# SafeNet Authentication Client Integration Guide

Using SafeNet Authentication Client CBA for MyID Version 10.8 Update 2



All information herein is either public information or is the property of and owned solely by Gemalto 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.

© 2010 - 2018 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 Number: 007-000161-001, Rev. A Release Date: October 2018

# Contents

Third-Party Software Acknowledgement	4
Description	4
Applicability	5
Environment	5
Audience	5
CBA Flow using SafeNet Authentication Client	6
Prerequisites	7
Supported Tokens and Smart Cards in SafeNet Authentication Client	7
Supported Tokens/Smart Cards in MyID Version 10.8 Update 2	8
Configuring MyID Version 10.8 Update 2	9
Configure certificate templates for issuance within MyID	9
Configure Credential Profile	.12
Client Side Configuration	.19
Running the Solution	20
Issue a Card	20
Smart Card Log in to MyID Desktop	26
Support Contacts	28

## **Third-Party Software Acknowledgement**

This document is intended to help users of Gemalto products when working with third-party software, such as MyID Version 10.8 Update 2.

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.

MyID Version 10.8 Update 2 enables deployment of digital identities to smart cards, virtual smart cards and mobile devices for securing access to corporate assets and information.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to MyID Version 10.8 Update 2 using SafeNet tokens.

It is assumed that the MyID Version 10.8 Update 2 environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

MyID Version 10.8 Update 2 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.
- Gemalto SafeNet MiniDriver 10.2
  - For more details about different SAC installation modes, refer to Customization section in *SafeNet Authentication Client Administrator Guide*.
- MyID Version 10.8 Update 2

### Environment

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

- SafeNet Authentication Client (SAC) 10.6
- Gemalto SafeNet MiniDriver 10.2
- MyID Version 10.8 Update 2 installed on Microsoft Windows server 2012R2
- Microsoft DC and CA installed in Windows Server 2008R2
- MyID Desktop 2.7.1000.1 Installed on Win 10 x64 1709

#### Audience

This document is targeted to system administrators who are familiar with MyID Version 10.8 Update 2, and are interested in adding certificate-based authentication capabilities using Gemalto tokens and smart cards. See Supported Tokens and Smart Cards in SafeNet Authentication Client, on page 7.

### **CBA Flow using SafeNet Authentication Client**

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



- 1. A privileged user connects to the MyID Version 10.8 Update 2 server from a client with the MyID Version 10.8 Update 2 Desktop client application.
- 2. The user inserts the Smart Card / Token and performs "Issue Card", and when prompted, enters a new user PIN in the **New PIN** and **Confirm PIN** fields, then clicks **Next** to continue.

After successful process 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 MyID Version 10.8 Update 2 using Gemalto tokens and smart cards:

- 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) must 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 Gemalto token or smart card with an appropriate certificate enrolled on it.
- SafeNet Authentication Client (10.6) must be installed on all client machines.
- When Working With SAC the "SAC Administrator Password Quality Check" Property Must be disabled. For more information see *SafeNet Authentication Client 10.6 (GA) Administrator Guide*.
- In the Myld configuration example demonstrated, in **Device Security** under **Gemalto .Net**, the following options were disabled: **Require Customer Global Platform Key** and **Require Customer PIV9B Key**.
- In MyID IDPrime MD cards device type names are recognized as .Net Cards.
- Issuing certificates that require a Signature Only policy is not supported with MyID. For More information See "MD840 Rev A and MD3840 smart cards and signature only policies" in *MyID Version 10.8 Update* 2 Smart Card Integration Guide.

# Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client (10.6) 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 B L2
- Gemalto IDPrime MD 830 B L3
- Gemalto IDPrime MD 840 B
- Gemalto IDPrime MD 940

For a full list of supported devices, refer to SafeNet Authentication Client Customer Release Notes.

