SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for MyID Version 10.8 Update 2

gemalto
security to be free

Document Number: 007-000161-001, Rev. A

Release Date: October 2018

Contents

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:

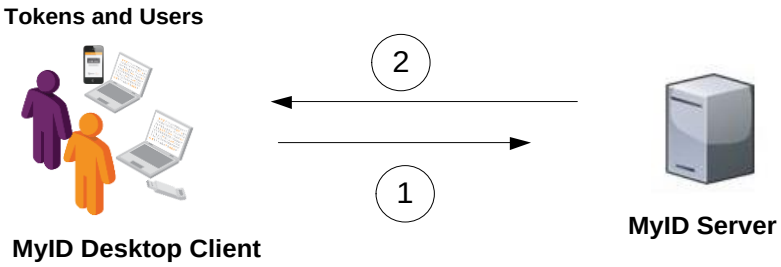
- **SafeNet Authentication Client (SAC)** - 10.6
- **Gemalto SafeNet MiniDriver - 10.2**
- **MyID Version 10.8 Update 2** - installed on Microsoft Windows server 2012R2
- **Microsoft DC and CA -** installed in Windows Server 2008R2
- **MyID Desktop - 2.7.1000.1 -** Installed on Win 10 x64 1709

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 certificate-based 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 MyId 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	Gemalto SafeNet MiniDriver
IDPrime MD 830 B L3	
IDPrime MD 830 B L2	
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

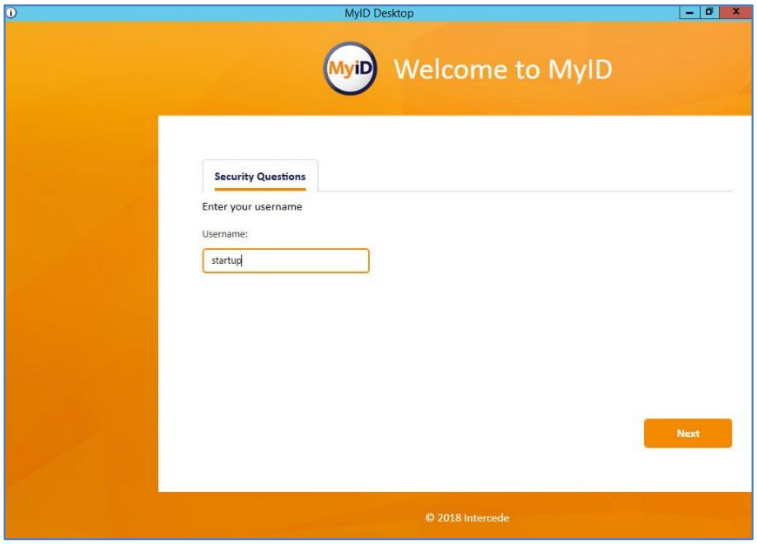
This section will demonstrate how to configure CBA with SafeNet Tokens in MyID Version 10.8 Update 2.

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.

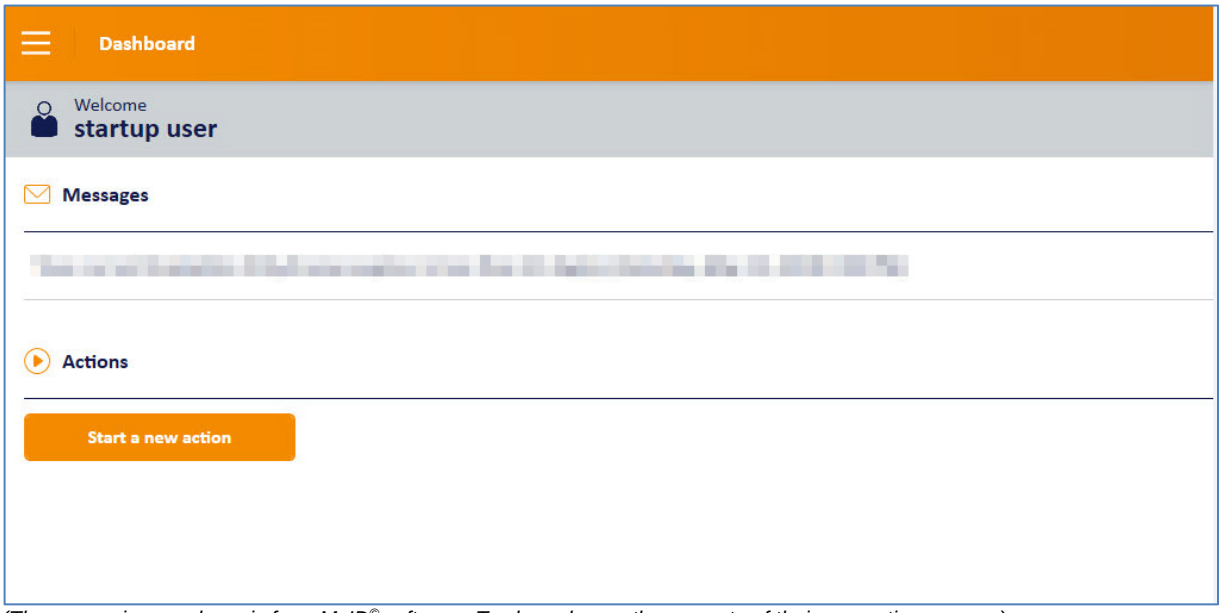
Configure certificate templates for issuance within MyID

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



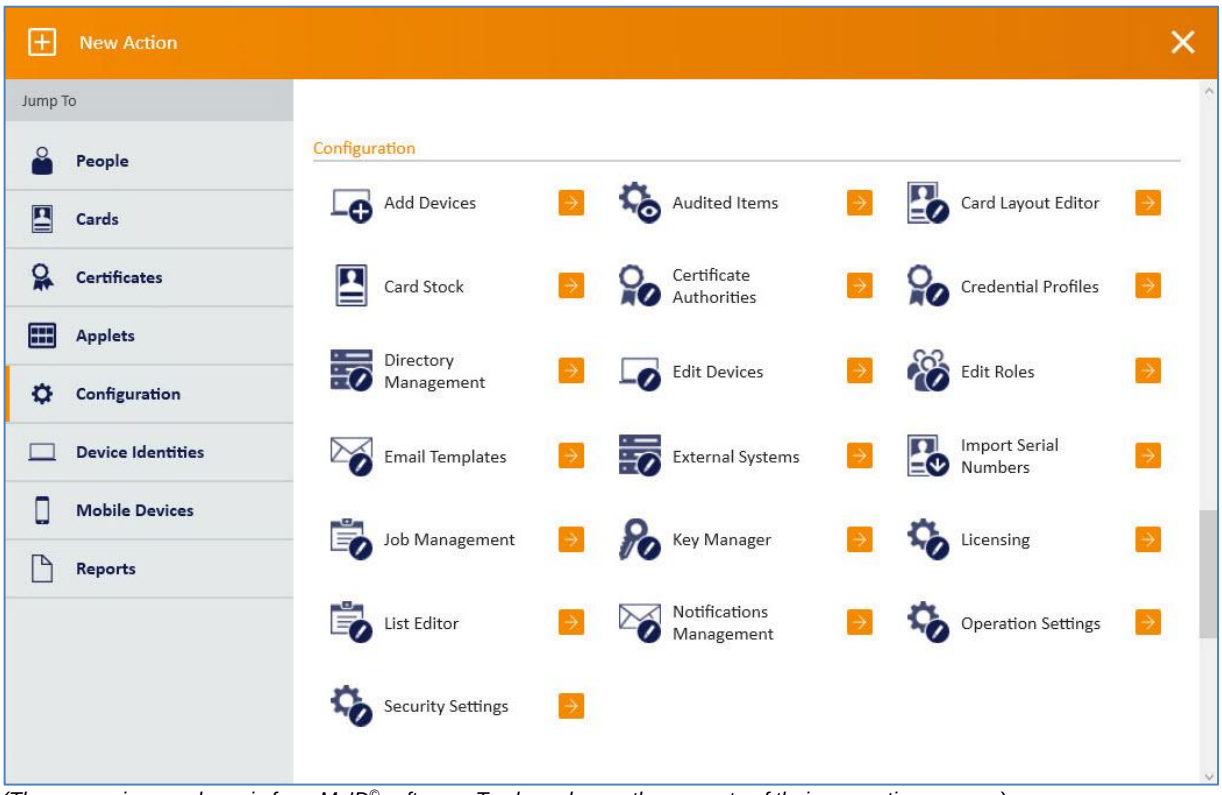
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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



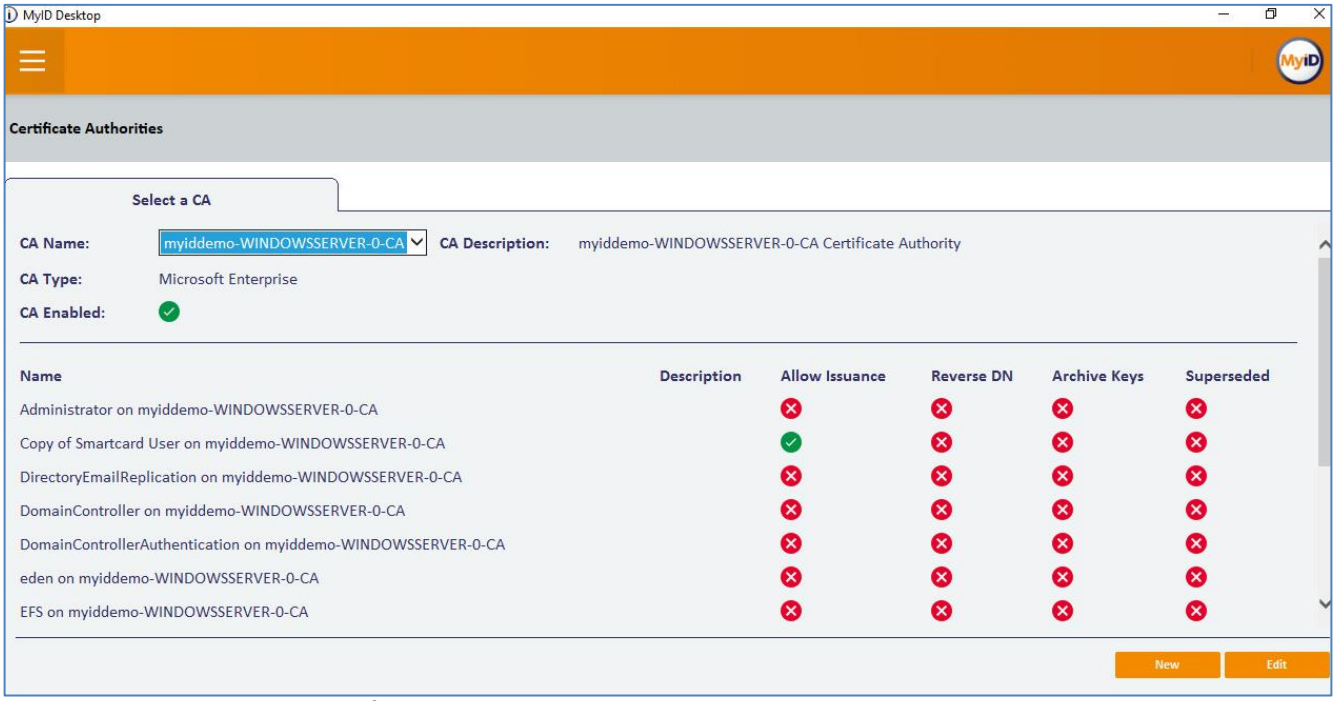
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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



