pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Identity Card Production, Personalization and Issuance

ITP Number	***Effective Date***
GEN-SEC013F	January 18, 2008
Category	***Supersedes***
Recommended Policy	
Contact	***Scheduled Review***
RA-ITCentral@pa.gov	Annual

1 Introduction

The purpose of this document is to define the Identity Card Production, Personalization and Issuance policy established in ITP-SEC013 - *Identity Protection and Access Management (IPAM) Architectural Standard*.

This document is intended to assist commonwealth agencies with the enrollment, identity proofing, issuance and maintenance processes for credentialing employees, non-employee first responders and business partners with Personal Identity Verification (PIV) Cards. These issuance procedures complement the enrollment, identity proofing and vetting processes detailed in GEN-SEC013D - *Enrollment, Identity Proofing and Vetting,* to establish and validate the prospective cardholder's identity, and bind that identity to the Commonwealth PIV Card at the time of issuance. Together, these processes establish the foundation for a "trusted" identity credential that may be accepted both within the commonwealth and nationally, in response to the critical business drivers described in ITP-SEC013.

This document adheres to all guidance and policy requirements specified in the references listed in APP-SEC013A - *IPAM Glossary*, and most particularly with NIST Special Publication 800-79-1*: Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations* and the *US Government Public Key Infrastructure Cross-Certification Criteria and Methodology*.

1.1 Organization

This document provides the following information:

- Section 2 provides an overview of the PIV enrollment, identity proofing, and issuance processes.
- Section 3 explains the critical roles associated with the PIV enrollment, identity proofing, and issuance processes.
    - Section 4 describes the major components of the PIV enrollment, identity proofing, and issuance process.
    - Section 5 details the primary processes for enrollment, identity verification, issuance and maintenance for the Commonwealth PIV Card.
    - Section describes several ancillary processes which, in addition to the primary processes described in chapter 5, are required to complete the overall PIV Card credentialing process.

- Section 7 identifies some additional considerations with respect to the PIV Card credentialing process that are not to be overlooked.
- References and acronym definitions are provided in GEN-SEC013A - *Identity Protection and Access Management Glossary*.

2. Overview

Adherence to a common standard for issuing secure and reliable forms of identification to commonwealth employees and business partners improves security, increases efficiency, reduces identity fraud, and protects personal privacy. A standardized and accredited identity framework facilitates the commonwealth's ability to establish reliable levels of trust for its identity credentials internally, with other states, and with federal agencies by eliminating the wide variation of quality and security in the forms of identification used to gain access to commonwealth physical assets (buildings, facilities) and logical assets (computer networks, applications).

Federal Information Processing Standards (FIPS) Publication 201-1 stipulates that the PIV Card credentialing process is to be certified and accredited. *Certification* in this context means a formal process of assessing and verifying the reliability and capability of a PIV Card Issuer (PCI) to enroll approved applicants and issue PIV Cards. *Accreditation* of a PCI is the official management decision of a Designated Accreditation Authority (DAA) to authorize a PCI to operate after determining that the reliability of the PCI has satisfactorily been established through appropriate assessment and certification processes. Federal accreditation is founded on the principle of trust, established via strict adherence to a common set of criteria for the secure transmission of data and for establishing levels of identity assurance. These assurance levels and their associate proofing methods are detailed in GEN-SEC013D - *Enrollment, Identity Proofing and Vetting*. Secure transmission of data is supported via a Public Key Infrastructure (PKI) as described in GEN-SEC013G - *Public Key Infrastructure.*

Within the commonwealth agencies provide the PCI service. The IPAM Architecture Team serves as the DAA to certify and accredit the credentialing process of each PCI. While the exact composition of these processes are left up to each agency (see the role description in Section 3.4, *Process Approval Authority*), they are to conform to the policies and practices established here and in the other related Information Technology Policies (ITPs).

Figure 1 below outlines the overall Identity Management model for the Commonwealth.

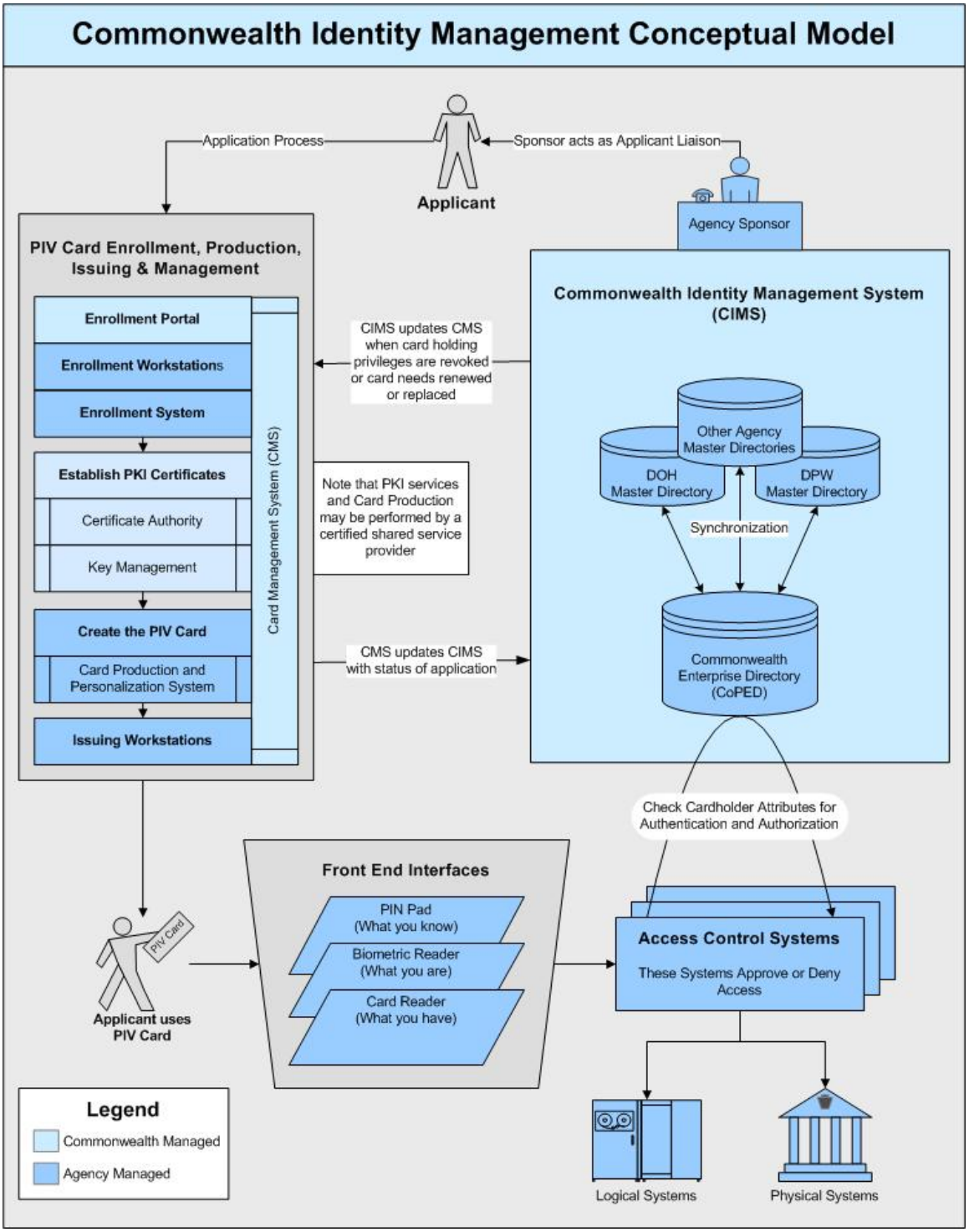


Figure 1

This document describes the PIV Card enrollment, production, issuing and management processes illustrated in the like-named box on the left in Figure 1.

