MyID

Version 10.8 Update 2

PIV Release Notes

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

Document reference: PHF1756-12

March 2018

Copyright

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

Licenses and Trademarks

Conventions Used in this Document

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

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

  For example:

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

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

  For example:

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

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

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

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

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

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

  For example:

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

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

  For example:

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

Contents

1 Introduction 6

1.1 Changes to the MyID application 6

1.2 More information 6

1.3 Prerequisites and installation 6

2 New and Updated Features 7

2.1 Updates to supported biometric devices 7

2.1.1 Aware PreFace v6 7

2.1.2 Crossmatch U.are.U 5300 fingerprint reader 7

2.1.3 SecuGen Hamster Pro Duo SC/PIV fingerprint reader 7

2.1.4 Cross Match Verifier 300/310 fingerprint reader 7

2.2 List of hair colors 8

2.3 Updated import schemas for Lifecycle API 8

3 Previously in MyID 10.8 Update 1 9

3.1 Enhanced derived credentials 9

3.1.1 Requisite User Data options 9

3.2 Mobile Device Management (MDM) System Integration 9

3.3 FASC-N uniqueness check for PIV-I 10

4 Previously in MyID 10.8 11

4.1 Change to fingerprint verification 11

4.2 Support for HSM key ceremony for diverse factory PIV 9B keys on PIV cards 11

4.3 Supported Oberthur PIV Card specifications 11

4.4 Supported Gemalto PIV Card specifications 11

4.5 Safenet Assured Technologies Luna SA for Government 12

5 Previously in MyID 10.7 13

5.1 PIV enrollment 13

5.2 Support for CNG signing certificates 13

6 Previously in MyID 10.6 14

6.1 Oberthur v8 PIV cards 14

6.2 PIV Derived Credentials for mobile devices 14

7 Previously in MyID 10.5 15

7.1 Faster PIV card issuance 15

8 Previously in MyID 10.4 16

9 Previously in MyID 10.3 17

9.1 Editing PIV applicants 17

9.2 PIV-D listener 17

10 Previously in MyID 10.2 18

10.1 Support for derived credentials 18

11 Previously in MyID 10.1 19

11.1 Support for FIPS 201-2 19

11.2 New PIV support module 19

11.3 PIV Derived Credentials 19

11.4 Database storage for images and files. 20

11.5 Data model change 20

11.6 Card issuance checks 20

11.7 Identity document lists 20

11.8 Authenticating people 20

11.9 Iris biometrics 20

11.10 Time period for card renewal requests 21
11.11 Card layouts 21
11.12 Biometric option name changes 21
11.13 PIV enrollment processes 22

12 Known Issues 23

1 Introduction

This document describes changes made to MyID® PIV. This edition of MyID contains features that provide support for FIPS 201-2 and derived credentials for PIV.

It allows issuance of smart cards for PIV, PIV-I, and CIV, in addition to a range of other credentials, including virtual smart cards, device identity certificates, and mobile identities.

1.1 Changes to the MyID application

This document provides information on the following:

- New and updated features
- Known issues

1.2 More information

See the ***Release Notes*** for details of the features of this release that are not specific to PIV installations.

1.3 Prerequisites and installation

For prerequisites and installation instructions, see the ***Installation and Configuration Guide***.

2 New and Updated Features

2.1 Updates to supported biometric devices

2.1.1 Aware PreFace v6

Support for facial biometric enrollment has been enhanced to provide a new, cleaner user interface for Aware Preface. You can use the updated user interface to capture a user photograph from a connected Canon EOS camera, or an image file, and obtain a facial biometric that complies with FIPS-201 requirements.

This replaces the previous integration with Aware Preface v5.9 that used an ActiveX control to provide the user interface.

The new user interface component is available for MyID Desktop, and requires the following additional software that are not part of the MyID release.

- MyID Image Capture – the updated photo capture user interface for Aware Preface.
- Canon EOS SDK – integration components for Canon EOS cameras.
- Aware Preface v6 (additional purchase required, unless upgrading from Aware Preface v5.9 that was purchased from Intercede).

All of these software modules are available on request from Intercede.

2.1.2 Crossmatch U.are.U 5300 fingerprint reader

The U.are.U 5300 is an optical fingerprint reader that you can use with MyID for fingerprint enrollment and verification.

See the ***U.are.U Integration Guide*** for further details.

2.1.3 SecuGen Hamster Pro Duo SC/PIV fingerprint reader

The SecuGen Hamster Pro Duo SC/PIV combines a smart card reader with an optical single fingerprint reader and is designed for use in PIV deployments. You can use this reader with MyID for fingerprint enrollment and verification.