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

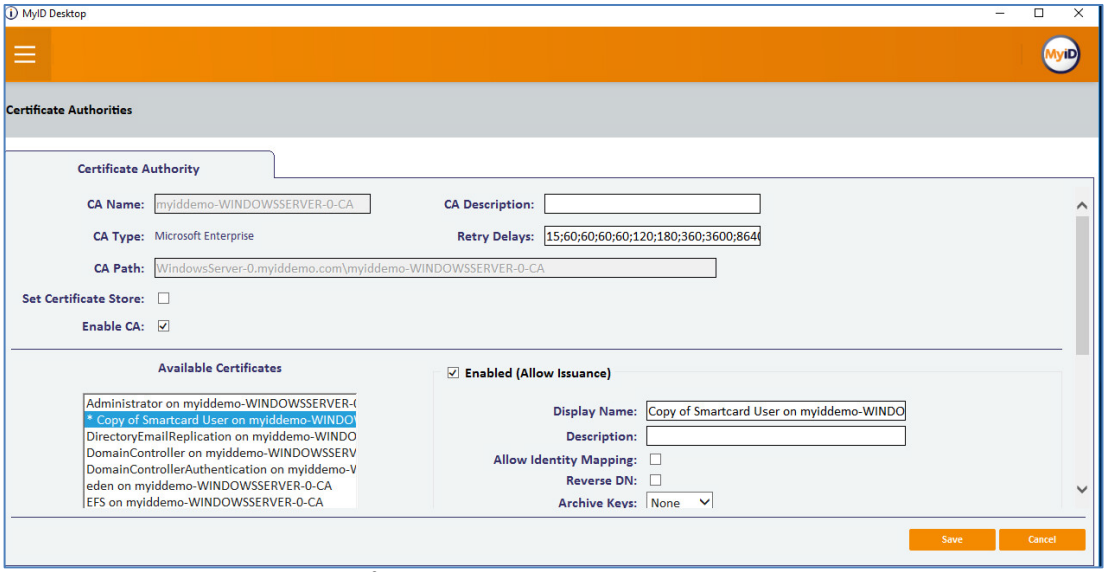
4. In the **Certificate Authorities** window, from the **CA Name** list, select your CA server and click **Edit.**



(The screen image above is from MyID® 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.

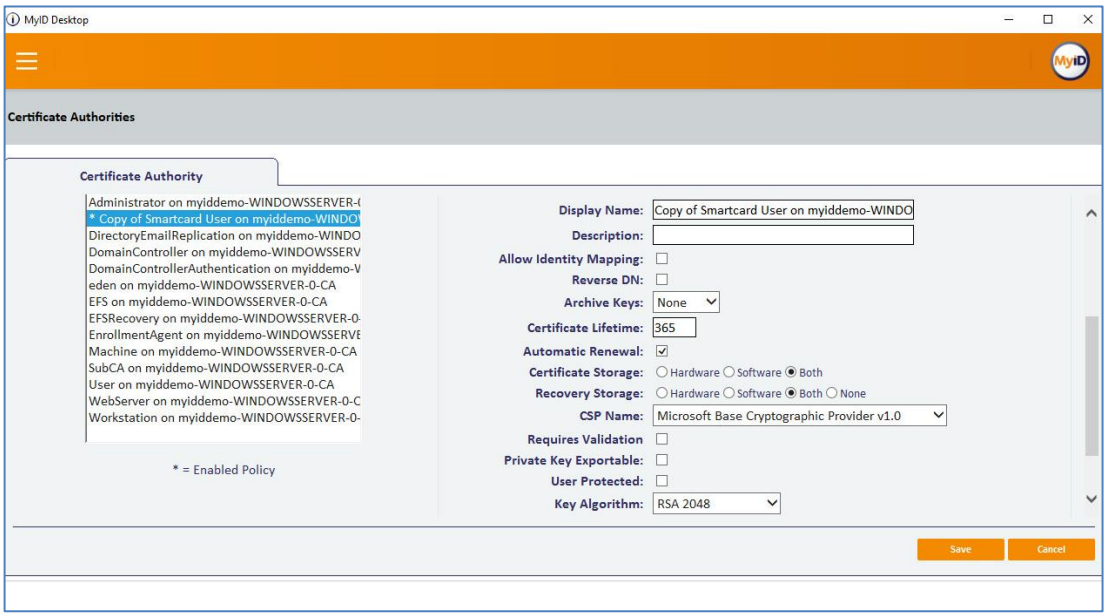


(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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.**

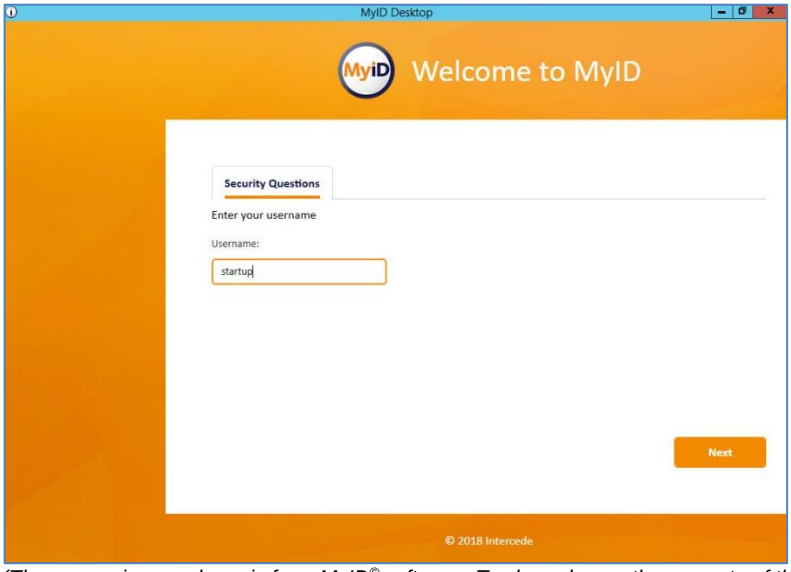


(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

Configure Credential Profile

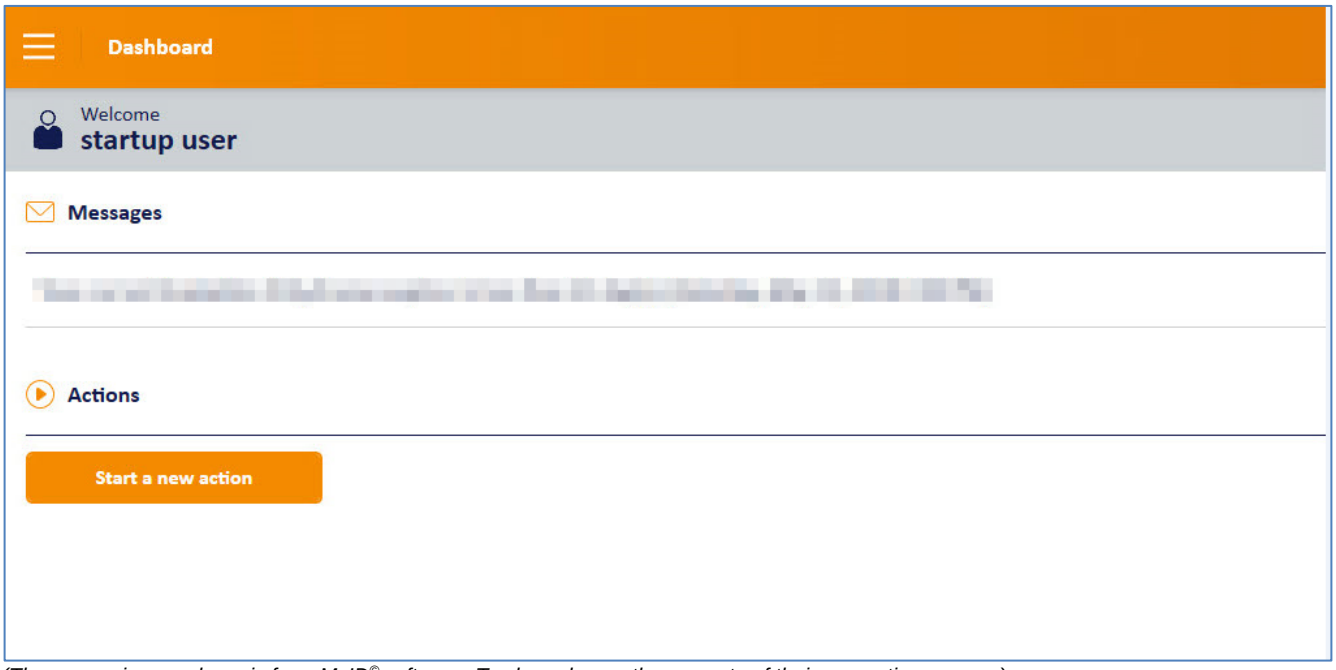
Credential profiles are used for setting all of the elements that you want to include when issuing credentials to the device. This profile will be used when issuing card.