### Supported Tokens/Smart Cards in MyID Version 10.8 Update 2

Token\Smart card	Installation Mode
IDPrime MD 840 B	
IDPrime MD 830 B L3	Comolto SofoNat MiniDriver
IDPrime MD 830 B L2	Gemaito Saleivet MiniDriver
IDPrime MD 940	
eToken 5110 CC	
eToken 5110 GA	SafeNet Authentication Client
eToken 5110 FIPS	

Operations tested:

- 1. Issue Card (RSA 2048)
- 2. Token Logon to MyID Desktop App
- 3. Reset Card PIN
- 4. Erase Card

### **Configuring MyID Version 10.8 Update 2**

This section will demonstrate how to configure CBA with SafeNet Tokens in MyID Version 10.8 Update 2.

#### Prerequisites:

- Copy of Smart Card User certificate template was created on MS CA.
- LDAP Directory Management configured, LDAP users imported and **Card Holder** role was assigned to LDAP user.

#### Configure certificate templates for issuance within MyID

1. From MyID Desktop client, connect to MyID server with privileged user.

0	MyID Desktop	- 0 X
	WiD Welcome to MyID	
	Security Questions Enter your username Username: startug	Next
	© 2018 Intercede	

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

2. In MyID Dashboard click Start a new action.

Dashboard
Welcome startup user
Messages
The recent is shallow in the investment of the interaction of the state of the state of the interaction of the
● Actions
Start a new action

3. In the left pane click **Configuration** and then click **Certificate Authorities**.

Ð	New Action						×
Jump	То						^
e	People	Configuration		1.41			
2	Cards	Add Devices	<u></u>	Audited Items	<u></u>	Card Layout Editor	2
	Certificates	Card Stock	÷	Certificate Authorities	Þ	Credential Profiles	2
	Applets	Directory					
٥	Configuration	Management	2	LO Edit Devices	2	Edit Roles	<u> </u>
	Device Identities	Email Templates	>	External Systems	>	Import Serial Numbers	2
	Mobile Devices	Job Management	-	& Key Manager	-		
ß	Reports						-
		List Editor	<mark>⇒</mark>	Notifications Management	>	Operation Settings	2
		Security Settings	>				

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

4. In the Certificate Authorities window, from the CA Name list, select your CA server and click Edit.

) MyID Desktop							- 0	×
=								vyiD
Co Norrei	Select a CA		middama WINDOWSSED	IED 0 CA Costificate 4	uthority			
CA Type:	Microsoft Enterprise	CA Description:	mylddemo-windOwsserv	ER-U-CA Certificate A	luthority			Í
CA Enabled:		-						
Name			Description	Allow Issuance	Reverse DN	Archive Keys	Superseded	
Administrator	on myiddemo-WINDOWSS	ERVER-0-CA		8	8	8	8	
Copy of Smart	card User on myiddemo-W	INDOWSSERVER-0-CA		0	8	8	8	
DirectoryEmai	ilReplication on myiddemo	-WINDOWSSERVER-0-CA		8	8	8	8	
DomainContro	oller on myiddemo-WINDO	WSSERVER-0-CA		8	8	8	8	
DomainContro	ollerAuthentication on myio	ddemo-WINDOWSSERVER-0-CA		8	8	8	8	
eden on myid	demo-WINDOWSSERVER-0	-CA		8	8	8	8	
	mo-WINDOWSSERVER-0-0	CA		8	×	8	8	•

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

5. Select the **Enable CA** checkbox then choose a certificate (in this example, **Copy of Smart Card Certificate**...was used), then select **Enabled (allow issuance)**.

The options are ungraded.

