer Smart Cards
Use this section to manage a user's smart cards. You can view details of a smart card and perform actions on the smart card, such as unblock.
Unblock a user's smart card
 Find a smart card
 View details of the smart card currently in the reader
Requests Use this section to manage requests. You can cancel a request you initiated that is in the pending state, distribute one-time passwords for a request that is approved, and view request information.
Find a request
 Browse completed requests
 Distribute one-time passwords for a request
A desired the second
Auministration
Use this section to manage prome temparas.
Manage profile templates
Reports
Use this section to produce reports that describe requests, certificates, profiles, or smart cards. Click on the report and then input the necessary criteria to produce the results.
Smart card inventory report
Request summary report

(The screen image above is from Microsoff[®] software. Trademarks are the property of their respective owners.)

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

Microsoft Identity Manager	r					-	
Profile Ten	nplate Manageme	ent					Help
Views All profile templates Smart card profile templates Software profile templates Duick Links	You can list profile templat Profile Template List To change a profile templa To copy a template, select	es, and then select one to change or copy. t te, click the template name. the check box, and then click Copy a selected profile tem .	plate.				
Main Menu	Selected	Name (click to edit)	Read only	Supports smart cards	Version	Description	
		FIM CM Sample Profile Template	x	x	0	Description of the template goes here	
	✓	FIM CM Sample Smart Card Logon Profile Template	X	1	21	Description of the template goes here	
		IDGO Gemalto MD cards "MS Provider" Base Of	x	1	7	Description of the template goes here	
		SAC "Aladdin Etoken" FIM CM Sample Smart Car	x	1	14	Description of the template goes here	
	° Соруаз	elected profile template					

(The screen image above is from Microsoff® 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**.

Microsoft Identity Manager	r		-
Duplicate I	Profile		Help
Quick Links Manage Profile Templates Main Menu	You can duplicate an existing profile template and name the new template. • Required item		
	Profile Template Name Select a name for the new profile template that you are creating. The new template's name must be unique.	Original profile template name: Copy Of FIM CM Sample Smart Car New profile template name: * SafeNet Gemalto Minidriver FIM CM	
			OK Cancel

(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.

	 Enroll a user for a new set of certificates or a smart card
	 View requests that need approvals
	 View requests that need completion
	Manage Users And Certificates
	Use this section to perform actions on a user or on a certificate. You will have to search on the user (or certificate) in order to perform an action on that user or certificate.
	• Find a user to view or manage their information
	• Find a certificate
	• Find a certificate revocation list
	Manage User Smart Cards
	Use this section to manage a user's smart cards. You can view details of a smart card and perform actions on the smart card, such as unblock.
	 Unblock a user's smart card
	 Find a smart card
	• View details of the smart card currently in the reader
	Requests
	Use this section to manage requests. You can cancel a request you initiated that is in the pending state, distribute one-time passwords for a request that is approved, and view request information.
	 Find a request
	Browse completed requests
	Distribute one-time passwords for a request
	Administration
	Use this section to manage profile templates.
	Manage profile templates
	Reports
	Use this section to produce reports that describe requests, certificates, profiles, or smart cards. Click on the report and then input the necessary criteria to produce the results.
	Smart card inventory report
	Request summary report
(T)	

(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.

Microsoft Identity Manager	_							
🛛 📑 Profile Ten	nplate I	Manageme	ent					Help
Views All profile templates Smart card profile templates Software profile templates Quick Links Main Menu	You can li Profile To change To copy a	ist profile templat Template Lisi e a profile templa template, select Selected	es, and then select one to change or copy. t te, click the template name. the check box, and then click Copy a selected profile Name (click to edit)	template. Read only	Supports smart cards	Version	Description	
			Copy 2 Of FIM CM Sample Smart Card Logon	x	1	1	Description of the template goes here	•
			Copy SAC MDcards FIM CM Sample Smart Car	x	1	9	Description of the template goes here	•
			SafeNet Gemalto MiniDriver FIM CM Sample S	×	1	8	Description of the template goes here	•
			Copy Of SAC FIM CM Sample Smart Card Logo	×	1	1	Description of the template goes here	•
			FIM CM Sample Profile Template	1	×	0	Description of the template goes here	
			FIM CM Sample Smart Card Logon Profile Te	×	1	22	Description of the template goes here	5
			IDGO BC FIM CM Sample Smart Card User Pro	×	1	35	Description of the template goes here	
			SAC FIM CM Sample Smart Card Logon Profile	×	1	8	Description of the template goes here	5
		° Copy a s	elected profile template					

(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.

