Strategic Operational Solutions

DEFINING STRATEGY | DELIVERING RESULTS

Defining Strategy | Delivering Results



Strategic Operational Solutions
DEFINING STRATEGY | DELIVERING RESULTS

Defining Strategy | Delivering Results

Practical Challenges in Adopting PIV/PIV-I

Hank Morris

Strategic Operational Solutions
DEFINING STRATEGY DELIVERING RESULTS

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:**
  - *Driving Factors*
  - *PIV Authentication Mechanisms*
  - *Interoperability*
  - *Solution Framework*
  - *PIV + Local BIO*
  - *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

Strategic Operational Solutions
DEFINING STRATEGY DELIVERING RESULTS

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

Strategic Operational Solutions
DEFINING STRATEGY DELIVERING RESULTS

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**

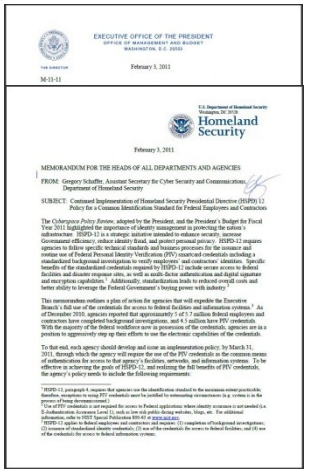
Source: DTM 09-012, "Interim Policy Guidance for Physical Access Control", change 1, September 30, 2010

Strategic Operational Solutions

DEFINING STRATEGY | DELIVERING RESULTS

OMB M-11-11: Raising the Bar for PIV Compliance

- **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**



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

February 3, 2011

M-11-11

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

February 3, 2011

MEMORANDUM FOR THE HEADS OF ALL DEPARTMENTS AND AGENCIES

FROM: Gregory Schaffer, Assistant Secretary for Cyber Security and Communications, Department of Homeland Security

SUBJECT: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors

The *Cyberspace Policy Review*, adopted by the President, and the President's Budget for Fiscal Year 2011 highlighted the importance of identity management in protecting the nation's infrastructure. HSPD-12 is a strategic initiative intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. HSPD-12 requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal Personal Identity Verification (PIV) enhanced credentials including a standardized background investigation to verify employees' and contractors' identities. Specific benefits of the standardized credentials required by HSPD-12 include secure access to federal facilities and disaster response sites, as well as multi-factor authentication and digital signature and encryption capabilities.[1] Additionally, standardization leads to reduced overall costs and better ability to leverage the Federal Government's buying power with industry.[2]

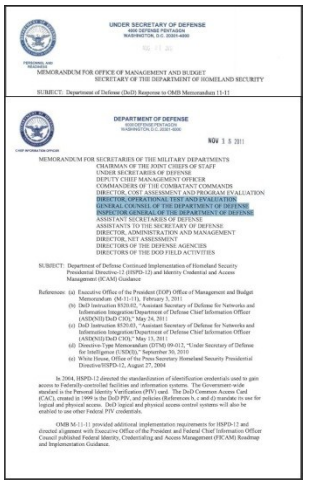
This memorandum outlines a plan of action for agencies that will expedite the Executive Branch's full use of the credentials for access to federal facilities and information systems.[3] As of December 2010, agencies reported that approximately 5 of 5.7 million Federal employees and contractors have completed background investigations, and 4.5 million have PIV credentials. With the majority of the federal workforce now in possession of the credentials, agencies are in a position to aggressively step up their efforts to use the electronic capabilities of the credentials.

To that end, each agency should develop and issue an implementation policy, by March 31, 2011, through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems. To be effective in achieving the goals of HSPD-12, and realizing the full benefits of PIV credentials, the agency's policy needs to include the following requirements:

[1] HSPD-12, paragraph 4, requires that agencies use the identification standard to the maximum extent practicable; therefore, exceptions to using PIV credentials must be justified by outstanding circumstances (e.g. systems is in the process of being decommissioned).

[2] Use of PIV credentials is not required for access to Federal applications where identity assurance is not needed (i.e. E-Authentication Assurance Level 1), such as low risk public-facing websites, blogs, etc. For additional information, refer to NIST Special Publication 800-63 at www.nist.gov.