You require SecuGen integration components, which are available on request from Intercede.

See the ***SecuGen Integration Guide*** for further details.

2.1.4 Cross Match Verifier 300/310 fingerprint reader

Earlier versions of MyID have provided support for Cross Match Verifier fingerprint readers. This reader has now reached end of sale by the manufacturer. Integration for these legacy devices has been re-introduced to MyID v10 to facilitate existing customers upgrading to the latest MyID product version.

Note: Support for this fingerprint reader is limited to Windows 7, and requires use of Cross Match SDK components that are supplied by the manufacturer.

See the ***Cross Match Integration Guide*** for further details.

2.2 List of hair colors

The list of hair colors available both in the **Edit PIV Applicant** workflow and the Lifecycle API has been updated to match the latest list provided by NIST. You can now specify the following additional hair colors:

- Blue
- Green
- Orange
- Pink
- Purple
- Streaked

The new values have been added to MyID; existing hair color values that are already set against users are not affected.

MyID PIV import schemas provided with MyID have been updated to support the new values. If you are using a customized version of the Lifecycle API schema, you must modify your import schemas to make use of the new colors.

See the ***Lifecycle API*** document for details of the codes for the new hair colors.

2.3 Updated import schemas for Lifecycle API

You can use the Lifecycle API to import user data to MyID, make requests for credentials, and to perform lifecycle management functions for credentials. This release includes updated core import schemas for MyID, including the following changes:

- Middle name field is extended to 50 characters.
- New `CardLayout` node.
- `SerialNumber` and `DeviceType` nodes for targeted issuance now available for PIV as well as CMS.
- Parameters for PIV and CMS schemas updated to be the same.
- New `ReplaceUnassignedCards` parameter.
- Updated list of hair colors in the PIV schema.

If you are using a customized import schema, you may need to make modifications to your current schema and configuration of the Lifecycle API to continue using it. Details of the amended schemas, and how to configure the API to use a customized schema are provided in the Lifecycle API document – you can find this in the APIs folder in the release.

The updated core schemas must be added separately to your installation. To install these, use the installer provided in the Custom Lifecycle Schema Enabler in the APIs folder of the MyID release.

3 Previously in MyID 10.8 Update 1

3.1 Enhanced derived credentials

This release of MyID incorporates several enhancements for issuing and managing Derived Credentials.

MyID has incorporated support for mobile derived credentials since version 10.3. This capability has been extended to:

- Support issuance of derived credentials to virtual smart cards on a computer, protected by a Trusted Platform Module or Intel Authenticate.
- Extract a User Principal Name from the PIV Authentication certificate and add it to a derived credential authentication certificate, enabling use for Windows logon.
- Provide better support for multi-valued DN formats on PIV Cards from other issuers.
- Allow derived credentials to be issued to cardholders that do not have an End Entity Signature certificate on their PIV card.
- Improve selection of a credential profile, to better guide the user through a choice of derived credentials for different device types.
- Validate required data is present on the PIV Card, to prevent issuance of an incompatible derived credential. For example, ensure presence of an Email address before a request for a derived credential that includes an email signing certificate.
- Provide the ability to send the one-time password for collection to an email address or display on screen at request.
- Allow one-time passwords to be provided in simple format (for easier readability) or complex format (for higher security).

Additional guidance is now provided to help with deployment choices to meet SP800-157 requirements. This can be found in the ***Derived Credentials SP800-157 Compliance Guidelines*** document.

For more detailed information on setting up MyID to issue derived credentials, see the ***Derived Credentials Installation and Configuration Guide***.

3.1.1 Requisite User Data options

If you select the **Requisite User Data** option on the **Issuance Processes** tab of the **Operation Settings** workflow, extra options appear in the **Credential Profiles** workflows that allow you to restrict the issuance of derived credentials on VSCs to users with the appropriate attributes; for example, if your VSC derived credential is to be used for email signing, you can restrict the credential profile to users who have the Email attribute mapped in their user account; similarly, for VSC derived credentials that are used for Windows logon, you can restrict the credential profile to users who have the UPN attribute mapped.

3.2 Mobile Device Management (MDM) System Integration

MyID has been capable of issue credentials (key and certificates) to mobile devices for a number of years. A key feature of MyID 10.8 Update 1 is out of the box integration with a range of market leading MDM vendors, including VMware AirWatch®, Citrix® XenMobile and MobileIron.

