MyID

Version 10.8 Update 2

Smart Card

Integration Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | @intercedemyid | +44 (0)1455 558111

Document reference: INT1740-21

April 2018

Copyright

Whilst Intercede Limited has made every effort in the preparation of this manual to ensure the accuracy of the information, the information contained in this manual is delivered without warranty, either express or implied. Intercede Limited will not be held liable for any damages caused, or alleged to be caused, either directly or indirectly by this manual.

Licenses and Trademarks

Conventions Used in this Document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important
  - Bulleted lists are used when the order is unimportant or to show alternatives

- **Bold** is used for menu items and for labels.

  For example:

  - "Record a valid email address in **'From' email address**"
  - Select **Save** from the **File** menu

- *Italic* is used for emphasis and to indicate references to other sections within the current document:

  For example:

  - "Copy the file *before* starting the installation"
  - "See *Issuing a Card* for further information"

- ***Bold and italic*** are used to identify the titles of other documents.

  For example: "See the ***Release Notes*** for further information."

  Unless otherwise explicitly stated, all referenced documentation is available on the installation CD.

- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.

- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.

- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

Warning: You must take a backup of your database before making any changes to it.

Contents

1 Introduction

This document describes the configuration necessary for administrators to enable MyID® to interoperate with smart cards. MyID supports smart cards in a variety of form factors – for example, smart cards with a contact chip that are used with card readers, and USB devices with smart card capabilities.

The following are currently supported by MyID:

- Athena. See section *2*, *Athena* for details.
- Gemalto. See section *3*, *Gemalto* for details.
- Giesecke & Devrient. See section *4*, *Giesecke & Devrient* for details.
- IDEMIA. See section *5*, *IDEMIA* for details.
- SafeNet. See section *6, SafeNet* for details.
- SafeNet Assured Technologies. See section *7*, *SafeNet Assured Technologies* for details.
- TCOS. See section *8*, *TCOS* for details.
- TicTok. See section *9*, *TicTok* for details.
- Yubico. See section *10*, *Yubico* for details.

MyID can be integrated with a broad range of smart cards – if you are interested in working with smart cards that are not listed in this document, contact customer support quoting SUP-76 for more information.

For information on issuing virtual smart cards (VSCs) see the ***Intel Virtual Smart Card Integration Guide*** and the ***Microsoft Virtual Smart Card Integration Guide***.

1.1 This document

The ***Smart Card Integration Guide*** was previously known as the ***Device Integration Guide***.

1.2 Supported features

This section lists the features that may be supported within MyID for various smart card types. Each section lists which features are supported for each smart card type; for example, if the smart card is listed as supporting PIN management, you can assume that the smart card supports all of the PIN management features unless specified otherwise.

- **MyID**

  Determines whether the smart card can be used within MyID with the following features:

  - Can be used to generate an RSA keypair that can be used for operations in MyID.
  - Can be used to sign data (including logon to MyID) with an RSA keypair on the smart card.
  - Can be used to encrypt data with an RSA keypair on the smart card.
  - MyID can set the label of the smart card.
  - MyID can erase the content of the smart card (excluding the printed card surface).

- **PIN management**

  Determines whether MyID can manage the PIN for the smart card. This incorporates the following features:

  - MyID can set the user PIN to be within a minimum and maximum limit as specified in the credential profile.
  - MyID can set the following character types in the user PIN as specified in the credential profile:
    - Lowercase
    - Uppercase
    - Numeric
    - Symbol.
  - MyID can lock the user PIN after issuing the smart card.
  - MyID can identify when the user PIN is locked.
  - MyID can replace the factory security officer PIN (SOPIN) with a randomized value.
  - MyID can replace the randomized SOPIN with the factory security officer PIN (SOPIN) at the cancellation of the smart card (when the smart card is present).
  - MyID can unlock the user PIN using the SOPIN to access the card.
  - MyID can provide an unlock code to a remote user to allow the smart card user PIN to be unlocked.

    Note: Earlier versions of MyID used the **Remote Unlock** workflow for this procedure. From MyID 10.7, the **Unlock Credential** workflow supersedes **Remote Unlock**.
  - MyID can reset the user PIN to a predefined value at the cancellation of the smart card (when the smart card is present).
- **GlobalPlatform**

  Determines whether MyID can work with the GlobalPlatform keys on the smart card. This incorporates the following features:

  - MyID can replace the factory GlobalPlatform keys with customer defined keys during issuance.
  - MyID can replace the customer defined keys with the factory GlobalPlatform key at cancellation of the smart card (when present).

  Many of the devices supported by MyID are based on card platforms that can support GlobalPlatform features. The GlobalPlatform keys, which are required to configure the features, are not always provided by card manufacturers, and so are tested only as part of specific project requirements or where the capabilities are a standard part of the card lifecycle management processes; for example, PIV cards. If you want to make more use of GlobalPlatform features and this document does not explicitly show support for them for your selected smart cards, contact Intercede to discuss your requirements in more detail.
- **Applets**

  Determines whether MyID can add and remove applets using GlobalPlatform technology. This incorporates the following features:

  - MyID can add an applet onto the smart card during issuance or update.
  - MyID can remove an applet from the smart card during update or cancellation.

- **PKI – RSA**

  Determines whether MyID can work with certificates using RSA keys on the smart card. This incorporates the following features:

  - MyID can force the smart card to generate a private key for use in a certificate request.
  - MyID can write a certificate to the smart card. This occurs during personalization of the smart card in smart card issuance, activation and update.
  - MyID can use a certificate on the smart card to sign data cryptographically.
  - MyID can specify the default certificate on the smart card that is used for Windows logon.
  - MyID can write certificates with RSA 1024 bit keys to the smart card.
  - MyID can write certificates with RSA 2048 bit keys to the smart card.
  - MyID can remove certificates and their associated private keys from the smart card. This occurs during update or cancellation of the smart card.
  - MyID can inject a private key to the smart card for certificate recovery operations.
  - MyID can enumerate all certificates on the card, and mark those expected to be present that are not present as missing in the **Identify Card** workflow.

- **PKI – ECC**

  Determines whether MyID can work with certificates using ECC keys on the smart card. This incorporates the following features:

  - MyID can force the smart card to generate a private key for use in a certificate request.
  - MyID can write a certificate to the smart card. This occurs during personalization of the smart card in smart card issuance, activation and update.
  - MyID can specify the default certificate on the smart card that is used for Windows logon.
  - MyID can write certificates with ECC NIST P256 Curve to the smart card.
  - MyID can write certificates with ECC NIST P384 Curve to the smart card.
  - MyID can write certificates with ECC NIST P521 Curve to the smart card.
  - MyID can remove certificates and their associated private keys from the smart card. This occurs during update or cancellation of the smart card.
  - MyID can enumerate all certificates on the card, and mark those expected to be present that are not present as missing in the **Identify Card** workflow.

- **PIV**

  Determines whether MyID can personalize and manage the smart card as a PIV card.

  Note: Issuance of PIV cards to NIST standards, in accordance with the NIST specification SP800-73-3 and the latest available version of the NIST SP800-85B Data Conformance Test Tool, is available only in PIV installations. You must configure your system to support the PIV standard for issuing PIV or PIV-I devices that conform to these specifications – see the ***PIV Integration Guide*** for details.

  MyID allows you to issue PIV cards without having a PIV system; however, PIV cards issued on non-PIV systems will not comply with NIST standards.

  - MyID can personalize a PIV card in accordance with the NIST specification SP800-73-3 – available on PIV systems only.
  - A PIV smart card issued by MyID must pass all applicable tests in the latest available version of the NIST SP800-85B Data Conformance Test Tool – available on PIV systems only.
  - MyID can replace the factory PIV 9B key with a value defined by the customer.
  - MyID can replace the customer PIV 9B key with the factory PIV 9B key at cancellation of the card (when present).
  - MyID can depersonalize a PIV card so no end user information remains on the card (excluding the printed card surface).
  - MyID can recover certificates into each of the historic key containers on the card (max 20).

    Note: MyID can recover only as many certificates as the card will hold. Some cards are manufactured with a restricted number of containers, and others may contain 20 containers but have only a smaller number available for key recover. Contact your card vendor to discuss your requirements for the number of available certificate recovery containers.
  - MyID can lock the GlobalPlatform keys on the smart card.
  - MyID can unlock the GlobalPlatform keys on the smart card.
  - MyID can unlock the PIN remotely with challenge response using the MyID Card Utility.

- **Printing**

  Determines whether MyID can print a card layout to the surface of the smart card.

- **Client OS**

  Determines whether MyID can issue the smart card to be used for Windows operations. This incorporates the following features:

  - The issued smart card can be used for Windows logon when it holds an appropriate certificate.