		Server key generator data:
External Certi In a profile templa • The numbe profile or s	ificates te, you can specify the following: er of external certificates to place in a mart card	Maximum number of external certificates:
Self-Registrat When you enable certificate with ke a smart card can setting to enable valid certificates f • Self RA red • Provider is • Self-Servic Replace an • EA is disab Renew	tion (Self-RA) self RA for a policy, by default, any y usage "digital signature" found within be used to sign requests. Use this Self-RA and to optionally constrain or self RA. uires the following to be true: Microsoft Base Smart Card CSP. e is enabled for Enroll, Duplication, id Renew led for Enroll, Duplication, Replace and	Enable Self RA (Require that the request is signed using a user certificate) Extended key usage contains OID: Extended key usage does not contain OID:
Smart Card St You can use a sm store certificates Note After you en additional policies templates.	upport art card-enabled profile template to on a smart card. hable support, you can configure related only to smart card profile	☑ Supports smart cards
		OK Cancel

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

6. Under Smart Card Configuration, click Change Settings.

Smart Card Configuration This section displays smart card settings, including	information about the car	d provider and certificate authority (CA)	certificates.		
Provider name: Provider id: Create/Destroy virtual smart card: Initialize new card prior to use: Reuse retired card: Use secure key injection: Install CA Certificate(s): Certificate label text: Maximum number of certificates: Diversify Admin Key: Card Initialization Provider Type: Card Initialization Provider Type: Card Initialization Provider Data: Admin Key initial value: Admin PIN rollover: Admin PIN Ingoth: Admin PIN initial value: User PIN character set: Print card:		Microsoft Smart Card Base CSP MSBaseCSP X X X (TemplateIcn.) Unlimited X Default X Not Applicable Not Applicable Not Applicable Server Distributed Ascii X			
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. Scillars Administrator Command Prompt C:\Users\Administrator\Desktop\AdminKey.exe 1234567890 Key: 1d6a4f?a652e18203e3d3b0c?045102210?r?420216e611b C:\Users\Administrator\Desktop\AdminKey>_
User PIN policy	Select User Provided.

Microsoft Identity Manager		
Edit Profile	Template [Copy Of FIM CM Sample Smart Card Logon Profile Template]	
Quick Links	You can review and change detailed smart card configuration settings for this profile templete.	
Menue Profile Templates Maina Menu	Provider Information Select the smart card provider name. This is the friendly name for the provider. The Web.config file defines these settings.	Provider name: Microsoft Smart Card Base CSP V Provider ID: ISBACCSP
	Processing	
	Configure smart card processing.	Create/Destroy virtual smart card
	Create/Destroy virtual smart card allows for automatic creation and destruction of virtual smart cards.	Initialize new card prior to use
	Initialize new card prior to use deletes all existing key and certificate information from the card.	Reuse retired card
	Reuse retired card allows a previously retired card to be used when a new card is required, potentially for a different user and/or profile template.	Use secure key injection
	Certificate label text can use dynamic data at the time the certificate is processed. You can use the following tags:	Certificate label text: *
	(User) - Cluseristonum) - (Templatelatribute)	L'itemplatein) Maximum number of certificates: © Unimited
	where attribute is an attribute name in Active Directory and User and Template are the User and certificate template objects in the directory.	O Set value:
	Microsoft Smart Card Base CSP	
	Specify the settings you want to use with the Microsoft Smart Card Base Cryptographic Service Provider (CSP).	Diversity Admin Key
		1664473652e18203e3
		Smart Card Initialization Provider
	Administrative PINs	
	Specify settings you want to use for the administrative Personal Identification Number (PIN).	Administrative PIN rollover
	Note These settings are not applicable when using the Microsoft Smart Card Base CSP.	Administrative PIN length: Administrative PIN character set: Custom character set:
		Administrative PIN Initial value:
	User PINs	
	Select specific details of the user PIN.	User PIN policy: User Provided
	Note If you use custom, server-distributed user PIN generation, you must have a fully-qualified .NET assembly type configured in FIM CM. When selecting the CustomUserPinGeneration option, the .NET type configured in Web.Config must implement the Clariford Inselection Selection option and the selection option option.	User PIN length: User PIN character set:

