Practical Challenges in Adopting PIV/PIV-I

Hank Morris
Purpose and Agenda

• Purpose: Explore the policy, process, and mechanisms to securely leverage biometrics to authenticate the presence of a PIV card owner and solicit feedback

• Agenda:
  o Driving Factors
  o PIV Authentication Mechanisms
  o Interoperability
  o Solution Framework
  o PIV + Local BIO
  o Biometrics Chain-of-Trust

The desired end-state will incorporate lessons learned, establish best practices and a solution framework, and realize economies and efficiencies while maintaining identity assurance and privacy
Mission Impact

• Enable timely access control decisions for authenticated persons
  - Reduce queue times for high volume entry points
  - Leverage existing credential capabilities

• Risk-acceptable identity authentication
  - Improve assurance for high-traffic control points
  - Leverage standard credential and equipment beyond standard functionality
DoD Minimum Standards for Physical Access

- DoD-wide and federally interoperable access control
- Authenticate USG physical access credentials
- Support access enrollment, authorization processes, and securely share information
- Support PIV (CAC) interoperability
  - Verify authenticity of Federal & DoD-issued cards
  - Authenticate cardholder identity
  - Authorize physical access
- Contact/Contactless IAW FIPS 201-1
  - Contactless will be the preferred technology
    - Provides for more rapid throughput
    - Reduces wear and tear on reader and card
- PIV-I acceptable with electronic verification and suitability determination

Source: DTM 09-012, “Interim Policy Guidance for Physical Access Control”, change 1, September 30, 2010
Ramps up efforts for Federal Agencies to issue and start making full use of PIV credentials to access Federal Facilities and Information Systems.

Asks for help in overseeing agency implementation of the plan of action and adoption of the PIV credentials

An attached DHS memo outlines a plan of action for agencies:
- All new systems under development must be enabled to use PIV
- Starting in FY12, existing PACS/LACS must be upgraded to use PIV prior to using development and technology refresh funds to complete other activities
- Procurements IAW HSPD and the FAR
- Processes must accept and electronically verify PIV credentials issued by other federal agencies
- Alignment with FICAM

DoD responded with their plan in Aug 2011 and with amplifying HSPD-12 and ICAM guidance in Nov 2011

“Continued Implementation of [HSPD-12]”, Feb 2011
### Authentication Factors of PIV Authentication Mechanisms

<table>
<thead>
<tr>
<th>PIV Authentication Mechanism</th>
<th>Have</th>
<th>Know</th>
<th>Are</th>
<th>Authentication Factors (HKA Vector)*</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAK + BIO (-A)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>3</td>
<td>Contact</td>
</tr>
<tr>
<td>BIO-A</td>
<td>x</td>
<td></td>
<td>x</td>
<td>2</td>
<td>Contact</td>
</tr>
<tr>
<td>PKI</td>
<td>x</td>
<td>x</td>
<td></td>
<td>2</td>
<td>Contact</td>
</tr>
<tr>
<td>BIO</td>
<td></td>
<td>x</td>
<td></td>
<td>1</td>
<td>Contact</td>
</tr>
<tr>
<td>CAK</td>
<td>x</td>
<td></td>
<td></td>
<td>1</td>
<td>Contact/Contactless</td>
</tr>
<tr>
<td>CHUID + VIS</td>
<td>x</td>
<td></td>
<td></td>
<td>1</td>
<td>Contact/Contactless</td>
</tr>
</tbody>
</table>

Source: SP 800-116, A Recommendation for the Use of PIV Credentials in PACS, 2008

* For all combined mechanisms not in the table, the sum of the HKA vectors correctly predicts the number of factors achieved. For example, PKI + BIO(-A) also achieves three-factor authentication, but is not present in the table because three factors are predicted by the sum of the HKA vectors of PKI and BIO(-A).
FIPS-201-1 Constrains BIO Authentication

- Only with contact read
- Only with PIN activation of card (privacy, not “know”)
- Only with reference samples for automated comparison
  - Face if present is not intended for facial recognition
  - Fingerprints are typical
  - Iris images optional (required in Draft FIPS 201-2 when fingerprints are not available)
Authentication with PIV CHUID

Some characteristics of the CHUID-based authentication mechanism are as follows:

• Digitally-signed object
• Can be used for rapid authentication for high volume access control
• Low resistance to use of unaltered card by non-owner of card
• Applicable with contact-based and contactless readers.
Some characteristics of the PKI-CAK authentication mechanism are as follows:

- Requires the use of online certificate status checking infrastructure
- Highly resistant to credential forgery
- Applicable with contact-based and contactless readers.