    Note: MyID communicates directly with PIV cards without using a driver or minidriver. You can use PIV cards for Windows logon; however, you may require additional software, such as a Windows minidriver. Contact your card vendor for details.
  - The issued smart card can be used for email signing when it holds an appropriate certificate.
  - The issued smart card can be used for email encryption when it holds an appropriate certificate.

1.3 General features

The following features are supported by MyID if they are available on individual smart cards. Support for these features does not depend on the type of smart card to which it is attached; for example, if a card has a magnetic stripe, and you have a card reader or printer that can write to magnetic stripes, MyID supports the ability to write user data to the magnetic stripe on a smart card.

- **HID Prox**

  MyID can import an HID correlation file containing the PROX serial numbers and facility codes. These are associated with smart card records in MyID, which can then be sent to a Physical Access System.

  You may require additional changes to your version of MyID to enable this feature. Contact customer support quoting reference SUP-77 for details.

  See the ***Administration Guide*** for details of importing serial numbers.

- **Magnetic Stripe**

  MyID can write user data to the magnetic stripe on a smart card.

1.4 Card readers

For this release, the following card readers have been tested:

- OMNIKEY 3021
- OMNIKEY 3121
- OMNIKEY 5125

  Note: You may experience problems with Omnikey readers if you do not use the drivers provided by Omnikey. You are recommended to use the Omnikey drivers rather than the equivalent Windows drivers.

- SCM Microsystems SCR331
- GemPC Twin
- Precise 250

1.5 Minidriver-based cards

All cards that use minidrivers require some additional setup.

1.5.1 Archive keys

To allow certificates with archive keys to be used, you must set the following registry settings each client:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Base Smart Card Crypto Provider]

"AllowPrivateSignatureKeyImport"=dword:00000001

"AllowPrivateExchangeKeyImport"=dword:00000001
```

1.5.2 Windows integrated unblock

If you want to use the card unblocking feature that is built into Windows for your minidriver-based smart cards, on Windows 7, 8, 8.1, and 10, you must enable the feature according to Microsoft's documentation. The Group Policy **AllowIntegratedUnblock** must be enabled in **Computer Configuration\Administrative Templates\Windows Components\Smart Card**.

The registry key is:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\SmartCardCredentialProvider]
```

```
"AllowIntegratedUnblock"=dword:00000001
```

This key can be pushed to clients by a global policy.

To unblock a card using this method, the cardholder uses the Windows unblock feature to generate a code. Once the cardholder has generated this code, they can call the helpdesk, who will use the **Unlock Credential** workflow within MyID to generate an unlocking code that you can use to unblock your smart card.

See the ***Administration Guide*** for details of using the **Unlock Credential** workflow.

1.5.3 Certificate propagation

For card issuance workstations, you must ensure that the Certificate Propagation service is not running on the client PC when using minidriver-based cards; if this service is running, the certificates are registered in the current user's certificate store.

For self-service clients, you can retain the Certificate Propagation service.

1.6 Upgrading existing systems

If you are upgrading from an earlier version of MyID, and are using cards that are not listed in this document, contact customer support quoting reference SUP-80.

If you are using older versions of minidrivers or middleware not listed in this document, you are recommended to upgrade to the listed versions. For more information, contact customer support quoting reference SUP-80.

1.7 Common criteria smart cards

You can obtain some of the smart cards listed in this document with common criteria functionality; however, MyID does not currently support this feature. In most cases this does not affect use of the device with MyID.

If you would like to discuss this further with Intercede, contact customer support quoting SUP-231.

1.8 Custom SOPINs

If your cards have been created with a non-standard factory Security Officer PIN (SOPIN), you must configure MyID to use this SOPIN – if you do not, you will be unable to issue a card.

If you are using the cards' GlobalPlatform keys, you can specify the factory SOPIN in the **Manage GlobalPlatform Keys** workflow.

If you are *not* using the cards' GlobalPlatform keys to manage the SOPIN on the issued cards, you must contact Intercede for assistance in configuring MyID to support these cards. Contact customer support quoting reference SUP-257.

1.9 PIN history

If your cards have been manufactured with a PIN history setting that prevents the same PIN from being re-used within a certain number of times, you will experience problems if you issue, cancel, and re-issue a card. When the card is cancelled, MyID attempts to reassign the SOPIN to the card; this causes a failure because the PIN is the same as a recent PIN used on the card.

1.10 Limit on number of smart cards

You can connect a maximum of ten smart cards (including both physical smart cards and VSCs) simultaneously to a PC.

2 Athena

2.1 Athena smart cards

MyID has been tested with the following Athena smart cards:

Smart card	Type	Middleware
Athena IDProtect	Smart card	IDProtect Client 7.1.2.7

Note: MyID has been tested with the minidrivers listed in the table above. Your version of the minidriver may be different, depending on which Windows updates you have installed. Make sure that you have the supported version of the minidriver installed.

Note: If you want to use Athena cards with Athena IDProtect PKCS#11 middleware, contact Intercede customer support for further information, quoting reference SUP-4.

2.2 Platforms

These smart cards have been tested on:

	Operating System			
Smart card	Windows 7 (32-bit)	Windows 7 (64-bit)	Windows 8.1	Windows 10
Athena IDProtect	Y	Y	Y	

Key:

- Y – Fully supported.
- blank – Not supported.

2.3 Supported features for Athena smart cards

See section *1.2*, *Supported features* for a description of the features supported by smart cards.

2.3.1 Features

The following MyID features are smart card or middleware specific. The table below indicates which smart card-dependent features are available in MyID with Athena smart cards.

	Features								
Smart card	**MyID**	**PIN management**	**GlobalPlatform**	**Applets**	**PKI – RSA**	**PKI – ECC**	**PIV**	**Printing**	**Client OS**
Athena IDProtect	Y	Y			Y	Y		Y	Y

Key:

- Y – Fully supported.
- blank – Not supported.

2.4 Installation and configuration

This section provides any information required when installing the middleware for the smart cards or configuring the smart cards either through their middleware or through MyID.

2.4.1 Using minidrivers for Athena smart cards

If you are using Athena smart cards with minidrivers, you must have the following:

- Athena IDProtect Client

See also section *1.5*, *Minidriver-based cards*.

Note: The IDProtect software has an installer like middleware, but is treated by MyID as a minidriver.

2.5 Interoperability

2.5.1 Known issues

- **Issues with smart card detection**

  Intercede has seen issues with version 7.1.2.7 of the IDProtect Client where MyID is not able to detect a new card. This is caused by the minidriver failing to return a serial number for the new card. This has been seen only with uninitialized cards, as they are delivered from the factory. NXP/Athena have provided Intercede with the following registry change to enable the serial number to be retrieved. You must apply this registry change to every client used to issue new cards:

  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\Athena Smartcard Solutions\IDProtect
  Client]

  "MDAllowWorkWithUnformattedCards"=dword:00000001

  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Athena Smartcard
  Solutions\IDProtect Client]