The integration allows MyID to write credentials into an MDM key store, enabling the MDM to use them for securing access to apps, data and services. The close integration, built in collaboration with each MDM vendor, allows credential issuance to be combined with device enrollment, providing a frictionless experience for end users.

For organizations wishing to comply with security standards such as FIPS 201-2 / (SP) 800-157, MyID enables credentials to be issued to mobile devices that are compliant with all of the required technical and business processes; in effect, derived credential enabling the MDM.

See the ***Mobile Identity Management Installation and Configuration Guide*** for details.

3.3 FASC-N uniqueness check for PIV-I

The FASC-N uniqueness check is relaxed for PIV-I credentials where the agency code is 9999.

4 Previously in MyID 10.8

4.1 Change to fingerprint verification

When validating fingerprints during card activation, earlier releases of MyID matched fingerprints that were written to the card during the card preparation stages. MyID now matches against fingerprints that are stored within the MyID database; that is, fingerprints that have been added using the MyID user interface or Lifecycle API. This better aligns MyID with the fingerprint verification requirements in NIST specification FIPS-201-2.

4.2 Support for HSM key ceremony for diverse factory PIV 9B keys on PIV cards

When PIV cards are manufactured, they are configured with a factory key to protect the PIV Applet.

MyID now supports importing a factory PIV 9B key to an HSM, using a Key Ceremony process. This is available when the factory PIV 9B key on each card is diversified from the value set at the factory.

For further details, see the ***Administration Guide***.

4.3 Supported Oberthur PIV Card specifications

For ID-One PIV (v2.3.2) cards, MyID supports the following Oberthur 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 ID-One PIV (v2.3.5) cards, MyID supports the following Oberthur specification:

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

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

4.4 Supported Gemalto PIV Card specifications

For Gemalto IDPrime PIV Card v2.0, MyID supports the following Gemalto specifications:

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

4.5 Safenet Assured Technologies Luna SA for Government

MyID now supports the SafeNet Assured Technologies Luna SA for Government configuration, and has been tested on the following system:

- A SafeNet Luna SA 5.4.7-3 running firmware version 6.21.2 or 6.10.9 using the v5.4.1 version of the SafeNet client software.

5 Previously in MyID 10.7

5.1 PIV enrollment

You can now use the **Edit PIV Applicant** workflow in MyID to edit the details of PIV applicants, including capturing fingerprints and scanning identity documents.

Note: If you want to use Aware PreFace to capture facial biometrics, contact customer support, quoting reference SUP-228.

You can also use the **Edit PIV Applicant** workflow to add new PIV applicants from a connected LDAP.

For more information, see the *Editing PIV applicants* section in the ***PIV Integration Guide***.

5.2 Support for CNG signing certificates

In previous versions of MyID, the signing certificate used for PIV had to be protected by CAPI (Cryptographic Service Provider). You can now use CNG (Key Storage Provider) as an alternative.

For more information, see the *Configure server signing certificates* section in the ***PIV Integration Guide***.

6 Previously in MyID 10.6

6.1 Oberthur v8 PIV cards

MyID now supports the latest generation of Oberthur's PIV card – ID-One PIV v2.3.5 on Cosmo V8 (APL #1354/1355).

For further details on supported card specifications, see the ***Smart Card Integration Guide***.

6.2 PIV Derived Credentials for mobile devices

Mobile Identity Management support is built into MyID 10.6. Previous versions of Mobile Identity Management required the installation of a separate module.

Support for Derived Credentials is now provided by a separate module. For more information, contact customer support, quoting reference SUP-217.

For more information, see the ***Release Notes***.

7 Previously in MyID 10.5

7.1 Faster PIV card issuance

You can now personalize PIV cards and securely lock the device in a single process, speeding up the PIV card activation process.

You can now use the 1-step encoding option set up a credential profile to pre-encode cards using the **Batch Issue Card** workflow; you do not need to carry out a separate **Batch Encode Card** step. The cardholder can then activate their card quickly without having to wait for certificates to be issued or the card to be printed.

The differences between the activation process with no pre-encode, 1-step pre-encode, and 2-step pre-encode is as follows:

None	1-Step	2-Step
Request card	Request card	Request card
Batch issue card	Batch issue card – card is encoded	Batch issue card
Activate card – card is encoded	Activate card	Batch encode card – card is encoded
		Activate card

For details of how this works within FIPS-201-2, see the ***PIV Integration Guide***.