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



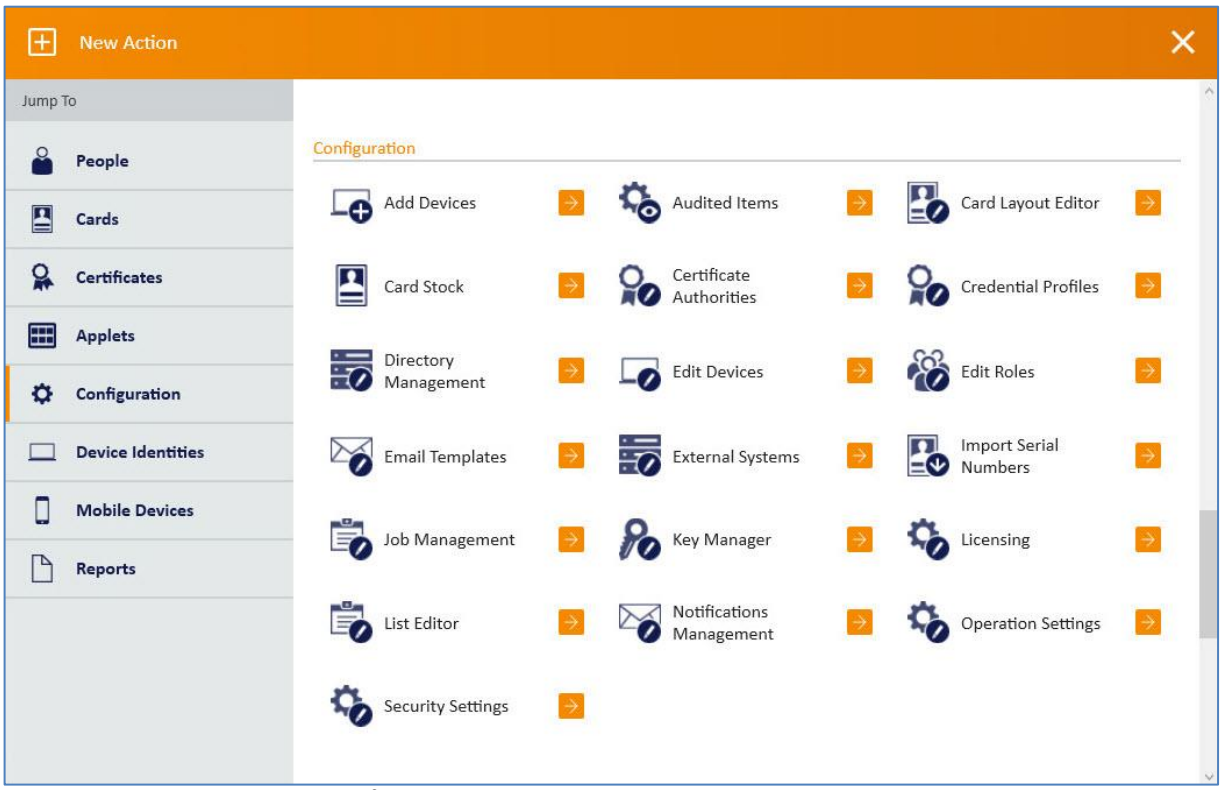
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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



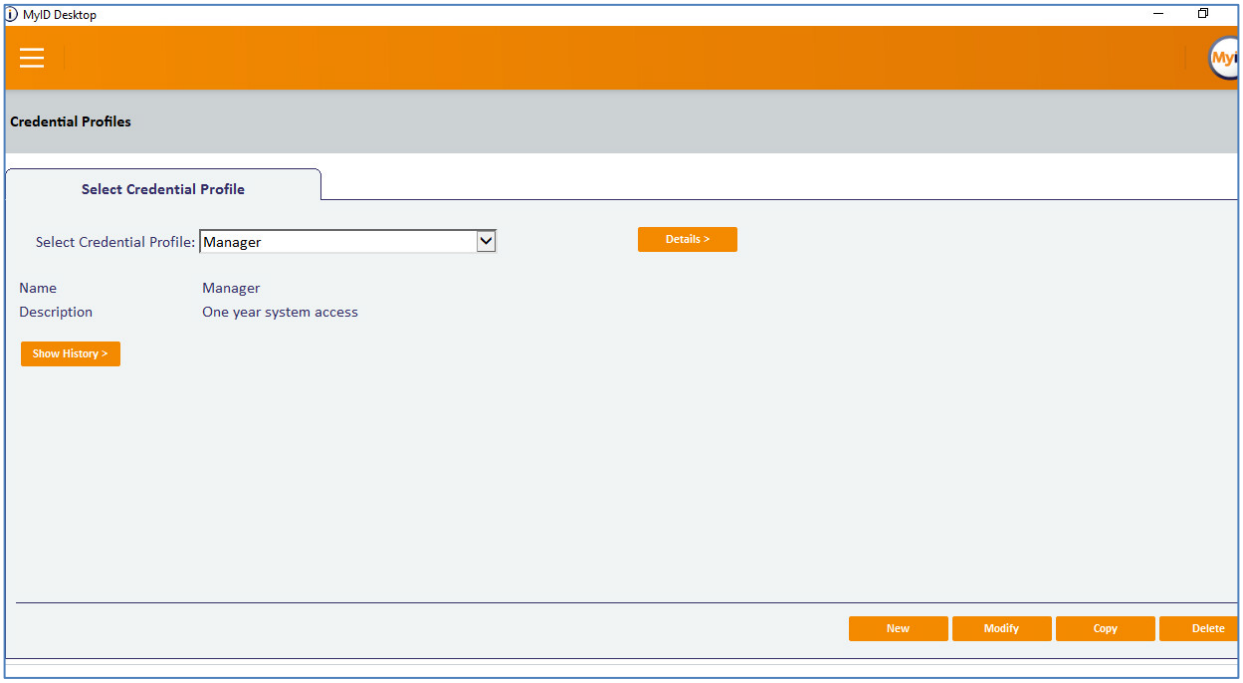
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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



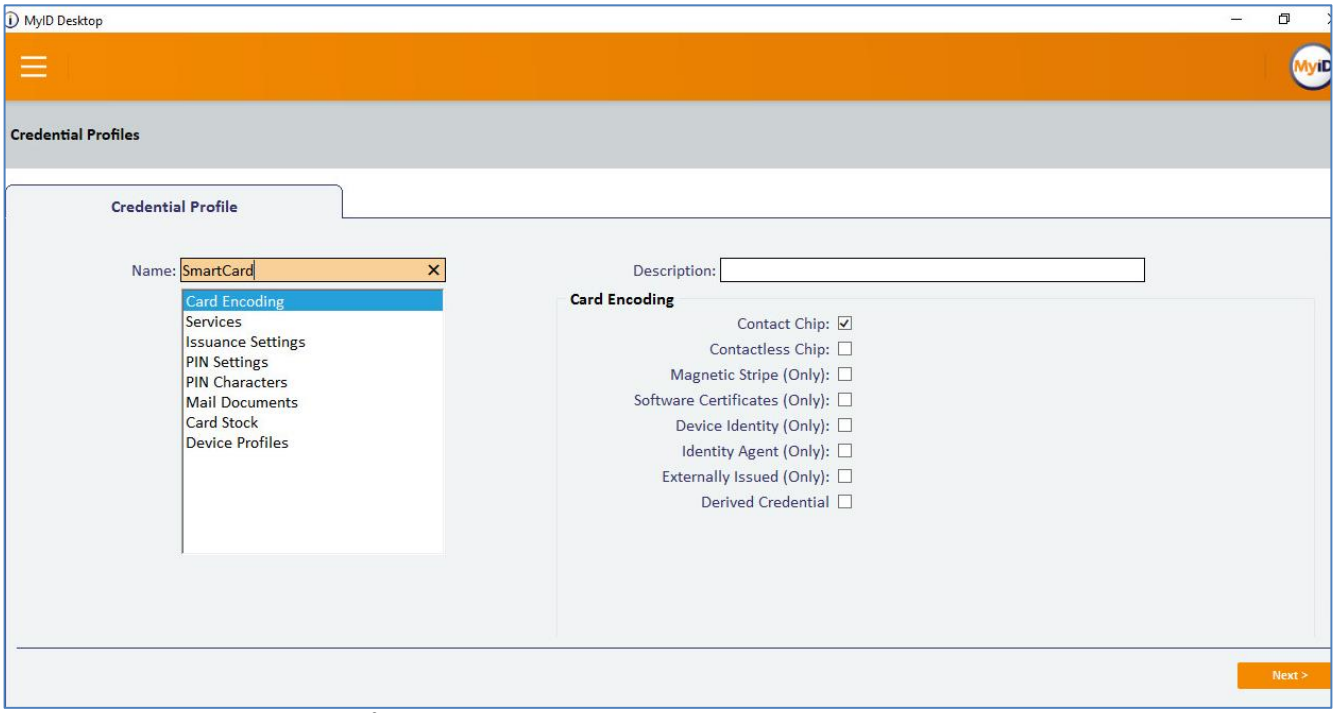
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

4. To create a new profile, click **New**



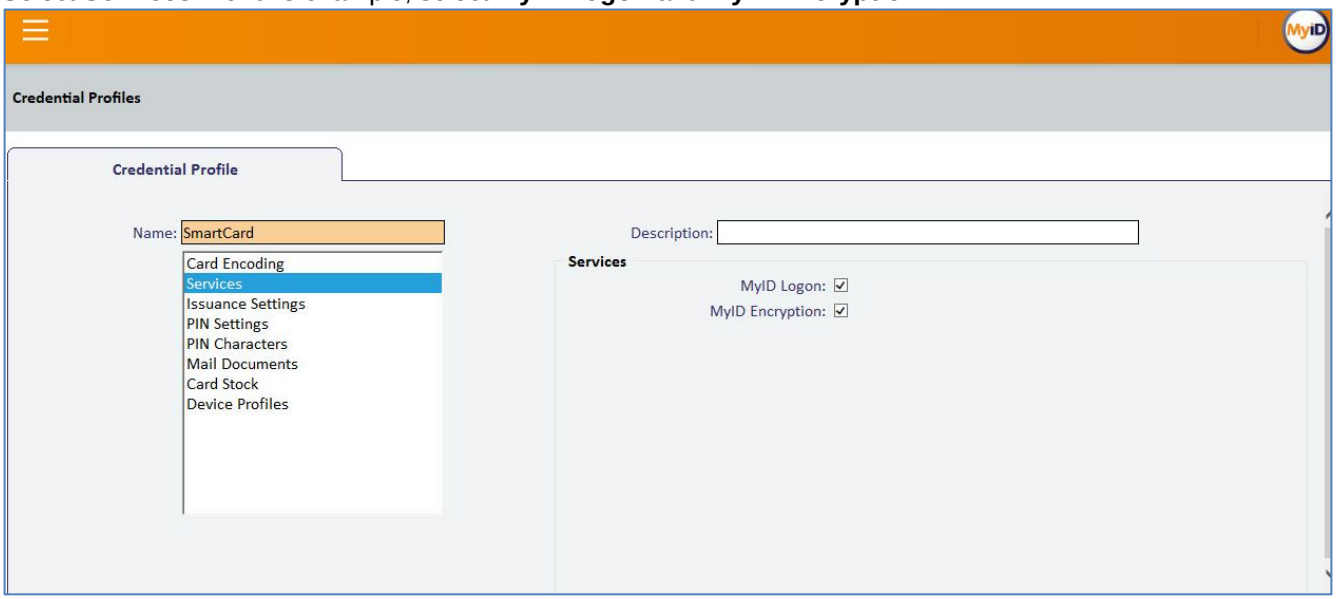
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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.



