

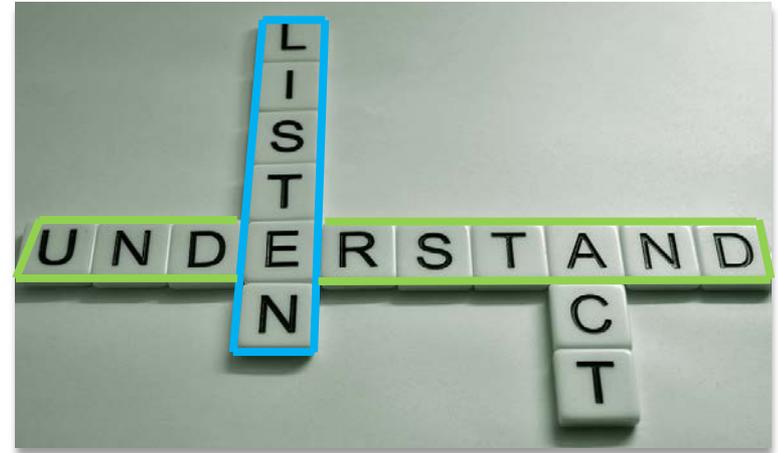
FIPS 201 Evaluation Program & FPKIPA

MA Industry Day
Chi Hickey
3/23/3015

Presentation Objectives

➤ Objectives

- Brief you about two programs and their related key initiatives
 - FIPS 201 Evaluation Program
 - Federal Public Key Infrastructure Policy Authority (FPKIPA Program)



- Overview of the FIPS 201 Evaluation Program
 - APL Vision
 - APL Overview
 - GEN2 Cards and PKI
 - APL Growth
 - A look Ahead
- Overview of the FPKIPA Program
 - About the Program
 - 2015 Docket
- 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.

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)



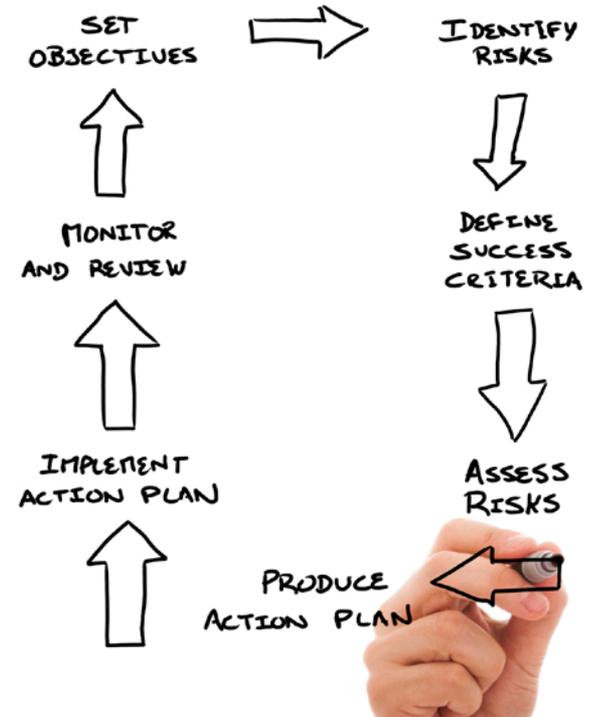
Many Benefits to Stakeholders

- 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

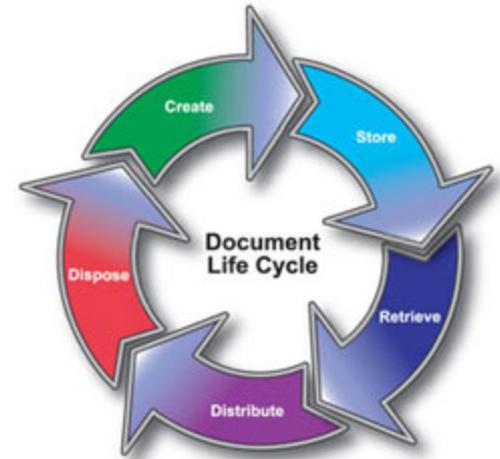
Functional Requirements and Test Cases (FRTC)

- 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)