[3] HSPD-12 applies to federal employees and contractors and requires: (1) completion of background investigations; (2) issuance of standardized identity credentials; (3) use of the credentials for access to federal facilities; and (4) use of the credentials for access to federal information systems.



UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-4000

MEMORANDUM FOR OFFICE OF MANAGEMENT AND BUDGET
SECRETARY OF THE DEPARTMENT OF HOMELAND SECURITY

SUBJECT: Department of Defense (DoD) Response to OMB Memorandum 11-11

DEPARTMENT OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON D.C. 20301-4000

NOV 18 2011

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Department of Defense Continued Implementation of Homeland Security Presidential Directive-12 (HSPD-12) and Identity Credential and Access Management (ICAM) Guidance

References: (a) Executive Office of the President (EOP) Office of Management and Budget Memorandum (M-11-11), February 3, 2011
(b) DoD Instruction 8520.02, "Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO)," May 24, 2011
(c) DoD Instruction 8520.03, "Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO)," May 13, 2011
(d) Directive-Type Memorandum (DTM) 09-012, "Under Secretary of Defense for Intelligence (USD(I))," September 30, 2010
(e) Deputy Secretary of Defense Memorandum, Homeland Security Presidential Directive/HSPD-12, August 27, 2004

In 2004, HSPD-12 directed the standardization of identification credentials used to gain access to Federally-controlled facilities and information systems. The Government-wide standard is the Personal Identity Verification (PIV) card. The DoD Common Access Card (CAC), created in 1999 in the DoD PIV, and policies (References b, c and d) mandate its use for logical and physical access. DoD logical and physical access control systems will also be enabled to use other Federal PIV credentials.

OMB M-11-11 provided additional implementation requirements for HSPD-12 and directed alignment with Executive Office of the President and Federal Chief Information Officer Council published Federal Identity, Credentialing and Access Management (FICAM) Roadmap and Implementation Guidance.

"Continued Implementation of [HSPD-12]", Feb 2011

Strategic Operational Solutions
DEFINING STRATEGY DELIVERING RESULTS

Authentication Factors of PIV Authentication Mechanisms

PIV Authentication Mechanism	Have	Know	Are	Authentication Factors (HKA Vector)*	Interface
CAK + BIO (-A)	x	x	x	3	Contact
BIO-A	x		x	2	Contact
PKI	x	x		2	Contact
BIO			x	1	Contact
CAK	x			1	Contact/ Contactless
CHUID + VIS	x			1	Contact/ Contactless

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).

Strategic Operational Solutions
DEFINING STRATEGY DELIVERING RESULTS

FIPS-201-1 Constrains BIO Authentication

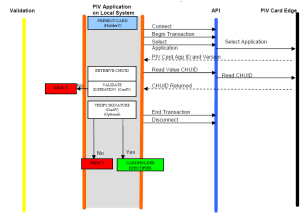
- **Only with contact read**
- **Only with PIN activation of card (privacy, not "know")**
- **Only with reference samples for automated comparison**
  - Face if present is not intended for facial recognition
  - Fingerprints are typical
  - Iris images optional (required in Draft FIPS 201-2 when fingerprints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

Strategic Operational Solutions
DEFINING STRATEGY DELIVERING RESULTS

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.



Process flow:

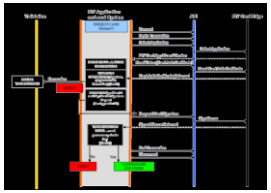
1. The CHUID is read electronically from the PIV Card.
2. The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted source and is unaltered. (Optional)
3. The expiration date on the CHUID is checked to ensure that the card has not expired.
4. A unique identifier within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

Strategic Operational Solutions
DEFINING STRATEGY DELIVERING RESULTS

Authentication with CAK

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:

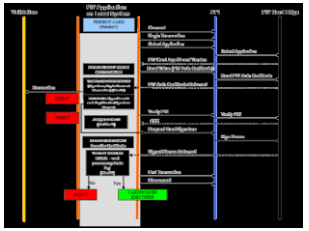
1. The reader reads the Card Authentication Key (CAK) certificate from the PIV Card Application.
2. The reader issues a challenge string to the card and requests an asymmetric operation in response.
3. The card responds to the previously issued challenge by signing it using the card authentication private 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.

Strategic Operational Solutions
DEFINING STRATEGY DELIVERING RESULTS

Authentication with PKI-AUTH

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)***



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.

