



**MyID**

**Version 10.8 Update 2**

# **Personal Identity Verification**

## **Integration Guide**

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK  
[www.intercede.com](http://www.intercede.com) | [info@intercede.com](mailto:info@intercede.com) | [@intercedemyid](https://twitter.com/intercedemyid) | +44 (0)1455 558111

## Copyright

© 2001-2018 Intercede Limited. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished exclusively under a restricted license or non-disclosure agreement. Copies of software supplied by Intercede Limited may not be used resold or disclosed to third parties or used for any commercial purpose without written authorization from Intercede Limited and will perpetually remain the property of Intercede Limited. They may not be transferred to any computer without both a service contract for the use of the software on that computer being in existence and written authorization from Intercede Limited.

The software or web site referred to in this manual may utilize or contain material that is © 1994-2000 DUNDAS SOFTWARE LTD., all rights reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Intercede Limited.

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**

The Intercede® and MyID® word marks and the MyID® logo are registered trademarks of Intercede in the UK, US and other countries.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such. All other trademarks acknowledged.

## 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

<b>Personal Identity Verification.....</b>	<b>1</b>
<b>1 Introduction.....</b>	<b>7</b>
1.1 Documentation.....	7
1.2 About PIV.....	8
1.2.1 FIPS 201.....	8
1.2.2 PIV smartcards .....	8
1.2.3 Non-Federal adoption of PIV cards.....	9
1.2.4 Derived Credentials .....	10
<b>2 Using MyID for FIPS 201-2 .....</b>	<b>11</b>
2.1 PIV identity proofing and registration .....	11
2.2 PIV card issuance.....	11
2.2.1 Cardholder authentication.....	12
2.3 PIV card reissuance.....	13
2.4 PIV card post-issuance update .....	13
2.4.1 Update the certificates on the card .....	14
2.4.2 Reprovision and reinstatement .....	14
2.4.3 Recover additional certificates onto the card .....	15
2.4.4 Certificate rekey (certificate renewal).....	16
2.5 PIV Card Verification Data Reset.....	16
2.5.1 Self-service PIN reset .....	16
2.5.2 Operator-led PIN reset.....	17
2.5.3 Biometric matching for PIN reset .....	17
2.5.4 Resetting other verification data .....	18
2.6 PIV Card Termination .....	18
2.6.1 Cancelling (revoking) a PIV card that is present .....	18
2.6.2 Remotely cancelling a PIV card that is not present.....	18
2.6.3 Erasing a PIV card that has been remotely cancelled .....	19
2.6.4 Notifications to other systems .....	19
2.6.5 Changing the disposal status of a card.....	19
<b>3 Configuring MyID.....</b>	<b>20</b>
3.1 Installing MyID Server software .....	20
3.1.1 Integrating MyID with other systems.....	20
3.2 Configuring MyID for FIPS 201-2 card issuance (PIV).....	21
3.3 Configuring MyID for non-Federal issuers (PIV-I, CIV) .....	23
3.3.1 PIV support levels.....	23
3.3.2 Issuing cards to the correct users.....	25
3.3.3 Maintaining multiple populations in a single system .....	25
3.3.4 Adding applicants .....	26
3.3.5 Operator permissions .....	26
3.3.6 Business rules .....	26
3.3.7 Authentication .....	27
3.3.8 Summary of requirements for PIV-I, and CIV.....	27
<b>4 After Installing MyID.....</b>	<b>28</b>
4.1 Controlling the content of subject alternative names .....	28
4.2 Configure server signing certificates.....	28
4.2.1 Troubleshooting the content signing certificate.....	30
4.3 Configuring the PIV server hash algorithm .....	30
4.4 Biometric identification .....	30
4.5 Setting up MyID when you have existing PIV cards.....	30
4.6 Controlling local and remote operations .....	32
<b>5 Using MyID for PIV .....</b>	<b>33</b>
5.1 PIV Card Application Administrator Key .....	33
5.1.1 Factory 9B keys .....	33
5.1.2 Customer 9B keys .....	34

5.2	GlobalPlatform keys for PIV cards .....	35
5.3	Specify which certificates to use .....	35
5.4	Setting up the credential profile .....	36
5.4.1	Updating existing card layouts .....	39
5.4.2	FASC-N values .....	40
5.5	Setting credential numbers .....	40
5.6	Manage agencies .....	41
5.6.1	Add agencies .....	41
5.6.2	Amend agencies .....	43
5.6.3	Remove agencies .....	43
5.6.4	Edit agencies .....	44
5.7	Batch issuing cards .....	46
5.8	Requiring facial biometrics .....	46
5.9	Card issuance checks .....	47
5.10	Displaying logon names .....	47
5.11	Preserving FASC-N and UUID .....	47
5.12	Approval of users on renewal and replacement .....	48
5.13	Card renewal period .....	48
5.14	Authenticating users .....	49
5.15	Editing PIV applicants .....	52
5.15.1	Editing PIV applicants .....	53
5.15.2	Adding PIV applicants from a directory .....	57
5.16	Remote PIN Management utility for PIV cards .....	58
<b>6</b>	<b>Card Layout and Printing .....</b>	<b>61</b>
6.1	Printers, cards and consumables .....	61
6.2	Card content and layout .....	61
6.2.1	General .....	61
6.3	Specific field data – front of card .....	62
6.3.1	Zone 1 – Photograph ( <b>GP.5 / CPS.11</b> ) .....	62
6.3.2	Zone 2 – Name ( <b>GP.6 / CPS.12</b> ) .....	62
6.3.3	Zone 8 – Employee Affiliation ( <b>GP.9 / CPS.15</b> ) .....	62
6.3.4	Zone 10 – Organizational Affiliation ( <b>GP.10 / CPS.16</b> ) .....	62
6.3.5	Zone 14 – Expiration date ( <b>GP.11 / CPS.17</b> ) .....	62
6.3.6	Zone 3 – Signature ( <b>GP.14 / CPS.20</b> ) .....	62
6.3.7	Zone 4 – Agency-specific text ( <b>GP.15 / CPS.21</b> ) .....	62
6.3.8	Zone 5 – Rank ( <b>GP.16 / CPS.22</b> ) .....	63
6.3.9	Zone 6 – 2D barcode ( <b>GP.17 / CPS.23</b> ) .....	63
6.3.10	Zone 9 – Header ( <b>GP.18, 19 / CPS.24, 25</b> ) .....	63
6.3.11	Zone 11 – Agency Seal ( <b>GP.20, 21 / CPS.26, 27</b> ) .....	63
6.3.12	Zone 12 – Footer ( <b>GP.22, 23 / CPS.28, 29</b> ) .....	63
6.3.13	Zone 13 – Issue Date ( <b>GP.24 / CPS.30</b> ) .....	63
6.3.14	Zone 15 – Background for Name ( <b>GP.25, 26, 27 / CPS.31, 32, 33</b> ) .....	63
6.3.15	Zone 16 – Photo Border ( <b>GP.29 / CPS.35</b> ) .....	64
6.3.16	Zone 17 – Agency Specific Data ( <b>GP.30 / CPS.36</b> ) .....	64
6.3.17	Zone 18 – Color Designator ( <b>SP800-104</b> ) .....	64
6.3.18	Zone 19 – Expiration Date (large) ( <b>SP800-104</b> ) ( <b>CPS.59, 60</b> ) .....	64
6.3.19	Zone 20 – Organizational Affiliation Abbreviation ( <b>SP800-104</b> ) ( <b>CPS.61, 62</b> ) .....	65
6.4	Specific field data – back of card .....	65
6.4.1	Zone 1 – Agency Card Serial Number ( <b>GP.12 / CPS.18</b> ) .....	65
6.4.2	Zone 2 – Issuer identification ( <b>GP.13 / CPS.19</b> ) .....	65
6.4.3	Zone 4 – Return To ( <b>GP.33 / CPS.39</b> ) .....	65
6.4.4	Zone 5 – Physical Characteristics ( <b>GP.34 / CPS.40</b> ) .....	65
6.4.5	Zone 6 – Additional Language ( <b>GP.35 / CPS.41</b> ) .....	65
6.4.6	Zone 7 – Section 499 Title 18 ( <b>GP.36 / CPS.42</b> ) .....	65
6.4.7	Zone 8 – Linear Barcode ( <b>GP.37, 38, 39 / CPS.43, 44, 45</b> ) .....	65
6.4.8	Zone 9 – Agency Specific Text ( <b>GP.40 / CPS.46</b> ) .....	65
<b>7</b>	<b>Standards Compliance .....</b>	<b>66</b>
7.1	Graphical Personalization .....	66
7.2	Electrical Personalization .....	67
7.2.1	CHUID .....	69

---

7.2.2	CBEFF .....	69
7.2.3	CCC .....	69
7.2.4	Certificate Containers .....	70
7.2.5	Printed Information .....	70
7.2.6	Card Holder Facial Image .....	71
7.2.7	Security Object .....	71
7.2.8	Key History .....	71
7.2.9	Discovery Object.....	71
7.2.10	Cardholder Iris Images .....	71
7.3	Key Management.....	72
7.4	Restrictions .....	72
7.5	Hashing Algorithm .....	72
<b>8</b>	<b>PIV Notifications .....</b>	<b>73</b>

# 1 Introduction

The United States government introduced the Personal Identity Verification (PIV) initiative in response to Homeland Security Presidential Directive 12 (HSPD-12), which called for establishing a single, government-wide standard for identification credentials issued by the United States government. Federal Information Processing Standard 201 (FIPS 201) defines a common identification standard for all federal employees and contractors. It incorporates the technical specification for data capture, details of the algorithms used to secure it, the background checks that must be made to ensure the identity of the individual and also the roles of the individuals within the process.

In 2013, a major revision of the FIPS 201 standard was released – FIPS 201-2. This document includes information about the changes made to MyID to support the revised standard.

This document describes how MyID supports FIPS 201 and describes additional configuration steps required to issue PIV cards that meet this standard. If you require further advice on using MyID to issue PIV cards for FIPS 201, contact Intercede.

## 1.1 Documentation

MyID is provided with a full set of documentation on the product CD.

- **Release Notes**

Make sure you read this document for a guide to new features in this version and a list of late-breaking issues that were not included in the other documents.

- **PIV Release Notes**

A list of what's new and other issues specifically relating to the PIV features of MyID.

- **Installation and Configuration Guide**

The Installation and Configuration Guide takes you through the steps necessary to install MyID and configure it for use.

- **PIV Integration Guide**

This document. The PIV Integration Guide contains procedures that are specific to PIV implementations.

**Note:** Read this integration guide before you start to install the software.

- **Integration Guides**

If you have been provided with additional documentation about the implementation of MyID 10.8 Update 2 in your own environment, please read those documents before you start to install the software.

For example, you must follow the instructions in the integration guide for the certificate authority you are using.

- **Administration Guide**

The Administration Guide provides information on using the administrative features of a MyID system. The guide is designed for a general-purpose MyID system, not a PIV system specifically, so some sections may not be directly relevant.

**Note:** Unless otherwise specified, all documents referred to are available from the MyID product CD.

## 1.2 About PIV

### 1.2.1 FIPS 201

In August 2004 the White House issued Homeland Security Presidential Directive 12 (HSPD-12), stating a need for a common identification standard for federal employees and contractors.

It further specified secure and reliable identification that:

- Is issued based on sound criteria for verifying an individual employee's identity
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Is issued only by providers whose reliability has been established by an official accreditation process.

In response to HSPD-12, the National Institute of Standards and Technology (NIST) produced Federal Information Processing Standards publication 201 (FIPS 201).

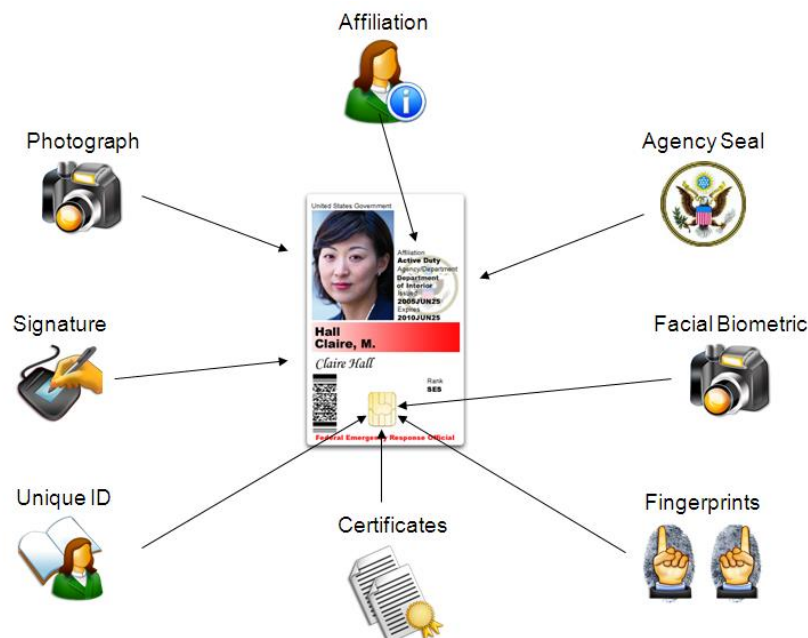
FIPS 201 specifies both the technical and process requirements a system must meet in order to issue a valid Personal Identity Verification (PIV) card.

FIPS 201 refers to various 'Special Publications' which detail specific elements of the overall solution; for example:

- SP 800-73 (card interface and data model)
- SP 800-76 (biometric specification)

### 1.2.2 PIV smartcards

PIV Smartcards are defined by the NIST standard SP 800-73. Each PIV card may contain the following data, which is gathered and verified during the Enrollment process.



There are four certificates expected on a PIV card, each in a named container on the card:

- PIV Authentication
- Digital Signature



- Key Management
- Card Authentication

Smart Cards used for FIPS 201 compliance must meet the technical requirements set by the SP800-73 standard. This standard defines the behavior of a Smart Card and also defines the data it can store.

MyID can support cards that comply with SP800-73-4, and can also personalize the following optional PIV containers on the card:

- Printed Information
- Discovery Object
- Key History Object
- 20 retired X.509 Certificates for Key Management (RSA keys only)
- Cardholder Iris Images (if iris data is imported to MyID)

One of the measures used to secure the smartcards is the PIV Card Application Administrator Key (sometimes referred to as key reference 9B). This key is shared between the smartcards and the smartcard management system, and prevents any unauthorized change to a card's contents

**Note:** All PIV cards (of the same device type) managed by a single installation of MyID must share the same 9B key.

### 1.2.3 Non-Federal adoption of PIV cards

#### **PIV Interoperable (PIV-I)**

The Personal Identity Verification (PIV) initiative is garnering a great deal of interest from parties external to the Federal government. These non-federal organizations want to issue identity cards that are technically interoperable with Federal government PIV systems, and issued in a manner that allows Federal government relying parties to trust the cards.

The Federal CIO Council has defined a set of minimum requirements that will enable trust of non-federally issued identity cards (PIV Interoperable, or PIV-I).

**Note:** Please refer to the document "Personal Identity Verification Interoperability For Non-Federal Issuers", issued by the Federal CIO Council for full details of the requirements of PIV-I.

Use of the standardized PIV Card technology in private enterprises (Commercial Identity Verification, or CIV) is becoming commonplace. They do not need to comply with the strict policy controls placed on PIV or PIV-I, but the cards and credentials issued do not provide any of the trust within Federal government.

MyID can support issuance of cards for PIV, PIV-I and CIV from within the same installation, whilst still complying with the strict issuance policies required for PIV and PIV-I.

Non Federal Issuers of PIV-Interoperable cards must undertake identity proofing of each applicant for an identity card, which incorporates In-person appearance and verification of two independent ID documents or accounts and a current biometric (e.g. photograph, fingerprints) in accordance with NIST SP 800-63, Assurance Level 4. The 'National Agency Check with Written Inquiries (NACI)' which is required prior to issuance of a PIV Card issuance by a Federal Agency, is not needed.

A PIV Interoperable identity card:

- Will use a smart card platform that is technically compatible with National Institute of Standards and Technology (NIST) technical requirements.
- Is visually distinguishable from PIV Card and contains distinctive markings indicating the identity of the issuing entity, including:
  - ♦ Organizational Affiliation (if exists; otherwise the issuer of the card)
  - ♦ Card holder Facial Image
  - ♦ Card holder Full Name
  - ♦ Card Expiration Date.
- Is electronically personalized, as defined by *Federal Bridge Certification Authority (FBCA) policy*, and will include:
  - ♦ Fingerprints
  - ♦ Card Holder Unique Identifier (CHUID) including the Universally Unique Identifier (UUID)
  - ♦ Authentication PKI Certificate (see note below), including the Universally Unique Identifier (UUID) in the subject-alt-name
  - ♦ Card Authentication PKI Certificate
  - ♦ Facial Image
  - ♦ Security Object
  - ♦ Card Capability Container.

**Note:** The PIV Authentication Certificate is where “trust” in the PIV Card resides. However, the policy object identifier (OID) for the PIV Authentication Certificate is available only to Federal government organizations. Therefore, a comparable Identity PKI Authentication Certificate that can be trusted by Federal government relying parties must be identified and used by NFIs. It must also be issued by a Certificate Authority (CA) that is cross-certified with the Federal Bridge Certification Authority (FBCA).

### Commercial Identity Verification (CIV)

A CIV card is effectively the same as a PIV Interoperable (PIV-I) card but does not require certificates that are issued by a CA cross-certified with the Federal Bridge Certification Authority (FBCA), or enrollment using an identity verification process that meets NIST SP 800-63, Assurance Level 4.

MyID can issue CIV cards with certificates only (therefore no personalization of the PIV applet within the card) or if required personalize the PIV applet – whilst all supported features of the PIV Applet are available, certain data elements such as the FASCN are *not* permitted to be used. See section [5.4, Setting up the credential profile](#) for details of configuring a credential profile in MyID to issue a CIV card.

## 1.2.4 Derived Credentials

FIPS 201-2 introduces the concept of *Derived Credentials* – issuance of certificates to another device belonging to a PIV card holder, based on the trust placed in the PIV card. This feature can be used to allow issuance of certificates to mobile devices such as a smart phone or tablet, or to virtual smart cards, that are associated to the PIV smart card. This includes defined authentication processes using the original smart card, and card revocation checks after issuance of the derived credentials.

You can issue credentials that have been derived from PIV smart cards that were issued by systems other than the current MyID system.

For more information, see the [Derived Credentials Installation and Configuration Guide](#).

## 2 Using MyID for FIPS 201-2

The key business processes that are covered by FIPS 201-2 are:

- PIV identity proofing and registration
- PIV card issuance
- PIV card reissuance
- PIV card post-issuance update
- PIV card verification data reset
- PIV card termination

These rules apply to PIV and PIV-I cards. They do not apply to CIV cards or other credential types.