  "MDAllowWorkWithUnformattedCards"=dword:00000001
  ```

3 Gemalto

3.1 Gemalto smart cards

MyID has been tested with the following Gemalto smart cards:

Smart card	Type	Middleware
MD3810	Smart card/Chip	Minidriver v8.5.0.7
MD830	Smart card/Chip	Minidriver v8.5.0.7
MD830 Rev B FIPS Level 2	Smart card/Chip	Minidriver v8.5.0.7
MD830 Rev B FIPS Level 3	Smart card/Chip	Minidriver v8.5.0.7
MD831	Smart card/Chip	Minidriver v8.5.0.7
MD3840	Smart card/Chip	Minidriver v8.5.0.7
MD840 Rev A	Smart card/Chip	Minidriver v8.5.0.7
IDClassic 3340	Smart card/Chip+CL (Dual Interface)	Classic Client 6.3.8 (IDGo 300)
IDClassic 310	Smart card/Chip	Classic Client 6.3.8 (IDGo 300)
IDClassic 340	Smart card/Chip	Classic Client 6.3.8 (IDGo 300)
IDClassic 300	Smart card/Chip	Classic Client 6.3.8 (IDGo 300)
IDPrime PIV Card v2.0	PIV card	n/a
IDPrime PIV Card v2.1	PIV card	n/a

Note: MyID has been tested with the minidrivers listed in the table above. Your version of the minidriver may be different, depending on which Windows updates you have installed. Make sure that you have the supported version of the minidriver installed.

3.1.1 Gemalto IDPrime PIV Card v2.0 configurations

Currently, MyID 10 is compatible with the following Gemalto IDPrime PIV Card v2.0 configurations:

- Gemalto customer item C1070904 – secure channel SCP-01 and 3-DES PIV 9B keys
- Gemalto customer item C1072203 – secure channel SCP-03 and AES-128 PIV 9B keys.

3.1.2 Secure Channel Protocol

The Secure Channel Protocol (SCP) is used in the **Manage GlobalPlatform Keys** workflow.

When configuring your GlobalPlatform keys, use the following Secure Channel Protocol:

Smart card	SCP
IDClassic 3340	SCP01
IDClassic 310	SCP01
IDClassic 340	SCP01
IDClassic 300	SCP01
IDPrime PIV Card v2.0	SCP03
IDPrime PIV Card v2.1	SCP03

3.1.3 Cryptographic keys for Gemalto IDPrime PIV cards

When you configure the cryptographic keys, use the following details:

	IDPrime PIV Card v2.0	**IDPrime PIV Card v2.1**
DeviceType in MyID	Gemplus PIV V2	Gemplus PIV V21
GlobalPlatform SCP	SCP03	SCP03
Factory GlobalPlatform Key Type	AES128	AES128
Factory GlobalPlatform Key Diversification Algorithm	Diverse108	Diverse108
Factory PIV 9B Key Type	3DES or AES128	AES128
PIV 9B Factory Key diversification algorithm	Static	Static
Recommended PIV 9B Customer Key diversification algorithm	Diverse2	Diverse2

3.1.4 Gemalto smart card names

Some Gemalto smart cards have been renamed. This document uses the new names for the smart cards.

Previous name	**New name**
Protiva TPC IS (CCv2 applet)	IDClassic 300
Protiva TPC IM (CCv2 applet)	IDClassic 310
Protiva TPC IM (CCv3 applet)	IDClassic 340
Protiva TPC DM	IDClassic 3340

Note: The Classic Client middleware has also been renamed to IDGo 300.

3.2 Platforms

These smart cards have been tested on:

	Operating System			
Smart card	**Windows 7 (32-bit)**	**Windows 7 (64-bit)**	**Windows 8.1**	**Windows 10**
MD3810	Y	Y	Y	Y
MD830	Y	Y	Y	Y
MD830 Rev B FIPS Level 2	Y	Y	Y	Y
MD830 Rev B FIPS Level 3	Y	Y	Y	Y
MD831	Y	Y	Y	Y
MD3840	Y	Y	Y	Y
MD840 Rev A	Y	Y	Y	Y
IDClassic 3340	Y	Y		
IDClassic 310	Y	Y		
IDClassic 340	Y	Y		
IDClassic 300	Y	Y		
IDPrime PIV Card v2.0	Y	Y	Y	Y
IDPrime PIV Card v2.1	Y	Y	Y	Y

Key:

- Y – Supported on this platform.
- blank – Not supported on this platform.

3.3 Supported features for Gemalto smart cards

See section *1.2*, *Supported features* for a description of the features supported by smart cards.

3.3.1 Features

The following MyID features are smart card or middleware specific. The table below indicates which smart card-dependent features are available in MyID with Gemalto smart cards.

	Features								
Smart card	**MyID**	**PIN management**	**GlobalPlatform**	**Applets**	**PKI – RSA**	**PKI – ECC**	**PIV**	**Printing**	**Client OS**
MD3810	Y	Y			Y	Y		Y	Y
MD830	Y	Y			Y	Y		Y	Y
MD830 Rev B FIPS Level 2	Y	Y			P	Y		Y	Y
MD830 Rev B FIPS Level 3	Y	Y			P	Y		Y	Y
MD831	Y	Y			Y	Y		Y	Y
MD3840	Y	Y			Y	P		Y	Y
MD840 Rev A	Y	Y			Y	P		Y	Y
IDClassic 3340[1]	Y	Y	Y	Y	Y			Y	Y
IDClassic 310[1]	Y	Y	Y	Y	Y			Y	Y
IDClassic 340[1]	Y	Y	Y	Y	Y			Y	Y
IDClassic 300[1]	Y	Y	Y	Y	Y			Y	Y
IDPrime PIV Card v2.0		Y	Y		P		Y	Y	Y
IDPrime PIV Card v2.1		Y	Y		P	P	Y	Y	Y

Key:

- Y – Fully supported.
- P – Partially supported. See below for details.
- blank – Not supported.

[1] The IDClassic cards have restricted functionality using the latest MyID Desktop workflows. See section *3.5.2*, *Using older smart cards with native MyID Desktop workflows* for details.

PKI – RSA

Some Gemalto smart cards support a limited range of PKI – RSA features:

	Smart card	
Feature	**IDPrime PIV Card v2.0**	**MD830 Rev B FIPS Level 2**
Generate a private key for a certificate request.	Y	Y
Write a certificate to the smart card.	Y	Y
Cryptographically sign or encrypt data.	Y	Y
Specify the default certificate for Windows logon.	Y	Y
Write 1024 bit certificates.		
Write 2048 bit certificates.	Y	Y
Remove certificates.	Y	Y
Inject a private key for certificate recovery.	Y	Y
Enumerate certificates on the card.	Y	Y

	Smart card	
Feature	**MD830 Rev B FIPS Level 3**	**IDPrime PIV Card v2.1**
Generate a private key for a certificate request.	Y	Y
Write a certificate to the smart card.	Y	Y
Cryptographically sign or encrypt data.	Y	Y
Specify the default certificate for Windows logon.	Y	Y
Write 1024 bit certificates.		
Write 2048 bit certificates.	Y	Y
Remove certificates.	Y	Y
Inject a private key for certificate recovery.	Y	Y
Enumerate certificates on the card.	Y	Y

Key:

- Y – Fully supported.
- blank – Not supported.

PKI – ECC

Some Gemalto smart cards support a limited range of PKI – ECC features:

	Smart card	
Feature	**MD3840**	**MD840 Rev A**
Generate a private key for a certificate request.	Y	Y
Write a certificate to the smart card.	Y	Y
Specify the default certificate for Windows logon.	Y	Y
ECC NIST P256 Curve	Y	Y
ECC NIST P384 Curve		
ECC NIST P521 Curve		
Remove certificates.	Y	Y
Enumerate certificates on the card.	Y	Y

	Smart card
Feature	**IDPrime PIV Card v2.1**
Generate a private key for a certificate request.	Y
Write a certificate to the smart card.	Y
Specify the default certificate for Windows logon.	Y
ECC NIST P256 Curve	Y
ECC NIST P384 Curve	Y
ECC NIST P521 Curve	
Remove certificates.	Y
Enumerate certificates on the card.	Y

Key:

- Y – Fully supported.
- blank – Not supported.

3.3.2 Unlocking features

Cardholders can unlock their smart cards without access to the MyID system by contacting a helpdesk and providing an alphanumeric code.

For Classic Client-based smart cards, use the **PIN Management** feature of the Classic Client Toolbox to generate the code; see your Gemalto documentation for details.

For minidriver-based smart cards, see section *1.5.2*, *Windows integrated unblock* for details.

3.3.3 Hybrid contactless cards

Gemalto provide hybrid versions of some IDPrime smart cards that incorporate a separate contactless interface; for example, the IDPrime MD831 is the hybrid contactless version of the IDPrime MD830.

These cards have the same contact chip capability as the Smart card/chip version of the card. Multiple configurations of these card types exist, with different contactless interface types. MyID can support functionality that makes use of contactless data; for example, the ability to read the ID from an HID PROX interface.

For more details on using PROX interfaces on a card with MyID, see the ***Administration Guide***. If you require support for other contactless interface types such as MIFARE or DesFire, contact Intercede to discuss your requirements in more detail.

3.4 Installation and configuration

This section provides any information required when installing the minidrivers or middleware for the smart cards or configuring the smart cards through their minidriver, middleware or through MyID.

3.4.1 Using minidrivers for Gemalto smart cards

If you are using Gemalto smart cards with minidrivers, you must have the following:

- Gemalto Minidriver

  You must install the `axaltocm.dll` file in the `Windows\System32` folder on each client. You can obtain this file from the Microsoft Update Catalog by searching for "Gemalto Minidriver". On Windows 7 this is installed automatically when a card is inserted into a reader. You can also obtain this file using the Gemalto IDGo 800 installer.

  You can also use the Safenet Authentication Client to install the Gemalto minidriver. To achieve this, ensure that the Safenet Authentication Client is configured for "IDGo 800 Minidriver Only" as described in the *SafeNet Authentication Client Administrator* guide.

See also section *1.5*, *Minidriver-based cards*.

- **IKB-210 – Issues with Safenet Authentication Client**

  Safenet Authentication Client (when configured to support Safenet eToken devices) may detect Gemalto ID Prime smart cards if both device types are connected to a MyID client at the same time. This will lead to errors when issuing or managing the Gemalto smart card – avoid using both card types at the same time with MyID.

3.4.2 Classic Client middleware

Install the standard version of the Classic Client Administrator and follow the instructions in the Gemalto IDGo 300 documentation to create a custom client setup program. You must then distribute and install the generated setup program on all client machines.

Make sure the PIN policies defined in Classic Client correspond with the policy configured in the MyID credential profile, then save your settings.

Note: Gemalto can manufacture cards with restrictive policies regarding their PINs; for example, your cards may allow only numeric PINs. Make sure you set up the PIN policy and the MyID credential profile to match the manufactured capabilities of your cards.

3.5 Interoperability

3.5.1 PIN characters for PIV cards

The SP800-73 PIV specification requires that PIV cards use numeric-only PINs. It is possible to configure MyID to use non-numeric PIN characters for PIV cards, although the smart cards will fail to issue.

Make sure you set up the credential profile correctly; in the **PIN Characters** section of the **Credential Profiles** workflow, set number to be **Mandatory**, and uppercase letters, lowercase letters, and symbols to **Not Allowed**.

3.5.2 Using older smart cards with native MyID Desktop workflows

Newer versions of MyID use updated workflows that use the native capabilities of MyID Desktop instead of embedded web pages. These workflows do not work with all smart cards.

For example, in MyID 10.8, the **Erase Card**, **Reset Card PIN**, **Print Card**, **Unlock Credentials**, **Cancel Credential**, **Collect Card**, and **Batch Collect Card** workflows do not work with older cards.

Cards that are unsupported with these workflows:

- IDClassic 3340
- IDClassic 310
- IDClassic 340
- IDClassic 300

3.5.3 MD840 Rev A and MD3840 smart cards and signature only policies

Gemalto MD840 Rev A and MD3840 smart cards have Common Criteria features that MyID does not support. Due to this limitation, issuing certificates that require a Signature Only policy is not supported with MyID.

3.5.4 IDPrime PIV 2.1 card status

IDPrime PIV v2.1 cards are delivered in in an ISD Status of `OP_READY`. Set the **Set GlobalPlatform Card Status** option (on the PINs page of the **Security Settings** workflow) to **Yes** to ensure the cards are issued in a ISD `SECURED` state.

3.5.5 Known issues

- **IKB-230 – Error reported from IDPrime MD smart cards when changing cards in a reader**

  In some circumstances, swapping a Gemalto IDPrime smart card in a single reader can cause a security violation error to be reported from the smart card. This situation may occur when the operator has authenticated to MyID with their own smart card, has started issuance of a card for another person, and is required to re-insert their smart card; for example, at the end of the issuance process to sign audit data. This situation does not occur if two smart card readers are connected to the MyID client, removing the need to swap cards over, or issuance is taking place with a smart card printer. Self-service operation (where no card swaps are required) is not affected.

  The error reported is:

  ```
  Failed in stage 2157
  -2146434966 - Error: 0x8010006a : Access was denied because of a
  security violation.

  Info: CardWriteFile file \cardcf
  -------------------------------
  Exception raised in function: md::MiniDriverBase::WriteFile
  In file MiniDriverBase.cpp at line 1182

  ---------------------------------
  ```

4 Giesecke & Devrient

4.1 Giesecke & Devrient smart cards

MyID has been tested with the following Giesecke & Devrient smart cards:

Smart card	Type	Middleware
SmartCafé Expert 3.2 (64K)	Smart card/Chip	AET SafeSign v3.0.87
Sm@rt Café® Expert 6.0	Smart card/Chip	AET SafeSign v3.0.97
SCE v7.0	PIV card	n/a

4.1.1 Secure Channel Protocol

The Secure Channel Protocol (SCP) is used in the **Manage GlobalPlatform Keys** workflow.

When configuring your GlobalPlatform keys, use the following Secure Channel Protocol:

Smart card	SCP
SCE v7.0	SCP03

4.1.2 Cryptographic keys for Giesecke & Devrient PIV cards

When you configure the cryptographic keys, use the following details:

	SCE v7.0
DeviceType in MyID	GieseckeDevrient PIV
GlobalPlatform SCP	SCP03
Factory GlobalPlatform Key Type	AES128
Factory GlobalPlatform Key Diversification Algorithm	Static
Factory PIV 9B Key Type	3DES
PIV 9B Factory Key diversification algorithm	Static
Recommended PIV 9B Customer Key diversification algorithm	Diverse2

4.2 Platforms

These smart cards have been tested on:

	Operating System			
Smart card	**Windows 7 (32-bit)**	**Windows 7 (64-bit)**	**Windows 8.1**	**Windows 10**
SmartCafé Expert 3.2 (64K)	Y	Y		
Sm@rt Café$^{®}$ Expert 6.0				Y
SCE v7.0	Y	Y	Y	Y

Key:

- Y – Fully supported.
- blank – Not supported.

4.3 Supported features for Giesecke & Devrient smart cards

See section *1.2*, *Supported features* for a description of the features supported by smart cards.

4.3.1 Features

The following MyID features are smart card or middleware specific. The table below indicates which smart card-dependent features are available in MyID with Giesecke & Devrient smart cards.

	Features								
Smart card	**MyID**	**PIN management**	**GlobalPlatform**	**Applets**	**PKI – RSA**	**PKI – ECC**	**PIV**	**Printing**	**Client OS**
SmartCafé Expert 3.2 (64K)	Y	Y			P			Y	Y
Sm@rt Café$^{®}$ Expert 6.0	Y	Y			Y			Y	Y
SCE v7.0		Y	Y		Y	P	Y	Y	Y

Key:

- Y – Fully supported.
- P – Partially supported. See below for details.
- blank – Not supported.

PKI – RSA

Some Giesecke & Devrient smart cards support a limited range of PKI – RSA features:

	Smart card
Feature	**SmartCafé Expert 3.2**
Generate a private key for a certificate request.	Y
Write a certificate to the smart card.	Y
Cryptographically sign or encrypt data.	Y
Specify the default certificate for Windows logon.	Y
Write 1024 bit certificates.	Y
Write 2048 bit certificates.[1]	
Remove certificates.	Y
Inject a private key for certificate recovery.	Y
Enumerate certificates on the card.	Y

Key:

- Y – Fully supported.
- blank – Not supported.

PKI – ECC

Some Giesecke & Devrient smart cards support a limited range of PKI – ECC features:

	Smart card
Feature	**SCE v7.0**
Generate a private key for a certificate request.	Y
Write a certificate to the smart card.	Y
Specify the default certificate for Windows logon.	Y
ECC NIST P256 Curve	Y
ECC NIST P384 Curve	Y
ECC NIST P521 Curve	
Remove certificates.	Y
Enumerate certificates on the card.	Y

Key:

- Y – Fully supported.
- blank – Not supported.

[1] Not all Giesecke & Devrient cards support 2048-bit certificates. Contact your card supplier for details.

4.3.2 Remote unlock

Note: Not all Giesecke & Devrient cards support remote unlocking. Contact your card supplier for more details.

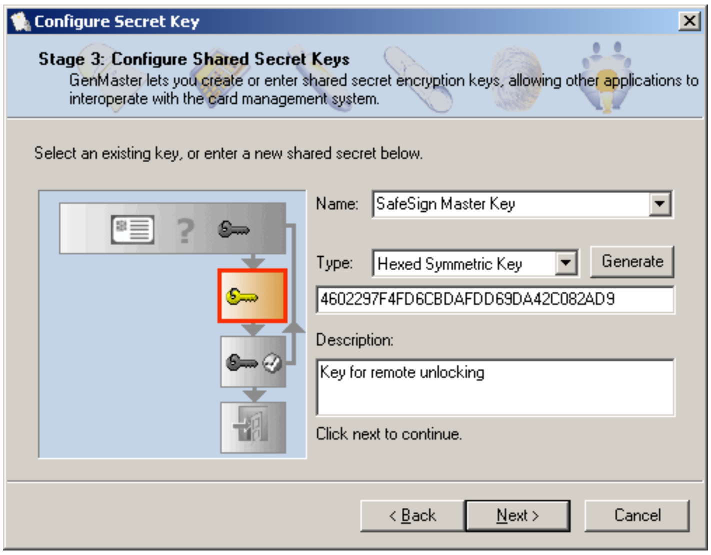
MyID supports remote unlocking of Giesecke & Devrient using the standard **Unlock Credential** workflow.

Note: If you set up your MyID system to use remote unlocking, you cannot issue any Giesecke & Devrient cards that do not support remote unlocking. If you attempt to issue a card that does not support remote unlocking, you will see any error similar to the following:

```
Initialize Error
-2147220734 Exception thrown: class CCardException
Message: A general smartcard error occurred
HRESULT: 80040302
PKCS Error: 30
From file: .\Card Drivers\GDSmartCard.cpp
From line: 395
Meaning: Smart Card Exception
```

Creating a secret key

1. Start GenMaster from the **Start** menu.
2. Select the option to **Configure Secret Keys**. Click **Next**.
3. The **Configure Shared Secret Keys** dialog is displayed.



Configure Secret Key

Stage 3: Configure Shared Secret Keys

GenMaster lets you create or enter shared secret encryption keys, allowing other applications to interoperate with the card management system.

Select an existing key, or enter a new shared secret below.

Name: SafeSign Master Key

Type: Hexed Symmetric Key

4602297F4FD6CBDAFDD69DA42C082AD9

Description:

Key for remote unlocking

Click next to continue.

   a) In **Name**, enter **SafeSign Master Key**.

   b) In **Type**, select **Hexed Symmetric Key**.

   c) Click **Generate**.

   d) Enter an appropriate **Description**.

   e) Click **Next**.

   Note: **Next** is disabled until all information has been entered.

4. A confirmation message is displayed – click **Next** to continue.
5. Click **Cancel** to close GenMaster.

Note: The secret keys are written to the cards when they are issued, so you will not be able to use the remote unlock facility with any cards that were issued prior to creating this key.

Configuration settings

A configuration setting specifies which remote unlocking method you are going to use:

- None – no remote unlocking
- Challenge – a 16-character challenge code is required
- Witness – a 56-character challenge code is required, that consists of both the challenge code and a HASH.

To specify the unlock method:

1. Select **Security Settings** from the **Configuration** category.
2. Select the **PINs** tab.
3. From the drop-down list for **Offline Unlock Method**, select **Challenge**, **Witness** or **None**, depending on the method you want to use.
4. Click **Save Changes**.

Operating instructions

If a cardholder repeatedly enters an incorrect PIN, the card will lock.

1. The cardholder contacts the Helpdesk operator by telephone.
2. The Helpdesk operator uses the **Unlock Credential** workflow within MyID and guides the cardholder through generating a challenge using the Giesecke & Devrient Token Administration Utility.

   When prompted, inform the cardholder to select **Unlock PIN via off-line PIN unlock**, then select either:

   - 3DES ECB Challenge/Response
   - 3DES ECB Witness/Challenge/Response

   See the ***Administration Guide*** for details of using the **Unlock Credential** workflow.

   Note: Earlier versions of MyID used the **Remote Unlock** workflow for this procedure. From MyID 10.7, the **Unlock Credential** workflow supersedes **Remote Unlock**.
3. The Helpdesk operator reads the unlocking code to the cardholder, who enters it into the Token Administration Utility. The code must be entered exactly as read, with no spaces. Case is not important.

4.4 Installation and configuration

This section provides any information required when installing the middleware for smart cards or configuring smart cards through either their middleware or through MyID.

Insert the middleware installation CD, and the installer should auto-run. If the computer is not configured to auto-run CDs, double-click on the `setup.exe`.

Note: While installing this middleware, ensure that the ‘CSP’ and ‘PKCS11’ subcomponents are selected – these are required in order for MyID to communicate with the Smart cards. The middleware must be installed before installing MyID.

4.4.1 Special usage notes for MyID

Note: It is claimed that production cards cannot be initialized twice. Like Identrus these cards are issued once and are issued for life.

4.5 Interoperability

4.5.1 Interoperability with AET middleware

If you have AET middleware installed, you may not be able to use PIV or minidriver-based cards with MyID; this is because the AET middleware attempts to communicate with the card, thereby preventing MyID from communicating directly with the card.

If you are using cards that do not require the AET middleware, you are recommended to make sure that AET middleware is not installed on any of your client workstations where you will be using these cards.

4.5.2 Initializing cards

If you are experiencing problems initializing cards, you may have to disable the certificate expiration check utility (`aetcrss1.exe`) on the client machine.

To disable the certificate expiration check utility:

1. Remove the check from the **Tasks** list within the **Token Utility**.
2. Remove the following key from the registry:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
   CertificateExpiration
   ```

