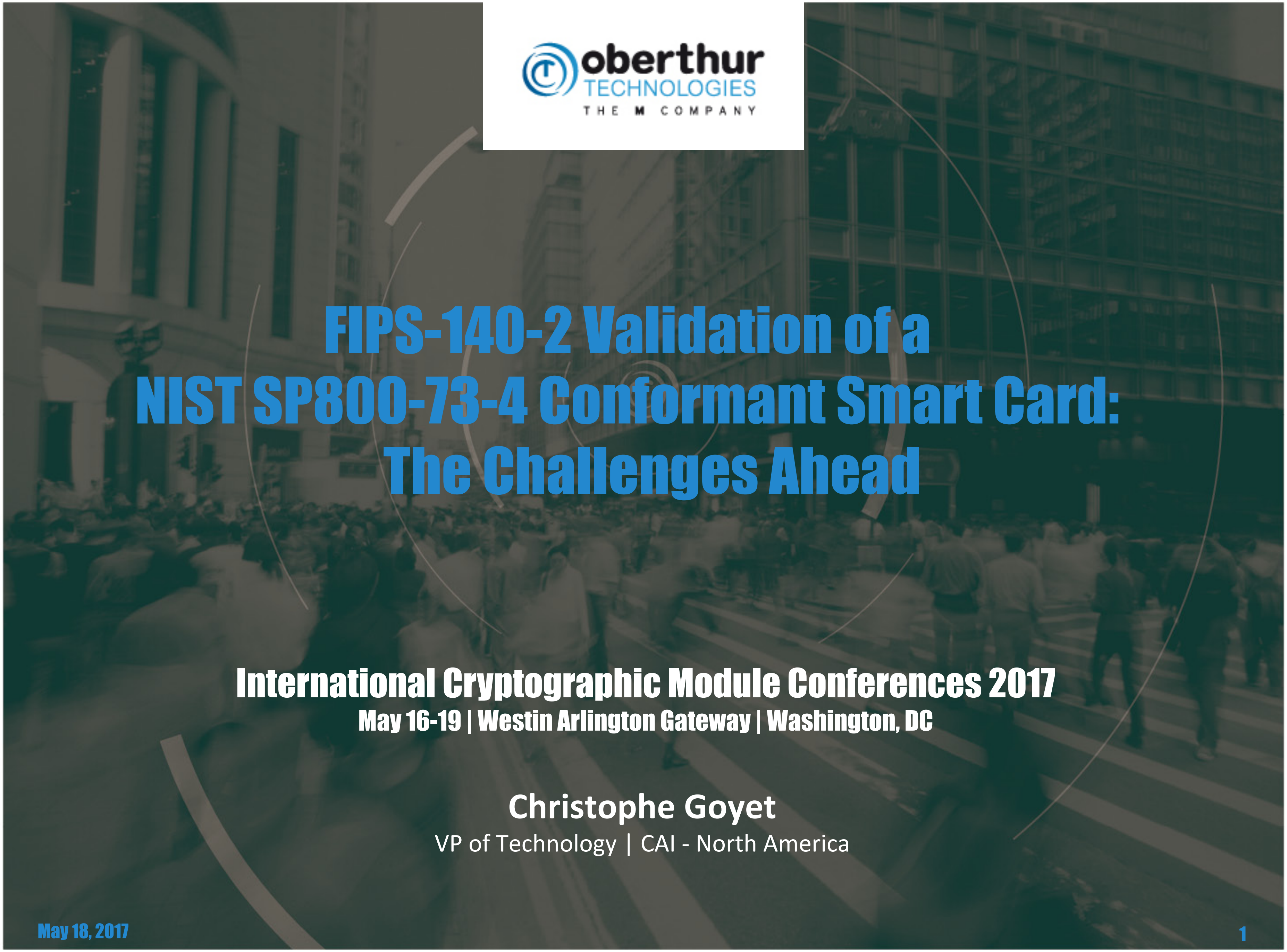


FIPS-140-2 Validation of a NIST SP800-73-4 Conformant Smart Card: The Challenges Ahead

International Cryptographic Module Conferences 2017

May 16-19 | Westin Arlington Gateway | Washington, DC

Christophe Goyet

VP of Technology | CAI - North America

Definitions

- FIPS 140-2
- SP 800-73-4

HSPD#12

- Policy for a Common Identification Standard for Federal Employees and Contractors (Whitehouse 2004).

