pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

# Information Technology Policy

## *Specification for a Commonwealth Personal Identity Verification (PIV) Card*

| **ITP Number** | **Effective Date** |
|---|---|
| GEN-SEC013E | January 25, 2008 |
| **Category** | **Supersedes** |
| Recommended Policy | |
| **Contact** | **Scheduled Review** |
| RA-ITCentral@pa.gov | Annual |

## 1. Introduction

The purpose of this document is to define the Commonwealth Personal Identity Verification (PIV) Card architectural policy that was established in ITP-SEC013 - *Identity Protection and Access Management (IPAM) Architectural Standard-Identity Management Services*.

This document defines the Office of Administration/Office for Information Technology (OA/OIT) policy for the characteristics of the PIV Card. This policy is compliant with Federal Information Processing Standard (FIPS) Publication 201-1 for PIV Cards, and also complies with International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7810 [ISO7810], ISO/IEC 10373 [ISO10373], ISO/IEC 7816 for contact cards [ISO7816], and ISO/IEC 14443 for contactless cards [ISO14443]. The card topology can be configured to adhere to the data standards of Section 202, paragraph (b) of H.R. 418 known as the Real ID Act of 2005.

### 1.1 Organization

This document provides the following information:

- Section 2 specifies the physical characteristics of the card. A detailed illustration is included at the end of the section.
- Section 3 defines the logical (computerized) card characteristics that are loaded into the card's smart chip.
- Section 4 describes cryptographic requirements.
- References and acronym definitions are provided in APP-SEC013A - *IPAM Glossary*.

## 2. Physical Characteristics

Having a common look for PIV Cards across all agencies allows the cards to be easily recognized as a commonwealth identity card. By adhering to federal PIV Card standards, these PIV Cards may also be leveraged to serve as an approved federal identification card, meeting the commonwealth goal of national interoperability. At the same time, the PIV Card's physical topology, appearance, and other characteristics are to be flexible enough to support individual department and agency requirements. The following subsections define the required physical characteristics and options available to agencies with respect to PIV Cards.

### 2.1 Durability and Tamper Proofing

All PIV Cards are to have an expiration date not to exceed five years. Issue and reissue policy is explained in GEN-SEC013F - *Identity Card Production, Personalization and Issuance*. To ensure durability and resistance to tampering, the PIV Cards are to comply with FIPS 201 card specifications. To guarantee compliance, all card stock is to be acquired from a commonwealth IPAM approved supplier. Personalization of the card stock is to be performed on commonwealth IPAM approved hardware. Agencies are directed to consult the appropriate ITP-SEC014 - *IPAM Architectural Standard – Identity Management Technology Standards* supplements for these solutions, and to consult the FIPS 201 approved products list (http://fips201ep.cio.gov/apl.php) and the General Services Administration schedule 70 for purchasing items not covered by ITPs.

### 2.2 Physical Requirements

The following list describes the required physical characteristics of the PIV Card:

- The PIV Card contains, at a minimum, a dual-interface Integrated Circuit Chip (ICC) which contains both a contact and a contactless interface.
- Commonwealth staff is to be issued tri-interface cards which include, in addition to the contact and contactless interfaces, an HID interface for interoperability with legacy Commonwealth access control systems.
- The PIV Card is to adhere to physical characteristics as described in International Standardization Organization (ISO)/International Electrotechnical Commission (IEC) 7810 [ISO7810], ISO/IEC 10373 [ISO10373], ISO/IEC 7816 for contact cards [ISO7816], and ISO/IEC 14443 for contactless cards [ISO14443]. The card material is to allow production of a flat card in accordance with [ISO7810] after lamination of both sides of the card.
- The PIV Card may not be embossed.
- Decals may not be adhered to the PIV Card.
- The card stock is to be white. Colored backgrounds on cards are not permitted.

The Commonwealth strongly recommends against punching holes in cards, based on federal experience and guidance. An alternative that allows the card to be worn without physically altering it is through the use of various commercially available card holders and carriers. Card carriers are strongly recommended in lieu of physically altering the card with an opening.

## 2.3 Visual Card Topography (Layout)

Figure 1 displays the front and back of a typical PIV Card.

