MyID PIV

Version 12.13

PIV Integration Guide

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

Document reference: IMP1959-12.13.0-PIV

December 2024

Copyright

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

© You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. ---

Conventions used in this document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important.
  - Bulleted lists are used when the order is unimportant or to show alternatives.
- **Bold** is used for menu items and for labels.

  For example:
  - Record a valid email address in **'From' email address**.
  - Select **Save** from the **File** menu.
- *Italic* is used for emphasis:

  For example:
  - Copy the file *before* starting the installation.
  - Do *not* remove the files before you have backed them up.
- ***Bold and italic*** hyperlinks are used to identify the titles of other documents.

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

  Unless otherwise explicitly stated, all referenced documentation is available on the product installation media.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.
- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

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

Contents

1 Introduction

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 201-3. 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.

2 About PIV

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).

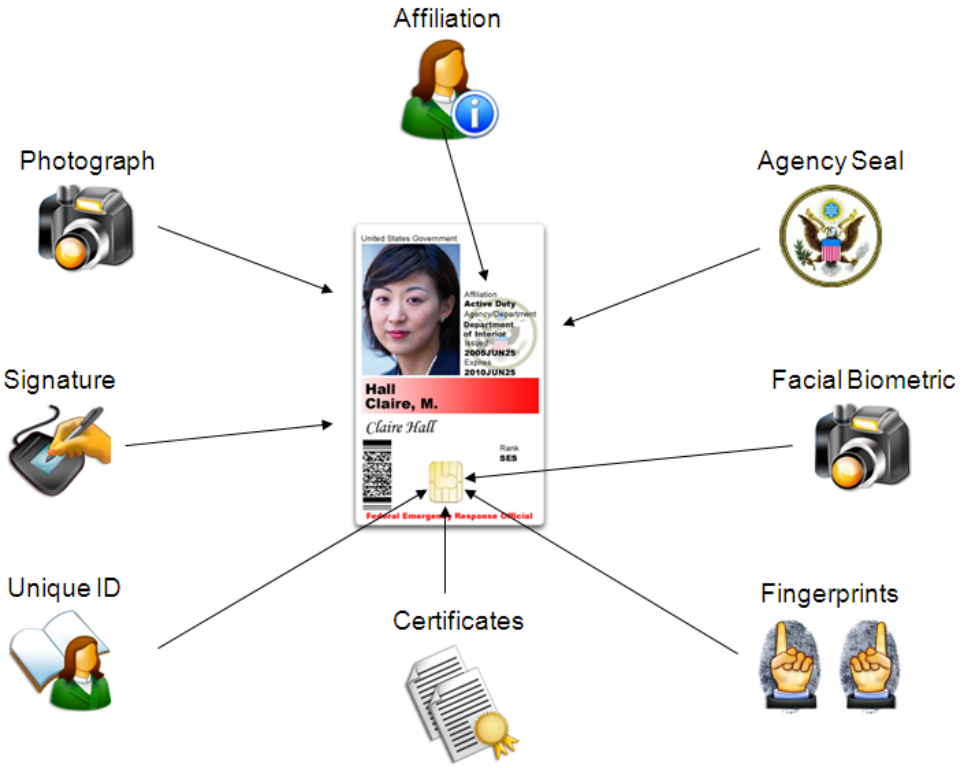
FIPS 201 specifies both the technical and process requirements a system must meet in order to issue a valid Personal Identity Verification (PIV) card.

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)

2.1 PIV smart cards

PIV smart cards 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 smart cards is the PIV Card Application Administrator Key (sometimes referred to as key reference 9B). This key is shared between the smart cards and the smart card 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.

2.2 Non-Federal adoption of PIV cards

While PIV cards are designed for Federal agencies, there are variants of the PIV technology that are used by non-Federal organizations: PIV-I and CIV.

2.2.1 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, while still complying with the strict issuance polices 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 (for example,. 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).

2.2.2 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 – while 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.

2.3 Derived Credentials

FIPS 201-3 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 Configuration Guide***.

3 Using MyID for FIPS 201-3

The key business processes that are covered by FIPS 201-3 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.

The standards governing PIV were revised in 2022 to address changing technical & business process requirements. MyID has been updated to support the following changes in FIPS-201-3:

- Authenticator types for PIV derived credentials

  The range of authenticator types that can be used for PIV Derived Credentials through the Self-Service Request Portal has been extended to allow a broader range of multi-factor cryptographic devices that meet the requirements for Authenticator Assurance Level (AAL) 2 or 3 as specified in the associated technical standard SP 800-63B. This could include FIDO Tokens, Microsoft Virtual Smart Cards, and Windows Hello for Business in addition to alternative smart cards, USB Tokens and mobile devices.

  See the *Setting up the credential profiles for derived credentials* section in the ***Derived Credentials Self-Service Request Portal*** guide.

- Notification of derived credential requests

  MyID can now generate an email notification to the PIV cardholder when they request PIV Derived Credentials. Depending on configuration, this can use an email address collected from the PIV credential, or the email address stored in MyID which may include information retrieved from a connected directory.

  See the *Configuring email notifications* section in the ***Derived Credentials Self-Service Request Portal*** guide or the *Configuring email notifications* section in the ***Derived Credentials Configuration Guide*** for details.

  MyID can also be configured to block requests for derived credentials if no email address can be located.

  See the *Requiring an email address* section in the ***Derived Credentials Self-Service Request Portal*** guide or the *Requiring an email address* section in the ***Derived Credentials Configuration Guide*** for details.

  Upon canceling devices issued by MyID, an email notification can also be sent to the PIV Cardholder holder to inform them that revocation has taken place.

  See the *Editing the cancellation email template* section in the ***Derived Credentials Self-Service Request Portal*** guide or the *Editing the cancellation email template* section in the ***Derived Credentials Configuration Guide***.

- Updates to identity document lists

  The list of suitable identity document types that can be captured during PIV Enrollment has been revised in line with changes in FIPS 201-3.

  See section *5.17*, *Identity documents* for details.

- Amendments to card layouts

  Default PIV card layouts in MyID 12.4.0 or later will not include Zone 6F: Portable Data File (PDF) 417 Two-Dimensional Bar Code as it is now deprecated. If you are upgrading from an earlier version of MyID, no modifications are automatically applied to existing layouts in your installation – you must review your use of this element and modify your card layouts as required.

  See section *5.4.1*, *Updating existing card layouts* for details.

- Capturing the client location in MyID audit records

  PIV enrollment may take place across multiple visits, in different locations and may be carried out by different people at each step. To help create a log of activities that have taken place, MyID can now track where an activity took place and capture this information in the MyID audit trail.

  See the *Logging the client IP address and identifier* and *Specifying a custom client identifier* sections in the ***Administration Guide*** for details.

3.1 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 in MyID, import them from a directory, or import them from an external system using the MyID Core API.

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

See the ***MyID Core API*** 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 *4.3.8*, *Summary of requirements for PIV-I and CIV* for more information.