8 Previously in MyID 10.4

There were no new PIV-specific features in MyID 10.4. For information on the general features and updates in this version of MyID, see the ***Release Notes***.

9 Previously in MyID 10.3

9.1 Editing PIV applicants

The **Edit PIV Applicant** workflow has now been extended to enable you to edit PIV attributes. Access to this feature is restricted by MyID role assignment to ensure that imported enrollment data is protected.

Note: This does not currently provide any FIPS-201 enrollment processing logic, or support biometric enrollment, document scanning or image capture.

See the ***PIV Integration Guide*** for details.

9.2 PIV-D listener

A notifications mechanism has been developed to provide a link between third party-issued PIV cards and MyID-issued PIV-derived credentials. This capability is critical to ensure MyID is notified of any changes to the PIV card so that the appropriate action can be taken by MyID to update or cancel the PIV-D credential issued to the mobile.

Any action executed by MyID is recorded for traceability in the audit trail.

The listener web service is provided in a separate software update.

See the ***Derived Credentials Notification Listener Application Interface*** document for details.

10 Previously in MyID 10.2

10.1 Support for derived credentials

This release of MyID provides enhanced support for derived credentials. You can now issue mobile credentials that have been derived from smart cards that were issued by systems other than the current MyID system.

Mobile identities require an additional software package.

See the ***Derived Credentials Installation and Configuration Guide*** in the MyID Mobile Identity Management release for details.

11 Previously in MyID 10.1

11.1 Support for FIPS 201-2

You must review your system configuration to ensure that you comply with FIPS 201-2.

Review your business processes in line with the requirements of FIPS 201-2. This document and the ***PIV Integration Guide*** provide general guidance, but you must also review the requirements set by NIST.

The *Using MyID for FIPS 201-2 Compliance* section of the ***PIV Integration Guide*** includes information on how MyID helps you meet the requirements of FIPS 201-2.

You must review your current system configuration, including:

- PIV signing certificates.

  See the *Configure server signing certificates* section in the ***PIV Integration Guide***.
- Certificate policy configuration.

  FIPS 201-2 requires that the UUID is included in the PIV Authentication and PIV Card Authentication certificate attributes.

  See your CA integration guide for details.
- Credential profile configuration.

  See the *Setting up the credential profile* section in the ***PIV Integration Guide***.
- Card layouts.

  MyID provides updated card layouts to support FIPS 201-2. You must update your credential profiles to use these layouts, or update your own layouts to meet the FIPS 201-2 requirements.

  See the *Setting up the credential profile* and *Updating existing card layouts* sections in the ***PIV Integration Guide***.
- Operation and security settings that affect new or amended operations in MyID.

  See the *Using MyID for PIV* section in the ***PIV Integration Guide***. This contains configuration details throughout the section.

11.2 New PIV support module

A major overhaul of PIV support in MyID to allow use of more core features in PIV installations.

This provides support for multiple user populations – MyID allows issuance of PIV, PIV-I, CIV and other credential types while maintaining distinct business processes and security features for FIPS 201 compliance.

11.3 PIV Derived Credentials

Recent changes in FIPS 201-2 mean that federal employees can now make use of derived credentials for mobile devices. This release allows issuance of certificates to mobile devices that are derived from trust in a PIV card. The new Self-Service Kiosk user interface allows users to interact with a simple mechanism to collect their derived PIV credentials onto their mobile device. See the ***Derived Credentials Installation and Configuration*** document for details.

Note: Additional updates are required to use this feature – contact Intercede quoting SUP-133 for further details.

11.4 Database storage for images and files.

Previously, all images (for example, user photographs and signatures), and files (for example, identity documents) were always stored as files on the MyID web server.

When you install MyID 10.1, the system is configured to store all of these files in the MyID database. This includes files imported through the Lifecycle API.

11.5 Data model change

The data models for PIV, which detail the structure of the data written to the cards, have been updated to comply with FIPS 201-2.

If you are upgrading from an earlier version of MyID and have your own custom data models, you must update them to remove the Authentication Key Map from the CHUID. For more information, contact customer support, quoting reference SUP-130.

11.6 Card issuance checks

For FIPS 201-2, you must configure MyID to prevent issuance when there are no facial biometrics captured, the PIV content signing certificate would expire during the lifetime of the card, or the biometric data will expire during the lifetime of the card.

MyID now provides configuration options that allow you to set these restrictions.

See the *Requiring facial biometrics* and *Card issuance checks* sections in the ***PIV Integration Guide***.