Strategic Operational Solutions
DEFINING STRATEGY DELIVERING RESULTS

Authentication Factors of PIV Authentication Mechanisms

PIV Authentication Mechanism	Have	Know	Are	Authentication Factors (HKA Vector)*	Interface
CAK + BIO (-A)	x	x	x	3	Contact
BIO-A	x		x	2	Contact
PKI	x	x		2	Contact
BIO			x	1	Contact
CAK	x			1	Contact/ Contactless
CHUID + VIS	x			1	Contact/ Contactless

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

Strategic Operational Solutions
DEFINING STRATEGY DELIVERING RESULTS

Interoperability (across issuers)

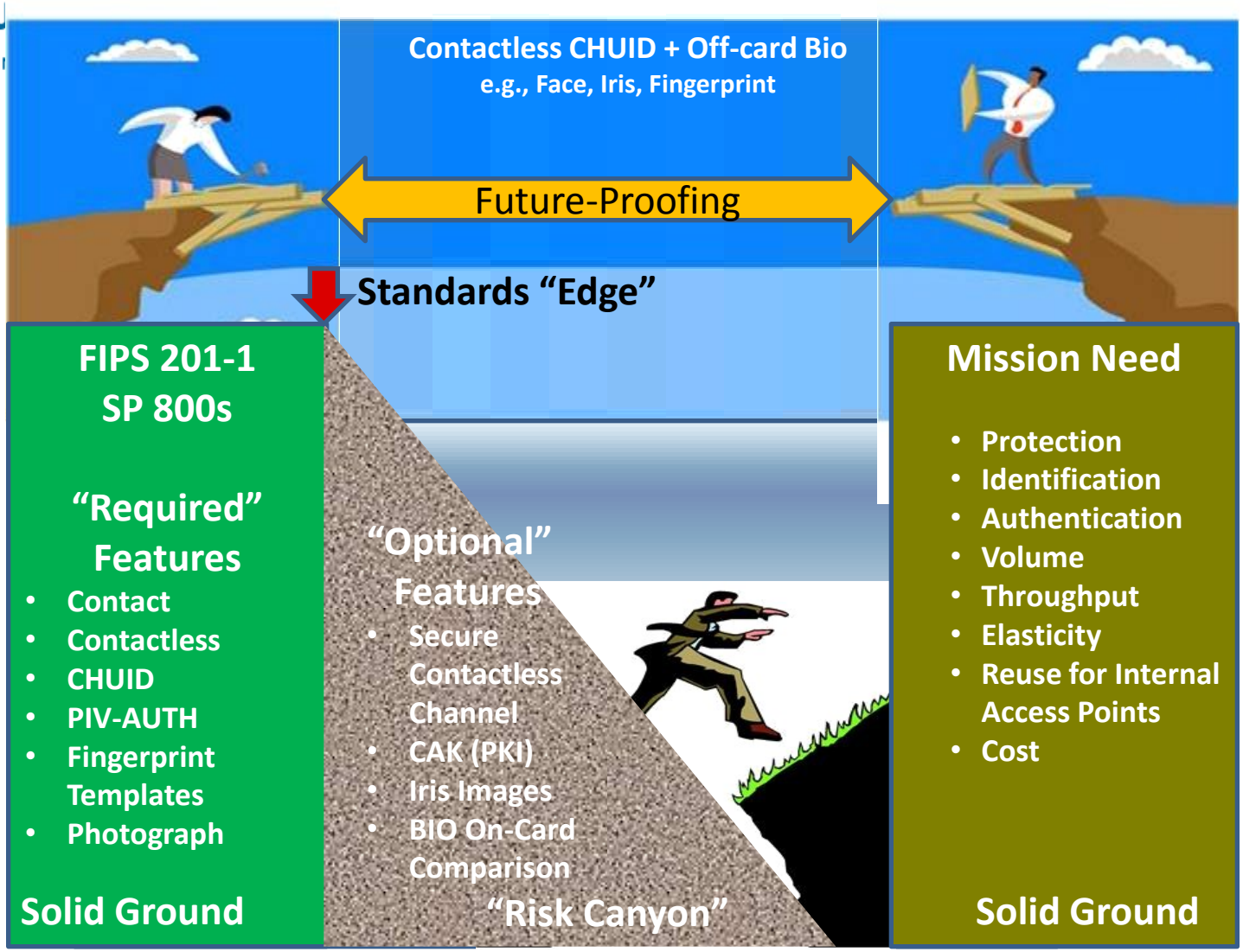
Authenticator	FIPS-201-1-1	FIPS-201-2-Draft	Interoperable
CHUID	Mandatory	Mandatory	Yes
PIV-Auth	Mandatory*	Mandatory	Yes (DoD requires activation)
Biometric, Fingerprint	Mandatory	Mandatory	Yes (when not available, fall back to PIV-Auth or Iris)
Biometric, Iris	Optional	Mandatory*	Required when fingerprint record cannot be issued
PKI-CAK	Optional	Mandatory	Yes, when available
symmetric CAK	Optional	Optional	No, issuer-specific
digital signature key	Optional*	Optional	No, issuer-option, DoD Std
key management key	Optional*	Optional	No, issuer-option, DoD Std
Other Biometrics or Keys (contact or wireless)	Optional	Optional	No, issuer-specific, issuer-option

