MyID Enterprise

Version 11.8

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: INT1967-10

December 2020

Copyright

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:

  For example:
  - Copy the file *before* starting the installation.
  - Do *not* remove the files before you have backed them up.
- ***Bold and italic*** hyperlinks 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 product installation media.
- 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 work 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 term "smart card" is used generically throughout this document to describe these devices.

The following are currently supported by MyID:

- Athena. See section *3*, *Athena smart cards* for details.
- Giesecke+Devrient. See section *4*, *Giesecke+Devrient smart cards* for details.
- IDEMIA. See section *5*, *IDEMIA smart cards* for details.
- TCOS. See section *6*, *TCOS smart cards* for details.
- Thales. See section *7*, *Thales authentication devices* for details.

  Note: Thales authentication devices have previously been listed under a range of different brands; for example, Gemalto or SafeNet.
- Thales Trusted Cyber Technologies. See section *8*, *Thales Trusted Cyber Technologies smart cards* for details.
- TicTok. See section *9*, *TicTok smart cards* for details.
- Yubico. See section *10*, *Yubico smart cards* 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 Microsoft virtual smart cards (VSCs) see the ***Microsoft VSC Integration Guide***.

For information on support for Intel VSCs, see the ***Intel Authenticate Integration Guide***.

1.1 Change history

Version	Description
INT1967-01	Released with MyID version 11.0.
INT1967-02	Released with MyID version 11.1.
INT1967-03	Released with MyID version 11.2.
INT1967-04	Released with MyID version 11.3.
INT1967-05	Released with MyID version 11.3.1.
INT1967-06	Released with MyID version 11.4.
INT1967-07	Released with MyID version 11.5.
INT1967-08	Released with MyID version 11.6.
INT1967-09	Released with MyID version 11.7.
INT1967-10	Released with MyID version 11.8.

2 Smart card features

This chapter contains information about the features supported on the smart card that MyID allows you to issue and manage.

2.1 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**

  PIN management – determines whether MyID can manage the PIN for the smart card. This incorporates the following features:

  - 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).
  - MyID can set on-card PIN policy settings.

    MyID allows you to set various policies for PINs using the settings in the credential profile. MyID enforces these settings (where possible) for any operations carried out by MyID. For some smart cards, some or all of these settings are applied directly to the card, which means that the settings will also be enforced by third-party tools and utilities.

- **GP**

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.

- **Applet**

  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.

- **RSA**

  PKI – RSA – determines whether MyID can work with certificates using RSA keys on the smart card. Some of the features listed below depend on the certificate authority you are using; see the integration guide for your CA.

  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.

- **ECC**

PKI – ECC – determines whether MyID can work with certificates using ECC keys on the smart card. Some of the features listed below depend on the certificate authority you are using; see the integration guide for your CA.

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 support archive certificate 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.

Note: MyID can issue certificates using ECC keys to appropriate smart cards, but using ECC certificates on smart cards with Windows operating system features requires an appropriate minidriver or middleware that supports ECC certificates for that feature to be installed. Injecting an ECC private key to the smart card for certificate recovery operations is not supported.

- **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.

  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.

  Note: You cannot use the additional identities feature of MyID with any card that has a PIV applet.

  - 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 recovers only as many certificates as the card will hold. During a certificate recovery operation, MyID actively interrogates the PIV card to determine the maximum number of certificates that can be recovered to it, and then restricts the number of certificates permitted for recovery to match. 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 recovery. 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; see the *Remote PIN Management utility for PIV cards* section in the ***Operator's Guide*** for details.

- **OPACITY**

  Determines whether MyID can personalize a card to support OPACITY.

  For more information, see section *2.11*, *Setting up OPACITY*.
  - MyID can enable the OPACITY capability of a PIV card, in Zero Key Management mode (OPACITY-ZKM)
  - MyID can generate an OPACITY pairing code for a PIV card when it is personalized, which is stored as an encrypted value in the MyID database.
- **Print**

  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.

    You may need additional configuration of your Windows environment, including specific settings where elliptic curve cryptography (ECC) is used. See your Microsoft documentation for details.

    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.

    For ECC certificates on PIV cards, the built-in Windows minidriver – which registers the smart card as "Identity Device (NIST SP 800-73[PIV])" in Windows Device Manager – does not allow the use of ECC certificates with functionality such as Windows logon.

- 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.

2.2 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 *Importing serial numbers* section of the ***Administration Guide*** for details of importing serial numbers.

- **Magnetic Stripe**

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

2.3 Smart 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

2.4 Minidriver-based smart cards

All cards that use minidrivers require some additional setup.

2.4.1 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
```

2.4.2 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 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 *Unlocking a credential remotely* section in the ***Operator's Guide*** for details of using the **Unlock Credential** workflow.

2.4.3 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.

2.5 Upgrading existing systems

If you are upgrading from an earlier version of MyID, and are using smart 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.

2.6 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.

2.7 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.

2.8 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 canceled, 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.

2.9 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.

2.10 Predetermined PIN policies

Smart cards may be manufactured with predetermined PIN policies – these PIN policies are not under the control of MyID.

If you have ordered smart cards like this from your manufacturer, make sure you create credential profiles in MyID that match the PIN policies that your cards can support.

2.11 Setting up OPACITY

The Open Protocol for Access Control Identification and Ticketing with privacY (OPACITY) provides a secure, high speed contactless interface for smart cards that support the protocol. MyID supports OPACITY Zero Key Management (ZKM), enabling interoperability with a range of readers or terminals.

When MyID personalizes the smart card, a Card Verifiable Certificate (CVC) is created on the card which is digitally signed, allowing an application to determine whether it trusts the card sufficiently to communicate over the contactless interface.

The OPACITY information on the smart card is reset when you erase the card; however, if you cancel the card using any other process (for example, **Cancel Credential**) the OPACITY information is not removed from the card, as the card is not physically affected by remote cancellation processes, and no certificate revocation takes place for the CVC.

Optionally, a pairing code can be generated when MyID personalizes the card, preventing the use of OPACITY over the contactless interface until a device has been able to provide the correct pairing code; this code is reset on the card when you erase it.

Note: MyID does not communicate with smart cards over the OPACITY contactless interface. You must always connect a smart card to a smart card reader to communicate with MyID.

2.11.1 Smart cards supported for OPACITY

See the tables of supported features in each chapter in this document for details of which cards support OPACITY. Any additional information about the specifics of the smart cards' support for OPACITY is detailed in the interoperability section in the appropriate chapter.

2.11.2 Setting up the CVC signing certificate

When MyID personalizes a smart card to support OPACITY, it creates a Card Verifiable Certificate (CVC) on the card; this certificate is digitally signed, which means that you must configure MyID to use a signing certificate for this purpose.

The signing certificate must be an ECC certificate with an appropriate size for the cards being issued; for example, IDEMIA ID-One PIV 2.4.1 cards support P256 and P384, therefore ECC NIST P384 Curve is recommended.

To configure the signing certificate in the MyID registry:

1. On the MyID application server, log on using the MyID COM+ account.
2. Request a certificate that will be protected by CNG (Key Storage Provider). You can issue a certificate from any certificate authority as long as it is available to CNG.

   Note: Do not enable strong private key protection on the certificate, as this will prevent processing of the request by the MyID account.
3. Once the certificate has been generated, install and save it as a `.cer` file (either Base64/PEM or binary format). You must save it in a location accessible to the MyID application, so save it to the `Components` folder within the MyID installation folder.

   Note: You may need administrative privileges to save files to this area.
4. Enter the filename of the certificate in the system registry.
   a. From the Start menu, run `regedit`.
   b. Navigate to:

      `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432Node\Intercede\Edefice\PIV`

      If this key does not exist, you can create it.
   c. Set the value of the following string to the full path and filename of the certificate:

      `CVCSigningCertificate`

      Create the value if it does not exist.

2.11.3 Setting up the credential profile

You must set up a credential profile in MyID to allow you to issue smart cards with support for OPACITY.

To set up a credential profile for OPACITY support:

1. From the **Configuration** category, select **Credential Profiles**.
2. Edit an existing credential profile or create a new one.
3. In the **Issuance Settings** section, set the following options:

- **OPACITY** – set this to one of the following values:
  - **None** – Do not attempt to perform OPACITY personalization.
  - **OPACITY without Pairing Codes** – Personalize the OPACITY CVC but do not set an OPACITY pairing code.
  - **OPACITY with Pairing Codes** – Personalize the OPACITY CVC and generate and set an OPACITY pairing code.
- **Send Pairing Code Emails** – when the card is issued, send an email to the cardholder containing the pairing code.

  See section *2.11.4*, *Distributing the pairing code*

4. In the **Mail Documents** section, set the following option:
   - **Select PIN Mailing Document** – select a PIN mailing document template that contains the user's pairing code.

     See section *2.11.4*, *Distributing the pairing code* for details of your options for distributing pairing codes.
5. Complete the credential profile.

See the *Managing credential profiles* section in the ***Administration Guide*** for details of setting up credential profiles.

Note: MyID can personalize a smart card to support OPACITY when it is issued; however, it *cannot* update an already-issued smart card to a new version of the credential profile that has had OPACITY added. If you want to issue smart cards to support OPACITY, you must set up the credential profile to support OPACITY before you initially issue the cards. Alternatively, you can reprovision a smart card to add OPACITY support with an updated credential profile, as this carries out a full personalization.

2.11.4 Distributing the pairing code

If you are setting up your smart cards to use pairing codes for OPACITY, you must send the code to the cardholder when the card is issued. You can provide the pairing code in the following ways:

- Using an email template.

  Select the **Send Pairing Code Emails** option in the credential profile, and MyID sends an email to the cardholder's email address using the **Pairing Code Notification** email template. You can edit this template using the **Email Templates** workflow.

  For information on editing email templates, see the *Changing email messages* section in the ***Administration Guide***.

  To confirm that a pairing code has been sent in an email notification, you can review the **Notifications Manager** workflow.
- Using a PIN mailing document.

  Note: Only the **Collect Card** and **Batch Collect Card** workflows supports mailing document templates. Other workflows, for example **Print Mailing Document**, use the previous Microsoft Word-based mail merge document templates, which do *not* support pairing codes. If you are using card activation, you are recommended to send pairing codes in an email instead.

Select a mailing document template from the **Select PIN Mailing Document** option in the credential profile, and MyID generates a document when the card is issued that you can print and send to the cardholder.

To include the pairing code in a mailing document, you must add the following substitution code to the template:

