FIPS 201 Evaluation Program

NIST Industry Day

3/2/3015

FIPS 201 Evaluation Program introduction

- Thanks for attending

- Objectives
  - Brief you on the Program
  - Discuss several key elements of the program

Agenda

- APL Vision
- APL Overview
- GEN2 Cards and PKI
- APL Growth
- A look Ahead
- Summary

APL Vision

Mission Statement

> *“Make the Approved Product List (APL) so valuable that no agency would consider doing procurement without referencing the APL, and no vendor would consider a product without factoring in the APL”*

Program Value for Stakeholders

Government	Reduces duplication of effort across agencies by having a unified testing program.
Agencies	Radically simplifies product selection and requirements definition.
ICAM SC	Reduces burden on agencies deploying ICAM capabilities.
General Service Administration (GSA)	Shows GSA commitment to supporting government-wide policy efforts and providing tools / capabilities to support agency procurement efforts.
Vendor/Industry	Creates a dynamic market and competitive advantage for vendors that participate on the APL.

Agenda

- ✓ APL Vision
- ➢ APL Overview
- Gen2 Cards and PKI
- APL Growth
- A look Ahead
- Summary

FIPS 201 Evaluation Program

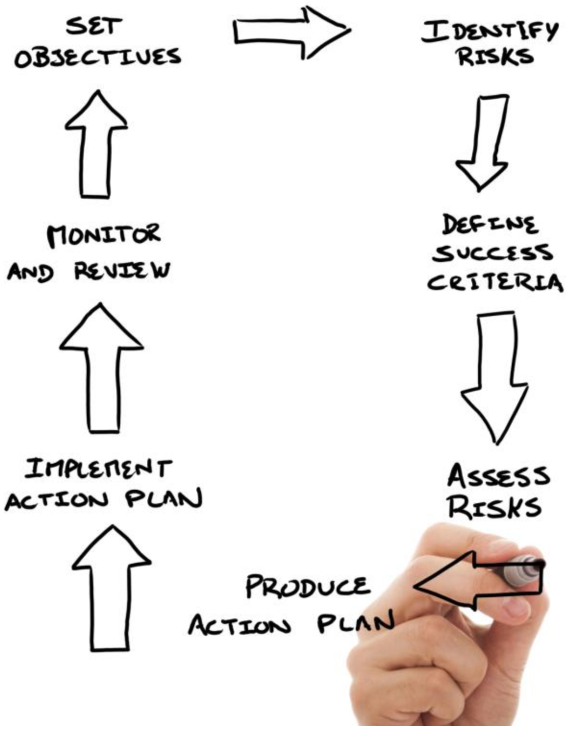
- FIPS 201 Evaluation Program (EP) operates a testing program for HSPD-12 related requirements
- The Approved Products List (APL) is the official list of products that have passed applicable Program testing
- The goal of the FIPS 201 EP is to help industry understand federal requirements
- The goal of the APL is to help agencies find conformant products
- In October 2012, an effort was launched to improve the FIPS 201 EP (e.g., improved testing, better support)

Many Benefits to Stakeholders

- Helps agencies implement systems and solutions that meet applicable standards, policies, and mandates
- Provides great value to both industry and government
  - Ensures reliable technical interoperability/integration
  - Ensures adequate level of security
  - Enhances/expedites government procurement process
  - Saves agencies the time/cost/complexity of testing products for compliance
  - Facilitates product availability and choice to the government
  - Provides vendors clear requirements/process so they know how to implement and test their products to be available to far more federal agencies

Methodology and Objectives

- Partnership approach
- Leverage lessons-learned from the first implementation
- Well-defined, incremental changes organized into “Spirals”
- Coordination with the EP Technical Working Group (EPTWG)
- Three essential objectives:
  - APL Clarification
  - Test Requirements Clarification/Refinement
  - Process Improvement