Strategic Operational Solutions
DEFINING STRATEGY DELIVERING RESULTS

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"

Strategic Operational Solutions
DEFINING STRATEGY DELIVERING RESULTS

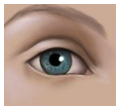
PIV + Local Bio -- Registration

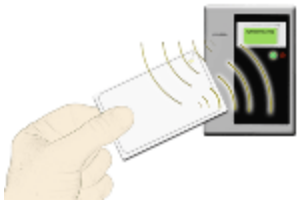
- **Registration**
  - Authenticate cardholder
    - *CHUID, PKI-CAK, PKI-Auth, BIO-A*
    - *Verify identifier, digital signatures, and certificate paths*
  - Enroll local record
    - *Identifier, CHUID Hash, PKI-CAK or PKI-Auth Cer*
    - *PIV biometric templates**
    - *Local biometric image/template**

- *** Dependent on local authentication needs; "SP 800-76 does specify d 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**

Strategic Operational Solutions
DEFINING STRATEGY DELIVERING RESULTS

PIV + Local BIO -- Authentication





- **Contactless (ISO/IEC 14443)**
  - Tee-up local record with PIV card CHUID (minimal)

  Or

  - Authenticate PIV card with PKI-CAK (preferred)

  Then

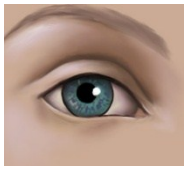
  - Capture live biometric sample and verify against **local reference**