(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 second way was and the second	
	 Enroll a user for a new set of certificates or a smart card
	• View requests that need approvals
	 View requests that need completion
	Manage Users And Certificates
	Use this section to perform actions on a user or on a certificate. You will have to search on the user (or certificate) in order to perform an action on that user or certificate.
	• Find a user to view or manage their information
	• Find a certificate
	• Find a certificate revocation list
	Manage User Smart Cards
	Use this section to manage a user's smart cards. You can view details of a smart card and perform actions on the smart card, such as unblock.
	 Unblock a user's smart card
	 Find a smart card
	• View details of the smart card currently in the reader
	Requests
	Use this section to manage requests. You can cancel a request you initiated that is in the pending state, distribute one-time passwords for a request that is approved, and view request information.
	• Find a request
	Browse completed requests
	Distribute one-time passwords for a request
	Administration
	Use this section to manage profile templates.
	Manage profile templates
	Reports
	Use this section to produce reports that describe requests, certificates, profiles, or smart cards. Click on the report and then input the necessary criteria to produce the results.
	Smart card inventory report
	Request summary report

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

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

You can list profile templa	ates, and then select one to change or copy.				
Profile Template Lie	et .				
To change a profile templ	late, click the template name.				
-					
To copy a template, selec	t the check box, and then click Copy a selected profile	e template.			
Selected	Name (click to edit)	Read only	Supports smart cards	Version	Description
	FIM CM Sample Profile Template	x	×	0	Description of the template goes here
	FIM CM Sample Smart Card Logon Profile Ter	nplate X	1	21	Description of the template goes here
 Image: A start of the start of	IDGO Gemalto MD cards "MS Provider" Base	OF FIN X	1	7	Description of the template goes here
	SAC "Aladdin Etoken" FIM CM Sample Smart	Car X	1	14	Description of the template goes here
[°] Сору а	selected profile template				
	Profile Template Li To change a profile temp To copy a template, selec Selected V Copy a	Profile Template List To change a profile template, click the template name. To copy a template, select the check box, and then click Copy a selected profil Selected Name (click to edit) FIM CM Sample Profile Template FIM CM Sample Smart Card Logon Profile Tem JIDGO Gematto MD cards "MS Provider" Base SAC "Aladdin Etoken" FIM CM Sample Smart Copy a selected profile template	Profile Template List To change a profile template, click the template name. To copy a template, select the check box, and then click Copy a selected profile template. Selected Name (click to edit) Read only FIM CM Sample Profile Template X FIM CM Sample Smart Cards "MS Provider" Base Of FIP X DGO Cemaito MD cards "MS Provider" Base Of FIP X SAC "Aladdin Etoken" FIM CM Sample Smart Car X Copy a selected profile template	Profile Template List To change a profile template, click the template name. To copy a template, select the check box, and then click Copy a selected profile template. Selected Name (click to edit) Read only Supports smart cards FIM CM Sample Profile Template X X IDGO Gemaito MD cards "MS Provider" Base Of FIN X ✓ SAC "Aladdin Etoken" FIM CM Sample Smart Car X ✓	Profile Template List To change a profile template, click the template name. To copy a template, select the check box, and then click Copy a selected profile template. Selected Name (click to edit) Read only Supports smart cards Version FIM CM Sample Profile Template X X 0 FIM CM Sample Smart Card Logon Profile Template ✓ 21 ✓ IDGO Gemait OMD cards "MS Provider" Base Of FIP X ✓ 7 SAC "Aladdin Etoken" FIM CM Sample Smart Car X ✓ 14 * Copy a selected profile template