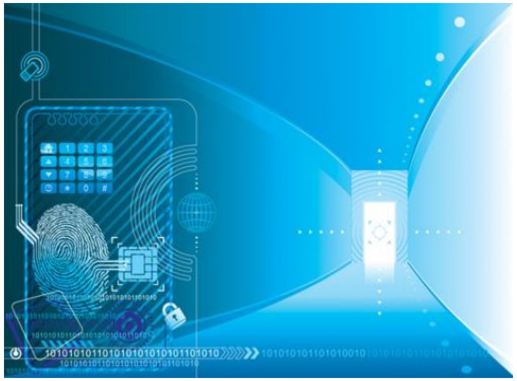


Key Policy Drivers

- Homeland Security Presidential Directive 12 (HSPD-12)
  - Requires mandatory Government-wide standard for secure and reliable forms of identification for Federal employees and contractors (i.e., FIPS 201, PIV Cards).
- OMB Memorandum M-05-24
  - GSA designated as “executive agent for Government-wide acquisitions of information technology" for products/services required for implementing HSPD-12.
- OMB Memorandum M-06-18
  - Directs that agencies must acquire products and services that are approved as compliant with Federal policy, standards and supporting technical specifications in order to ensure government-wide interoperability.
- OMB Memorandum M-11-11
  - Requires continued Implementation of HSPD-12.
- FICAM Roadmap and Implementation Guidance
  - Support of the ICAM mission to provide a common segment architecture and implementation guidance for use by federal agencies as they continue to invest in ICAM programs.
- NIST Special Publication 800-53:
  - IA-5(15) The organization uses only FICAM-approved path discovery and validation products and services.
  - IA-8(3) The organization employs only FICAM-approved information system components in [Assignment: organization defined information systems to accept third-party credentials.
  - SA-4(10) The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems

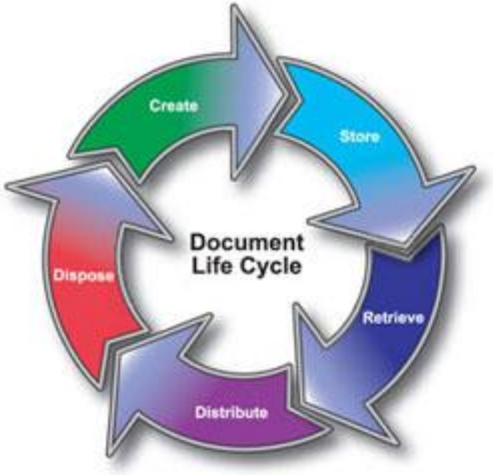
Functional Requirements and Test Cases (FRTC)

- Original FRTC 1.20 released 10/25/13
  - 251 Test Cases
  - 2 Topologies
- Released FRTC Draft v1.3.0 on 06/13/14
  - FRTC Draft v1.3.0 is not yet operational
- FRTC v1.3.0 Final
  - Will be the next release used for operational testing
  - Industry comments received have been incorporated
  - Incorporated all changes in Draft v1.3.0
  - Incorporated Mobile Handheld requirements
    - Added 110 test cases to support MHH



FRTC Change Process

- Now a ***one year cycle*** to better line up with vendor engineering and product schedules
  - Still can publish if significant security or infrastructure risks are identified
  - Added Severity Levels
    - Not all test cases represent critical risks to the Federal infrastructure
    - Compliance on an individual test case basis is now tied to a severity level
    - Products that fail to comply within the time limit will be moved to the Removed Products List (RPL)