```
%%rawdevice.PairingCode_decrypt%%
```

For details of configuring templates for PIN mailing documents, contact customer support, quoting reference SUP-255.

To confirm that a pairing code has been printed, you can review the **Audit Reporting** workflow for the **Print Mailing Document** operation.

Note: If you generate a mailing document and the document contains the text "Pairing Code" instead of an actual pairing code, check that you have set the **OPACITY** option in the credential profile to **OPACITY with Pairing Codes**.

2.11.5 Identifying SPE cards

You can confirm whether a card has been issued with support for OPACITY Secure PIN Entry (SPE) by using the **Identify Card** workflow. The **Chip Type** displayed in the workflow includes "SPE" if the card requires OPACITY Secure PIN Entry.

2.11.6 Audit details

You can confirm that a card has been issued with support for OPACITY by checking the **Audit Reporting** workflow in MyID.

1. From the **Reports** category, select **Audit Reporting**.
2. From the **Operation** drop-down list, select **Issue Card**.
3. Click **Search**.
4. Click the green icon on the audit record for the card issuance you want to view.

   This displays the breakdown of the actions carried out during the card issuance.
5. Click the green icon for the top action in the list.
6. In the Audit Information Gathered dialog, click **Card Content**.

   At the bottom of the list, an entry similar to the following means that the card has been issued with support for OPACITY:

   ```
   2019-04-04 15:18:56 Personalised the Secure Messaging CVC object. Success
   ```

2.11.7 Troubleshooting OPACITY smart cards

If you see an error similar to the following when attempting to collect a smart card set up for OPACITY:

```
Unable to perform the requested operation
Solutions:
A problem occurred attempting to process your selection.
Please contact your administrator.
Error Number: 890493
```

The audit for the failure may additionally mention the `LoadCVC` operation.

This error may be caused by the following:

- Using an older version of MyID Desktop.

  Update your client software to the latest version.

- Using a smart card reader that does not support extended APDU commands.

  Use a smart card reader that supports extended APDU commands; see section *5.5.7*, *Smart card readers supported for OPACITY* for details.

- Attempting to create a CVC but the CVC signing certificate is not present or invalid.

  Set up a CVC signing certificate; see section *2.11.2*, *Setting up the CVC signing certificate*.

If you see an error similar to the following:

```
An unexpected error has occurred.
Solutions:
Please contact your administrator.
Error Number: -2147220720
```

The extra information may contain the following:

```
Error: 0x80040310: Not logged into card
Extra Info: Error caused by function Unlock Pin
```

This error may be caused by attempting to collect an SPE card using a credential profile that is not set up for OPACITY.

2.12 Issuing smart cards that have PIV applets

Many of the smart cards and USB tokens that are supported by MyID contain a PIV applet; this applet is used to store certificates and information on the device, and is designed to support compliance with the Personal Identity Verification standards (FIPS 201-2) as laid down for federal agencies by the US Government.

To issue a PIV card that is fully compliant with the standards, you must use the PIV edition of MyID; however, if you have the non-PIV edition of MyID, you can issue these smart cards without having to comply fully with the US Government standards – this is sometimes referred to as CIV (Commercial Identity Verification).

To issue a card with a PIV applet, you must carry out the following:

1. Set up a PIV 9B key for the credential type.

   This is sometimes known as the "management key".

   You must use the **Key Manager** workflow within MyID to add a factory **PIV 9B Card Administration Key** to the system. See the *Managing keys* section in the ***Administration Guide*** for details.

2. Set up a GlobalPlatform key for the credential type.

   GlobalPlatform keys are required to carry out operations on some types of smart card.

   If your smart cards support GlobalPlatform keys, you must use the **Manage GlobalPlatform Keys** workflow to add a factory GlobalPlatform key. See the *GlobalPlatform keys* section in the ***Administration Guide*** for details.

3. Set up a credential profile to specify a CIV-compatible card format.

   The card format determines which containers are available for certificates.

In the **Credential Profiles** workflow, in the **Device Profiles** section, from the **Card Format** drop-down list select the following:

- `CivCertificatesOnly.xml`

You can then select containers for the certificates on the Select Certificates screen.

See the *Managing credential profiles* section in the ***Administration Guide*** for details.

See the appropriate chapter of this guide for any specific requirements for your type of smart card; for example, some smart card types may require customer PIV 9B keys in addition to the factory PIV 9B key.

Note: If you require customized data in the PIV applet (for example, creating CHUID values, custom data, or signed data objects) contact your Intercede account manager to discuss your requirements.

Warning: PIV applets hold certificates in named containers. The Card Authentication (9E) container is designed for physical access control, so certificates within this container can be accessed without providing the user PIN, even over a contactless interface; you must ensure that the certificate contains only necessary information and does not expose cardholder details. If you do not have a suitable certificate policy, you are recommended to leave this container empty; do not assign a certificate policy to it when configuring the credential profile.

2.13 Unlocking smart cards that have a PIV applet

For cards that include a PIV applet (that is, PIV cards, and devices such as the YubiKey tokens that use PIV technology in a USB form factor) MyID provides the MyID Card utility, which allows a user to carry out a remote challenge/response unlock operation, and to change the user PIN.

For information on using the MyID Card Utility, see the *Remote PIN Management utility for PIV cards* section in the ***Operator's Guide***.

MyID also provides an unlock credential provider that allows a user to unlock their PIV-based device from the Windows logon screen. This provides the same functionality as the MyID Card Utility for remotely unlocking cards.

For details of installing and configuring the unlock credential provider, see the *Installing the unlock credential provider* section in the ***Installation and Configuration Guide***.

For details of using the unlock credential provider to unlock a PIV card, see the *Unlock credential provider* section in the ***Operator's Guide***.

See the interoperability section of each chapter in this document for details of which devices support the MyID Card Utility and the unlock credential provider.

2.14 Transaction locking

During the collection of a smart card, MyID makes use of transaction locks on the smart card reader. This is to ensure that the interaction with the smart card is not interrupted by other applications. If other applications are allowed access, then the collection will fail.

MyID will hold a transaction lock on a smart card only when it is necessary for card personalization.

During smart card collection it is strongly recommended that you *do not* lock your workstation. If any user input is required, for example user PIN entry, you will not be able to unlock your workstation. This is due to MyID having an active transaction lock. The only way to recover from this is to remove the smart card you are collecting.

If you are carrying out a batch issuance, if you set the **Suppress errors during batch issue** option, you can lock and unlock your workstation without any problems.

2.14.1 Issues with transaction locking

Different smart cards and middlewares behave in different ways, and you may encounter some problems with transaction locking with some smart cards under certain circumstances.

For example:

- If you log on to Windows with a SafeNet SC650 card, log on to MyID, then attempt to issue another SC650 to another user, if you lock and unlock the machine several times you may experience a signing error within MyID, or an error when trying to unlock Windows.
- When using IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1 smart cards with Secure PIN Entry (SPE) support, if you have another, unissued, SPE cards in a card reader, you may experience problems if you lock your workstation, launch the UAC process, or use another application to access the smart card.
- When logged on to MyID using a PIV card, if you use the Identify Card workflow to identify a card issued to another user, then lock your workstation, the transaction lock is not released, and you must remove your operator card before you can log back in.
- If you log on to Windows using a Giesecke+Devrient Sm@rt Café® Expert 6.0 smart card, log on to MyID, then lock your workstation, you cannot log back in to Windows. This is an issue with the middleware.
- If you log on to Windows using a smart card, log on to MyID, then use the Switch User option in Windows to log back in as the same user, you may experience visual glitches in the MyID interface. If this happens, you can use the menu button at the top left of MyID Desktop to return to the Dashboard, or to log off and log on again.
- If you lock your workstation in the middle of a workflow, when you unlock, you may be required to log back in with your card.
- If you log on to Windows with a YubiKey USB token, log on to MyID, then lock your workstation in the middle of a workflow, when you unlock, you may experience a signing error. You can restart the workflow to resolve the problem.

3 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.

3.1 Platforms for Athena smart cards

These smart cards have been tested on:

	Operating System	
Smart card	Windows 8.1	Windows 10
Athena IDProtect	Y	

Key:

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

3.2 Supported features for Athena smart cards

See section *2.1*, *Supported features* for a description of the features supported by smart cards.

3.2.1 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	GP	Applet	RSA	ECC	PIV	OPACITY	Print	Client OS
Athena IDProtect	Y	P			Y	P			Y	Y

Key:

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

PIN management

The following Athena cards support a limited range of PIN management features:

	Smart card
Feature	**Athena IDProtect**
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.	Y
Reset the PIN at cancellation.	Y
Configure on-card PIN policy.	P

Key:

- Y – Fully supported.
- P – Partially supported. For details of supported on-card PIN policy features, see section *3.4.1, PIN policy settings*.
- blank – Not supported.

PKI – ECC

The following Athena smart cards support a limited range of PKI – ECC features:

	Smart card
Feature	**Athena IDProtect**
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	Y
Remove certificates.	Y
Archive certificates.	
Enumerate certificates on the card.	Y

Key:

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

3.3 Installation and configuration for Athena smart cards

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.

3.3.1 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 *2.4, Minidriver-based smart cards*.

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

3.4 Interoperability for Athena smart cards

This section contains information about any considerations for using these smart card with other systems.

3.4.1 PIN policy settings

MyID allows you to set various policies for PINs using the settings in the credential profile. MyID enforces these settings for any operations carried out by MyID. For some smart cards, some or all of these settings are applied directly to the card, which means that the settings will also be enforced by third-party tools and utilities.

The following settings are supported for on-card PIN policy settings:

	Smart card
PIN Setting	**Athena IDProtect**
Maximum PIN Length	Y
Minimum PIN Length	Y
Repeated Characters Allowed	
Sequential Characters Allowed	
Logon Attempts	Y
PIN Inactivity Timer	Y
PIN History	Y
Lowercase PIN Characters	Y (optional or mandatory)
Uppercase PIN Characters	Y (optional or mandatory)
Numeric PIN Characters	Y (optional or mandatory)
Symbol PIN Characters	Y (optional or mandatory)
Lifetime	Y

- Y – Supported.
- blank – Not supported.

3.4.2 Known issues

- **Issues with smart card detection**

  Intercede has seen issues with the IDProtect Client software 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
  ```

4 Giesecke+Devrient smart cards

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

Smart card	Type	Middleware
Sm@rt Café® Expert 6.0	Smart card/Chip	AET SafeSign v3.0.97
SCE v7.0	PIV card	n/a

4.1 Keys for Giesecke+Devrient smart cards

This section provides information you need when setting up keys for Giesecke+Devrient smart cards.