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

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

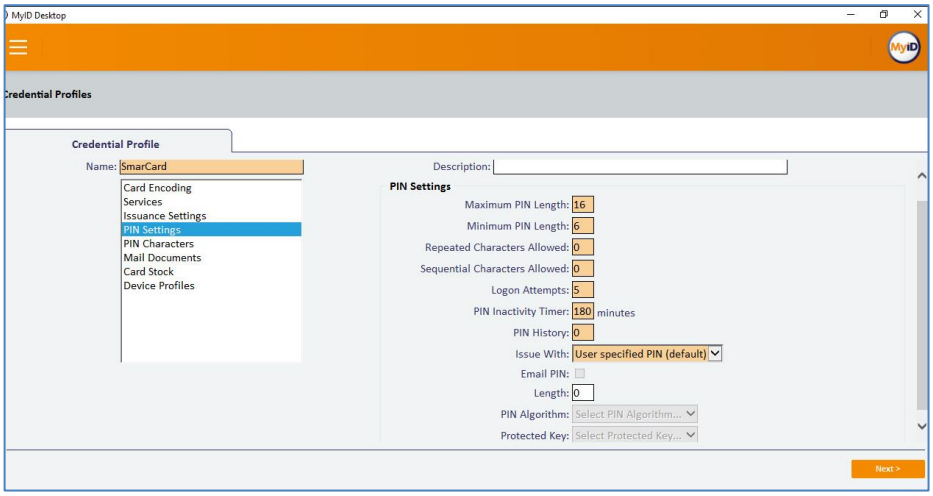


(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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.

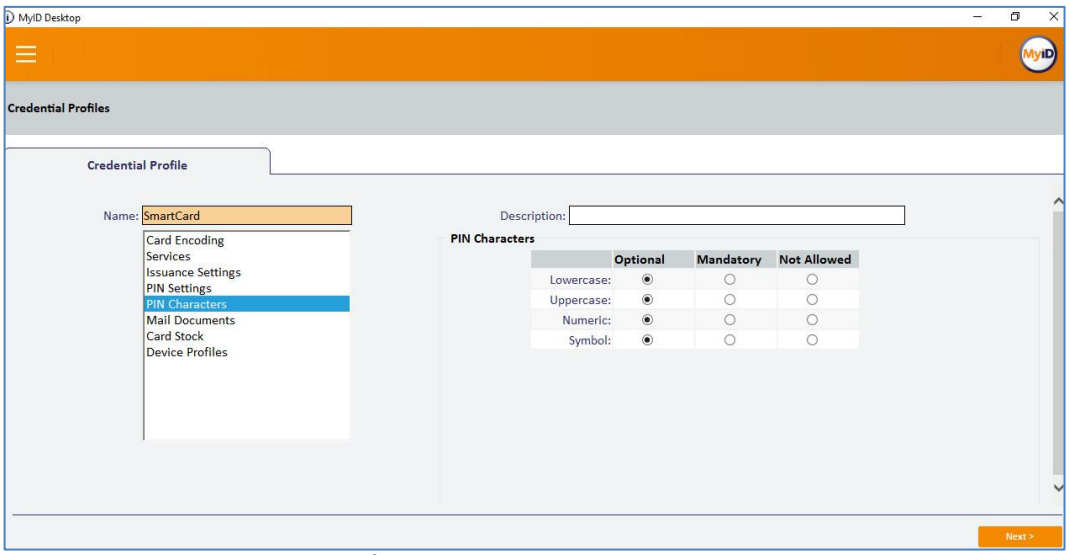


(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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**.).**

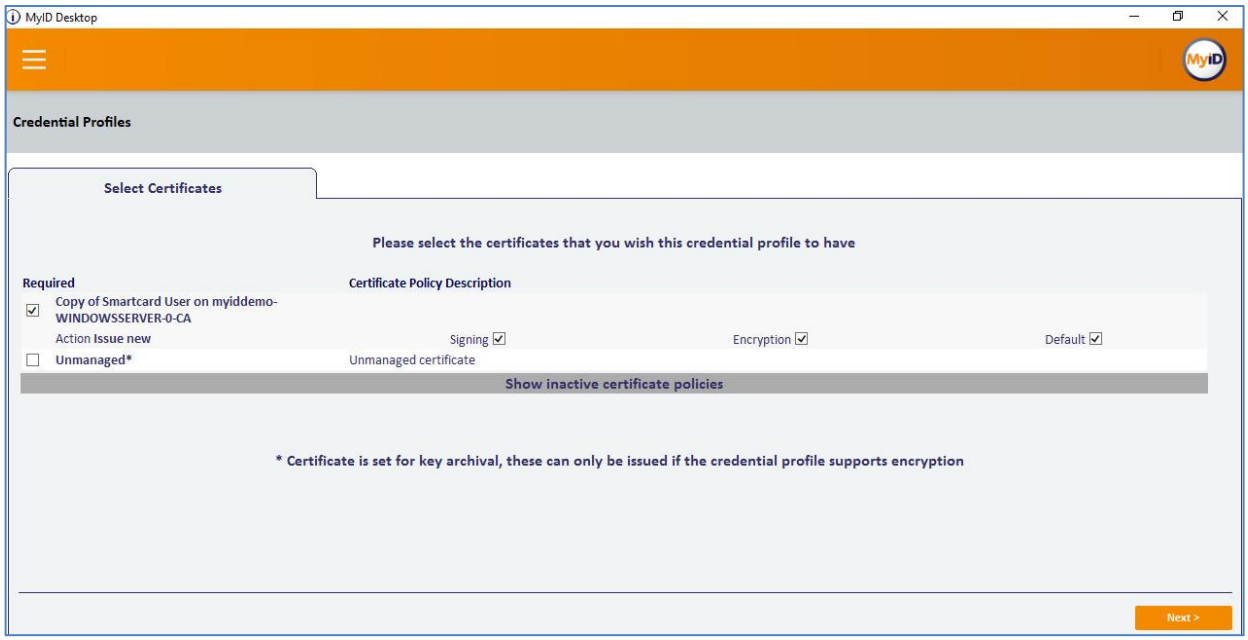
   - When using a smart card, make sure you set up the PIN policy and the MyID credential profile to match the policy and capabilities of the Card.
   - When using SAC, make sure the PIN password policies defined in SafeNet Authentication Client correspond with the policy configured in the MyID credential 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)



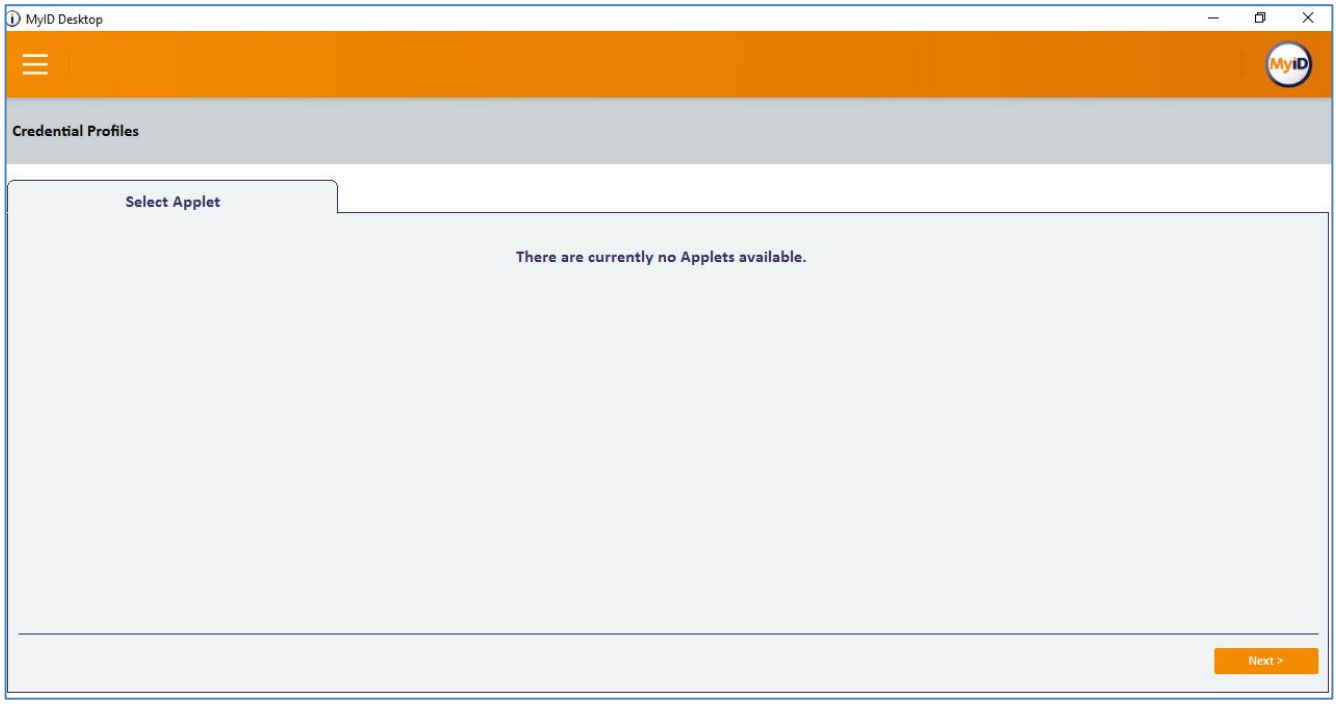
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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.**



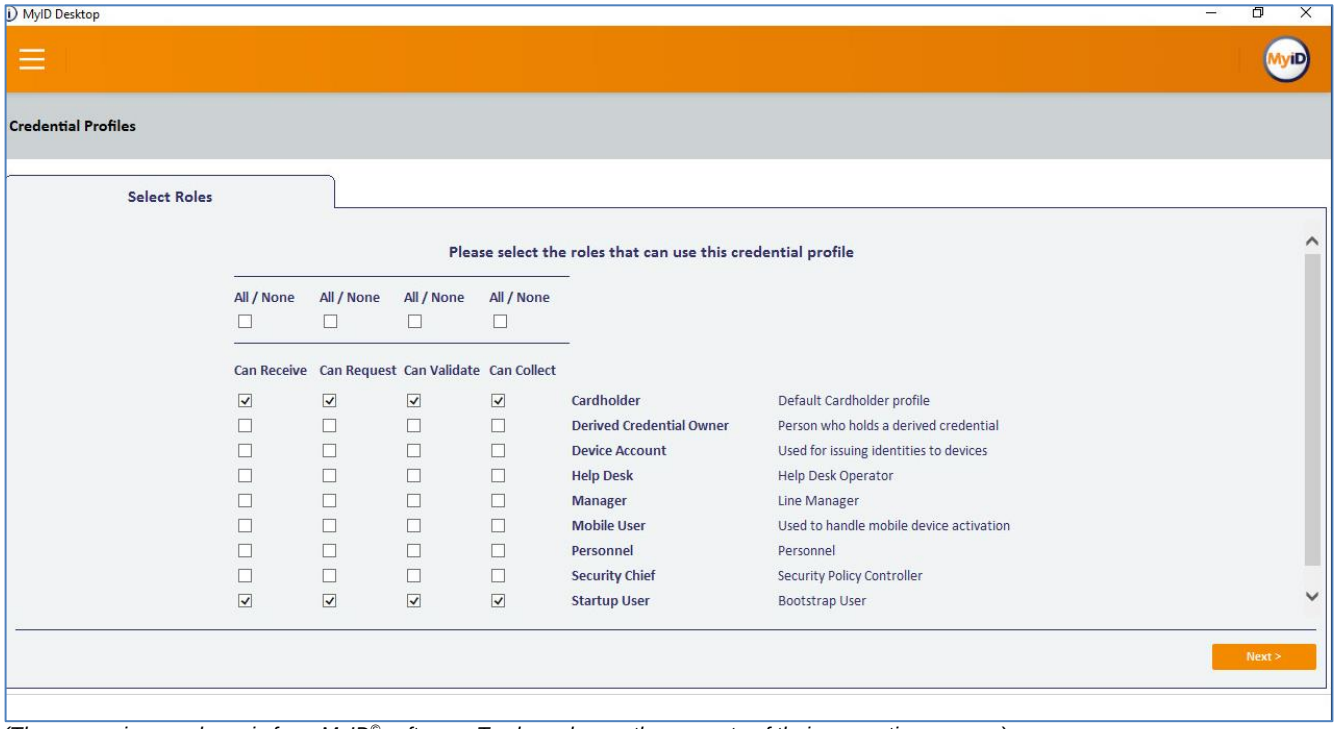
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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