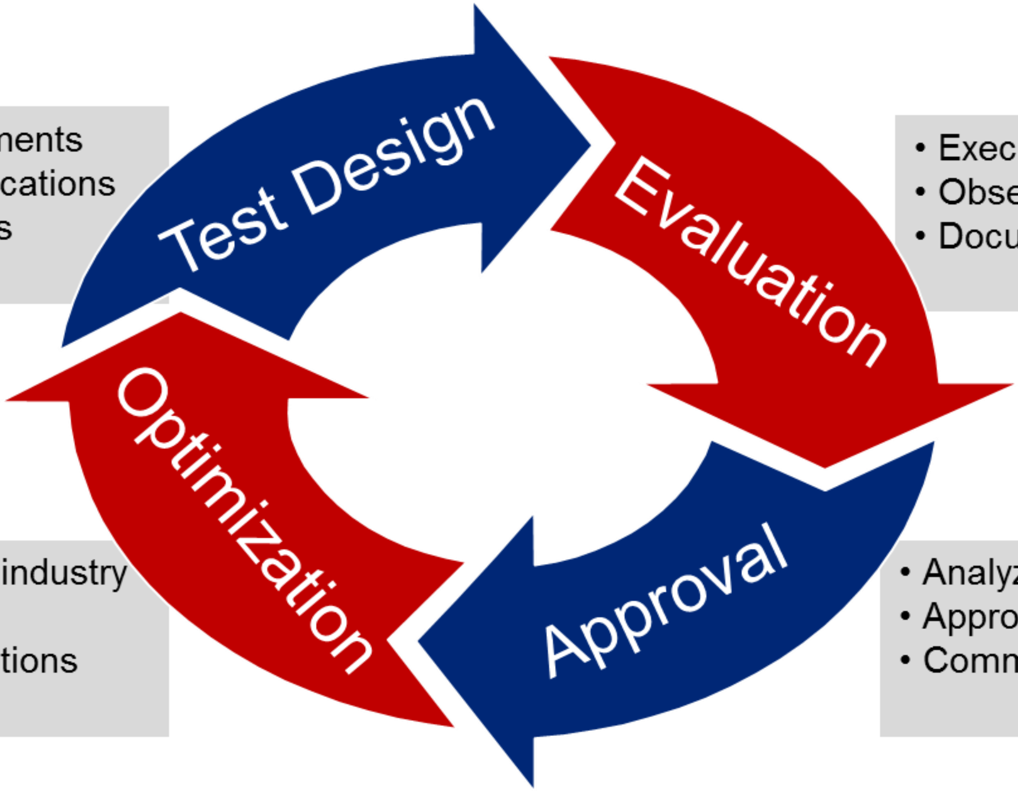
Vendor Input Has Been Key

A Few Milestones Accomplished in Just the Past 18 Months

- PACS Testing
  - ICAM Lab for advanced testing
  - Functional Requirements & Test Cases (251)
  - PIV, PIV-I, and CAC integrated
- 23 Gen 1 ICAM Cards
- Support for multiple topologies
- Variability reduction analysis
- Buyer’s Agent / Procurement Guidance
- Product Series Testing (PST)
- Added / Deprecated APL Categories
- Industry stakeholder relationships
- SAML Test Requirements (123) & Testing
- Mobile Initiatives Effort
- LACS Survey
- PACS Integrator Training
- PIV in E-PACS Published

- Several Significant FRTC Updates
- Type B Cards Deprecated
- Transparent Readers Deprecated
- Removed Products List
- Coordination with NIST 73-4, 157, 166
- SAML 2.0 Metadata Profile
- 64/128 Bit Transition
- Gen 2 ICAM Cards
- PKITS Analysis
- Established FICAM TFS Lab
- Leveraged federal PKI Test Environment
- PACS Implementation Lessons Learned
- PKI Copy & Paste Tool
- Card Dumper Tool

FIPS 201 EP in a Nutshell



- Create test requirements
- Develop test specifications
- Determine test types
- Define roles

- Execute test procedures
- Observe tests
- Document results

- Analyze test reports
- Approve products
- Communicate with vendors

- Collect agency and industry feedback
- Adopt recommendations
- Maintain program

Continuous Improvement
("Spirals")

Agenda

- ✓ APL Vision
- ✓ APL Overview
- ➢ APL Growth
- Gen2 Cards and PKI
- A look Ahead
- Summary

PACS APL

- Test Infrastructure:
  - 251Test Cases
  - Gen1 ICAM Test Cards
  - 2 Topologies adopted
- PACS APL: 16 End-to-End PACS Solutions Approved
  - 320 operationalized configurations (Product Series Testing)
  - 16 different PACS vendors represented (6 more in queue to be tested)
  - 20 readers approved