While some of these functions may be automated or relegated to accredited service providers, individual agencies maintain responsibility for enrolling applicants, collecting identity proofing documents, and issuing the PIV Cards.

This document specifies the minimum steps necessary for agencies to meet commonwealth standards and Federal Bridge Certification Authority (FBCA) accreditation requirements (as specified in NIST SP800-79-1) for these functions. Individual agencies may enhance or expand upon these processes to meet their organizational needs as long as the resulting process is also auditable, secure, and meets each of the requirements set forth in this document.

2.1 Minimum Requirements

Minimum requirements for the PIV enrollment, identity proofing, and issuance process include:

a. Accredited Process - The proofing and registration process of each agency is to be approved and accredited by the commonwealth.
b. Process Adherence - The approved and accredited proofing and registration processes are to be followed.
c. Accredited Systems - Only accredited systems and accredited third party providers may be used.
d. Physical Presence - Applicants are to appear in person at least twice – once before an Enrollment Official when applying for the Commonwealth PIV Card, and a second time before the issuing official to receive the card.
e. Separation of Roles - No single individual may have the power to request issuance of a PIV credential without the approval of a second authorized person.
f. Secure Transmissions - All data transmitted throughout the system is to be encrypted to ensure the security of the card issuance process, including both the integrity of the process and the confidentiality of any personal private information.
g. Credentialed Officials – Sponsors, Enrollment Officials, Application Approval Officials, Issuing Officials, and Revocation Officials are to have already been issued a valid PIV Card, at an assurance level at least as high as that requested for the applicant.

3. Roles for the Enrollment, Identity Proofing, and Issuing Processes

Agencies may establish independent enrollment/proofing/issuing systems. The critical roles associated with the PIV enrollment, identity proofing, and issuance processes are explained in this chapter. Any or all of these roles and corresponding processes may be performed by accredited service providers who comply with this standard. Any role may be an ancillary responsibility assigned to personnel who have other primary duties, and the same individual may be assigned more than a single role; however, for security reasons, no single individual may simultaneously fulfill more than one of the roles that contain the word “Official” in its title, except as noted in the following role descriptions.

Figure 2 below depicts how the major roles are involved in the eight primary PIV enrollment, identity proofing and issuance processes.

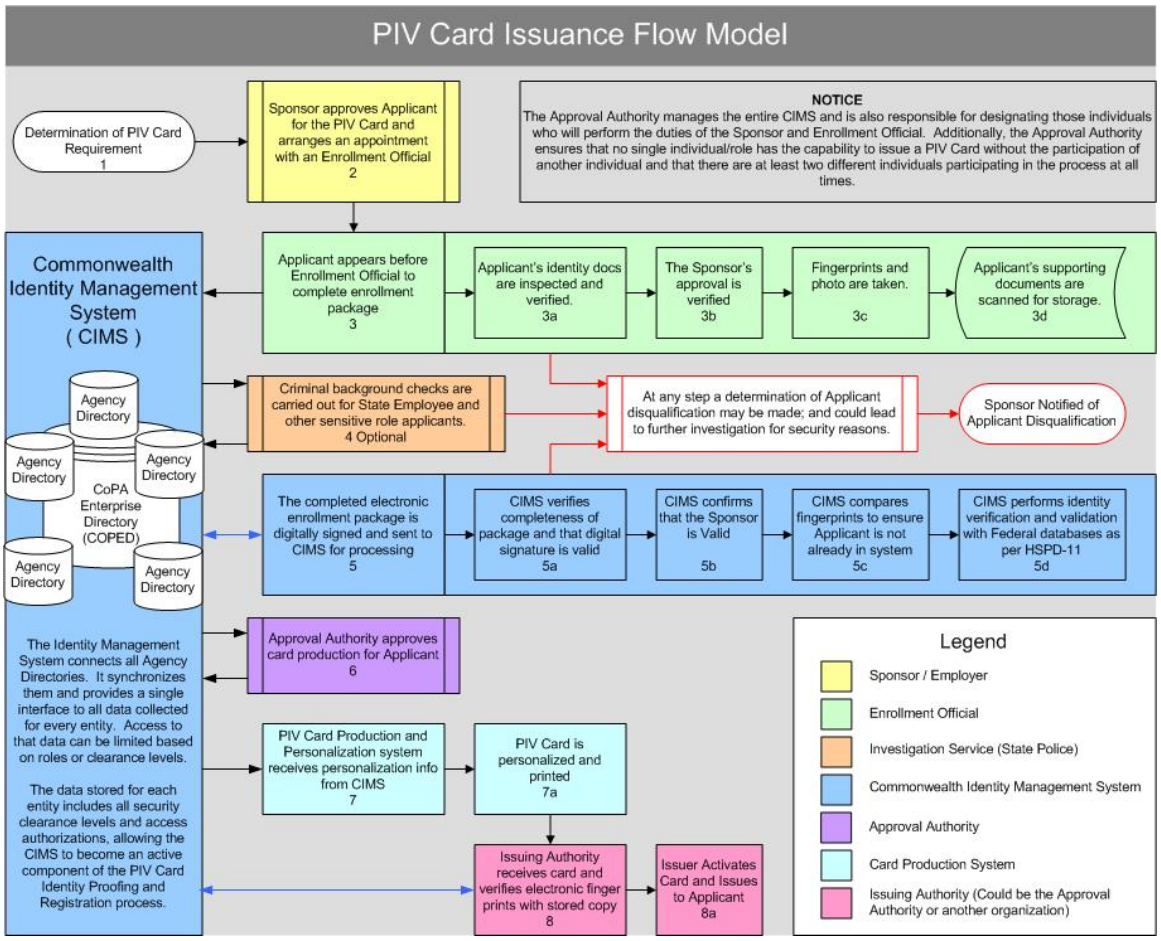


Figure 2

a. Applicant

The applicant is the individual for whom a commonwealth PIV Card has been requested. Applicants are to have a sponsor in order to apply for a PIV Card, and are responsible for providing the necessary supporting identity source-documents to prove their claimed identity.

b. Sponsor

The sponsor is the individual who validates an applicant's requirement for a PIV Card and who authorizes the applicant's request. A sponsor may not also be an approval official. The PIV Sponsor is to:

- Be authorized in writing by the Process Approval Authority to request a PIV Card on behalf of the applicant.
- Have valid justification for requesting a PIV Card for an applicant.
- Be a Commonwealth employee or authorized agent.
- Already have been issued a valid PIV Card, and carry an assurance level rating which is at least as high as that for which the applicant is applying.

- Have successfully completed the Commonwealth PIV Sponsor training.

c. Enrollment Official

The Enrollment Official initiates the chain of trust for identity verification. He or she confirms sponsorship, ensures that the applicant's biometric (photo, fingerprints) is in the enrollment package, validates the applicant's source identity-proofing documentation, and verifies that any required background checks are successfully completed. The Enrollment Official is responsible for ensuring that the enrollment packages are complete and that they are digitized into the Card Management System (CMS).