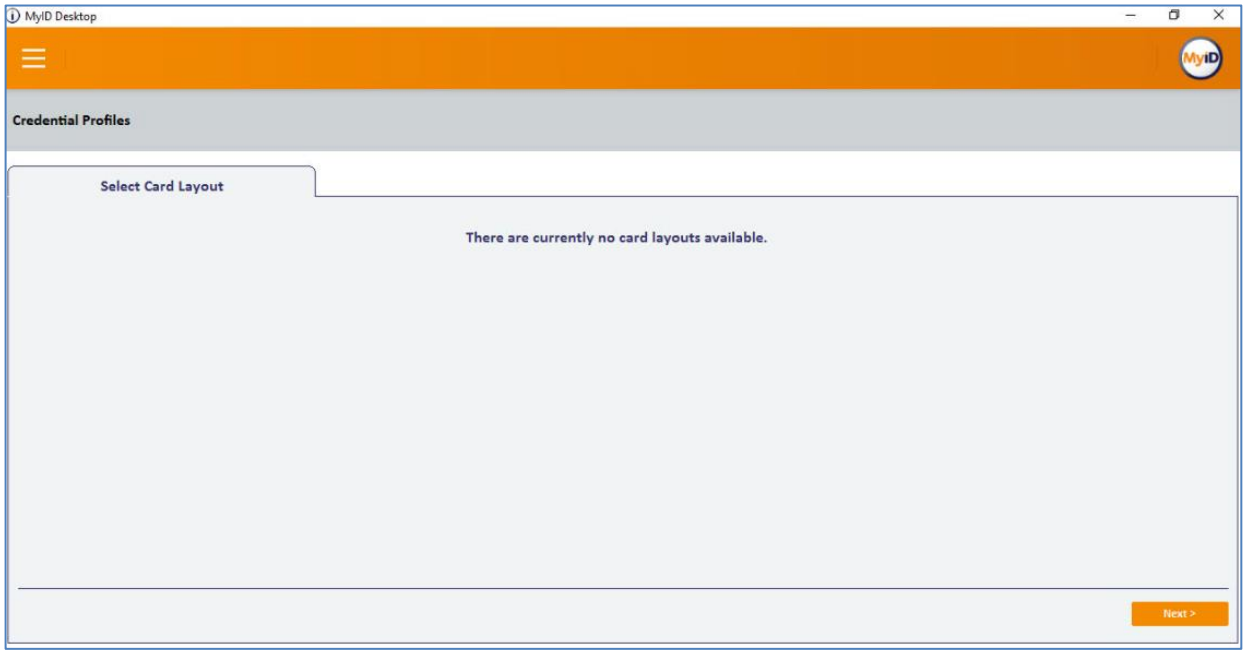
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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



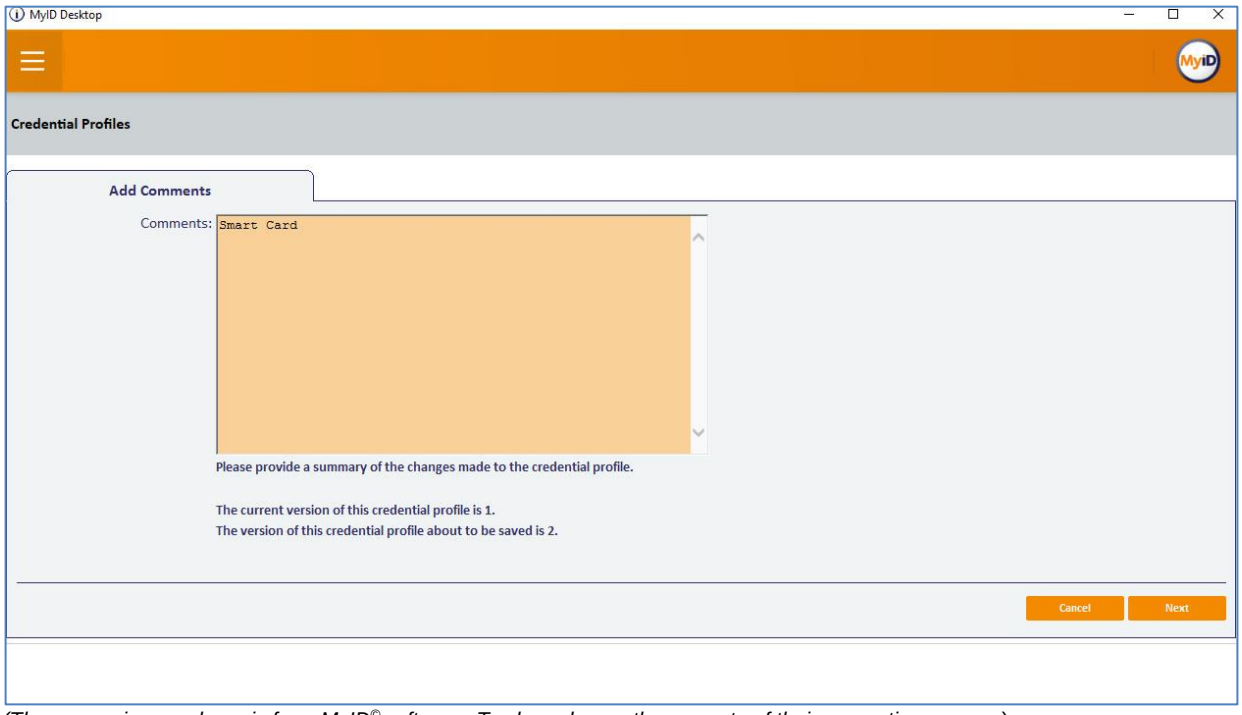
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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



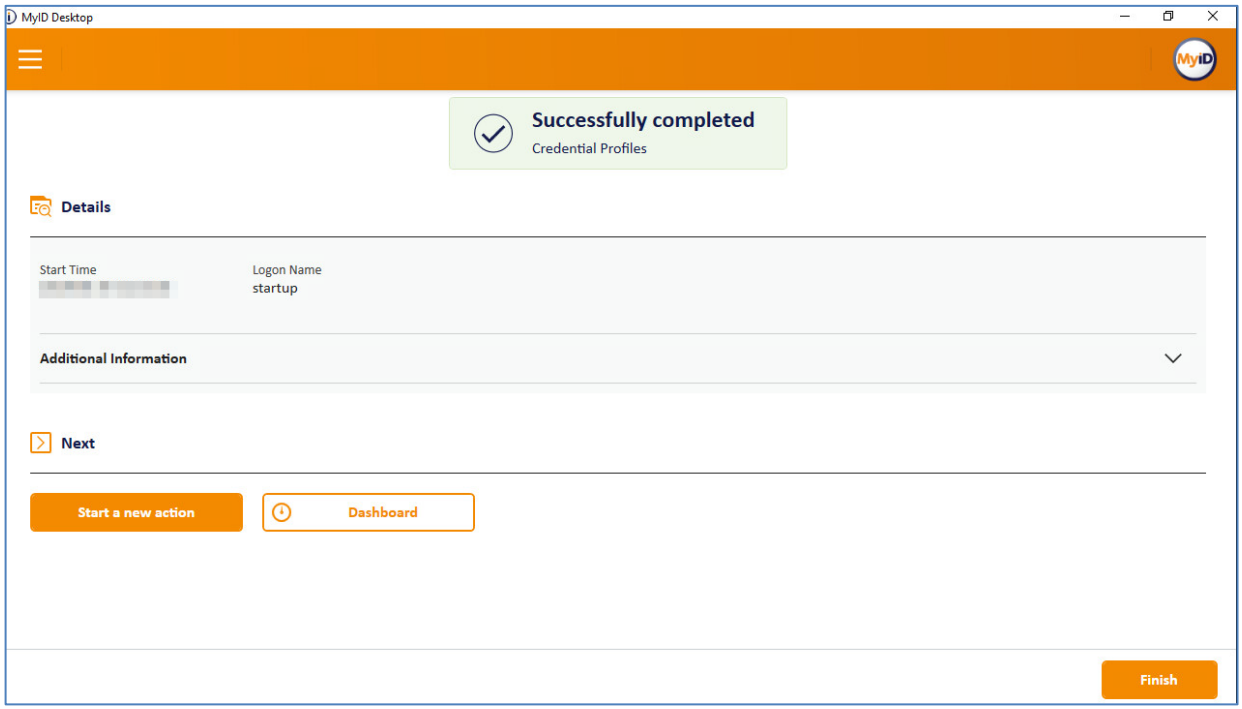
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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



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

18. Click **Finish**



(The screen image above is from MyID© 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*