Each operation that takes place in MyID creates an audit record, providing an audited sequence of enrollment events that have involved the use of MyID. You can view this information on the **History** tab on the View Person screen in the MyID Operator Client. Changes to attributes that have occurred over time are listed on the **Attribute Changes** tab. Additional reports that allow you to carry out comprehensive searches of audit records are also available .

For further information, see the *Viewing a person's history* section in the ***MyID Operator Client*** guide.

3.2 PIV card issuance

The card issuance process is as follows:

1. Approve the applicant

   Before you can request a card for a person, you must mark the completion of their PIV enrollment and approve them to be issued a PIV card. This also allows you to set the vetting date and apply a maximum expiry date for any credentials they are issued.

   Use the **Status** tab and the **Approve Person** option on the View Person screen.

   See the *Setting the person's status* and *Approving user data* sections in the ***MyID Operator Client*** guide.

2. 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.

   Use the **Request Device** option on the View Person screen to collect the device.

   See the *Requesting a device for a person* section in the ***MyID Operator Client*** guide.

3. 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 **Approve Request** option on the View Request screen to collect the device.

   See the *Approving, rejecting, and canceling requests* section in the ***MyID Operator Client*** guide.

4. 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 **Collect** option on the View Request screen to collect the device.

   See the *Collecting a device request* section in the ***MyID Operator Client*** guide.

   You can also use the **Batch Collect Card** workflow; see the *Collecting a batch of cards* section in the ***Operator's Guide*** for details.

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

5. 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** or **Batch Collect Card** processes, 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.

6. Activate

   Make sure that the credential profile is set up to use activation. Set the **Require Activation** option to **Allow self collection** or **Assisted 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 App or through the self-service menu in the MyID Operator Client; see the *Collecting self-service requests* section in the ***MyID Operator Client*** guide.

   Alternatively, an operator can guide the cardholder through activation using the **Assisted Activation** option on the View Device screen, depending on how you have set the **Require Activation** option in the credential profile; see the *Activating a device* section in the ***MyID Operator Client*** guide.

   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 201-3 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.

3.2.1 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** operation 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** workflow 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 201-3) 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. See the *Authenticating a person* section in the ***MyID Operator Client*** guide.

3.3 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 MyID Core API, Lifecycle API, or the PIV applicant editing screens 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 **Approve Request** option on the View Request screen) 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 201-3 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`.

3.4 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.
- Reinstate the card after incorrect cancellation.
- Recover additional certificates onto the card.
- Certificate rekey (renewal).

3.4.1 Update the certificates on the card

You can an update the certificates on the card using the **Request Update** option on the View Device screen followed by the **Collect Updates** option; see the *Requesting an update for a device* and *Updating a device* sections in the ***MyID Operator Client*** guide

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 201-3.

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.

3.4.2 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** features.

- **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.

  See the *Reprovisioning cards* section in the ***Operator's Guide***.
- **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.

  See the *Reprovisioning a device* section in the ***MyID Operator Client*** guide

If you cancel a card by mistake, issuing a new card may be difficult or time consuming. Instead, you can use the **Reinstate Card** option to return the canceled card to an active state; see the *Reinstating a device* section in the ***MyID Operator Client*** guide

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 reinstate 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.

3.4.3 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.

Note: When you recover certificates to a PIV card, all retired certificate containers are overwritten. This affects any smart card with a PIV applet.

3.4.3.1 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.

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 *Recovering your own certificates* section in the ***Operator's Guide*** for details.

3.4.3.2 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.

3.4.3.3 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.

3.4.4 Certificate rekey (certificate renewal)

The MyID certificate renewal process generates a new key pair (rekey) as defined by FIPS 201-3.

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 of the ***Administration Guide***.

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

3.5 PIV card verification data reset

This section contains information on resetting the PIN on the PIV card. The cardholder can reset the PIN themselves using a self-service PIN reset process, or can reset the PIN with the assistance of a MyID operator.

3.5.1 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 201-3 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 201-3:

  - 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 activation 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 **Change PIN** workflow to change your PIN. You must re-enter your old PIN before you supply the new PIN; see the *Changing a device PIN* section in the ***MyID Operator Client*** guide.

  Alternatively, you can use the Reset PIN option on the Self-Service App. 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 the *Remote PIN Management utility for PIV cards* section in the ***Operator's Guide*** for details.

Note: Currently, this utility does not allow fingerprint verification, and therefore is not recommended for use with cards that require FIPS 201-3.

3.5.2 Operator-led PIN reset

You can use the **Reset Card PIN** workflow to reset another person's card PIN; see the *Resetting a card's PIN* section in the ***Operator's Guide***.

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*.

3.5.3 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.

3.5.4 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.

3.6 PIV card termination

The following processes apply to revoking an issued PIV card:

- Canceling (revoking) a PIV card that is present.
- Remotely canceling a PIV card that is not present.
- Erasing a PIV card that has been remotely canceled.
- Changing the disposal status of a card.

3.6.1 Canceling (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; the *Erasing a device* section in the ***MyID Operator Client*** guide.

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.

3.6.2 Remotely canceling a PIV card that is not present

You can remotely cancel a card in the following ways:

- Using the MyID Core API.
- Using the **Cancel Credential** workflow; the *Canceling a device* section in the ***MyID Operator Client*** guide.
- 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 canceling a PIV card that is present. No change is made to the data on the card.

3.6.3 Erasing a PIV card that has been remotely canceled

When a card has been remotely canceled, 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; the *Erasing a device* section in the ***MyID Operator Client*** guide.

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.

3.6.4 Notifications to other systems

FIPS 201-3 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, contact customer support quoting reference SUP-222.

3.6.5 Changing the disposal status of a card

The disposal status of a canceled 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 a device* section in the ***MyID Operator Client*** guide.

4 Configuring MyID

This chapter contains information about configuring MyID for PIV issuance, including:

- Installing the MyID server software.
- Integrating with other systems.
- Configuring MyID for FIPS 201-3 issuance.
- Configuring MyID for non-Federal issuers (PIV-I and CIV).
- Controlling the content of subject alternative names.
- Configuring server signing certificates.
- Configuring the PIV server hash algorithm.
- Setting up biometric identification.
- Setting up MyID when you have existing PIV cards.
- Controlling local and remote operations.

4.1 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***.

4.1.1 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.

