pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Authentication via the PIV Card

ITP Number	***Effective Date***
BPD-SEC013J	January 18, 2008
Category	***Supersedes***
Recommended Policy	
Contact	***Scheduled Review***
RA-ITCentral@pa.gov	Annual

1. Introduction

In the context of Personal Identity Verification (PIV) Cards, identity authentication is defined as the process of establishing confidence, or assurance, in the identity of the cardholder. The authenticated identity can then be used to determine the permissions/authorizations granted for that identity to access various physical (door, gate, checkpoint, building) and logical (computer system, network, data file) resources.

The entity performing the authentication establishes confidence in the identity of the PIV cardholder through the following:

- The rigor of the identity proofing process conducted prior to issuance of the PIV Card. The four assurance levels defined in GEN-SEC013D - *Enrollment, Identity Proofing and Vetting* are used to quantify the extent to which the identity credential may be trusted to actually represent the individual named in the credential.
- The security of the PIV Card issuance and maintenance processes. A strictly controlled process is defined in GEN-SEC013F - *Identity Card Production, Personalization and Issuance.*
- The strength of the technical authentication mechanisms used to verify that the cardholder is the owner of the PIV Card. Best practices for PIV Card authentication are described below.

Technically, a PIV Card bears a number of visual and logical credentials (i.e., photo, fingerprint, digital signature, physical description). Depending upon the specific PIV credentials used, varying levels of assurance can be achieved that the holder of the PIV Card is the true owner of the card. The commonwealth's certified and accredited identity-proofing and issuance process for PIV credentials (defined in GEN-SEC013F) establishes a common level of assurance in the proofing and issuance processes, and in conjunction with the Assurance Level identity proofing standards defined in GEN-SEC013D, allows agencies across the enterprise to share identical levels of confidence in the credentials on the PIV card.

Individual agencies are responsible for determining their own physical and logical access control permissions, assigning assurance levels to their physical and logical assets, and implementing the authentication mechanisms (i.e., PIV card readers, biometric readers, asset access points).

PIV Cards can be used for identity authentication in environments equipped with card readers as well as those that lack card readers (via visual inspection). Card readers, when present, can be contact readers, barcode scanners or contactless readers. The parameters of the usage environment are vital factors when determining which PIV identity authentication mechanisms may be applied, or required, for a particular situation.

1.1 Organization

The PIV Card can be used as the sole authentication token, or in combination with other authentication mechanisms, to improve the overall Strength of Authentication. The following sections describe how basic types of authentication mechanisms, supported by the core (minimum required) PIV credential elements, are used.

- Section 2 describes authentication using visual inspection of the PIV card.
- Section 3 describes authentication using the PIV card holder unique identifier (CHUID) number
- Section 4 describes authentication using the PIV biometric
- Section 5 describes authentication using PIV asymmetric cryptography (Private Key Infrastructure)

2. Authentication Using Visual Inspection of the PIV Card

Visual authentication of a PIV cardholder is used only to support access control to physical facilities and resources.

The PIV Card has several mandatory topographical features on the front and back that support visual identification and authentication:

- Cardholder's Photograph
- Cardholder's Name
- Employee affiliation employment identifier
- Expiration date
- Agency card serial number (back of card)
- Issuer identification (back of card)

The PIV Card may also bear the following optional components, depending on classification of cardholder and specific agency requirements:

- Agency name and/or department
- Department or agency seal
- Cardholder's physical characteristics
- Cardholder's Signature

A complete list of required and optional features is supplied in GEN-SEC013E -*Specification for a Commonwealth Personal Identity Verification Card.*

When a cardholder attempts to pass through an access control point for a controlled facility, a human guard performs visual inspection of the PIV card and cardholder, and compares the card specified attributes to the features of the cardholder. The guard then determines whether the identified individual is to be allowed through the control point. A series of steps are applied in the visual authentication process:

1. The human guard at the access control entry point determines whether the PIV Card appears to be genuine and has not been altered or tampered with in any way.
2. The guard compares the cardholder's facial features with the picture on the card to ensure they match.
3. The guard checks the expiration date on the card to ensure that the card has not expired.
4. The guard compares the cardholder's physical characteristics and descriptions to those of the cardholder. (Optional)
5. The guard collects the cardholder's signature and compares it with the signature on the card. (Optional)
6. One or more data elements on the card (e.g., name, employee affiliation employment identifier, agency card serial number, issuer identification, agency name) are used to determine whether the cardholder is to be granted access, or the confirmed identity is cross-referenced with a predefined access list.

3. Authentication Using the PIV CHUID Number

The PIV Card provides a mandatory logical credential on its Integrated Circuit Chip (ICC) called the CHUID (Card Holder Unique ID) which contains the following data elements:

- Federal Agency Smart Credential Number (FASC-N).
- Expiration date.
- Asymmetric signature field (Digital Signature).