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
Credential Type in MyID	GieseckeDevrient PIV
GlobalPlatform Secure Channel	SCP03
Factory GlobalPlatform Key Type	AES128
Factory GlobalPlatform Key Diversification Algorithm	Static
Factory PIV 9B Key Encryption Type	3DES
PIV 9B Factory Key Diversity	Static
Recommended PIV 9B Customer Key Diversity	Diverse2

4.2 Platforms for Giesecke+Devrient smart cards

These smart cards have been tested on:

	Operating System	
Smart card	Windows 8.1	Windows 10
Sm@rt Café® Expert 6.0		Y
SCE v7.0	Y	Y

Key:

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

4.3 Supported features for Giesecke+Devrient smart cards

See section *2.1*, *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**	**GP**	**Applet**	**RSA**	**ECC**	**PIV**	**OPACITY**	**Print**	**Client OS**
Sm@rt Café® Expert 6.0	Y	P			Y				Y	Y
SCE v7.0		P	Y		P	P	Y		Y	Y

Key:

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

PIN management

The following Giesecke+Devrient cards support a limited range of PIN management features:

	Smart card	
Feature	**Sm@rt Café® Expert 6.0**	**SCE v7.0**
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
Configure on-card PIN policy.		

Key:

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

PKI – RSA

The following Giesecke+Devrient smart card supports a limited range of PKI – RSA features:

	Smart card
Feature	**SCE v7.0**
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.[1]	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.

PKI – ECC

The following 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	
ECC NIST P521 Curve	
Remove certificates.	Y
Archive certificates.	
Enumerate certificates on the card.	Y

Key:

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

4.3.2 Remote unlock

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

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

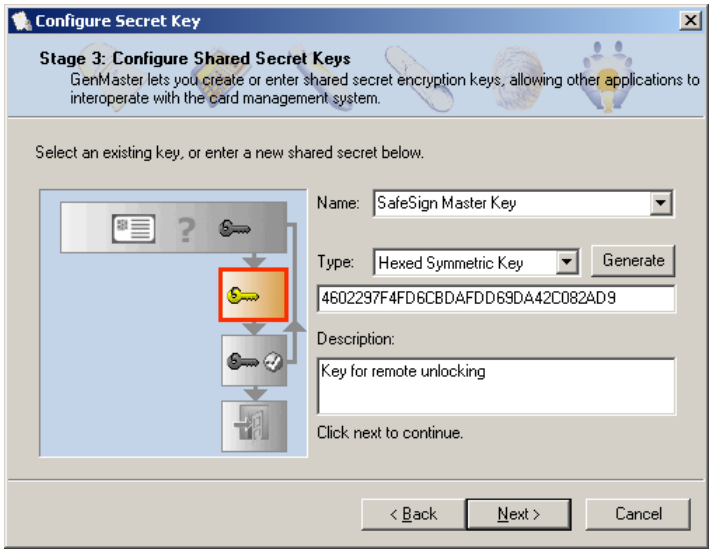
MyID supports remote unlocking of Giesecke+Devrient using the standard **Unlock Credential** workflow.

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.



   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

The **Offline Unlock Method** configuration option specifies which remote unlocking method you are going to use.

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 one of the following:
   - **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.
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 *Unlocking a credential remotely* section in the ***Operator's 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 for Giesecke+Devrient smart cards

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

4.4.1 Installation options

While installing this middleware, ensure that the 'CSP' and 'PKCS11' subcomponents are selected – these are required for MyID to communicate with the smart cards. You must install the middleware before installing MyID.

4.4.2 Special usage notes for MyID

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

4.4.3 Issuing smart cards that have PIV applets

For information on issuing smart cards that have PIV applets using a non-PIV MyID system, see section *2.12*, *Issuing smart cards that have PIV applets*.

4.5 Interoperability for Giesecke+Devrient smart cards

This section contains information about any considerations for using these smart card with other systems.

4.5.1 Unlocking Giesecke+Devrient PIV cards

Giesecke+Devrient SCE v7.0 PIV cards include a PIV applet, which means that you can use the MyID Card Utility to carry out a remote challenge/response unlock operation and change the user PIN, and the unlock credential provider to unlock the devices from the Windows logon screen.

See section *2.13*, *Unlocking smart cards that have a PIV applet*.

4.5.2 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.

4.5.3 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.

4.5.4 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.

4.5.5 Collecting a Sm@rt Café card on a PC with a VSC

You may experience problems when issuing Sm@rt Café cards if there is a VSC present on your PC. For more information, contact customer support quoting reference SUP-291.

4.5.6 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**.

4.5.7 Additional identities and PIV cards

You cannot use the additional identities feature of MyID with any smart card that has a PIV applet. This includes the Giesecke+Devrient SCE v7.0.

4.5.8 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 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

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.

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)*
- *BAP#087483 – ID-One PIV 2.4 on Cosmo v8.1 SPE*

Note: For more information about Secure PIN Entry (SPE), see section *5.5.6, OPACITY Secure PIN Entry support*.

5.1 Keys for IDEMIA smart cards

This section provides information you need when setting up keys for IDEMIA smart cards.

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)
Credential Type in MyID	Oberthur ID-One PIV	Oberthur ID-One PIV	Oberthur ID-One PIV v8
GlobalPlatform Secure Channel	OT-SCP03	OT-SCP03	SCP03
Factory GlobalPlatform Key Type	AES128	AES128	AES256
Factory GlobalPlatform Key Diversification Algorithm	Diverse3	Diverse3	DiverseOT108
Factory PIV 9B Key Encryption Type	3DES	3DES	AES256
PIV 9B Factory Key Diversity	Static	Static	DiverseOT108
Recommended PIV 9B Customer Key Diversity	Diverse2	Diverse2	DiverseOT108

	Oberthur ID-One PIV (v2.4.0)	IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1
Credential Type in MyID	Oberthur ID-One PIV v8	IDEMIA ID-One PIV v81
GlobalPlatform Secure Channel	SCP03	SCP03
Factory GlobalPlatform Key Type	AES256	AES256

	Oberthur ID-One PIV (v2.4.0)	IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1
Factory GlobalPlatform Key Diversification Algorithm	DiverseOT108	DiverseOT108
Factory PIV 9B Key Encryption Type	AES256	AES256
PIV 9B Factory Key Diversity	DiverseOT108	DiverseOT108
Recommended PIV 9B Customer Key Diversity	DiverseOT108	DiverseOT108

5.2 Platforms for IDEMIA smart cards

These smart cards have been tested on:

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

Key:

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

5.3 Supported features for IDEMIA smart cards

See section *2.1*, *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**	**GP**	**Applet**	**RSA**	**ECC**	**PIV**	**OPACITY**	**Print**	**Client OS**
Oberthur ID-One Cosmo v7.0.1 with IAS Standard applet	Y	P			Y				Y	Y
Oberthur ID-One PIV (v2.3.2) "ID-One PIV (Type A) Large D"		P	Y		Y	P	Y		Y	Y
Oberthur ID-One PIV (v2.3.4)		P	Y		Y	P	Y		Y	Y

Smart card	Features									
	MyID	PIN	GP	Applet	RSA	ECC	PIV	OPACITY	Print	Client OS
Oberthur ID-One PIV (v2.3.5)		P	Y		Y	P	Y		Y	Y
Oberthur ID-One PIV (v2.4.0)		P	Y		Y	P	Y		Y	Y
IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1		P	Y		Y	P	Y	Y	Y	Y

Key:

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

PIN management

The following IDEMIA cards support a limited range of PIN management features:

Feature	Smart card	
	Oberthur ID-One Cosmo v7.0.1 with IAS Standard applet	Oberthur ID-One PIV (v2.3.2) "ID-One PIV (Type A) Large D"
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
Configure on-card PIN policy.		

Feature	Smart card	
	Oberthur ID-One PIV (v2.3.4)	Oberthur ID-One PIV (v2.3.5)
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
Configure on-card PIN policy.		

Feature	Smart card	
	Oberthur ID-One PIV (v2.4.0)	IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1
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
Configure on-card PIN policy.		P

Key:

- Y – Fully supported.
- P – Partially supported. For details of supported on-card PIN policy features, see section *5.5.2, PIN policy settings*.
- blank – Not supported.

PKI – ECC

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

Feature	Smart card	
	Oberthur ID-One PIV (v2.3.2) "ID-One PIV (Type A) Large D"	Oberthur ID-One PIV (v2.3.4)
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
Archive certificates.	Y	Y
Enumerate certificates on the card.	Y	Y

Feature	Smart card	
	Oberthur ID-One PIV (v2.3.5)	Oberthur ID-One PIV (v2.4.0)
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
Archive certificates.	Y	Y
Enumerate certificates on the card.	Y	Y

Feature	Smart card
	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

Feature	Smart card
	IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1
ECC NIST P256 Curve	Y
ECC NIST P384 Curve	Y
ECC NIST P521 Curve	
Remove certificates.	Y
Archive certificates.	Y
Enumerate certificates on the card.	Y

Key:

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

ECC support for PIV cards

The ECC features you can use for PIV cards are defined in NIST sp800-78-4:

- The `piv-auth` and `cardauth` containers can hold P256 certificates.
- The `dig-sig` and `key-management` containers can hold P256 or P384 certificates.
- P521 certificates are not allowed.

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, bureau issuance with card activation, through **Batch Encode Card**, or deferred activation, MyID will enable the contactless portion of the card if it is not already enabled.

IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1 cards support the following additional feature:

- Symmetric PIV 9E key.

  To enable this feature, set the **Manage PIV 9E key on supported devices** configuration option (on the **Device Security** page of the **Security Settings** workflow) to Yes. The symmetric 9E key is diversified using the 9B Master Key. During card issuance the 9E Key is set using the Customer 9B master key, while the Factory 9B master key is used when the device is erased.

5.4 Installation and configuration for IDEMIA smart cards

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

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 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.

5.4.3 Issuing smart cards that have PIV applets

For information on issuing smart cards that have PIV applets using a non-PIV MyID system, see section *2.12, Issuing smart cards that have PIV applets*.

5.5 Interoperability for IDEMIA smart cards

This section contains information about any considerations for using these smart card with other systems.

5.5.1 Unlocking IDEMIA PIV cards

IDEMIA and Oberthur ID-One PIV cards include a PIV applet, which means that you can use the MyID Card Utility to carry out a remote challenge/response unlock operation and change the user PIN, and the unlock credential provider to unlock the devices from the Windows logon screen.

See section *2.13, Unlocking smart cards that have a PIV applet*.

- **IKB-284 – Cannot use the unlock credential provider with IDEMIA cards manufactured for SPE**

  It is not currently possible to unlock an IDEMIA PIV card that has been manufactured to require Secure Pin Entry (BAP#087483 – ID-One PIV 2.4 on Cosmo v8.1 SPE).

5.5.2 PIN policy settings

MyID allows you to set various policies for PINs using the settings in the credential profile. MyID enforces these settings for any operations carried out by MyID. For some smart cards, some or all of these settings are applied directly to the card, which means that the settings will also be enforced by third-party tools and utilities.

The following settings are supported for on-card PIN policy settings:

	Smart card
PIN Setting	**IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1**
Maximum PIN Length	
Minimum PIN Length	
Repeated Characters Allowed	
Sequential Characters Allowed	
Logon Attempts	Y
PIN Inactivity Timer	
PIN History	
Lowercase PIN Characters	
Uppercase PIN Characters	
Numeric PIN Characters	
Symbol PIN Characters	
Lifetime	

- Y – Supported.
- blank – Not supported.