Security with tap-and-go convenience/performance

Path checks off-line/batch, within refresh requirements

Strategic Operational Solutions
DEFINING STRATEGY DELIVERING RESULTS

PIV + Local BIO -- Authentication



- **Contact (ISO/IEC 7816)**
  - Tee-up local record with PIV card CHUID

  Or
  - Authenticate PKI-CAK or PIV-AUTH

  Then
  - Capture live biometric sample and verify against local reference

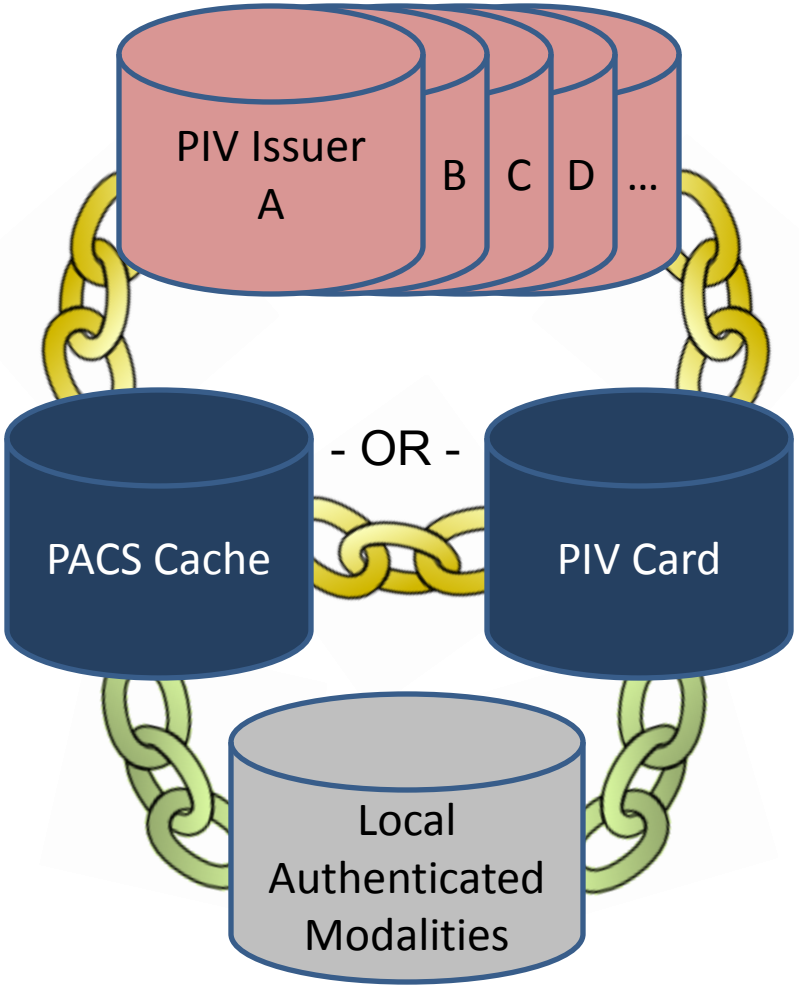
Alternative to on-card templates or where contactless is not an option

Path checks off-line/batch, within refresh requirements

Strategic Operational Solutions

DEFINING STRATEGY | DELIVERING RESULTS

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

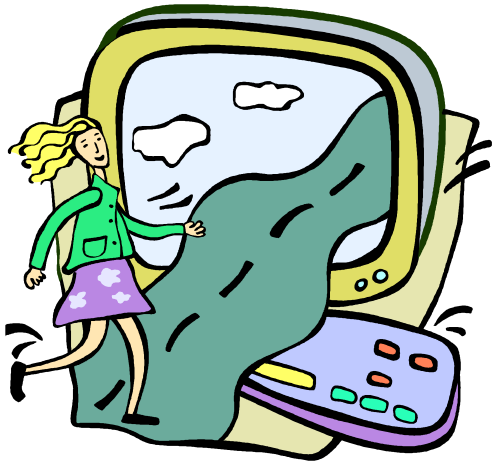
- **Local Authenticated Source**: Locally enrolled biometric modality, not available from an authoritative source, where the person is authenticated to the authoritative source

