Interagency Advisory Board

Meeting Agenda, Wednesday, December 7, 2011

1. **Opening Remarks** *(Mr. Tim Baldridge, IAB Chair)*
2. **FIPS 201-2 Goes Mobile** *(Bill MacGregor, NIST)*
3. **Logon to Google Apps Using NASA Issued PIV** *(Tim Baldridge, NASA, IAB Chair)*
4. **Implementing PKE for JPAS** *(Maxwell Funk and Autumn Crawford-Grijalva, DoD)*
5. **Provisioning PACS using the GAMS** *(Bill Lin, GSA)*
6. **Closing Remarks** *(Mr. Tim Baldridge, IAB Chair)*

FIPS 201-2 Goes Mobile

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

IAB Meeting, Room 203
GSA OCS 1275 North First St NE, Washington, DC
7Dec2011

National Institute of Standards and Technology

Homeland Security Presidential Directive #12

HSPD-12 set the goal for FIPS 201, the Personal Identity Verification (PIV) Standard:

…it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing **a mandatory, Government-wide standard for secure and reliable forms of identification** issued by the Federal Government to its employees and contractors…

Identity on Mobile Devices

In the context of mobile devices alone, personal identity today is not

- Subject to a mandatory Government-wide standard, and
- Subject to Government-wide security and reliability assurance processes, and
- Required for all Federal employees and contractors.

PIV, however, is…

Identification that

a) is issued based on sound criteria for verifying an individual employee's identity;

b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;

c) can be rapidly authenticated electronically; and

d) is issued only by providers whose reliability has been established by an official accreditation process.

PIV Card Issuance Status

OMB Summary as of 1Sep2011

Employees	4,270,560	90.6%
Contractors	846,365	80.7%

The value of mobile devices

The value of mobile devices and cloud computing cannot be ignored:

- Efficiency
- Availability
- Usability

Mobile Devices + Personal Identity Verification = ?

"…[agencies] shall, to the maximum extent practicable, require the use of identification…that meets the Standard…" **- HSPD-12**

Standard Strategy Goals

- Leverage Federal PIV identities with smart phones, tablets and other mobile devices
- Satisfy HSPD-12 and OMB-11-11 guidance
- Achieve usability demanded by mobility,
  - *with the flexibility to use COTS devices,*
  - *and all or most PIV Card capabilities.*
- Supply authenticated PIV identity:
  - *To apps on the local mobile device*
  - *To applications or services on remote systems*
- Provide other PIV services to the device

Current Approaches

1. "Conventional"

   Contact card reader, middleware on device

2. Battery-Powered Sled

   Sled holds PIV Card; uses Wi-Fi or Bluetooth

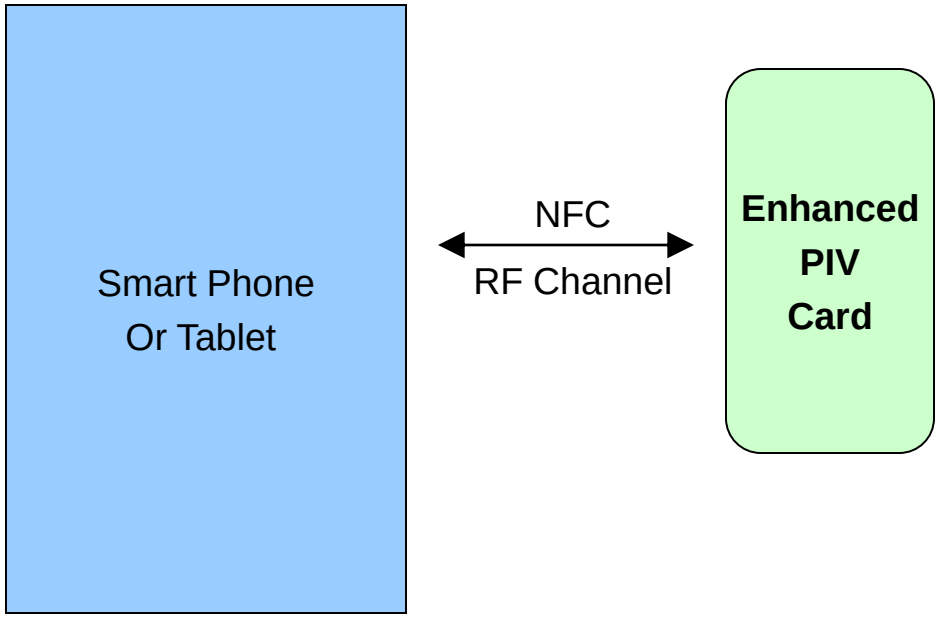
3. Federal Bridge or Trust Framework Provider

   Apply either of these two ICAMSC models

(1) and (2) use PIV Cards, but require extra parts.