<ol> <li>MyID Desktop</li> </ol>		- 🗆 X
=		M
Certificate Authorities		
Certificate Authority		
CA Name: myiddemo-WINDOWSSERVER-0-CA C	A Description:	^
CA Type: Microsoft Enterprise	Retry Delays: 15;60;60;60;60;120;180;3600;3600;864	
CA Path: WindowsServer-0.myiddemo.com\myiddemo-WINDO	WSSERVER-0-CA	
Set Certificate Store:		
Enable CA: 🗹		
Available Certificates	✓ Enabled (Allow Issuance)	
Administrator on myiddemo-WINDOWSSERVER-	Display Name: Copy of Smartcard User on myiddemo-WINDO	
DirectoryEmailReplication on myiddemo-WINDO	Description:	
DomainController on myiddemo-WINDOWSSERV	Allow Identity Mapping:	
eden on myiddemo-WINDOWSSERVER-0-CA	Reverse DN:	~
EFS on myiddemo-WINDOWSSERVER-0-CA	Archive Kevs: None 🗸	
	Comp.	Cancel
	Save	Cancel

(The screen image above is from MyID<sup>©</sup> software. Trademarks are the property of their respective owners.)

- 6. Scroll down and set the options for the policy (in this example the following was configured):
  - Certificate Storage Both
  - Recovery Storage Both
  - CSP Name Microsoft base cryptographic provider v1.0
  - Key algorithm RSA 2048
  - Key purpose Signature an Encryption
- 7. Click Save and Finish.

te Authorities	
te Authorities	
Certificate Authority	
Administrator on myiddemo-WINDOWSSERVER-	Display Name: Copy of Smartcard User on myiddemo-WINDO
DirectoryEmailReplication on myiddemo-WINDO	Description:
DomainController on myiddemo-WINDOWSSERV	Allow Identity Mapping:
DomainControllerAuthentication on myiddemo-V eden on myiddemo-WINDOWSSERVER-0-CA	Reverse DN:
EFS on myiddemo-WINDOWSSERVER-0-CA	Archive Keys: None 🗸
EFSRecovery on myiddemo-WINDOWSSERVER-0-	Certificate Lifetime: 365
Machine on myiddemo-WINDOWSSERVER-0-CA	Automatic Renewal: 🔽
SubCA on myiddemo-WINDOWSSERVER-0-CA	Certificate Storage: O Hardware O Software O Both
WebServer on myiddemo-WINDOWSSERVER-0-C	Recovery Storage: O Hardware O Software O Both O None
Workstation on myiddemo-WINDOWSSERVER-0-	CSP Name: Microsoft Base Cryptographic Provider v1.0
	Requires Validation
* = Enabled Policy	Private Key Exportable:
	Key Algorithm: KSA 2048
	Save

(The screen image above is from MyID<sup>©</sup> software. Trademarks are the property of their respective owners.)

#### **Configure Credential Profile**

Credential profiles are used for setting all of the elements that you want to include when issuing credentials to the device. This profile will be used when issuing card.

1. Open MyID Desktop client and connect to MyID server with privileged user.

0	MyID Desktop	- 0 X
	WiD Welcome to MyID	
	Security Questions Enter your username Username: startug	
		Next
	© 2018 Intercede	

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

2. In MyID Dashboard, click Start a new action.

Dashboard				
Welcome startup user				
Messages				
The second baseline display	erester the last to be	COMPANY AND A	10.5	
• Actions				
Start a new action				
(The screen image above is from M	yID <sup>©</sup> software. Trademarks are	the property of their respec	tive owners.)	

3. In the left pane click Configuration and then click Credential profiles.

Ð	New Action									×
Jump <sup>-</sup>	Го									^
è	People	Configu	ration		1/2/14					
	Cards	-0	Add Devices	>	Co.	Audited Items	≥	-0	Card Layout Editor	2
	Certificates	2	Card Stock	Þ		Certificate Authorities	⇒	20	Credential Profiles	>
	Applets		Directory			- 11		502		
٥	Configuration		Management	7	-0	dit Devices	7	$\mathcal{O}$	Edit Roles	
	Device Identities		Email Templates	÷	0	External Systems	÷	-0	Import Serial Numbers	•
	Mobile Devices		Job Management		0	(ev Manager		Ċ.	licensing	
	Reports	-0	soo monsperiere		00	ici manager		~0	LICENSING	- I
		Ó	List Editor	×		Notifications Management	$\rightarrow$	¢,	Operation Settings	<b>&gt;</b>
		ŝ	Security Settings	÷						
										~

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

4. To create a new profile, click New

i) MyID Desktop							- 0
							My My
Credential Profiles							
Select Credenti	al Profile						
Select Credential Profil	e: Manager	V	Details >				
Name	Manager						
Description	One year system access						
Show History >							
				New	Modify	Сору	Delete

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

5. In the **Name** field, enter the profile name (in this example **SmartCard**) and select the features you use on the card (in this example **Contact Chip**). Enter a description if required.

