FIPS 201-2 Revision: Requirements & Goals

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

With thanks to Ketan Mehta for the use of his slides.

ISPAB
Washington, DC
3Mar2011

Status of HSPD-12 Implementation

- First the eggs, then the chickens

- OMB PIV Issuance Quarterly Reports
  - http://www.whitehouse.gov/omb/e-gov/hspd12_reports/

- Approximately
  - 4.6M PIV Cards issued to employees (80%)
  - 1.6M PIV Cards issued to contractors (30%)

- FICAM Roadmap and Implementation Guidance
  - Eggs and chickens: “Federal Identity Credentialing and Access Management”
  - Part A: ICAM Segment Architecture completed Sep2009
  - Part B: Implementation Guidance work-in-progress
  - *Much of the new work is organized in the ICAMSC toward the FICAM Roadmap.*

Useful URLs

- http://csrc.nist.gov/groups/SNS/piv/standards.html
- http://www.idmanagement.gov/
- http://www.idmanagement.gov/drilldown.cfm?action=hspd12_faqs
- http://fips201ep.cio.gov/
- http://www.nist.gov/itl/iad/

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

The Revision of FIPS 201-1

- As a matter of standing policy and specific language in FIPS 201-1, NIST is obligated to consider the need for revision of FIPS 201 every five years.
- Over the past two years, NIST determined that there is a need for revision of FIPS 201-1, and has prepared draft FIPS 201-2.
- The launch of the revision will be announced in the Federal Register, and at about the same time, draft FIPS 201-2 will be published on the NIST website for a 90 day comment period.
- A public workshop will be held at NIST in mid-April (the dates will be in the FRN). The workshop will also be webcast, receive-only.

FIPS 201 Business Requirements Meeting

- NIST hosted a Business Requirements Meeting on July 12th, 2010 at Gaithersburg, MD.
- Meeting was open to government participants only.
- Purpose of the meeting was to gather business requirements for FIPS 201 from Federal departments and agencies.
- Agencies provided additional requirement for FIPS 201 in writing after the meeting.
- NIST compiled and processed all the business requirements.

Status

- This presentation discusses **selected comments** gathered from the BRM meeting.
- Requirements that met general consensus are discussed.
- These requirements are currently being reviewed and processed.
- Approval of specific text in the public draft will occur through the DoC launch decision process.
- All proposals mentioned here are subject to change.

Agenda – Discuss FIPS 201 business requirements

- Change Management
- PIV Card Lifecycle Management
- Visual Card Topography
- PIV Card Logical Credentials
- PACS and LACS Application Development

Change Management

- Two principles of Change Management:
  - Do no harm, don’t break what works
  - Anything we change should not astonish anyone
- Changes should be introduced over 5 to 6 year period to allow agencies time to execute transition plans.
- FIPS 201 should contain only the requirements that change infrequently and details implementation should be in NIST Special Publications.
- A new requirement should be introduced as an option in a FIPS 201 revision, and as mandatory, if appropriate, in the next revision.

PIV Card Lifecycle Management

- Chain-of-trust is required. Issuer must implement and maintain chain-of-trust record which includes latest biometric authentication data.
- Update reissuance and renewal requirements to:
  - Reduce number of in-person visits
  - Use the chain-of-trust for identity proofing
  - Extend the expiration date when feasible
- Synchronize lifecycle of card, certificates, and biometric data.
- Allow remote post-issuance updates to the PIV Card.

Visual Card Topography

- Include requirements for Section 508 compliance.
- FIPS 201 should describe the card topography requirements at a high-level and the details should go into the SP 800-104. Also, make SP 800-104 normative.
- Clarify requirements for Name format and size.
- Everything printed on the card should also be electronically recorded on the chip.

PIV Logical Credentials

- Make Asymmetric Card Authentication Key mandatory, symmetric optional (both can be present).
- Add requirement to capture alternate biometric to fingerprint when reliable fingerprints cannot be collected.
- Add On-card comparison and mutual authentication secure session as optional features.
- Clarify requirements for PIN reset and PIN unblock.
- Clarify requirements for hardware versus software keys.