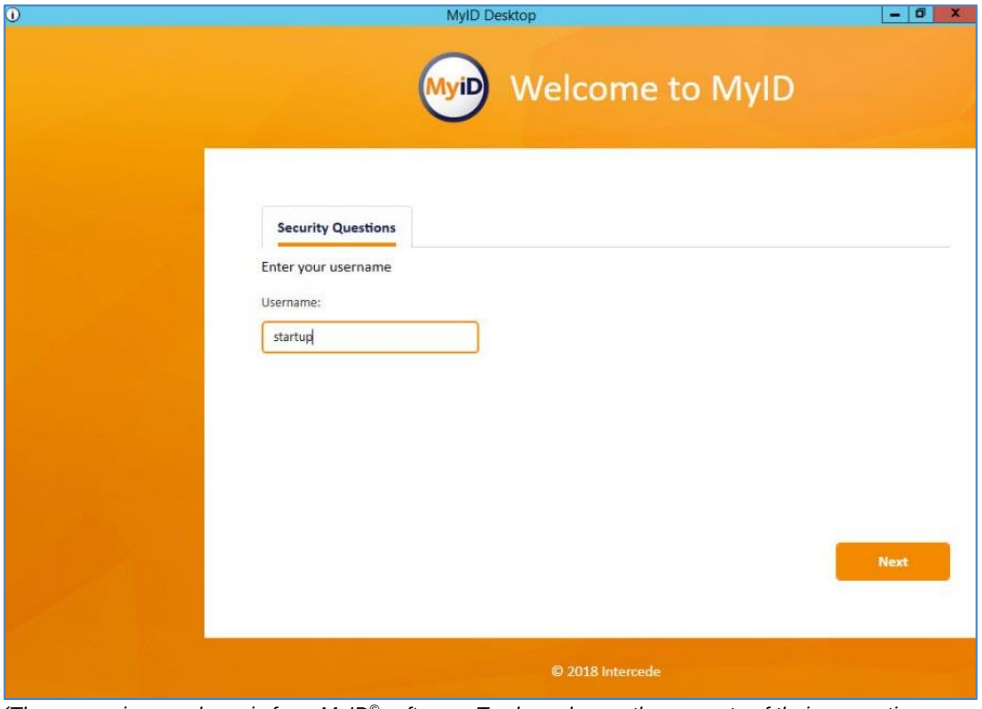
Running the Solution

Issue a Card

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

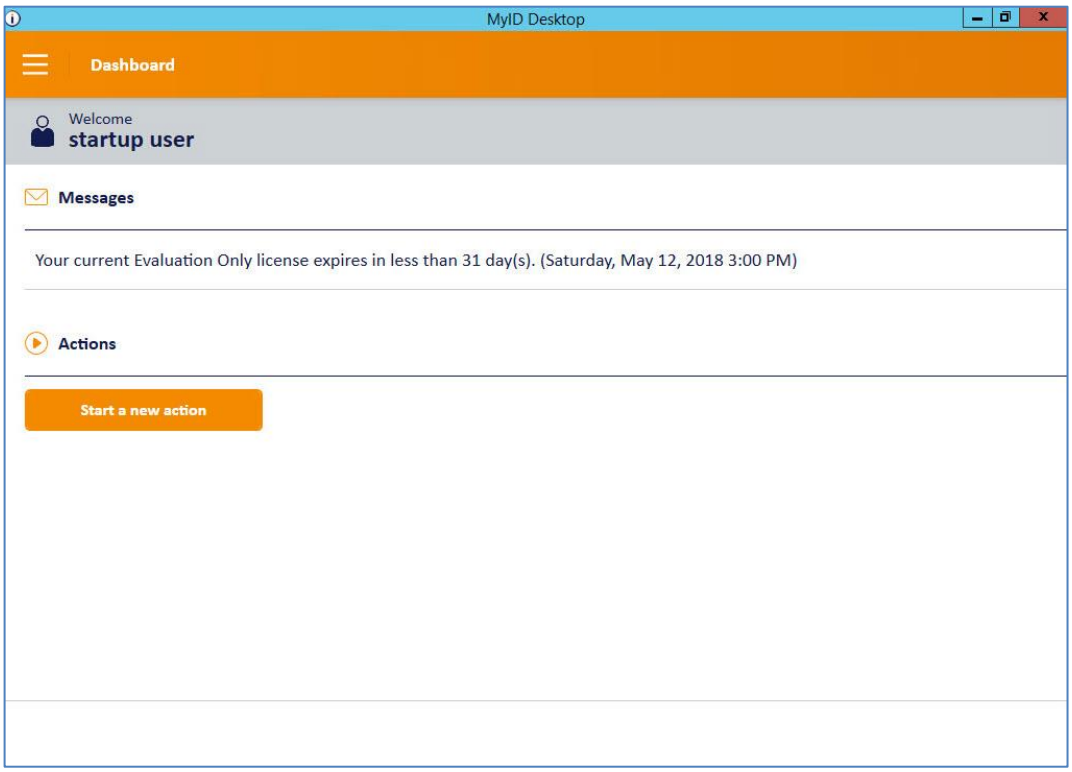
- eToken smart card is connected to the machine.

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



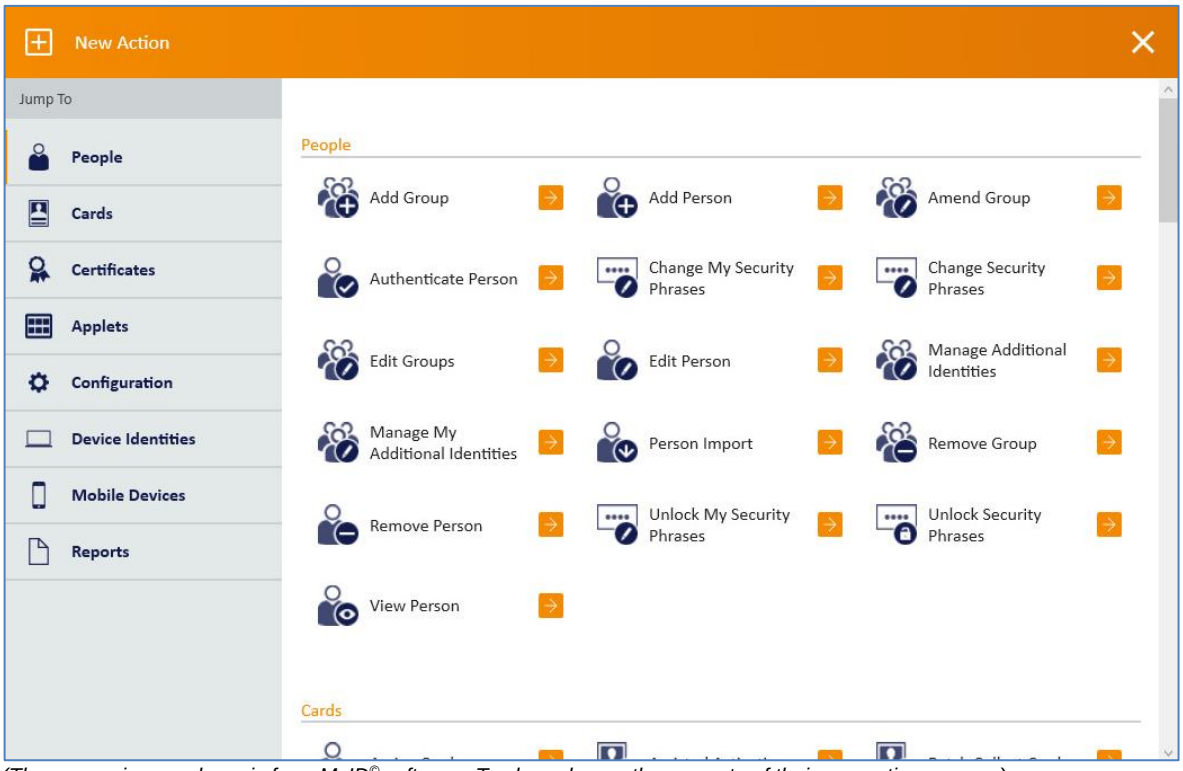
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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



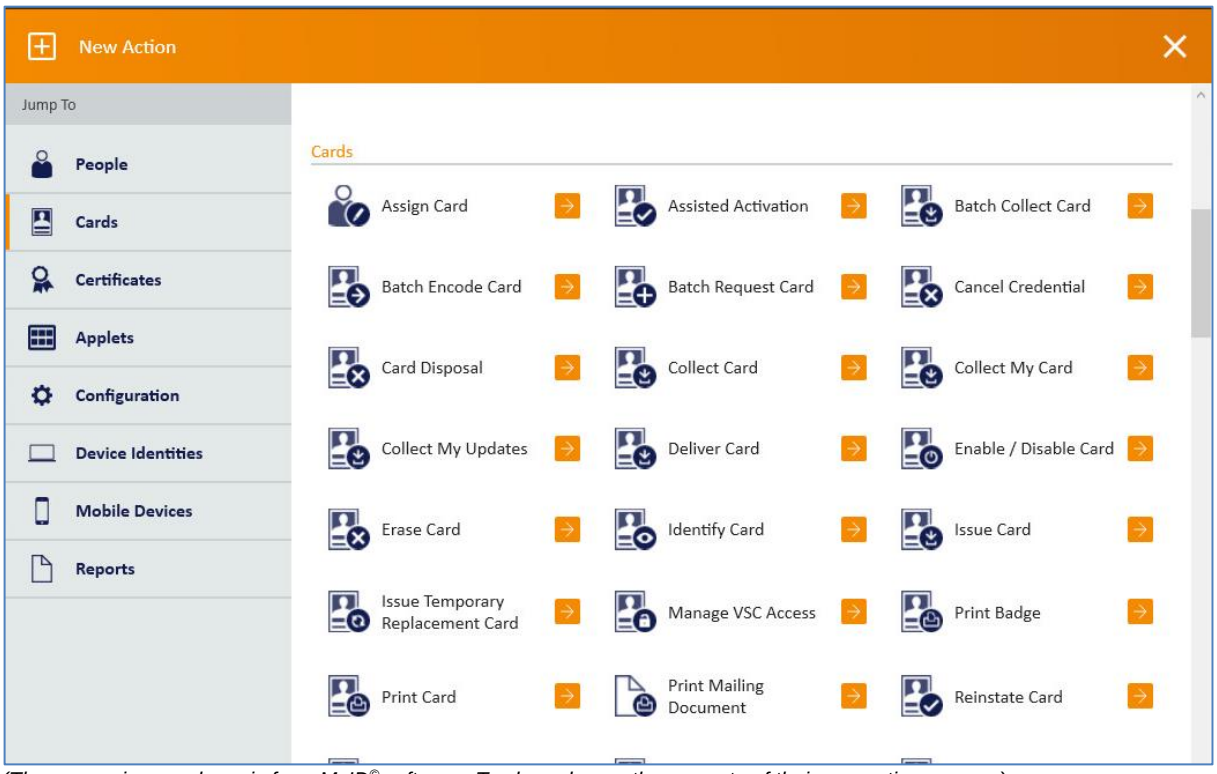
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