Extending the Biometric Chain of Trust

Strategic Operational Solutions
DEFINING STRATEGY DELIVERING RESULTS

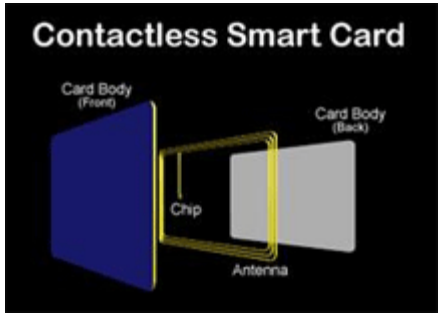
Potential for Logical Access Control

- **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

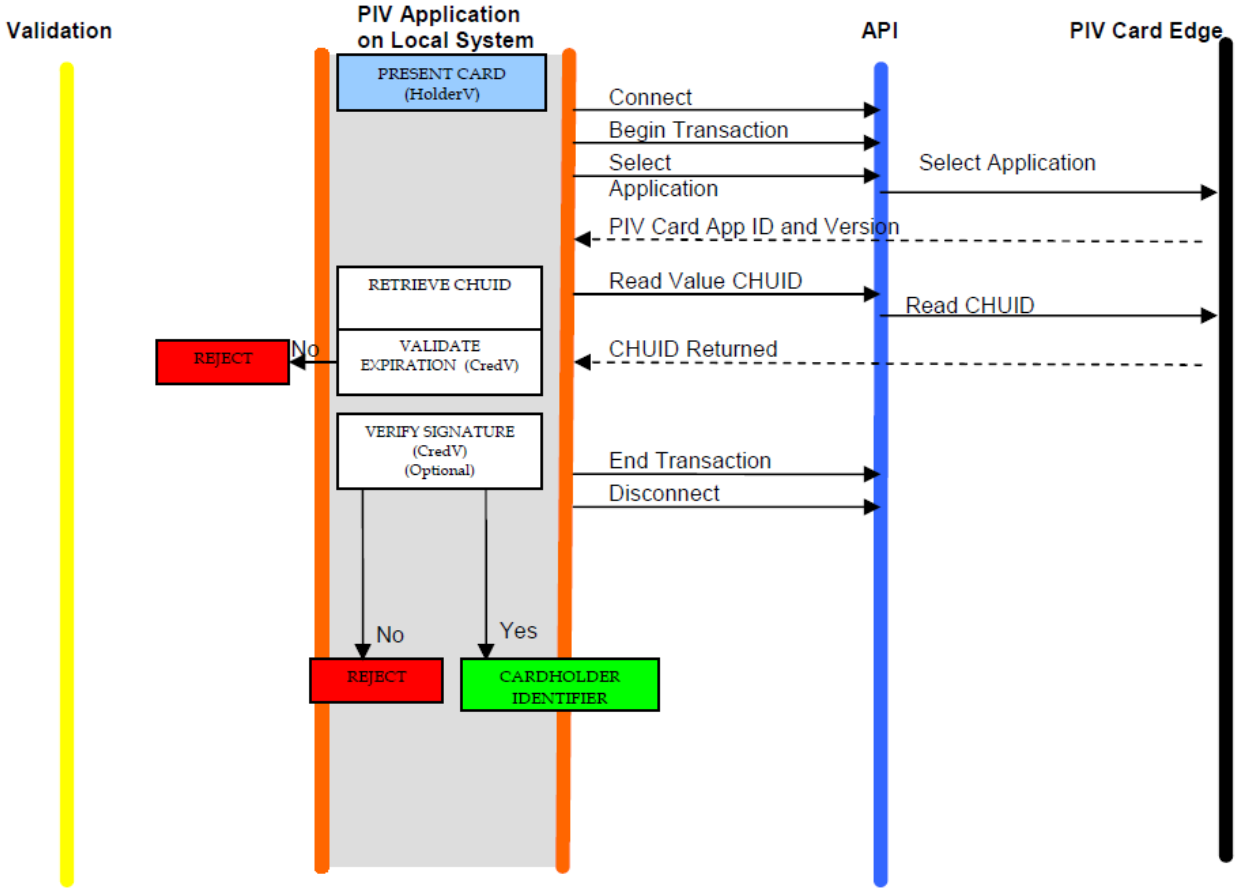
Strategic Operational Solutions, Inc. (STOPSO)
8381 Old Courthouse Road, Suite 330
Vienna, VA 22182

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

Backup

Strategic Operational Solutions

Authentication with PIV CHUID



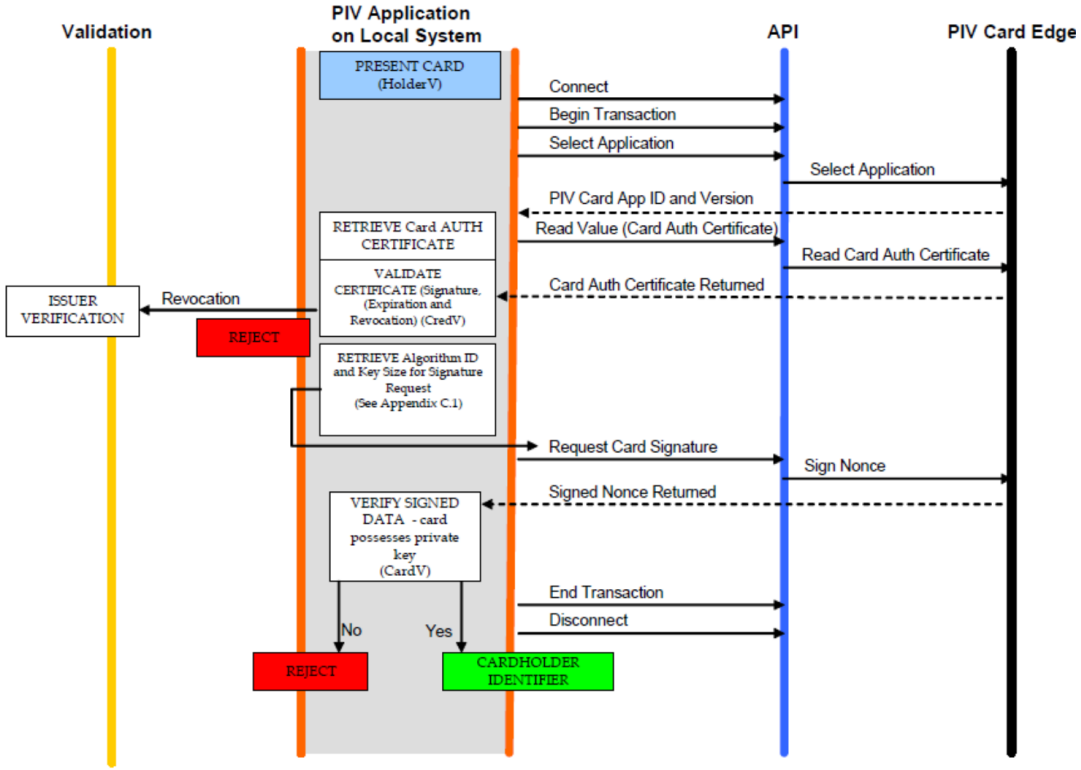
Process flow:

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.

Strategic Operational Solutions

DEFINING STRATEGY DELIVERING RESULTS

Authentication with CAK



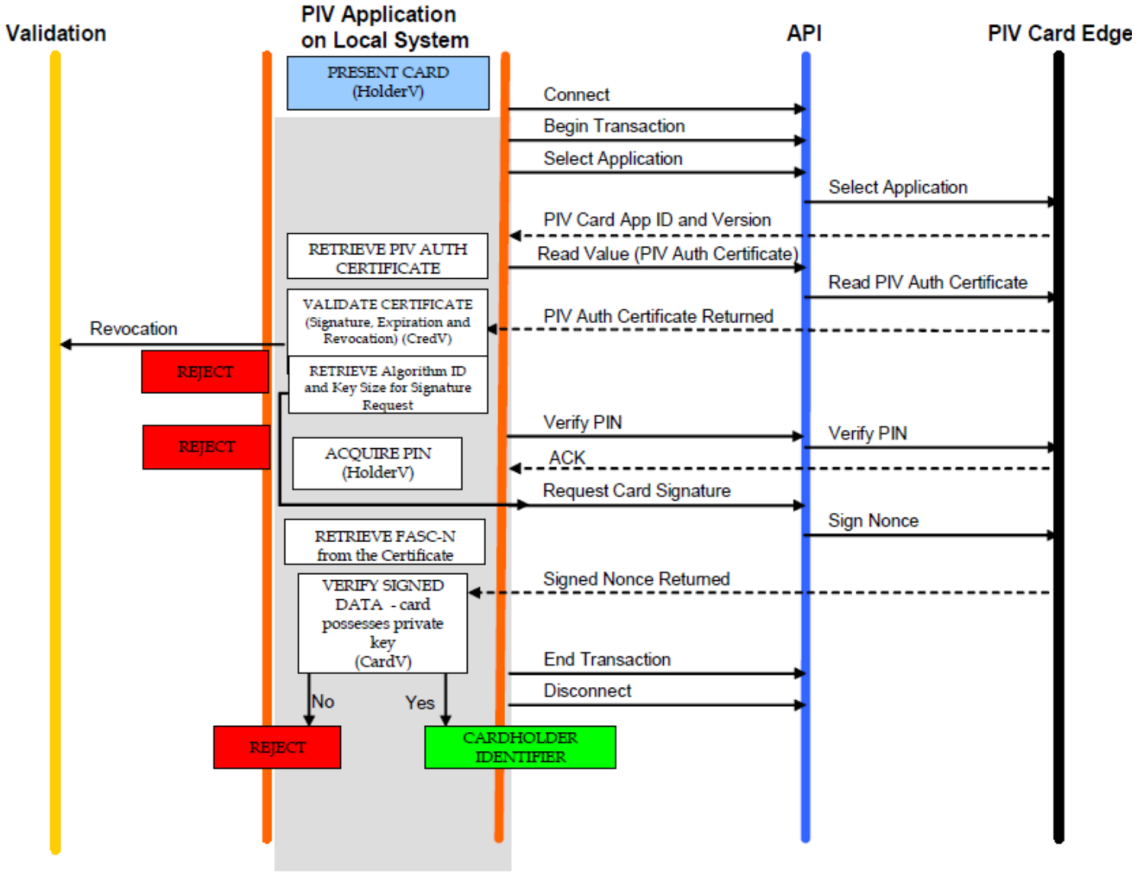
Process Flow:

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.