) MyID Desktop				- 0
=				e e e e e e e e e e e e e e e e e e e
Credential Profiles				
Credential F	Profile			
Name: Sn	nartCard	×	Description:	
C Si IS P P M C D	ard Encoding ervices isuance Settings IN Settings IN Characters fail Documents ard Stock eevice Profiles		Card Encoding Contact Chip:  Contactless Chip: Contactless Chip: Magnetic Stripe (Only): Software Certificates (Only): Device Identity (Only): Identity Agent (Only): Externally Issued (Only): Derived Credential	
				Next >

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

6. Select Services. For this example, select MyID Logon and MyID Encryption.

rofiles		
Credential Profile		
Name: SmartCard	Description:	
Card Encoding Services Issuance Settings PIN Settings PIN Characters Mail Documents Card Stock Device Profiles	Services MyID Logon: 🗹 MyID Encryption: 🗹	

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

- 7. Click **PIN Settings (**in this example, **Issuance Settings** default settings were used).
  - When using smart card, make sure you set up the PIN policy and the MyID credential profile to match the policy and capabilities of the card.
  - When using SAC, make sure the PIN password policies defined in SafeNet Authentication Client correspond with the policy configured in the MyID credential profile, then save your settings. See "Token Settings" in SafeNet Authentication Client 10.5 Windows User Guide

In this example **Max pin Length** is changed to 16 and **Min pin Length** is changed to 6. All other settings are left as default.

lesktop		- 0
tial Profiles		
Credential Profile		
Name: SmarCard	Description:	
Card Encoding Services Issuance Settings PIN Characters Mail Documents Card Stock Device Profiles	PIN Settings Maximum PIN Length: 16 Minimum PIN Length: 6 Repeated Characters Allowed: 0 Sequential Characters Allowed: 0 Logon Attempts: 5 PIN Inactivity Timer: 180 minutes PIN Inactivity Timer: 180 minutes PIN History: 0 Issue With: User specified PIN (default) ✓ Email PIN: 5	
	Length: D PIN Algorithm: Select PIN Algorithm V Protected Key: Select Protected Key V	
		Next >

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

- 8. Click **PIN Characters** and under **PIN Characters** specify the format of the passwords. Click **Next (**Mail documents, Cars Stock, Device Profile left as default.).
  - When using a smart card, make sure you set up the PIN policy and the MyID credential profile to match the policy and capabilities of the Card.
  - When using SAC, make sure the PIN password policies defined in SafeNet Authentication Client correspond with the policy configured in the MyID credential profile, then save your settings. See "Token Settings" in "SafeNet Authentication Client\_10.5\_Windows\_GA\_User\_Guide\_Rev A"

(In this example, PIN Characters are left as default)

Credenti	al Profile						
Name	SmartCard	Descri	ption:				
	Card Encoding Services	PIN Characters	0	ptional	Mandatory	Not Allowed	
	Issuance Settings		Lowercase:	۲	0	0	
	PIN Settings PIN Characters		Uppercase:	۲	0	0	
	Mail Documents		Numeric:	۲	0	0	
	Card Stock Device Profiles		Symbol:	۲	0	0	

SafeNet Authentication Client: Integration Guide Using SafeNet Authentication Client CBA for MyID Version 10.8 Update 2 Document Number: 007-000161-001, Rev. A

- 9. Leave Mail Documents, Card Stock, and Device Profile with their default settings.
- 10. Click Next.
- 11. Select the Certificate to be enrolled (in this example Copy of Smart Card User was used).
- 12. Select the required **Action Issue new** settings (in this example **Signing**, **Encryption** and **Default** were enabled).
- 13. Click Next.