Agenda

- ✓ Introductions
- ✓ APL Vision
- ✓ APL Overview
- ✓ APL Growth
- ➢ Gen2 Cards and PKI
- ▪ A look Ahead
- ▪ Summary

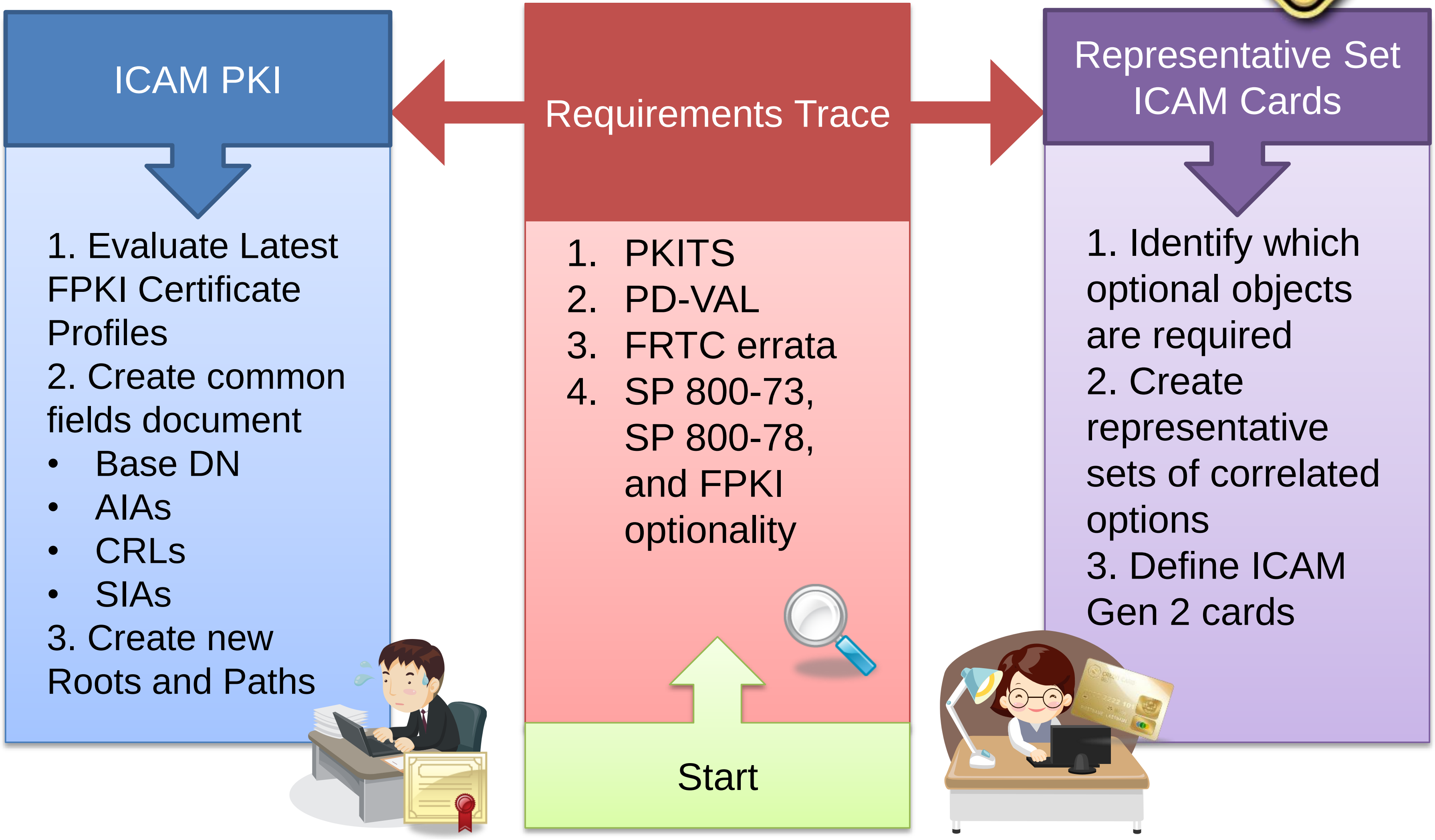
Gen2 Cards: Why Gen2 & PKI?