Strategic Operational Solutions

DEFINING STRATEGY DELIVERING RESULTS

Authentication with PKI-AUTH

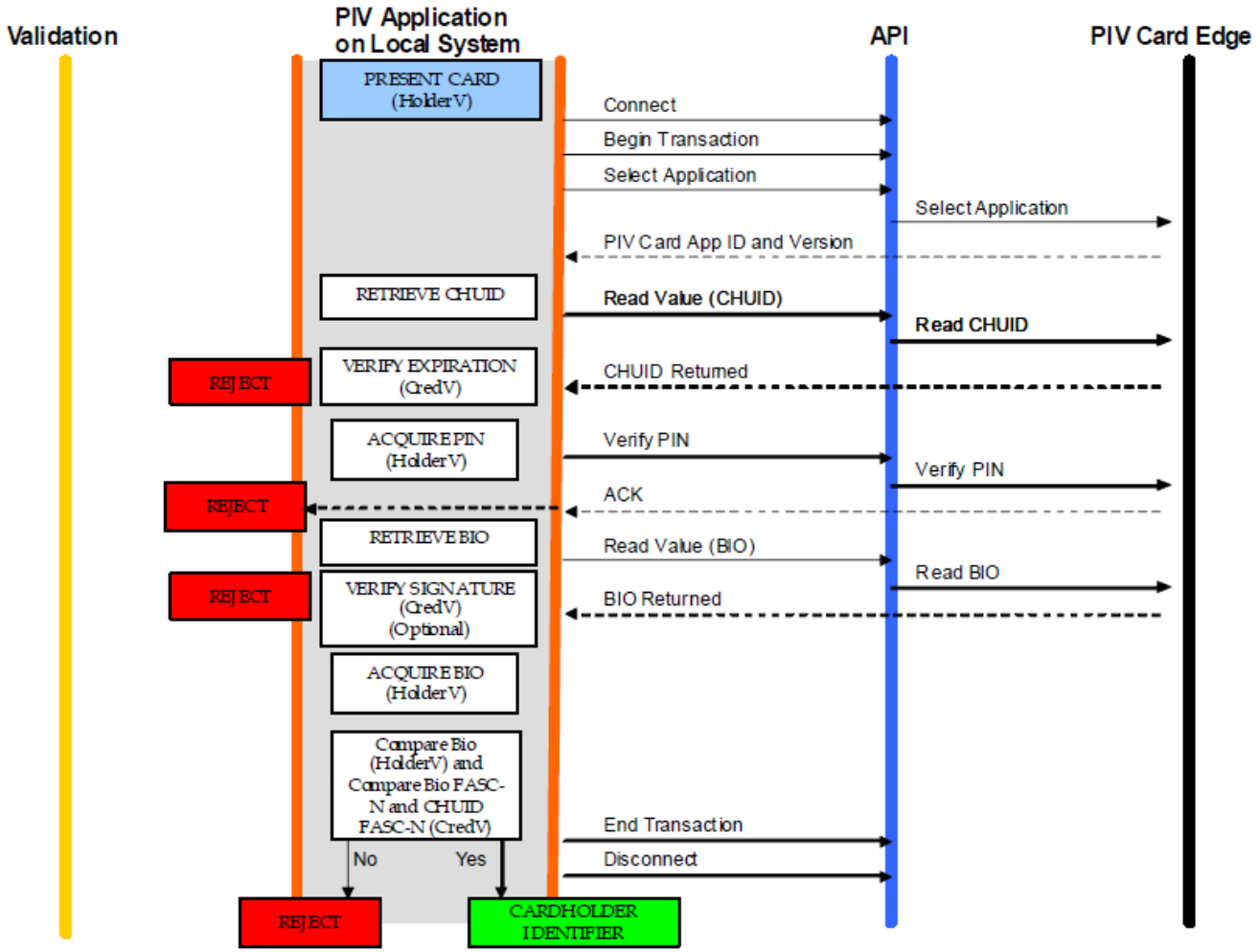


Process Flow:

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.

Strategic Operational Solutions

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