### 2.1 PIV identity proofing and registration

This release of MyID provides an enrollment capability that can be used to gather data for use on a PIV, PIV-I or CIV card. You can create user records may be created in MyID, or import them from a directory or from an external system using the Lifecycle API.

You can enroll biometric data; for example, by capturing fingerprint or facial biometrics from connected devices, or importing Iris data using the Lifecycle API.

See the [Lifecycle API](#) document for details.

You must ensure any additional processes required for identity proofing and registration take place, in accordance with FIPS-201 guidelines where applicable, before marking the user record as *User Data Approved*.

See section [3.3.8, Summary of requirements for PIV-I, and CIV](#) for more information.

### 2.2 PIV card issuance

The card issuance process is as follows:

#### 1. Request

A card request is made in MyID to create a job for issuance. A credential profile is selected for use, and optionally an expiry date set.

The card request is made through the Lifecycle API.

If you already have an applicant enrolled, you can request a card for that user with the **Request Card** workflow.

#### 2. Approve

The card request is reviewed and either approved or rejected. The credential profile and expiry date is reviewed and if necessary amended.

To include a validation stage in the process, set the **Validate Issuance** option on the credential profile.

Use the MyID **Validate Request** workflow to approve the card request.

#### 3. Assign

The card to be issued is assigned to the user account, card security is configured (Administrator PINs and keys are set) and the card surface is printed.

Use the MyID **Collect Card** or **Batch Collect Card** workflows.

**Note:** Do not use the **Issue Card** workflow. This does not support the PIV card issuance process.

#### 4. Personalize

The electronic data within the applet is written, including the FASC-N, CHUID, Printed Information and Biometric data. Certificates are generated and written to the card.

If you want to personalize the card electronically (including certificate issuance) before the cardholder carries out the activation process, you can choose when this takes place in MyID. This is optional – if you do not personalize the card at this stage, the electronic personalization takes place during card activation.

Card personalization can take place at the following points in the process:

- ♦ During the **Collect Card** or **Batch Collect Card** workflows, at the same time as the Assign step.
- ♦ Using the **Batch Encode Card** workflow as a separate encoding stage.

Additional checks are made during this process to ensure that:

- ♦ The PIV card expiry date does not exceed the lifetime of the signing certificate.
- ♦ The biometric data will not expire during the lifetime of the card.
- ♦ Facial biometric data is present for the applicant.

#### 5. Activate

Make sure that the credential profile is set up to use activation. Set the **Require Activation** option to **Allow self collection** or **Attended activation only**.

The cardholder authenticates to MyID using fingerprint verification – set the **Require fingerprints at Issuance** option in the credential profile – sets the user PIN, and activates the card. The card is now fully issued and can be used.

The cardholder can carry out a self-service activation using the Self-Service Kiosk. Alternatively, an operator can guide the cardholder through activation using the MyID **Assisted Activation** workflow, depending on how you have set the **Require Activation** option in the credential profile.

**Note:** MyID uses the term "activation" to refer to the final handover stage of the PIV card to the cardholder.

You can also combine the personalization and activation stages; however, as it may take some time to generate four 2048-bit key pairs on a card during the personalization stage, if you want to keep the cardholders' time spent interacting with MyID to a minimum, it is recommended that you personalize the cards before the cardholders activate them.

**Note:** FIPS 201-2 requires more than one person to be involved in issuing a PIV card. MyID will not permit the same person to request and validate, or validate and collect a PIV card. However, MyID allows the same operator to request and collect a card – if you do not have a validation stage, you can use the **Edit Roles** workflow to assign the request and collect workflows to different roles and ensure that more than one person is involved in issuing a PIV card.

### 2.2.1 Cardholder authentication

With self-service activation, the cardholder is prompted to provide a fingerprint for authentication before the card can be activated. If the cardholder cannot verify their fingerprints, they will not be able to activate their card without assistance from a MyID operator.

The **Assisted Activation** workflow can be used to allow fingerprint authentication to be retried – if a fingerprint match still cannot be achieved, the operator can override the need for fingerprint verification.

In situations where the identity of the cardholder needs to be proven before carrying out an operation on their behalf, such as activating a card, the **Authenticate Person** operation can be used to record how the cardholder was identified. This operation allows details of the identity documents (approved for use for identification in FIPS 201-2) to be recorded and stored as part of the MyID audit records for future reference. Details of the authentication can be viewed in the Audit History tab of the cardholder's user account record in MyID.

## 2.3 PIV card reissuance

PIV card reissuance covers the following cases:

- The PIV card is to be replaced due to employee status or attribute change.
- The PIV card is to be replaced due to the original being compromised, lost, stolen or damaged.
- The PIV card is to be replaced due to pending expiry.

An external system can request a replacement card using the Lifecycle API.

If the employee status or attributes have changed, you can use the Lifecycle API or the **Edit PIV Applicant** workflow to make any updates to the MyID record.

An operator can request a replacement card using the user interface:

- During the operation a revocation reason must be selected. Each may have different revocation actions, which are described in the user interface.
- For card renewals, the request may be denied if the period to expiry is greater than is allowed. The period is defined in the **Card Renewal Period** configuration flag. On collection of the replacement, the card expiry period will be defined by the credential profile.
- The replacement card may require additional approval (using the **Validate Request** workflow) based on the **Validate Issuance** setting in the credential profile, or the **Approve Replacement Cards** option on the **Process** page of the **Security Settings** workflow.
- FIPS 201-2 requires that the user must be re-enrolled where the chain of trust is not maintained, or the original PIV card had expired prior to collecting the replacement. MyID helps enforce this with the **Applicants Re-Approve for Card Renewal** and **Applicants Re-Enroll for Card Replacement** configuration options.

As MyID holds the original card issuance record and user account data, a 1:1 fingerprint match may be used to confirm the identity of the cardholder prior to activating the replacement card.

It is not possible to request a replacement for a card that has already expired.

Once the replacement card has been requested, and if needed approved, it may be collected using any of the supported card issuance models described above. For all replacement cards other than renewal, the original card expiry date will be maintained. Certificates will not be allowed to exceed this expiry date when configuration flag **(Restrict certificate lifetimes to the card)** is set to **Yes**.

## 2.4 PIV card post-issuance update

MyID can update a PIV card after the initial issuance in the following ways:

- Update the certificates on the card.
- Reprovision the electronic content of the card.

- Reinstall the card after incorrect cancellation.
- Recover additional certificates onto the card.
- Certificate rekey (renewal).

#### 2.4.1 Update the certificates on the card

You can update the certificates on the card using the **Update Card** workflow, or by collecting a card update job that has been created using the **Request Card Update** workflow. You can also use the Lifecycle API. This allows a cardholder to receive an update to the latest version of the assigned credential profile, or to a new credential profile that they are permitted to receive.

This operation does not amend any electronic data held in the PIV applet other than certificates – that is, the FASC-N, CHUID, printed information and biometrics are unchanged. Updates to the card take place over a secure channel in accordance with FIPS 201-2.

The cardholder must enter their PIN to collect the update. You can also configure MyID to require biometric authentication – the **Verify fingerprints during card update** option, on the **Biometrics** tab of the **Operation Settings** workflow, controls this.

#### 2.4.2 Reprovision and reinstatement

Reprovision allows the electronic data on the card to be rewritten. This is useful where the certificate policies have been amended or change is required to the electronic data on the card.

You can reprovision cards using the **Reprovision Card** and **Reprovision My Card** workflows.

- **Reprovision My Card** is intended for cardholders to reprovision their own cards; you may not want to allow this for all users. You can control access by creating an additional role, giving it access to the **Reprovision My Card** workflow, and assigning the role to the cardholders you want to be able to reprovision their own cards.
- **Reprovision Card** is intended for operators to reprovision a card belonging to someone else. Operators can reprovision cards belonging only to users who are within their scope.

If you cancel a card by mistake, issuing a new card may be difficult or time consuming. Instead, you can use the **Reinstall Card** workflow to return the cancelled card to an active state.

If the card is reinstated using an activation job, the credential profile settings for **Require fingerprints at Issuance** will be honored.

If the card is reinstated using an update job, the user must authenticate to MyID first. The **Verify fingerprints during card update** option on the **Biometrics** tab of the **Operation Settings** workflow determines whether fingerprint verification is used.

You cannot reprovision or reinstall a card where:

- The signing certificate or biometric data of the user account will expire within the lifetime of the card.
- The user account does not have *User Data Approved* and this is required by the latest version of the credential profile.

Notes:

- Card printing cannot be performed using this operation (as the card has already been printed).
- New certificates are issued, as they have been revoked at cancellation.

- Depending on how your system is set up, archived certificates are recovered to the card and stored in the key history containers.
- By default, it does not allow the FASC-N or UUID to be rewritten to the card: the original values will be re-added. For more information, see section [5.11, Preserving FASC-N and UUID](#).

If the *User Data Approved* flag has been unset on the user account, the workflow cannot personalize the card. If you change the user data in an external system that provides data to MyID using the Lifecycle API, you must unset the *User Data Approved* flag while the user undergoes the re-enrollment process.

If the user's data has been amended after the initial issuance, and data that appears on the printed surface of the PIV card has been modified, the electronic data within the card would become out of step with the printed surface.

### 2.4.3 Recover additional certificates onto the card

You can recover certificates and their associated private keys onto a smart card in the following scenarios:

- Self-service key recovery:
  - ♦ Automated key recovery.
  - ♦ End user selects certificates to recover.
- Recovery on to another person's card.
- Recovery for investigation.

#### Self-service key recovery

A cardholder can use the **Recover My Certificates** workflow to select certificates to recover to their card. When recovery takes place, all key history containers on the card are rewritten – this will wipe previous content on the card. If MyID is configured to do so, the key history containers are overwritten when automated key recovery takes place.

All retired certificate containers are overwritten.

**Note:** Fingerprint verification is required for all self-service operations.

Based on configuration in MyID, certificates (from any assigned card) are automatically recovered on to their card in the following cases:

- Reprovisioning a card.
- Reinstating a card.
- Updating a card.
- Replacing a card.

The options that affect this functionality are determined by the certificate options in the credential profile.

See the [Administration Guide](#) for details.

#### Recovery on to another person's card

MyID allows you to recover certificates onto another person's smart card. Typically this is used when the certificate owner requires another trusted person to deputize for them (and therefore requires encryption certificates to be shared).

It can also be used by a MyID operator to recover certificates to the PIV cardholder's issued card where they cannot fulfill the biometric verification requirements of the self-service operations. Use the **Authenticate Person** option to create an audited authentication of the PIV cardholder.



Use the **Recover Certificates** workflow to recover the certificates. The smart card used must be in an issued state, and existing key history containers on the card will be erased.

### Recovery for investigation

When certificates are to be recovered for investigative purposes, a strictly controlled business process must be enforced, ensuring that multiple people are involved who hold the required permissions and the process is fully audited.

MyID allows you to generate a request, including identifying the user account which must collect the request. The request itself uses a specific credential profile for this purpose, which ensures that only recovered certificates are written to the card. The PIN may also be set to a random generated value, which is hidden from the collector, and sent to an email address identified in the request.

See the *Key Recovery* section of the [Administration Guide](#) for details.

#### 2.4.4 Certificate rekey (certificate renewal)

The MyID certificate renewal process generates a new key pair (rekey) as defined by FIPS 201-2.

MyID can automatically generate jobs as certificates approach their expiry date. When you collect the job, MyID replaces the original certificate with a newly issued certificate. At the point of issuing the certificate, the latest data from the user account is used in the certificate request.

The original certificate policy may have been superseded by a new policy, which are used instead. See the *Superseding certificate policies* section in the [Administration Guide](#).

This process does not alter any content of the PIV applet (for example, the FASC-N, CHUID, or printed information).

## 2.5 PIV Card Verification Data Reset

### 2.5.1 Self-service PIN reset

You can reset the PIN in the following situations:

- When the PIN is locked because of multiple incorrect attempts at authentication.

You can reset a locked PIN by inserting your card on the logon screen. Once authentication is attempted, if the card PIN is locked you are prompted to unlock the card.

This operation must be authenticated – the type of authentication is determined by the credential profile used to issue your card, and MyID configuration settings.

FIPS 201-2 requires that a fingerprint is used to authenticate a person before the PIN can be reset.

The system default setting for MyID PIV is to require a fingerprint to unlock a card.

You can configure the credential profile to require additional biometric authentication. This can be used where the installation supports multiple credential types, including non-PIV cards and use of PIV cards for CIV. In this case, the global configuration can be set to not require a fingerprint to unlock a card – the credential profile will override this for cards associated with it.

The following authentication rules are supported by MyID, but are not recommended for use with FIPS 201-2:

- ♦ Require an authentication code (credential profile rule)



- ♦ Where the credential profile setting is 'System Default' both biometrics and security questions can be required, based on global configuration.
- ♦ Where the credential profile carries no additional authentication requirements (it is set to Never) there will be no requirement for biometric or authentication code, overriding the global configuration. It will not be possible to unlock a card with no authentication, therefore security questions should be configured.

**Note:** Before unlocking a card, MyID checks the latest version of the credential profile – therefore policy changes made after card issuance will be enforced.

- When the user decides to change their PIN to a new value.

You can use the MyID **Reset Card PIN** workflow to change your PIN. You must re-enter your old PIN before you supply the new PIN.

Alternatively, you can use the Reset PIN option on the Self-Service Kiosk. Similarly, you must re-enter your old PIN before you supply the new PIN.

MyID has a PIN unlock utility that allows you to perform a challenge/response PIN unlock or to change the card's PIN. See section [5.16, Remote PIN Management utility for PIV cards](#) for details.

**Note:** Currently, this utility does not allow fingerprint verification, and therefore is not recommended for use with cards that require FIPS 201-2.

## 2.5.2 Operator-led PIN reset

You can use the **Reset Card PIN** workflow to reset another person's card PIN. This operation:

- Cannot be used to unlock your own card – the self-service operations must be used instead.
- Can only be used to unlock a card belonging to a user account in the current operator's scope.
- Does not enforce any additional authentication – use the **Authenticate Person** operation to create an audited record of the user authentication. This operation allows an authenticated MyID operator, with appropriate permissions in their role to:
  - ♦ Attempt fingerprint verification.
  - ♦ Bypass fingerprint verification if necessary.
  - ♦ Record details of the identity documents presented by the user.
  - ♦ Override any further authentication.

For more information, see section [5.14, Authenticating users](#).

## 2.5.3 Biometric matching for PIN reset

When MyID carries out a biometric match for PIN reset it is:

- Taking the fingerprint templates provided by the cardholder (translated from a raw image by the biometric template generator).
- Matching it against the fingerprint captured at enrollment – this is biometric data stored in the MyID database, and provides an off-card 1:1 biometric match. Matching takes place on the MyID server.
- The matching library used by MyID can be selected in global configuration.

#### 2.5.4 Resetting other verification data

In this release, other verification data (biometrics, printed information, and so on) may only be reset when the electronic data within the card is re-issued. This can occur at:

- Repersonalize Card.
- Reinstate Card.
- Collection of a replacement card.

## 2.6 PIV Card Termination

The following processes apply to revoking an issued PIV card:

- Cancelling (revoking) a PIV card that is present.
- Remotely cancelling a PIV card that is not present.
- Erasing a PIV card that has been remotely cancelled.
- Changing the disposal status of a card.

### 2.6.1 Cancelling (revoking) a PIV card that is present

The **Erase Card** workflow is used to revoke and erase a smart card that is in the possession of the operator. This operation:

- Disassociates the card from the user account (the cardholder).
- Using the revocation reason selected, revokes the certificates on the PKI.

The following reasons immediately revoke the certificates: Lost, Stolen, Damaged, Revocation (Other).

- Resets the content of the PIV applet.
- Deletes all private keys on the card.
- Cancels all jobs in MyID associated with the card serial number.
- Resets the Global Platform and PIV 9B Keysets to factory values.
- Optionally allows the disposal status of a card to be set, preventing reuse of the card.

### 2.6.2 Remotely cancelling a PIV card that is not present

You can remotely cancel a card in the following ways:

- Using the Lifecycle API.
- Using the **Cancel Credential** workflow.
- Disabling the group to which the user account belongs.
- Disabling the user account.
- Directory synchronization.
- Remove person.

In each of these operations, a revocation reason is supplied that determines the PKI actions that are taken. The revocation reasons perform the same actions as cancelling a PIV card that is present. No change is made to the data on the card.

### 2.6.3 Erasing a PIV card that has been remotely cancelled

When a card has been remotely cancelled, it retains the electronic data held on the card. It is best practice to erase the card once it has been returned to a MyID operator.

Use the **Erase Card** workflow to erase the card. This workflow carries out the following:

- Resets the content of the PIV applet.
- Deletes all private keys on the card.
- Cancels all jobs in MyID associated with the card serial number.
- Resets the Global Platform and PIV 9B Keysets to factory values.

### 2.6.4 Notifications to other systems

FIPS 201-2 requires that any databases maintained by the PIV card issuer that indicate current valid (or invalid) FASC-N or UUID values must be updated to reflect the change in status.

You can configure MyID to send notification messages containing information about card cancellations. For more information on notifications, see the [Administration Guide](#), or contact customer support quoting reference SUP-222.

### 2.6.5 Changing the disposal status of a card

The disposal status of a cancelled PIV card can be recorded in the MyID audit trail. This ensures that the card cannot be re-issued. You can use the **Card Disposal** workflow to set the disposal status. For information, see the *Disposing of cards* section in the **Administration Guide**.

## 3 Configuring MyID

### 3.1 Installing MyID Server software

PIV support is enabled when you install MyID PIV. This software builds on the MyID core product and adds specific features and configurations for PIV, PIV-I and CIV card issuance. Instructions for installation of the product, and information about deployment options, hardware and software requirements are found in the [Installation and Configuration Guide](#).

#### 3.1.1 Integrating MyID with other systems

MyID can be used to integrate other systems into a fully featured PIV solution. Further details of the requirements for each system supported can be found in the appropriate Integration Guide for each specific system.

- Smartcard Readers and Printers

If PIV cards are to be issued and managed from a MyID client, smartcard readers will be required to allow MyID to communicate with the card.

Often they are integrated into Smartcard Printers, that allow a batch of cards to be processed sequentially, including electronic personalization following by printing of the physical card.

- Certificate Authorities

The Certificate Authority is used to generate digital certificates that are included within the PIV card. This is an essential element in a PIV solution.

- Hardware Security Modules (HSM)

An HSM is a secure device used to generate and store cryptographic keys. MyID can use the features of a HSM to secure the MyID database, generate keys for securing smartcards and certificates used for encrypting sensitive data. This is an essential element of a PIV solution.

- Biometric Capture Devices

A Biometric reader can be used to capture a fingerprint from an Applicant. This is then stored as a digital representation and can be used to verify the identity of the Applicant. Biometric data is stored on a PIV card as well as the MyID database.

- Additional Integration Capabilities

MyID can integrate with a wide range of additional hardware and software, but may require additional configuration or software updates. If you are interested in using these features, please contact Intercede for further details.