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

Microsoft Identity Manager	-		
📕 Edit Profile	e Template [Etoken FIM CM Sample Smart Card	d Logon Profile Template]	Help
Select a view Profile Details Duplicate Policy Enroll Policy Online Update Policy Recover On Behalf Policy Disable Policy Retire Policy Temporary Cards Policy Unblock Policy	You can set properties related to enrollment for this profile template, include Workflow: General This section displays workflow information related to enrollment of this profile Policy enabled: Self service enabled: Enrollment agent required: Allow collection of comments: Allow collection of request priority: Default request priority: Number of approvals: Number of approvals:	ing items related to workflow, data collection, or password distribution.	
Quick Links Manage Profile Templates Main Menu	 Change general settings Workflow: Smart Card Application Applet Management This section displays smart card applet application management settings. Enable personalization: Personalization profile: 	×	
	Change smart card application management setting: Workflow: Initiate Enroll Requests The following users and groups can initiate an enroll request for this profile Selected Principal (click to edit) NT AUTHORITY\SYSTEM SAFENETDEMO\Domain Users SAFENETDEMO\FIM CM Smart Card Subsc	s template: Enroll Initiate Grant Grant Grant Grant Grant Grant Cribers Grant	
	• Add new principal for enroll request initiation		

(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.

Personalizatio	nalization: X		
° Change	smart card application management settings		
Tublete F			
w: initiate E	nron kequests		
ving users and	groups can initiate an enroll request for this profile template:		
Selected	groups can initiate an enroll request for this profile template: Principal (click to edit)	Enroll Initiate	
Selected	groups can initiate an enroll request for this profile template: Principal (click to edit) NT AUTHORITY\SYSTEM	Enroll Initiate Grant	
Selected	groups can initiate an enroll request for this profile template: Principal (click to edit) NT AUTHORITY\SYSTEM SAFENETDEMO\Domain Users	Enroll Initiate Grant Grant	
Selected	groups can initiate an enroll request for this profile template: Principal (click to edit) NT AUTHORITY\SYSTEM SAFENETDEMO\Domain Users SAFENETDEMO\bob	Enroll Initiate Grant Grant Grant	

(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**.

Microsoft Identity Manager	er	-
📑 Edit Profile	le Template [Etoken FIM CM Sample Smart Card Logon Profile ⁻	Template]
Nuick Links Return To Enroll Policy Manage Profile Templates Main Menu	You can set up permissions for users or groups. Permission Set the permissions you want for the principal (that is, the user or group) that you have specified. Enroll Initiate permission: Grant	Lookup
		OK Cancel

(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.

Microsoft Identity Manager	-		-
📑 Edit Profile	e Template [Etoken FI	Aircosoft Forefront Identity Manager 2010 Certificate Management Webpage Di	Help
Juick Links Return To Enroll Policy Manage Profile Templates Main Menu	You can set up permissions for us Permission Set the permissions you want for group) that you have specified.	Search for Users and Groups Complete your search criteria and click Search Search for the following:	D

(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.

Microsoft Identity Manager	-	
Edit Profile	Template [Etoken FI 🗃 Microsoft Forefront Identity Manager 2010 Certificate Management Webpage Di 🧮	
tick Links Leturn To Enroll Policy Ianage Profile Templates Iain Menu	You can set up permissions for us Permission Set the permissions you want for group) that you have specified. Search for Users and groups Users Groups Forest: safenetdemo.com Name: Bob x Search Cancel User Logon SAFENETDEMO\bob	D

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

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

Microsoft Identity Manager	<u>r</u>		
📕 Edit Profile	e Template [Etoken FIM CM Sample Smart C	ard Logon Profile Template]	Help
Quick Links Return To Enroll Policy Manage Profile Templates Main Menu	You can set up permissions for users or groups. Permission Set the permissions you want for the principal (that is, the user or group) that you have specified.	Principal: SAFENETDEMO\bob Lookup Enroll Initiate permission: Grant V	
			OK Cancel

(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.