   Note: On 64-bit systems, this is:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\
   CurrentVersion\Run\CertificateExpiration
   ```

3. Restart the machine.

4.5.3 Deleting individual certificates from PIV cards

If you update a Giesecke & Devrient PIV card with a credential profile that has a certificate removed, the certificate is not removed from the card. This is because the PIV standard does not specify a delete command; other PIV card manufacturers may provide custom commands to delete individual certificates from their PIV cards, but this is not possible with Giesecke & Devrient PIV cards. Certificates are removed from the card only when it is erased.

4.5.4 Known issues

- **IKB-239 – Giesecke & Devrient PIV cards cannot be issued without the full PIV data model being used**

  You must use Giesecke & Devrient SCE v7.0 PIV cards with the PIV data model (`PivDataModel.xml`) – configure this in the credential profile. Attempting to issue this card with an alternative data model will fail with an error 890493.

5 IDEMIA

5.1 IDEMIA smart cards

Note: IDEMIA cards were previously issued under the Oberthur name.

MyID has been tested with the following IDEMIA smart cards:

Smart card	Type	Middleware
Oberthur ID-One Cosmo v7.0.1 with IAS Standard applet	Smart card/Chip	Oberthur IAS-ECC minidriver v2.2.8
Oberthur ID-One PIV (v2.3.2) “ID-One PIV (Type A) Large D”	PIV card	n/a
Oberthur ID-One PIV (v2.3.4)	PIV card	n/a
Oberthur ID-One PIV (v2.3.5)	PIV card	n/a
Oberthur ID-One PIV (v2.4.0)	PIV card	n/a
IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1	PIV card	n/a

For Oberthur ID-One PIV (v2.3.2) cards, MyID supports the following specification:

- *BAP#087284 – ID-One (Type A) default configuration for Intercede CMS.pdf*.

  If you intend to use ID-One PIV (v2.3.2) cards manufactured to another specification, contact customer support for more information, quoting reference SUP-9.

For Oberthur ID-One PIV (v2.3.5) cards, MyID supports the following specification:

- *BAP#087424 – ID-One PIV (NPIVP-Basic) on Cosmo v8, high speed*

For Oberthur ID-One PIV (v2.4.0) cards, MyID supports the following specifications:

- *BAP#087430 – ID-One PIV (NPIVP-Basic) on Cosmo v8*
- *BAP#087434 – ID-One PIV (NPIVP-Basic) on Cosmo v8, high speed*
- *BAP#087432 – ID-One PIV (CIV) on Cosmo v8*

  Note: Oberthur ID-One PIV (v2.4.0) cards are supported on MyID only in conjunction with specific integration for a particular customer. If you want to use these cards with MyID, contact your Intercede account manager.

For IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1 cards, MyID supports the following specifications:

- *BAP#087484 – ID-One PIV 2.4 on Cosmo v8.1 NPIVP*
- *BAP#087494 – ID-One PIV 2.4 on Cosmo v8.1 NPIVP (transitional configuration)*

Note: MyID has been tested with the minidrivers listed in the table above. Your version of the minidriver may be different, depending on which Windows updates you have installed. Make sure that you have the supported version of the minidriver installed.

5.1.1 Secure Channel Protocol

The Secure Channel Protocol (SCP) is used in the **Manage GlobalPlatform Keys** workflow.

When configuring your GlobalPlatform keys, use the following Secure Channel Protocol:

Smart card	SCP
Oberthur ID-One PIV (v2.3.2) “ID-One PIV (Type A) Large D”	OT-SCP03
Oberthur ID-One PIV (v2.3.4)	OT-SCP03
Oberthur ID-One PIV (v2.3.5)	SCP03
Oberthur ID-One PIV (v2.4.0)	SCP03
IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1	SCP03

5.1.2 Cryptographic keys for ID-One PIV cards

When you configure the cryptographic keys, use the following details:

	Oberthur ID-One PIV (v2.3.2) “ID-One PIV (Type A) Large D”	Oberthur ID-One PIV (v2.3.4)	Oberthur ID-One PIV (v2.3.5)
DeviceType in MyID	Oberthur ID-One PIV	Oberthur ID-One PIV	Oberthur ID-One PIV v8
GlobalPlatform SCP	OT-SCP03	OT-SCP03	SCP03
Factory GlobalPlatform Key Type	AES128	AES128	AES256
Factory GlobalPlatform Key Diversification Algorithm	Diverse3	Diverse3	DiverseOT108
Factory PIV 9B Key Type	3DES	3DES	AES256
PIV 9B Factory Key diversification algorithm	Static	Static	DiverseOT108
Recommended PIV 9B Customer Key diversification algorithm	Diverse2	Diverse2	DiverseOT108

	Oberthur ID-One PIV (v2.4.0)	IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1
DeviceType in MyID	Oberthur ID-One PIV v8	IDEMIA ID-One PIV v81
GlobalPlatform SCP	SCP03	SCP03
Factory GlobalPlatform Key Type	AES256	AES256
Factory GlobalPlatform Key Diversification Algorithm	DiverseOT108	DiverseOT108
Factory PIV 9B Key Type	AES256	AES256
PIV 9B Factory Key diversification algorithm	DiverseOT108	DiverseOT108
Recommended PIV 9B Customer Key diversification algorithm	DiverseOT108	DiverseOT108

5.2 Platforms

These smart cards have been tested on:

	Operating System			
Smart card	**Windows 7 (32-bit)**	**Windows 7 (64-bit)**	**Windows 8.1**	**Windows 10**
Oberthur ID-One Cosmo v7.0.1 with IAS Standard applet	Y	Y	Y	
Oberthur ID-One PIV (v2.3.2) “ID-One PIV (Type A) Large D”	Y	Y	Y	Y
Oberthur ID-One PIV (v2.3.4)	Y	Y	Y	
Oberthur ID-One PIV (v2.3.5)	Y	Y	Y	Y
Oberthur ID-One PIV (v2.4.0)	Y	Y	Y	Y
IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1	Y	Y	Y	Y

Key:

- Y – Fully supported.
- blank – Not supported.

5.3 Supported features for IDEMIA smart cards

See section *1.2*, *Supported features* for a description of the features supported by smart cards.

5.3.1 Features

The following MyID features are smart card or middleware specific. The table below indicates which smart card-dependent features are available in MyID with IDEMIA smart cards.

	Features								
Smart card	**MyID**	**PIN management**	**GlobalPlatform**	**Applets**	**PKI – RSA**	**PKI – ECC**	**PIV**	**Printing**	**Client OS**
Oberthur ID-One Cosmo v7.0.1 with IAS Standard applet	Y	Y			Y			Y	Y
Oberthur ID-One PIV (v2.3.2) “ID-One PIV (Type A) Large D”		Y	Y		Y	P	Y	Y	Y
Oberthur ID-One PIV (v2.3.4)		Y	Y		Y	P	Y	Y	Y
Oberthur ID-One PIV (v2.3.5)		Y	Y		Y		Y	Y	Y
Oberthur ID-One PIV (v2.4.0)		Y	Y		Y	P	Y	Y	Y
IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1		Y	Y		Y	P	Y	Y	Y

Key:

- Y – Fully supported.
- P – Partially supported. See below for details.
- blank – Not supported.

PKI – ECC

Some IDEMIA smart cards support a limited range of PKI – ECC features:

	Smart card		
Feature	**Oberthur ID-One PIV (v2.3.2) "ID-One PIV (Type A) Large D"**	**Oberthur ID-One PIV (v2.3.4)**	**Oberthur ID-One PIV (v2.4.0)**
Generate a private key for a certificate request.	Y	Y	Y
Write a certificate to the smart card.	Y	Y	Y
Specify the default certificate for Windows logon.	Y	Y	Y
ECC NIST P256 Curve	Y	Y	Y
ECC NIST P384 Curve	Y	Y	Y
ECC NIST P521 Curve			
Remove certificates.	Y	Y	Y
Enumerate certificates on the card.	Y	Y	Y

	Smart card
Feature	**IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1**
Generate a private key for a certificate request.	Y
Write a certificate to the smart card.	Y
Specify the default certificate for Windows logon.	Y
ECC NIST P256 Curve	Y
ECC NIST P384 Curve	Y
ECC NIST P521 Curve	
Remove certificates.	Y
Enumerate certificates on the card.	Y

Key:

- Y – Fully supported.
- blank – Not supported.

5.3.2 Additional features

ID-One PIV smart cards can be provided by IDEMIA to support the following additional features:

- HID prox support.
- IDEMIA may ship their ID-One PIV cards with the contactless portion disabled. When you first issue an ID-One PIV card through MyID, whether by standard issuance, deferred activation, bureau issuance with card activation, or through **Batch Encode Card**, MyID will enable the contactless portion of the card if it is not already enabled.

5.4 Installation and configuration

5.4.1 PIN characters for PIV cards

The SP800-73 PIV specification requires that PIV cards use numeric-only PINs. It is possible to configure MyID to use non-numeric PIN characters for some PIV cards, although some smart cards will fail to issue; for example the Oberthur ID-One PIV (v2.3.4), Oberthur ID-One PIV (v2.3.5), and Oberthur ID-One PIV (v2.4.0).

Make sure you set up the credential profile correctly; in the **PIN Characters** section of the **Credential Profiles** workflow, set number to be **Mandatory**, and uppercase letters, lowercase letters, and symbols to **Not Allowed**.

5.4.2 Serial numbers for IDEMIA PIV cards

ID-One PIV cards have a serial number which consists of the IIN and CIN.

Oberthur ID-One PIV v2.3.2 and v2.3.4 cards arrive from the factory with a serial number (IIN and CIN) already prepersonalized on the cards. When ordering cards from IDEMIA the customer would specify the IIN, and IDEMIA would create a unique CIN for each card.

Oberthur ID-One PIV v2.3.5 and Oberthur ID-One PIV v2.4.0 cards arrive without a serial number. MyID will create a serial number (IIN and CIN) during personalization.

MyID generates a CIN for each card, but the IIN (the first part of the serial number) is taken from a configuration value in MyID.

Important: On any MyID system that is intended to issue ID-One PIV v2.3.5 or v2.4.0 cards, you *must* configure MyID with the required IIN value.

To configure the IIN value to be personalized on ID-One PIV v2.3.5 or v2.4.0 cards, in the **Operation Settings** workflow, on the **Devices** tab, set the **Serial Number IIN** to the required value. The default is `0123456789`.

When MyID issues an Oberthur ID-One PIV v2.3.5 card or Oberthur ID-One PIV v2.4.0 card, this IIN, and a generated CIN value, will be personalized on the card.

If the card already has a serial number (if it has already been issued by MyID), the serial number will not be repersonalized. Therefore any cards issued previously issued by MyID will keep the IIN with which they were previously personalized.

IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1 cards use the IDEMIA CUID (personalized by IDEMIA at the factory) for the serial number, except for cases where IIN and CIN are present on the card already; in which case MyID uses the IIN and CIN as the serial number. MyID does not personalize IIN and CIN during personalization for IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1 cards.

5.5 Interoperability

5.5.1 Lock attempts

The number of attempts to lock a card may be set by the manufacturer according to the BAP and may not be configurable through MyID. For example, if you set the number of locking attempts to 5, the following cards lock after the listed number of attempts:

- Oberthur ID-One PIV (v2.3.2) (Type A) Large D – 10 attempts.
- Oberthur ID-One PIV (v2.3.4) – 10 attempts.
- Oberthur ID-One PIV (v2.3.5) – 10 attempts.
- Oberthur ID-One PIV (v2.4.0) – 10 attempts.
- IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1 – 3 attempts.

5.5.2 Card readers

Oberthur ID-One PIV (v2.3.5), Oberthur ID-One PIV (v2.4.0) cards, and IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1 cards have been found to have interoperability problems with SCR331 card readers.

5.5.3 Windows logon using Oberthur ID-One PIV (v2.4.0) or IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1 cards

If you want to use Oberthur ID-One PIV (v2.4.0) or IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1 cards to log on to Windows, you must install the Oberthur minidriver for PIV cards (version 1.3.4.438).

This minidriver is used only for Windows logon – you do not need to install the minidriver to use the cards with MyID.

6 SafeNet

6.1 SafeNet smart cards

MyID has been tested with the following SafeNet smart cards:

Smart card	Type	Middleware
SafeNet eToken 4000	Smart card/Chip	SafeNet Authentication Client v10.4
SafeNet eToken 4100	Smart card/Chip	SafeNet Authentication Client v10.4
SafeNet eToken 5100	USB Token/Chip	SafeNet Authentication Client v10.4
SafeNet eToken 5110	USB Token/Chip	SafeNet Authentication Client v10.4
SafeNet eToken 5110 FIPS	USB Token/Chip	SafeNet Authentication Client v10.4

Note: MyID supports the eToken 5110 and 5110 FIPS, but does not support the eToken 5110 CC.

6.2 Platforms

These smart cards have been tested on:

	Operating System			
Smart card	**Windows 7 (32-bit)**	**Windows 7 (64-bit)**	**Windows 8.1**	**Windows 10**
SafeNet eToken 4000	Y	Y		
SafeNet eToken 4100	Y	Y		
SafeNet eToken 5100	Y	Y	Y	Y
SafeNet eToken 5110	Y	Y	Y	Y
SafeNet eToken 5110 FIPS	Y	Y	Y	Y

Key:

- Y – Fully supported.
- blank – Not supported.

6.3 Supported features for SafeNet smart cards

See section *1.2*, *Supported features* for a description of the features supported by smart cards.

6.3.1 Features

The following MyID features are smart card or middleware specific. The table below indicates which smart card-dependent features are available in MyID with SafeNet smart cards.

	Features								
Smart card	**MyID**	**PIN management**	**GlobalPlatform**	**Applets**	**PKI – RSA**	**PKI – ECC**	**PIV**	**Printing**	**Client OS**
SafeNet eToken 4000	Y	P			Y			Y	Y
SafeNet eToken 4100	Y	P			Y			Y	Y
SafeNet eToken 5100	Y	P			Y				Y
SafeNet eToken 5110	Y	P			Y				Y
SafeNet eToken 5110 FIPS	Y	P			P				Y

Key:

- Y – Fully supported.
- P – Partially supported. See below for details.
- blank – Not supported.

PIN management

Some SafeNet cards support a limited range of PIN management features:

	Smart card		
Feature	**SafeNet eToken 4000**	**SafeNet eToken 4100**	**SafeNet eToken 5100**
Set minimum and maximum PIN lengths.	Y	Y	Y
Set the character types.	Y	Y	Y
Lock the PIN after issuance.	Y	Y	Y
Identify when the PIN is locked.	Y	Y	Y
Replace the SOPIN with a randomized value.		Y	Y
Replace the SOPIN with the factory SOPIN at cancellation.		Y	Y
Unlock the PIN using the SOPIN.	Y	Y	Y
Provide a remote unlock code.	Y	Y	
Reset the PIN at cancellation.	Y		Y

	Smart card	
Feature	**SafeNet eToken 5110**	**SafeNet eToken 5110 FIPS**
Set minimum and maximum PIN lengths.	Can set minimum, but not maximum.	Can set minimum, but not maximum.
Set the character types.	Y	Y
Lock the PIN after issuance.	Y	Y
Identify when the PIN is locked.	Y	Y
Replace the SOPIN with a randomized value.	Y	Y
Replace the SOPIN with the factory SOPIN at cancellation.	Y	Y
Unlock the PIN using the SOPIN.	Y	Y
Provide a remote unlock code.	Y	Y
Reset the PIN at cancellation.	Y	Y

Key:

- Y – Fully supported.
- blank – Not supported.

PKI – RSA

Some SafeNet cards support a limited range of PKI – RSA features:

	Smart card
Feature	**SafeNet eToken 5110 FIPS**
Generate a private key for a certificate request.	Y
Write a certificate to the smart card.	Y
Cryptographically sign or encrypt data.	Y
Specify the default certificate for Windows logon.	Y
Write 1024 bit certificates.	
Write 2048 bit certificates.	Y
Remove certificates.	Y
Inject a private key for certificate recovery.	Y
Enumerate certificates on the card.	Y

Key:

- Y – Fully supported.
- blank – Not supported.

6.4 Installation and configuration

This section provides any information required when installing the middleware for the smart cards or configuring the smart cards through either their middleware or through MyID.

6.4.1 Standard mode

You must install the SafeNet Authentication Client middleware in **Standard** mode (that is, *not* the BSec-compatible mode). Standard mode is the first option that is presented when you run the middleware installer.

6.4.2 Complexity requirements

When you set up the SafeNet client tools, you must set the complexity requirement option to **None**. This option may be labeled **Must meet complexity requirements** or **Password Complexity**, depending on the version of the middleware you are using.

6.4.3 Password change prompt

When you first issue a smart card, you may be prompted by the SafeNet middleware to change your password. Click **Cancel** to continue without changing the password.

Also, if you select the **Token Password must be changed on first logon** option when performing a challenge/response unlock, when the user logs in to MyID with the unlocked card, they will be prompted to change the PIN. To avoid this, deselect the **Token Password must be changed on first logon** option when unlocking the smart card.

6.4.4 Credential profiles for SafeNet smart cards

You must make sure that you have set the credential profile to use the same settings as the SafeNet client installation. Check the SafeNet middleware to ensure that the values you use are correct.

If you do not use the same settings in the credential profile and the SafeNet client installation, you will experience an error similar to the following:

```
Initialize Error
Cause: Invalid PIN
Solution: Please enter a new PIN.
-2147220729 Exception thrown: class CCardException
Error: 0x80040307 : You entered an incorrect pass phrase or PIN
PKCS Error: 0x00000020 Data invalid
```

To set the credential profile properties:

1. From the **Configuration** category, select **Credential Profiles**.
2. Select the credential profile you want to edit, then click **Modify**.
3. Click **PIN Settings**.
4. Set the following options to match the settings used in the SafeNet client installation:
   - **Maximum PIN Length** – the default SafeNet client value is 16.
   - **Minimum PIN Length** – the default SafeNet client value is 6.
   - **Logon Attempts** – the default SafeNet client value is 3.
5. Click **Next** and complete the workflow.

6.5 Interoperability

There are no known issues with interoperability.

7 SafeNet Assured Technologies

7.1 SafeNet Assured Technologies smart cards

MyID has been tested with the following SafeNet Assured Technologies smart cards:

Smart card	Type	Middleware
SafeNet SC650 V4.1	Smart card/Chip	SafeNet AT High Assurance Client V2.12.020

7.1.1 Secure Channel Protocol

The Secure Channel Protocol (SCP) is used in the **Manage GlobalPlatform Keys** workflow.

When configuring your GlobalPlatform keys, use the following Secure Channel Protocol:

Smart card	SCP
SafeNet SC650 V4.1	SCP02

7.2 Platforms

These smart cards have been tested on:

	Operating System			
Smart card	Windows 7 (32-bit)	Windows 7 (64-bit)	Windows 8.1	Windows 10
SafeNet SC650 V4.1	Y	Y	Y	Y

Key:

- Y – Fully supported.
- blank – Not supported.

7.3 Supported features for SafeNet Assured Technologies smart cards

See section *1.2*, *Supported features* for a description of the features supported by smart cards.

7.3.1 Features

The following MyID features are smart card or middleware specific. The table below indicates which smart card-dependent features are available in MyID with SafeNet smart cards.

	Features								
Smart card	**MyID**	**PIN management**	**GlobalPlatform**	**Applets**	**PKI – RSA**	**PKI – ECC**	**PIV**	**Printing**	**Client OS**
SafeNet SC650 V4.1	Y	P	Y		Y			Y	Y

Key:

- Y – Fully supported.
- P – Partially supported. See below for details.
- blank – Not supported.

PIN management

Some SafeNet Assured Technologies cards support a limited range of PIN management features:

	Smart card
Feature	**SafeNet SC650 V4.1**
Set minimum and maximum PIN lengths.	
Set the character types.	
Lock the PIN after issuance.	Y
Identify when the PIN is locked.	Y
Replace the SOPIN with a randomized value.	Y
Replace the SOPIN with the factory SOPIN at cancellation.	Y
Unlock the PIN using the SOPIN.	Y
Provide a remote unlock code.	
Reset the PIN at cancellation.	Y

Key:

- Y – Fully supported.
- blank – Not supported.

7.4 Installation and configuration

This section provides any information required when installing the middleware for the smart cards or configuring the smart cards through either their middleware or through MyID.

7.4.1 SafeNet High Assurance Client configuration

In the SafeNet High Assurance Client configuration, in the Client Settings, you must make sure that the **Copy user certificates to a local store** option is not set. If you set this option, you may experience problems when using the **Unlock Credential** workflow.

7.5 Interoperability

7.5.1 SC650 cards

If you are using SC650 cards, and MyID cannot detect the cards on the logon screen while the SafeNet middleware *can* detect the cards, you may have to adjust the settings for your card reader. You may also experience a problem with collecting SC650 cards that displays an error similar to the following:

```
Error : -2147023779 - Error: 0x8007045d : The request could not be
performed because of an I/O device error.
```

This is a known issue with SafeNet cards and Omnikey readers. To set up an Omnikey card reader to use 3 volts as the startup state, and therefore be able to detect the SC650 cards properly, set the following in the registry on the client PC:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CardMan]

"MHzRequired"=dword:00000037

"PowerUpOrder"=dword:00000003

"TPDU_T1Mode"=dword:00000001
```

7.5.2 Card issuance error if logged on with an SC650 operator card

If there are two SC650 cards connected to the MyID client, and one of the cards is used to log on to MyID, an error may occur during card issuance operations.

This issue has been reported to SafeNet and is waiting for resolution.

7.5.3 Slow card detection with SC650 cards

When an SC650 is inserted to the card reader, detection of the card in MyID may take longer than expected; allow approximately 10 seconds for the card to be detected.

This issue has been reported to SafeNet and is waiting for resolution.

7.5.4 Known issues

- **IKB-157 – Compatibility issues with SC650 and Oberthur ID-One PIV cards**

  If you connect an Oberthur ID-One PIV card to MyID at the same time as a SafeNet SC650 card, the Oberthur card will be incorrectly identified and will not be usable by MyID. Remove one of the cards to continue.

8 TCOS

8.1 TCOS smart cards

MyID has been tested with the following TCOS smart cards:

Smart card	Type	Middleware
TCOS	Smart card	TCOS3 Smart Card Minidriver v1.7.5.0

Note: MyID has been tested with the minidrivers listed in the table above. Your version of the minidriver may be different, depending on which Windows updates you have installed. Make sure that you have the supported version of the minidriver installed.

8.2 Platforms

These smart cards have been tested on:

	Operating System			
Smart card	**Windows 7 (32-bit)**	**Windows 7 (64-bit)**	**Windows 8.1**	**Windows 10**
TCOS	Y	Y	Y	

Key:

- Y – Fully supported.
- blank – Not supported.

