FIPS 201
PIV-II Requirements

Ketan Mehta

June 27, 2005

Agenda

□Identity Proofing

□Card Issuance and maintenance

□Logical Credentials

□Authentication Mechanism

□Card Topology

FIPS 201 REQUIREMENTS

PIV Identity Proofing and Registration Requirements

- ❑ All PIV I control objectives must be met.
- ❑ In addition, following biometrics information must be captured during the identity proofing and registration process.
  - o A full set of fingerprints for law enforcement checks
  - o An electronic facial image used for printing on the card
  - o Two electronic fingerprint for storage on the card

Agenda

- ❑Identity Proofing
- ❑Card Issuance and maintenance
- ❑Logical Credentials
- ❑Authentication Mechanism
- ❑Card Topology

FIPS 201 REQUIREMENTS

Card Issuance and Maintenance Requirements

Card Issuance

- ❑ All PIV I requirements must be met.
- ❑ Issue a card while a NACI is pending.
- ❑ Revoke the credential if NACI is not completed and favorably adjudicated in six months.
- ❑ Issuer shall perform 1:1 biometric match of the applicant against the biometric included in the PIV Card.

FIPS 201 REQUIREMENTS

Card Issuance and Maintenance Requirements

Card Renewal – replace the card when it expires

- ❑ Card shall be valid no more than 5 years
- ❑ No need to repeat the full registration procedure
- ❑ NACI checks must be followed in accordance with OPM guidance
- ❑ Expired card must be collected and destroyed
- ❑ Same biometric data may be reused with the new PIV Card but digital signature must be recomputed with new FASC-N
- ❑ Expiration date of the PIV authentication certificate and optional digital signature certificate cannot be later than the expiration date of the PIV Card

FIPS 201 REQUIREMENTS

Card Issuance and Maintenance Requirements

Card Reissuance – issue a new card if the old card has been compromised.

- ❑ The entire registration and issuance process, including fingerprint and facial image capture, shall be conducted
- ❑ Old PIV card is revoked
- ❑ Certificate corresponding to PIV authentication key must be revoked
- ❑ OCSP responders shall be updated

FIPS 201 REQUIREMENTS

Card Issuance and Maintenance Requirements

PIN Reset – unlock the card

- ❑ Agencies determine the number of invalid PIN tries
- ❑ Cardholder’s biometric match the stored biometric on the card

FIPS 201 REQUIREMENTS

Card Issuance and Maintenance Requirements

Card Termination – permanently destroy and invalidate the use of the card

- Card is collected and destroyed
- Card is revoked
- Certificate corresponding to PIV authentication key must be revoked
- OCSP responders shall be updated
- Cardholder data is disposed of in accordance with the stated privacy and data retention policies of the department or agency.

Agenda

- ❑Identity Proofing
- ❑Card Issuance and maintenance
- ❑Logical Credentials
- ❑Authentication Mechanism
- ❑Card Topology

Logical Credentials

Mandatory:

1. **Personal Identification Number (PIN)**
   - Something the cardholder knows
   - Used to prove the identity of the cardholder to the card
   - PIN should not be easily guessable or otherwise individually identifiable
   - Meet identity-based authentication requirements of FIPS 140-2 Level 2

Logical Credentials

Mandatory:

2. **Cardholder Unique Identifier (CHUID)**

   - ❑ Something the cardholder possess
   - ❑ Used to prove the identity of the cardholder to the external entity such as a host computer system
   - ❑ Includes Federal Agency Smart Credential Number (FASC-N) which uniquely identifies each card
   - ❑ Accessible from both contact and contactless interfaces – free read
   - ❑ Includes expiration date and an Asymmetric Signature field
   - ❑ Includes the X.509 certificate which can be used to verify the signature

Logical Credentials

Mandatory:

3. **PIV Authentication Key**

- ❑ Something the cardholder possess
- ❑ Used to authenticate the card and prove the identity of the cardholder to the external entity
- ❑ Key shall be generated on the card and the private key exportation is not permitted
- ❑ PIN must be supplied before the first use
- ❑ Cryptographic operations performed only through contact interface
- ❑ All cryptographic operations using this key are performed on-card

Logical Credentials

Mandatory:

4. **Two biometric fingerprints**
   - ❑ Something that uniquely identifies the cardholder
   - ❑ Used to prove the identity of the cardholder to the external entity
   - ❑ Biometrics only available through contact interface after a PIN is successfully verified.