- Smart card Readers and Printers

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

  Often they are integrated into smart card 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 smart cards 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)

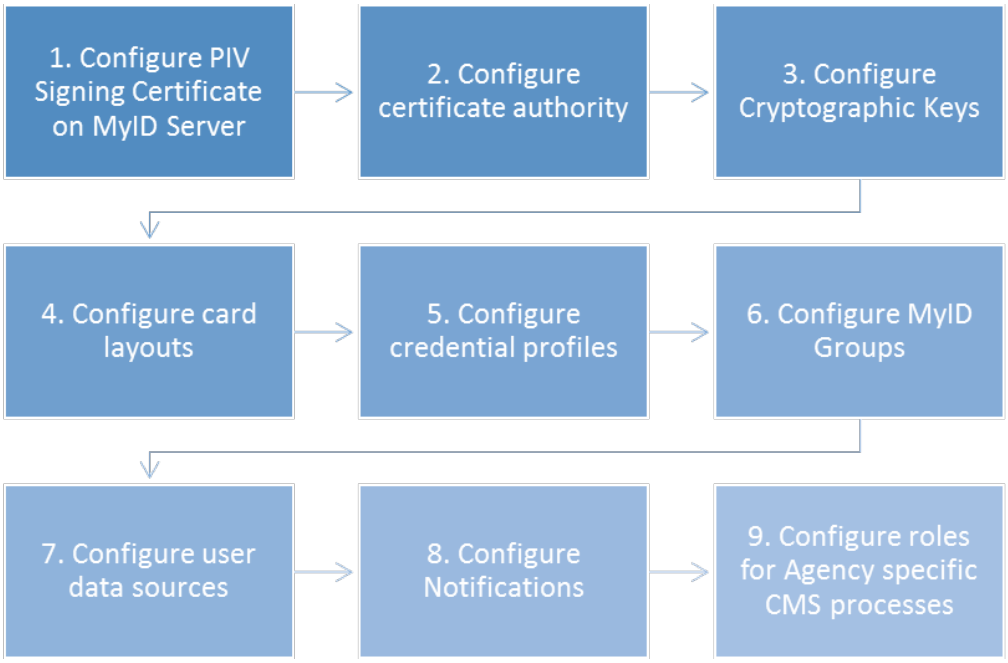
  PAC Systems allow an Applicants PIV card to be granted access to a room or building by presenting their PIV card. MyID can integrate with PACS by providing applicant and card data, and allowing an operator to identify which areas they may be allowed to access.

- 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.

4.2 Configuring MyID for FIPS 201-3 card issuance (PIV)

To set up the enrollment and issuance models you require for your installation of MyID for PIV, you must follow these steps:



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.	See section *4.5*, *Configure server signing certificates*
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.	See section *5.1*, *PIV card application administration key (9B)*.
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.	See section *5.4*, *Setting up the credential profile*. See section *5.4.1*, *Updating existing card layouts*.

Step	Description	See
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.	See section *5.4*, *Setting up the credential profile*.
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.	See section *5.6*, *Manage agencies*
Configure User Data Sources	You can add and amend PIV user attributes using the following: • MyID Core API. This requires the configuration of a data feed from your enrollment system. • Manually adding users with the MyID workflow **Add Person**. • Importing users from a connected LDAP compliant directory using MyID Desktop or the MyID Operator Client. • The PIV applicant editing screens allows PIV specific attributes to be updated and fingerprint and facial biometric enrollment to take place. • Lifecycle API. This is deprecated in favor of the MyID Core API.	See section *5.15*, *Editing PIV applicants*.
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, 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 *Roles, groups, and scope* section in the ***Administration Guide***.

4.3 Configuring MyID for non-Federal issuers (PIV-I and 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.

4.3.1 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. **Note:** 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 or 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 or Applet personalization	Use of PIV card technology, where the format and source of the CHUID and PIV applet data is the same as PIV or 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 or PIV-I. PIV attribute values on card may be hard coded to predetermined values.	As Project Requirement	No	Yes*
CIV – certificates only	Use of PIV card technology, with no CHUID or 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

* With CIV module installed. Further customization may be needed.

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.

- NACI 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 or Sponsoring Organization (for example, 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. You can use the Card Layout Editor in MyID to create and amend the card layouts – see the *Designing card layouts* section in the ***Administration Guide*** for details.

4.3.2 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.

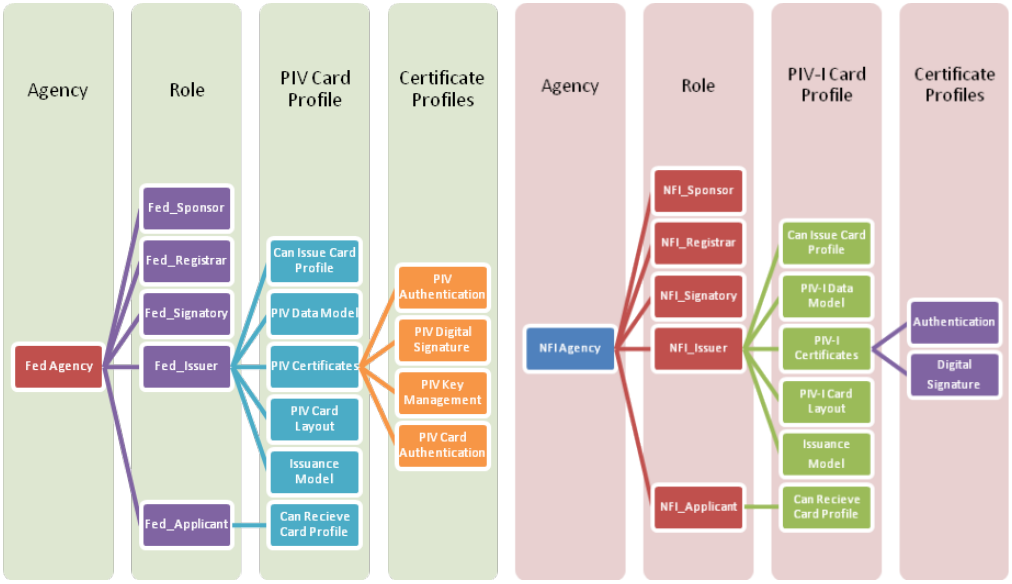
You must restrict the roles that are permitted to issue and receive the FIPS 201 PIV and PIV-I credential profiles; you can request cards using the MyID GUI in addition to the Lifecycle API – the available profiles for selection are restricted based on the roles held by the current operator requesting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

4.3.3 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 *Scope and security* and *Administrative groups* sections of 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-I or CIV.

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



4.3.4 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 or applet personalization)
  - User accounts must be imported using MyID Core API (or the Lifecycle API) to set the PIV attributes, manually added using the Add Person screen, or imported from LDAP using the Edit Person (Directory) screen. 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.

4.3.5 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 using the Edit Person screen. Instead, you can use the PIV applicant editing screens. 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.

4.3.6 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 or UUID recreation when updating a card).

4.3.7 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.

4.3.8 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 or 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 card layouts.
  - Select **CivCertificatesOnly.xml** or **CivCertificatesOnlyCompressed.xml** from the **Card Format** drop-down list in the credential profile.

4.4 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*.

4.5 Configure server signing certificates

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

- 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 SHA-256 or SHA-384 in the `digestAlgorithm` of the `SignerInfo`.
- Use SHA-256 or SHA-384 in the `AlgorithmIdentifier` of the signature.
- Be issued using the CSP or KSP 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.

  You can use any RSA key, including 3072 and 4096 bit keys.