5.5.3 Logon attempts

The number of attempts to log on to a card before it is locked may be set by the manufacturer according to the BAP and may not be configurable through MyID, depending on the smart card being used. For example, if you set the number of logon attempts to 5, the following cards lock after the listed number of attempts, ignoring the value set in MyID:

- 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.

The **Logon Attempts** option in the credential profile *is* encoded as the PIN try counter for the following:

- IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1

This means that you can configure the number of logon attempts through MyID for this smart card.

Note: It is a feature of PIV cards that PIN attempts that are too short (for example, four digits) are rejected without being sent to the smart card, and therefore do not count towards the number of PIN attempts. Only PIN attempts that provide six or more digits are counted towards the number of attempts.

5.5.4 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.

5.5.5 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 minidriver for PIV cards. The recommended versions are:

- Oberthur ID-One PIV (v2.4.0) – Oberthur minidriver for PIV cards version 1.1.3.1025.
- IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1 (including SPE smart cards) – IDEMIA minidriver for PIV cards version 1.2.3.279.

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

5.5.6 OPACITY Secure PIN Entry support

OPACITY Secure PIN Entry (SPE) requires that whenever a PIN or PUK is sent in an APDU (Application Protocol Data Unit) command to a smart card, it is sent using an encrypted secure channel.

Important: To issue smart cards that are manufactured to use SPE, you *must* set up the credential profile to use OPACITY; if you attempt to issue an SPE card with a credential profile that is not set up to use OPACITY, issuance of the card will fail. An error with number `-2147220720` may appear; the audit may contain the message `Not logged into card` for the failure. See section *2.11*, *Setting up OPACITY* for details of setting up your credential profile.

Note: Smart cards that are manufactured to use SPE are *not* PIV compliant.

This feature is supported within MyID on IDEMIA smart cards that have this capability. Currently, this includes the following:

- IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1 smart cards, manufactured to *BAP#087483 – ID-One PIV 2.4 on Cosmo v8.1 SPE*.

You can confirm whether a card has been issued with support for OPACITY Secure PIN Entry (SPE) by using the **Identify Card** workflow. The **Chip Type** displayed in the workflow includes "SPE" if the card requires OPACITY Secure PIN Entry.

If you want to use cards manufactured to different specifications for SPE with MyID, contact your Intercede account manager to discuss your requirements.

Note: SPE-EP (Secure PIN Entry – Enhanced Privacy) is not supported.

5.5.7 Smart card readers supported for OPACITY

OPACITY personalization is supported for IDEMIA PIV cards when using a smart card reader that supports Extended APDU; for example, OmniKey 5x21 or OmniKey 5x25.

Only OPACITY personalization requires these readers; other operations are not restricted.

5.5.8 Additional identities and PIV cards

You cannot use the additional identities feature of MyID with any smart card that has a PIV applet. This includes all Oberthur/IDEMIA ID-One PIV smart cards.

6 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.

6.1 Platforms for TCOS smart cards

These smart cards have been tested on:

	Operating System	
Smart card	Windows 8.1	Windows 10
TCOS	Y	

Key:

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

6.2 Supported features for TCOS smart cards

See section *2.1*, *Supported features* for a description of the features supported by smart cards.

6.2.1 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	GP	Applet	RSA	ECC	PIV	OPACITY	Print	Client OS
TCOS	P	P			P				Y	Y

Key:

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

MyID

The following 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.

PIN management

The following TCOS cards support a limited range of PIN management features:

	Smart card
Feature	**TCOS**
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.	Y
Reset the PIN at cancellation.	Y
Configure on-card PIN policy.	

Key:

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

PKI – RSA

The following 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

	Smart card
Feature	**TCOS**
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.

6.3 Installation and configuration for TCOS smart cards

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.

6.3.1 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 *2.4*, *Minidriver-based smart cards*.

7 Thales authentication devices

Thales authentication devices have previously been listed under a range of different brands; for example, Gemalto or SafeNet. These legacy names continue to be referenced in MyID.

These devices are distinct from the SC650 devices provided by Thales Trusted Cyber Technologies; see section *8*, *Thales Trusted Cyber Technologies smart cards* for details.

MyID has been tested with the following Thales authentication devices:

Smart card	Type	Middleware	Part number	Support
IDPrime MD3810	Smart card/Chip	SafeNet Minidriver 10.8 R2	O1095608	Supported
IDPrime MD830	Smart card/Chip	SafeNet Minidriver 10.8 R2		Supported
IDPrime MD830 Rev B FIPS Level 2	Smart card/Chip	SafeNet Minidriver 10.8 R2	O1094404	Supported
IDPrime MD830 Rev B FIPS Level 3	Smart card/Chip	SafeNet Minidriver 10.8 R2	O1094403	Supported
IDPrime MD831	Smart card/Chip	SafeNet Minidriver 10.8 R2		Supported
IDPrime MD3840	Smart card/Chip	SafeNet Minidriver 10.8 R2	O1095676	Supported
IDPrime MD840 Rev A	Smart card/Chip	SafeNet Minidriver 10.8 R2		Supported
IDPrime MD940	Smart card/Chip	SafeNet Minidriver 10.8 R2	O1132421	Supported
IDPrime MD930 FIPS Level 2	Smart card/Chip	SafeNet Minidriver 10.8 R2	O1151236	Supported
IDPrime MD3930 FIPS Level 2	Smart card/Chip	SafeNet Minidriver 10.8 R2	O1152066	Supported
IDPrime 931 FIPS 140-2 L2	Smart card/Chip	SafeNet Minidriver 10.8 R2	O1152492 O1152483	Supported
IDPrime MD3940	Smart card/Chip	SafeNet Minidriver 10.8 R2	O1130317	Supported
IDPrime 3940 FIDO	Smart card/Chip	SafeNet Minidriver 10.8 R2	O1157191	Supported
IDPrime PIV Card v2.0	PIV card	n/a	C1070904 C1072203	Deprecated
IDPrime PIV Card v2.1	PIV card	n/a	O1110994	Supported
IDPrime PIV Card v3.0	PIV card	n/a	O1138439	Supported
SafeNet eToken 4100	Smart card/Chip	SafeNet Authentication Client 10.8 R2		Deprecated

Smart card	Type	Middleware	Part number	Support
SafeNet eToken 5100	USB Token/Chip	SafeNet Authentication Client 10.8 R2		Deprecated
SafeNet eToken 5110	USB Token/Chip	SafeNet Authentication Client 10.8 R2		Deprecated
SafeNet eToken 5110 FIPS	USB Token/Chip	SafeNet Authentication Client 10.8 R2	909-000451-001	Supported
SafeNet eToken 5110+	USB Token/Chip	SafeNet Authentication Client 10.8 R2	909-000417-002	Supported
SafeNet eToken 5110 CC	USB Token/Chip	SafeNet Mini Driver v10.8	909-000115-001	Deprecated

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.

For smart cards that use the SafeNet Authentication Client, see section *7.4, Installation and configuration for Thales authentication devices* for details of configuring the SAC software for middleware or minidriver operation.

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

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

Note: All Thales minidriver-based cards, including the SafeNet eToken 5110 CC, are displayed in the **Identify Card** workflow with a **Chip Type** of "Gemalto IDPrime MD8310".

7.1 Keys for Thales authentication devices

This section provides information you need when setting up keys for Thales authentication devices.

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
IDPrime PIV Card v2.0	SCP03
IDPrime PIV Card v2.1	SCP03
IDPrime PIV Card v3.0	SCP03

7.1.2 Cryptographic keys for IDPrime PIV cards

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

	IDPrime PIV Card v2.0	IDPrime PIV Card v2.1	IDPrime PIV Card v3.0
Credential Type in MyID	Gemplus PIV V2	Gemplus PIV V21	Gemplus PIV V3
GlobalPlatform Secure Channel	SCP03	SCP03	SCP03
Factory GlobalPlatform Key Type	AES128	AES128	AES128
Factory GlobalPlatform Key Diversification Algorithm	Diverse108	Diverse108	Diverse108
Factory PIV 9B Key Encryption Type	3DES or AES128	AES128	AES128
PIV 9B Factory Key Diversity	Static	Static	Static
Recommended PIV 9B Customer Key Diversity	Diverse2	Diverse2	Diverse2

7.1.3 Cryptographic keys for Thales minidriver devices

For Thales minidriver-based cards (for example, IDPrime MD830, MD831, MD840, MD3810, MD3840, or SafeNet eToken 5110 CC), the card technology supports GlobalPlatform keys, but the actual cryptographic key details depend on the cards you order from the manufacturer; for example, the manufacturer may provide you with the necessary cryptographic key details (secure channel, GlobalPlatform keys, and so on), or the cards may be shipped with diversified keys, where the key is kept private by the manufacturer.

To issue cards whose keys are unknown, you must disable customer GlobalPlatform keys within MyID for this device type – use the settings on the **Devices** page of the **Security Settings** workflow. Disabling customer GlobalPlatform keys produces a security message within MyID; for information about disabling this warning, contact customer support to discuss your requirements, quoting reference SUP-273.

See also the *Securing Devices* section in the ***System Security Checklist*** document for important information about device security.

7.2 Platforms for Thales authentication devices

These smart cards have been tested on:

	Operating System	
Smart card	**Windows 8.1**	**Windows 10**
IDPrime MD3810	Y	Y
IDPrime MD830	Y	Y
IDPrime MD830 Rev B FIPS Level 2	Y	Y
IDPrime MD830 Rev B FIPS Level 3	Y	Y
IDPrime MD831	Y	Y
IDPrime MD3840	Y	Y

	Operating System	
Smart card	**Windows 8.1**	**Windows 10**
IDPrime MD840 Rev A	Y	Y
IDPrime MD940	Y	Y
IDPrime MD930 FIPS Level 2	Y	Y
IDPrime MD3930 FIPS Level 2	Y	Y
IDPrime 931 FIPS 140-2 L2	Y	Y
IDPrime MD3940	Y	Y
IDPrime 3940 FIDO	Y	Y
IDPrime PIV Card v2.0	Y	Y
IDPrime PIV Card v2.1	Y	Y
IDPrime PIV Card v3.0	Y	Y
SafeNet eToken 4100		Y
SafeNet eToken 5100	Y	Y
SafeNet eToken 5110	Y	Y
SafeNet eToken 5110 FIPS	Y	Y
SafeNet eToken 5110+	Y	Y
SafeNet eToken 5110 CC	Y	Y

Key:

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

7.3 Supported features for Thales authentication devices

See section *2.1*, *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 Thales authentication devices.