Logical Credentials

Optional:

- □ **PIV Card Authentication Key**
  - □ Used to authenticate the card
  - □ May employ symmetric or asymmetric key algorithms
  - □ Allow contactless access
  - □ Cryptographic operations may be performed without explicit user action (e.g., the PIN need not be supplied)
- □ **Digital Signature Key**
  - □ Used to generate digital signatures
  - □ Key shall be generated on the card and the private key exportation is not permitted
  - □ Cryptographic operations must only be performed using the contact interface
  - □ Private key operations may not be performed without explicit user action

Logical Credentials

Optional:

- ❑ **Key Management Key**
  - ❑Key may be generated on the card or imported to the card
  - ❑Must only be accessible through contact interface
  - ❑Cryptographic operations may be performed without explicit user action (e.g., the PIN need not be supplied)
  - ❑Key is sometimes called an encryption key or encipherment key
- ❑ **Card Management Key**
  - ❑Imported onto the card by the issuer
  - ❑Is a symmetric key used for personalization or post-issuance activities
  - ❑Must only be accessible through contact interface

FIPS 201 REQUIREMENTS

Logical Credentials

Key Management

- ❑ CA shall participate in the hierarchical PKI for the Common Policy managed by the Federal PKI.
- ❑ Certificates shall be issued under the id-CommonHW and id-CommonAuth policy

X.509 Certificate Requirements

- ❑ CA shall maintain a LDAP directory server that holds the CRLs for the certificates it issues
- ❑ CA shall operate an OCSP server
- ❑ Authority Information Access (AIA) extensions shall include pointers to the appropriate OCSP status responders in addition to LDAP URIs.
- ❑ Certificate associated with PIV Authentication key shall not assert the nonRepudiation bit in the keyUsage extension and must include the PIV Card’s FASC-N in the subject alternative name field.
- ❑ CAs that issue certificate corresponding to the PIV private keys shall issue CRLs every 18 hours
- ❑ PIV Authentication certificate contains FASC-N in the subject alternative name extension; hence, these certificates shall not be distributed publicly via LDAP or HTTP.

Agenda

- ❑Identity Proofing
- ❑Card Issuance and maintenance
- ❑Logical Credentials
- ❑Authentication Mechanism
- ❑Card Topology

FIPS 201 REQUIREMENTS

Authentication Mechanisms

- ❑ Three Identity Authentication Assurance levels
- ❑ Authentication using PIV Visual Credentials
- ❑ Authentication using the PIV CHUID
- ❑ Authentication using PIV Biometric
- ❑ Authentication using PIV Asymmetric Cryptography (PKI)

FIPS 201 REQUIREMENTS

Graduated Assurance Levels for Identity Authentication

Authentication for Physical and Logical Access

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism **Physical Access**	Applicable PIV Authentication Mechanism **Logical Access** Local Workstation Environment	Applicable PIV Authentication Mechanism **Logical Access** Remote/Network System Environment
SOME confidence	VIS, CHUID	CHUID	PKI
HIGH confidence	BIO	BIO	PKI
VERY HIGH confidence	BIO-A, PKI	BIO-A, PKI	PKI

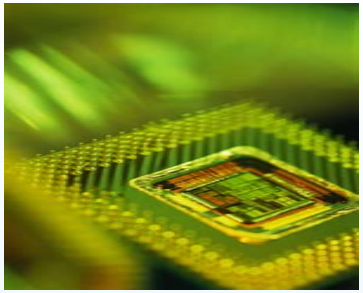
Agenda

- ❑Identity Proofing
- ❑Card Issuance and maintenance
- ❑Logical Credentials
- ❑Authentication Mechanism
- ❑Card Topology

FIPS 201 REQUIREMENTS

PIV Card Requirements

- ❑ Mandatory
  - ❑ Integrated Circuit to Store/Process Data
  - ❑ One Security Feature to Resist Tempering



- ❑ Interfaces:
  - ❑ Contact (ISO/IES 7816)
  - ❑ Contactless (ISO/IES 14443)
- ❑ Optional
  - ❑ Magnetic Stripe
  - ❑ Bar Code
  - ❑ Linear 3 of 9 Bar Code

In Summary

- Identification is based on sound criteria for verifying an individual employee’s identity
- The PIV logical credentials shall contain multiple data elements for the purpose of verifying the cardholder’s identity at graduated assurance levels.
- Multiple data elements support a variety of authentication mechanisms
- Specifications to support interoperability
  - SP 800-73 – *Interfaces for Personal Identity Verification* (card interface commands and responses)
  - SP 800-76 – *Biometric Data Specification for Personal Identity Verification*
  - SP 800-78 – *Recommendation for Cryptographic Algorithms and Key Sizes*
  - SP 800-79 – *Issuing Organization Accreditation Guideline*