Note: By default, MyID uses a hash algorithm of SHA-256 for SCEP signing. The certificate that you use for signing must therefore have been produced using a KSP or CSP that supports SHA-256; some older CSPs (for example, the Microsoft Strong Cryptographic Provider) do not support SHA-256; the Microsoft Enhanced RSA and AES Cryptographic Provider does support SHA-256, however. You can choose to use SHA-384; similarly, in this case, the KSP or CSP must support SHA-384.

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 Entrust nShield HSM, the nShield CSP must not be configured to protect the private key with an operator card set that requires PIN entry. For nShield HSMs, the

content signer certificate can be protected either by the module, or by an operator card set without PIN.

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

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 SHA-256 or SHA-384 for the PIV server hash algorithm; see section *4.6*, *Configuring the PIV server hash algorithm* for details. You must make sure that the CSP you use to issue the certificate supports SHA-256 or SHA-384.

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\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.

Note: For details of setting up the CVC signing certificate for OPACITY, see the *Setting up the CVC signing certificate* section in the ***Smart Card Integration Guide***.

4.5.1 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.

4.6 Configuring the PIV server hash algorithm

You can specify the PIV server hash algorithm. PIV data can be hashed using SHA-256 or SHA-384 (required for PIV compliance) or SHA-1 (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`
   - `SHA384`
4. Click **Save changes**.

You must set the hash algorithm to SHA-256 or SHA-384 for PIV compliance and to follow best security practice. You are not recommended to run with SHA-1 on a production system.

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 change the algorithm to SHA-384, the collection of certificate renewals fails due to a hash mismatch error. Other affected processes include collecting a key recovery, or adding additional certificates to the card.

4.7 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
- SecuGen Hamster Pro Duo SC/PIV
- SecuGen Pro 10

- SecuGen Pro 20
- U.are.U 5300
- DigitalPersona EikonTouch 710

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

- ***SecuGen Integration Guide***
- ***U.are.U Integration Guide***

4.8 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.

4.9 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 *Roles* section in 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 *Job filtering* section in the ***Web Service Architecture*** 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.
  - **Assisted Activation Only** – applicants must activate their cards with the assistance of a MyID operator.

5 Using MyID for PIV

This chapter contains information on using MyID to issue and manage PIV cards.

Before you can begin, you must have an account that you can use to log on to MyID. See the *Using GenMaster* section in the ***Installation and Configuration Guide*** for details of using the GenMaster utility to set 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 administration key (9B)

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 ***csrc.nist.gov***.

5.1.1 Factory 9B keys

When PIV 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 either 32 or 48 characters in hexadecimal format.

1. From the **Configuration** category, select **Key Manager**.

   You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the ***MyID Operator Client*** guide for details.
2. From the **Select Key Type to Manage** list, select **PIV 9B Card Administration Key** and 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 the attributes for the key if required:
   - **Exportable** – the key can subsequently be exported.
6. Select **Factory** from the **Key Type** drop-down list. This means that you are using the key provided by your supplier.
7. From the **Key Diversity** drop-down list, select **Static** for static keys, or one of the Diverse options for diversified keys.

   See the ***Smart Card Integration Guide*** for the key diversity option for your type of card.
8. From the **Encryption Type** drop-down list, select the encryption used.

   See the ***Smart Card Integration Guide*** for the encryption option for your type of card.

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

10. If you are storing the key in the database, choose one of the following options:
    - **Automatically Generate Encryption Key in Software and Store on Database** – this option automatically creates an encryption key.
    - **Encryption Key** – type the hexadecimal key in the box. Optionally, you can include the **KeyChecksum Value**.
    - **Use Key Ceremony** – if you have the key in key ceremony format (encrypted by a Transport Key), select this option. When you click **Enter Keys**, the key ceremony wizard will launch, allowing you to enter the key ceremony data into the database.
11. If you are storing the key on an HSM, and have selected **Diverse** key diversity, select one of the following options:
    - **Automatically Generate Encryption Key on HSM and Store 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.
    - **Use Key Ceremony** – if you have the key in key ceremony format (encrypted by a Transport Key), select this option. When you click **Enter Keys**, the key ceremony wizard will launch, allowing you to enter the key ceremony data into the HSM.

    Note: If an HSM is available, Intercede recommends it is used as it provides stronger protection for the key.
12. 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.

Note: If the customer 9B key for a PIV card is not created, the card will continue to use the factory 9B key after issue. The factory 9B key may be known to third parties, so may not be secure. We recommend that a diverse customer 9B key is generated in the HSM for all PIV device types to be issued. PIV compliant installations *must* specify diverse customer 9B keys in the HSM.

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**.

   You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the ***MyID Operator Client*** guide for details.
2. From the **Select Key Type to Manage** list, select **PIV 9B Card Administration Key** and 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 the attributes for the key if required:
   - **Exportable** – the key can subsequently be exported.
6. Select **Customer** from the **Key Type** drop-down list.
7. Select **Static**, **Diverse2**, or **Diverse108** from the **Key Diversity** drop-down list.

   Intercede recommends using diverse 9B customer keys as this enhances the security of the solution.

   See the ***Smart Card Integration Guide*** for the appropriate diversity option for your type of card. If the guide does not list the diversification algorithm for your card type, choose **Diverse2**.
8. Select the same **Encryption Type** as you specified for the factory key.
9. Type a **Description** for the key.
10. If you are storing the key in the database, choose one of the following options:
    - **Automatically Generate Encryption Key in Software and Store on Database** – this option automatically creates an encryption key.
    - **Encryption Key** – type the hexadecimal key in the box. Optionally, you can include the **KeyChecksum Value**.
    - **Use Key Ceremony** – if you have the key in key ceremony format (encrypted by a Transport Key), select this option. When you click **Enter Keys**, the key ceremony wizard will launch, allowing you to enter the key ceremony data into the database or HSM (if available).

    If you are storing the key on an HSM, and have selected **Diverse** key diversity, select one of the following options:
    - **Automatically Generate Encryption Key on HSM and Store 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.

    Note: If an HSM is available, Intercede recommends it is used as it provides stronger protection for the key.
11. 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 a 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.
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.