- General Objectives
  - Common, secure, reliable identification for government employees and contractors
  - Visual and electronic identity verification
  - Government-wide technical interoperability

- Department of Commerce and National Institute of Standards and Technology (NIST) tasked to prepare the standard

Federal Information Processing Standard Publication 201

- **Personal Identity Verification (PIV) of Federal Employees and Contractors**

- FIPS 201 defines the identity vetting, enrollment, and issuance requirements for a common identity credential and the technical specifications for an interoperable government employee and contractor ID card - the PIV card.
- It is supplemented by a series of Special Publications

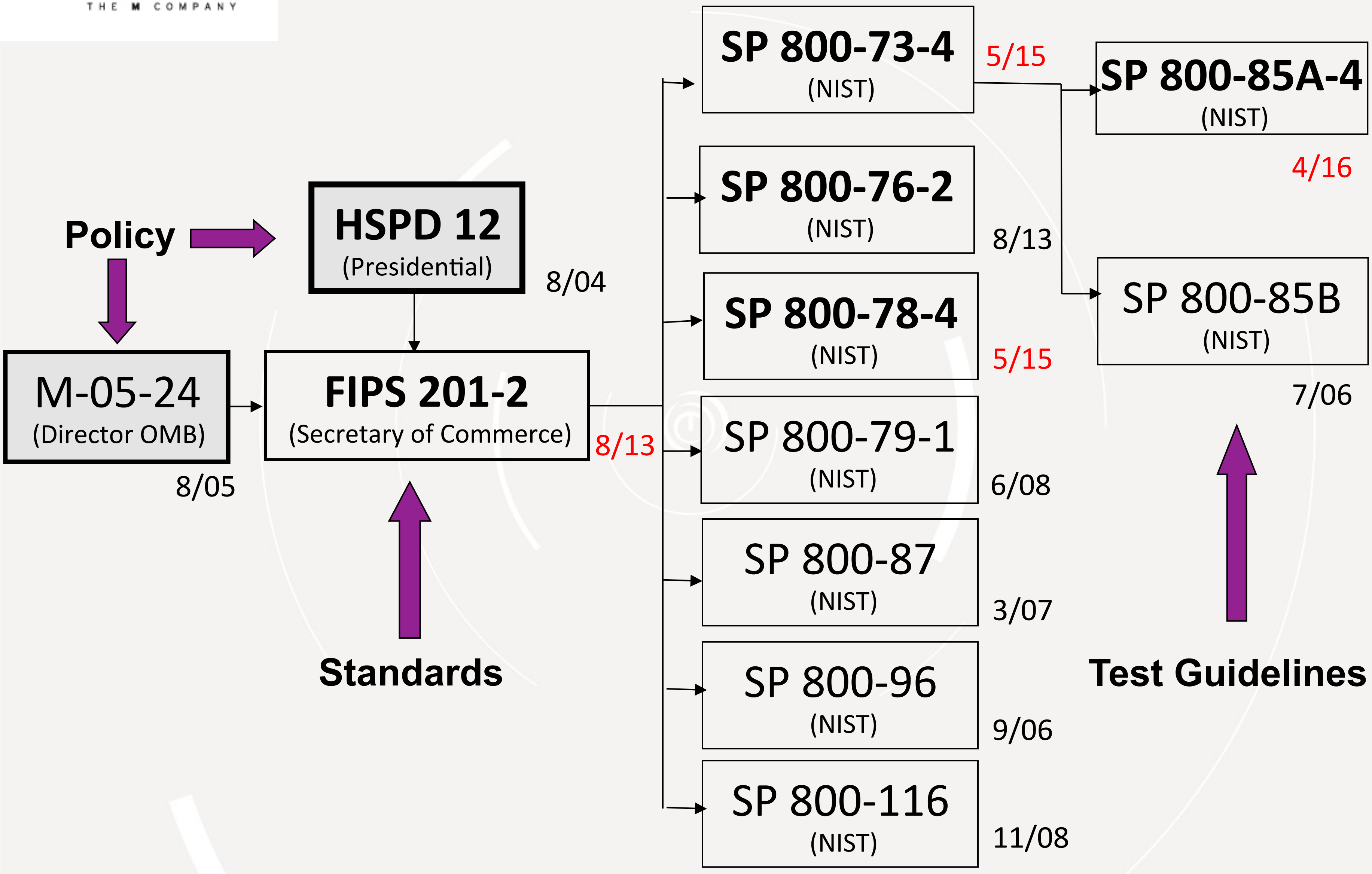
- Public Specifications freely available to benefit other sectors
  - Corporate (US and Worldwide)
  - Government (Worldwide)