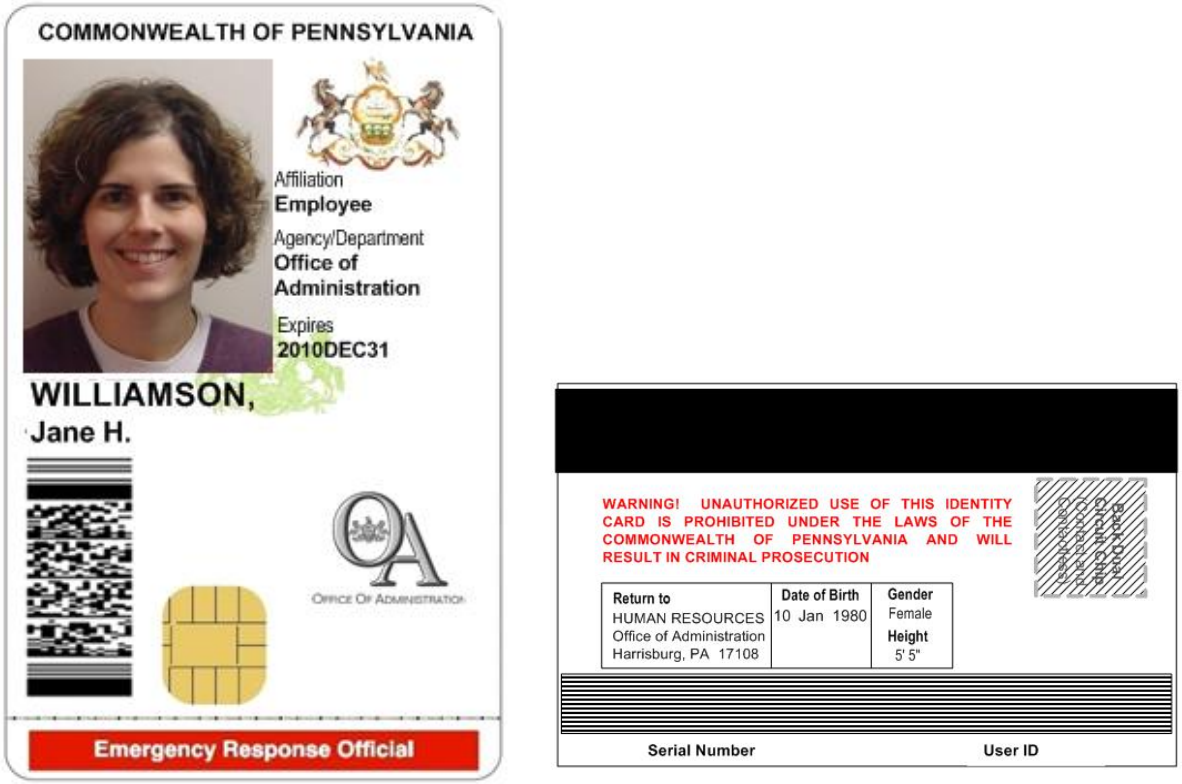


**Figure 1: Typical PIV Card**

FIPS 201 divides the topographical elements of the card into zones. The FIPS 201 zones relevant to the PIV Card are displayed in Figures 2 through 4. Figure 2 displays an Emergency Response Official's card.