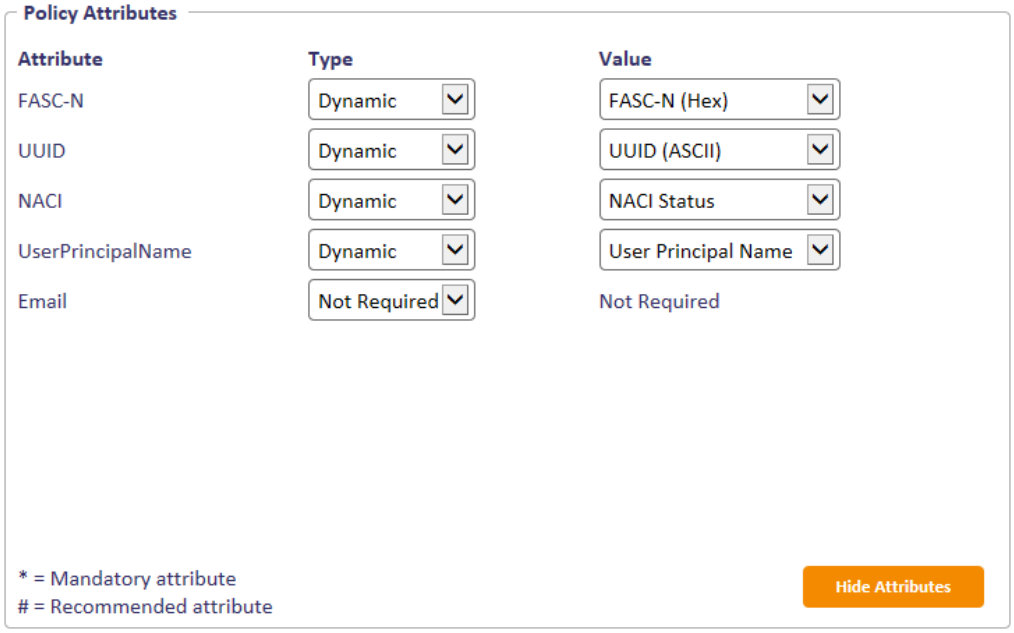
   a. Make the relevant policies available.

   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.



   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.
   - **CivCertificatesOnlyCompressed.xml** – used for CIV cards that do not require CHUID and applet customization, using compressed data.
   - **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.

     If you are using the Biometric On-Card Comparison feature, select **PivDataModelMOC.xml** instead. See the *Biometric On-Card Comparison* section of the ***Smart Card Integration Guide***.

     Note: If you select the **PivDataModelMOC.xml** model, MyID writes biometric data to supported devices; however, to allow the biometrics to be used for authentication, you must also select the **Biometric On-Card Comparison** option in the **PIN Settings** section.
   - **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 **Requisite User Data**.

   You can use this feature to ensure necessary data is present before cards are requested; for example, select **Employee ID** (which is displayed in MyID Desktop as the **Security** field) and **PIV Distinguished Name** to reduce potential errors during card issuance.

   For more information see the *Requisite User Data* section in the ***Administration Guide***.

9. Click **Next**.

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

Select the required certificates and assign them to the correct containers.

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** for one certificate. 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*** for details of whether your credentials contain the PIV applet.

Click **Next**.

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

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

12. 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.
- In the **Can Validate** column, select the roles you want to be able to validate requests for this profile.
- In the **Can Collect** column, select the roles you want to be able to collect requests for this profile.

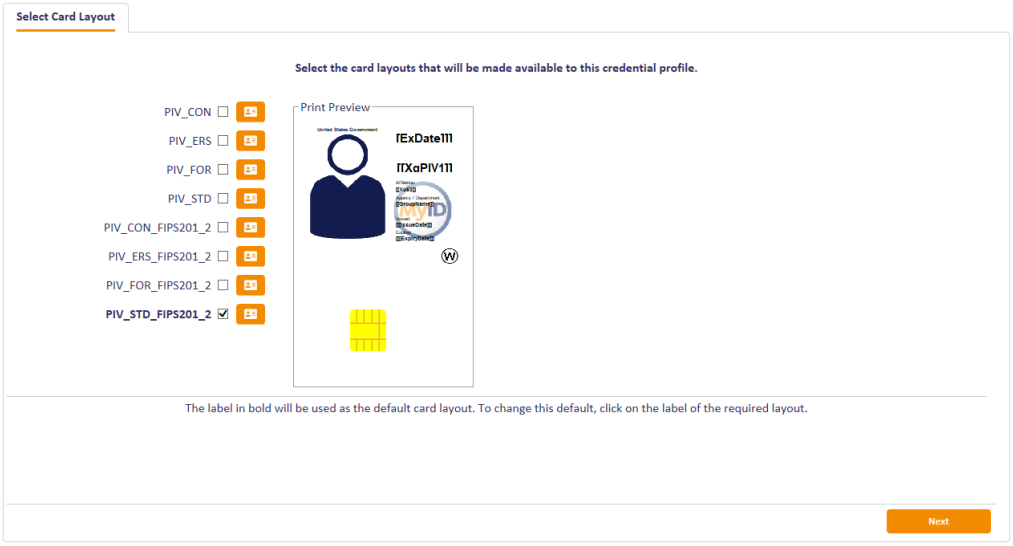
Note: The options available on this screen are determined by the following configuration options on the **Process** page of the **Security Settings** workflow:

- **Constrain Credential Profile Issuer**
- **Constrain Credential Profile Validator**

- **Constrain Credential Profile Collector**
- **Constrain Credential Profile Unlock Operator** – not set by default.

See the *Linking credential profiles to roles* section in the ***Administration Guide*** for details.

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



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 *Designing card layouts* section in the ***Administration Guide*** for details.

14. 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 201-3. 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.

5.4.1.1 Updating from FIPS 201-1 to FIPS 201-2

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 **Formatter** 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 **Formatter** 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.

5.4.1.2 Updating from FIPS 201-2 to FIPS 201-3

To update your card layouts from FIPS 201-2 to FIPS 201-3:

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 **2D Barcode** element from the card layout.
      This is the element used for zone 6.
   c. Save the card layout.
3. For each back layout:
   a. Open the layout you want to update:
   b. Delete the **Linear Barcode** element from the card layout.
      This is the element used for zone 8.
   c. Save the card layout.

Note: It is very important that you confirm that any customized layouts you produce are fully compliant with the FIPS 201-3 standards. See your NIST FIPS 201-3 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 in EJBCA and Symantec CAs to provide a printable version of the FASC-N.

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:

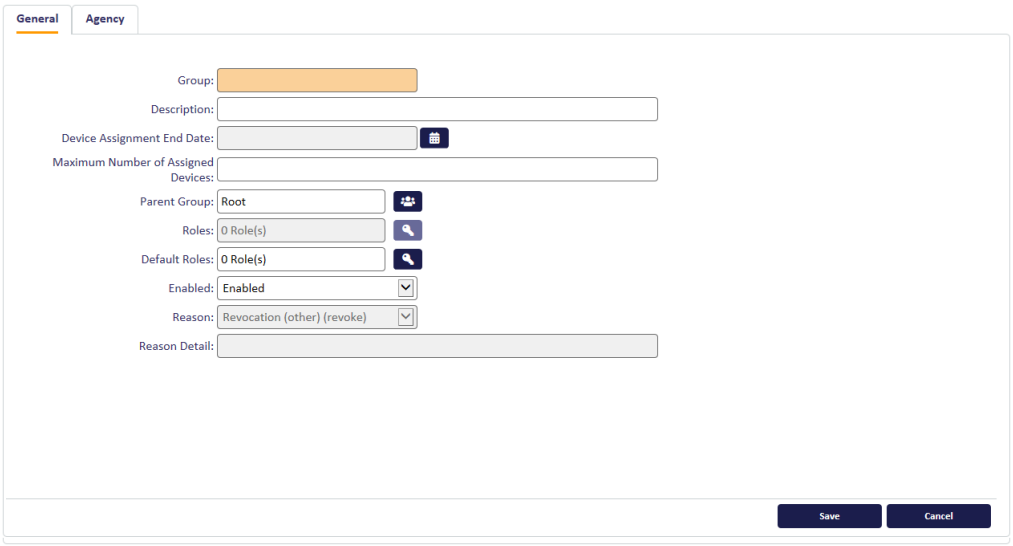
- **Add Group**
- **Amend Group**
- **Remove Group**
- **Edit Groups**

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. Optionally, set the following license options:
   - **Device Assignment End Date** – select the last date on which you can assign or issue devices for this group. After this date, you will no longer be able to assign or issue devices to people in this group.
   - **Maximum Number of Assigned Devices** – type the maximum number of devices you can assign or issue to this group. Once the number of devices assigned or issued to people in this group reaches this number, you will no longer be able to assign or issue devices to people in this group.
5. 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.