(3) Requires no extra parts, but does not conform to FIPS 201-1.

Enhanced PIV Card



- Requires use of PIV Card with mobile device
- Near Field Communication ISO/IEC 14443 channel
- Secured transactions between device and card
- **Standardize:** PIV-Card-to-device interface

Pros

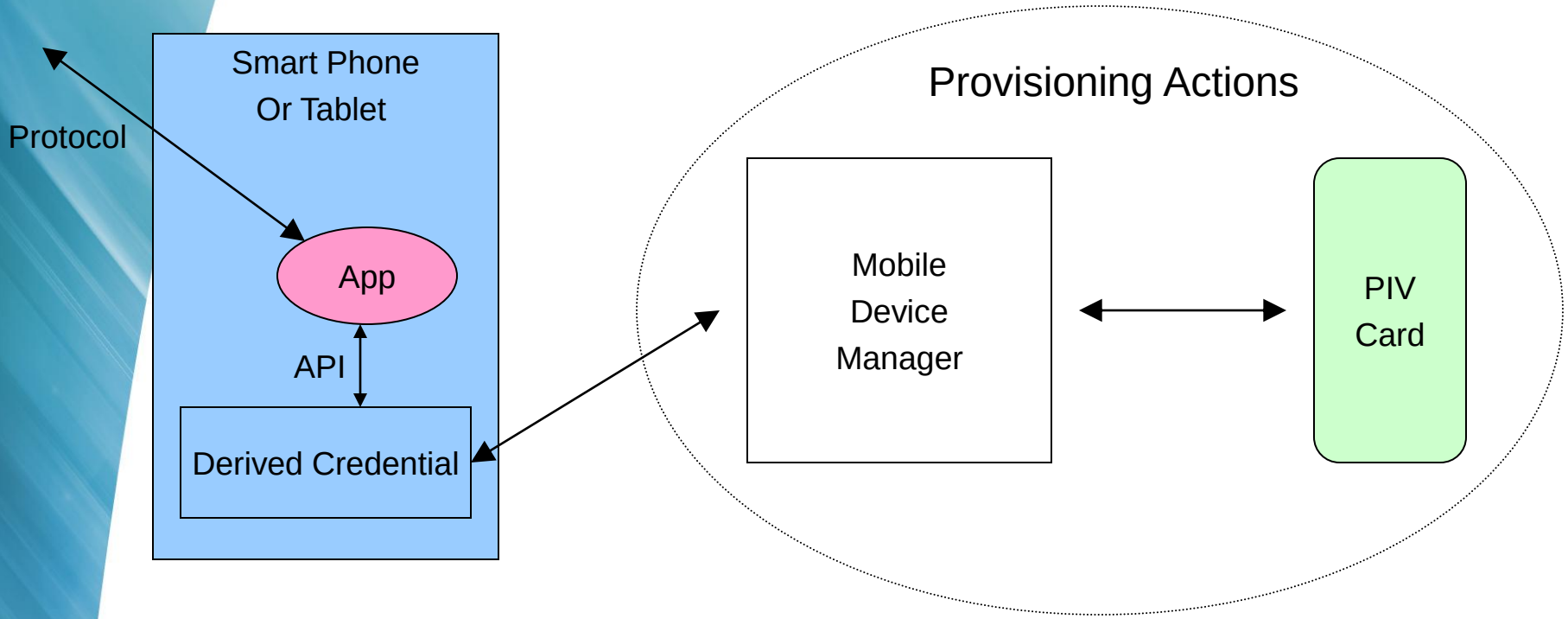
Enhanced PIV Card

- Leverages PIV Card fully
- Has minimal impact on other components
- It is an SL 2+, AAL 4 credential, always

Con

- Requires presence of PIV Card

Derived Credential



- PIV Card authorizes MDM to create derived credential
- New logical credential stored within mobile device
- Maximize reuse of PIV data model & PIV behaviors
- **Standardize:** API and protocol bindings

Pros

Derived Credential

- Integral to mobile, better usability
- Differs as necessary from PIV, e.g.,
  - CAK identifies mobile, is revocable
  - NFC, Bluetooth, Wi-Fi, & other bindings
- Could be SL 1 or 2, AAL 3 or 4 credential

Con

- Integration with MDM adds complexity

Has been done

- SP 800-63-1 added “assertions” and “derived credentials”
- FIPS 201-2 written concept of PIV-derived credentials (& other)

Remains to be done

- FIPS 201-2 revision
- SP 800-73-4 revision (credential & mw)
  - Derived Credential Profiles
- SP 800-76-2 revision (biometrics)
- SP 800-79-2 revision (PCI assessment)
  - SP 800-85A & B, & test tool revisions

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/pages.cfm/page/IDManagement-HSPD12-frequently-asked-questions **- HSPD-12 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.