- ♦ Facial Biometric Capture

MyID can integrate with software that allows a photograph to be captured from a digital camera, which is then processed to provide a PIV compliant facial biometric sample. This is written to the PIV Card during card personalization.

- ♦ Adjudication Systems

The adjudication process for PIV cards may require the Applicant to be vetted by an external body before being permitted to receive a PIV card. This can be carried out by an organization such as the Office of Personnel Management. Alternatively a local check can be made against a database of biometric data using matching software installed on the MyID server.

- ♦ Physical Access Control Systems (PACS)

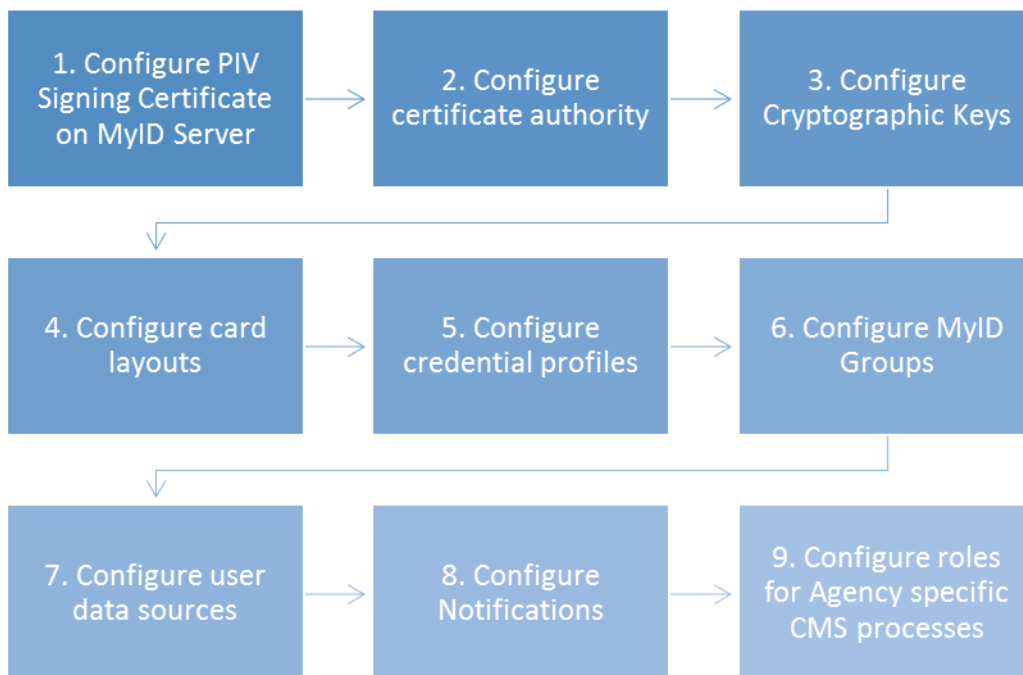
PAC Systems allow an Applicants PIV card to be granted access to a room or building by presenting their PIV card. MyID can integrate with PACS by providing applicant and card data, and allowing an operator to identify which areas they may be allowed to access.

- Card Production Bureau

Large deployments of MyID for PIV may require personalization of PIV cards to take place at a manufacturing facility rather than within the offices of the agency. A card production facility allows rapid production and issuance of PIV cards and can be integrated with a secure issuance model that postpones creation of the most sensitive data until the card is in the hands of the verified cardholder.

### 3.2 Configuring MyID for FIPS 201-2 card issuance (PIV)

In order to achieve the enrollment and issuance models you require for your installation of MyID for PIV, a number of steps must be followed.



Step	Description	See
Configure PIV Signing Certificate on MyID Server	PIV card issuance must be electronically signed using a certificate. The certificate must be issued and configured on the MyID server.	Section <a href="#">4.2, Configure server signing certificates</a> .
Configure Certificate Authority	A connection must be established to the Certificate Authority to allow certificate policies to be downloaded and configured for issuance by MyID.  Specific data attributes must be included in each certificate for PIV compliance – but note that these attributes may be different if you are using MyID for a non US Federal site (PIV-I or CIV).	The integration guide for your CA.
Configure Cryptographic Keys	PIV Cards are secured using cryptographic keys that are written to the card. These keys must be configured in MyID to allow issuance, and then update of the keys to a value only known to MyID.	Section <a href="#">5.1, PIV Card Application Administrator Key</a> .

Step	Description	See
Configure card layouts	FIPS 201 defines the physical layout of a PIV card as well as the electronic elements. MyID is supplied with card layout templates that are ready to use, but can also be customized to meet any specific needs.	Section <a href="#">5.4, Setting up the credential profile</a> . Section <a href="#">5.4.1, Updating existing card layouts</a> .
Configure credential profiles	Credential profiles define what content is to be added to the PIV card and the issuance model used to issue the card.  If you are using MyID for a non US Federal site (PIV-I or CIV), ensure you select the appropriate card data model.	Section <a href="#">5.4, Setting up the credential profile</a> .
Configure MyID groups	In MyID, the group can be used to represent an agency. This requires some specific data to be added that is used to form data written to each PIV card issued to the agency.	Section <a href="#">5.6, Manage agencies</a> .
Configure User Data Sources	You can add and amend PIV user attributes using the following: <ul style="list-style-type: none"> <li>▪ Lifecycle API. This requires the configuration of a data feed from your enrollment system.</li> <li>▪ Manually adding users with the MyID workflow <b>Add Person</b>.</li> <li>▪ Importing users from a connected LDAP compliant directory using <b>Edit Person</b> or <b>Edit PIV Applicant</b>.</li> <li>▪ <b>Edit PIV Applicant</b> workflow allows PIV specific attributes to be updated and fingerprint and facial biometric enrollment to take place.</li> </ul>	Section <a href="#">5.15</a> , Editing PIV applicants.  The <a href="#">Lifecycle API</a> document.
Configure Notifications	MyID can generate notifications to other systems during issuance or cancellation. This can be used to ensure that other systems are kept up to date with the latest information from MyID.	For more information on notifications, see the <a href="#">Administration Guide</a> , or contact customer support quoting reference SUP-222..
Configure roles for Agency-specific processes	Configuration of MyID roles helps role separation to be enforced, and provides access to necessary operations for each user.	The <a href="#">Roles, Groups and Scope</a> section in the <a href="#">Administration Guide</a> .

### 3.3 Configuring MyID for non-Federal issuers (PIV-I, CIV)

You can issue PIV, PIV-I and CIV smart cards in the same MyID installation. However there are some differences in how MyID should be configured, and methods used for adding user data.

It is also possible to issue other non-PIV credential types, such as certificates for mobile devices, Microsoft Virtual Smart Cards or software certificates from the same system.

#### 3.3.1 PIV support levels

The following table describes each PIV support level that can be achieved with MyID, and describes some of the difference between each.

PIV support level	Description	User data entry method	In PIV	In core
FIPS 201 PIV	Use of PIV card technology for federal agencies following FIPS 201 requirements. Agency code is present but not 9999. Specific PKI requirements for trust to the federal bridge. <b>Note:</b> You must ensure any additional processes required for identity proofing and registration take place, in accordance with FIPS-201 guidelines where applicable, before marking the user record as User Data Approved.	LDAP, PIV Lifecycle API, or Manual	Yes	No
PIV-I	Use of PIV card technology for associates/contractors to Federal agencies. Agency code is 9999. Specific PKI requirements for trust to the federal bridge.	LDAP, PIV Lifecycle API, or Manual	Yes	No
CIV – with CHUID/Applet personalization	Use of PIV card technology, where the format and source of the CHUID and PIV applet data is the same as PIV/PIV-I. PIV Attributes required for card issuance. Agency code is 9999. No specific PKI requirements.	LDAP, PIV Lifecycle API, or Manual	Yes	No
Custom CIV	The format or source of the CHUID and PIV applet data is different to PIV/PIV-I. PIV attribute values on card may be hard coded to predetermined values.	As Project Requirement	No	Yes <sup>1</sup>

<sup>1</sup> With CIV module installed. Further customization may be needed.

PIV support level	Description	User data entry method	In PIV	In core
CIV – certificates only	Use of PIV card technology, with no CHUID/PIV applet data personalization. No PIV attributes required.	LDAP, Core Lifecycle API or Manual	Yes	Yes
Non-PIV	Not using PIV card technology. No PIV attributes required.	LDAP, Core Lifecycle API or Manual	Yes	Yes

Due to differing requirements between PIV, PIV-I and CIV there are some additional aspects of configuration and user data that must be considered.

- **Card Type and Data Format**  
In order to issue cards that are PIV-Interoperable or CIV, a PIV card supported by MyID must be used. Non-PIV cards will not be able to support the required data structures. When configuring the credential profile for these cards, ensure that the correct data model is used.
- **NAC-I Checks**  
If the Non Federal Issuer has chosen not to undertake the National Agency Check with Written Inquiries (NACI), the 'NACI Status' field used during enrollment of the Applicant should be left at 'Not Requested'.
- **Certificate Policies**  
Certificates used on PIV-I cards must not be configured to include the FASC-N attribute. The UUID attribute should be present in the Card Authentication Certificate and the Authentication Certificate, and be issued from a Certificate Authority that is cross-certified with the Federal Bridge Certification Authority (FBCA). This is essential in order to establish the trust relationship with Federal Agencies.  
  
The PIV-I Authentication Certificate and the Card Authentication Certificate are not required for PIV Compatible cards.  
  
Certificate Profiles to be used on PIV-I or CIV cards should also not be configured to include NACI (piv-interim) attribute where these checks are not undertaken during enrollment.
- **Group Configuration**  
A Non-Federal Issuer must use the agency code '9999', system code '9999' and provide a DUNS value.
- **Card Layouts**  
The layout and images present on a PIV-I or CIV card must be easily distinguishable from a PIV card and are expected to include the Issuing/Sponsoring Organization (e.g. Company name), Card holder Photograph, Card holder Full Name and Card Expiration Date. At a minimum, images or logos on a PIV-I Card shall not be placed entirely within Zone 11, Agency Seal, as defined by FIPS 201. The Card Layout Editor in MyID can be used to create and amend the card layouts – see the [Administration Guide](#).



### 3.3.2 Issuing cards to the correct users

You must ensure that FIPS 201 PIV and PIV-I cards can only be issued to genuine PIV Applicants who have been through all the relevant enrollment business processes in accordance with FIPS 201.

You must set up the credential profiles for FIPS 201 to require that the user account has the **Require user data to be approved** option set. This ensures that only user accounts who have been through appropriate processes for enrollment and verification (managed using an external system such as an IDMS) can receive FIPS 201 PIV cards.

You must make sure that FIPS 201 PIV certificate policies and printed card layouts are only assigned to credential profiles that have the **Require user data to be approved** option set.

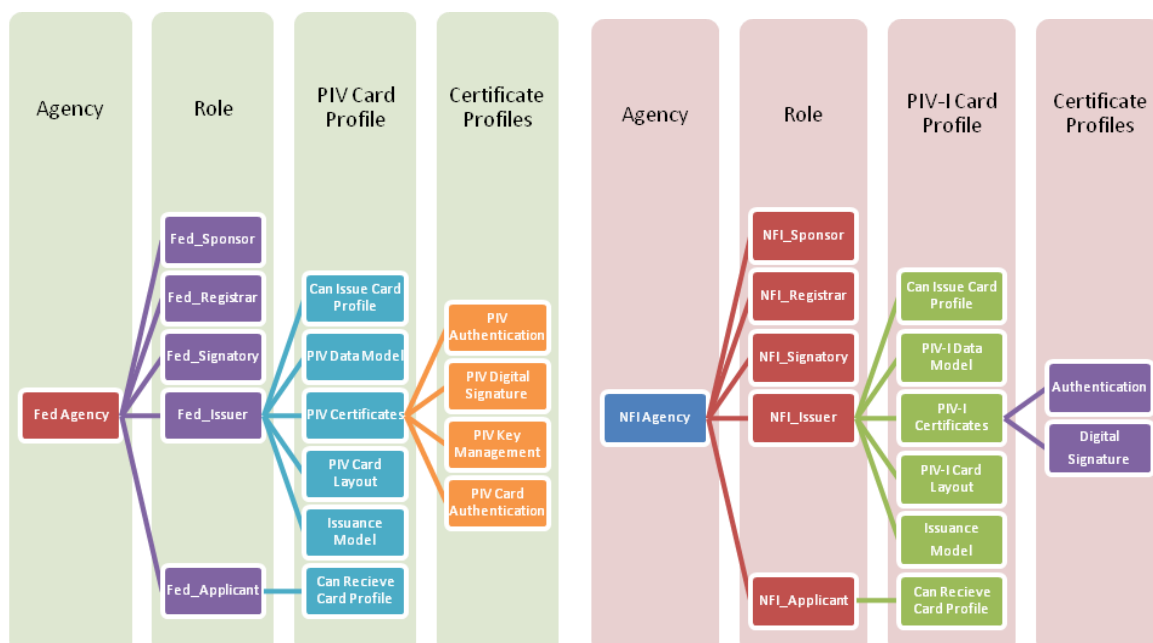
You must restrict the roles that are permitted to issue and receive the FIPS 201 PIV and PIV-I credential profiles; you can request cards using the MyID GUI in addition to the Lifecycle API – the available profiles for selection are restricted based on the roles held by the current operator requesting the card, and the person selected to receive the card.

### 3.3.3 Maintaining multiple populations in a single system

Separation between PIV, PIV-I and CIV card holders can be achieved by registering each Non-Federal Issuer as a separate Group within MyID. Operator access to each group can be controlled using Scope rules, and if necessary 'Administrative Groups'. Further information about these features can be found in the Administration Guide.

Security may be extended further by creating specific roles for each Group, and restricting roles that can belong to the group to those that can issue, manage or be issued PIV-I or CIV cards. Credential profiles for PIV-I or CIV cards can then also be restricted to these roles. This will ensure the role separation that is required to distinguish cards issued using the FIPS 201 process and those that are PIV-Interoperable or CIV.

The following diagram illustrates a recommended configuration for an installation supporting issuance of PIV and PIV-I cards.



### 3.3.4 Adding applicants

The method you use to add applicants to MyID depends on the type of user.

**Note:** If you attempt to issue cards where the credential profile in MyID uses a data model that requires PIV attributes, but the attributes are not present on the user account, card issuance will fail.

- FIPS 201 PIV, PIV-I, and CIV (with CHUID/applet personalization)
  - ♦ User accounts must be imported using PIV Lifecycle API to set the PIV attributes, manually added using the **Edit PIV Applicant** workflow, or imported from LDAP using the **Edit PIV Applicant** workflow. The additional role of **PIV Applicant** is used to identify these user accounts.
  - ♦ In order to receive a FIPS 201 level PIV card, the *User Data Approved* flag must be set. Use of this flag in combination with the requirement for it in the credential profile can be used to tailor the issuance processes to suit your organization.  
  
For example, CIV credential profiles may still use a PIV data model, but not require *User Data Approved* to be set due to a more flexible enrollment policy.
  - ♦ Assign them to a group that has PIV agency attributes defined, or import these as part of the data in the Lifecycle API.
  - ♦ If the users in the group are part of a federal agency, set the appropriate agency code.
  - ♦ If the users in the group are not part of a federal agency, set the Agency code to 9999.
- CIV (certificates only) and non-PIV
  - ♦ PIV user attributes are not needed. You can use the CMS Lifecycle API schema, or manually add user accounts using Add Person or Edit Person (with import from directory). You cannot add PIV attributes using the user interface.
  - ♦ Users can be assigned to groups that have PIV attributes – but there will be no use of the attributes during card issuance.

### 3.3.5 Operator permissions

You must ensure that applicants with PIV attributes can be administered only by operators who have been permitted to do so.

User accounts that hold the **PIV Applicant** role (as set at import) cannot be edited in the **Edit Person** workflow. Instead, you can use **Edit PIV Applicant**. See section [5.15, Editing PIV applicants](#) for details.

PIV attributes are visible in **View Person** and during card issuance and management operations.

If access to these records is to be limited, you can set group and scope restrictions to control access to user accounts. By putting PIV applicants in a specific group or group hierarchy, you can limit access to these applicants based on MyID scope restrictions. If access to these users is needed by operators outside of this group hierarchy, you can use the Administrative Groups feature to assign access.

### 3.3.6 Business rules

Specific business rules that apply to FIPS 201 PIV, PIV-I and CIV cardholders that will not affect other users managed by MyID:

- Card issuance rules (signing certificate expiry, biometric expiry, mandatory biometrics).

- Card re-issuance rules (requirement for re-enrollment before card re-issue).
- Post issuance update rules (prevent FASC-N/UUID recreation when updating a card).

### 3.3.7 Authentication

As non-PIV and CIV may have no requirement for the user to register biometric data, you must ensure that authentication settings are configured appropriately to provide the required levels of security in self service operations.

### 3.3.8 Summary of requirements for PIV-I, and CIV

When issuing PIV-I and CIV cards, make the following changes:

- PIV-I
  - ♦ When setting up the group, set the following fields on the **Agency** tab:
    - **Issuing Agency** – set to 9999.
    - **Site Code** – set to 9999.
  - ♦ The certificates must contain the FASC-N.
  - ♦ The cards must not look like FIPS 201 cards – do not use the PIV cards layouts.
  - ♦ Select **PivDataModel.xml** from the **Card Format** drop-down list in the credential profile.
- CIV (with CHUID/Applet personalization)
  - ♦ When setting up the group, set the following fields on the **Agency** tab:
    - **Issuing Agency** – set to 9999.
    - **Site Code** – set to 9999.
  - ♦ The certificates must *not* contain the FASC-N.
  - ♦ The cards must not look like FIPS 201 cards – do not use the PIV cards layouts.
  - ♦ Select **PivDataModel.xml** from the **Card Format** drop-down list in the credential profile.
- CIV (with certificates only)
  - ♦ When setting up the group, set the following fields on the **Agency** tab:
    - **Issuing Agency** – set to 9999.
    - **Site Code** – set to 9999.
  - ♦ The certificates must *not* contain the FASC-N.
  - ♦ The cards must not look like FIPS 201 cards – do not use the PIV cards layouts.
  - ♦ Select **CivCertificatesOnly.xml** from the **Card Format** drop-down list in the credential profile.

## 4 After Installing MyID

### 4.1 Controlling the content of subject alternative names

By default, the content for subject alternative names is controlled by the CA, and content specified in a certificate request is not accepted. To specify content for subject alternative names, you may have to modify the configuration of the CA.

For details of any specific changes you need to make to the CA to allow the specification of content for subject alternative names, see the relevant CA implementation guide.

To control the content of subject alternative names in MyID, see section [5.3, Specify which certificates to use](#).