6. 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.

7. 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.

8. Click the **Agency** tab.

9. In **Issuing Agency**, enter the standard four-character code for the agency issuing the credential.

   For PIV-I and CIV cards, enter `9999`.

10. Enter the standard **Site Code**.

    For PIV-I and CIV cards, enter `9999`.

11. Type the **Abbreviation** for the agency to appear on the printed card.

12. Select the correct **Category** from the list available (Federal, State, Commercial or Foreign).

13. Enter the **Dept Code**, if you have one.

    Note: To ensure that PIV electronic personalization and physical card printing match, set this to six digits, front padded with zeros; for example, `000123`.

14. 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:

    - Federal – The agency code (as recorded in **Agency Code**).
    - State – The state code.
    - Commercial – The code for the company.
    - Foreign – The numeric country code.

15. Click the image to upload an image of the agency's seal.
16. If you select **Commercial** as the **Category**, enter the Agency DUNS code in the **DUNS** field.
17. Enter **Contact** information (including the name, **Address**, **Phone** number and **Email** address) for an individual who can answer questions relating to this agency.
18. The **Department** field defaults to the name of the **ParentGroup** as defined in the **General** tab. You can change this value if necessary.
19. In the **Component** field, type the component within the agency. This field is optional.
20. Enter the **Base DN**.

    This value is 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.

5.6.1.1 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**.

5.6.4.1 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**.

5.6.4.2 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**.

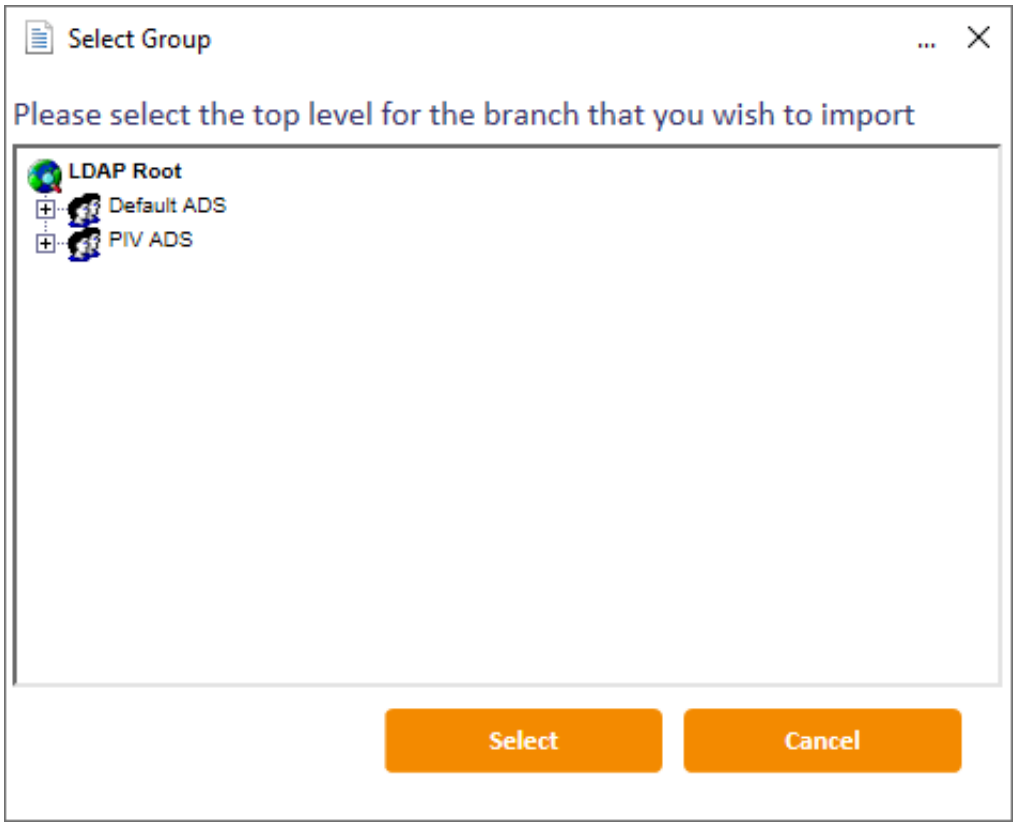
5.6.4.3 Rename an agency

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**.

5.6.4.4 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**.

5.6.4.5 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 *Configuring a credential profile for activation* section in 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 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 201-3.

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 201-3.
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 201-3 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 201-3.

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 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 201-3, you must confirm the identity of the cardholder before carrying out changes on their card.

For more information, see the *Authenticating users* section of the ***Operator's Guide***.

5.15 Editing PIV applicants

Important: The **Edit PIV Applicant** workflow, which was previously available in MyID Desktop, is now End of Support, and has been replaced with equivalent functionality in the MyID Operator Client; see the *Editing a PIV applicant* section in the ***MyID Operator Client*** guide for details.

The MyID Operator Client provides the following screens to allow you to edit the details of PIV applicants:

- Initial PIV Enrollment – used to edit people accounts that do not yet have fingerprints enrolled.
- Update PIV Applicant – used to edit people accounts that already have fingerprints enrolled. You must authenticate to this screen by providing the person's fingerprints.
- Edit PIV Applicant – used as an administrative tool to edit people accounts whether or not they have fingerprints enrolled. No biometric authentication is required to access this screen.

Each screen provides the same information and allows you to edit the same details.

You are recommended to assign the Initial PIV Enrollment and Update PIV Applicant options in the **Edit Roles** workflow to your operators who carry out PIV enrollment, and to assign the Edit PIV Applicant option only to administrative users who may need to carry out edits on people accounts that already have fingerprints enrolled, but cannot use the person's fingerprints to authenticate.

For FIPS 201 compliance, subsequent updates to an applicant's record after the initial enrollment should be authenticated using the applicant's fingerprints; for more information about compliance with FIPS 201, see section *5.15.1*, *The PIV Applicant Editor role*.

You can add applicants to MyID in the following ways:

- Enroll using the MyID Core API.

