Interagency Advisory Board

Meeting Agenda, Tuesday, November 1, 2011

1. **Opening Remarks** *(Mr. Tim Baldridge, IAB Chair)*

2. **FIPS 201-2 Update and Panel Discussion with NIST Experts in Q&A Session** *(Bill MacGregor and Hildy Ferraiolo, NIST)*

3. **Securing Mobile Devices for Government Specific Apps** *(Debb Blanchard, Verizon)*

4. **Enabling HSPD-12 and Biometrics to Secure the Pentagon and Mark Center** *(Derek Nagel and Roger Roehr, PFPA)*

5. **An Example of Enabling HSPD-12 in Multi-Tenant Building by Operating a PACS Platform as a Service** *(Tom Corder, Bridgepoint Systems)*

6. **DoD PIV-I Update** *(Paul Grant, DoD)*

7. **Closing Remarks** *(Mr. Tim Baldridge, IAB Chair)*

UPDATES ON THE PERSONAL IDENTITY VERIFICATION STANDARDS

Hildegard Ferraiolo
Computer Security Division
NIST ITL

Government Smart Card

Interagency Advisory Board (IAB) Meeting

1Nov2011

FIPS 201 History and Projection

- 2005 – 2010 -- Collected comments on FIPS 201-1 in anticipation and preparation of the next revision.

2011

March Publication of Draft FIPS 201-2

April Draft FIPS 201-2 workshop

June End of public comment period

- » 1K+ comment received from
- » Federal Agencies and Department
- » Industry
- » Private Sector

April – Today Comment Resolution

2011 2012

Next Steps…

- Continue Comment Resolution
- 2nd Draft FIPS 201-2 released for public comment period (~30 days)
- Resolve Comments on 2nd Draft FIPS 201-2
- Deliver Candidate FIPS 201-2 to the Secretary of DoC for consideration
- Announce Final FIPS 201-2 with Federal Register Notice
- Publish Final FIPS 201-2 at csrc.nist.gov
- Publish public comments and resolutions

General Goal

1. Improved Efficiency
   - *Simple models for in-person visits to PIV Issuer*
2. Improved Security
   - *Reduce reliance on CHUID authentication*
3. Add Requested Capabilities
   - *Biometric On-Card Comparison*
   - *Mobile device authentication*
4. Updated References & Inclusions
   - *I-9 identity documents*
   - *OPM "Final Credentialing Standards…"*

Improved Security

- Reduce reliance on CHUID authentication

  – CHUID does not provide level 2 “some assurance”

  – Alternative PACS mechanism: CAK

- CHUID will be deprecated in FIPS 201-2 and eliminated in FIPS 201-3

Topic Area: Biometric On Card Comparison

2005 2010

Biometric On Card Comparison (Biometric OCC) for authentication is viable and desired by federal agencies

OCC and FIPS 201-2

- *Enable Biometric OCC for contactless applications, esp., PACS*
  - client side authenticated secure channel protocol for transmission of life scan to card
  - Can we leverage secure channel for mobility?
  - …..should use mutual authenticated secure channel
- *Enable Biometric OCC to reset the PIN*
  - Satisfies 'remote' PIN resets requests

Topic Area: Card Capability – PIN Reset

- Many divergent comments
  - *In-person appearance required for PIN Reset*
  - *Please specify remote PIN Reset capability (from Business Requirement Meeting)*
  - *Allow biometric OCC to reset the PIN*
  - *We need guidelines*
- *FIPS 201-2 states PIV baseline requirements*
  - *Implementation guidelines are out of scope of FIPS 201-2*
- *Special publication will address guidelines:*
  1. *PIN reset followed by BIO-A (FIPS 201-1 status quo)*
  2. *PIN reset + Biometric OCC - 1 command (remote solution -- kiosk)*
     - PIV card will not reset PIN, if biometric match fails
  3. *Chain-of-trust followed by PIN reset (remote or in person)*
     - PIV card will not be reset PIN by CMS, if biometric match fails
  4. *Primary identity source documents (in person)*
- *Current proposal is to allow both remote and in-person resets.*

Topic Area: PIV Card Topography

- Printed Name
  - *PIV Card is an official USG identity document*
  - *In general, follow ICAO specification*
    - *DoS 7 FAM 1300 Appendix C also informative*
  - *Recognize need for name changes*
  - *Allow for pseudonyms to protect employees*
- Section 508 Compliance (Card Orientation Feature)
  - *"Current proposed feature is too small"*
  - *Considering other features & placement*

Topic Area: Authentication Mechanism

Many divergent comments

- *Deprecate CHUID,*
- *Deprecate VIS,*
- *Include (VIS and CHUID)*

Under active discussion.

Topic Area: Mobility

2005 2010

Move from 'stationary' desktop/laptop environment to mobile 'anytime and anywhere' federal workforce. (laptop, tablets, smart phones….)

Mobility and FIPS 201-2

- *Engaged with SP 800-63 team & stakeholders to enable PIV derived credentials for portable devices*
  - embedded for remote access/services
  - E.g. access 'same' services/application from different devices using credentials derived for the PIV Card
  - Challenge: Maintain HSPD-12 goal of "Common Identification" in mobile devices.
- *Defining use cases for mobile device activation with the PIV card*
  - PIV card's communication channel (contactless) restricts solution to NFC? Smart phone becomes NFC reader?
  - New requirements for secure channels emerge? One-way and/or mutual channel authentication?
  - FIPS 201-2 will not contain the technical detail.

SmartCard Alliance Conference

- **Track 1 - NIST Updates on Personal Identity Verification Standards**
- *9:00 am – 10:15 am:*

- *FIPS 201-2 Updates,* Hildegard Ferraiolo, NIST
- *PIV and Mobile Devices,* Bill MacGregor, NIST
- David Cooper, NIST, *Cryptography for Authentication Related to PIV & Derived*

Question?

Panelists:

Hildegard Ferraiolo

William MacGregor

Ketan Mehta

Annie Sokol

Thank you!

Hildegard Ferraiolo
hferraio@nist.gov

National Institute of Standards and Technology