The PIV Enrollment Official is to:

- Be designated in writing as a PIV Enrollment Official by the Process Approval Authority.
- Be able to assess the reasonableness of the applicant's identity-proofing documents. Reasonableness in this context indicates that the PIV Enrollment Official is trained to detect any improprieties in these documents.
- Be able to evaluate whether a PIV application is satisfactory and also able to apply appropriate commonwealth or agency-specific processes to an unsatisfactory PIV Card application. Thus, the PIV Enrollment Official is to have been trained on commonwealth and agency processes and procedures for adjudicating an unsatisfactory PIV Card application.
- Be a commonwealth employee or authorized agent.
- Already have been issued a valid PIV Card, and carry an assurance level rating which is at least as high as that for which the applicant is applying.
- Have successfully completed a Pennsylvania Access to Criminal History (PATCH) check.
- Have successfully completed the PIV Enrollment Official training.

d. Process Approval Authority

The Process Approval Authority establishes the organizational hierarchy for the enrollment and issuance processes, and manages the total scope of the chain of trust established for the PIV Card enrollment, identity verification, issuance, and maintenance processes. The agency's processes are subject to approval by the Designated Accreditation Authority (DAA). This includes designating approved sponsors and credentialing officials. These responsibilities are to be delegated in writing, and only to designated commonwealth officials or agents. The Process Approval Authority also manages all related privacy and security controls. The Process Approval Authority is to be designated in writing by the agency head (Cabinet Secretary or equivalent). The Process Approval Authority may not hold any other roles within the enrollment, identity proofing, or issuance processes, except the role of sponsor.

e. Application Approval Official

The PIV Application Approval Official provides adjudication of an identity claim if any of the core checks identify a potential risk.

Approval for a requested PIV Card may be automatic if all identity proofing and background checks return positive results. In the absence of an automated approval process, and upon successful completion of the appropriate identity verification process, it is the PIV Application Approval Official who approves the PIV Card's production. The PIV Application Approval Official may approve issuance of a PIV Card prior to completion of all core checks for identity verification and validation if these processes exceed ten (10) days and the issuance of the PIV Card is urgent. The PIV Application Approval Official is to:

- Be designated in writing by the Process Approval Authority as a PIV Application Approval Official.
- Be a commonwealth employee or authorized agent.
- Already have a valid PIV Card, and carry an assurance level rating which is at least as high as that for which the applicant is applying.
- Have successfully completed a PA PATCH check.
- Have successfully completed the PIV Application Approval Official Training.

f. Issuing Official

The PIV Issuing Official activates PIV Card and issues it to an applicant following the positive completion of all identity proofing, background checks, and related approvals. The PIV Issuing Official is responsible for the security of the PIV Cards from time of receipt (from the card production facility) until issuance to the card holder. The PIV Issuing Official and PIV Revocation Official roles may be held by the same person, thereby simplifying re-issuance tasks. The PIV Issuing Official is to:

- Be designated in writing by the Process Approval Authority as a PIV Issuing Official.
- Be a commonwealth employee or authorized agent.
- Already have a valid PIV Card, and carry an assurance level rating which is at least as high as that for which the applicant is applying.
- Have successfully completed a PA PATCH check.
- Have successfully completed the PIV Issuing Official Training.

g. Revocation Official

Certain circumstances (such as employment termination) require a PIV Card to be suspended, revoked, or destroyed. Agencies are to have strict policies governing the circumstances that would result in such an action. The PIV Revocation Official ensures compliance with these policies and is responsible for performing the required operations. The PIV Issuing Official and PIV Revocation Official roles may be held by the same person, thereby simplifying re-issuance tasks.

The PIV Revocation Official is to:

- Be designated in writing by the Process Approval Authority as a PIV Revocation Official.
- Be a commonwealth employee or authorized agent.
- Already have been issued a valid PIV Card, and carry an assurance level rating which is at least as high as that of the cardholder being addressed.
- Have successfully completed the PIV Revocation Official Training.

h. Senior Agency Privacy Official

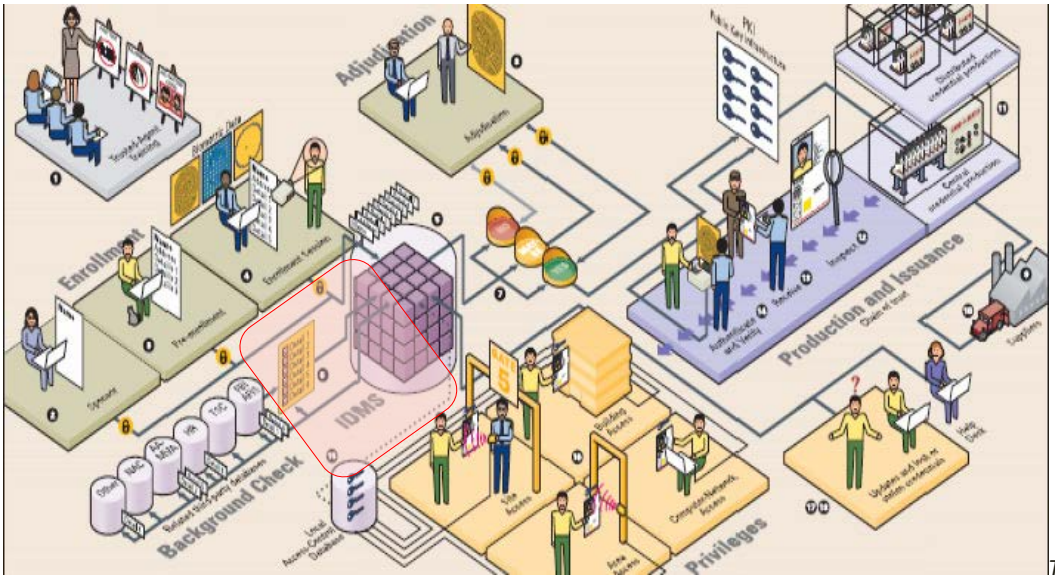
Agencies are required to appoint a PIV Senior Agency Privacy Official. This individual may not assume any other operational role in the PIV system (i.e., sponsor or official). The PIV Senior Agency Privacy Official is to be the lead for implementing PIV privacy policies, and ensure that they are being applied and maintained in a consistent manner throughout an agency's PIV life cycle process. The PIV Senior Agency Privacy Official is to have intimate knowledge of commonwealth and agency-specific privacy policies and best practices**.** The agency's Privacy Officer, as stipulated in ITP-PRV002 - *Electronic Information Privacy Officer*, would be a logical candidate to fulfill this role.

4. Components

This section describes the major components of the PIV enrollment, identity proofing, and issuance processes. In addition to components to be implemented by each agency as part of its PIV processes, this section also includes components implemented by the commonwealth as "shared services" provided by accredited service providers.

a. Card Management System

Figure 3 below illustrates how the various components of the PIV Card provisioning and issuance process interconnect.



This illustration reproduced from a BearingPoint slide presentation on FIPS 201 PIV Credentialing.

Figure 3

The CMS is a commonwealth-managed shared service that serves as the system of record for PIV Cards issued by the commonwealth and its agencies. The CMS monitors and manages workflow for the enrollment and issuance processes, ensuring adherence to commonwealth standards, and tracks the status of a PIV Card credential throughout its lifecycle, from initial production request through personalization and printing, activation and issuance, suspension, revocation, and final destruction. The CMS provides automation for some of the workflow steps, and interfaces with the Identity Management System (IDMS) for status reporting and cardholder cross-referencing. This IDMS is shown in Figure 3, highlighted in red, and is discussed fully in GEN-SEC013B - *Directory Services Architecture*. The CMS also performs searches on various attributes of the applicant to ensure that he or she has not already been enrolled under a different name or for another agency.

The CMS provides services that:

- Notify the applicants of the status of their PIV Card application;
- Notify the sponsor of the status of the PIV Card application;
- Enable authorized users to verify whether an issued PIV Card is still valid.