  See the ***MyID Core API*** guide for details.
- Manually add using the **Edit Person** workflow (in MyID Desktop) or the Add Person screen (in the MyID Operator Client) and assign the PIV Applicant role.
- Edit a person from a directory using the Edit Person (Directory) screen in the MyID Operator Client, 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.

- If you use the **Request Card** workflow to import a user, by default the user will not be assigned the PIV Applicant role, and you will be unable to edit the users using the Edit PIV Applicant screen. To remedy this, you can set the default roles for the group to which you are adding the user to include the PIV Applicant role.

  See the *Default roles* section in the ***Administration Guide*** for details.

  However, you *can* edit the person using the Initial PIV Enrollment screen, even if the person does not have the PIV Applicant role.

5.15.1 The PIV Applicant Editor role

The PIV Applicant Editor role is created by default, and on initial configuration provides access to the Edit PIV Applicant and Edit Person screens in the MyID Operator client. 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.

You must assign the PIV Applicant Editor role to the operators you want to be able to assign the PIV Applicant role to applicants.

Important: The PIV Applicant Editor role is created with its logon mechanisms set to Smart Card only – if you log on to MyID using security phrases or integrated Windows logon, you *cannot* assign the PIV Applicant role to any users. In the MyID Operator Client, the PIV Applicant role does not appear in the list if you cannot assign it; in MyID Desktop, if you attempt to assign the PIV Applicant role without logging on with the correct mechanism, an error similar to the following appears:

```
Supplied logon name is invalid. Please enter a new logon name.
```

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. For FIPS 201 compliance, subsequent updates to an applicant's record after the initial enrollment should be authenticated using the applicant's fingerprints; therefore you are recommended to remove access to the Edit PIV Applicant workflow from the PIV Applicant Editor role (as this screen overrides any biometric authentication requirements) and instead provide access to the Initial PIV Enrollment screen (which allows you to carry out the initial enrollment, including capturing biometrics, but cannot be used once fingerprints have been saved) and Update PIV Applicant screen (which allows you to update an applicant's account that already has fingerprints captured, but requires fingerprint authentication to access).

If you assign both **Initial PIV Enrollment** and **Update PIV Applicant** to an operator in the **Edit Roles** workflow, the MyID Operator Client displays the appropriate option for the applicant at their stage in the enrollment process; if the applicant does not yet have fingerprints enrolled, the operator sees only the **Initial PIV Enrollment** option. Once the applicant's fingerprints have been saved, the operator sees only the **Update PIV Applicant** option.

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.

See the *Remote PIN Management utility for PIV cards* section in the ***Operator's Guide*** for details.

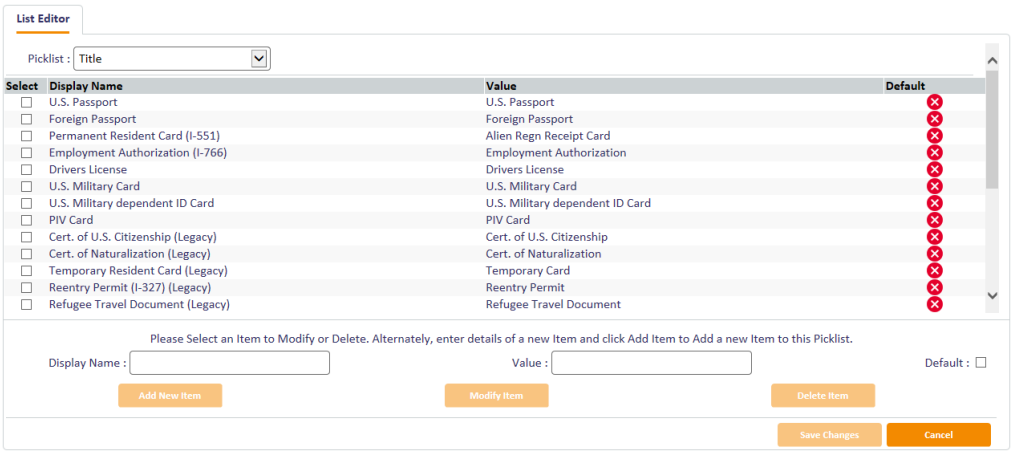
5.17 Identity documents

MyID 12.4 provides an updated list of the identity documents available on the **APPLICATION** tab of the Edit PIV Applicant screen to match the specifications of the section 2.7 of the FIPS 201-3 PIV Identity Proofing and Registration Requirements (***pages.nist.gov/FIPS201/requirements/#s-2-7***).

If you are upgrading from a system earlier than MyID 12.4, the upgrade process does not change the existing list of identity documents. You must use the **List Editor** workflow to update your system to include the latest list of primary and secondary identity documents.

You can add, remove, and edit entries in these lists using the **List Editor** workflow; see the *Changing list entries* section in the ***Administration Guide***.

Note: Both the **First identity document** and the **Second identity document** lists appear in the **Picklist** drop-down list of the **List Editor** workflow under the name **Title**; this is the name of the field on the **APPLICATION** tab of the Edit PIV Applicant screen that displays the contents of these lists, which is the same for both documents. The first **Title** list is the **First identity document** list (starting **U.S. Passport**, **Foreign Passport** on systems before MyID 12.4):



Similarly, the second **Title** list is the **Second identity document** list (starting **U.S. Passport**, **Cert. of U.S. Citizenship** on systems before MyID 12.4).

Update the lists to include the following:

First identity document	
Value	**Display Value**
U.S. Passport	U.S. Passport
U.S. Passport Card	U.S. Passport Card
Foreign Passport	Foreign Passport
Permanent Resident Card (I-551)	Permanent Resident Card (I-551)
Employment Authorization (I-766)	Employment Authorization (I-766)
Drivers License	Drivers License
REAL-ID compliant ID Card	REAL-ID compliant ID Card
U.S. Military Card	U.S. Military Card
U.S. Military Dependent ID Card	U.S. Military Dependent ID Card
PIV Card	PIV Card

Second identity document	
Value	**Display Value**
U.S. Passport	U.S. Passport
U.S. Passport Card	U.S. Passport Card
Foreign Passport	Foreign Passport
Permanent Resident Card (I-551)	Permanent Resident Card (I-551)
Employment Authorization (I-766)	Employment Authorization (I-766)
Drivers License	Drivers License
REAL-ID compliant ID Card	REAL-ID compliant ID Card
U.S. Military Card	U.S. Military Card
U.S. Military Dependent ID Card	U.S. Military Dependent ID Card
PIV Card	PIV Card
Government issued Photo ID Card	Government issued Photo ID Card
Merchant Mariner Card	Merchant Mariner Card
Cert. of U.S. Citizenship	Cert. of U.S. Citizenship
Cert. of Naturalization	Cert. of Naturalization
U.S. Citizen ID	U.S. Citizen ID
U.S. Resident Citizen Card (I-179)	U.S. Resident Citizen Card (I-179)
Certificate of Birth Abroad (Form FS-545)	Certificate of Birth Abroad (Form FS-545)
Certificate of Report of Birth (Form DS-1350)	Certificate of Report of Birth (Form DS-1350)
Reentry Permit (Form I-327)	Reentry Permit (Form I-327)
Employment Auth Doc (DHS)	Employment Auth Doc (DHS)
Canadian Drivers License	Canadian Drivers License
Native American Tribal	Native American Tribal
Birth Certificate	Birth Certificate

Note: Section 2.7 of the FIPS-201-3 PIV Identity Proofing and Registration Requirements also lists a U.S. Social Security Card issued by the Social Security Administration as an accepted second identity document; this has been omitted from the above list due to feedback from users. You can add this document type if required.