Colocted	Name (click to adit)	Courses	Validation	Charmen
Selected ✓	Sample Data Item	Subscriber	Data Type	Database
• Add ne • Delete One-Time Password This section displays info	w data collection item data collection items Is rmation for password generatio	Message from webpage	items?	iswords are distributed, see the Passwords Distribu
Password Pro Password Pro Change	vider Type: vider Initialization Data: password provider settings	ОК	Cancel	
Passwords Distribut Each password that is ge corresponds to distributi	tion merated must be distributed. If ng the second password.	you have two passwords, the fi	st row in this table corresponds to	distributing the first password, and the second row
Distribution	method (click to edit)	Mail from		Mail subject
	screen			
Display on Document Printing This section allows you t	o control which profile template	documents to print:		
Display on Document Printing This section allows you t Selected * Add ne	o control which profile template Document title (click to edi w documents to print	documents to print: t)	Print location	

(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.

Certificate Templates (4ThDCCAmin	Template Display Name 🔺	Minimum Supported CAs	Version	Intended Purpose 🔺
	Administrator	Windows 2000	4.1	
	Authenticated Session	Windows 2000	3.1	
	Basic EFS	Windows 2000	3.1	
	🖳 CA Exchange	Windows Server 2003 Ent	106.0	Private Key Archiv
	CEP Encryption	Windows 2000	4.1	
	Reference Code Signing	Windows 2000	3.1	
	R Computer	Windows 2000	5.1	
	Record Cross Certification Authority	Windows Server 2003 Ent	105.0	
	Directory Email Replication	Windows Server 2003 Ent	115.0	Directory Service
	Domain Controller	Windows 2000	4.1	
	Domain Controller Authentication	Windows Server 2003 Ent	110.0	Client Authenticat
	EFS Recovery Agent	Windows 2000	6.1	
	🖳 Enrollment Agent	Windows 2000	4.1	
	Renrollment Agent (Computer)	Windows 2000	5.1	
	Rechange Enrollment Agent (Offline i	request) Windows 2000	4.1	
	Rechange Signature Only	Windows 2000	6.1	
	🗟 Exchange User	Windows 2000	7.1	
	FIM Enrollment Agent	Windows Server 2003 Ent	100.2	Certificate Reque
	🚇 FIM User	Windows Server 2003 Ent	100.2	Client Authenticat
	I FIMCM Key Recovery Agent	Windows Server 2003 Ent	100.1	Key Recovery Age
	IPSec	Windows 2000	8.1	
	IPSec (Offline request)	Windows 2000	7.1	
	Rerberos Authentication	Windows Server 2003 Ent	110.0	Client Authenticat
	Rev Recovery Agent	Windows Server 2003 Ent	105.0	Key Recovery Age
	🚇 Mim Smartcard User	Windows Server 2008 Ent	100.2	Smart Card Logon
	I OCSP Response Signing Du	uplicate Template 8 Ent	101.0	OCSP Signing
	RAS and IAS Server Re	eenroll All Certificate Holders 3 Ent	101.0	Client Authenticat
	Root Certification Authority Ch	nange Names	5.1	
	Router (Offline request)	Tasks	4.1	
	🖳 Smartcard Logon		6.1	
	Smartcard Logon CC Certificat De	elete 3 Ent	100.3	Smart Card Logon
	Smartcard User	roperties	11.1	
	Representation Auth		5.1	
	Trust List Signing He	elp	3.1	
	A licer	Windows 2000	2.1	

(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.