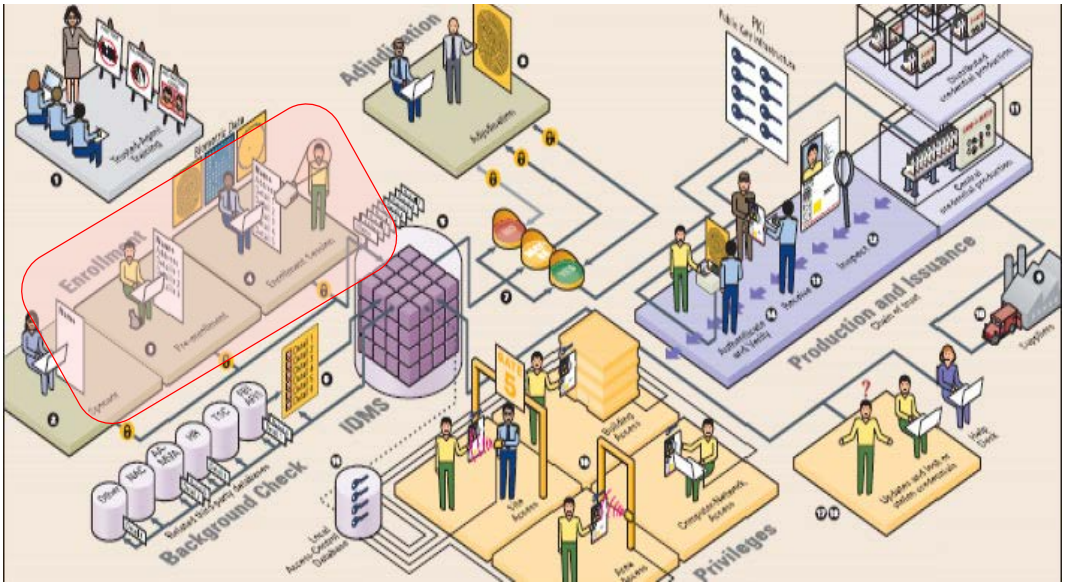
The CMS manages the following information:

- A digitized copy of the completed and signed PIV enrollment package, including:
  - Identity source documents;
  - The completed and signed background form received from the applicant; and
  - Any other materials used to prove the identity of the applicant;
- Results of the required background check;
- The credential identifier such as an identity credential serial number;
- The expiration date of the identity credential;
- Unique identifier for each approved applicant;
- Permanent record (live or archive, depending on the status of the card) of each card's information listed above; and
- The original biometric data captured at enrollment (photo and fingerprints), stored encrypted in the database for security purposes.

The CMS also provides complete personalization and printing information to the card production facility for the production of all approved PIV credentials.

b. Enrollment System

Figure 4 below illustrates how the Enrollment System is used within the provisioning and issuance process.

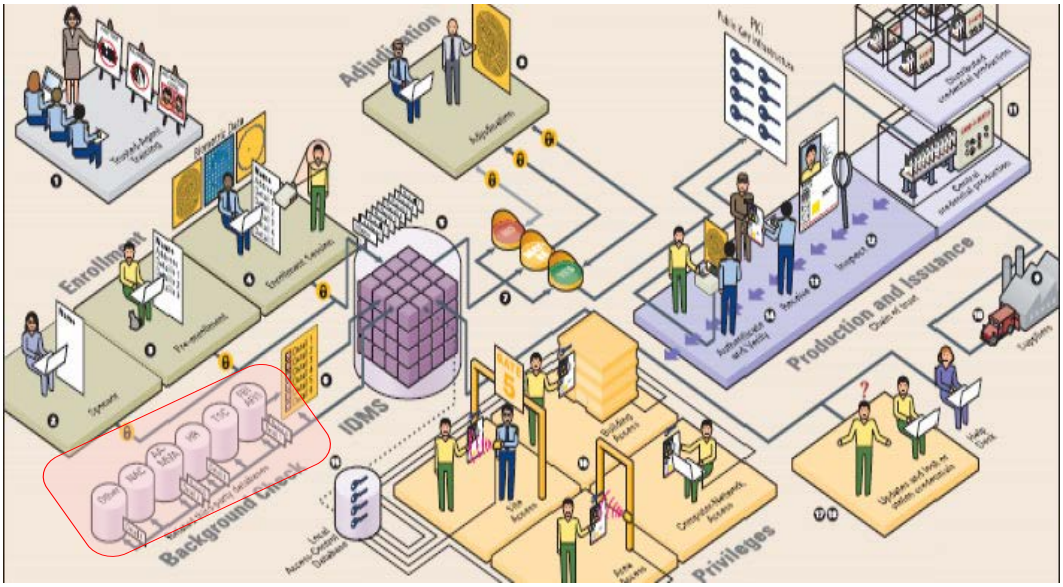


This illustration reproduced from a BearingPoint slide presentation on FIPS 201 PIV Credentialing.

Figure 4

The PIV Enrollment Official uses the Enrollment System to initiate the chain of trust for identity proofing. The Enrollment System provides tools for the Enrollment Official to confirm sponsorship, bind applicants to their biometrics, and validate identity claim documentation. The Enrollment System delivers the secured enrollment package to the CMS for tracking and storage, making it available as needed for identity proofing and adjudication.

c. Investigative Service

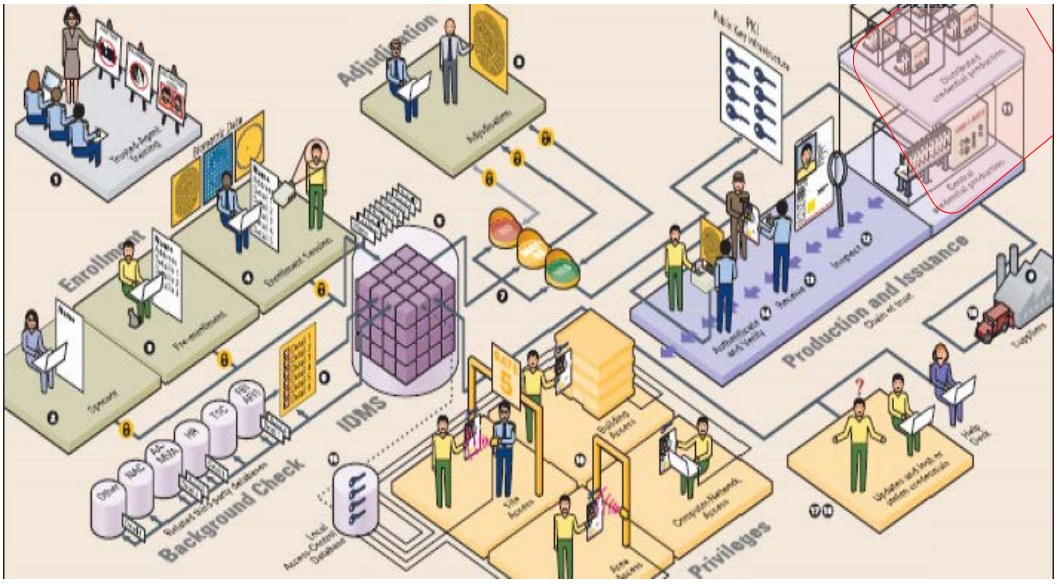


This illustration reproduced from a BearingPoint slide presentation on FIPS 201 PIV Credentialing.