### 4.2 Configure server signing certificates

To increase the level of security, MyID digitally signs some of the data objects that are written to the smartcard:

- CHUID (Card Holder Unique ID)
- CBEFF (Biometric fingerprint data)
- Security Object

The server can either use a single certificate to sign the data objects or a separate certificate can be configured for each object.

You can also configure MyID to use multiple signing certificates for the same type of data object – for example, if you have both PIV and PIV-I cards in circulation. For more information, contact customer support, quoting reference SUP-118.

FIPS 201 requires that each PIV card issuance is signed by a certificate issued in accordance with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.

**Note:** For PIV compliance, this certificate must be protected by an HSM.

The signing certificate must:

- Use SHA256 in the `digestAlgorithm` of the `SignerInfo`.
- Use SHA256 in the `AlgorithmIdentifier` of the signature.
- Be issued using the CSP of the HSM for key generation.
- Be issued to the MyID COM+ account that is configured to run the MyID server components.
- Use an RSA key – ECC is not supported.

For full FIPS 201 card issuances, the certificate must contain an extended key usage attribute of:

- `id-PIV-content-signing (2.16.840.1.101.3.6.7)`

For PIV-I, the certificate must contain:

- `id-fpki-certpcy-pivi-contentSigning (2.16.840.1.101.3.2.1.3.20)`
- `id-fpki-pivi-content-signing (2.16.840.1.101.3.8.7)`

The signing certificate must not require any user intervention when signing:

- Do not set the private key as User Protected; this requires a PIN entry dialog during signing.
- If the key is protected by an HSM, do not configure the key to launch a PIN entry dialog. For an nCipher HSM, the nCipher CSP must not be configured to protect the private key with an operator card set that requires PIN entry. For nCipher HSMs, the content signer certificate can be protected either by the module, or by an operator cardset without PIN.

**Note:** You must configure the server signing certificates on the server prior to issuing PIV-compliant smartcards.

Refer to the FIPS 201 documentation for additional requirements relating to the PIV content signing certificate.

Before MyID can use a certificate to sign objects, the certificate must be available to the account used to run the MyID components.

**Note:** For PIV and PIV-I, you must use SHA256 for the PIV server hash algorithm; see section 4.3, *Configuring the PIV server hash algorithm* for details. You must make sure that the CSP you use to issue the certificate supports SHA256.

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 either by CAPI (Cryptographic Service Provider) or by CNG (Key Storage Provider). You can issue a certificate from any certificate authority as long as it is available to CAPI or 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, click **Run** and type `regedit` in the dialog displayed. Click **OK**.

- b) Navigate to:

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

- c) Set the value of the following keys to the full path of the certificate:

- `CBEFFSigningCertificate`
- `CHUIDSigningCertificate`
- `SecurityObjectSigningCertificate`

**Note:** The server signing certificate will expire. Once the lifetime of issued cards goes beyond the expiration date of the server signing certificate, the issued card is no longer valid.

This means that the date at which the server signing certificate must be renewed depends not only on the expiration date of the server signing certificate, but also the intended card lifetime of the cards being issued.

To prevent a situation where the server signing certificate is not valid for the lifetime of the issued certificate, you must set up a procedure to ensure that the server signing certificate is manually renewed before issuing cards that have an expiration date that may exceed the expiration date of the server signing certificate.

#### 4.2.1 Troubleshooting the content signing certificate

If you have made any mistakes in setting up the configuration for the content signing certificate (for example, omitting the path from the registry) you may see an error similar to the following when attempting to issue a card:

```
Data Model failed validation
```

If you see an error like this, check that you have configured the signing certificate correctly.

### 4.3 Configuring the PIV server hash algorithm

You can specify the PIV server hash algorithm. PIV data can be hashed using SHA256 (which is required for PIV compliance) or SHA1 (for systems that do not require full PIV compliance). The default is SHA 256.

1. From the **Configuration** category, select **Security Settings**.
2. Click the **Server** tab.
3. Select a value for the **PIV Server hash algorithm** option.

You can select one of the following:

- ♦ SHA1
- ♦ SHA256

4. Click **Save changes**.

**Note:** Changing the PIV server hash algorithm has an impact on existing issued cards if you use MyID to renew certificates on a card or perform updates to the content of the card after it is issued. For example, when you issue cards with a SHA-256 hash and then modify the MyID configuration to revert back to SHA-1, the collection of certificate renewals will fail due to a hash mismatch error. Other affected processes include collecting a key recovery, or adding additional certificates to the card.

You must set this option to SHA256 for PIV compliance and to follow best security practice. You are not recommended to run with SHA1 on a production system.

### 4.4 Biometric identification

PIV requires that fingerprints in 378 format are captured during enrollment, and then written to the card when it is issued. Support for the biometric reader and validation software must be installed before this functionality can operate correctly.

The fingerprint reader and supporting software must be compliant with the INCITS 378-2004 format. The following fingerprint scanners are supported:

- SecuGen Hamster IV
- SecuGen iD-USB-SC/PIV

See the integration guide for your fingerprint reader for installation and configuration details.

### 4.5 Setting up MyID when you have existing PIV cards

If you already have issued PIV cards from a system other than MyID, and are switching over to use MyID as your PIV card management system, you must bear in mind that PIV cards use a value called the credential number, along with other attributes, to form a unique identified known as the FASC-N. You must avoid clashes between the FASC-N on the issued cards and the new cards issued by MyID.

**Note:** The FASC-N only appears on FIPS 201 PIV cards – PIV-I and CIV cards do not allow use of the FASC-N. A GUID is used instead to uniquely identify the card. PIV-I and CIV cards will have the credential number set to a fixed value of 999999. This occurs when the agency code is set to 9999.

- The base credential number is set at installation of the product.  
By default it is set to 250000 for a new installation.  
If the installation is an upgrade from a previous version of MyID, no change is made to the credential number.
- If you have existing PIV cards in circulation (issued by another CMS or managed service, using the same agency code as you intend to use), you must:
  - ♦ Amend the value of the base credential number before you starting issuing cards in the production environment, *or*
  - ♦ Supply the credential number for each card as part of the request generated using the Lifecycle API; this means that an external system must ensure that the value provided is unique and not duplicated within your agency.

There are various approaches that can be taken to managing the uniqueness of the credential number:

- Card requests are generated by MyID  
When a card is requested (either new issuance or a replacement) the next available credential number is assigned and stored as part of the user account. The base credential number will be incremented at this point.
- Card requests are generated by an external system  
You can import a credential number using the Lifecycle API. It is stored as part of the MyID user account. MyID does not change the base credential number.
- Card requests are generated by both MyID and an external system.
  - ♦ Separate credential number ranges  
A distinct number range is assigned to each system. When a card request is created in MyID, the base credential number is incremented. When an external system creates a card request there is no change to the base credential number.  
  
You must monitor usage of credential numbers to ensure the numbers do not overlap.
  - ♦ MyID controls the credential number  
The configuration option **Credential Number Per Device** identifies the field holding the credential number; this is used at card issuance. You can remove the value of this configuration option, meaning that each card issuance will generate a new credential number and not retrieve it from the user account. When this occurs, the base value is incremented by 1. The credential number used is stored against the user account.

**Note:** The base credential number managed by MyID will roll over from 999999 to 000000, as credential number is a six-digit value. This causes the re-use of existing values.

If you want to change the base credential number used by MyID, contact Intercede customer support, quoting reference SUP-127. The credential number must be carefully considered to ensure that duplicate credential numbers are not used.

See also section [5.5, Setting credential numbers](#) for more information.



## 4.6 Controlling local and remote operations

You can configure MyID to control access to local (that is, operator-led) operations and remote (self-service) operations.

You can use the following features to control access:

- Use the **Edit Roles** workflow to allow or prevent access to individual workflows.  
For example, you can prevent the Applicant role from accessing the **Change My Security Phrases** workflow if you want to require applicants to change their security phrases only with the assistance of an operator.  
See the [Administration Guide](#) for details of using the **Edit Roles** workflow.
- Use the job filtering feature of the MyID web services to allow or prevent jobs being processed by the Self-Service App.  
See the [Web Service Architecture Installation and Configuration Guide](#) for details of setting up job filtering.
- Set up a separate instance of the MyID web services to allow only specific Self-Service Kiosks to process card activation jobs.  
You are also recommended to set up 2-way SSL to ensure that only known clients can access this web service.
- Use the **Credential Profiles** workflow to set up your credential profile to set the **Require Activation** option to one of the following:
  - ♦ **Allow self collection** – applicants can collect and activate their own cards.
  - ♦ **Attended activation only** – applicants must activate their cards with the assistance of a MyID operator.



## 5 Using MyID for PIV

See the [Installation and Configuration Guide](#) for details of setting the password for the startup user. You can log in to MyID with this user, and use it to create more permanent users with password or smart card access.

### 5.1 PIV Card Application Administrator Key

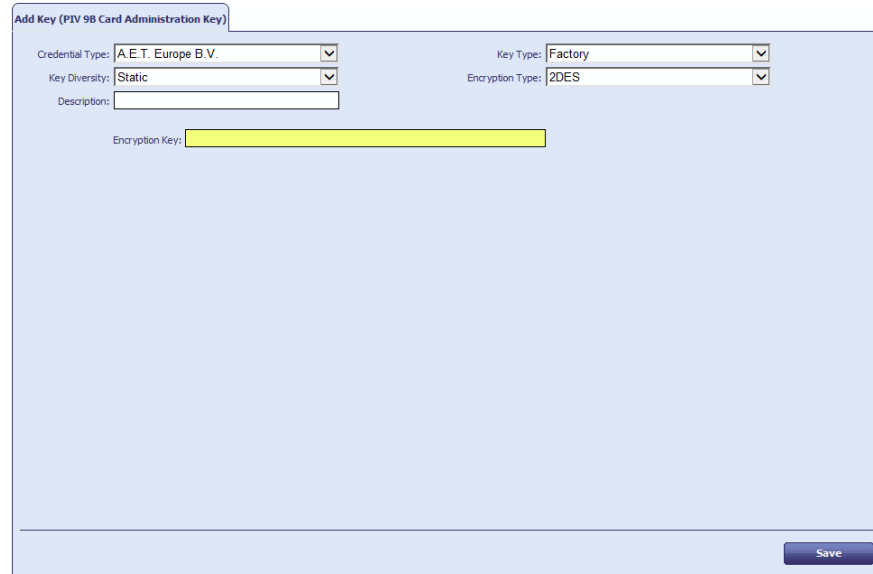
You must enter the values of secret shared keys (9B keys) to enable the smart card management system to authenticate (and therefore manage) the smart cards. If you do not have this factory key, you cannot issue cards.

9B keys and related specifications are defined in *SP 800-73 – Interfaces for Personal Identity Verification* available at <http://csrc.nist.gov>.

#### 5.1.1 Factory 9B keys

When cards are manufactured, they are provided with a factory key. You will have been given this factory 9B key by your smart card supplier; this is a string of characters in hexadecimal format.

1. From the **Configuration** category, select **Key Manager**.
2. From the **Select Key Type to Manage** list, select **PIV 9B Card Administration Key**, then click **Next**.
3. Click **Add New Key**.



4. Select the **Credential Type** from the drop-down list. This is the type of card you are using.
5. Select **Factory** from the **Key Type** drop-down list. This means that you are using the key provided by your supplier.
6. Select **Static** from the **Key Diversity** drop-down list. You can select only **Static** for factory keys.
7. Select the **Encryption Type** from the drop-down list.

**Warning:** Make sure you select the **Encryption Type** supported by the devices you are using. If you select the wrong length of key, you will not be able to issue cards.

8. Type a **Description** for the key.

9. Type the hexadecimal 9B key provided by your smart card supplier in the **Encryption Key** box.
10. Click **Save**.

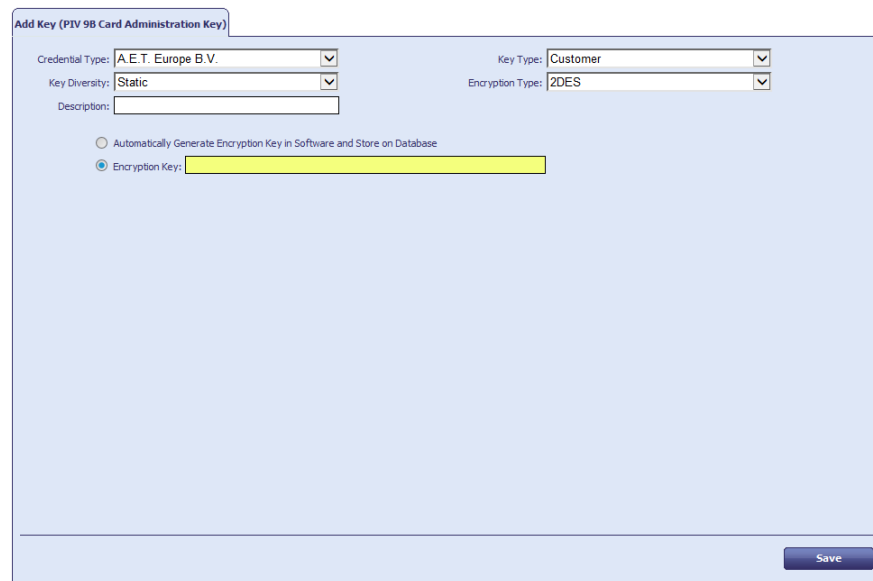
### 5.1.2 Customer 9B keys

You can configure a customer 9B key for PIV systems. When issuing a card, MyID will change the factory 9B key to the customer 9B key.

This means that if you need to be able to reuse the card in different installations, you must cancel the card – canceling a card changes the customer 9B key back to the factory 9B key so the card can be reused.

**Note:** If you lose the key data held in the database, you will no longer be able to cancel or unlock the card.

1. From the **Configuration** category, select **Key Manager**.
2. From the **Select Key Type to Manage** list, select **PIV 9B Card Administration Key**, then click **Next**.
3. Click Add New Key.
4. Select the **Credential Type** from the drop-down list. This is the type of card you are using.
5. Select **Customer** from the **Key Type** drop-down list.



6. Select **Static** or **Diverse** from the **Key Diversity** drop-down list.  
Diverse keys are more secure, as a new key is generated for each device.
7. Select the same **Encryption Type** as you specified for the factory key.
8. Type a **Description** for the key.
9. If you are storing the key in the database, choose one of the following options:
  - ♦ **Automatically Generated Encryption Key** – this option automatically creates an encryption key.
  - ♦ **Encryption Key** – type the hexadecimal key in the box.

If you are storing the key on an HSM, choose one of the following options:

- ♦ **Automatically Generate Encryption Key on HSM** – this option generates a key on the HSM.
- ♦ **Existing HSM Key Label** – if you have an existing key on your HSM that you want to use, type its label.

10. Click **Save**.

## 5.2 GlobalPlatform keys for PIV cards

If you want to specify customer PIV keys for certain types of PIV cards, you must have an GlobalPlatform factory keyset defined for the cards – the GlobalPlatform key is used to authenticate any change to the PIV 9B key.

To create a GlobalPlatform key, click the **Applets** category and select the **Manage GlobalPlatform Keys** workflow from the list.

## 5.3 Specify which certificates to use

You can specify which certificates to use for each role in the system; for example, you can select the certificates to be used for the **Applicant** role.

1. Log on to MyID using the Security Officer card.
2. Click the **Configuration** category and select the **Certificate Authorities** workflow from the list.
3. Add or edit the CA that you want to use.

See the Integration Guide for your CA for any specific setup information.

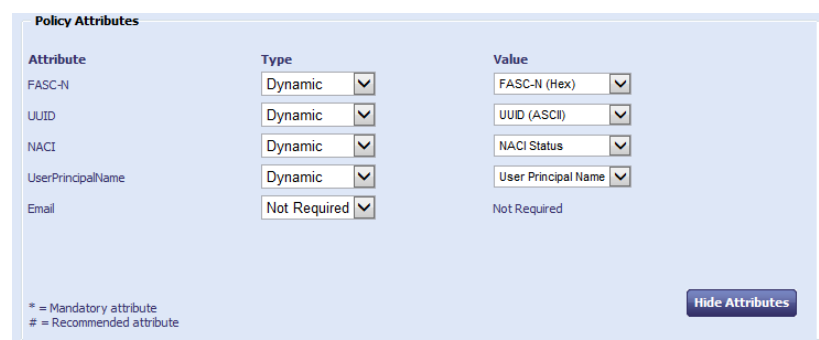
- a) Make the relevant policies available.

**Note:** The selected policies must create certificates that are 2000 bytes or less in size to comply with the PIV specification.

- b) Click **Edit Attributes**.

**Note:** Make sure you have set up your CA to allow editing the policy. See your CA integration guide for details.

- c) Select the value you want to associate with the listed attributes.



Attribute	Type	Value
FASC-N	Dynamic	FASC-N (Hex)
UUID	Dynamic	UUID (ASCII)
NACI	Dynamic	NACI Status
UserPrincipalName	Dynamic	User Principal Name
Email	Not Required	Not Required

\* = Mandatory attribute  
# = Recommended attribute

Hide Attributes

Your CA integration guide contains information about attribute mapping for PIV systems.

See section [5.4.2, FASC-N values](#) for details of choosing the value for the FASC-N attribute.

- d) Click **Hide Attributes** to return to the **Certificate Authority** form.

**Note:** This does not complete the workflow. It is possible to edit attributes for more than one certificate policy.

- e) Set the **Archive Keys** option to **None** for the Authentication, Card Authentication and Digital Signature certificates.
- f) Set the **Archive Keys** option to **Internal** for the Key Management certificate.
- g) Click **Save** to save the changes made and complete the workflow.

## 5.4 Setting up the credential profile

1. From the **Configuration** category, select **Credential Profiles**.
2. Select **PIV Card** from the list available in **Select Profile**.
3. Click **Modify**.
4. Click **Issuance Settings**.

**Note:** PIV systems do not support additional identities. Make sure you do not select the **Issue Additional Identities** option.

For PIV cards, you must select the **Require user data to be approved** option – the option ensures that the cards can be issued only to users who have the *User Data Approved* flag set on their account.

This flag certifies that the applicant has been through the correct enrollment process and has been approved to receive a PIV card. The flag is set when you import an applicant using the Lifecycle API.

The maximum **Lifetime** of a PIV card is six years.

From the **Pre-encode Card** drop-down list, select one of the following:

- ♦ **None** – the card is encoded during activation.
- ♦ **1-Step** – the card is encoded during collection.
- ♦ **2-Step** – the card is encoded using the **Batch Encode Card** workflow after collection.

**Note:** Both **1-Step** and **2-Step** pre-encode card options require activation – select an activation option from the **Require Activation** drop-down list.

5. Click **PIN Settings**.

**Note:** You can modify the PIN policies for PIV cards in the **PIN Settings** section only within certain limits. This means if you make changes to the following settings outside the accepted parameters, they are ignored:

- ♦ **Maximum PIN Length** – the maximum length of PIN for a PIV card is 8.
- ♦ **Minimum PIN Length** – the minimum length of PIN for a PIV card is 6.
- ♦ **Logon Attempts** – you cannot set this option for PIV cards.
- ♦ **PIN Inactivity Timer** – you cannot set this option for PIV cards.
- ♦ **PIN History** – you cannot set this option for PIV cards.