11.7 Identity document lists

The list of identity documents supported in MyID has been updated to match the FIPS 201-2 requirements.

11.8 Authenticating people

The authentication process has been updated in this release.

When an operator is carrying out a procedure on behalf of a cardholder, the operator must authenticate the cardholder's identity. The new workflow **Authenticate Person** allows you to carry out this authentication using a configurable set of authentication criteria, including biometric verification and identity documents. See the *Authenticating users* section of the ***PIV Integration Guide*** for details of using this workflow.

11.9 Iris biometrics

You can now import iris biometrics using the Lifecycle API and write them to the PIV applet on the card.

See the ***Lifecycle API*** document for details.

If you want to write iris biometrics to your cards, you must have the following:

- An appropriate version of the MyID Client Components. The version of the MyID Client Components provided with this release is suitable For information on other versions that are suitable, contact customer support, quoting reference SUP-135.
- PIV cards capable of storing iris biometrics. It is possible to order Oberthur or Gemalto PIV cards that do not have the iris container.

- A credential profile that uses one of the standard PIV card format files:
  - **PivDataModel.xml**
  - **PivDataModelCompressed.xml**
  - **CBPivDataModel.xml**

If you have variant Oberthur ID-One PIV or Gemalto PIV v2 cards that do *not* support iris biometrics, use an alternative data model, or MyID will attempt to write iris biometrics to non-existent iris containers; for example, use the following card formats:

- **PivDataModelNoIris.xml**
- **PivDataModelCompressedNoIris.xml**
- **CBPivDataModelNoIris.xml**

11.10 Time period for card renewal requests

You can now configure the length of time before expiry that you can request a card renewal using the **Request Replacement Card** workflow. For example, if the card has 60 days left before expiry, and you set the **Card Renewal Period** to 40, you cannot request a card renewal. If the card has 30 days left before expiry and you set the **Card Renewal Period** to 40, MyID allows you to request the card renewal.

See the *Card renewal period* section in the ***PIV Integration Guide***.

11.11 Card layouts

This release provides updated card layouts for FIPS 201-2:

- **PIV_CON_FIPS201_2** – a FIPS 201-2-compliant layout for contractors.
- **PIV_ERS_FIPS201_2** – a FIPS 201-2-compliant layout for emergency response officials.
- **PIV_FOR_FIPS201_2** – a FIPS 201-2-compliant layout for foreign nationals.
- **PIV_STD_FIPS201_2** – a FIPS 201-2-compliant layout for standard PIV cards.

Corresponding card back layouts are also provided.

These layouts provide improved name formatting and color coding for employee affiliation.

If you have your own layouts, you must update them to meet the requirements of FIPS 201-2. See the *Updating existing card layouts* section in the ***PIV Integration Guide***.

11.12 Biometric option name changes

The following configuration options in the **Operation Settings** workflow, relating to fingerprints, have new names:

- **Bypass biometric verification when no fingerprints enrolled?**

  Renamed to **Bypass fingerprint verification when no fingerprints enrolled?**
- **Use a Biometric reader during card creation**

  Renamed to **Verify fingerprints during card creation**.
- **Use a Biometric reader during card update**

  Renamed to **Verify fingerprints during card update**.
- **Use a Biometric reader during unlocking cards**

  Renamed to **Verify fingerprints during card unlock**.

The following option in the **Credential Profiles** workflow has been renamed:

- **Require Biometrics at Issuance**

  Renamed to **Require Fingerprints at Issuance**.

The names have been updated as these options refer only to fingerprint biometrics, not to facial biometrics or iris biometrics.

11.13 PIV enrollment processes

Previous releases of MyID provided a range of features that supported a FIPS 201-compliant enrollment process within MyID, including:

- PIV sponsorship through Active Directory.
- Biometric enrollment, including facial biometrics and fingerprint capture.
- Adjudication through the Office of Personnel Management.
- Enforced enrollment processes compliant with FIPS 201.

This release does not provide these features. To enroll users, you must import FIPS 201-2-compliant user data into MyID using the Lifecycle API. See the ***PIV Integration Guide*** and the ***Lifecycle API*** documents for details.

Future versions of MyID will contain more enrollment features.

12 Known Issues

- **IKB-44 – Cannot request credentials for LDAP users**

  MyID PIV requires certain attributes to be present for PIV card issuance. During request card, a warning message is displayed that certain attributes are missing from the user account if they are not present. If the user requires a PIV card, issuance will fail. If the request is for other credential types that do not use PIV applet personalization, the request can continue and issuance will succeed.