	Features									
Smart card	**MyID**	**PIN**	**GP**	**Applet**	**RSA**	**ECC**	**PIV**	**OPACITY**	**Print**	**Client OS**
IDPrime MD3810	Y	P			Y	P			Y	Y
IDPrime MD830	Y	P			Y	P			Y	Y
IDPrime MD830 Rev B FIPS Level 2	Y	P			P	P			Y	Y
IDPrime MD830 Rev B FIPS Level 3	Y	P			P	P			Y	Y
IDPrime MD831	Y	P			Y	P			Y	Y
IDPrime MD3840	Y	P			Y	P			Y	Y

	Features									
Smart card	MyID	PIN	GP	Applet	RSA	ECC	PIV	OPACITY	Print	Client OS
IDPrime MD840 Rev A	Y	P			Y	P			Y	Y
IDPrime MD940	Y	P			Y	P			Y	Y
IDPrime MD930 FIPS Level 2	Y	P			P	P			Y	Y
IDPrime MD3930 FIPS Level 2	Y	P			P	P			Y	Y
IDPrime 931 FIPS 140-2 L2	Y	P			P	P			Y	Y
IDPrime MD3940	Y	P			P	P			Y	Y
IDPrime 3940 FIDO	Y	P			P	P			Y	Y
IDPrime PIV Card v2.0		P	Y		P	P	Y		Y	Y
IDPrime PIV Card v2.1		P	Y		P	P	Y		Y	Y
IDPrime PIV Card v3.0		P	Y		P	P	Y		Y	Y
SafeNet eToken 4100	Y	P			P				Y	Y
SafeNet eToken 5100	Y	P			P					Y
SafeNet eToken 5110	Y	P			P					Y
SafeNet eToken 5110 FIPS	Y	P			P					Y
SafeNet eToken 5110+	Y	P			P					Y
SafeNet eToken 5110 CC	Y	P			P	P				Y

Key:

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

PIN management

The following Thales authentication devices support a limited range of PIN management features:

	Smart card	
Feature	IDPrime MD3810	IDPrime MD830
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

Feature	Smart card	
	IDPrime MD3810	IDPrime MD830
Unlock the PIN using the SOPIN.	Y	Y
Provide a remote unlock code.	Y	Y
Reset the PIN at cancellation.	Y	Y
Configure on-card PIN policy.		

Feature	Smart card	
	IDPrime MD830 Rev B FIPS Level 2	IDPrime MD830 Rev B FIPS Level 3
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
Configure on-card PIN policy.		

Feature	Smart card	
	IDPrime MD831	IDPrime MD3840
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
Configure on-card PIN policy.		

	Smart card	
Feature	**IDPrime MD840 Rev A**	**IDPrime MD940**
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
Configure on-card PIN policy.		

	Smart card	
Feature	**IDPrime MD930 FIPS Level 2**	**IDPrime MD3930 FIPS Level 2**
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
Configure on-card PIN policy.		

	Smart card		
Feature	**IDPrime 931 FIPS 140-2 L2**	**IDPrime MD3940**	**IDPrime 3940 FIDO**
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	Y
Replace the SOPIN with the factory SOPIN at cancellation.	Y	Y	Y
Unlock the PIN using the SOPIN.	Y	Y	Y

	Smart card		
Feature	**IDPrime 931 FIPS 140-2 L2**	**IDPrime MD3940**	**IDPrime 3940 FIDO**
Provide a remote unlock code.	Y	Y	Y
Reset the PIN at cancellation.	Y	Y	Y
Configure on-card PIN policy.			

	Smart card	
Feature	**IDPrime PIV Card v2.0**	**IDPrime PIV Card v2.1**
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
Configure on-card PIN policy.		

	Smart card	
Feature	**IDPrime PIV Card v3.0**	**SafeNet eToken 4100**
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	
Configure on-card PIN policy.		P

Feature	Smart card	
	SafeNet eToken 5100	SafeNet eToken 5110
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
Reset the PIN at cancellation.	Y	Y
Configure on-card PIN policy.	P	P

Feature	Smart card	
	SafeNet eToken 5110 FIPS	SafeNet eToken 5110+
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
Configure on-card PIN policy.	P	P

Feature	Smart card
	SafeNet eToken 5110 CC
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.	Y
Reset the PIN at cancellation.	Y
Configure on-card PIN policy.	

Key:

- Y – Fully supported.
- P – Partially supported. For details of supported on-card PIN policy features, see section *7.5.2, PIN policy settings*.
- blank – Not supported.

PKI – RSA

The following Thales authentication devices support a limited range of PKI – RSA features:

	Smart card	
Feature	**IDPrime MD830 Rev B FIPS Level 2**	**IDPrime MD830 Rev B FIPS Level 3**
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	**IDPrime MD940**	**IDPrime MD930 FIPS Level 2**	**IDPrime MD3930 FIPS Level 2**
Generate a private key for a certificate request.	Y	Y	Y
Write a certificate to the smart card.	Y	Y	Y
Cryptographically sign or encrypt data.	Y	Y	Y
Specify the default certificate for Windows logon.	Y	Y	Y
Write 1024 bit certificates.			
Write 2048 bit certificates.	Y	Y	Y

	Smart card		
Feature	**IDPrime MD940**	**IDPrime MD930 FIPS Level 2**	**IDPrime MD3930 FIPS Level 2**
Remove certificates.	Y	Y	Y
Inject a private key for certificate recovery.	Y	Y	Y
Enumerate certificates on the card.	Y	Y	Y

	Smart card		
Feature	**IDPrime 931 FIPS 140-2 L2**	**IDPrime MD3940**	**IDPrime 3940 FIDO**
Generate a private key for a certificate request.	Y	Y	Y
Write a certificate to the smart card.	Y	Y	Y
Cryptographically sign or encrypt data.	Y	Y	Y
Specify the default certificate for Windows logon.	Y	Y	Y
Write 1024 bit certificates.			
Write 2048 bit certificates.	Y	Y	Y
Remove certificates.	Y	Y	Y
Inject a private key for certificate recovery.	Y	Y	Y
Enumerate certificates on the card.	Y	Y	Y

	Smart card	
Feature	**IDPrime PIV Card v2.0**	**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.		

Feature	Smart card	
	IDPrime PIV Card v3.0	SafeNet eToken 4100
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

Feature	Smart card	
	SafeNet eToken 5100	SafeNet eToken 5110
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

Feature	Smart card	
	SafeNet eToken 5110 FIPS	SafeNet eToken 5110+
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

	Smart card	
Feature	**SafeNet eToken 5110 FIPS**	**SafeNet eToken 5110+**
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	**SafeNet eToken 5110 CC**
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.

PKI – ECC

The following Thales authentication devices support a limited range of PKI – ECC features:

	Smart card	
Feature	**IDPrime MD3810**	**IDPrime MD830**
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	Y	Y
Remove certificates.	Y	Y
Archive certificates.		
Enumerate certificates on the card.	Y	Y

	Smart card	
Feature	**IDPrime MD830 Rev B FIPS Level 2**	**IDPrime MD830 Rev B FIPS Level 3**
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	Y	Y
Remove certificates.	Y	Y
Archive certificates.		
Enumerate certificates on the card.	Y	Y

	Smart card	
Feature	**IDPrime MD831**	**IDPrime MD3840**
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	
ECC NIST P521 Curve	Y	
Remove certificates.	Y	Y
Archive certificates.		
Enumerate certificates on the card.	Y	Y

	Smart card	
Feature	**IDPrime MD840 Rev A**	**IDPrime MD940**
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		

	Smart card	
Feature	**IDPrime MD840 Rev A**	**IDPrime MD940**
Remove certificates.	Y	Y
Archive certificates.		
Enumerate certificates on the card.	Y	Y

	Smart card	
Feature	**IDPrime MD930 FIPS Level 2**	**IDPrime MD3930 FIPS Level 2**
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	Y	Y
Remove certificates.	Y	Y
Archive certificates.		
Enumerate certificates on the card.	Y	Y

	Smart card		
Feature	**IDPrime 931 FIPS 140-2 L2**	**IDPrime MD3940**	**IDPrime 3940 FIDO**
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		
ECC NIST P521 Curve	Y		
Remove certificates.	Y	Y	Y
Archive certificates.			
Enumerate certificates on the card.	Y	Y	Y

	Smart card	
Feature	**IDPrime PIV Card v2.0**	**IDPrime PIV Card v2.1**
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
ECC NIST P256 Curve	Y	Y
ECC NIST P384 Curve	Y	Y
ECC NIST P521 Curve		
Remove certificates.	Y	Y
Archive certificates.	Y	Y
Enumerate certificates on the card.		

	Smart card	
Feature	**IDPrime PIV Card v3.0**	**SafeNet eToken 5110 CC**
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	
ECC NIST P521 Curve		
Remove certificates.	Y	Y
Archive certificates.	Y	
Enumerate certificates on the card.		Y

Key:

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

ECC support for PIV cards

The ECC features you can use for PIV cards are defined in NIST sp800-78-4:

- The `piv-auth` and `cardauth` containers can hold P256 certificates.
- The `dig-sig` and `key-management` containers can hold P256 or P384 certificates.
- P521 certificates are not allowed.

7.3.2 Unlocking features

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

For SafeNet Authentication Client-based smart cards, see the SAC documentation for details.

For minidriver-based smart cards, see section *2.4.2*, *Windows integrated unblock* for details.

7.3.3 Hybrid contactless cards

Thales 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 *Issuance Settings* section in 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.

7.4 Installation and configuration for Thales authentication devices

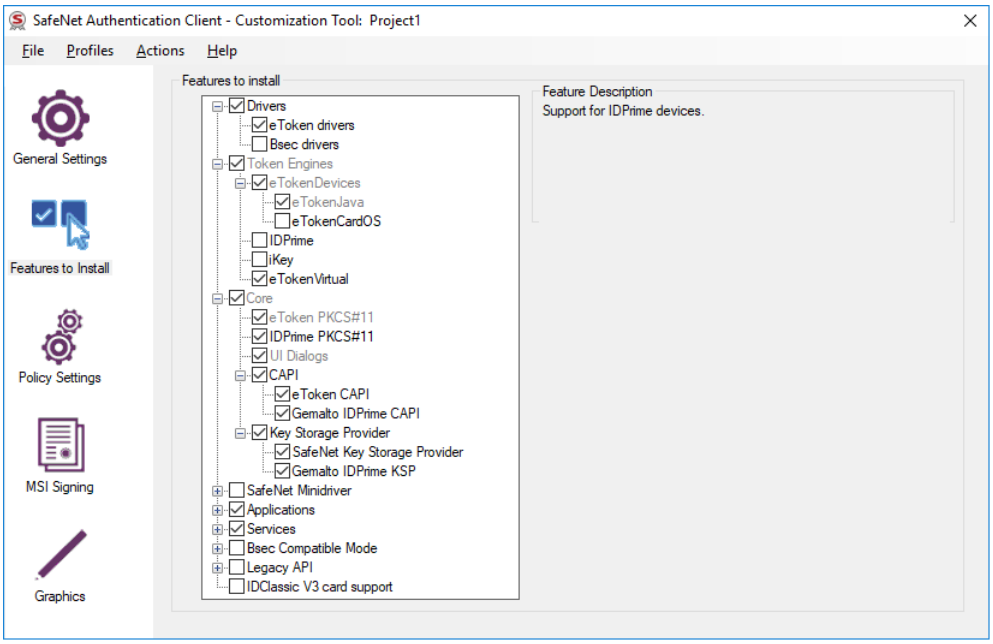
This section provides any information required when installing the minidrivers or middleware for the smart cards or configuring the smart cards through their minidriver, middleware or through MyID.