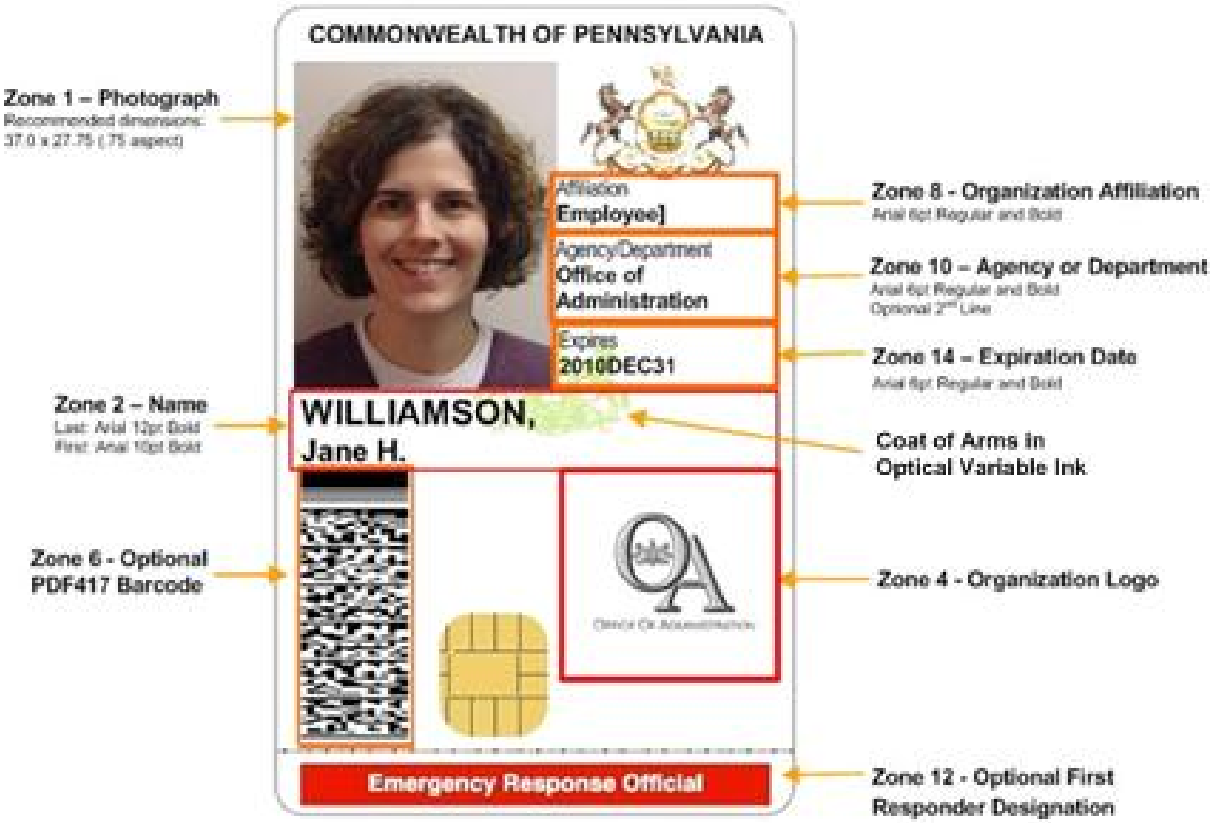


**Figure 2: Emergency Responder PIV Card with Zones**

Figure 3 includes a color-coded name field to denote a contractor affiliation, and also points out a micro-text line included for tamper resistance. This line repeats the words "Commonwealth of Pennsylvania" in text too small to easily reproduce.

