PAIIWG++
Meeting #1

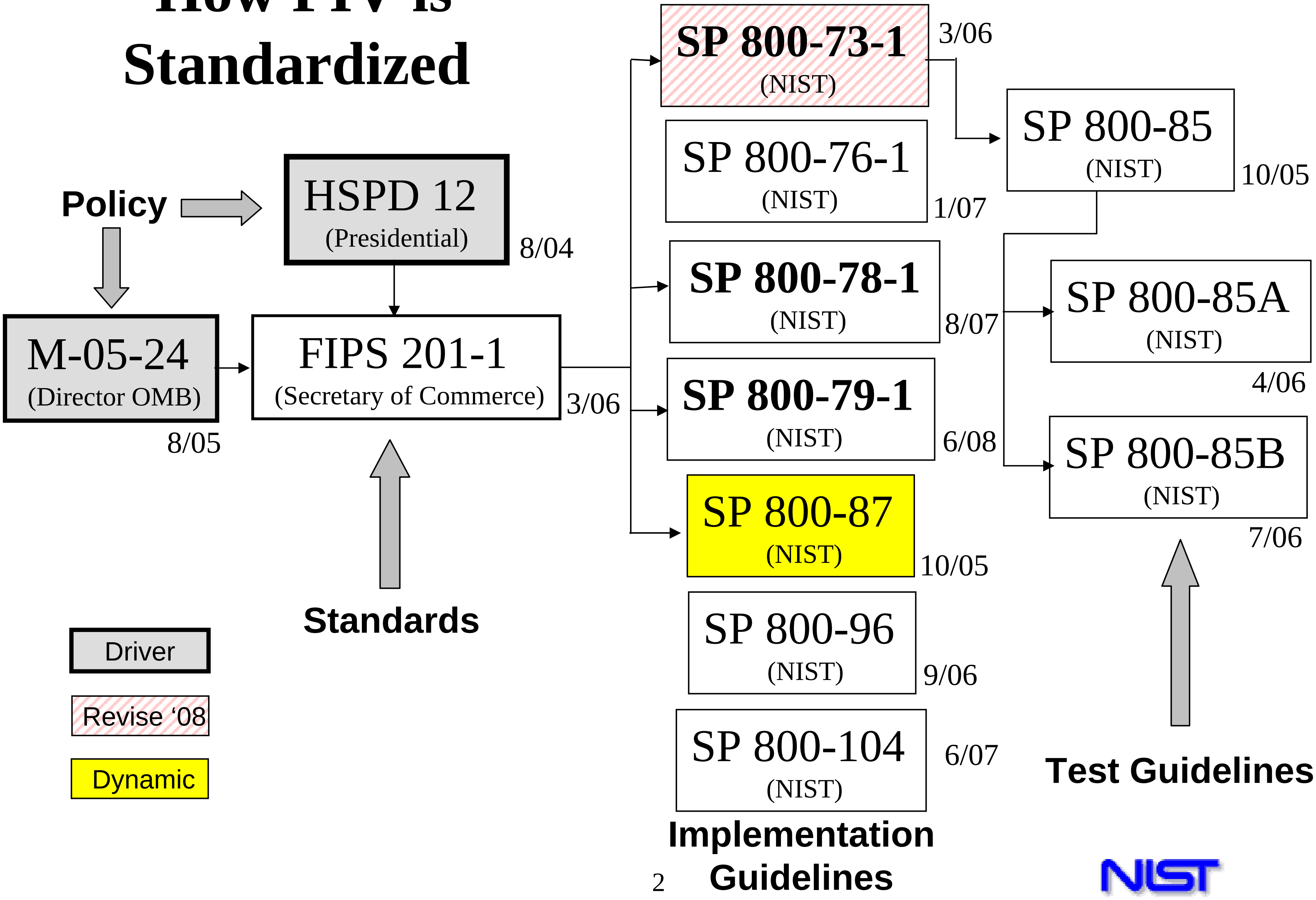
William I. MacGregor

william.macgregor@nist.gov

National Institute of Standards and Technology

16 Sep 2008

How PIV is Standardized



Policy

HSPD 12
(Presidential)
8/04

M-05-24
(Director OMB)
8/05

FIPS 201-1
(Secretary of Commerce)
3/06

Standards

SP 800-73-1
(NIST)
3/06

SP 800-76-1
(NIST)
1/07

SP 800-78-1
(NIST)
8/07

SP 800-79-1
(NIST)
6/08

SP 800-87
(NIST)
10/05

SP 800-96
(NIST)
9/06

SP 800-104
(NIST)
6/07

Implementation Guidelines

SP 800-85
(NIST)
10/05

SP 800-85A
(NIST)
4/06

SP 800-85B
(NIST)
7/06

Test Guidelines

Driver

Revise '08

Dynamic

What NIST documents overlap PAIIWG++ concerns?

The answer depends on the recommendations.

Cryptographic Soundness & Card Authentication Key

FIPS 201, SP800-73, SP800-78, SP800-116

SP800-85 (A&B, & test tools), SP800-79, PACS 2.2?

PIV Identifier Model

FIPS 201, SP800-73, SP800-116, SP800-76

SP800-85B, (GSA) BAE, SP800-87? (FPKIPA) CP’s?

These are basic, there are probably others!

Starting Thoughts

Replace the FASC-N, replace its two uses:

- Identifying the credential and cardholder
- Linking five PIV objects together

Leverage existing identifier schemes

- FASC-N, UEID, IPv6, EUI, OpenID, OID, UUID,…

Utilize familiar, standard representations

- E.g., ASN.1 with BER-TLV encoding

Allow fixed & variable length identifiers

- Fixed: FASC-N, IPv6; Variable: OpenID, OID

An Identity Domain Registry?

A *Registry* is a published, numbered list of entries.

If each entry names an Identity Domain, then…

…(entryNumber, domainIdentifier) is unique.

Example:

(34.4.117.10.1, <a 25 byte FASC-N>)

If the Domains are large (e.g., “IPv6”, “OpenID”), the registry will be small & change infrequently.

Each entry includes its governing authority.