7.4.1 SafeNet Authentication Client 10.8 R2

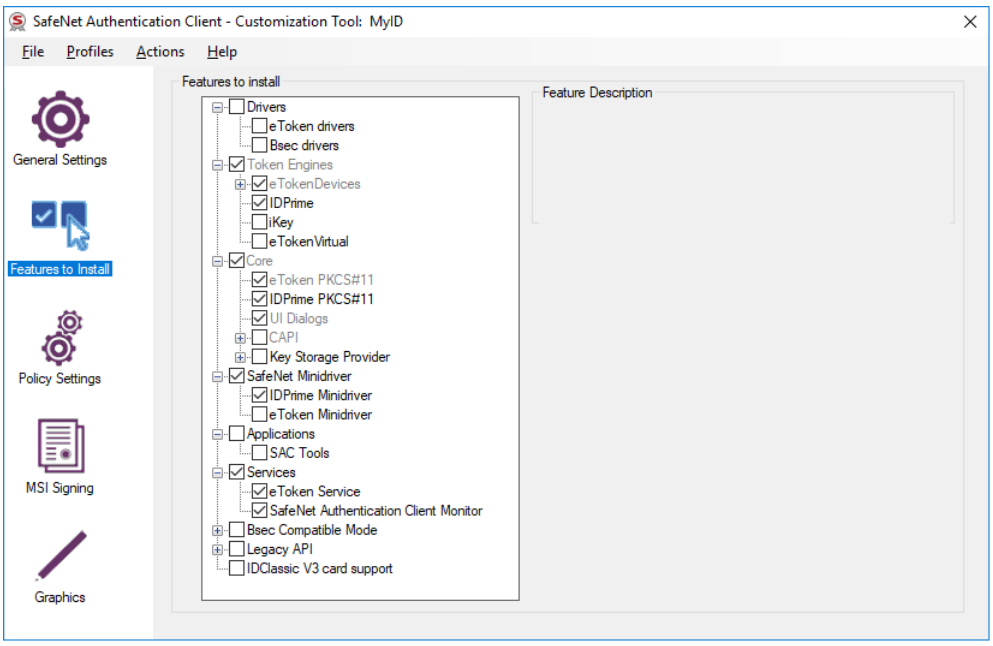
You must configure SafeNet Authentication Client (SAC) 10.8 R2 separately for Minidriver and SafeNet eToken support.

You can configure the SAC 10.8 R2 middleware using the SAC Customization Package, obtained from Thales.

For eToken devices, use the following settings:



For minidriver-based devices, use the following settings:



See also section *2.4, Minidriver-based smart cards*.

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

  SafeNet Authentication Client (when configured to support SafeNet eToken devices) may detect IDPrime 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 smart card – avoid using both card types at the same time with MyID.

7.4.2 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.

7.4.3 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.

7.4.4 Initialization keys for eToken 51xx

Initialization of SafeNet eToken 5100, 5110, 5110 FIPS and 5110+ credentials is protected using an initialization key. Unless the customer has requested a diversified factory initialization key, the tokens are shipped from the factory with a default key, which is already configured in MyID.

To secure the tokens after issuance, use the **Key Manager** workflow to configure a customer initialization key:

1. From the **Configuration** category, select the **Key Manager** workflow.
2. From the **Select Key Type to Manage** drop-down list, select **Initialization Key**.
3. Click **Next**.
4. Click **Add New Key**.
5. Set the following values:
   - **Credential Type**: Aladdin eToken
   - **Key Type**: Customer
   - **Encryption Type**: 2DES

   You can configure the rest of the values as required.
6. Click **Save**.

If the tokens were ordered with a diversified Factory key, use the same procedure, except for the **Key Type**, select Factory instead of Customer.

7.4.5 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.

7.4.6 Credential profiles for SafeNet Authentication Client smart cards

You must make sure that you have set the credential profile to use the same settings as the SafeNet Authentication 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.

7.4.7 Issuing smart cards that have PIV applets

For information on issuing smart cards that have PIV applets using a non-PIV MyID system, see section *2.12*, *Issuing smart cards that have PIV applets*.

7.5 Interoperability for Thales authentication devices

This section contains information about any considerations for using these smart card with other systems.

7.5.1 Unlocking PIV cards

PIV cards include a PIV applet, which means that you can use the MyID Card Utility to carry out a remote challenge/response unlock operation and change the user PIN, and the unlock credential provider to unlock the devices from the Windows logon screen.

See section *2.13*, *Unlocking smart cards that have a PIV applet*.

7.5.2 PIN policy settings

MyID allows you to set various policies for PINs using the settings in the credential profile. MyID enforces these settings for any operations carried out by MyID. For some smart cards, some or all of these settings are applied directly to the card, which means that the settings will also be enforced by third-party tools and utilities.

The following settings are supported for on-card PIN policy settings:

	Smart card	
PIN Setting	**SafeNet eToken 4100**	**SafeNet eToken 5100/5110/5110 FIPS/5110+**
Maximum PIN Length		
Minimum PIN Length	Y	Y
Repeated Characters Allowed		
Sequential Characters Allowed		
Logon Attempts	Y	Y
PIN Inactivity Timer	Y	Y
PIN History		Y
Lowercase PIN Characters		Y
Uppercase PIN Characters		Y
Numeric PIN Characters		Y
Symbol PIN Characters		Y
Lifetime		Y

- Y – Supported.
- blank – Not supported.

7.5.3 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**.

7.5.4 IDPrime MD840 Rev A and IDPrime MD3840 smart cards and signature only policies

IDPrime MD840 Rev A and IDPrime 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.

7.5.5 IDPrime PIV card status

IDPrime PIV v2.1 and v3.0 cards are delivered 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.

7.5.6 Available certificate slots on IDPrime MD cards

IDPrime MD cards are manufactured with a limited number of slots for each key type. It is important that you order cards that can accommodate the certificates you want to use.

For example, your smart cards may be manufactured with a profile that allows only two ECC keys; if you attempt to issue a credential profile that has three ECC certificates to the card, it will fail with an error similar to:

```
There has been an error generating a certificate request
Solutions:
Please contact your administrator.
Error Number: -2147220715
```

7.5.7 Additional identities and PIV cards

You cannot use the additional identities feature of MyID with any smart card that has a PIV applet. This includes the IDPrime PIV Card v2.0, IDPrime PIV Card v2.1, and IDPrime PIV Card v3.0.

7.5.8 Problems with Windows logon

If you have problems logging on to Windows, remove the Calais and SAC cache and then reboot.

The SAC cache is:

```
C:\Windows\temp\etoken.cache
```

The Calais cache is in the registry:

```
HKLM\Software\Microsoft\Cryptography\Calais\Cache
```

8 Thales Trusted Cyber Technologies smart cards

MyID has been tested with the following Thales Trusted Cyber Technologies smart cards:

Smart card	Type	Middleware
SafeNet SC650 V4.1	Smart card/Chip	SafeNet AT High Assurance Client V2.12.020
SC650 – CoolKey	Smart card/Chip	CoolKey applet v1.4

The CoolKey applet is currently supported on SafeNet SC650 V4.0 smart cards. Support for the CoolKey applet on these cards requires an additional software update. If you are using SC650 smart cards with the CoolKey applet, you cannot use SafeNet SC650 V4.1 smart cards as listed in the table above – the cards have the same identifier and cannot be distinguished within MyID. If you install the configuration update for CoolKey support, the cards are identified as "SC650 – CoolKey".

For information about acquiring the CoolKey update, contact customer support quoting reference SUP-323.

Note: Thales Trusted Cyber Technologies cards were previously known as SafeNet Assured Technologies smart cards.

8.1 Keys for Thales Trusted Cyber Technologies smart cards

This section provides information you need when setting up keys for Thales Trusted Cyber Technologies smart cards.

8.1.1 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
SC650 – CoolKey	SCP01

8.2 Platforms for Thales Trusted Cyber Technologies smart cards

These smart cards have been tested on:

	Operating System	
Smart card	Windows 8.1	Windows 10
SafeNet SC650 V4.1	Y	Y
SC650 – CoolKey	Y	Y

Key:

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

8.3 Supported features for Thales Trusted Cyber Technologies smart cards

See section *2.1*, *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 Thales Trusted Cyber Technologies smart cards.

	Features									
Smart card	**MyID**	**PIN**	**GP**	**Applet**	**RSA**	**ECC**	**PIV**	**OPACITY**	**Print**	**Client OS**
SafeNet SC650 V4.1	Y	P	Y		Y				Y	Y
SC650 – CoolKey	Y	P	Y		P				Y	Y

Key:

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

PIN management

The following Thales Trusted Cyber Technologies cards support a limited range of PIN management features:

	Smart card	
Feature	**SafeNet SC650 V4.1**	**SC650 – CoolKey**
Lock the PIN after issuance.	Y	Y
Identify when the PIN is locked.	Y	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	Y
Configure on-card PIN policy.		

Key:

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

PKI – RSA

The following Thales smart card supports a limited range of PKI – RSA features:

	Smart card
Feature	**SC650 – CoolKey**
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 for Thales Trusted Cyber Technologies smart cards

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 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.

8.4.2 CoolKey configuration

Information about configuring MyID to issue CoolKey cards is included in the document supplement provided with the additional software update that is required for support for the CoolKey applet on these cards.

For information about acquiring this update, contact customer support quoting reference SUP-323.

8.5 Interoperability for Thales Trusted Cyber Technologies smart cards

This section contains information about any considerations for using these smart card with other systems.

8.5.1 Omnikey card reader drivers for SC650 cards

When using an Omnikey smart card reader for SC650 cards, you must use the HID X-CHIP driver, and *not* the HID CCID driver. You are recommended to use the following driver:

- HID® OMNIKEY® X-CHIP WINDOWS BU & RU DRIVER V.1.2.29.156 (X64 AND X86)

This driver is available from the drivers page of the HID Global website.