🖳 Certificate Templates Console		
File Action View Help		
		Mim Smartcard User Properties
Certificate Templates (4ThDCCAmir	Template Display Name ▲ Image: Administrator Image: Administrator Image: Computer Image: Computer Image: Exchange: Signature Only Image: Exchange: User Image: Fild: Findlement Agent Image: Fild: Exchange: User Image: Fild: Exchange: User Image: Fild: Exchange: User Image: Fild: Exchange: User Image: Fild: Exchange: User Image: Fild: Exchange: User Image: Exchange: User Image: Fild: Exchange: User Image: Exchange: User Image: Fild: Exchange: User Image: Exchange: User Image: Fild: Exchang	Cryptography Subject Name Issuance Requirements ons General Request Handling More Actions Indicate Templates (4T Supenseded Templates Extensions Security Server More Actions Indicate Templates (4T Supenseded Templates Extensions Security Server Server Indicate Templates (4T More Actions Supenseded Templates Extensions Security Server Indicate Templates (4T More Actions Group or user names: Indicate Templates (4T Indicate Templates (4T More Actions Indicate Templates (4T Group or user names: Indicate Templates (4T Indicate Templates (4T More Actions Indicate Templates (4T Group or user names: Indicate Templates (4T Indicate Templates (4T More Actions Indicate Templates (4T General Computers, Service Accounts, or Groups Select Users, Computers, Service Accounts, or Groups Indicate Types For special permissions or advanced settings, click Advanced Locations Enter the object names to select (examples): Iniminus/service (4t OK Cancel Indite templates Advanced

(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**.



SafeNet Authentication Client: Integration Guide

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 Microsoff® 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.

Rective Directory Sites and Servi	ces		<u>_0×</u>
File Action View Help			
🔄 🔿 💆 🖬 🔀 🖬 🖉			
Active Directory Sites and Services	Name	Туре	Description
Sites Services MsmoServices	FIM CM Sample Profile Template FIM CM Sample Smart Card Logon Profile Template	msClm-ProfileTe msClm-ProfileTe	Description of the templat Description of the templat
Imanger vices Imanger vices Imanger vices Imanger vices Imanger vices	MS Base OF FIM CM Sample Smart Card Logon Profile Tem SAC FIM CM Sample Smart Card Logon Profile Template	msClm-ProfileTe	Description of the templat Description of the templat
Poblic Rey Services P G AIA C CDP Certificate Templates Certification Authorities E Certification Authoritint E Certification	SAC FIM CM Sample Smart Card Logon Profile Templa Select Users, Computers, Service Accounts, or Group Select this object type: Users, Groups, or Built-in security principals From this location: mimsafenetdemo.com Enter the object names to select (examples): mim-subscribers	Is Object	? × Types tions Names
<u>▲</u>	Advanced	OK C	

(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.

Active Directory Sites and Servi	ces		
File Action View Help			
🗢 🔿 🗡 📅 🗙 🖬 🙆	🖸 🖬 🔁		
Active Directory Sites and Services	Name	Туре	Description
🕀 🚞 Sites	🖬 FIM CM Sample Profile Template	msClm-ProfileTe	Description of the templat
E Services	🖬 FIM CM Sample Smart Card Logon Profile Template	msClm-ProfileTe	Description of the templat
MsmqServices	MS Base Of FIM CM Sample Smart Card Logon Profile Tem	msClm-ProfileTe	Description of the templat
NetServices	📾 SAC FIM CM Sample Smart Card Logon Profile Template	msClm-ProfileTe	Description of the templat
Public Key Services	CAC ITM CM Consult Count Count I areas Durities Townshi		1
	SAC FIFTCH Sample Smart Card Logon Profile Templa	ate Prope	85
E COP	General Object Security Attribute Editor		
Certification Authorities		1	
Enrolment Services	Group or user names:		
E KRA	Image: ClmAuthAgent (clmAuthAgent@mimsafenetdemo.com)		
F OID	CIMEnrollAgent (clmEnrollAgent@mimsafenetdemo.com	m)	
Profile Templates	mim-subscribers (MIMSAFENETDEMO\mim-subscribe	rs)	
🕀 📔 RRAS	Domain Admins (MIMSAFENETDEMO\Domain Admin Ministry Company Administry Company Adminis	is)	
🕀 🚞 Windows NT	Bomain Users (MIMSAFENETDEMO\Domain Users)		
	Reference Admins (MIMSAFENETDEMO\Enterprise A	dmins) 🔟	
	Add	Remove	
	Permissions for mim-subscribers Allow	Deny	
	Full control		
	Bead	- H	
	Write D	- H - H	
		- H - H	
			1.1
	For special permissions or advanced settings, click Advanced.	Ad <u>v</u> anced	

SafeNet Authentication Client: Integration Guide

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.