Associated Special Publications

- **SP800-73**, Interfaces for Personal Identity Verification
  - Specifies the interfaces and card architecture for storing and retrieving identity credentials from a smart card
- **SP800-76**, Biometric Specifications for Personal Identity Verification
  - Specifies the interfaces and data formats of biometric information
- **SP800-78**, Cryptographic Algorithms and Key Sizes for Personal Identity Verification
  - Specifies the requirements for cryptographic algorithms

- SP800-79, Guidelines for the Accreditation of Personal Identity Verification Card Issuers
- SP800-87, Codes for the Identification of Federal and Federally-Assisted Organizations.
- SP800-96, PIV Card to Reader Interoperability Guidelines
- SP800-156, Representation of PIV Chain-of-Trust for Import and Export
- SP800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials

Current PIV related Specifications



Policy

HSPD 12 (Presidential) 8/04

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

FIPS 201-2 (Secretary of Commerce) 8/13

Standards

SP 800-73-4 (NIST) 5/15

SP 800-76-2 (NIST) 8/13

SP 800-78-4 (NIST) 5/15

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

SP 800-87 (NIST) 3/07

SP 800-96 (NIST) 9/06

SP 800-116 (NIST) 11/08

SP 800-85A-4 (NIST) 4/16

SP 800-85B (NIST) 7/06

Test Guidelines

Implementation Guidelines

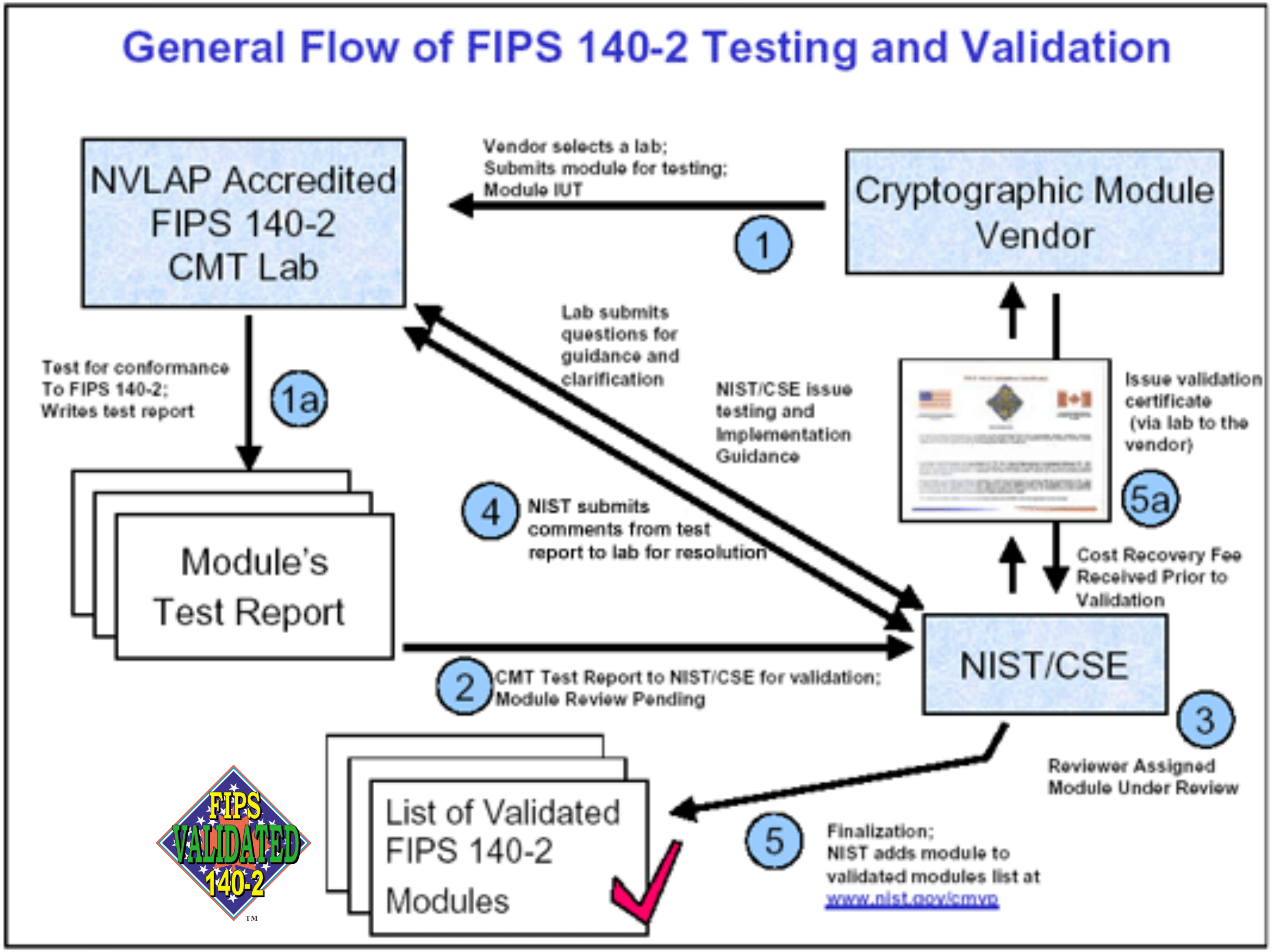
Requirements for "FIPS201 Compliant" label

- The PIV Card Application Interface must have a validation certificate issued by NIST Personal Identity Verification Program (NPIVP)
  - http://csrc.nist.gov/groups/SNS/piv/npivp/

- The associated cryptographic module must be validated for FIPS 140-2 Standard conformance
  - IG 1.18 PIV Reference
    - *"The accompanying FIPS 140-2 validation certificate must reference the NPIVP certificate"*

Timing Challenge

FIPS 140 Validation Process



General Flow of FIPS 140-2 Testing and Validation

NVLAP Accredited FIPS 140-2 CMT Lab

Cryptographic Module Vendor

1 Vendor selects a lab; Submits module for testing; Module IUT

1a Test for conformance To FIPS 140-2; Writes test report

Module's Test Report

Lab submits questions for guidance and clarification

NIST/CSE issue testing and Implementation Guidance

4 NIST submits comments from test report to lab for resolution

2 CMT Test Report to NIST/CSE for validation; Module Review Pending

NIST/CSE

3 Reviewer Assigned Module Under Review

5a Issue validation certificate (via lab to the vendor)

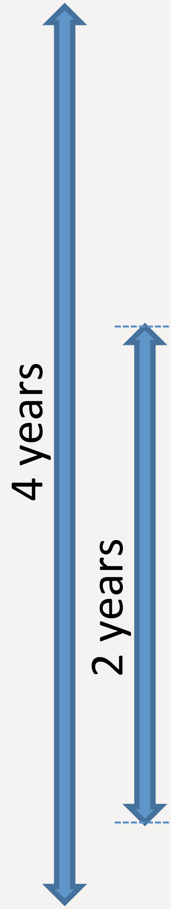
Cost Recovery Fee Received Prior to Validation