Figure 5

PATCH checks, conducted by the Pennsylvania State Police (PSP), are required for commonwealth employees and first responders applying for PIV Cards. These PATCH checks provide the functional equivalent to the FIPS 201-1 requirement that all federal employees require National Agency Checks initiated by the Office of Personnel Management.

d. Card Production and Personalization Systems



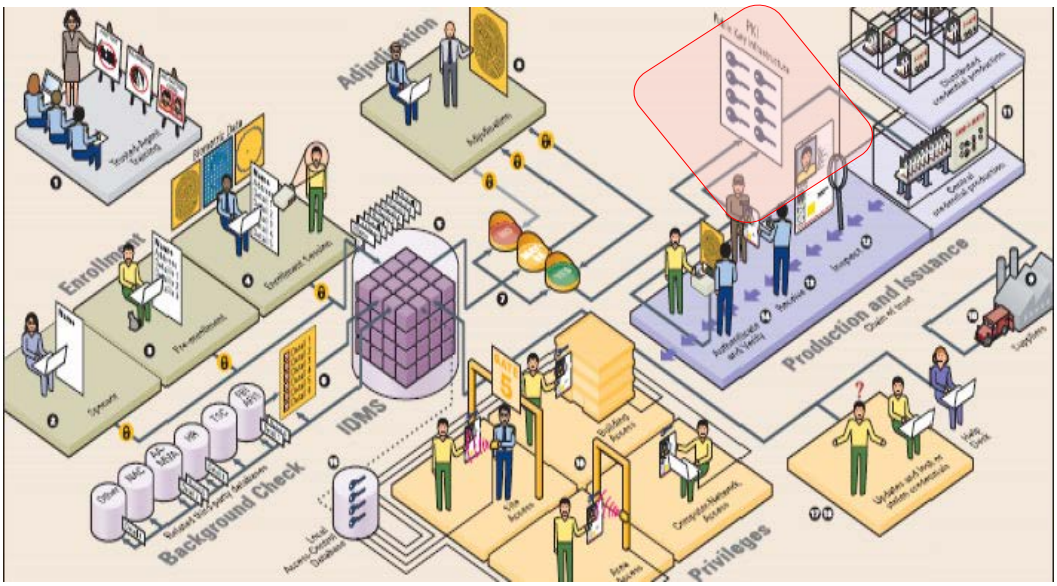
This illustration reproduced from a BearingPoint slide presentation on FIPS 201 PIV Credentialing.

Figure 6

The Card Production and Personalization Systems provide an inventory-controlled process to create and personalize Commonwealth approved, agency specific PIV Cards. Personalization is the function of adding personal data (name, title, and photograph) to this credential. The Production and Personalization Systems also include mechanisms to track PIV Card production status, and to control and protect inventory (blank card stock as well as personalized/printed card stock waiting to be issued to the applicant). Agencies are authorized to stand up their own Card Production and Personalization Systems, or to use a federally accredited shared service provider.

The PIV Card Production System provider is responsible for controlling PIV Card stock (i.e., manages stock and verifies that depleted stock is due solely to the issuance of valid credentials), maintaining Card Production and Personalization System records, and producing the actual PIV Cards with appropriate digital certificates and personalization as determined by the PCI. For approved card production system providers, refer to the FIPS Approved Products List (http://fips201ep.cio.gov/apl.php).

e. Public Key Infrastructure



This illustration reproduced from a BearingPoint slide presentation on FIPS 201 PIV Credentialing.

Figure 7

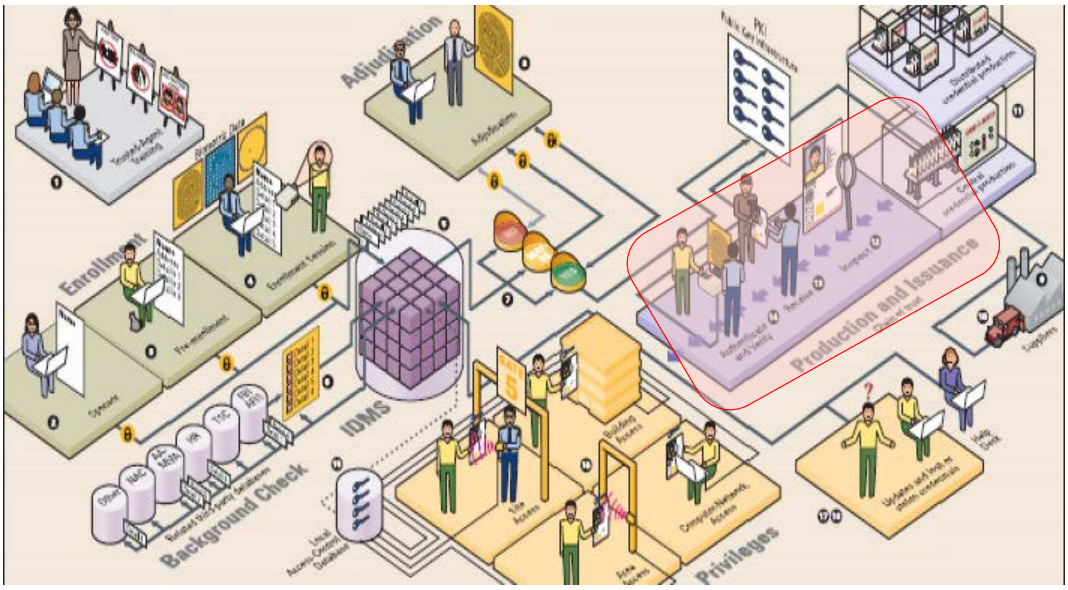
The Public Key Infrastructure (PKI) assigns asymmetric encryption key pairs (Public and Private) to each PIV Cardholder, as per the Commonwealth x.509 PKI Certificate Policy and GEN-SEC013G - *Public Key Infrastructure.* This ITP explains the commonwealth's relationship with an accredited Shared Service Provider (SSP) for PKI key management. The SSP manages issuance of private keys to the Card Production and Personalization Systems, publishes the private keys in digital certificates, maintains the key archives for retrieval of encrypted information for lost private keys, maintains a digital certificate revocation list (CRL), and manages key and certificate expirations. The SSP also maintains an interface to the Card Production and Personalization System to enable public key certificates to be written directly to the PIV Cards without excessive intermediate storage requirements.

The SSP provides all PKI-related functions for the enrollment and issuance process, including:

- Digitally signs the card recipient's PIV biometrics and the Cardholder User Identification (CHUID).
- Signs and issues the card recipient's authentication certificate that is stored on the PIV Card.
- As a federally accredited SSP, participates in the Federal PKI for the Common Policy managed by the Federal PKI Policy Authority.

Reference STD-SEC014C for the Commonwealth's named SSP for PKI management.

f. Card Issuance System

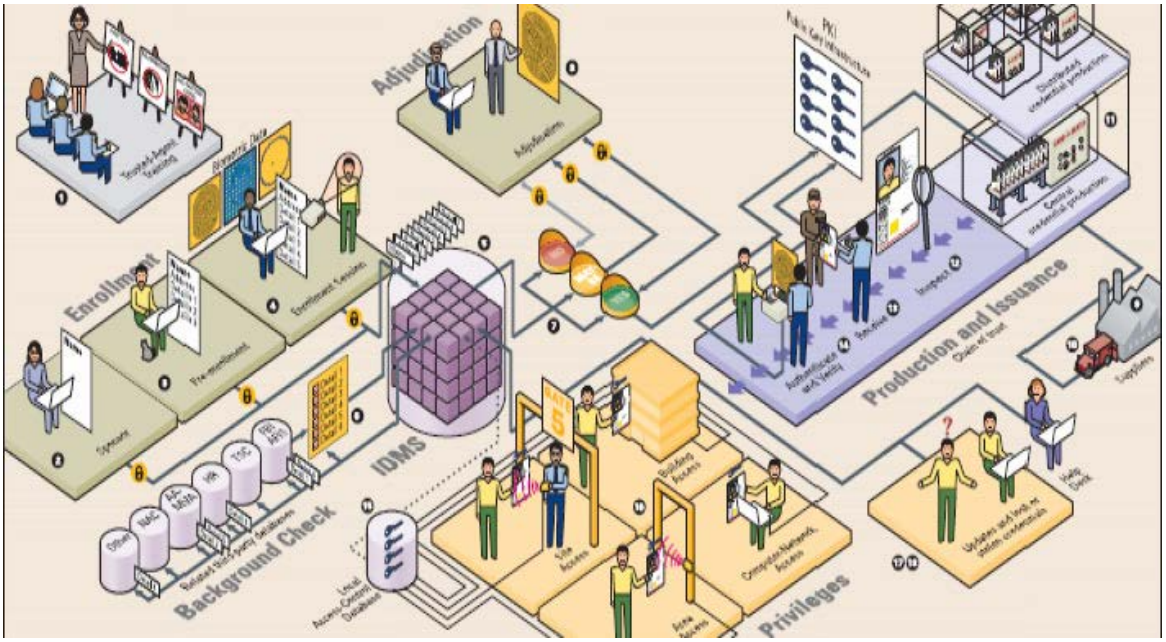


This illustration reproduced from a BearingPoint slide presentation on FIPS 201 PIV Credentialing.