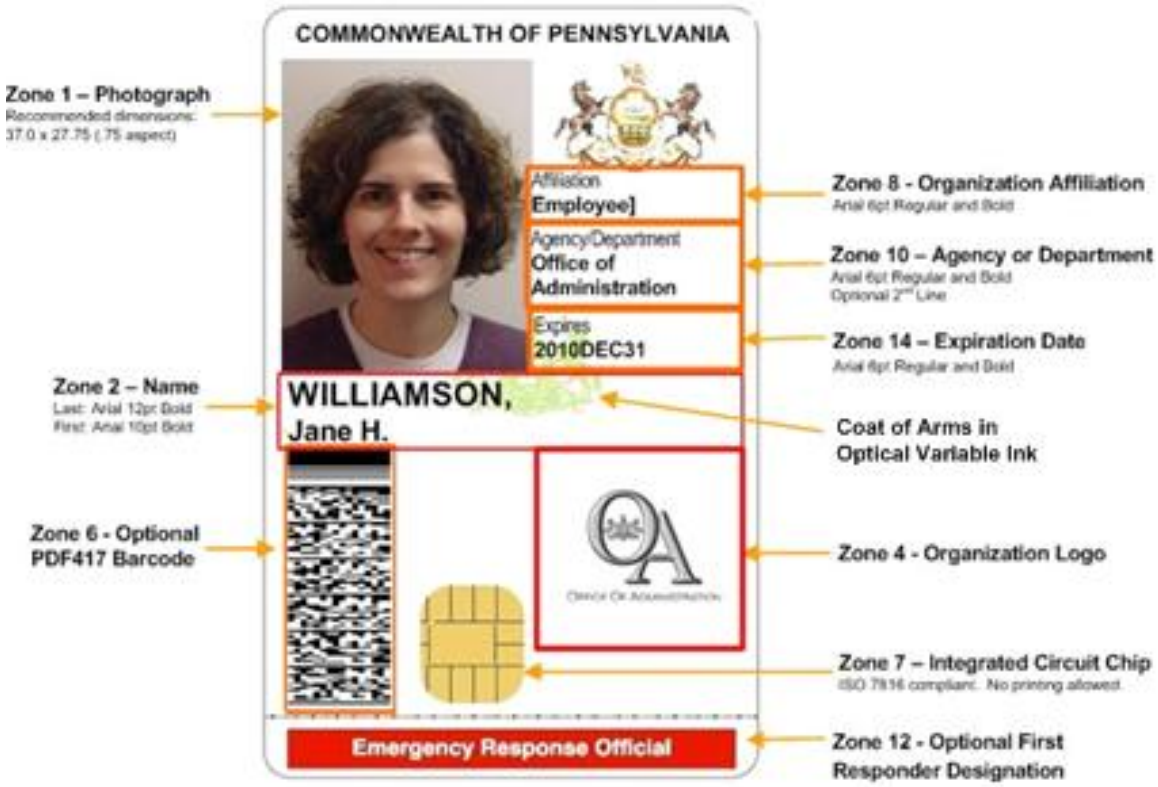


**Figure 3: Contractor PIV Card with Zones**

Figure 4 identifies the zones used on the back of the PIV Card.