5 Finalization; NIST adds module to validated modules list at www.nist.gov/cmvp

List of Validated FIPS 140-2 Modules

NPIVP Validation Process

Timeline



- **August 2013**: FIPS 201-2 Publication
  - Introduces new features for PIV cards (OCC, VCI)
    - Manufacturers develop these new features using draft of SP800-73-4
- **May 2015**: SP800-73-4 Publication
  - Specifies interfaces to support these new features
    - Manufacturers fine-tune implementation to match official release of SP800-73-4
    - MANUFACTURERS READY TO SUBMIT PRODUCT FOR NPIVP VALIDATION
    - NPIVP not ready to accept submissions
- **April 2016**: SP 800-85A-4 Publication
  - Specifies how to test compliance with SP800-73-4
  - But does not provide the NVLABS the SW tool (Test Runner) to validate compliance
    - NPIVP still not ready to accept submissions
- **May 2017 (?)**: First fully functional version of Test Runner released to NVLABS
  - Manufacturers may **finally** submit products for NPIVP validation
- **June 2017 (?)**: NPIVP validation certificate issued by NIST
  - **Manufacturers can now submit products for FIPS 140-2 validation**
- **September 2017 (?)**: FIPS 140-2 validation certificate issued

Technical Challenge:

How to deal with what looks like conflicting specifications between two NIST Special Publications

SP800-73-4 Part 2 NPIVP

v.s.

SP800-56A rev 2 CMVP

Technical Challenge

Conflicting specifications between NPIVP and CMVP

- Doing FIPS 140-2 validation, the NVLAB ran into what appears to be a conflict between SP 800-73-4 Part 2 and SP 800-56A Rev 2.
- Guidance was seek from NIST as to what SP shall prevail
- Iissue brought to both NPIVP and CMVP by the NVLAB in 2014
- Several attempts were made by the NVLAB to get NPIVP and CMVP come to a resolution, but no success
- As of today, still no guidance from NIST.
- This could put on hold the validation and commercial launch of new PIV products
- As a vendor we need a mechanism to get answers from NIST when question asked

Conflict between SP 800-73-4 Part 2 and SP 800-56A rev 2

SP 800-73-4 Part 2

- Table 14 "Cipher Suite for PIV Secure Messaging“ specifies a 192 bit channel strength option (using P-384, SHA-384 and AES-256).
- Section 4.1.1 specifies AES CMAC as the algorithm used for key confirmation in the One-Pass Diffie-Hellman, C(1e, 1s, ECC CDH) scheme.
  - See Step H13, bottom of page 23

SP 800-56A rev 2

- Section 5.9.3 states (page 56, the last sentence above Section 6):
  - " ... however, **AES CMAC shall not be used** for domain parameter sets ED and EE, because the maximum length of the MacTag that an AES CMAC can generate is only 128 bits, the AES output block length.“
  - Domain parameter set ED is the 192-bit strength option.