8.5.2 CoolKey applets

You can issue SC650 V4.0 smart cards that have the CoolKey applet. These smart cards are displayed within MyID with a device type of "SC650 – CoolKey".

Support for the CoolKey applet on these cards requires an additional software update – for information about acquiring this update, contact customer support quoting reference SUP-323.

Note: You may experience problems if you attempt to use GemPC Twin smart card readers with smart cards that have the CoolKey applet loaded. You are recommended to use a different card reader.

8.5.3 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 SC650 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
```

8.5.4 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.

8.5.5 Card issuance error if using a single card reader

If you have logged on to MyID using an SC650 operator card on a PC with a single smart card reader, and attempt to issue another smart card, an error may occur when signing the certificates to be written to the card.

This error does not occur if you have two smart card readers – one for the operator card, and the other for the card you are issuing.

8.5.6 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.

8.5.7 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.

9 TicTok smart cards

MyID has been tested with the following TicTok smart cards:

Smart card	Type	Middleware
TicTok v1.1	Smart card	IDProtect Minidriver 7.18.02 (lasermd.dll v7.1.7.0)
TicTok v2.0	Smart card	IDProtect Minidriver 7.18.02 (lasermd.dll v7.1.7.0)
TicTok v3.0	Smart card	IDProtect Minidriver 7.18.02 (ciamd.dll v7.1.8.0)

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.

9.1 Platforms for TicTok smart cards

These smart cards have been tested on:

	Operating System	
Smart card	Windows 8.1	Windows 10
TicTok v1.1	Y	Y
TicTok v2.0	Y	Y
TicTok v3.0	Y	Y

Key:

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

9.2 Supported features for TicTok smart cards

See section *2.1*, *Supported features* for a description of the features supported by smart cards.

9.2.1 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	GP	Applet	RSA	ECC	PIV	OPACITY	Print	Client OS
TicTok v1.1	Y	P			Y				Y	Y
TicTok v2.0	Y	P			Y	P			Y	Y
TicTok v3.0	Y	P			Y	P			Y	Y

Key:

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

PIN management

The following TicTok cards support a limited range of PIN management features:

	Smart card	
Feature	**TicTok v1.1**	**TicTok v2.0**
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
Configure on-card PIN policy.	P	P

	Smart card
Feature	**TicTok v3.0**
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.	Y
Reset the PIN at cancellation.	Y
Configure on-card PIN policy.	P

Key:

- Y – Fully supported.
- P – Partially supported. For details of supported on-card PIN policy features, see section *9.4.1, PIN policy settings*.
- blank – Not supported.

PKI – ECC

The following TicTok smart cards support a limited range of PKI – ECC features:

	Smart card	
Feature	**TicTok v2.0**	**TicTok v3.0**
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

	Smart card	
Feature	**TicTok v2.0**	**TicTok v3.0**
ECC NIST P521 Curve	Y	Y
Remove certificates.	Y	Y
Archive certificates.		
Enumerate certificates on the card.	Y	Y

Key:

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

9.3 Installation and configuration for TicTok smart cards

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.

9.3.1 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 *2.4, Minidriver-based smart cards*.

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

9.3.2 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.

9.3.3 Support for TicTok v1.1 cards

You must edit the registry on each client on which you want to issue TicTok v1.1 cards to allow them to support the secure messaging keys.

In the following locations:

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

and:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Athena Smartcard Solutions\IDProtect Client
```

set the following:

```
aseSMFormatType = 0
```

9.3.4 Support for TicTok v3.0 cards

To support TicTok v3.0 cards, you must update the registry on each client on which you want to issue these cards to add the ATR (Answer to Reset) values for TicTok v3.0 smart cards. Contact your card vendor for more information.

9.4 Interoperability for TicTok smart cards

This section contains information about any considerations for using these smart card with other systems.

9.4.1 PIN policy settings

MyID allows you to set various policies for PINs using the settings in the credential profile. MyID enforces these settings for any operations carried out by MyID. For some smart cards, some or all of these settings are applied directly to the card, which means that the settings will also be enforced by third-party tools and utilities.

The following settings are supported for on-card PIN policy settings:

	Smart card
PIN Setting	**TicTok v1.1/v2.0/v3.0**
Maximum PIN Length	Y
Minimum PIN Length	Y
Repeated Characters Allowed	
Sequential Characters Allowed	
Logon Attempts	Y
PIN Inactivity Timer	Y
PIN History	Y
Lowercase PIN Characters	Y (optional or mandatory)
Uppercase PIN Characters	Y (optional or mandatory)
Numeric PIN Characters	Y (optional or mandatory)
Symbol PIN Characters	Y (optional or mandatory)
Lifetime	Y

- Y – Supported.
- blank – Not supported.

Note: There is currently an issue with the minidriver where you can still set a PIN without symbol characters even if you specify symbol PIN characters as mandatory.

9.4.2 Known issues

- **Issues with smart card detection**

  Intercede has seen issues with the IDProtect Client software 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 smart cards

MyID has been tested with the following Yubico smart cards:

Smart card	Type	Middleware
YubiKey 4	Smart card/USB	n/a
YubiKey 5	Smart card/USB	n/a
YubiKey FIPS	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; see the *Remote PIN Management utility for PIV cards* section in the ***Operator's Guide*** for details.

Note: MyID does not require middleware or a minidriver to work with Yubico smart cards. However, if you want to use your Yubico smart card with other applications, (for example, certificates for Windows logon) you may need to install a minidriver such as the Windows Inbox Smart Card Minidriver. For more information, see section *10.5.2*, *Minidrivers*.

10.1 Yubico form factors

Yubico devices are available in a variety of form factors. MyID groups these individual devices and treats them as the same credential type – this means that the same level of functionality is applied by MyID when issuing, personalizing, or managing the smart card.

Form Factor	Credential Type in MyID
YubiKey 4	YubiKey 4
YubiKey 4C	YubiKey 4
YubiKey 4 Nano	YubiKey 4
YubiKey 4C Nano	YubiKey 4
YubiKey 5 NFC	YubiKey 5
YubiKey 5 Nano	YubiKey 5
YubiKey 5C	YubiKey 5
YubiKey 5Ci	YubiKey 5
YubiKey 5C Nano	YubiKey 5
YubiKey FIPS	YubiKey FIPS
YubiKey Nano FIPS	YubiKey FIPS
YubiKey C FIPS	YubiKey FIPS
YubiKey C Nano FIPS	YubiKey FIPS

Note: MyID does not currently modify or work with the NFC element of Yubico devices.

10.2 Keys for Yubico smart cards

This section provides information you need when setting up keys for Yubico cards.

10.2.1 Cryptographic keys for Yubico cards

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

	YubiKey 4	YubiKey 5	YubiKey FIPS
Credential Type in MyID	YubiKey 4	YubiKey 5	YubiKey FIPS
GlobalPlatform Secure Channel	n/a	n/a	n/a
Factory GlobalPlatform Key Type	n/a	n/a	n/a
Factory GlobalPlatform Key Diversification Algorithm	n/a	n/a	n/a
Factory PIV 9B Key Encryption Type	3DES	3DES	3DES
PIV 9B Factory Key Diversity	Static	Static	Static
Recommended PIV 9B Customer Key Diversity	Diverse2	Diverse2	Diverse2

10.3 Platforms for Yubico smart cards

These smart cards have been tested on:

	Operating System	
Smart card	Windows 8.1	Windows 10
YubiKey 4	Y	Y
YubiKey 5	Y	Y
YubiKey FIPS	Y	Y

Key:

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

10.4 Supported features for Yubico smart cards

See section *2.1*, *Supported features* for a description of the features supported by smart cards.

10.4.1 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	GP	Applet	RSA	ECC	PIV	OPACITY	Print	Client OS
YubiKey 4	Y	P			P	P				Y
YubiKey 5	Y	P			P	P				Y
YubiKey FIPS	Y	P			P	P				Y

Key:

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

PIN management

The following Yubico cards support a limited range of PIN management features:

	Smart card	
Feature	**YubiKey 4**	**YubiKey 5**
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
Configure on-card PIN policy.	P	P

	Smart card
Feature	**YubiKey FIPS**
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.	Y
Reset the PIN at cancellation.	Y
Configure on-card PIN policy.	P

Key:

- Y – Fully supported.
- blank – Not supported.
- P – Partially supported. For details of supported on-card PIN policy features, see section *10.6.2, PIN policy settings*.

PKI – RSA

The following Yubico smart cards support a limited range of PKI – RSA features:

	Smart card		
Feature	**YubiKey 4**	**YubiKey 5**	**YubiKey FIPS**
Generate a private key for a certificate request.	Y	Y	Y
Write a certificate to the smart card.	Y	Y	Y
Cryptographically sign or encrypt data.	Y	Y	Y
Specify the default certificate for Windows logon.	Y	Y	Y
Write 1024 bit certificates.	Y	Y	

	Smart card		
Feature	**YubiKey 4**	**YubiKey 5**	**YubiKey FIPS**
Write 2048 bit certificates.	Y	Y	Y
Remove certificates.	Y	Y	Y
Inject a private key for certificate recovery.	Y	Y	Y
Enumerate certificates on the card.			

Key:

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

PKI – ECC

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

	Smart card		
Feature	**YubiKey 4**	**YubiKey 5**	**YubiKey FIPS**
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
Archive certificates.			
Enumerate certificates on the card.			

Key:

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

10.5 Installation and configuration for Yubico smart cards

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.

10.5.1 Yubico management key

You must configure MyID to use the management key for your Yubico smart cards. In MyID, this key is known as the PIV 9B key. To configure this key, you must use the **Key Manager** workflow within MyID to add a factory **PIV 9B Card Administration Key** to the system.

10.5.2 Minidrivers

Yubico provide a Windows minidriver that can enable extended usage of certificates on the smart card, beyond the capabilities provided by the Windows Inbox Smart Card Minidriver. To use YubiKey devices with the minidriver, the minimum version of the minidriver is v4.1.0.172; additionally, you must issue the devices with a *customer* PIV 9B key.

10.5.3 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 one of the following from the **Card Format** drop-down list:

- `CivCertificatesOnly.xml` – This card format is used by MyID to personalize the PIV applet and set the default values on elements required by the smart card's PIV applet.
- `Yubikey.xml` – This card format contains the PIV applet settings from `CivCertificatesOnly.xml`, and also sets up on-device PIN policy settings. See section *10.6.2, PIN policy settings* for details.
- `YubikeyNoOTP.xml` – This card format is the same as `Yubikey.xml`, but disables the Touch OTP feature. See section *10.6.2, PIN policy settings* for details.

This card format is used by MyID to personalize the PIV applet and set the default values on elements required by the smart card's PIV applet.

10.5.4 Issuing smart cards that have PIV applets

For information on issuing smart cards that have PIV applets using a non-PIV MyID system, see section *2.12, Issuing smart cards that have PIV applets*.