6. Click **PIN Characters**.

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 devices will fail to issue.

For PIV cards, set number to be **Mandatory**, and uppercase letters, lowercase letters, and symbols to **Not Allowed**.

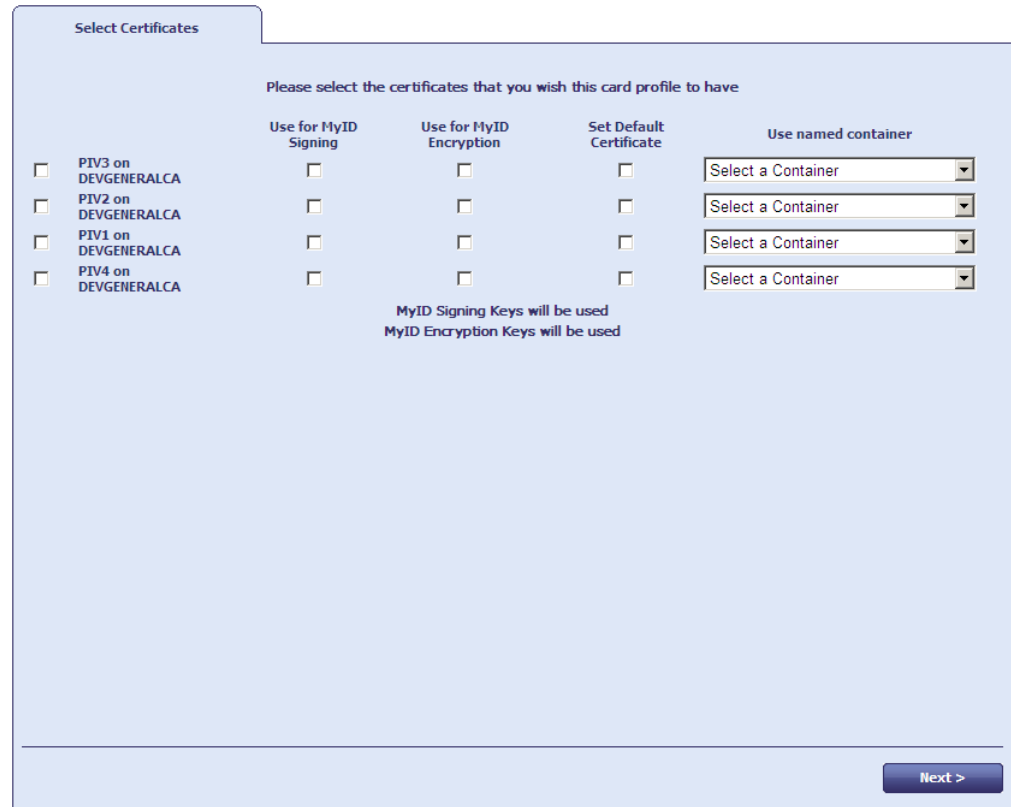
7. Click **Device Profiles**. From the drop-down list, select the **Card Format** you want to use.

The Card Format uses PIV data model files that determine the format of the content of the PIV cards; that is, which data goes in which field.

Choose one of the following card formats:

- ♦ **None** – select this for non-PIV cards.
- ♦ **CBPivDataModel.xml** – used for systems customized for Codebench only.  
If you are using variant cards that do not support iris biometrics, select **CBPivDataModelNoIris.xml** instead.
- ♦ **CivCertificatesOnly.xml** – used for CIV cards that do not require CHUID and applet customization.
- ♦ **PivDataModel.xml** – the standard PIV data model. Use for all standard PIV cards or for non US Federal sites who want to implement a PIV Interoperable (PIV-I) card.  
If you are using variant cards that do not support iris biometrics, select **PivDataModelNoIris.xml** instead.
- ♦ **PivDataModelCompressed.xml** – a data model that uses compressed data.  
If you are using variant cards that do not support iris biometrics, select **PivDataModelCompressedNoIris.xml** instead.

8. Click **Next**.
9. The **Select Certificates** stage is highlighted.



Select Certificates

Please select the certificates that you wish this card profile to have

	Use for MyID Signing	Use for MyID Encryption	Set Default Certificate	Use named container
<input type="checkbox"/> PIV3 on DEVGENERALCA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Select a Container
<input type="checkbox"/> PIV2 on DEVGENERALCA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Select a Container
<input type="checkbox"/> PIV1 on DEVGENERALCA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Select a Container
<input type="checkbox"/> PIV4 on DEVGENERALCA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Select a Container

MyID Signing Keys will be used  
MyID Encryption Keys will be used

Next >

Select the required certificate and assign it to the correct container.

You must select a PIV Authentication certificate and Card Authentication certificate for all smart cards. If the cardholder has a government-issued email account at the time of issuance, you must also select a Digital Signature certificate and a Key Management certificate.

If the card is to be used to log on to MyID, you must select **Use for Signing**. You are advised to use the PIV Authentication Certificate for signing; you cannot use the Digital Signature Certificate.

**Note:** You can issue the PIV Authentication Certificate and PIV Card Authentication certificate only to credentials that contain a PIV applet. See the [Smart Card Integration Guide](#) or other credential guide for details of whether your credentials contain the PIV applet.

Click **Next**.

10. The **Select Applets** stage is highlighted.

Select the applets you want to copy onto the card. Click **Next**.

11. The **Roles** stage is highlighted.

In the **Can Receive** column, select the role you use for applicants.

In the **Can Issue** column, select the roles you want to be able to request cards using this profile.

12. The **Select Card Layout** stage is highlighted.

Select Card Layout

Select the card layouts that will be made available to this card profile.

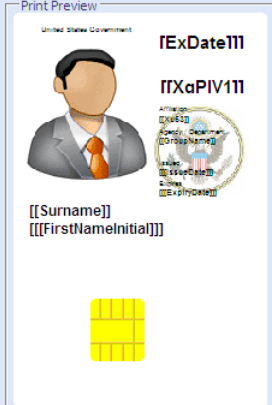
PIV\_CON ☐

PIV\_ERS ☐

PIV\_FOR ☐

PIV\_STD ☒

Print Preview



The label in bold will be used as the default card layout. To change this default, click on the label of the required layout.

Next >

Select the appropriate PIV card layout; for example, **PIV\_STD\_FIPS201\_2**. You can either select multiple card layouts for a single credential profile, or create multiple credential profiles, each of which has a single card layout. You must ensure that you select the correct layout for the type of cardholder.

A selection of sample PIV card layouts are provided:

- ♦ **PIV\_CON\_FIPS201\_2** – a FIPS 202-2-compliant layout for contractors.
- ♦ **PIV\_ERS\_FIPS201\_2** – a FIPS 202-2-compliant layout for emergency response officials.
- ♦ **PIV\_FOR\_FIPS201\_2** – a FIPS 202-2-compliant layout for foreign nationals.
- ♦ **PIV\_STD\_FIPS201\_2** – a FIPS 202-2-compliant layout for standard PIV cards.

The following layouts are also available. These are the original layouts that were designed before FIPS 202-2.

- ♦ **PIV\_CON** – for contractors.

- ♦ **PIV\_ERS** – for emergency response officials.
- ♦ **PIV\_FOR** – for foreign nationals.
- ♦ **PIV\_STD** – standard PIV card layout.

You can select several card layouts to be available in the profile. If so, the issuer selects the layout when printing the card.

You can customize and create new layouts using the **Card Layout Editor** in the **Configuration** category. See the [Administration Guide](#) for details.

13. Click **Next** to complete the workflow.

#### 5.4.1 Updating existing card layouts

The card layouts provided with FIPS201\_2 in their name comply with FIPS 201-2. If you have existing card layouts that you want to use, you must update them to use the correct format.

**Note:** Different manufacturers and models of card printer may print your layouts in different ways, and the layout of different names may cause issues on some printers. You are strongly recommended to test your card layouts, with a variety of names of different lengths, on the appropriate printer before printing production cards.

To update your card layouts from FIPS 201-1 to FIPS 201-2:

1. From the **Configuration** category, select **Card Layout Editor**.
2. For each card layout, edit the format of the name field:
  - a) Open the layout you want to update.
  - b) Delete the **Last Name** and **First Name and Initial** elements from the card layout.
 

These are the elements used for zone 2a and 2b. These have been replaced by a single custom image that formats the full name in zone 2.
  - c) On the toolbar, click **Insert User Image**.
  - d) From the **Image Source** drop-down list, select **fips201name**.
  - e) From the **Template** drop-down list, select **PIV-Front**.
  - f) From the **Zone** drop-down list, select **2: Name**.
  - g) Save the card layout.
3. For each back layout (with a name ending in **\_back**), edit the format of the serial number field and adjust the location of the issuer ID:
  - a) Open the layout you want to update:
  - b) Delete the **Card Serial Number** element from the card layout.
  - c) On the toolbar, click **Insert User Image**.
  - d) From the **Image Source** drop-down list, select **SerialNoFormatter**.
  - e) From the **Template** drop-down list, select **PIV Back**.
  - f) From the **Zone** drop-down list, select **1: Card number**.
  - g) Select the **IssuerID** element.
  - h) From the **Zone** drop-down list, select **None**.
  - i) From the **Zone** drop-down list, select **2: Issuer ID**.
  - j) Save the card layout.
4. For the Emergency Response Official layout (based on PIV\_ERS), change "Emergency Response Official" to "Federal Emergency Response Official":

- a) Open the emergency response official layout.
  - b) Select the bar at the bottom of the screen with the text `Emergency Response Official`.
  - c) Edit the text in the **Content** box to read `Federal Emergency Response Official`.
  - d) Save the card layout.
5. For the standard layout (based on PIV\_STD), add a white stripe with a circled W as the name background:
- a) Open the standard layout.
  - b) Click the Insert Picture button.
  - c) From the list, double-click the **White.jpg** image.
  - d) From the **Template** drop-down list, select **PIV-Front**.
  - e) From the **Zone** drop-down list, select **15: Name background**.
  - f) Right-click the image, then from the pop-up menu select **Send to back**.
  - g) Save the card layout.

**Note:** It is very important that you confirm that any customized layouts you produce are fully compliant with the FIPS 201-2 standards. See your NIST FIPS 201-2 documentation for details.

#### 5.4.2 FASC-N values

There are two methods of providing FASC-N information: FASC-N (ASCII) and FASC-N (Hex). These values are available when you edit the attributes in the **Certificate Authorities** workflow.

The majority of certificate authorities use the Hex version. The ASCII version is currently used only for VeriSign Certificate Authorities.

**Note:** Make sure that you use the correct version for your policy and certificate authority: if you use the wrong version, the certificate fails to issue.

## 5.5 Setting credential numbers

You can use the **Credential Number Per Device** option to enforce a unique credential number for every device issued, whether or not a CredNo value is supplied in the Lifecycle API.

To set the **Credential Number Per Device** option:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **Devices** tab, set the following option:
  - **Credential Number Per Device** – set this option to `Xu48` – this is the controlling field for a standard PIV installation of MyID. When this is set, each device issued by MyID is given a unique credential number from a DeviceCredNo sequence, which starts at value 1.

If you set this flag to a blank value:

- If a credential number is supplied through the Lifecycle API and a card request is made through the Lifecycle API, then the supplied credential number is used. MyID makes no effort to ensure this is a unique value.



- If a card request is made through a workflow in MyID, then the credential number is set to a unique number from a CredNo sequence, which starts at value 250000 for new installations. Any credential number supplied through the Lifecycle API is lost.
- If a card request is made through the Lifecycle API, but the CredNo is not supplied, then card issuance will fail.

3. Click **Save changes**.

## 5.6 Manage agencies

Agency details are managed using four workflows in the **People** category:

- **Add Group**
- **Amend Group**
- **Remove Group**
- **Edit Groups**

**Note:** If you make changes to an agency, the information held within the records of people added before the change was made will not contain the new details. It is important to carefully consider your agency structure and details, as you will either have to manually edit the appropriate people's records or write an SQL script to update them.

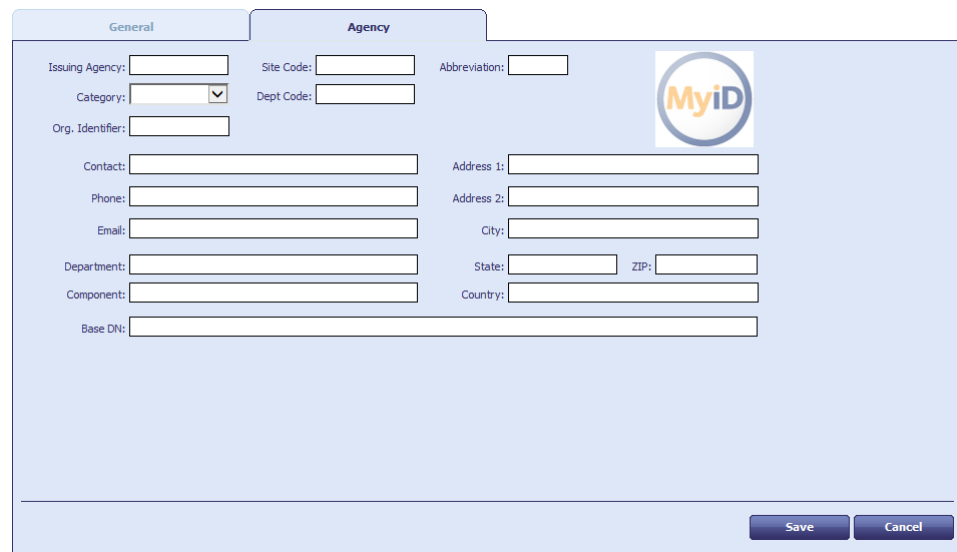
Agencies are used to hold groups of individuals and form the hierarchy of agencies within MyID. Information recorded about agencies forms part of the unique identification number written to a card and so must be created before people can be added to MyID.

### 5.6.1 Add agencies

1. From the **People** category, select **Add Group**.

2. In **Group**, type the name of the agency.
3. Enter a short **Description** for the agency.
4. Click the icon to the right of **Parent Group**. A list of available parent agencies is displayed.
  - ♦ If you are entering details of your top-level agency, select **Root**. The only other options available at this time are MasterAdmin and System Startup, which contains the startup users.

- ♦ If you have already created other agencies, select the one to contain the new agency you are creating.
- 5. Click the icon to the right of **Roles** and select the roles that can be placed in this agency from the list displayed.  
Click **OK**. The number of roles that you have selected is displayed in the **Roles** box.
- Note:** If you do not select any roles, and leave the option displaying **0 Role(s)**, this means that the agency is unrestricted and all roles are available to the agency.
- 6. By default, a new agency is **Enabled**.  
If you set this agency to **Disabled**, you can specify a reason. A “no entry” sign is displayed against the agency when you view it in the **Parent Group** list.
- 7. Click the **Agency** tab.



- 8. In **Issuing Agency**, enter the standard four-character code for the agency issuing the credential.  
For PIV-I and CIV cards, enter 9999.
- 9. Enter the standard **Site Code**.  
For PIV-I and CIV cards, enter 9999.
- 10. Type the **Abbreviation** for the agency to appear on the printed card.
- 11. Select the correct **Category** from the list available (Federal, State, Commercial or Foreign).
- 12. Enter the **Dept Code**, if you have one.
- 13. Type an **Org. Identifier** for the agency. This is the ID code of the applicant's organization. The value depends on the **Category** you specified.

Category	Value
Federal	The agency code (as recorded in <b>Agency Code</b> ).
State	The state code.
Commercial	The code for the company.
Foreign	The numeric country code.

- 14. Click the image to upload an image of the agency's seal.
- 15. If you select **Commercial** as the **Category**, enter the Agency DUNS code in the **DUNS** field.

16. Enter **Contact** information (including the name, **Address**, **Phone** number and **Email** address) for an individual who can answer questions relating to this agency.
17. The **Department** field defaults to the name of the **Parent Group** as defined in the **General** tab. You can change this value if necessary.
18. In the **Component** field, type the component within the agency. This field is optional.
19. Enter the **Base DN** that will be appended to the individual's common name to form the DN of every person added to this agency.

For example: `c=us, o=agency, ou=agency.`

**Warning:** MyID does not validate the information you enter here. Enter the information in comma-separated LDAP format and carefully check the information. An incorrect entry could prevent the issue of cards and certificates to people in this agency.

### Escaping characters in the base DN

MyID assumes that the base DN is correctly escaped; if it is not, any people in that agency will have invalid DNs. To correct this, you must remove the person, correct the agency base DN, then add the person again.

The characters that you must escape are:

`, = + < > \ # ; "`

To use any of these characters, you must enclose them in double quotes. Additionally, you must prefix any " (double quote) or \ (slash) character with a \ (slash).

For example:

`John Smith, Jnr`

should be escaped as

`cn="John Smith, Jnr", o=...`

If you have an `o` value of:

`Smith "Budget" Cars`

this should be escaped as:

`o="Smith \"Budget\" Cars", c=...`

You can now issue cards following the PIV process.

## 5.6.2 Amend agencies

1. Click the **People** category and select the **Amend Group** workflow from the list.
2. Select the agency you want to change from the list and click **Continue**.  
If you have selected the wrong agency, click the icon to the right of **Select a Group** to display the list of agencies again.
3. Information entered when the agency was added can be amended. For further information, see section [5.6.1, Add agencies](#).

**Note:** If you disable an agency, all user accounts within that agency are disabled.

## 5.6.3 Remove agencies

1. Click the **People** category and select the **Remove Group** workflow from the list.
2. Select the agency you want to change from the list.  
If you have selected the wrong agency, click the **Agency** icon to the right of **Select an Agency** to display the list of agencies again.

3. Click **Continue**.
4. Click **Remove**.

**Note:** You cannot remove an agency that contains other entries. Instead, you must use the **Edit Groups** workflow where you will be prompted for a new location for the agency's contents.

#### 5.6.4 Edit agencies

Using the **Edit Groups** option, you can add, rename, edit and remove agencies and import an LDAP directory branch into your agency structure.

1. From the **People** category, click **Edit Groups**.  
Existing agencies are displayed in a tree structure:
  - ♦ Click the plus sign to the left of an agency name to view the agencies nested within it.
  - ♦ Click the minus sign to the left of an agency name to collapse the view, hiding any agencies nested within it.
  - ♦ Click the name of an agency to select it.
2. Right-click the name of a selected agency to display a menu. From here you can:
  - ♦ Add a new agency
  - ♦ Move an agency to a new location in the tree structure
  - ♦ Rename an agency
  - ♦ Import an LDAP branch, choosing whether to:
    - Import an OU and its children
    - Import just the children of an OU
  - ♦ Remove an agency, choosing whether to:
    - Remove an agency, moving any agencies it contains and the users to a new agency
    - Remove the agency and any agencies it contains, moving only the users to a new agency
3. When you have made all the necessary changes, click **Save**.