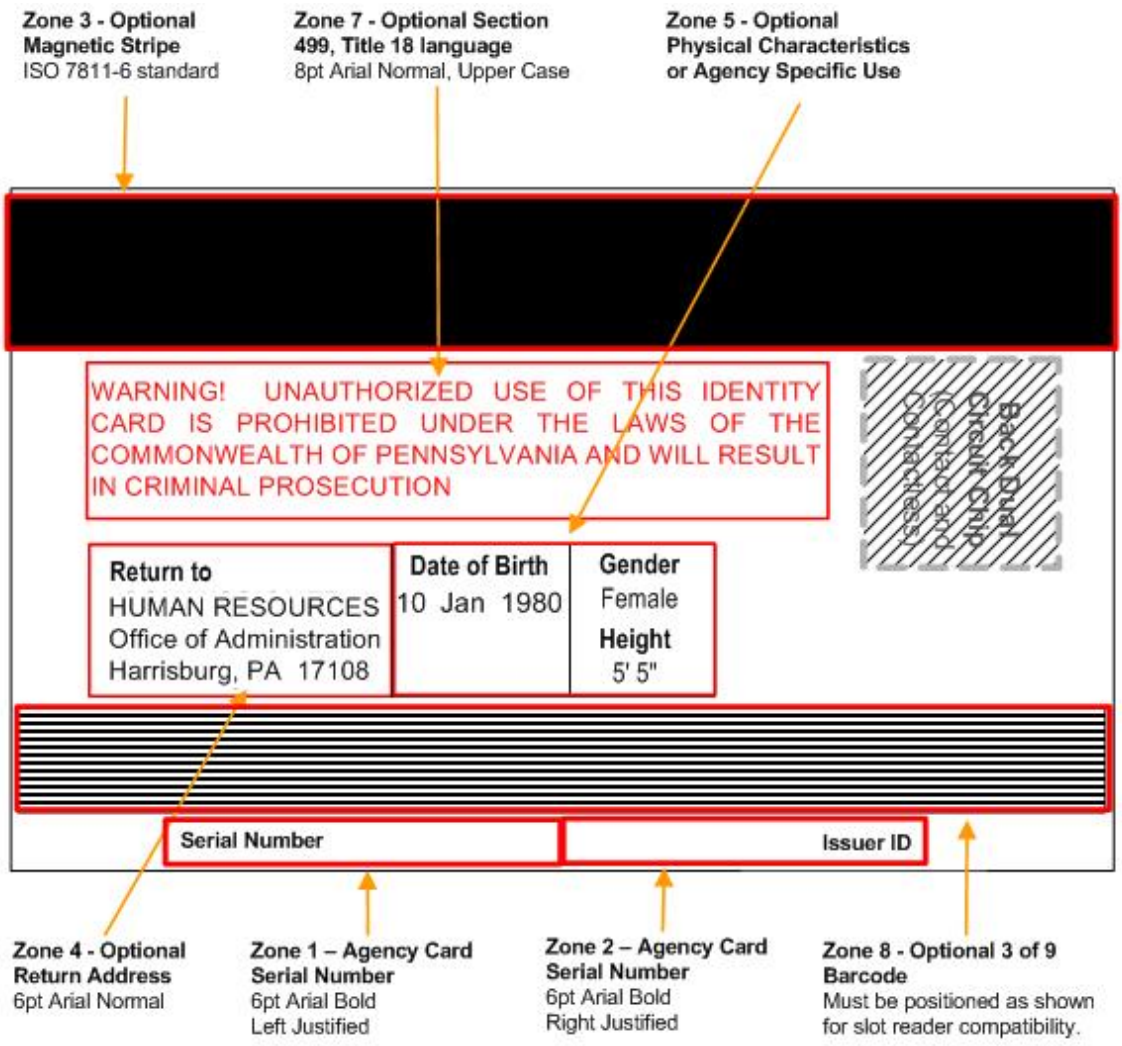


**Figure 4: Back of PIV Card with Zones**

Each of the zones depicted in these figures are defined in Tables 1 and 2 below, for the front and back of the PIV Card respectively. Gaps in the sequential order of the zones exist because only the FIPS 201 zones relevant to the PIV Card were used. Zones marked "Mandatory" are required elements of the PIV Card. "Optional" zones may be used at the discretion of the agency. Data loaded into the bar codes or magnetic stripe, if used, are also determined solely by the agency. ICC data elements are discussed in Section 3, *Logical Characteristics*.

| Table 1: Commonwealth PIV Card Topology Using FIPS 201 Zones – FRONT | | | | |
|---|---|---|---|---|
| **Zone** | **Data Element** | **Description** | **Format** | **Option** |
| 1 | Photograph | Full frontal pose from top of the head to shoulder. The gray background is preferred, but you may use other colors in the background. Consider the clarity and contrast of the photo against various colored backgrounds. | A minimum 300 DPI is to be used. The recommended dimensions are 37.0 mm x 27.75 mm, which is a .75 mm aspect ratio (width divided by height). The background is to be uniform and no darker than 18 percent gray. | Mandated |
| 2 | Name | Last Name, First Name, Middle Initial | Last Name Arial 12 pt bold. All capital letters. First Name and Middle Initial, Arial 10 pt bold. The dimensions of this zone are 8.5 mm x 49.0 mm. | Mandated |
| | Background Color Coding for Zone 2 (*Name*) | FIPS mandates that the following colors be used:<br>• White—employees<br>• Blue—foreign nationals<br>• Green—contractors | The dimensions of this zone are 8.5 mm x 49.0 mm. | Mandated |
| 4 | Organization Logo | This area is used to display the agency or department logo for immediate recognition. | At the department or agency's discretion. | Optional |
| 6 | Portable Data File (PDF) Barcode Two-Dimensional Bar Code | Whether to use the 2-D barcode and what data is loaded onto it remains solely at the discretion of the agency. | PDF417 barcode is to be on left side of card. | Optional |
| 7 | Integrated Circuit Chip No printing allowed | Location of the dual interface integrated circuit chip is fixed. Consult with the IPAM Architecture Team for available memory capacity. | ISO 7816 Compliant | Mandated |
| 8 | Organization Affiliation | Individual affiliation | Arial 6 pt bold for individual affiliation. | Mandated |
| 10 | Agency or Department | Sponsoring organization | Arial 6 pt bold | Mandated |
| 12 | Footer – First Responder Designation | This zone is reserved to designate first responders and other emergency response individuals. | Arial 7 pt white bold with red background for first responders. | Optional |
| 14 | Expiration Date | Expiration date will be no more than five years from issue. For cards using Public Key Infrastructure (PKI), the certificate expiration date of the PKI certificate is to be no later than the expiration date of the PIV Card (see GEN-SEC013G, *PKI*, for details). | Arial 6 pt bold – The card expiration date is to be printed in YYYYMMDD format. | Mandated |

| Table 1: Commonwealth PIV Card Topology Using FIPS 201 Zones – FRONT | | | | |
|---|---|---|---|---|
| **Zone** | **Data Element** | **Description** | **Format** | **Option** |
| 18 | Affiliation Color Code | The affiliation color code "B" for Blue or "G" for Green is to be printed in a white circle in Zone 2 for Foreign Nationals and Contractors, respectively. | The diameter of the circle is not to be more than 5mm. See SP 800-104. | Mandated |