3. In the left pane, click **Cards**



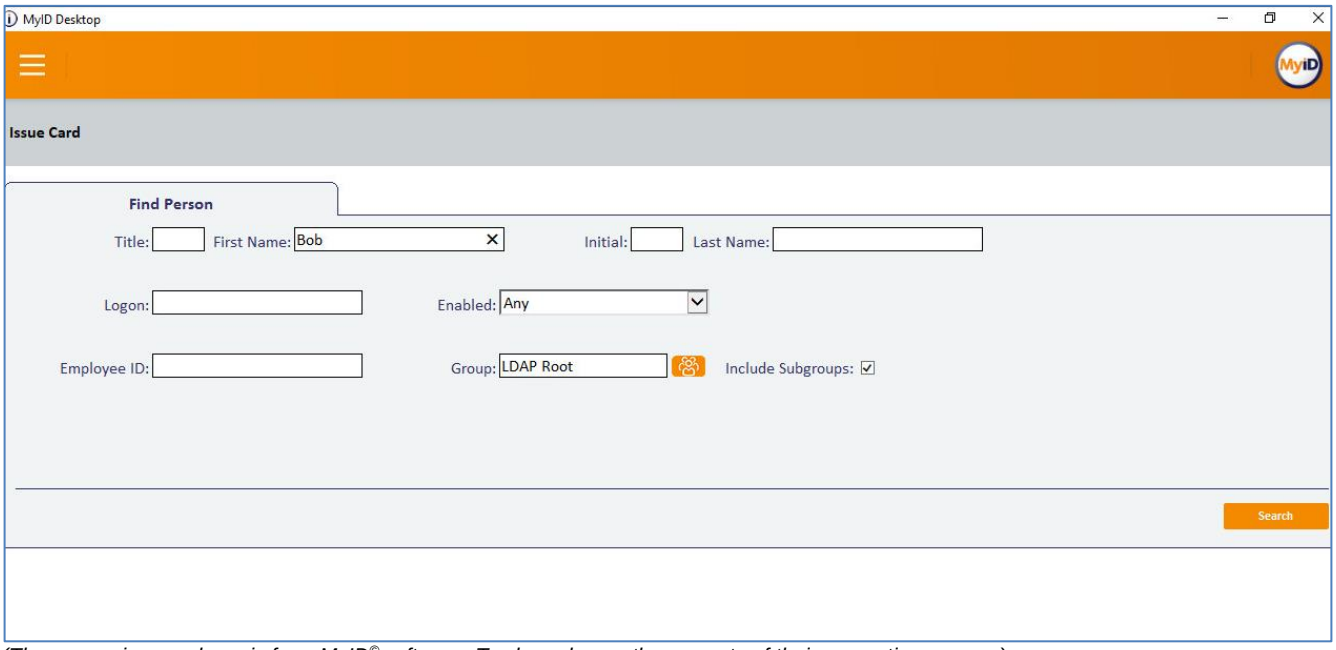
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

4. In the **Cards** window click **Issue Card.**



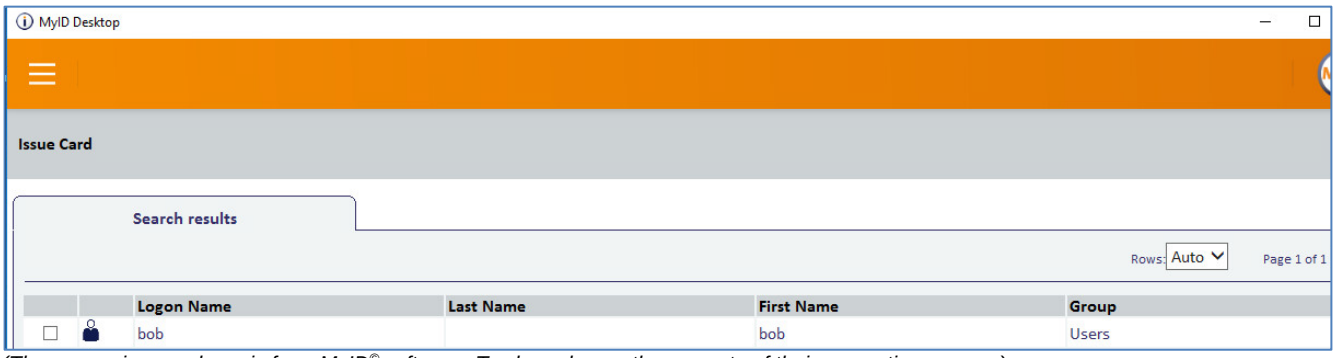
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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



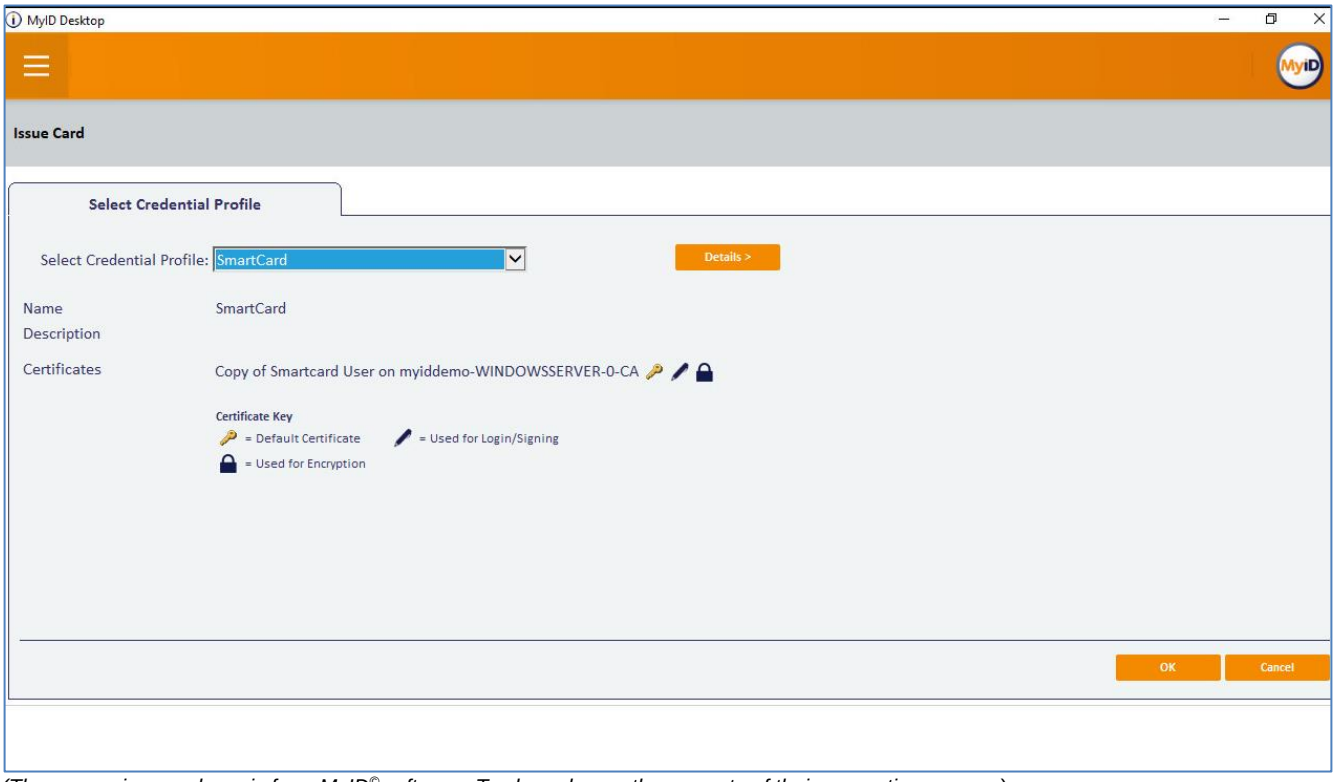
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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



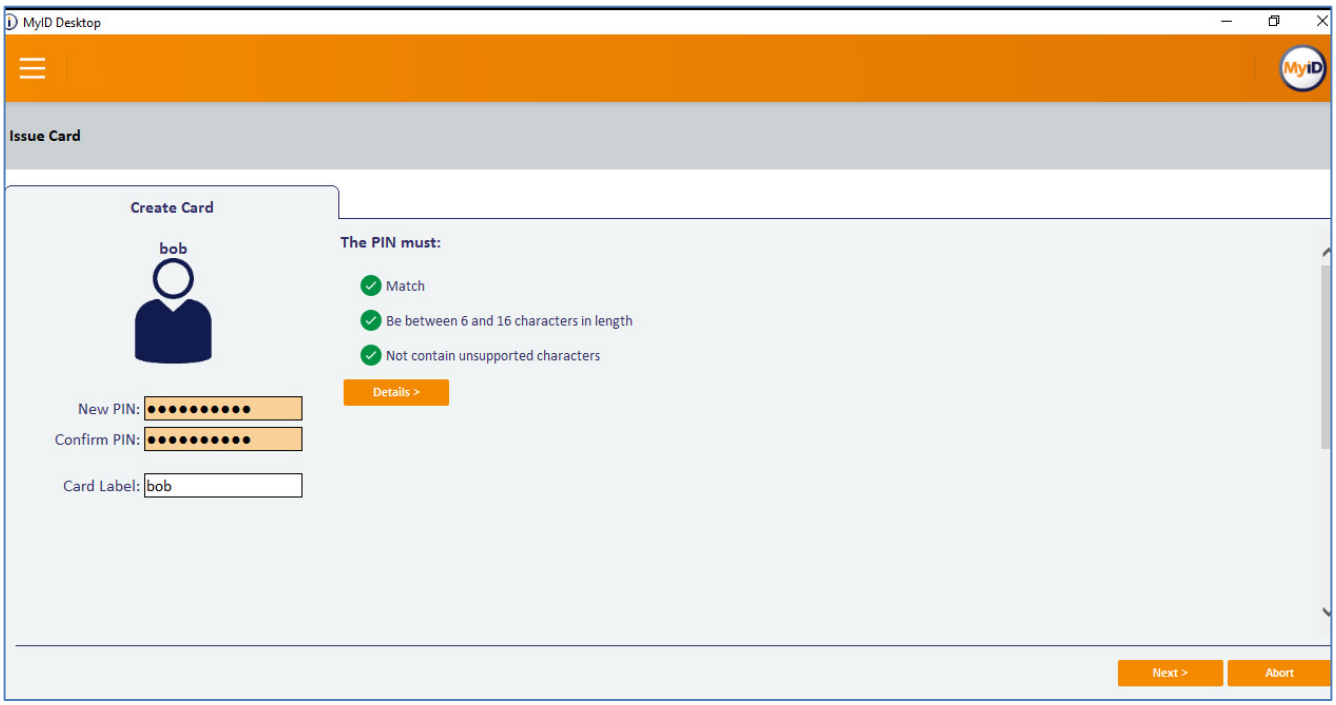
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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.**



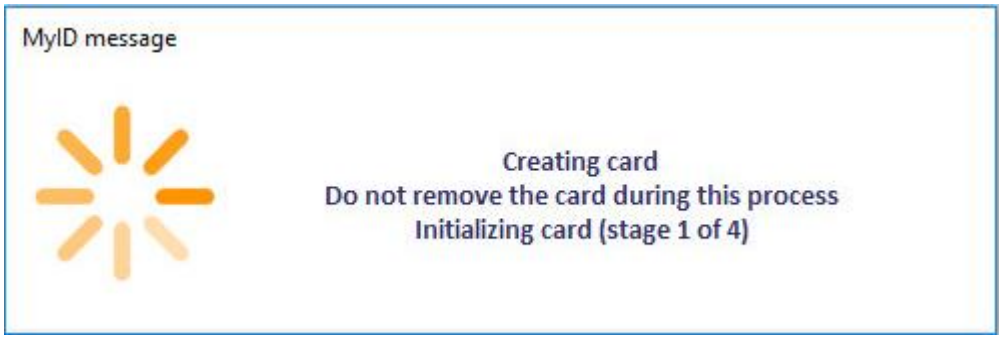
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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