Figure 8

The PIV Issuing Official uses the Card Issuance System to activate and issue the PIV Cards. He or she provides tools for conducting a biometric match to ensure that the individual receiving the card is the original applicant, and includes an interface to the CMS to support status tracking.

5. Issuance Process



This illustration reproduced from a BearingPoint slide presentation on FIPS 201 PIV Credentialing.

Figure 9

The following paragraphs detail the entire life cycle for enrollment, identity verification, issuance and maintenance processes for the PIV Card. These processes are illustrated in Figure 9 above; the numbers in the illustration correspond to the numbered paragraphs below. All actions taken by participants in this process for approval or denial of requests are to have an audit trail that can support both forensic and system management capabilities. This audit trail is a critical control component for the chain of trust for PIV issuance and management.

a. Trusted Agent Training

Training is required to ensure that data is collected, verified and stored appropriately, that process policy is adhered to rigorously, and to minimize the potential for errors.

- Training for PIV duties is required of trusted agents, including sponsors, PIV Enrollment Officials, Issuing Officials, Applicant Approval Officials, and Revocation Officials.
- Training may be instructor led, CD-ROM, or Web-based sessions to certify PIV officials in topics from fraudulent documents detection to privacy requirements.

b. Application to Sponsor

The applicant begins the process for obtaining an identification credential by providing a formal Commonwealth PIV Credential request to his or her sponsor. This process may be applicant-initiated or sponsor-initiated. The sponsor validates the applicant's PIV Credential request and forwards it to the Enrollment Official.

c. Pre-Enrollment

Pre-enrollment saves time by allowing the applicants to submit data about themselves in advance – potentially via an agency Web site.

- The information collected includes name, date of birth, position, and the applicant's contact information.
- Web-based pre-enrollment provides on-line appointment scheduling with the Enrollment Official and directions to the enrollment location.
- The pre-enrollment package includes the standard Commonwealth form for collecting the required background check information.
- Completed pre-enrollment packages are received by the Enrollment Official.

d. Enrollment Session

It is the Enrollment Official's responsibility to ensure that all required enrollment procedures are carried out.

- The Enrollment Official verifies the PIV request has valid sponsorship.
- The applicant appears in person and provides a valid current primary government photo ID that contains applicant's picture, and either address of record or nationality (e.g., driver's license or passport).
    - Applicants for a credentialing official role are to provide an additional independent ID document. This may be for a financial account, such as a credit card.

  - Acceptable identity source documents are listed in the Federal Employment Eligibility Verification Form I-9 (OMB No. 1115-0136); see Appendix A of this document.
- The PIV Enrollment Official conducts a visual inspection of the identification documents for validity and authenticity:
  - No signs of tampering or alteration.
  - Photos resemble the applicant.
  - Documents have not expired.
- For applicants requiring higher assurance levels (i.e. 300 or above, as explained in GEN-SEC013C - *Access Management and Control*) the PIV Enrollment Official electronically verifies the authenticity of the source documents. When electronic verification is not an available option, the PIV Enrollment Official is to use other available methods to authenticate the source and integrity of the identity source documents. This includes verification of the ID numbers and account numbers through record checks either with the applicable agency or institution, or through credit bureaus or similar databases. The PIV Enrollment Official confirms that name, date of birth, address, and other personal information in those records are consistent with the application, and sufficient to uniquely identify the individual.
- Validated documents are scanned into the enrollment system.
- The PIV Enrollment Official digitally photographs the applicant's face, as per NIST SP 800-76 specifications. This facial image is maintained in the CMS, printed on the card, and embedded electronically in the card's Integrated Circuit Chip (ICC). For more information on what is stored on the ICC and printed on the PIV Card, see GEN-SEC013E - *Specification for a Commonwealth Personal Identity Verification Card.*
- The PIV Enrollment Official electronically captures all ten fingerprints of the applicant. The fingerprints will be used for one-to-many matching with the database of fingerprints maintained by the FBI, and are to be captured using FBI-certified scanners and transmitted using FBI standard transactions. Minutia from two of the collected fingerprints, the right and left index fingers, will be stored electronically in the Commonwealth PIV Card ICC as described in Chapter 3 of GEN- SEC013E. If for any reason either or both of these two fingers cannot be imaged, use the next available fingers from the following list:
  - Right thumb
  - Left thumb
  - Right middle finger
  - Left middle finger
  - Right ring finger
  - Left ring finger
  - Right little finger
  - Left little finger

- The fingerprint samples and photographs are to be verified to ensure proper performance of the biometric comparison system.
- After collecting the fingerprints, the Enrollment Official is to use the CMS to perform a fingerprint search to assure that the individual identified in the package has not applied previously under a different name.

e. Submit Enrollment Package

The Enrollment Official binds the completed electronic enrollment package with his or her digital signature and submits the package to the CMS.

The completed PIV enrollment package includes:

- Scanned documents supporting identity claim.
- Fingerprint minutia templates (right and left index fingers) and digital photograph.
- Personal biographic and organizational information.
- Digital signature of PIV Enrollment Official.

The CMS initiates the enrollment workflow process.

f. Background Checks

The CMS receives the completed enrollment package and verifies its integrity:

- Confirms that all required documents, fingerprints, photographs have been submitted.
- Verifies the PIV Enrollment Official's digital signatures.

The CMS also initiates the background checks:

- Submits the request for PA PATCH background checks.
- Completes a one-to-many fingerprint search against FBI National Criminal History database.

Note: *Applicants with a valid PA PATCH background check on file do not require an additional PA PATCH background check.*

g. Ruling

If the enrollment package fulfills all of the requirements for the requested assurance level, and the applicant is found to meet agency minimum standards, the application will be approved.

The Application Approval Official may approve issuance of a PIV credential prior to completion of all core checks for identity verification and validation if these processes exceed ten days.

h. Adjudication

Adjudication is required for cases where obtaining an unequivocal "yes" or "no" decision isn't possible.

- The Application Approval Official assesses the details to make a valid determination about each case.
- The Application Approval Official also provides adjudication of identity claim if any unfavorable results or potential risks present themselves.

Agencies are to define an adjudication process specific to their individual standards. This process is to include timely notification and appeal methods for the applicant.

i. Suppliers

Suppliers of the credential components (card stock) are responsible for inventory control and security management.

j. Supply Chain

The supply chain is to be secured from beginning to end to ensure that no information or components are compromised. This is a joint responsibility of the Commonwealth and the supplier.

k. PIV Credential Personalization

The card topology is configured according to the issuing agency's criteria and in accordance with GEN-SEC013E.

Depending on the arrangement each agency or COP makes with the card production facility and according to the personalization hardware available for use by that agency, either the card producer, another accredited service provider, or the agency's own personalization station personalizes the PIV Card with the applicant's data.