**Table 1: Commonwealth PIV Card Topology using FIPS 201 Zones -- FRONT**

| Table 2: Commonwealth PIV Card Topology Using FIPS 201 Zones – BACK | | | | |
|---|---|---|---|---|
| **Zone** | **Data Element** | **Description** | **Format** | **Option** |
| 1 | Agency Card Serial Number | Contains the unique serial number from the issuing agency or department. | Arial 6 pt bold Left justified | Mandated |
| 2 | Issuer Identification | Consists of six characters for department code, four characters for agency code, and a five-digit number that uniquely identifies the issuing facility within the department or agency. | 6 pt Arial bold right justified | Mandated |
| 3 | Magnetic Stripe | Stripe is to be of high coercivity and placed in accordance with [ISO7811]. | ISO 7811-6 | Optional |
| 4 | "Return to" or Agency Specific Text | If used, "return if lost" language is to be placed in Zone 4. If "return if lost" is not required, then this zone can be used for agency specific text. | 6 pt Arial normal | Optional |
| 5 | Physical Characteristics or Agency Specific Text | If used the physical characteristics (e.g., height, eye color, hair color) are to be placed in Zone 5. Use English units instead of metric units. If physical characteristics are not required then this zone can be used for agency specific text. | Arial 6 pt bold (optional) | Optional |
| 7 | Title 18 Language or Agency Specific Text | If used, Standard Section 499, Title 18, language warning against counterfeiting, altering, or misusing the card is to be printed. Agency-specific text can be used if Title 18 language is not required. Zone 7 cannot be used in conjunction with Zone 9. | 8 pt Arial normal | Optional |
| 8 | Linear 3 of 9 Bar Code | The beginning and end points of the bar code are not to interfere with the contactless ICC component. | As per Automatic Identification and Mobility (AIM) Standards | Optional |

**Table 2: Commonwealth PIV Card Topology using FIPS 201 Zones -- BACK**

## 3. Logical Characteristics

Logical requirements refer to the computerized information stored on the PIV Card. Specific data elements have been mandated in FIPS 201 for the purpose of verifying the cardholder's identity at graduated assurance levels (see GEN-SEC013D - *Enrollment, Identity Proofing and Vetting* for an explanation of assurance levels). These data elements include:

- **Card Holder Unique Identifier (CHUID)**
  CHUID proves the identity of the cardholder to an external entity (CTE authentication), such as a network computer system. The format of the CHUID is specified in "Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems v2.2" published by the Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group on July 27, 2004, commonly referred to as PACS v2.2, and is composed of pre-defined, fixed length data elements. Detailed information about the CHUID can be found in Section 4.2 of FIPS 201 (and subsequent change documents) and SP 800-73.

  The CHUID is a free read data element from both the contact and contactless interfaces (i.e., the PIV Card doesn't have to be activated for an electronic reader to read the CHUID). The CHUID contains the following:

  a. **Federal Agency Smart Credential Number (FASC-N).**
  The FASC-N uniquely identifies each federal PIV Card.
  Non-federal Issuers (NFIs) of PIV Cards are to generate and use a FASC-N in all locations required by NIST SP 800-73 and NIST SP 800-76, just as federal issuers are to; but for NFIs the composition of the FASC-N differs. The *Personal Identity Verification (PIV) Interoperability For Non-Federal Issuers* publication, released May 2009 by the federal CIO Council was published to provide guidance for non-federal issuers -- such as the Commonwealth of PA -- to issue their own PIV Interoperable (PIV-I) Cards. This publication describes these three components of the FASC-N:
     1. Local Card ID number and Person identifier – As per SP 800-73, this is a locally established element – meaning the numbers are to be unique to cards issued within the commonwealth. To eliminate any opportunity for duplication, the algorithm to generate this element is to be implemented into the enterprise CMS.
     2. Federal agency code – Because NFIs are not federal agencies, they do not have federal agency codes. All NFIs are therefore to use 9999 in place of the federal agency code.
     3. Organizational identifier – To differentiate the NFIs, this additional tag length identifier (TLI) is required. The TLI is to correspond with the Dun & Bradstreet Data Universal Numbering System (DUNS) code, as this is a long standing and universally accepted business identifier. The DUNS number of the Commonwealth Executive Offices (005534883) will be utilized for issuance of commonwealth-sponsored personal identity verification cards.