MyID Desktop			– 0 ×
			<b>M</b>
Credential Profiles			
Select Certificates	]		
	Please select the certificates that you	wish this credential profile to have	
Required	Certificate Policy Description		
Copy of Smartcard User on myiddemo- WINDOWSSERVER-0-CA			
Action Issue new	Signing 🗹	Encryption 🗹	Default 🗹
Unmanaged*	Unmanaged certificate		
	Show inactive ce	rtificate policies	
* Cer	tificate is set for key archival, these can only b	e issued if the credential profile supports encry	ption
			Next >

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

14. Applets were not used in this example, click Next.

<ol> <li>MyID Desktop</li> </ol>		- 0 ×
		M
Credential Profiles		
Select Applet		
	There are currently no Applets available.	
		Next >

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

15. In Select Roles Select the role that will use this Credential profile (in this example Cardholder and Startup user) click next.

Select Roles							
			Plea	ise select th	e roles that can use this cre	edential profile	
	All / None	All / None	All / None	All / None			
	Can Receive	Can Reques	st Can Validat	e Can Collect	_		
	~	~	~	~	Cardholder	Default Cardholder profile	
					Derived Credential Owner	Person who holds a derived credential	
					Device Account	Used for issuing identities to devices	
					Help Desk	Help Desk Operator	
					Manager	Line Manager	
					Mobile User	Used to handle mobile device activation	
					Personnel	Personnel	
					Security Chief	Security Policy Controller	
		~	1	~	Startup User	Bootstrap User	

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

16. Card layouts were not used in this example. Click Next.

<ol> <li>MyID Desktop</li> </ol>		
		M
Credential Profiles		
Select Card Layout		 
	There are currently no card layouts available.	
		Next >

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

#### 17. In the Comments text box, add your comment and click Next

(i) MyID Desktop		- 🗆 X
=		M
Credential Profiles		
Add Comments		
Comments: S Pl Th Th	ease provide a summary of the changes made to the credential profile. ease provide a summary of the changes made to the credential profile. e current version of this credential profile is 1. e version of this credential profile about to be saved is 2.	
	Cancel	Next

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

#### 18. Click Finish

D MyID Desktop			- 0 ×
≡ (			MyiD
		Successfully completed Credential Profiles	
👩 Details			
Start Time	Logon Name startup		
Additional Information			~
> Next			
Start a new action	Dashboard		
			Finish

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

#### **Client Side Configuration**

- On the client side, the smart card/token middleware must be installed and the devices recognized.
- MyID Desktop version 2.7.1001 must be installed.

#### **Important Note**

When using SafeNet Authentication Client the property **SAC Administrator Password Quality Check** must be disabled.

For more information see SafeNet Authentication Client 10.5 (GA) Administrator Guide

# **Running the Solution**

#### **Issue a Card**

In this example a privileged user will issue a card for domain user with SAC 10.6 installed.

- eToken smart card is connected to the machine.
- 1. In MyID Desktop client, connect to MyID server with privileged user.

0	MyID Desktop	- 0 X
	Win Welcome to MyID	
	Security Questions Enter your username Username: startup	
		Next
	© 2018 Intercede	

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

2. In MyID Dashboard click Start a new action.

<b>i</b>	MyID Desktop	- 0 X
Ξ	Dashboard	
ê	Welcome startup user	
	Messages	
You	r current Evaluation Only license expires in less than 31 day(s). (Saturday, May 12, 2018 3:00 PM)	
	Actions	
	Start a new action	