Personalization includes:

- Printing the cardholder's personal information onto the PIV Card (e.g., name, personal characteristics like gender and height, photo).
- Programming the card's ICC.
- Loading the ICC operating system with the card serial number and security keys.

The card information is locked when loaded into the ICC; the card cannot be used until unlocked (activated) by the PIV Card Issuing Official.

Whether performed in-house or outsourced, the card personalization and production service is to include the following:

- Maintain a full inventory control of blank initialized or pre-issued (e.g., with the manufacturer's keys) stock, consumables and manufacturing materials.
- Retain and use a list of approved commonwealth or agency application approval officials who may submit requests for PIV Card production separate from the CMS.
- Provide acknowledgement of each commonwealth agency request to produce one or more PIV Cards.
- Notify the CMS upon completion of PIV credential production.
- Retain and use a list of approved issuers at each agency which may activate and issue PIV credentials.
- Send information regarding production of PIV credentials to approved authorities.
- Send fully completed and personalized PIV credentials to approved PIV Card Issuers.
- Document, implement, and maintain a card production, activation and Issuance Security Policy.

l. Quality Assurance

The PIV Card Production Provider employs strong quality assurance measures to ensure that compliant credentials are distributed, and periodically provides a commonwealth defined audit report detailing its quality metrics for the preceding period. The PIV Card Production Provider will provide the commonwealth an audit report detailing its quality metrics for the preceding period. The content, format, and time frame of these reports will be determined by the commonwealth.

m. Receipt

Each agency is responsible for developing a precise business process for receipt and distribution of the PIV Credentials.

The PIV Card Production Provider will securely deliver the locked PIV Cards to the agency's issuers at one or more designated issuing facilities, completing an uninterrupted chain of security. An agency may receive its locked cards at a single receiving facility and then securely distribute them by courier to the agency's various other issuing facilities, thereby maintaining the chain of security.

n. Issuance

The applicant is to appear in person to the PIV Issuing Official to receive the PIV credential. Agencies are to plan their issuance strategies carefully in order to comply with this requirement. Agencies that need to issue PIV Cards over wide geographic areas are to develop an issuance infrastructure appropriate to support their unique logistical circumstances.

Before the newly created PIV Card is given to the applicant, the PIV Issuing Official completes the following steps to ensure that the recipient is indeed the original applicant:

1 Have the recipient present the same commonwealth or federal government-issued picture identity source document that was presented during enrollment.

2 Confirm that the picture and name on this source document match the picture and name on the newly personalized PIV credential.

3 Confirm that the recipient resembles the picture on the PIV credential.

4 Confirm that the fingerprint of the recipient matches the stored fingerprint embedded in the PIV Card ICC, in accordance with SP 800-76 guidance.

When the recipient's identity is affirmed, the PIV Issuing Official activates (i.e., unlocks) the card. The issuer then releases the credential to the individual and informs him or her of the following responsibilities:

- If the PIV Card begins to wear (e.g., laminate coming loose, ink rubbing off, cuts/rips/tears occur in the card), the cardholder is to return the card to the PIV issuing official immediately. The PIV issuing official will be able to disable the old card and request a replacement card.

- If the PIV Card is lost or stolen, the cardholder is to notify the PIV Issuer immediately. The PIV issuer will be able to disable the old card and request a replacement card.
- If the PIV Card does not operate properly when inserted into a logical or physical access reader, the cardholder is to notify the PIV issuer immediately. The PIV issuer will have the old card deactivated and request a replacement card.
- If any personal information changes, such as changes in affiliation, name, or other personal information, the cardholder is to notify the sponsor immediately. The sponsor then determines if the change warrants a re-issuance of the PIV Card, and coordinates with the Revocation Official as necessary.

o. Write to Directory

Once the PIV Card has been issued, the CMS will create the user's account in the agency's master directory or update the account if one already exists. The CMS stores:

- User's unique ID as determined by the agency in accordance with related commonwealth policy.
- PIV credential serial number.
- PIV credential issue and/or expiration date.
- User's public key digital certificate.
- User's public key digital certificate issue and/or expiration date.
- A record of any non-commonwealth standard background checks performed.

Once this information is written into the agency's master directory, the Commonwealth Identity Synchronization process (metadirectory) will create or update the user's account in the Commonwealth of Pennsylvania Enterprise Directory (CoPED).

CoPED is leveraged by the various access control mechanisms deployed by the agencies to protect physical and logical resources. It also serves as the primary authentication source of the Enterprise Portal. See GEN-SEC013B - *Directory Services Architecture,* for complete details on the use of CoPED and commonwealth directory services.

6. Ancillary Processes

In addition to the primary credential issuance processes described above, several ancillary processes are required to complete the overall PIV Card credentialing process. Those ancillary processes are described in this section.

Agencies will need to develop specific business processes based on those described below for the suspension, revocation, re-issuance, and destruction of PIV Cards. The processes are to be secure and protect the privacy of PIV Cardholders. It is recommended that agencies implement a method that allows real-time updating of the CMS.

a. PIN Reset

The Personal ID Number (PIN) on a PIV Card may need to be reset if the contents of the card are locked due to the usage of an invalid PIN more than the allowed number of retries stipulated by the agency. PIN resets may be performed by the PIV Issuer. Before the reset PIV Card is returned to the cardholder, the issuing official verifies the holder's identity using the same process as when the card was issued. An agency may adopt more stringent procedures for PIN reset (including disallowing PIN reset, or requiring locked PIV Cards to be revoked); such procedures are to be formally documented by the agency.

b. Suspension, Revocation, and Destruction

Certain circumstances require a PIV credential to be suspended, revoked, or destroyed. Agencies are to have strict policies in place governing these actions, and are to specifically identify the situations that would warrant such an action, as well as an appeals process for the cardholder. These functions are carried out by the revocation official. The processes are to be secure and protect the privacy of PIV Cardholders.

The CMS maintains real-time status of PIV Cards not only throughout the issuing process, but through the card's entire lifecycle, and updates the Commonwealth Identity Management System (CIMS) to simplify both status checking by authorized officials and automated updates to the Commonwealth and Agency Access Control Systems. The revocation official is responsible for seeing that the CMS is updated when suspension, revocation, or destruction of a PIV credential occurs.

i. Suspension

Agencies may suspend credentials for various reasons. Most commonly such suspensions will be temporary. Agencies must develop reinstatement policies for suspended PIV Cards, and, depending upon business application, may elect to print a temporary card. In those cases which could lead to revocation and/or reduction of access privileges, the revocation official may confiscate the card for secure storage until such time as the matter is resolved.

Criteria for suspension of a PIV Card are to include:

- The card is temporarily misplaced.
- The cardholder is on temporary suspension.
- Extended absence or temporary reassignment in excess of 90 days.

ii. Revocation

Revocation is different than a suspension. A PIV credential is permanently rendered invalid as a result of revocation.

Criteria for revocation of a PIV Card might include:

- The card has been compromised (i.e., stolen or lost).
- An agency has terminated employment of an individual.

- The individual's status has changed (due to promotion, transfer, or change in first responder classification) and a new ID card needs to be issued.

The process for revoking a PIV Card is to include the following:

- Deactivation of the logical data elements on the card. FIPS 201 stipulates that deactivation is to occur within eighteen (18) hours of cardholder separation, notification of loss of card, revocation, or expiration.
- Update the CMS to indicate that the PIV Card has been revoked.
- Inform the SSP. The SSP will update the Certificate Authority, revoke the certificate corresponding to the PIV authentication key on the PIV Card, and update the Certificate Revocation Lists (CRLs) to include the appropriate certificate serial numbers. The SSP will also update Online Certificate Status Protocol (OCSP) responders so that queries with respect to certificates on the PIV Card are answered appropriately.
- If the card is available, destroy the PIV Card.

iii. Destruction

Whenever possible, revoked or expired PIV Cards are to be destroyed so as to preclude any chance of misuse.