  b. **Expiration date.** In machine readable format, the expiration date data element is to specify when the card expires, and facilitate status checking in the asymmetric signature field. The expiration date format and encoding rules are specified in SP800-73. This field is to be eight bytes in length and is to be encoded as YYYYMMDD.

  c. The **asymmetric signature field** (digital signature). The asymmetric signature data element of the PIV Card's CHUID is to be encoded as a Cryptographic Message Syntax (CMS) external digital signature, as defined in RFC 3852. The digital signature is to be

computed over the entire contents of the CHUID, excluding the asymmetric signature field. Algorithm and key size requirements for the asymmetric signature are detailed in SP800-78.

The issuer asymmetric signature is implemented as a *SignedData* Type, as specified in RFC 3852, and is to include the following information:

- The message is to include a *version* field specifying version v3
- The *digestAlgorithms* field is to be as specified in SP800-78
- The *encapContentInfo* is to:
  - Specify an *eContentType* of *id-PIV-CHUIDSecurityObject*
  - Omit the *eContent* field
- The certificates field is to include only a single X.509 certificate which can be used to verify the signature in the *SignerInfo* field
- The *crls* field is to be omitted
- *SignerInfos* is to be present and include only a single *SignerInfo*
- The *SignerInfo* is to:
  - Use the *issuerAndSerialNumber* choice for *SignerIdentifier*
  - Specify a *digestAlgorithm* in accordance with SP800-78
  - Include, at a minimum, the following signed attributes:
    - A *MessageDigest* attribute containing the hash computed over the concatenated contents of the CHUID, excluding the asymmetric signature field
    - A *pivSigner-DN* attribute containing the subject name that appears in the PKI certificate for the entity that signed the CHUID
  - Include the digital signature.

- **Cryptographic Keys:** The PIV Authentication Key, Card Authentication Key, Digital Signature Key, Key Management Key, and Card Management Key are discussed thoroughly in Section 4.
- **Minutia of Two biometric fingerprints:** Used by the card to prove the identity of the cardholder, and is especially useful when agencies choose to implement on-card matching of biometric information. Actual images of the fingerprints are not stored, but only the minutia as established according to the International Committee for Information Technology Standard 358 for minutia and as conforms to Section 3 of NIST Special Publication 800-76 Biometric Data Specifications for Personal Identity Verification. The two fingerprints are to be accessible only over the contact interface and after presentation of a valid Personal Identification Number (PIN).
- **Digital image of cardholder's face**. This image is used to prove the identity of the cardholder. The intent is to allow the cardholder's image to appear on a screen for visual inspection, not to interface with facial recognition software. Facial images will conform to the full frontal type defined in Section 5 of NIST Special Publication 800-76 Biometric Data Specifications for Personal Identity Verification and, like the fingerprints, accessible only over the contact interface and after presentation of a valid PIN.
- **Personal Identification Number (PIN):** Used to prove or authenticate that the bearer of the card is the actual owner to an external entity (CTE authentication) that's connected to a card-reader.

## 4. Cryptographic Requirements

Cryptography can be used to provide data integrity and confidentiality protection for data communications and storage by scrambling the information so that it is unintelligible until deciphered. Modern cryptographic techniques use sophisticated algorithms to scramble the data, and require a secret "key" to decipher the message.

Symmetric-key cryptosystems typically use the same key for encryption and decryption. Keeping track of each key for every message eventually results in a significant key management challenge, but even more challenging can be finding how to securely pass that key to the message recipient. Public-key cryptosystems, utilizing a PKI, resolve that issue by creating public keys that can be distributed freely, but require the paired private key to remain secret.

The commonwealth has adopted the PKI cryptosystem, which is documented in GEN-SEC013G - *Public Key Infrastructure*. To be used for cryptographic purposes, the PIV Card is to, at a minimum, store one asymmetric private key and a corresponding public key certificate. Cryptographic operations are performed using the asymmetric private key. Cryptographic operations with this key are performed only through the contact interface. Accessibility through the contactless interface could make it possible for covert electronic capture of the information, and impose a real security risk.