**Process Flow:**
1. The reader reads the Card Authentication Key (CAK) certificate from the PIV Card Application.
2. The reader issues a challenge string to the card and requests an asymmetric operation in response.
3. The card responds to the previously issued challenge by signing it using the card authentication private key.
4. 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.
5. The response is validated as the expected response to the issued challenge.
6. The FASC-N from the card authentication certificate is extracted and passed as input to the access control decision.
Some of the characteristics of the PKI-AUTH authentication mechanism are as follows:

- Requires the use of online certificate status checking infrastructure
- Highly resistant to credential forgery
- Strong resistance to use of unaltered card by non-owner since PIN is required to activate card
- Applicable with contact-based card readers.

The PKI-AUTH shall be the alternative authentication mechanism, in cases where neither the fingerprints nor its alternative iris images could be collect for on-card storage. (Draft FIPS 201-2)
## Authentication Factors of PIV Authentication Mechanisms

<table>
<thead>
<tr>
<th>PIV Authentication Mechanism</th>
<th>Have</th>
<th>Know</th>
<th>Are</th>
<th>Authentication Factors (HKA Vector)*</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAK + BIO (-A)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>3</td>
<td>Contact</td>
</tr>
<tr>
<td>BIO-A</td>
<td>x</td>
<td></td>
<td>x</td>
<td>2</td>
<td>Contact</td>
</tr>
<tr>
<td>PKI</td>
<td>x</td>
<td>x</td>
<td></td>
<td>2</td>
<td>Contact</td>
</tr>
<tr>
<td>BIO</td>
<td></td>
<td></td>
<td>x</td>
<td>1</td>
<td>Contact</td>
</tr>
<tr>
<td>CAK</td>
<td>x</td>
<td></td>
<td></td>
<td>1</td>
<td>Contact/Contactless</td>
</tr>
<tr>
<td>CHUID + VIS</td>
<td>x</td>
<td></td>
<td></td>
<td>1</td>
<td>Contact/Contactless</td>
</tr>
</tbody>
</table>

Source: SP 800-116, A Recommendation for the Use of PIV Credentials in PACS, 2008
## Interoperability (across issuers)

<table>
<thead>
<tr>
<th>Authenticator</th>
<th>FIPS-201-1-1</th>
<th>FIPS-201-2-Draft</th>
<th>Interoperable</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHUID</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Yes</td>
</tr>
<tr>
<td>PIV-Auth</td>
<td>Mandatory*</td>
<td>Mandatory</td>
<td>Yes (DoD requires activation)</td>
</tr>
<tr>
<td><strong>Biometric, Fingerprint</strong></td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Yes (when not available, fall back to PIV-Auth or Iris)</td>
</tr>
<tr>
<td><strong>Biometric, Iris</strong></td>
<td>Optional</td>
<td>Mandatory*</td>
<td>Required when fingerprint record cannot be issued</td>
</tr>
<tr>
<td>PKI-CAK</td>
<td>Optional</td>
<td>Mandatory</td>
<td>Yes, when available</td>
</tr>
<tr>
<td>symmetric CAK</td>
<td>Optional</td>
<td>Optional</td>
<td>No, issuer-specific</td>
</tr>
<tr>
<td><strong>digital signature key</strong></td>
<td>Optional*</td>
<td>Optional</td>
<td>No, issuer-option, DoD Std</td>
</tr>
<tr>
<td><strong>key management key</strong></td>
<td>Optional*</td>
<td>Optional</td>
<td>No, issuer-option, DoD Std</td>
</tr>
<tr>
<td><strong>Other Biometrics or Keys</strong> (contact or wireless)</td>
<td>Optional</td>
<td>Optional</td>
<td>No, issuer-specific, issuer-option</td>
</tr>
</tbody>
</table>
Interoperability = “Least Common Denominator”

• “Mandatory” features “least common denominator”
  - Expected of all issuers
  - Establishes the threshold of interoperability

• “Optional” features
  - Not expected of all issuers
  - When implemented, may be standard
  - Not interoperable across all issuers/relying parties
Solution Framework