- The revocation official is responsible for ensuring the card is destroyed.
- PIV Cards turned in for destruction are to be shredded within 90 days, as per Federal Register Doc E6-15848.

c. Re-issuance to Current PIV Cardholders

Re-issuance will occur when a PIV Card has been lost, stolen or destroyed, or when the cardholder is reinstated after a suspension or revocation of access privileges.

Re-issuance requires the issuing official to perform the following:

- Query the CMS to ensure that the PIV Card is not expired (past its expiration date).
- Ensure that if a valid Commonwealth background check is required for PIV Card issuance, one is on file before the card is reinstated.
- Verify the identity of the individual requesting re-issuance of the PIV Card by using the same process as when the card was issued.
- Issue a new card and update the CMS record for the individual.
- Digitally sign the biometrics and new card record.

Depending upon business application, agencies may elect to issue a temporary card.

7. Additional Considerations

This section identifies additional considerations in the PIV Card credentialing process.

a. Affected Systems

In addition to the process components described above, the following systems are affected by the PIV Card credentialing process:

- Commonwealth Identity Management System (CIMS) – as shown in the model in Section 2, CIMS describes the conceptual model of the entire Commonwealth Identity Management System, including the Commonwealth of Pennsylvania Enterprise Directory (CoPED), the agency master directories, the shared Identity Data Synchronization process (the metadirectory), and associated shared services for authentication and provisioning. Although CIMS is not a direct part of the PIV Card Credentialing Process, it has several touch points to the process as noted in the process steps above.
- Commonwealth of Pennsylvania Enterprise Directory (CoPED) – The IPAM initiative defines a Shared Identity Information Store, CoPED, to be provided to the agencies in the Commonwealth. CoPED is used by the Shared Authentication Service, among others, and includes information to allow PIV Cardholders to use their cards to authenticate and gain access to secured commonwealth resources. Interactions include:
  - CoPED serves as the authentication directory for officials (Enrollment Officials, Issuing Officials) when authenticating to perform their PIV Card Credentialing Process roles.
  - The CMS writes new users into the agency master directory, as described in Section 5.15. Once written to the master directory, the metadirectory synchronizes the user's account to CoPED.
- Access Control Systems (ACS) – An agency may have updates from the CMS also applied to its Physical ACS, so that when it has issued (or suspended or revoked) PIV Cards to its employees or contractors, access privileges are updated automatically. This interaction is not provided by the commonwealth as a shared service.

b. Privacy

Agencies may have a wide variety of uses for the PIV Card Credentialing Process and its components that were not intended or anticipated by HSPD-12 or FIPS-201. In considering whether a proposed use of this process or its components is appropriate, agencies are to consider the spirit and letter of all privacy controls specified in those documents, as well those specified in federal and commonwealth privacy laws and policies. Also consider the purpose of the PIV standard presented in HSPD-12, "to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy." Agencies are not to implement a use of the PIV credential, CMS, or other Card Credentialing Process component inconsistent with these control objectives.

To ensure the privacy of applicants, each agency is to assign an individual to the role of Senior Agency Privacy Official. To be effective, this individual is to have intimate knowledge of commonwealth and agency-specific privacy policies and best practices. The Senior Agency Privacy Official is responsible

for leading the implementation of PIV privacy policies, including those specified in FIPS-201, and ensuring that PIV Card privacy policies are applied and maintained in a consistent manner throughout the agency's PIV Card life cycle process.

The Senior Agency Privacy Official is also responsible for ensuring that agencies perform the following:

- Conduct a comprehensive Privacy Impact Assessment (PIA) on systems containing personal Information in Identifiable Form (IIF) for the purpose of implementing PIV, in consultation with appropriate agency personnel responsible for privacy issues (e.g., Chief Information Officer).
- Write, publish, and maintain a clear and comprehensive document listing the types of information that will be collected (e.g., transactional information, personal IIF), the purpose of collection, what information may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information at the Agency. PIV Card applicants are to be provided full disclosure of the intended uses of the PIV credential and the related privacy implications.
- Assure that systems containing IIF for the purpose of enabling the implementation of PIV are handled in full compliance with fair information practices as defined in the Federal Privacy Act of 1974.
- Maintain appeals procedures for those who are denied a credential or whose credentials are revoked.
- Ensure that only personnel with a legitimate need for access to IIF in the CMS are authorized to access the IIF.
- Coordinate with appropriate department or agency officials to define consequences for violating privacy policies of the PIV Card Credentialing Process and the CMS.
- Assure that the technologies used in the agency's implementation of the PIV Card Credentialing Process allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program.
- Utilize security controls described in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* to accomplish privacy goals where applicable.

Appendix A

Form I-9, OMB No. 1115-0136

Identity verification requires one document from List A, or one document from each of List B and List C.

List A **Documents that Establish Both Identity and Employment Eligibility**	List B **Documents that Establish Identity**	List C **Documents that Establish Employment Eligibility**
U.S. Passport (unexpired or expired)	Driver's license or ID card issued by a state or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address	U.S. social security card issued by the Social Security Administration (other than a card stating it is not valid for employment)
Certificate of U.S. Citizenship (INS Form N-560 or N-561)	ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address	Certification of Birth abroad issued by the Department of State (Form FS-545 or Form DS-1350)
Certificate of Naturalization (INS Form N-550 or N-570)	School ID card with a photograph	Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal.
Unexpired foreign passport, with I-551 stamp or attached INS Form I-94 indicating unexpired employment authorization	Voter's registration card	Native American tribal document
Permanent Resident Card or Alien Registration Receipt Card with photograph(INS Form I-151 or I-551)	U.S. Military card or draft record	U.S. Citizen ID Card (INS Form I-197)
Unexpired Temporary Resident (INS I-668)	Military dependent's ID card	ID Card for use of Resident Citizen in the United States (INS Form I-179)
Unexpired Employment Authorization Card (INS Form I-688A)	U.S. Coast Guard Merchant Mariner Card	Unexpired employment authorization document issued by the INS (other than those listed under list A)

List A	List B	List C
Documents that Establish Both Identity and Employment Eligibility	**Documents that Establish Identity**	**Documents that Establish Employment Eligibility**
Unexpired Reentry Permit (INS Form I-327)	Native American tribal document	
Unexpired Refugee Travel Document (INS 1-571)	Driver's license issued by a Canadian government authority	
Unexpired Employment Authorization Document issued by the INS which contains a photograph (INS Form I-688B)	(persons under 18 and provide any or the above items) School record or report card	
	(persons under 18 and provide any or the above items) Clinic, doctor or hospital record	
	(persons under 18 and provide any or the above items) Day-care or nursery school record	

8. Related ITPs/Other References

- ITP-SEC013 - *Identity Protection and Access Management (IPAM) Architectural Standard-Identity Management Services*
- APP-SEC013A - *IPAM Glossary*
- GEN-SEC013B - *Directory Services Architecture*
- GEN-SEC013C - *Access Management and Control*
- GEN-SEC013D - *Enrollment, Identity Proofing and Vetting*
- GEN-SEC013E - *Specification for a Commonwealth Personal Identity Verification Card*
- GEN-SEC013G - *Public Key Infrastructure (PKI)*
- NIST Special Publication 800-79-1*: Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations and the US Government Public Key Infrastructure Cross-Certification Criteria and Methodology*
- ITP-PRV002 - *Electronic Information Privacy Officer*
- STD-SEC014C - *Product Standards for Public Key Infrastructure/Shared Service Provider*

9. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

10. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	1/18/2008	Base Policy
Revision	6/22/2009	Updated and refreshed document
	4/2/2014	ITP Reformat