SafeNet Authentication Client: Integration Guide

Important Notes

Enable ActiveX

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

This webpage wants to run the following add-on: 'gscBsi.dll' from 'Microsoft Corporation'.	What's the risk?

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.



SafeNet Authentication Client: Integration Guide

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 Microsoff® software. Trademarks are the property of their respective owners.)

4. Select Request a permanent smart card

quests Welcome MIMSAFENETDEMO\bob1 to the Microsoft Forefront Identity Manager 2010 - Certificate Management Portal. pproved [1] FIM Certificate Management (FIM CM) enables you to request new certificates and smart cards, and manage the certificates and smart cards that have been provided to you. Common Tasks Image: Complete a new set of certificates • Request a new set of certificates • Request a temporary smart card • Complete a request with one-time passwords • Change my smart card PIN View My Information Use this section to view the following information: • Show details of my certificate • Show details of my smart card	Home		Help
used Fine test is the test is th	Home	Welcome MIMSAFFNFTDEMOloph1 to the Microsoft Eorefront Identity Mananer 2010 - Certificate Mananement Portal.	neip
Common Tasks Use this section to perform the following tasks:	roved [1] cutable [4]	FIM Certificate Management (FIM CM) enables you to request new certificates and smart cards, and manage the certificates and smart cards that have been provided to you.	
Use this section to perform the following tasks:		Common Tasks	
 Request a new set of certificates Request a permanent smart card Request a temporary smart card Complete a request with one-time passwords Complete a request with one-time passwords Change my smart card PIN View My Information Use this section to view the following information: Show details of my certificate Show details of my smart card 		Use this section to perform the following tasks:	
		Request a new set of certificates	
		Request a permanent smart card	
Complete a request with one-time passwords Change my smart card PIN Use My Information Use this section to view the following information: Show details of my certificate Show details of my smart card		Request a temporary smart card	
Change my smart card PIN View My Information Use this section to view the following information: Show details of my certificate Show details of my smart card		 Complete a request with one-time passwords 	
View My Information Use this section to view the following information: • Show details of my certificate • Show details of my smart card		Change my smart card PIN	
Use this section to view the following information: Show details of my certificate Show details of my smart card		View My Information	
 Show details of my certificate Show details of my smart card 		Use this section to view the following information:	
Show details of my smart card		Show details of my certificate	
		 Show details of my smart card 	
 Show my request history 		 Show my request history 	

(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.

You can select a profile template for enrollment.		
Select a Profile Template Select the profile template you want, and then click Next.	Profile template: IDGO BC FIM CM Sample Smart Card Logon Profile Template	
	Next	t

(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.

Poquest Initiation		
Four certificate enrollment process is about to start four can use this page to request one or more new certificates. Additional Information specify any comments or additional information.	Comments:	
		Next Cancel

(The screen image above is from Microsoff[®] 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.

1	72
	2
l	

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

	New PIN:	
	Confirm PIN:	
Valid	PIN Rule	
	Maximum PIN length: 14 Minimum PIN length: 4	

(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

Microsoft Identity Man	ager		-
Request	t Complete		Help
Quick Links Request Summary Smart Card Details	The following summarizes the request that was just executed. Request Summary For more details about the request, click the request type. Request type: Request type: Request attus: Request originator: Date of submission:	Enroll Completed MIMSAFENETDEMO\bob1 Thursday, November 10, 2016 1:19:26 PM	
	Smart Card Summary For more information, click the profile name. Smart Card: Status:	MS8aseCSP:{021bf81c-d479-db3b-416e-a993d51d7d27} Active	
			Main Menu

(The screen image above is from Microsoff® 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