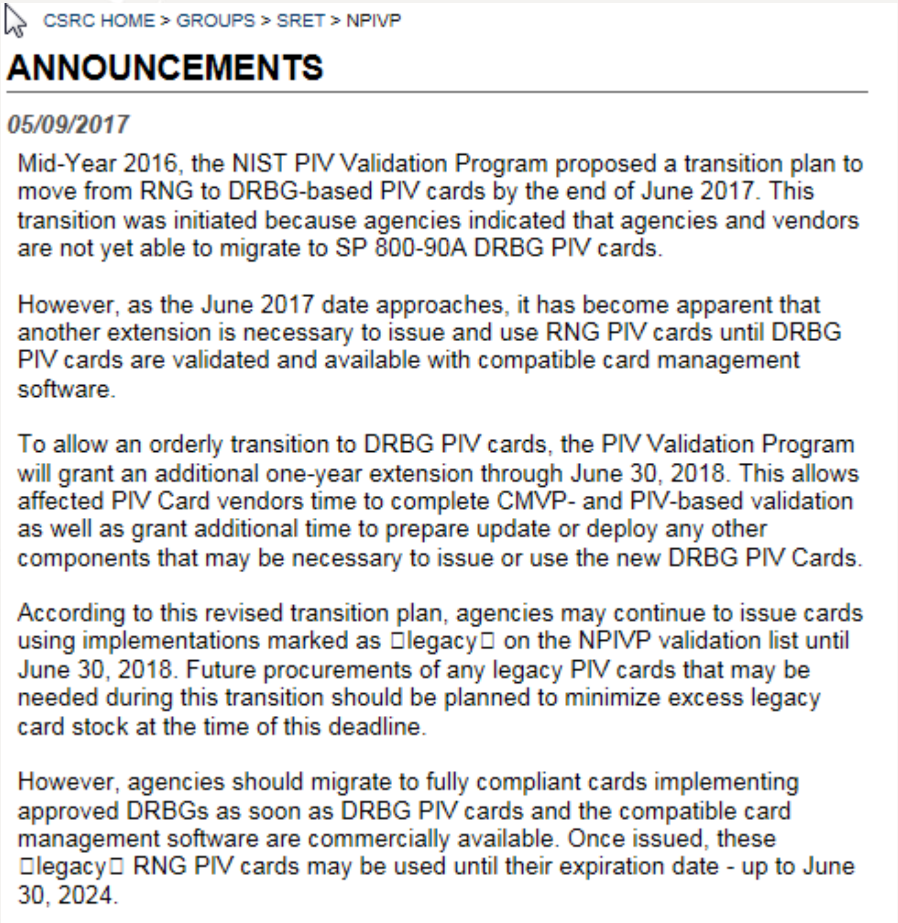
➡ the 192 bit strength option in Table 14 is not approvable in combination with the use of key confirmation using AES CMAC.

- Should AES CMAC be replaced with AES HMAC for 192-bit strength option ?

Consequences of these Challenges

Delay in compliance with SP 800-131A re sunset of cryptographic algorithms

- Cards that have been moved in Jan 2016 to the “legacy” category by CMVP can still be issued till June 2018 and used up to June 30, 2024 according to NPIVP.
  - http://csrc.nist.gov/groups/SNS/piv/npivp/announcements.html



CSRC HOME > GROUPS > SRET > NPIVP

ANNOUNCEMENTS

05/09/2017

Mid-Year 2016, the NIST PIV Validation Program proposed a transition plan to move from RNG to DRBG-based PIV cards by the end of June 2017. This transition was initiated because agencies indicated that agencies and vendors are not yet able to migrate to SP 800-90A DRBG PIV cards.

However, as the June 2017 date approaches, it has become apparent that another extension is necessary to issue and use RNG PIV cards until DRBG PIV cards are validated and available with compatible card management software.

To allow an orderly transition to DRBG PIV cards, the PIV Validation Program will grant an additional one-year extension through June 30, 2018. This allows affected PIV Card vendors time to complete CMVP- and PIV-based validation as well as grant additional time to prepare update or deploy any other components that may be necessary to issue or use the new DRBG PIV Cards.

According to this revised transition plan, agencies may continue to issue cards using implementations marked as □legacy□ on the NPIVP validation list until June 30, 2018. Future procurements of any legacy PIV cards that may be needed during this transition should be planned to minimize excess legacy card stock at the time of this deadline.

However, agencies should migrate to fully compliant cards implementing approved DRBGs as soon as DRBG PIV cards and the compatible card management software are commercially available. Once issued, these □legacy□ RNG PIV cards may be used until their expiration date - up to June 30, 2024.

Consequences of these Challenges

Economic and Security Impacts

- **Economic** Impact for vendors
  - New products, faster and more secure available since the new standard publication, cannot be sold and stay on shelves for 4 years waiting for a validation certificate.
- **Security** Impact for the industry
  - By extending the authorized use of older generation products that do not comply with NIST SP 800-131 from December 31st 2015 till June 30th 2024, we significantly increase our vulnerability to cyber attacks.

Were the benefits that CMVP sought when publishing

IG 11.8

really worth such Security risk ?