To comply with the commonwealth PKI, which adheres to FIPS 201, the PIV Card is to implement the following cryptographic operations and support functions:

- RSA or elliptic curve key pair generation
- RSA or elliptic curve private key cryptographic operations
- Importation and storage of X.509 certificates. (The X.509 certificate incorporates a digital signature to bind a public key with an identity, and stores these with a Certificate Authority [CA] for public reference and validation.)

Additional asymmetric keys and PKI certificates (key containers) may be included as required for business purposes. Consult FIPS 201 and SP800-78 for specifics.

The PIV Card has a single federally mandated key (the Card Management Key) and four classes of optional keys. These key classes are described below, along with storage and access requirements, and key management requirements where applicable.

- **Card Management Key.** This mandatory symmetric key is used for personalization and post-issuance activities. This key will enable the Commonwealth to securely make changes to data on the PIV Card's ICC.
    - The card management key is imported onto the card by the issuer. The card management key is to only be accessible using the contact interface of the card.
    - The PIV Card may also import and store X.509 certificates for use in PKI path validation. These trust anchor certificates may be accessed through the contact interface using an activated PIV Card without explicit cardholder action. If supported, initialization and update of trust anchor certificates are to require explicit cardholder action (entering a PIN), in addition to activation of the card.

- **PIV Authentication Key**. This optional asymmetric private key supports card authentication for an interoperable environment, and it is federally mandated for all federally interoperable PIV Cards. The PIV authentication key supports the interoperable physical and logical access using the contact interface.

  - This PIV authentication key is to be generated on the PIV Card itself. The PIV Card is not to permit exportation of the PIV authentication key. As an added security measure, the PIV authentication key is to be available only through the contact interface of the identification card. Private key operations may be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation).
  - The PIV Card is to store a corresponding X.509 certificate to support validation of the public key. The X.509 certificate is to include the FASC-N in the subject alternative name extension using the PIV FASC-N attribute to support physical access procedures. The expiration date of the certificate is to be no later than the expiration date of the PIV Card.

- **Card Authentication Key.** This optional key may be either a symmetric (secret) key or an asymmetric private key for physical access. It supports contactless physical access for many currently employed physical access systems.
  - The PIV Card is not to permit exportation of the card authentication key. Private/secret key operations may be performed using this key without explicit user action (e.g., the PIN need not be supplied). This standard does not specify key management protocols or infrastructure requirements.

- **Digital Signature Key**. The digital signature key is an optional asymmetric private key supports document signing.
  - The PIV Card digital signature key is to be generated on the PIV Card. The PIV Card is not to permit exportation of the digital signature key. If present, cryptographic operations using the digital signature key may only be performed using the contact interface of the PIV Card. Private key operations may not be performed without explicit user action.
  - The PIV Card is to store a corresponding X.509 certificate to support validation of the digital signature key.

- **Key Management Key**. The key management key is an optional asymmetric private key supports key establishment and transport. It can also be used as an encryption key and is useful for encrypting e-mail or other sensitive documents.
  - This key may be generated on the PIV Card or imported to the PIV Card. If present, the key management key is to only be accessible using the contact interface of the PIV Card. Private key operations may be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation). The key management key is sometimes called an encryption key or an encipherment key.
  - The PIV Card imports and stores a corresponding X.509 certificate to support validation of the key management key. FIPS 201 specifies the certificate format and the key management infrastructure for PIV key management keys.

All PIV Card cryptographic keys are to be generated within an FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above (see GEN-SEC013C -*Access Management and Control* for an explanation of the levels). In addition to an overall validation of Level 2, the PIV Card is to provide Level 3 physical security to protect the PIV private keys in storage.

## 5. Related ITPs/Other References

- ITP-SEC013- *Identity Protection and Access Management (IPAM) Architectural Standard – Identity Management Services*
- GEN-SEC013C - *Access Management and Control*
- GEN-SEC013D - *Enrollment, Identity Proofing and Vetting*
- GEN-SEC013F - *Identity Card Production, Personalization and Issuance*
- GEN-SEC013G - *Public Key Infrastructure (PKI)*
- ITP-SEC014 - *IPAM Architectural Standard – Identity Management Technology Standards*

## 6. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

## 7. 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 | 9/22/2006 | Base Policy |
| Revision | 10/23/2009 | (Replaces SEC014B) - Updated Figures 2 and 3; refreshed document |
| | 4/2/2014 | ITP Reformat |