Leverage Lessons Learned to provide a structured path or “bridge” over the “risk canyon”
PIV + Local Bio -- Registration

• Registration
  - Authenticate cardholder
    - CHUID, PKI-CAK, PKI-Auth, BIO-A
    - Verify identifier, digital signatures, and certificate paths
  - Enroll local record
    - Identifier, CHUID Hash, PKI-CAK or PKI-Auth Cer.
    - PIV biometric templates*
    - Local biometric image/template*

  * Dependent on local authentication needs; “SP 800-76 does specify or off, shall be wrapped in the header defined in section 6.” Patrick Grother, SP800-76 FAQs, http://csrc.nist.gov/groups/SNS/piv/npivp/SP80076FAQ.htm
• **Contactless (ISO/IEC 14443)**
  - Tee-up local record with PIV card CHUID (minimal)

Or

- Authenticate PIV card with PKI-CAK (preferred)

Then

- Capture live biometric sample and verify against **local reference**

Security with tap-and-go convenience/performance

Path checks off-line/batch, within refresh requirements
• **Contact (ISO/IEC 7816)**
  - Tee-up local record with PIV card CHUID
  - Authenticate PKI-CAK or PIV-AUTH
  - Capture live biometric sample and verify against local reference

  Alternative to on-card templates or where contactless is not an option

Path checks off-line/batch, within refresh requirements
PIV Biometric Repositories

- **Authoritative Source**: Each PIV Issuer maintains the authoritative source repository for their respective cardholders.

- **Local Trusted Source**:
  - Each PIV card is a subset of the PIV issuer’s repository
  - A PACS may cache a subset of one or more authoritative sources to support local operations

- **Local Authenticated Source**: Locally enrolled biometric modality, not available from an authoritative source, where the person is authenticated to the authoritative source

*Extending the Biometric Chain of Trust*
Potential for Logical Access Control

- Biometric authentication will not / cannot replace use of PKI for remote authentication (at least not in the near future)

- Biometric authentication can
  - Perhaps with adjustments to technology and policy
  - Activate PKI private key operations
  - Resume or unlock an established session
  - Authenticate to mobile devices, activating PKI or other crypto keys
Summary

- Need for assurance with high throughput
- PKI and Biometric authentication currently requires contact read and cardholder interaction
- Reviewed authentication methods
- Proposed PIV + local BIO methods
- Biometric Chain-of-Trust
Questions and Feedback

Mr. Hank Morris

hank.morris@stopso.com

Strategic Operational Solutions, Inc. (STOPSO)
8381 Old Courthouse Road, Suite 330
Vienna, VA 22182

E-mail: info@stopso.com
Telephone: (703) 942- 8590
Fax: (703) 942- 8597
Web: http://www.stopso.com
Backup
Authentication with PIV CHUID

Process flow:
1. The CHUID is read electronically from the PIV Card.
2. The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted source and is unaltered. (Optional)
3. The expiration date on the CHUID is checked to ensure that the card has not expired.
4. A unique identifier within the CHUID is used as input to the authorization check to determine whether the cardholder should be granted access.
Authentication with CAK

Process Flow:
1. The reader reads the Card Authentication Key (CAK) certificate from the PIV Card Application.
2. The reader issues a challenge string to the card and requests an asymmetric operation in response.
3. The card responds to the previously issued challenge by signing it using the card authentication private key.
4. 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.
5. The response is validated as the expected response to the issued challenge.
6. The FASC-N from the card authentication certificate is extracted and passed as input to the access control decision.
Authentication with PKI-AUTH

Process Flow:
1. The reader reads the PIV Authentication Key certificate from the PIV Card Application.
2. The cardholder is prompted to submit a PIN.
3. The submitted PIN is used to activate the card.
4. The reader issues a challenge string to the card and requests an asymmetric operation in response.
5. The card responds to the previously issued challenge by signing it using the PIV authentication private key.
6. 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.
7. The response is validated as the expected response to the issued challenge.
8. The Subject Distinguished Name (DN) and unique identifier from the authentication certificate are extracted and passed as input to the access control decision.
Authentication with BIO(-A)

Process flow:
1. Present card for contact read
2. Present PIN
3. Unlock card and verify PIV CHUID expiry
4. Retrieve BIO reference sample
5. Present BIO live sample
6. Compare BIO samples