6 Card layout and printing

MyID lets you specify the physical appearance of the smart cards 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. See:

pages.nist.gov/FIPS201/frontend/#s-4-1-4

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 (that is, 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

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 1F – 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 2F – 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 201-3 section 4.1.4.1. See the *Externally formatted image fields* section in the ***Administration Guide*** for details.

6.3.3 Zone 8F – 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 10F – Agency, Department, or Organization (**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 14F – Card 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 YYYYMMMDD, to be FIPS 201 compliant.

6.3.6 Zone 3F – 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 4F – Agency-Specific Text Area (GP.15 / CPS.21)

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

6.3.8 Zone 5F – Rank (GP.16 / CPS.22)

This zone should be associated with the **Rank** attribute of the cardholder.

6.3.9 Zone 6F – Portable Data File (PDF) 417 Two-Dimensional Bar Code (Deprecated) (GP.17 / CPS.23)

This zone is now deprecated, and you are recommended to update your card layouts to remove this zone. New installations of MyID provide card layouts that do not contain this zone.

6.3.10 Zone 9F – 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 11F – 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 12F – 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 13F – 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 YYYYMMMDD, in order to be FIPS 201 compliant.

6.3.14 Zone 15F – Color-Coding for Employee Affiliation (GP.25, 26, 27 / CPS.31, 32, 33)

This zone is the background for the 'Name' field (Zone 2F) 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 16F – Photograph 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 17F – 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 18F – Color Code for Employee Affiliation (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 19F – Card Expiration Date (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 20F – 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 1B – Agency Card Serial Number (GP.12 / CPS.18)

The card serial number should be entered in this zone.

6.4.2 Zone 2B – Issuer Identification Number (GP.13 / CPS.19)

The issuer identification should contain the Issuer ID.

6.4.3 Zone 4B – Return Address (GP.33 / CPS.39)

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

6.4.4 Zone 5B – Physical Characteristics of Cardholder (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 6B – Additional Language for Emergency Response Officials (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 7B – Section 499, Title 18 Language (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 8B – Linear 3 of 9 Bar Code (Deprecated) (**GP.37, 38, 39 / CPS.43, 44, 45**)

This zone is now deprecated, and you are recommended to update your card layouts to remove this zone. New installations of MyID provide card layouts that do not contain this zone.

6.4.8 Zone 9B and Zone 10B – 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 3rd 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 SP800-73-4.

7.2.1 PIV conformance tests

A PIV card issued to a NIST-compliant user by the current version of MyID has been tested for PIV conformance using the GSA PIV Conformance tool:

github.com/GSA/piv-conformance

The following version of the tool was used:

- `piv-conformance v1.0.9`

The PIV card passed the tests as expected.

7.2.2 Data objects

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 (where supported by the card). (**EP.3**, **EP.4**, **EP.6**, **EP.7**, **EP.9**)

Buffer Description	BER-TLV Tag	M/O	Supported by MyID
Card Capabilities Container	'5FC107'	M	Yes
Card Holder Unique Identifier	'5FC102'	M	Yes
X.509 Certificate for PIV Authentication (9A)	'5FC105'	M	Yes
Card Holder Fingerprints	'5FC103'	M	Yes
Printed Information	'5FC109'	O	Yes
Card Holder Facial Image	'5FC108'	O	Yes **EP.7**
X.509 Certificate for Digital Signature (9C)	'5FC10A'	O	Yes
X.509 Certificate for Key Management (9D)	'5FC10B'	O	Yes
X.509 Certificate for Card Authentication (9E)	'5FC101'	O	Yes
Security Object	'5FC106'	M	Yes
Discovery Object	'7E'	O	Yes
Key History Object	'5FC10C'	O	Yes
Retired X.509 Certificate for Key Management 1 (Key reference '82')	'5FC10D'	O	Yes
Retired X.509 Certificate for Key Management 2 (Key reference '83')	'5FC10E'	O	Yes
Retired X.509 Certificate for Key Management 3 (Key reference '84')	'5FC10F'	O	Yes
Retired X.509 Certificate for Key Management 4 (Key reference '85')	'5FC110'	O	Yes

Buffer Description	BER-TLV Tag	M/O	Supported by MyID
Retired X.509 Certificate for Key Management 5 (Key reference '86')	'5FC111'	O	Yes
Retired X.509 Certificate for Key Management 6 (Key reference '87')	'5FC112'	O	Yes
Retired X.509 Certificate for Key Management 7 (Key reference '88')	'5FC113'	O	Yes
Retired X.509 Certificate for Key Management 8 (Key reference '89')	'5FC114'	O	Yes
Retired X.509 Certificate for Key Management 9 (Key reference '8A')	'5FC115'	O	Yes
Retired X.509 Certificate for Key Management 10 (Key reference '8B')	'5FC116'	O	Yes
Retired X.509 Certificate for Key Management 11 (Key reference '8C')	'5FC117'	O	Yes
Retired X.509 Certificate for Key Management 12 (Key reference '8D')	'5FC118'	O	Yes
Retired X.509 Certificate for Key Management 13 (Key reference '8E')	'5FC119'	O	Yes
Retired X.509 Certificate for Key Management 14 (Key reference '8F')	'5FC11A'	O	Yes
Retired X.509 Certificate for Key Management 15 (Key reference '90')	'5FC11B'	O	Yes
Retired X.509 Certificate for Key Management 16 (Key reference '91')	'5FC11C'	O	Yes
Retired X.509 Certificate for Key Management 17 (Key reference '92')	'5FC11D'	O	Yes
Retired X.509 Certificate for Key Management 18 (Key reference '93')	'5FC11E'	O	Yes
Retired X.509 Certificate for Key Management 19 (Key reference '94')	'5FC11F'	O	Yes
Retired X.509 Certificate for Key Management 20 (Key reference '95')	'5FC120'	O	Yes
Cardholder Iris Images	'5FC121'	O	Yes
Secure Messaging Certificate Signer	'5FC122'	O	Yes
Pairing Code Reference Data	'5FC123'	O	Yes

7.2.3 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.

7.2.4 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.

7.2.5 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

Data Element (TLV)	Tag	Type	Max. Bytes	Supported by MyID
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
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

7.2.6 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

7.2.7 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.

7.2.8 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**)

7.2.9 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

7.2.10 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.

7.2.11 Discovery Object

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

7.2.12 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.