GEN-SEC013E provides detailed specifications for the CHUID. The following sequence is used for CHUID based PIV cardholder authentication:

- The CHUID is read electronically from the PIV Card.
- The digital signature (see GEN-SEC013E for details) on the CHUID is checked to ensure a trusted source signed the CHUID and it is unaltered. (Optional, depending on the required assurance level)
- The expiration date is checked to ensure the card has not expired.
- One or more CHUID data elements are used as input to the authorization check to determine whether the cardholder is to be granted access.

Some reasons for choosing a CHUID-based authentication mechanism include:

- Potential for rapid authentication with high volume access control.
- Low resistance to use of unaltered card by non-owner of card.
- Applicability with contact-based and contactless readers.

4. Authentication Using PIV Biometric

The PIV Card hosts a mandatory signed biometric that can be read from the card following cardholder-to-card (CTC) authentication using a personal identification number (PIN) supplied by the cardholder. The PIV biometric is designed to support a cardholder-to-external system (CTE) authentication mechanism through a match-off-card scheme.

Some reasons for choosing a PIV Biometric authentication mechanism include:

- A slower mechanism because it requires two interactions with the cardholder.
- A strong resistance to use of unaltered card by non-owner because of biometric. The PIN is also required to activate the card for reading the biometric.

- A digital signature on the biometric, which can be checked to further strengthen the mechanism.
- Applicability only with contact-based card readers.

The following subsections define two authentication schemes which make use of the PIV biometric.

4.1 Unattended Authentication Using PIV Biometric

Unattended authentication indicates that the cardholder is alone with the card reader when he authenticates. The following sequence is followed for unattended authentication of the PIV biometric:

1. The CHUID is read from the card.
2. The expiration date in the CHUID is checked to ensure the card has not expired.
3. The cardholder is prompted to submit a PIN, activating the PIV Card.
4. The PIV biometric is read from the card.
5. The signature on the biometric is verified to ensure the biometric is intact and is from a trusted source. (optional)
6. The cardholder is prompted to submit a live biometric sample.
7. If the biometric sample matches the biometric read from the card, the cardholder is authenticated as the owner of the card.
8. The FASC-N in the CHUID is compared with the FASC-N in the signed attributes field of the external digital signature on the biometric.
9. One or more of the CHUID data elements are used as input to the authorization check to determine whether the cardholder is to be granted access.

4.2 Attended Authentication Using PIV Biometric

Attended authentication indicates that a security official is present at the access point to prompt the cardholder and ensure all appropriate identification checks are properly completed. The following sequence is followed for attended authentication of the PIV biometric:

1. The CHUID is read from the card.
2. The expiration date in the CHUID is checked to ensure the card has not expired.
3. The cardholder is prompted to submit a PIN. The PIN entry is done in view of an attendant.
4. The submitted PIN is used to activate the card. The PIV biometric is read from the card.
5. The signature on the biometric is verified to ensure the biometric is intact and from a trusted source. (Optional)
6. The cardholder is prompted to submit a live biometric sample. The biometric sample is submitted in view of an attendant.
7. If the biometric sample matches the biometric read from the card, the cardholder is authenticated as the owner of the card.
8. The FASC-N in the CHUID is compared with the FASCN in the Signed Attributes field of the external digital signature on the biometric.
9. One or more CHUID data elements are used as input for the authorization check to determine whether the cardholder is to be granted access.

This authentication mechanism is similar to the unattended biometric credential check. The only difference is that an attendant (e.g., security guard) supervises PIV Card and PIN submission and the cardholder's biometric.

5. Authentication Using PIV Asymmetric Cryptography

The PIV Card carries a mandatory asymmetric authentication private key and corresponding certificate.

The following steps are used to perform authentication using the PIV asymmetric authentication key:

1. The cardholder is prompted to submit a PIN.
2. The submitted PIN is used to activate the card.
3. The reader issues a challenge string to the card and requests an asymmetric operation in response.
4. The card responds to the previously issued challenge by signing the challenge string using the PIV authentication private key and attaching the associated certificate.
5. The response signature is verified and standards-compliant PKI path validation is conducted. The related digital certificate is checked to ensure that it is from a trusted source. The revocation status of the certificate is checked to ensure current validity.
6. The response is validated as the expected response to the issued challenge.
7. The Subject Distinguished Name and FASCN from the authentication certificate are extracted and passed as input to the authorization function.

Some reasons for choosing a private key infrastructure-based authentication mechanism include:

- Requirement to use online certificate status checking infrastructure;
- Resistance to credential forgery;
- Resistance to use of unaltered card by non-owner since PIN is required to activate card;
- Applicability with contact-based card readers

6. Related ITPs/Other References

- GEN-SEC013D - *Enrollment, Identity Proofing and Vetting*
- GEN-SEC013E - *Specification for a Commonwealth Personal Identity Verification Card*
- GEN-SEC013F - *Identity Card Production, Personalization and Issuance*

7. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

8. 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	9/25/2009	Refreshed Document
	4/2/2014	ITP Reformat