##### Add a new agency

1. Right-click the name of the agency that you want to contain the new agency.
2. Select **Add**, then **New Group** from the menu.  
A new agency is created, called **New**.  
If the parent agency is closed, you may not see the new agency. Click the **+** sign next to the parent agency to view it.
3. Right-click the name of the agency and select **Rename Group** from the menu.
4. Select the existing name of the agency and enter a new one.
5. Click **Save**.

##### Move an agency

1. Right-click the name of the agency that you want to move.
2. Select **Move Group** from the menu.
3. Click the name of the agency that you want to contain it.

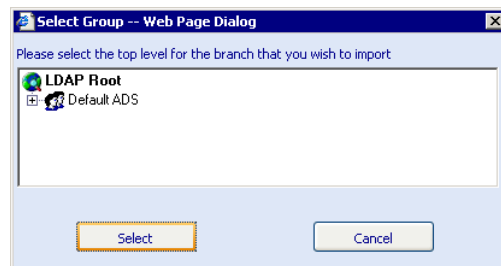
4. Click **Save**.

### Rename an agency

1. Right-click the name of the agency that you want to rename.
2. Select **Rename Group** from the menu.
3. Highlight the existing name of the agency and enter a new name.
4. Click **Save**.

### Import an LDAP branch

1. Right-click the name of the agency into which you want to import a branch from an LDAP directory.
2. Select **Import LDAP Branch** from the menu.
3. Select either:
  - ♦ **OU and Children** to import the agency and all its contents
  - ♦ **Just Children** to import just the contents of the agency
4. The Select Agency dialog is displayed.



Locate and select the Organizational Unit (OU) that you want to import and click **Select**.

5. Click **Save**.

### Remove an agency

1. Right-click the name of the agency you want to remove.
2. Select **Remove Group** from the menu.
3. Select either:
  - ♦ **Remove Group, Move Sub-Groups and Users** to delete the agency but move any sub-agencies and people to another agency.
  - ♦ **Remove Group and Sub-Groups, Move Users** to delete the agency and any sub-agencies within it but move the people to another agency.
4. A message is displayed asking you to confirm that you want to delete the agency. Click **Yes** to continue.
5. The Reparent Users dialog is displayed.  
Click the name of the agency into which you want to move any sub-agencies and people, then click **Select**.
6. Click **Save**.

## 5.7 Batch issuing cards

The **Batch Collect Card** workflow is not available by default to any of the standard roles. If you want to issue cards in a batch, you must add the workflow to one of the roles in the system:

1. From the **Configuration** category, select **Edit Roles**.
2. Make sure **Batch Collect Card** is selected for the role you want to be able to batch issue cards.
3. Click **Save Changes**.


You must also set up MyID to require activation: this allows you to collect the cards, but does not make them available for use – the card must be activated by an operator or the cardholder before it can be used.

See the [Administration Guide](#) for details of the **Require Activation** option.

## 5.8 Requiring facial biometrics

You can configure MyID to check that facial biometrics have been captured before authorizing card issuance.

To set the option:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **Devices** tab, make sure the **PIV Facial Biometrics Required** option is set to Yes .

When you install a new MyID system or upgrade an existing system, this option is initially set to Yes.

3. Click **Save changes**.

You can also set this requirement for each credential profile:

1. From the **Configuration** category, select **Credential Profiles**.
2. Select the credential profile you want to edit and click **Modify**.
3. Click **Issuance Settings**.
4. Set the **Require Facial Biometrics** option to one of the following:
  - ♦ **System Default** – the requirement is based on the **PIV Facial Biometrics Required** configuration option.  
When you upgrade an existing system, the default value for existing credential profiles is **System Default**.
  - ♦ **Always** – facial biometrics are always required for issuance of cards using this credential profile. The **PIV Facial Biometrics Required** configuration option is ignored.
  - ♦ **Never** – facial biometrics are never required for issuance of cards using this credential profile. The **PIV Facial Biometrics Required** configuration option is ignored.
5. Click **Next** and complete the workflow.

You must review your configuration options and credential profile settings to ensure that your system configuration meets your requirements for FIPS 201-2.

## 5.9 Card issuance checks

You can configure MyID to check the following when issuing cards:

- The content signing certificate expiration date.
- The age of the biometric data recorded for the applicant.

To set these options:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **Devices** tab, set the following:
  - ♦ **Check Content Signing Certificate Expiration** – set to Yes ☒ so MyID checks that the PIV content signing certificate will not expire in the lifetime of the card.
  - ♦ **PIV Biometric Maximum Age** – set to the maximum age of the biometric data in years. MyID checks that the biometrics will not exceed this age in the lifetime of the card.
3. Click **Save changes**.

If configured, these checks are performed when a card is presented for issuance. In the event of either of these checks failing, MyID will prevent the issuance of the card. In this situation, it will be possible to collect the issuance job later, after the underlying reason for failure has been corrected.

## 5.10 Displaying logon names

You can configure MyID to display or hide the applicant's full name on the logon screen.

To set the option:

1. From the **Configuration** category, select **Security Settings**.
2. On the **Logon** tab, set the **Show Full Name at Logon** option to Yes ☒ to display the applicant's name, or No ☒ to hide the applicant's name on the logon screen.
3. Click **Save changes**.

## 5.11 Preserving FASC-N and UUID

MyID allows you to prevent changes to the CHUID on the card during repersonalize and reinstate card operations – the FASC-N and UUID are preserved.

To set the option:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **Devices** tab, set the **Preserve FASCN and UUID for card update** option to Yes ☒ to prevent the FASC-N and UUID from being changed, or No ☒ to generate new FASC-N and UUID values during card repersonalization and reinstatement.

**Note:** Setting this option to No does not meet the requirements of FIPS 201-2.

3. Click **Save changes**.

## 5.12 Approval of users on renewal and replacement

MyID allows you to configure whether you need to re-enroll or re-approve the cardholders when you renew or replace their cards.

It is a requirement of FIPS 201-2 that you carry out the enrollment process again when you renew or replace cards, including capturing fresh biometrics, so in this release these configuration options are set to Yes to require re-enrollment. If you set these options to No, you must be aware that you are no longer compliant with FIPS 201-2.

To set the options:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **Identity Checks** tab, set the following:
  - ♦ **Applicants Re-Approve for Card Renewal** – set to Yes ☒ to require re-enrollment for card renewals, or No ☐ to allow renewals without re-enrollment.
  - ♦ **Applicants Re-Enroll for Card Replacement** – set to Yes ☒ to require re-enrollment for card replacements, or No ☐ to allow replacements without re-enrollment.
3. Click **Save changes**.

The effect of these configuration flags is to set the card issuance approved flag on the cardholder's account to No, requiring the user to go through the enrollment process again to allow the replacement or renewal of their card.

If you attempt to request a replacement for your own card through the Kiosk, for example, an error similar to the following appears:

```
An error has occurred.
```

```
The user account data must be approved before credentials can be issued or updated. Please contact an Administrator.
```

In addition, if your system is configured for adjudication, these flags reset the adjudication flags on the cardholder's account, requiring them to go through the adjudication process again.

## 5.13 Card renewal period

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.

To set the card renewal period:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **Devices** tab, set the following:
  - ♦ **Card Renewal Period** – set this to the number of days before expiry when cards become available for renewal.
3. Click **Save changes**.



## 5.14 Authenticating users

The **Authenticate Person** workflow allows a MyID operator to authenticate the identity of a cardholder. The authentication is recorded in the MyID audit trail.

This workflow allows you to carry out authentication when required to by your process; for example, for FIPS 201-2, you must confirm the identity of the cardholder before carrying out changes on their card.

**Note:** MyID does not enforce the authentication of cardholders for operator-led workflows, but by recording the details of the authentication in the audit trail it allows you to verify that your operators have been following the process correctly.

The **Authenticate Person** workflow allows the following methods of authentication:

- **Match Enrolled Fingerprints** – the operator guides the cardholder through providing their fingerprint biometrics. The fingerprint is matched against the enrolled fingerprints in the MyID database.
- **Identity Documents** – the operator checks the details of the provided identity documents and records their details, including expiry dates and serial numbers.
- **Security Phrases** – the operator asks the user their security questions. For more information on setting the number of security phrases required to authenticate, see the **Number of security questions for operator authentication** option in the [Administration Guide](#).
- **Operator Approval** – if the cardholder cannot provide fingerprints, identity documents, or provide their security phrases, the operator can override the check. The operator *must* provide a reason why they are providing approval.

You can control which methods of authentication are available to operators using the **Edit Roles** workflow. Underneath the **Authenticate Person** workflow in the list of available options, you can select which methods are available to operators with that role:

Authenticate Person	<input checked="" type="checkbox"/>
Match Enrolled Fingerprints	<input checked="" type="checkbox"/>
Identity Documents	<input checked="" type="checkbox"/>
Operator Approval	<input checked="" type="checkbox"/>
Security Questions	<input checked="" type="checkbox"/>

To authenticate a cardholder:

1. From the **People** category, select **Authenticate Person**.
2. In the Find Person screen, type the details of the person you want to authenticate, then click **Search**.
3. Select the person you want to authenticate from the list of search results.

Authenticate Person

Select Authentication Mechanism

☐ Match Enrolled Fingerprints
 ☐ Identity Documents
 ☐ Operator Approval
 ☐ Security Phrases

Please provide any further comments, especially if the Authentication is rejected

Comments:

< Back

Authenticate

Reject

Cancel

4. Select the authentication mechanism.

The list of available authentication mechanisms is determined by your MyID role permissions.

For **Match Enrolled Fingerprints**:

Authenticate Person

Select Biometric Reader: Crossmatch PIV Verifier

Capture:

1 - Preferred

2 - Suitable

N - Not suitable

Please provide any further comments, especially if the Authentication is rejected

Comments:

< Back

Authenticate


Reject

Cancel

Select the fingerprint you want to match, and guide the cardholder to use the fingerprint scanner.

## For Identity Documents:

### Authenticate Person



Title:

Issued by:

Number:

Expiration:

Title:

Issued by:

Number:

Expiration:

Select Authentication Mechanism

☐ Match Enrolled Fingerprints
 ☒ Identity Documents
 ☐ Operator Approval
 ☐ Security Phrases

Please provide any further comments, especially if the Authentication is rejected

Comments:

< Back

Authenticate

Reject


Cancel

Record the details of two identity documents provided by the cardholder, including:

- ♦ **Title** – the type of document.
- ♦ **Issued by** – the issuer of the document.
- ♦ **Number** – the serial number of the document.
- ♦ **Expiration** – the expiration date of the document.

## For Operator Approval:

### Authenticate Person



Please provide the steps taken to identify jane.smith, including the reasons why this was done manually.

Comments:

Select Authentication Mechanism

☐ Match Enrolled Fingerprints
 ☐ Identity Documents
 ☒ Operator Approval
 ☐ Security Phrases

Please provide any further comments, especially if the Authentication is rejected

Comments:

< Back

Authenticate

Reject

Cancel

Provide the details of your manual authentication of the cardholder. Include as many details as possible as to why the cardholder could not provide fingerprints or identity documents.

For **Security Phrases**:

**Authenticate Person**

**Shared Secrets**

Question	Answer
Password	<input type="text"/>
Mothers maiden name?	<input type="text"/>

**Verify Secrets**

**Select Authentication Mechanism**

- ☐ Match Enrolled Fingerprints
- ☐ Identity Documents
- ☐ Operator Approval
- ☒ Security Phrases

**Comments:** Please provide any further comments, especially if the Authentication is rejected

**< Back** **Authenticate** **Reject** **Cancel**

Ask the user their security questions and type the answers, and click **Verify Secrets**.

The number of questions you need to ask is independent of the number of questions the user has stored in the system – for example, the user may have four questions stored, and you may be required to ask two of them for operator-led authentication.

For more information on setting the number of security phrases required to authenticate, see the **Number of security questions for operator authentication** option in the [Administration Guide](#).

5. Type your comments in the **Comments** box. These comments are included in the MyID audit trail.
6. Click **Authenticate** to approve the cardholder's identity or **Reject** if you are not satisfied.

## 5.15 Editing PIV applicants

The **Edit PIV Applicant** workflow allows you to edit the details of applicants. You can add applicants to MyID in the following ways:

- Enroll using the Lifecycle API.
- Manually add using **Edit Person** and assign the PIV Applicant role.
- Import from a directory using **Person Import** and assign the PIV Applicant role.
- Import from a directory using **Edit PIV Applicant** and assign the PIV Applicant role.

**Note:** If you import a user from a directory, and have set up directory synchronization, the MyID applicant records can be updated by changes in the directory.

The PIV Applicant Editor role is created by default, and has access to the **Edit PIV Applicant** and **Edit Person** workflows. This role is also set as the manager for the PIV Applicant role, which means that you *must* have the PIV Applicant Editor role to assign the PIV Applicant role to any users.

Assign the PIV Applicant Editor role to the operators you want to be able to edit the details of applicants, and to be able to assign the PIV Applicant role to applicants.

**Note:** You must make sure that your business processes still meet the requirements for FIPS 201 (if applicable). You may want to restrict or prevent access to editing a PIV applicant's details after enrollment.

## 5.15.1 Editing PIV applicants

To edit a PIV applicant:

1. From the **People** category, select **Edit PIV Applicant**.

2. Use the Find Person screen to enter the search criteria for the applicant you want to edit, then click **Search**.

You can use the **User Data Approved** field to search for applicants.

3. Select the applicant from the list of results.

4. Edit the applicant's details on the **Personal** tab.

See the [Administration Guide](#) for details of the standard user account details as available in the **Edit Person** workflow. The additional PIV-specific fields are:

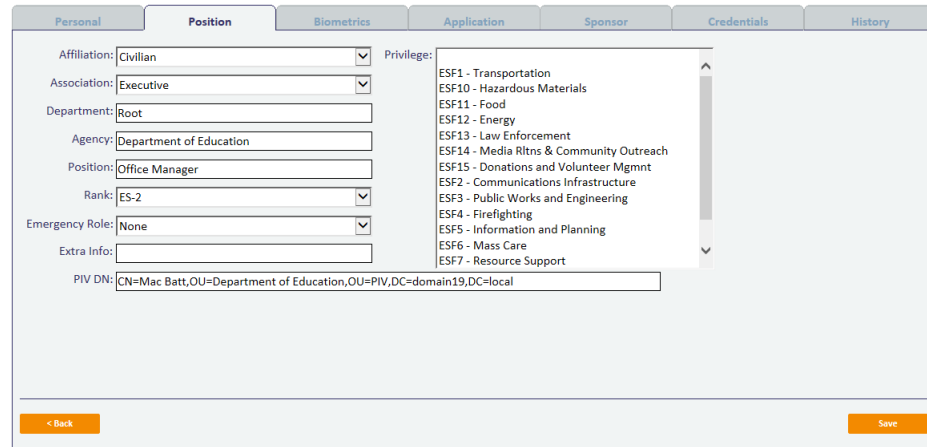
- ♦ **Nickname** – If the applicant is known by a nickname, you must enter it. For example, the applicant's first name may be James but he may be known as Jim. Enter Jim as the applicant's nickname.
- ♦ **Suffix** – used for names with a suffix; for example, Jr.
- ♦ **D.O.B.** – select the applicant's date of birth.
- ♦ **Security** – a unique person identifier. For a PIV user (that is, a user who belongs to an agency that does not have a code of 9999) this value is used for the PI (Person Identifier) value in the FASC-N. Due to restrictions on the PI field in the FASC-N, this identifier must be a maximum of 10 numeric digits.
- ♦ **NACI Status** – records the status of the NACI check.

**Note:** You must use this only in accordance with FIPS 201-2 guidelines. For PIV-I and CIV, set this to **Not Required**.

- ♦ **User Data Approved** – if the credential profile has the **Require user data to be approved** option set (this is required for PIV cards) the cards can be issued only to users who have the **User Data Approved** flag set on their account.

This flag certifies that the applicant has been through the correct enrollment process and has been approved to receive a PIV card.

5. Click the **Position** tab.



The screenshot shows the 'Position' tab in the Intercede system. The form includes the following fields and options:

- Affiliation:** Civilian (dropdown)
- Association:** Executive (dropdown)
- Department:** Root (text input)
- Agency:** Department of Education (text input)
- Position:** Office Manager (text input)
- Rank:** ES-2 (dropdown)
- Emergency Role:** None (dropdown)
- Extra Info:** (text input)
- PIV DN:** CN=Mac Batt,OU=Department of Education,OU=PIV,DC=domain19,DC=local (text input)
- Privilege:** A list of privileges including ESF1 - Transportation, ESF10 - Hazardous Materials, ESF11 - Food, ESF12 - Energy, ESF13 - Law Enforcement, ESF14 - Media Rltns & Community Outreach, ESF15 - Donations and Volunteer Mgmt, ESF2 - Communications Infrastructure, ESF3 - Public Works and Engineering, ESF4 - Firefighting, ESF5 - Information and Planning, ESF6 - Mass Care, and ESF7 - Resource Support.

At the bottom of the form are two buttons: '< Back' and 'Save'.

- ♦ **Affiliation** – the cardholder's role or position within the organization; for example, Contractor or Emergency Responder.
- ♦ **Association** – indicates how the cardholder is associated to the agency; for example, Employee or Contractor. These options are defined by FIPS 201.
- ♦ **Department** – the department's name within the agency.
- ♦ **Agency** – the group name from the **Personal** tab.
- ♦ **Position** – the position of the applicant within the agency.
- ♦ **Rank** – the rank of the applicant.
- ♦ **Emergency Role** – the specific role in the event of an emergency of the applicant, if any.
- ♦ **Extra Info** – contains any extra information about the applicant's position.
- ♦ **Privilege** – select the applicant's privileges from the list. This is agency-specific data that can be printed on the card.
- ♦ **PIV DN** – the distinguished name for the user.

If the applicant's PIV DN field in the database is empty when you edit the account in this workflow, MyID automatically populates the **PIV DN** field from the Base DN of the applicant's group and the applicant's name; this value is saved to the database when you complete the workflow.

6. Click the **Biometrics** tab.

The screenshot shows the 'Biometrics' tab in the Intercede user management interface. It includes a 'Camera Type' dropdown set to 'Canon EOS', a user photo, and an 'Iris Captured' status with a green checkmark. A legend indicates finger capture status: N (Not captured), P (Print taken), R (Roll taken), U (Finger unprintable), and M (Finger missing). Two hand diagrams show which fingers are marked with 'P'. Below the hands are input fields for Height (6' 0"), Weight (160 lbs), Gender (Male), Hair (Blonde), Eyes (Brown), and Race (White). Navigation buttons for '< Back' and 'Save' are at the bottom.