- ICAM Gen1 focused on invalid conditions
  - Each has an injected security fault
  - ICAM Test Cards (23)
  - ICAM PKI Paths (40)
- Vendors pointed out the high number of possible variations
  - There are over 5.5 million valid cards currently issued
- Can lead to failures in operational environment
  - Variations must be supported by interoperable systems and components

Gen2 Cards: Objectives

- Gen2 is focused on ***valid*** variations – one stop shop
  - Cards
  - PKI end-entity certificates and certificate paths to roots
  - Both PACS and LACS were considered
- Introduce the concept of “Representative Sets” for cards
- Incorporating NIST PKITS into ICAM PKI

Gen2 Cards: Process



ICAM PKI

1. Evaluate Latest FPKI Certificate Profiles
2. Create common fields document
   - Base DN
   - AIAs
   - CRLs
   - SIAs
3. Create new Roots and Paths

Requirements Trace

1. PKITS
2. PD-VAL
3. FRTC errata
4. SP 800-73, SP 800-78, and FPKI optionality

Start

Representative Set ICAM Cards

1. Identify which optional objects are required
2. Create representative sets of correlated options
3. Define ICAM Gen 2 cards

GEN2 Sample Card Table & Descriptions

Card #	Description	Test
25	FASC-N: AC||SC||C#||CS||ICI all have valid data; PI||OC||OI||POA are all zeros. GUID coded as all zeros (0x00)	Standard PIV Cred #s
26	FASC-N: AC||SC||C# coded as all 9's; CS||ICI||PI||OC||OI||POA are all zeros GUID is the UUID	Standard PIV-I Cred #s
29	PKI-AUTH Cert not present PKI-CAK Cert RSA 2048 SHA-256 present	Missing mandatory PKI-AUTH
30	PKI-AUTH Cert RSA 2048 SHA-256 present PKI-DIGSIG Cert RSA 2048 SHA-256 present PKI-CAK Cert RSA 2048 SHA-256 present	Golden card
32	PKI-AUTH Cert RSA 2048 SHA-256 present PKI-DIGSIG not present PKI-CAK Cert RSA 2048 SHA-256 present	Buffer not present
39	Key History Object present and populated Retired Key 1 Certificate present and populated	Buffers present and populated
49	This card has both the Application PIN and the Global PIN. The Application PIN is set as the primary PIN. A new Security Object to address the new Discovery Object.	Application and Global PINs are present. Application PIN is primary.
50	This card has both the Application PIN and the Global PIN. The Global PIN is set as the primary PIN. [SPH: is this Discovery object tag 0x5F2F is present First byte: 0x60, Second byte: 0x20]	Both PINs present, Global is primary.
56	PKI-AUTH and PKI-CAK end-entity certificates have p-256 keys and the Signing CA has RSA 2048 key.	ECC P-256 mixed path with RSA 2048

Agenda

- ✓ Welcome & Introductions
- ✓ APL Vision
- ✓ APL Overview
- ✓ APL Growth
- ✓ Gen2 Cards and PKI
- ✓ A look Ahead
- ➢ Summary

Look Ahead: High Speed PACS

- Improving PACS speed
- LACS
- Mobile

Agenda

- ✓ Welcome & Introductions
- ✓ APL Vision
- ✓ APL Overview
- ✓ APL Growth
- ✓ Gen2 Cards and PKI
- ✓ A look Ahead
- ➢ Summary

Summary

- The FIPS201 Evaluation Program has a continuing process of evaluating testing needs based on security vulnerabilities and new government standards.

- Shares lessons learned in the lab with other agencies to support field implementations and procurement personnel