10.6 Interoperability for Yubico smart cards

This section contains information about any considerations for using these smart card with other systems.

10.6.1 Unlocking YubiKey tokens

YubiKey tokens include a PIV applet, which means that you can use the MyID Card Utility to carry out a remote challenge/response unlock operation and change the user PIN, and the unlock credential provider to unlock the devices from the Windows logon screen.

See section *2.13, Unlocking smart cards that have a PIV applet*.

10.6.2 PIN policy settings

MyID allows you to set various policies for PINs using the settings in the credential profile. MyID enforces these settings for any operations carried out by MyID. For some smart cards, some or all of these settings are applied directly to the card, which means that the settings will also be enforced by third-party tools and utilities.

The following settings are supported for on-card PIN policy settings:

	Smart card		
PIN Setting	**YubiKey 4**	**YubiKey 5**	**YubiKey FIPS**
Maximum PIN Length			
Minimum PIN Length			
Repeated Characters Allowed			
Sequential Characters Allowed			
Logon Attempts	Y	Y	Y
PIN Inactivity Timer			

	Smart card		
PIN Setting	**YubiKey 4**	**YubiKey 5**	**YubiKey FIPS**
PIN History			
Lowercase PIN Characters			
Uppercase PIN Characters			
Numeric PIN Characters			
Symbol PIN Characters			
Lifetime			

- Y – Supported.
- blank – Not supported.

MyID also supports the following YubiKey-specific settings by creating a customized card data model file:

- PUK Retries
- Per Container PIN Policy
- Per Container Touch-to-Sign Policy
- Touch OTP

The following settings are supported:

	Smart card		
PIN Setting	**YubiKey 4**	**YubiKey 5**	**YubiKey FIPS**
PUK Retries	Y	Y	Y
Per Container PIN Policy	Y	Y	Cannot set to "never"
Per Container Touch-to-Sign Policy	Y	Y	Y
Touch OTP	Y	Always on; cannot configure.	Y

You can configure the on-device settings by editing the card format file; these settings are applied when you issue, reprovision, or update the YubiKey token.

The `Yubikey.xml` card format file is located on the MyID application server in the following default folder:

```
C:\Program Files (x86)\Intercede\MyID\Components\CardServer\CardFormats\
```

Important: Do not edit the base `Yubikey.xml` file, as it may be overwritten by subsequent MyID updates or upgrades – instead, make a copy of the file in the same folder and give it a name that you can use to identify its purpose; for example, if you create a file to change the number of PUK retries to 5, you may want to name the copied file `Yubikey_5_PUK_retries.xml`.

To select the card format file, in the **Credential Profiles** workflow, in the **Device Profiles** section, from the **Card Format** drop down list select the copy of the `Yubikey.xml` file you created; for example, **Yubikey_5_PUK_retries.xml**.

You can configure the YubiKey on-device settings as follows:

- PUK Retries

  In the data model file, set the `CardDataModel/PukRetries` node to the number of retries.

  The default is 10.

- Per Container PIN Policy

  In the data model file, set the `Container/PinPolicy` node to one of the following:

  - `01` – never
  - `02` – once (default, except for Digital Sign Container)
  - `03` – always (default for Digital Sign Container)

  Important: Do not set the Per Container PIN Policy for the authentication container to `03` (always) – this causes problems when collecting updates. Any signing operation fails if the card is already in an authenticated state, which can occur as a result of authenticating with MyID or Windows. If this occurs, you can collect the updates through the Self-Service App by reinserting the token and retrying the update. However, to prevent this problem from occurring, you are recommended to leave this option at `02` (once) for the authentication container.

- Per Container Touch-to-Sign Policy

  In the data model file, set the `Container/TouchPolicy` node to one of the following:

  - `01` – never (default)
  - `02` – always
  - `03` – cached

  Note: If you set the Per Container Touch-to-Sign Policy to a value other than `01` (never) there is no on-screen indication when you need to touch the token to proceed; when the token displays a slow steady flashing light, touch the token. If you set this option to always, you must touch the token for each certificate operation; if you set this option to cached, the token caches the authentication for approximately 15 seconds.

- Touch OTP

  You can enable or disable the Touch OTP feature of Yubico devices at issuance (including reprovision) or as a post-issuance device update.

  In the data model file, set the `CardDataModel/OTP` node to one of the following:

  - `<OTP>` – if this node is not present, the Touch OTP feature is enabled on issuance or update (according to existing behavior).
  - `<OTP>0</OTP>` – the Touch OTP feature is disabled on issuance or update.
  - `<OTP>1</OTP>` – the Touch OTP feature is enabled on issuance or update.

  The `Yubikey.xml` data model file does not contain the OTP node, which means that the touch OTP feature is enabled by default. An additional card data model, `YubikeyNoOTP.xml`, is provided that has the Touch OTP feature disabled, with the OTP node set to 0.

Warning: Do not amend any other parts of the card format file. Incorrect configuration may lead to failure to issue a token.

Updating existing YubiKey tokens

You can update existing issued YubiKey tokens to use the on-device settings; you can request a card update through MyID, or you can use the Lifecycle API.

When deciding whether to update your existing YubiKey tokens, consider the following:

- If you *update* the YubiKey token, MyID determines whether any additional certificates need to be added; revoked certificates replaced, and so on; these may require certificates to be added or removed. For any new certificates written to the device, the container that protects the certificate keys will be set to use the Per Container PIN Policy and Per Container Touch-to-Sign Policy as configured in the card format file. No other certificates, and no other on-device policies are affected. The user does not need to set a new PIN for their token.
- If you *reprovision* the YubiKey token, all content is rewritten to the device, including all certificates, and all on-device settings as configured in the card format file are applied to the device. The user must set a new PIN for their token.

To update an existing YubiKey:

1. Use the **Request Card Update** workflow to request an update.

   For more details about using this workflow and how it affects your credentials, see the *Requesting a card update* section in the ***Operator's Guide***.
2. Select one of the following options:
   - **Request a resync of the card to the same version of the current profile** – select this option if you have made no changes to the credential profile used to issue the token.
   - **Request an upgrade of the card to the latest version of the current profile** – select this option if you have made changes to the credential profile used to issue the token.
   - **Request an upgrade of the card to the latest version of the following profile** – select this option if you have created a new credential profile to use for the on-device PIN policy settings.
3. Select the appropriate reason.
   - To carry out a reprovision, replacing all of the certificates on the token, select the **There is a problem with the device** reason.
   - To carry out an update, which affects only the Per Container PIN Policy or Per Container Touch-to-Sign Policy, and only for certificates that are required to be added because of the update, select the **New certificates need to be added to the device** reason.
4. Collect the update using the Self-Service App.

For systems with a large user population, you may prefer to create update requests using the Lifecycle API. The relevant section of the submission for generating a card update request is shown below.

For carrying out a full reprovision using the CMSCardRequest schema:

```
<Card>
 <CardProfile>Yubikey NoOTP</CardProfile>
 <CardRequestedBy>System</CardRequestedBy>
 <OriginalSerialNumber>8115516</OriginalSerialNumber>
 <OriginalDeviceType>YubiKey 4</OriginalDeviceType>
 <StatusMapping>84</StatusMapping>
 <Reprovision>1</Reprovision>
</Card>
```

For carrying out an update:

```
<Card>
 <CardProfile>Yubikey NoOTP</CardProfile>
 <CardRequestedBy>System</CardRequestedBy>
 <Update>
  <OriginalSerialNumber>8115516</OriginalSerialNumber>
  <OriginalDeviceType>YubiKey 4</OriginalDeviceType>
  <StatusMapping>86</StatusMapping>
 </Update>
</Card>
```

Replace the values of the nodes in the example above with values corresponding to the user population in your system.

For more information on the Lifecycle API, see the ***Lifecycle API*** document.

Using YubiKey tokens for Windows logon

If you want to use your YubiKey tokens for Windows logon, you must set the Per Container Touch-to-Sign Policy to `03` (cached) and Per Contain PIN Policy to `02` (once).

10.6.3 Unsupported functionality

MyID supports the "Smart Card (PIV-Compatible)" interface for Yubico devices. MyID does not enable or modify the following Yubico features:

- HFC
- FIDO2
- FIDO U2F
- OATH
- OpenPGP
- NFC
- PIV Attestation

10.6.4 Unlocking

MyID typically sets a randomized personal unlocking key (PUK) when it issues a Yubico smart card. This PUK is not available to any system other than MyID. If you want to unlock a Yubico smart card, you must use MyID (for example, the Self-Service App, MyID Desktop, or the MyID Card Utility).

For information on the MyID Card Utility, see the *Remote PIN Management utility for PIV cards* section in the ***Operator's Guide***.

10.6.5 PIN attempts

The number of attempts to enter a PIN for a Yubico device is set by the manufacturer, but MyID can override this using the **Logon Attempts** option on the credential profile.

10.6.6 PIN characters

The SP800-73 PIV specification requires that PIV cards use numeric-only PINs; however, although YubiKey tokens use PIV technology, it is possible to configure MyID to use non-numeric PIN characters for YubiKey tokens. YubiKey tokens support numeric, upper case, lower case, and symbol characters.

10.6.7 PIN length

YubiKey devices have fixed minimum and maximum PIN lengths of 6 and 8 characters respectively. Make sure you set up the credential profile to have a **Minimum PIN Length** of 6 and a **Maximum PIN Length** of 8.

10.6.8 Additional identities and PIV cards

You cannot use the additional identities feature of MyID with any smart card that has a PIV applet. This includes all YubiKey tokens.

10.6.9 Identification of YubiKey 4 and YubiKey FIPS

YubiKey 4 and YubiKey FIPS devices share an ATR value, and can be differentiated only by their firmware version.

If a YubiKey device has the following ATR:

- `3BF81300008131FE15597562696B657934D4`

MyID identifies the device based on the firmware as follows:

- the device has firmware version 4.4.*x* – YubiKey FIPS.
- the device has any other firmware – YubiKey 4.

10.6.10 Displaying YubiKey firmware versions

The **Identify Card** workflow displays the firmware version of your YubiKey devices in the **Device Version** field.

This value is stored in the MyID database at the point of device personalization from MyID 11.5 onwards – this means that you cannot view the firmware version of YubiKey devices that were issued in previous versions of MyID.

10.6.11 Updating YubiKey devices with incorrect 9B keys

If you are attempting to use MyID Desktop to update a YubiKey device using the **Collect My Updates** workflow, but the 9B key is incorrect (which may be caused by an issue with earlier versions of the Yubico minidriver, prior to v4.0.4, setting the factory 9B key to a value not known to MyID) you are automatically directed to the **Reprovision My Card** workflow instead, which recovers your card into a usable state. This process is seamless; note, however, that you must have a role that has access to both the **Collect My Updates** and **Reprovision My Card** workflows.