- ◆ To use Aware PreFace to capture the user's facial biometrics, select the **Camera Type** from the drop-down list then click the user image.
- Note:** If you want to use Aware PreFace, contact customer support, quoting reference SUP-228.
- ◆ The **Iris Captured** option provides a read-only indication of whether iris data has been imported for the user.
  - ◆ To capture a signature using a signature pad, click the signature placeholder and use the Image Capture dialog to upload a signature.



- ◆ To capture fingerprints, click the finger image.

See your biometric integration guide for details of setting up and using fingerprint biometrics.

When you click the finger image, the workflow prompts you to capture fingers until the configured number of fingerprints have been captured. You can choose to skip fingers once this process has begun.

The preferred order of taking fingerprints, taking into account fingers that are most suitable for the majority of users, is:

- Right index
- Left index
- Right middle
- Left middle
- Right thumb
- Left thumb
- Right ring

- Left ring
- Right little
- Left little

You are recommended to start with the right index finger and proceed with the capture as directed. The capture stops once it has captured (or skipped) the "Left little" finger and the minimum number of fingers have been captured.

You can skip fingers that cannot be captured (due to injury or other special circumstances).

- ◆ Record the applicant's **Height** in feet and inches. You can enter the two sets of digits separated by a space and the units will automatically be applied.

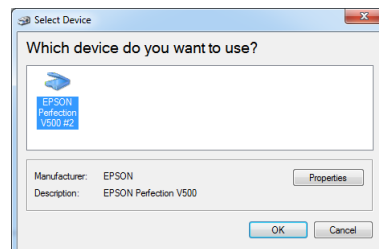
For example, if the applicant is 5 feet 10 inches tall, you can enter 5 10. This will be correctly displayed as 5'10".

- ◆ Enter the applicant's **Weight** in pounds. For example, if the applicant weighs 154 pounds, enter 154.
- ◆ Select the applicant's **Gender** from the list.
- ◆ Select the color of the applicant's **Hair** and **Eyes** from the list of options.
- ◆ Select the applicant's **Race** from the list.

7. Click the **Application** tab.

You can provide scans of two identity documents and an SF85 or OPM form.

To scan a document, click the image placeholder, then select the scanner you want to use in the Select Device dialog.

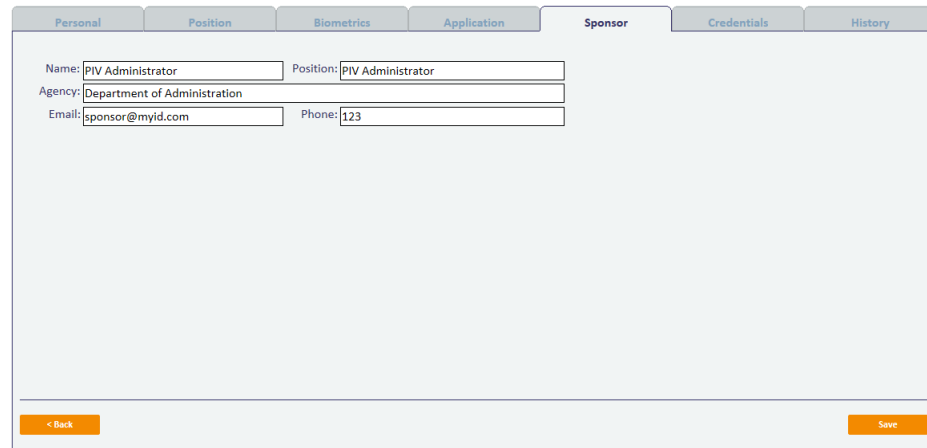


Complete the additional data for the identity documents:

- ◆ **Title** – select the document type. Only documents of the types listed are acceptable as proof of identity.
- ◆ **Issued by** – enter details of the organization that issued the document.
- ◆ **Number** – the document's serial number.
- ◆ **Expiration** – the expiration date of the document.



- ♦ Select the **Nationality** and **Place of Birth** of the applicant.
8. Click the **Sponsor** tab.



This tab records details of the applicant's sponsor. These details are visible in **View Person** and during card issuance approval.

9. The **Credentials** and **History** tab allow you to view the same details as the **Edit Person** and **View Person** workflows. You cannot change any details.
10. Click **Save**.

### 5.15.2 Adding PIV applicants from a directory

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

The user must belong to an LDAP group that is mapped to an existing MyID group, and the **Search a Directory** option (on the **LDAP** page of the **Operation Settings** workflow) must be set to **Yes** or **Ask**.

If you use the Find Person stage of the **Edit PIV Applicant** workflow to select a user who is not already in the MyID database, the user is imported, given the Cardholder and PIV Applicant roles, and assigned to the group that matches their LDAP group. You can then edit the user's details as normal.

To add PIV applicants from a directory, you must set up the groups in MyID before you begin:

- Both the LDAP group the PIV applicant belongs to, and the parent LDAP group, must have been imported from LDAP into MyID. The hierarchy between the group the user belongs to and the parent group must be the same in both MyID and the LDAP. There are various ways to achieve this:
  - ♦ In the **Edit Groups** workflow, select **Import LDAP Branch/OU and children** to import a group above the group the user belongs to. This will ensure that the hierarchy of the group and parent group is consistent in both MyID and LDAP.
  - ♦ Alternatively, you can create the parent group first, then import the group the user belongs to as a child of the parent group.
  - ♦ If this hierarchy of group and parent group is not set up correctly, you will see the following error when trying to import users from LDAP in the **Edit PIV Applicant** workflow:
 

```
Target is not associated with a MyID group
```
- Additionally, you must ensure that the PIV attributes have been configured for the group that the MyID user belongs to; you can do this using the **Amend Group** workflow.

- The logged on user must have the PIV Editor role and access to the **Edit PIV Applicant** workflow to import users from LDAP using the **Edit PIV Applicant** workflow.

## 5.16 Remote PIN Management utility for PIV cards

The `MyIDCardUtility.exe` program allows you to carry out a remote unlock or change the PIN on a PIV card.

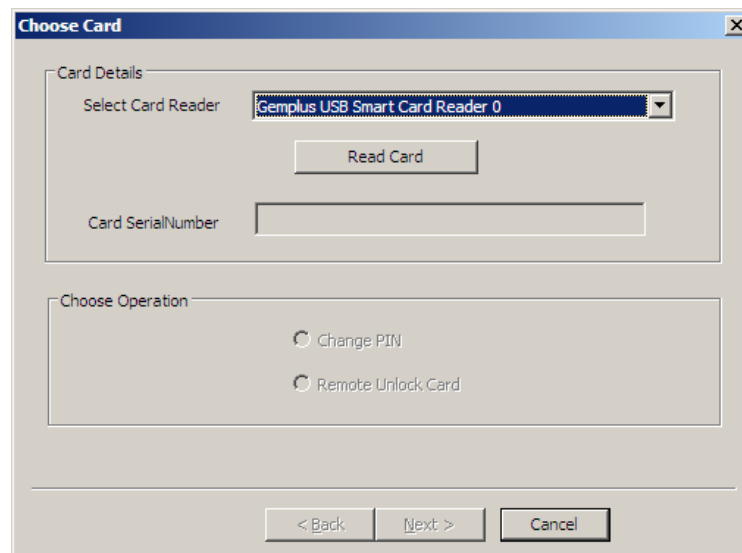
This utility has been developed with Oberthur (PIV cards and ID-One PIV cards) and Gemplus PIV cards.

This utility is installed to the `Utilities` folder on the MyID application server. You can copy this utility manually to any client PC you want to be able to use the functionality.

To use the card utility:

1. Copy the `MyIDCardUtility.exe` file to the client PC.
2. In Windows Explorer, double-click the `MyIDCardUtility.exe` file.

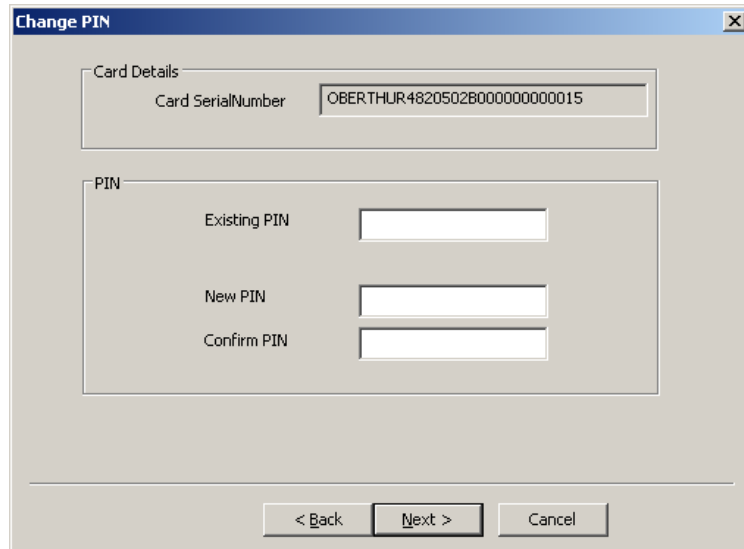
You can also set up a shortcut to run this utility.



3. If you are using multiple card readers, select the appropriate reader from the **Select Card Reader** drop-down list.
4. Click **Read Card**.  
The utility reads the card, and the card serial number appears.
5. Select one of the following options:
  - ♦ **Change PIN**
  - ♦ **Remote Unlock Card**

To change the PIN:

- a) Click **Change PIN**.
- b) Click **Next**.



**Change PIN**

Card Details

Card SerialNumber: OBERTHUR4820502B000000000015

PIN

Existing PIN:

New PIN:

Confirm PIN:

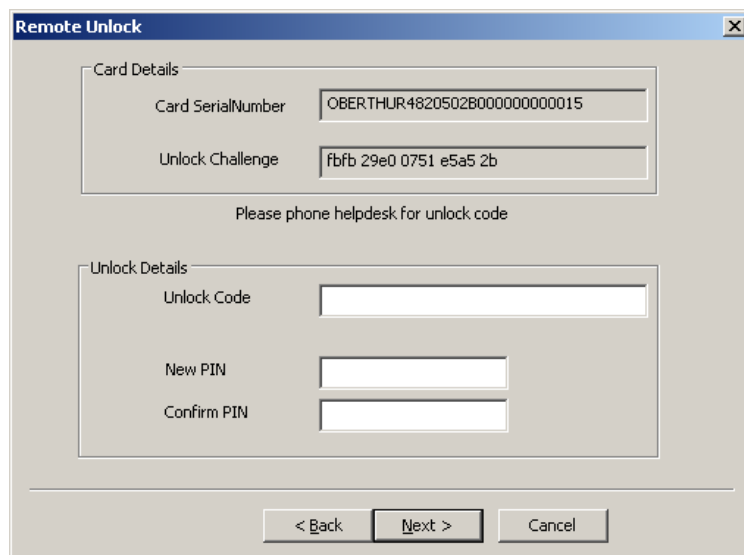
< Back   Next >   Cancel

- c) Type the card's **Existing PIN**.
- d) Type the **New PIN**, and confirm the new PIN in the **Confirm PIN** box.
- e) Click **Next**.

The card PIN is changed.

To remote unlock the card:

- a) Click **Remote Unlock Card**.
- b) Click **Next**.



**Remote Unlock**

Card Details

Card SerialNumber: OBERTHUR4820502B000000000015

Unlock Challenge: fbfb 29e0 0751 e5a5 2b

Please phone helpdesk for unlock code

Unlock Details

Unlock Code:

New PIN:

Confirm PIN:

< Back   Next >   Cancel

- c) Call the helpdesk and provide the **Unlock Challenge**.
- d) The helpdesk operator must then open MyID, go to the **Unlock Credential** workflow, and type the **Unlock Challenge** into the **Challenge Code** boxes before clicking Confirm.

The helpdesk operator can then read out the unlocking code.

See the [Administration Guide](#) for details of using the **Unlock Credential** workflow.

- e) Type the unlocking code from the helpdesk operator into the **Unlock Code** box.
- f) Type a **New PIN** and confirm the new PIN in the **Confirm PIN** box.

- g) Click **Next**.

The card is unlocked, and is given a new PIN.

## 6 Card Layout and Printing

MyID lets you specify the physical appearance of the smartcards it issues, which can be printed using a desktop card printer (CPS.3). This section provides guidelines for producing FIPS 201 compliant ID cards and references the Graphical Personalization Approval Procedure published by the US General Services Administration (GSA).

The Zones referred to are the areas on the card referred to in FIPS 201. The GP and CPS numbers are the associated GSA FIPS 201 Evaluation Program requirements.

**Note:** If you are sending card requests to an external bureau, the layout and printing of the cards is controlled by the bureau.

### 6.1 Printers, cards and consumables

We recommend that you use a high quality color desktop card printer offering indirect (print-to-film rather than print-to-card) printing technology. The card printer must not deposit debris on the printer rollers during printing and laminating (CPS.1). Laminating material must include a 'window' that avoids obstructing the smart card contacts (CPS.2). You should also check that your chosen printer is compatible with dual interface cards (i.e. ones containing contactless chip technology) (CPS.4).

The printer should have a 'yield rate' of at least 98% (CPS.5), and support at least 300dpi resolution (CPS.6); see your printer vendor for details.

Using an ISO-7810 compliant security laminate (preferably a custom design) complies with GSA requirements GP.1 / CPS.7 and GP.2 / CPS.8 for anti-counterfeiting security features. Embossing units must NOT be used (GP.3, CPS.9) and you must not apply decals to the cards (GP.4, CPS.10).

You may obtain cards from any of our supported vendors but you must verify that the cards you choose have passed GSA approval for FIPS 201. If you need cards that include a magnetic strip, these must be high coercivity types (GP.31) and placed in accordance with ISO-7811 (GP.32)

### 6.2 Card content and layout

#### 6.2.1 General

Attributes in MyID can be mapped to each of the data fields referenced in the sample card layouts in FIPS 201. These attributes may be populated during face-to-face registration, either using MyID enrollment or by importing from an external Identity Management System (IDMS). The Card Layout Editor in MyID maps these attributes to the correct location (zone) on the card surface.

MyID provides templates for some of the permitted layouts, to help you to achieve a compliant design. Please refer to FIPS 201 for the permitted content, size and position of each field when designing your card layouts and take care when aligning content to ensure it matches the guides precisely. MyID supports all of the attributes and zones required for SP800-104 compliance, with sample card layouts for each recommended category of cardholder.

MyID also includes a PIV layout template that defines the size, position and expected attribute mapping for each of the recognized zones. When defining a card layout, select this template from the list and then pick the appropriate zone for each of the attributes you need to display. Each item will be automatically positioned to match the standard.

Unless otherwise stated, set text labels to be 5 points (GP.41 / CPS.47) and data fields to be 6 points in height (GP.42 / CPS.48). All text must be in Arial font.

## 6.3 Specific field data – front of card

### 6.3.1 Zone 1 – Photograph (GP.5 / CPS.11)

Photographs of applicants may be captured within MyID (either from a camera or scanner) or imported from an external enrollment application. To comply with FIPS 201, it must be possible to print the photograph at a size of 37mm x 27.75mm, at a resolution of at least 300 dpi. This means that the image must be at least 437 x 328 pixels. For a 640x480 pixel resolution webcam, you must use a nearly full-frame height to meet this condition; so position your camera and subject accordingly.

MyID copes with much higher resolution images and scales them to fit the region on the card.

**Note:** If you are using images from an external source, you must ensure that they meet the requirement for an aspect ratio of 0.75. MyID retains the aspect ratio of the original image when placing it into the zone on the card.

### 6.3.2 Zone 2 – Name (GP.6 / CPS.12)

If you change the display of Zone 2, keep the text size at 10 point (GP.8 / CPS.14).

**Note:** MyID prints the name in uppercase. (GP.7 / CPS.13)

Additional formatting is carried out by MyID to ensure the name matches the requirements defined in FIPS-201-2 section 4.1.4.1.

### 6.3.3 Zone 8 – Employee Affiliation (GP.9 / CPS.15)

This zone should be associated with the **Employee Affiliation** attribute in MyID and represents the relationship between the cardholder and the Agency.

By default, the registrar may select one of the following values: 'Contractor', 'Civilian', 'Active Duty', 'Foreign National'. You may change the list using the MyID **List Editor** configuration option.

**Note:** Employee Affiliation is independent of both the Person / Organization Association field and the Roles assigned to each applicant.

### 6.3.4 Zone 10 – Organizational Affiliation (GP.10 / CPS.16)

This zone is used to display the name of the agency to which the cardholder is affiliated and must be taken from the name of the MyID Agency to which the cardholder belongs.

### 6.3.5 Zone 14 – Expiration date (GP.11 / CPS.17)

This area displays the date the card expires – this is the 'ValidUntil' property of the card. MyID automatically formats this as YYYYMMDD, to be FIPS 201 compliant.

### 6.3.6 Zone 3 – Signature (GP.14 / CPS.20)

This (optional) area displays the cardholder's signature. You may enter the signature at enrollment either by scanning a document or using a signature capture tablet.

### 6.3.7 Zone 4 – Agency-specific text (GP.15 / CPS.21)

This (optional) area can be used for additional data you need to place on the card.

- 6.3.8      **Zone 5 – Rank (GP.16 / CPS.22)**
- This zone should be associated with the **Rank** attribute of the cardholder.
- 6.3.9      **Zone 6 – 2D barcode (GP.17 / CPS.23)**
- MyID requires additional configuration to support 2D barcodes. Please contact customer support quoting reference SUP-155 for more information.
- 6.3.10     **Zone 9 – Header (GP.18, 19 / CPS.24, 25)**
- The header may either contain static text (“United States Government”) or, for emergency responder credential profiles, the cardholder’s responder role. The list of permitted emergency responder roles can be changed by using the MyID **List Editor** configuration option.
- 6.3.11     **Zone 11 – Agency Seal (GP.20, 21 / CPS.26, 27)**
- The Agency Seal is an image (jpeg, bmp or gif). It can be uploaded using the **Upload Image** option in the **Card Layout Editor** and then placed on the layout as a static image in the appropriate zone. Where multiple seals are required though, a better option is to associate this zone with the Agency Seal attribute (xg18) of each Agency.
- Note:** If you want to replace the seal in the predefined layouts, you can overwrite the `USASeal2.gif` image in `upimages\UpImagesEditor`.
- It must be easy to read the text printed on top of the seal, so you should use a ‘faded’ image. Adjust the image (using any suitable image editor) to increase the brightness and reduce contrast. FIPS 201 diagram 4-2 suggests initial settings of 65% brightness and 25% contrast, but you may need to experiment with your graphics editing package for best results.
- Once you have added the image, move it to the back, so that the data fields are visible above it – right-click the image and select **Move to back**.
- 6.3.12     **Zone 12 – Footer (GP.22, 23 / CPS.28, 29)**
- You may use this zone for cards issued to Emergency Responders. If so, it must contain the static text “Federal Emergency Response Official”. If you do this, you may also use Zone 9 to indicate the responder’s role. You are recommended to use the lower of the two locations for this zone, so that you do not block the use of Zone 17.
- This zone can also be used to show the nationality of foreign workers. The Nationality attribute provides a pick list of the ISO 3166-1 3-character country codes for this purpose. (CPS.55)
- 6.3.13     **Zone 13 – Issue Date (GP.24 / CPS.30)**
- This area displays the issue date of the card – this is the ‘ValidFrom’ property of the card. MyID automatically formats this as YYYYMMDD, in order to be FIPS 201 compliant.
- 6.3.14     **Zone 15 – Background for Name (GP.25, 26, 27 / CPS.31, 32, 33)**
- This zone is the background for the ‘Name’ field and may be used as a color-coded indication of the cardholder’s role. You do not have to use it, but if you do you must follow the color scheme stated by FIPS 201 and SP800-104.
- Note:** Do not use the reserved colors for other purposes.
- Blue (0,255,255) – foreign nationals (CPS.65)

Red (254,92,79) – emergency responders (deprecated by SP800-104) (**CPS.66**)

Green (203,255,203) – contractors (**CPS.64**)

White (255,255,255) – others (**CPS.63**)

To apply a color to the zone, insert a static image of the correct color. You may need to use differential scaling to make it fit – hold the 'Alt' key while you drag the lower right corner of the image into place. MyID supplies standard solid colored images for you to use. If you prefer a graduated background, create a suitable image in a graphics editor of your choice and upload it to the **Card Layout Editor**. The **White.jpg** image provided for standard layouts contains a circled W. MyID also includes correctly colored and sized images for the SP800-104 compliant Contractor and Foreign schemes, with the 'B' and 'G' zone 18 designators included. (**CPS.56, 57, 58**)

Once you have added the image, move it to the back, so that the **Name** field is visible above it – right click and select **Move to back**.