8.3 Supported features for TCOS smart cards

See section *1.2*, *Supported features* for a description of the features supported by smart cards.

8.3.1 Features

The following MyID features are smart card or middleware specific. The table below indicates which smart card-dependent features are available in MyID with TCOS smart cards.

	Features								
Smart card	**MyID**	**PIN management**	**GlobalPlatform**	**Applets**	**PKI – RSA**	**PKI – ECC**	**PIV**	**Printing**	**Client OS**
TCOS	P	Y			P			Y	Y

Key:

- Y – Fully supported.
- P – Partially supported. See below for details.
- blank – Not supported.

MyID

TCOS smart cards support a limited range of MyID features:

	Smart card
Feature	**TCOS**
Can be used to generate an RSA keypair that can be used for operations in MyID.	
Can be used to sign data (including logon to MyID) with an RSA keypair on the smart card.	
Can be used to encrypt data with an RSA keypair on the smart card.	
MyID can set the label of the smart card.	Y
MyID can erase the content of the smart card (excluding the printed card surface)	Y

Key:

- Y – Fully supported.
- blank – Not supported.

PKI – RSA

TCOS smart cards support a limited range of PKI – RSA features:

	Smart card
Feature	**TCOS**
Generate a private key for a certificate request.	Y
Write a certificate to the smart card.	Y
Cryptographically sign or encrypt data.	Y
Specify the default certificate for Windows logon.	Y
Write 1024 bit certificates.	
Write 2048 bit certificates.	Y
Remove certificates.	Y
Inject a private key for certificate recovery.	Y
Enumerate certificates on the card.	Y

Key:

- Y – Fully supported.
- blank – Not supported.

8.4 Installation and configuration

This section provides any information required when installing the middleware for the smart cards or configuring the smart cards through either their middleware or through MyID.

8.4.1 Using minidrivers for TCOS smart cards

If you are using TCOS smart cards with minidrivers, you must have the following:

- TCOS3 Smart Card Minidriver (`tcos3cmd.dll`)

See also section *1.5*, *Minidriver-based cards*.

9 TicTok

9.1 TicTok smart cards

MyID has been tested with the following TicTok smart cards:

Smart card	Type	Middleware
TicTok v1.1	Smart card	IDProtect Client 7.1.2.7
TicTok v2.0	Smart card	IDProtect Client 7.1.2.7

Note: This card is based on the Athena IDProtect Smart card. MyID has been tested with the minidrivers listed in the table above. Your version of the minidriver may be different, depending on which Windows updates you have installed. Make sure that you have the supported version of the minidriver installed.

9.2 Platforms

These smart cards have been tested on:

	Operating System			
Smart card	**Windows 7 (32-bit)**	**Windows 7 (64-bit)**	**Windows 8.1**	**Windows 10**
TicTok v1.1	Y	Y	Y	Y
TicTok v2.0	Y	Y	Y	Y

Key:

- Y – Fully supported.
- blank – Not supported.

9.3 Supported features for TicTok smart cards

See section *1.2*, *Supported features* for a description of the features supported by smart cards.

9.3.1 Features

The following MyID features are smart card or middleware specific. The table below indicates which smart card-dependent features are available in MyID with TicTok smart cards.

	Features								
Smart card	**MyID**	**PIN management**	**GlobalPlatform**	**Applets**	**PKI – RSA**	**PKI – ECC**	**PIV**	**Printing**	**Client OS**
TicTok v1.1	Y	Y			Y			Y	Y
TicTok v2.0	Y	Y			Y	Y		Y	Y

Key:

- Y – Fully supported.
- blank – Not supported.

9.4 Installation and configuration

This section provides any information required when installing the middleware for the smart cards or configuring the smart cards through either their middleware or through MyID.

9.4.1 Using minidrivers for TicTok smart cards

If you are using TicTok smart cards with minidrivers, you must have the following:

- Athena IDProtect Minidriver

See also section *1.5*, *Minidriver-based cards*.

Note: The IDProtect software has an installer like middleware, but is treated by MyID as a minidriver.

9.4.2 PIN Inactivity Timer for TicTok smart cards

The credential profile contains a **PIN Inactivity Timer** setting in the **PIN Settings**. This value is in minutes.

Important: In previous versions of MyID, for TicTok cards, this setting was in seconds, and users were recommended to set up a separate credential profile for TicTok cards, and to set the **PIN Inactivity Timer** setting to the required number of minutes multiplied by 60. *This is no longer the case*. You must now specify a value in minutes. If you set up this workaround for a previous version, you must contact Intercede customer support, quoting reference SUP-203.

9.5 Interoperability

9.5.1 Known issues

- **Issues with smart card detection**

  Intercede has seen issues with version 7.1.2.7 of the IDProtect Client where MyID is not able to detect a new card. This is caused by the minidriver failing to return a serial number for the new card. This has been seen only with uninitialized cards, as they are delivered from the factory. NXP/Athena have provided Intercede with the following registry change to enable the serial number to be retrieved. You must apply this registry change to every client used to issue new cards:

  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\Athena Smartcard Solutions\IDProtect Client]

  "MDAllowWorkWithUnformattedCards"=dword:00000001

  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Athena Smartcard Solutions\IDProtect Client]

  "MDAllowWorkWithUnformattedCards"=dword:00000001
  ```

10 Yubico

10.1 Yubico smart cards

MyID has been tested with the following Yubico smart cards:

Smart card	Type	Middleware
YubiKey 4	Smart card/USB	n/a
YubiKey Nano	Smart card/USB	n/a

Note: MyID integrates with YubiKey devices as a PIV Compatible smart card. The cards support PIV features but are not PIV compliant, due to their form factor. You cannot use Windows PIN unblock functionality for these tokens; instead, you can use the MyID Card Utility to unblock the PIN.

10.1.1 Cryptographic keys for Yubico cards

When you configure the cryptographic keys, use the following details:

	YubiKey 4	YubiKey Nano
DeviceType in MyID	YubiKey 4	YubiKey Nano
GlobalPlatform SCP	n/a	n/a
Factory GlobalPlatform Key Type	n/a	n/a
Factory GlobalPlatform Key Diversification Algorithm	n/a	n/a
Factory PIV 9B Key Type	3DES	3DES
PIV 9B Factory Key diversification algorithm	Static	Static
Recommended PIV 9B Customer Key diversification algorithm	Diverse2	Diverse2

10.2 Platforms

These smart cards have been tested on:

	Operating System			
Smart card	**Windows 7 (32-bit)**	**Windows 7 (64-bit)**	**Windows 8.1**	**Windows 10**
YubiKey 4	Y	Y	Y	Y
YubiKey Nano	Y	Y	Y	Y

Key:

- Y – Fully supported.
- blank – Not supported.

10.3 Supported features for Yubico smart cards

See section *1.2*, *Supported features* for a description of the features supported by smart cards.

10.3.1 Features

The following MyID features are smart card or middleware specific. The table below indicates which smart card-dependent features are available in MyID with Yubico smart cards.

	Features								
Smart card	**MyID**	**PIN management**	**GlobalPlatform**	**Applets**	**PKI – RSA**	**PKI – ECC**	**PIV**	**Printing**	**Client OS**
YubiKey 4	Y	Y			Y	P	N		Y
YubiKey Nano	Y	Y			Y	P	N		Y

Key:

- Y – Fully supported.
- P – Partially supported. See below for details.
- blank – Not supported.

PKI – ECC

Some Yubico smart cards support a limited range of PKI – ECC features:

	Smart card	
Feature	**YubiKey 4**	**YubiKey Nano**
Generate a private key for a certificate request.	Y	Y
Write a certificate to the smart card.	Y	Y
Specify the default certificate for Windows logon.	Y	Y
ECC NIST P256 Curve	Y	Y
ECC NIST P384 Curve	Y	Y
ECC NIST P521 Curve		
Remove certificates.	Y	Y
Enumerate certificates on the card.	Y	Y

Key:

- Y – Fully supported.
- blank – Not supported.

10.4 Installation and configuration

This section provides any information required when installing the middleware for the smart cards or configuring the smart cards through either their middleware or through MyID.

10.5 Card format

Yubico smart cards have PIV features, but are not fully PIV-compliant. In the **Device Profiles** section of the **Credential Profiles** workflow, you must select the following from the **Card Format** drop-down list:

- CivCertificatesOnly.xml

10.6 Interoperability

MyID does not support the Yubico PIV Attestation functionality.

10.6.1 Known issues

- **IKB-207 – Integrated Windows Logon with YubiKey 4**

  You can use a YubiKey 4 to log on to Windows 7.

  You *cannot* use a YubiKey 4 to log on to Windows 8.1.

  To use a YubiKey 4 to log on to Windows 10, you must install the following Microsoft update:

  - KB3216755