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

3. In the left pane, click Cards



(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

4. In the Cards window click Issue Card.

Đ	New Action									×
Jump 1	o									^
<b>e</b>	People	Cards								
	Cards		Assign Card	$\rightarrow$	Assi:	sted Activation	→	-0	Batch Collect Card	
	Certificates	-0	Batch Encode Card	$\rightarrow$	Batc	h Request Card	$\rightarrow$		Cancel Credential	
	Applets	-	Card Disposal	_→		ect Card	→		Collect My Card	3
Φ	Configuration	E			EQ			EØ	1	-
	Device Identities	20	Collect My Updates	$\rightarrow$	Deliv	ver Card	⇒	-0	Enable / Disable Card	2
	Mobile Devices	-8	Erase Card	→	Iden	itify Card	>	-0	Issue Card	<b>•</b>
B	Reports									
		-0	Issue Temporary Replacement Card	>	Po Man	nage VSC Access	(>	-0	Print Badge	<b>&gt;</b>
		-0	Print Card	≥	Print Doct	t Mailing ument	>		Reinstate Card	Þ

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

5. In the Issue Card screen enter the user's name (In this Example Bob.) and click Search.

D Desktop		 ٥
Card		
Find Person		
Title: First Name: Bob	X Initial: Last Name:	
Logon:	Enabled: Any	
Employee ID:	Group: LDAP Root Rolude Subgroups: 오	
		Se

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

6. In the Issue Card screen, under Search results, select the user's checkbox.

(i) MyID Desktop				- 0
Issue Card				
	Search results			
a				Rows: Auto Y Page 1 of 1
	Logon Name	Last Name	First Name	Group
	bob		bob	Users

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

7. In the Issue Card screen, in the Select Credential Profile drop-down list, select the required profile (in this example, Smart Card) and click OK.

<ol> <li>MyID Desktop</li> </ol>			– 0 ×
=			<b>MD</b>
Issue Card			
Select Creden	tial Profile		
Select Credential Pro	file: SmartCard Details >		
Name Description	SmartCard		
Certificates	Copy of Smartcard User on myiddemo-WINDOWSSERVER-0-CA 🤌 🖍 🖴 Certificate Key P = Default Certificate X = Used for Login/Signing = Used for Encryption		
		ок	Cancel

(The screen image above is from MyID<sup>®</sup> software. Trademarks are the property of their respective owners.)

8. Enter and confirm the **Pin**, according to the policy configured, and click **Next**.

D MyID Desktop		- 0 >
		MyiD
Issue Card		
Create Card	1	
bob	The PIN must:	
0	🖉 Match	
	Se between 6 and 16 characters in length	
	Not contain unsupported characters	
New PIN:	Details >	
Confirm PIN:		
Card Label: bob		
		Next > Abort

(The screen image above is from  $MyID^{\odot}$  software. Trademarks are the property of their respective owners.)

The card issuance procedure starts.



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

9. When successfully completed, the Issue Card procedure is complete. Click Finish.

① MyID Desktop	-	٥	×
		My	9
Successfully completed Issue Card			
Details			2
Start Time Logon Name start up			
Additional Information		~	
> Next			
Start a new action Dashboard			0
	_		
	Fi	nish	

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

#### Smart Card Log in to MyID Desktop

- 1. Connect an enrolled token or smart Card.
- 2. Open MyID Desktop.

() My/D Desktop	WP Welcome to MyID	_ 0 >
	Smart Card Logon       Security Questions         Connect or select a smart card         Image: Serial Number:       C2822996         Serial Number:       C2822996         Type:       Aladdin eToken         Enter PIN:	
	Log on Reset PIN	
	© 2018 Intercede	

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

3. Enter the token or smart card PIN (in this example, eToken is demonstrated) and click Login.

🕽 MyID Desktop		- 0	×
	WID Welcome to MyID		
	Smart Card Logon     Security Questions       Connect or select a smart card		
	Serial Number: 02822996 Type: Aladdin eToken Enter PIN:		
	Log on Reset PIN		
	© 2018 Intercede		

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

The user successfully logged in to MyID desktop.

) MyID Desktop	– 0 ×
Dashboard	M
Welcome bob	
Messages	
The system is not configured for production use - please contact your administrator	
Actions	
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)	

# **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			
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017 USA			
Phone	United States	1-800-545-6608		
	International	1-410-931-7520		
Technical Support Customer Portal	https://serviceportal.safenet-inc.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.			