There are three overlapping attributes that relate to a cardholder's position. These are:

1. The cardholder's role, which is set by the registration officer at enrollment and may be extended by the system administrator. Roles determine which credential profiles, and therefore card layouts, can be used for a cardholder. The list of roles should include any that need a color-coded card layout. By default, roles are provided for Foreign National, Contractor and Emergency Responder.
2. The Person/Organization Association Category (POA) has fixed values defined by the FASC-N field construction rules, which are: Employee, Civil, Executive Staff, Uniformed Service, Contractor, Organizational Affiliate, and Organizational Beneficiary. This list should not be altered or extended.
3. The Employee Affiliation is a value from a list defined by each agency. Examples include 'Contractor', 'Civilian', 'Active Duty', and 'Foreign National'. You may edit this list to add or remove entries to suit your needs.

These lists overlap, with the same values appearing in more than one. MyID separates the fields for maximum flexibility.

### 6.3.15 Zone 16 – Photo Border (**GP.29 / CPS.35**)

The photo border is a rectangular image, slightly larger than the photograph and located behind the photo placeholder to avoid any possible overlap (**GP.28 / CPS.34**). Follow the same guidelines as for Zone 15. Note that the use of this border is no longer advised by SP800-104.

### 6.3.16 Zone 17 – Agency Specific Data (**GP.30 / CPS.36**)

This zone may be used for your own data – the example given in FIPS 201 cites 'Privilege' as a typical use. You can map whichever fields you want into this zone, but for your convenience, MyID provides a 'Privilege' text field for this purpose. Note that this field overlaps zones 3 & 12, so cannot be used if these zones are in use.

### 6.3.17 Zone 18 – Color Designator (**SP800-104**)

The color indicator (B or G in a white circle) should be included within the image used for Zone 15, since this results in the best anti-aliased representation. Suitable images are provided.

### 6.3.18 Zone 19 – Expiration Date (large) (**SP800-104**) (**CPS.59, 60**)

A second, large typeface expiration date is needed for SP800-104 compliance. MyID will automatically format the date for this zone as MMMYYYY if you associate it with the "Ex Date" attribute. This should be set to 12pt bold text.



### 6.3.19 Zone 20 – Organizational Affiliation Abbreviation (**SP800-104**) (**CPS.61, 62**)

The 3 character abbreviation of the cardholder's organization is shown in zone 20. This may either be static text, or mapped to the Agency Abbreviation attribute (XgPIV1). This should be set to 12pt bold text.

## 6.4 Specific field data – back of card

### 6.4.1 Zone 1 – Agency Card Serial Number (**GP.12 / CPS.18**)

The card serial number should be entered in this zone.

### 6.4.2 Zone 2 – Issuer identification (**GP.13 / CPS.19**)

The issuer identification should contain the Issuer ID.

### 6.4.3 Zone 4 – Return To (**GP.33 / CPS.39**)

This is optional – position the static text you want to print in this zone.

### 6.4.4 Zone 5 – Physical Characteristics (**GP.34 / CPS.40**)

This zone can be used to display the Height, Weight, Hair Color and Eye Color of the cardholder. Associate a dynamic text field with the appropriate user attribute in the card layout editor.

### 6.4.5 Zone 6 – Additional Language (**GP.35 / CPS.41**)

MyID does not reserve an attribute for this purpose. You may choose to use one of the 'general purpose' fields for this (Privilege, Additional Information).

### 6.4.6 Zone 7 – Section 499 Title 18 (**GP.36 / CPS.42**)

This zone should contain static text stating the standard section 18 terms of use statement:

This credential is the property of the U.S. Government. Counterfeiting, altering or misusing violates Section 499, Title 18 of the U.S. Code.

### 6.4.7 Zone 8 – Linear Barcode (**GP.37, 38, 39 / CPS.43, 44, 45**)

MyID supports linear 3 of 9 barcodes. Barcode text is automatically prefixed and suffixed with the "\*" character as required by AIM standards. Check characters are not included; these can be added through scripted extensions if required. You may need to adjust the end points of the region to avoid printing over the contactless chip area (although we have no evidence to suggest that this will impair the function of the chip in any way, it is a FIPS 201 recommendation).

### 6.4.8 Zone 9 – Agency Specific Text (**GP.40 / CPS.46**)

MyID does not reserve an attribute for this purpose. You may choose to use one of the 'general purpose' fields for this zone (Privilege, Additional Information).

## 7 Standards Compliance

MyID performs fully standards compliant electronic and graphical personalization of PIV cards. The degree of compliance, supported optional elements and implementation details are given in the following sections; these are intended to support an evaluator through the product accreditation process.

For other aspects of the MyID solution, technical compliance is a function of the 3<sup>rd</sup> party components that you choose to integrate; MyID simply provides data entry, tracking and process control for the entire solution. When assembling a fully compliant solution therefore, it is important that you source components that are themselves FIPS 201 compliant. This applies especially to image capture devices, fingerprint scanners, NAC submissions systems and certification authorities.

It should be noted though, that simply having a collection of certified components does not necessarily constitute an overall compliant solution.

Some specific process-related aspects to consider are:

- Integrated, secure audit facilities
- Quality checks on captured information (for example, NFIQ for prints, electronic ID document verification)
- Role-separated workflow processes
- Notifications between individuals in each process

For advice on integrating third party components, please contact customer support.

In the following sections, GSA approval procedure references are included for your convenience. These appear as, for example, **EP.6** for item 6 in the Electronic Personalization approval procedure.

**Note:** In 2016, NIST modified the approval processes for FIPS-201 compliance, replacing the approved product list category "Electronic Personalization" with "FPKIPA Annual PIV Card Issuer Testing". The following information is retained for guidance only.

### 7.1 Graphical Personalization

MyID can produce compliant PIV cards using suitable desktop printers. A full description of the capabilities and instructions for each zone are given in Section 6, [Card Layout and Printing](#). Note that for the current release, all elements described in FIPS 201-1 (apart from 2D barcodes) are supported. Magnetic stripe encoding can also be provided if required.

## 7.2 Electrical Personalization

Electrical personalization of PIV cards is performed in a manner that is compliant with SP800-73-1, SP800-76 and SP800-78-2. The following sections indicate which of the optional components are implemented and which of the valid forms of each data type are available through MyID. The following tables are based on those in SP800-73-3.

Data objects populated in containers contain all the appropriate tags and lengths for each element in the object. The following table identifies the content currently supported by MyID ([EP.3](#), [EP.4](#), [EP.6](#), [EP.7](#), [EP.9](#))

Buffer Description	BER-TLV Tag	Max Len (Bytes)	Access Rule	Contact / Contactless	M/O	Supported by MyID
Card Capabilities Container	'5FC107'	291	Always	Contact	M	Yes
Card Holder Unique Identifier	'5FC102'	3408	Always	Contact and Contactless	M	Yes
X.509 Certificate for PIV Authentication (9A)	'5FC105'	2000	Always	Contact	M	Yes
Card Holder Fingerprints	'5FC103'	4000	PIN	Contact	M	Yes
Printed Information	'5FC109'	158	PIN	Contact	O	Yes
Card Holder Facial Image	'5FC108'	12704	PIN	Contact	O	Yes <a href="#">EP.7</a>
X.509 Certificate for Digital Signature (9C)	'5FC10A'	2000	Always	Contact	O	Yes
X.509 Certificate for Key Management (9D)	'5FC10B'	2000	Always	Contact	O	Yes
X.509 Certificate for Card Authentication (9E)	'5FC101'	2000	Always	Contact and Contactless	O	Yes
Security Object	'5FC106'	1025	Always	Contact	M	Yes
Discovery Object	'7E'	20	Always	Contact and Contactless	O	No
Key History Object	'5FC10C'	128	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 1 (Key reference '82')	'5FC10D'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 2 (Key reference '83')	'5FC10E'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 3 (Key reference '84')	'5FC10F'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 4 (Key reference '85')	'5FC110'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 5 (Key reference '86')	'5FC111'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 6 (Key reference '87')	'5FC112'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 7	'5FC113'	2005	Always	Contact	O	Yes

Buffer Description	BER-TLV Tag	Max Len (Bytes)	Access Rule	Contact / Contactless	M/O	Supported by MyID
(Key reference '88')						
Retired X.509 Certificate for Key Management 8 (Key reference '89')	'5FC114'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 9 (Key reference '8A')	'5FC115'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 10 (Key reference '8B')	'5FC116'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 11 (Key reference '8C')	'5FC117'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 12 (Key reference '8D')	'5FC118'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 13 (Key reference '8E')	'5FC119'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 14 (Key reference '8F')	'5FC11A'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 15 (Key reference '90')	'5FC11B'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 16 (Key reference '91')	'5FC11C'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 17 (Key reference '92')	'5FC11D'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 18 (Key reference '93')	'5FC11E'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 19 (Key reference '94')	'5FC11F'	2005	Always	Contact	O	Yes
Retired X.509 Certificate for Key Management 20 (Key reference '95')	'5FC120'	2005	Always	Contact	O	Yes
Cardholder Iris Images	'5FC121'	7106	PIN	Contact	O	Yes

## 7.2.1 CHUID

Card Holder Unique Identifier

EP.12

The CHUID is written to the card in the TLV format defined in SP800-73 as follows:

Data Element (TLV)	Tag	Type	Max. Bytes	Supported by MyID
Buffer Length (Optional)	0xEE	Fixed	2	Yes
FASC-N	0x30	Fixed Text	25	Yes
Organization Identifier (Optional)	0x32	Fixed Text	4	Yes
DUNS (Optional)	0x33	Fixed Numeric	9	Yes
GUID	0x34	Fixed Numeric	16	Yes
Expiration Date §	0x35	Date (YYYYMMDD) EP.5	8	Yes EP.4
Issuer Asymmetric Signature §	0x3E	Variable	2816	Yes
Error Detection Code	0xFE	LRC	0	Yes

**Notes:**

§ The expiration date matches that of the card

§ The signature confirms the CHUID content and is created as defined in FIPS 201.

## 7.2.2 CBEFF

Card Holder Fingerprints

EP.6, EP.7, EP.14

Biometric data is written to the card in a CBEFF format, comprising a CBEFF\_HEADER, a STD\_BIOMETRIC\_RECORD and a CBEFF\_SIGNATURE\_BLOCK. Primary and secondary fingerprint template data are written in the form that they are presented to MyID; it is therefore the responsibility of the enrollment system to ensure that these are in a compliant INCITS 378 format. MyID performs the necessary CBEFF format wrapping to combine the two fingerprints into a single minutiae template on the PIV card.

Data Element (TLV)	Tag	Type	Max. Bytes	Supported by MyID
Fingerprint 1	0xBC	Variable	2000	Yes
Fingerprint 2	0xBD	Variable	2000	Not used
Error Detection Code	0xFE	LRC	0	Yes

Note: Up to 2 fingerprint minutiae templates are combined into the Fingerprint 1 container, in accordance with SP800-73-1 (EP.6). The Fingerprint 2 container is not used.

## 7.2.3 CCC

Card Capabilities Container

Data Element (TLV)	Tag	Type	Max. Bytes	Supported by MyID
Card Identifier	0xF0	Fixed	21	Yes
Capability Container version number	0xF1	Fixed	1	Yes
Capability Grammar version number	0xF2	Fixed	1	Yes
Applications CardURL	0xF3	Variable	128	Yes
PKCS#15	0xF4	Fixed	1	Yes
Registered Data Model number	0xF5	Fixed	1	Yes
Access Control Rule Table	0xF6	Fixed	17	Yes
CARD APDUs	0xF7	Fixed	0	Yes
Redirection Tag	0xFA	Fixed	0	Yes
Capability Tuples (CTs)	0xFB	Fixed	0	Yes

Data Element (TLV)	Tag	Type	Max. Bytes	Supported by MyID
Status Tuples (STs)	0xFC	Fixed	0	Yes
Next CCC	0xFD	Fixed	0	Yes
Extended Application CardURL (optional)	0xE3	Fixed	48	No
Security Object Buffer (optional)	0xB4	Fixed	48	No
Error Detection Code	0xFE	LRC	0	Yes

## 7.2.4 Certificate Containers

X.509 Certificate for PIV Authentication **EP.13**

X.509 Certificate for Digital Signature **EP.19**

X.509 Certificate for Key Management **EP.20**

X.509 Certificate for Card Authentication **EP.21**

For PIV-III compliant cards only: X.509 Certificate for Retired Key Management 1 to 20

Data Element (TLV)	Tag	Type	Max. Bytes	Supported in MyID
Certificate	0x70	Variable	2005	Yes
CertInfo	0x71	Fixed	1	Yes
MSCUID (Optional)	0x72	Variable	38	No
Error Detection Code	0xFE	LRC	0	Yes

## 7.2.5 Printed Information

Printed Information **EP.18**

Data Element (TLV)	Tag	Type	Max. Bytes	Supported in MyID
Name	0x01	Fixed Text	32	Yes
Employee Affiliation	0x02	Fixed Text	20	Yes
Expiration date	0x04	Fixed Text	9	Yes
Agency Card Serial Number	0x05	Fixed Text	10	Yes
Issuer Identification	0x06	Fixed Text	15	Yes
Error Detection Code	0xFE	LRC	0	Yes

The **Employee Affiliation line 2** has been deprecated in SP800-73-3, and has therefore been removed from recent card formats.

## 7.2.6 Card Holder Facial Image

Capturing a facial biometric (385 template) within MyID is supported. (EP.7, EP.17, EP.63)

### Card Holder Facial Image

The card holder facial image is generated by a third-party image capture and processing library. This creates the image in a JPEG2000 format with single region of interest compression, compliant with SP800-76-1. Only one such image may be written to each card.

Data Element (TLV)	Tag	Type	Max. Bytes	Supported in MyID
Image for Visual Verification	0xBC	Variable	12704	Yes
Error Detection Code	0xFE	LRC	0	Yes

Notes:

1. Only one image is stored in this container (EP.7)
2. The internal format of the facial biometric will depend on the IDMS sending the data to the CMS. When using MyID to capture facial images, this will usually be in JPEG2000 with ROI compression. (EP.63)

## 7.2.7 Security Object

Security Object EP.15

Data Element (TLV)	Tag	Type	Max. Bytes	Supported in MyID
Mapping of DG to ContainerID	0xBA	Variable	100	Yes
Security Object	0xBB	Variable	900	Yes
Error Detection Code	0xFE	LRC	0	Yes

## 7.2.8 Key History

The key history object is only present on PIV-III compliant cards. EP.178

Data Element (TLV)	Tag	Type	Max. Bytes	Supported in MyID
Key with On Card Certificates	0xC1	Fixed	1	Yes
Key with Off Card Certificates	0xC2	Fixed	1	No
Off Card Cert URL	0XF3	Variable	128	No
Error Detection Code	0xFE	LRC	0	Yes

MyID only supports **On Card Certificates**. The **Off Card Certificates** count is always set to zero. Therefore the **Off Card Cert URL** is never present.

## 7.2.9 Discovery Object

The optional discovery history object can only be present on PIV-III compliant cards. It is not supported by MyID.

## 7.2.10 Cardholder Iris Images

The Cardholder Iris Images object is only present on PIV-III compliant cards.

Data Element (TLV)	Tag	Type	Max. Bytes	Supported in MyID
Images for Iris	0xBC	Variable	7100*	Yes
Error Detection Code	0xFE	LRC	0	Yes

MyID stores the certificate the signed the images for iris in the CHUID, in accordance with SP800-73-3\_Part 1 – Page 28 footnote.

## 7.3 Key Management

In order for MyID to write data to a PIV card, it must first authenticate itself to the card using the Card Management Key (CMK - the '9B' symmetric key) through a challenge-response protocol. (EP.1)

MyID supports diversification of the CMK. At system commissioning time, the 'factory' key can be set to a static value for the 'blank' cards and a diversified key must be specified for the 'customer key'. The diversification master will then be created on the connected HSM. It is important that you choose a FIPS 140-2 certified HSM for this purpose, since this is mandated for FIPS 201 compliance.

As cards are issued, their static 9B keys are replaced by the key derived from the master (on the HSM) and the card serial number. In this manner, all issued cards have a different CMK that is derived from a key held on a FIPS 140-2 security module. (EP.2, EP.167)

Asymmetric key pair generation for X.509 certificates is all performed on-card. For this reason, you should ensure that the devices you choose as your PIV cards have a FIPS 140-2 certification.

## 7.4 Restrictions

Currently, dual-chip cards are not supported. All personalization is performed using the contact interface and is therefore able to work with dual-interface, single chip devices. This feature will be implemented in future versions of MyID, but may also be attainable on a project basis before full release.

Please contact customer support if you require this feature.

## 7.5 Hashing Algorithm

You can specify the PIV server hash algorithm. PIV data must be hashed using SHA256 (the default option) or SHA1. This is in compliance with the PIV specifications. (EP.176, EP.177)



## 8 PIV Notifications

You can configure MyID to send notifications to email addresses or external web servers.

A default installation of PIV includes sample email templates, triggers, and URL notifications; however, no notifications are configured to be sent.

For information on configuring MyID to send email or web notifications, contact customer support quoting reference SUP-222.