

Interagency Advisory Board

Meeting Agenda, March 23, 2011

1. **Open Remarks** (*Mr. Tim Baldridge, IAB Chair*)
2. **Impact of M-11-11 on PACS** (*Ron Martin, HHS*)
3. **FIPS 201-2 Update** (*Bill MacGregor, NIST*)
4. **Status Brief on ICAM Roadmap** (*Shelly Hartsook, Deloitte*)
5. **Status of FPKI Management Authority** (*MA Team, GSA*)
6. **Closing Remarks** (*Mr. Tony Cieri*)



FIPS 201-2 Revision: Status & Highlights

William I. MacGregor
NIST ITL Computer Security Division
william.macgregor@nist.gov

NIST, Gaithersburg
22Mar2011



Status of HSPD-12 Implementation

- First the eggs, then the chickens...
 - PIV Cards are the eggs
 - Applications are the chickens
- How many eggs? Roughly,
 - 4.6M PIV Cards issued to employees (80%)
 - 1.6M PIV Cards issued to contractors (30%)
- Now it's time for chickens...
 - “Federal Identity Credentialing and Access Management (FICAM) Roadmap and Implementation Guidance”
 - Part A: ICAM Segment Architecture completed Sep2009
 - Part B: Implementation Guidance work-in-progress



Useful URLs

- http://www.whitehouse.gov/omb/e-gov/hspd12_reports/ - **OMB quarterlies**
- <http://csrc.nist.gov/groups/SNS/piv/standards.html> - **FIPS 201 & NIST pubs**
- <http://www.idmanagement.gov/> - **ICAMSC & GSA ID management resources**
- http://www.idmanagement.gov/drilldown.cfm?action=hspd12_faqs - **FAQs**
- <http://fips201ep.cio.gov/> - **HSPD-12 Evaluation Program (APL)**
- <http://www.nist.gov/itl/iad/> - **NIST biometrics resources**

- There are now dozens of OMB Memoranda, NIST publications, CIO Council publications, Federal PKI Policy Authority publications, GSA documents, OPM documents, and others relevant to HSPD-12.
- And, of course, OMB M-11-11.



The Larger Context

- Built on DoD Common Access Card experience.
- Enhanced to scale US Government-wide:
 - Simple, self-contained app, with assurance processes.
 - Authenticate, Encrypt/Decrypt, Sign/Verify.
 - Defined issuance processes, limited crypto capabilities.
- Expanding to other communities:
 - PIV Interoperable (PIV-I) Cards issued by Non-Federal Issuers.
 - PIV-I uses same blank card stock as PIV.
 - The Federal Bridge unifies the trust model for all participants.
- After five years, new requirements are being heard!
 - Mutual authentication (i.e., token $\leftarrow \rightarrow$ application)?
 - Alternate token form factors (e.g., smartphone)?
 - Cardholder privacy policies and selective disclosure?



The Revision of FIPS 201-1

- NIST was obligated to consider the need for revision of FIPS 201 five years after publication (i.e., in 2010).
- NIST determined that FIPS 201-1 should be revised, and prepared Draft FIPS 201-2.
- The revision was announced in the Federal Register on 8Mar2011.
- On the same day, Draft FIPS 201-2 was available on the NIST website for a 90 day public comment period.



Status of the Revision

- See the launch announcement
 - http://csrc.nist.gov/news_events/index.html#mar8
- Workshop at NIST on **18-19Apr2011**
 - Attend in person, registration fee \$160
 - Watch & listen via webcast, free
- Comments must be received by **6Jun2011**



FIPS 201 Business Requirements Meeting

- NIST hosted a Business Requirements Meeting on July 12th, 2010 at Gaithersburg, MD.
- The meeting was open to government participants only.
- Purpose of the meeting was to gather and validate business requirements from Federal departments and agencies.
- Agencies provided additional requirements for FIPS 201 in writing after the meeting.
- Meeting input validated many comments heard before, and clarified important requirements.



Notes to the Reader

- The draft is not perfect!
 - *We need your opinions and good ideas.*
- Just because text was left untouched...
 - *Doesn't mean it shouldn't change!*
- Proposed changes can be improved
 - *Completed, simplified, coordinated, etc.*



“Top Ten” List of Proposed Changes (there are more...)

1. Make the Card Authentication Key mandatory
 - ▶ A stronger alternative for PACS than the CHUID authentication method, government-wide interoperable.
2. Extend the maximum length of the printed name
 - ▶ Eliminate name truncation, if possible, and the resulting irritation and inaccuracies that result.
3. Allow chain-of-trust “reconnect” to IDMS record via biometric match
 - ▶ Eliminate repeat Background Investigations in the event of a lost, stolen, or damaged card, with biometric match.
4. Bring I-9 Identity Source Document specifications into FIPS 201-2
 - ▶ Define the permitted combinations of I-9 Identity Source Documents in FIPS 201-2, reducing confusion and mistakes.
5. Make card lifecycle management more efficient
 - ▶ Increase nominal time between in-person visits to the issuer from 2.5 years to 4 years.