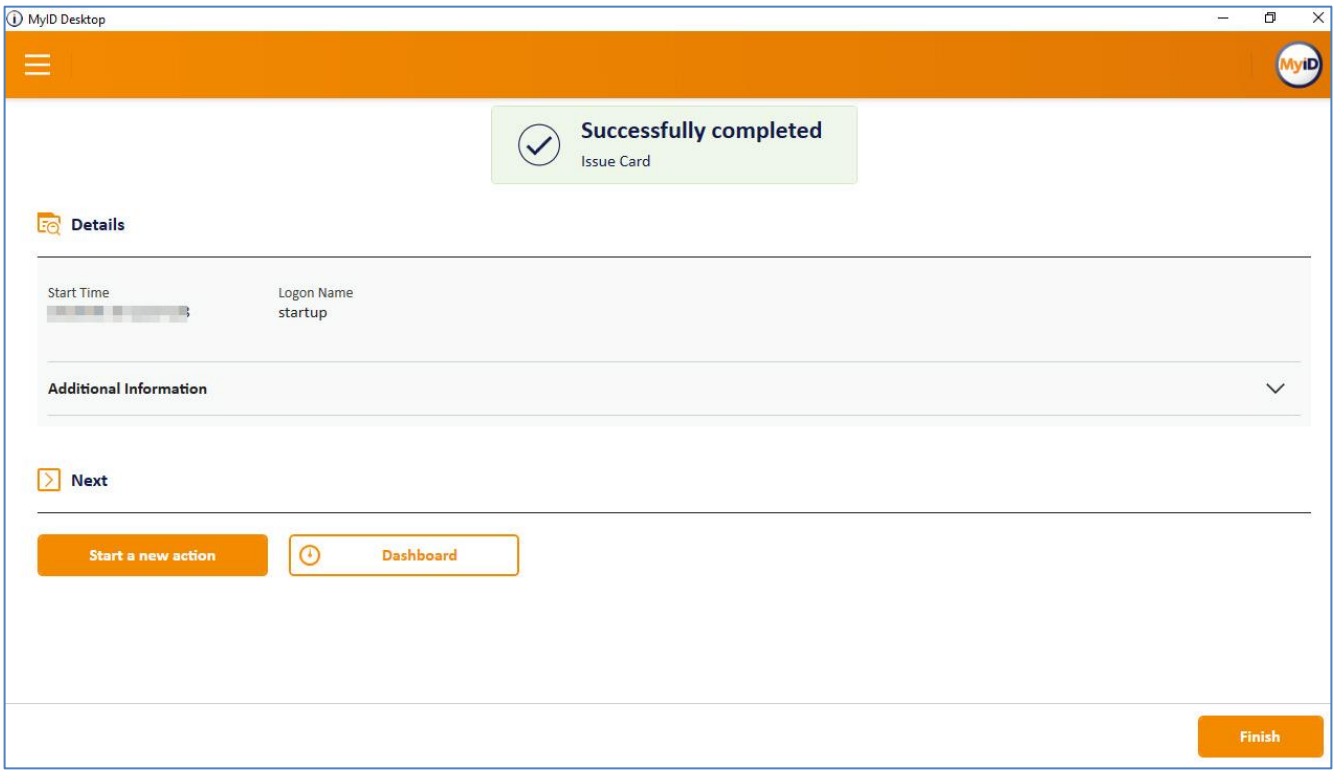
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

The card issuance procedure starts.



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

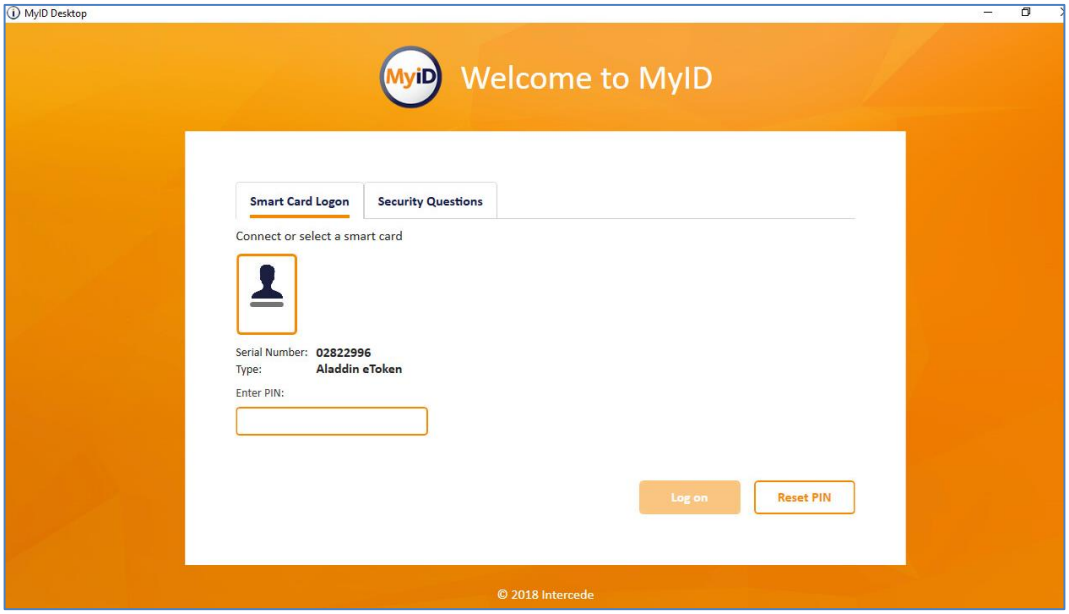
9. When successfully completed, the Issue Card procedure is complete. Click **Finish.**



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

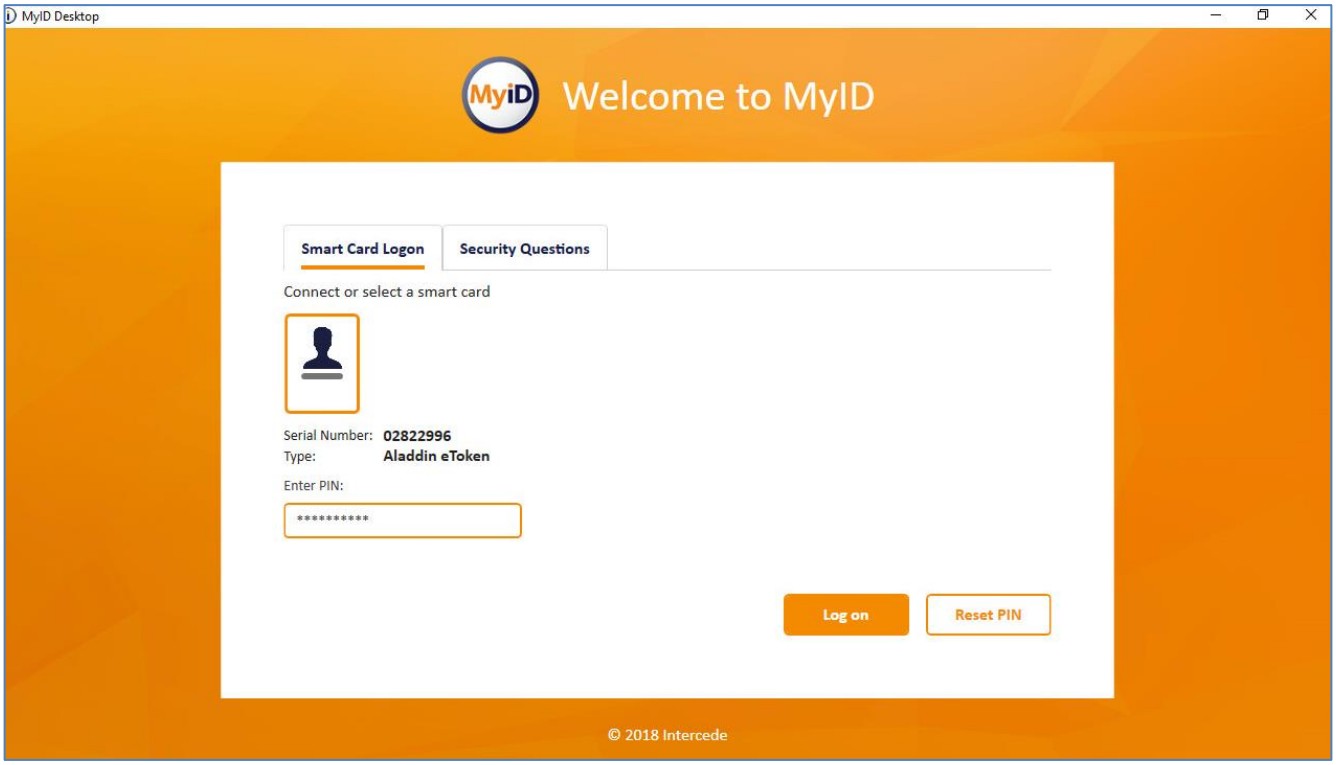
Smart Card Log in to MyID Desktop

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



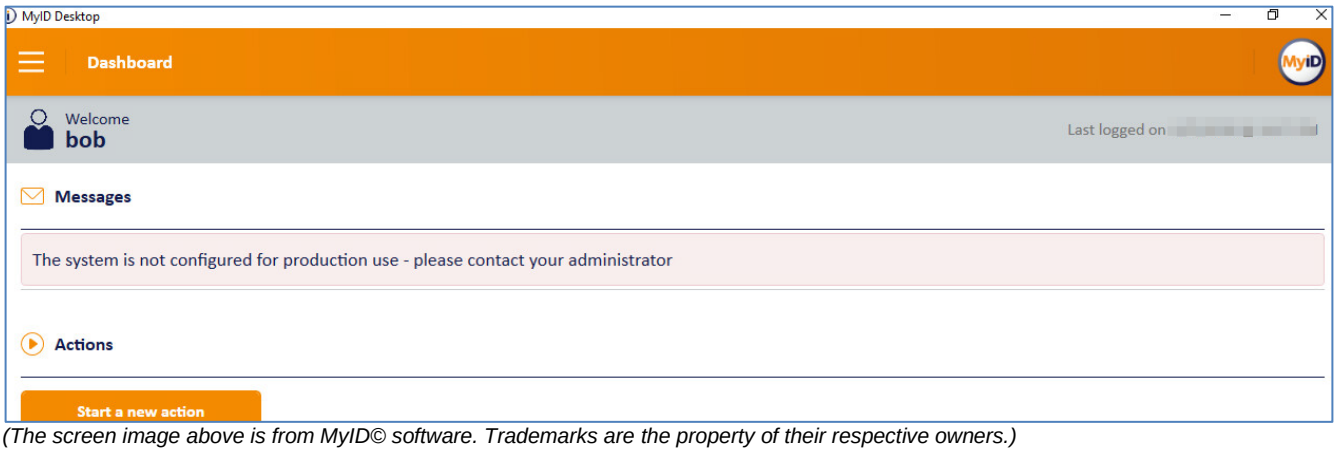
(The screen image above is from MyID© software. Trademarks are the property of their respective owners.)

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



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

The user successfully logged in to MyID desktop.



(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.	