2004: Homeland Security
Presidential Directive #12
HSPD-12 set the goal for FIPS 201, the Personal Identity Verification (PIV) Standard:

“Subject: Policy for a Common Identification Standard for Federal Employees and Contractors” …..
“…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…”
2005: FIPS 201
A Smart Card based Solution

- **HSPD-12**: for “…. physical access to Federally controlled facilities and logical access to Federally controlled information systems”
  
  - A portable solution for both environment:
    - "tab and go" for physical access to federal facilities
    - logical access to IT resources via laptop / desktop and their applications / web services.

FIPS 201-1:
A Smart Card based Solution

- **HSPD-12**: “….graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application.”

  - A solution for multi-factor Authentication that
  - accommodates several credentials for LoA 2 to LoA4
FIPS 201-1: A Smart Card based Solution

- **HSPD-12**: “…. secure forms of Identification”
  - Security Level (SL) 2 -- FIPS 140-2 Level 2

- **HSPD-12**: “…. resistant to… tampering”
  - In addition to SL 2, SL 3 physical security is needed

FIPS 201 History and Projection

- **Logical Access**: A move from ‘stationary’ desktop/laptop environment to mobile ‘anytime and anywhere’ federal workforce. (smart phones, tablets ….)
- **Physical Access**: Less significant changes
Standard Strategy Goals

- Continue to satisfy HSPD-12 and OMB-11-11 guidance
- Leverage Federal PIV identities with smart phones, tablets and other mobile devices for Logical Access
- 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*

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

- Leverages PIV Card fully
- Has minimal impact on other components
- It is an SL 2+, LoA 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

Features / Options

Derived Credential

- Integral to mobile, better usability
- Differs as necessary from PIV, e.g.,
  - PIV Derived CAK identifies mobile, is revocable
- Could be SL 1 with up to LoA 3 credential
  - When embedded as a ‘credential store/container
- Could be SL 2 with up to LoA 4 credential
  - If implemented as a hard token (SIM, MicroSD)
Has been done

- SP 800-63-1 added “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 800-79-2 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://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.

Questions?

Thank you!

Hildegard Ferraiolo
hferraio@nist.gov