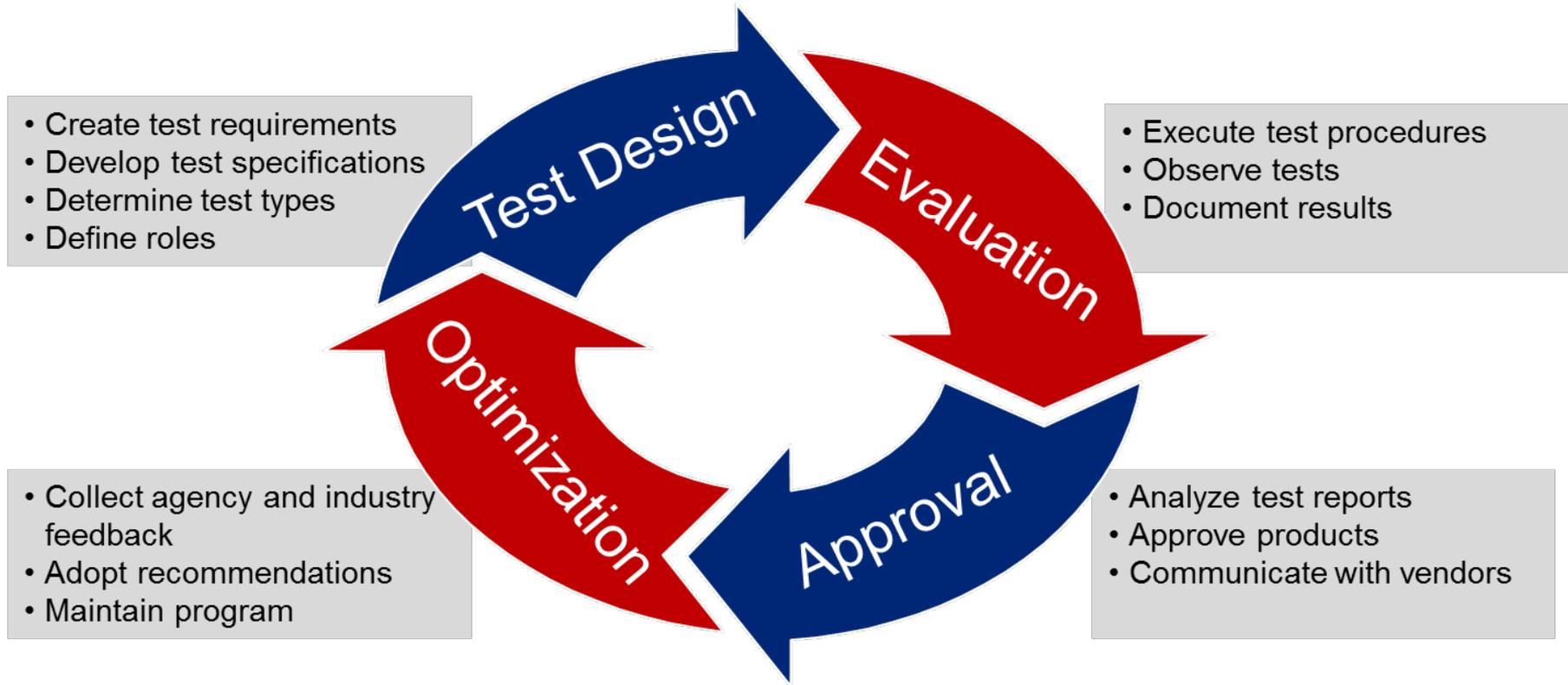
Vendor Input Has Been Key

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



Continuous Improvement
("Spirals")

➤ Test Infrastructure:

- 251 Test 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



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

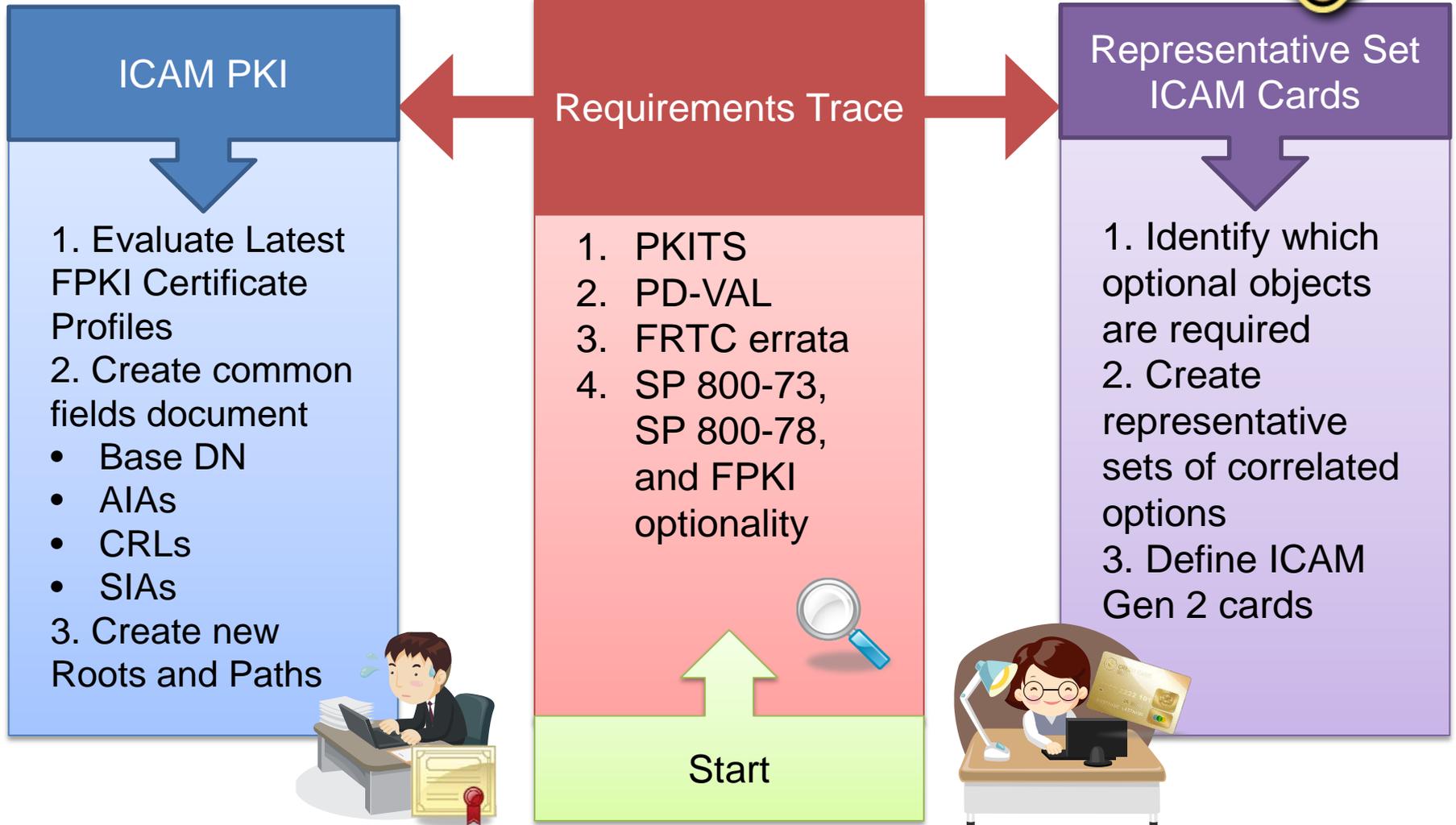


Gen2 Cards: Objectives

- 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





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



Updating Schedule 70

- OMB Memorandum M-05-24
 - GSA will make approved products and services available through BPA under Federal Supply Schedule 70 for IT.
 - Departments and agencies are encouraged to use the acquisition services provided by GSA.
- Other Related OMB Memos: M-06-18, M-11-11
- GSA is updating selected SINs (130-60 - 62) to make it **easier** for government to find and buy **approved** products
- Chief improvements include:
 - Streamlined SIN language
 - Primary qualification is listing on an appropriate approval list
 - e.g., APL, FICAM TFS Approved Identity Services List, Qualified HSPD-12 Service Providers List, Certified Shared Services Providers List
 - Updated procurement guidance for agencies
- Longer-term, will incorporate the use of special indicators

Look Ahead: High Speed PACS

- Improving PACS speed
- LACS
- Mobile



- Overview of the FIPS 201 Evaluation Program
 - APL Vision
 - APL Overview
 - GEN2 Cards and PKI
 - Updated SINS (Schedule 70 & 84)
 - A look Ahead
- Overview of the FPKIPA Program
 - About the Program
 - 2015 Docket
- Summary



➤ The FPKIPA

- Is an interagency body
- Was established by the Chief Information Officer (CIO) Council
- Governs the Federal PKI including the Federal Government's Trust Anchor and interoperable credentials such as Personal Identity Verification (PIV), PIV-Interoperable (PIV-I), and other government / non-government credentials.



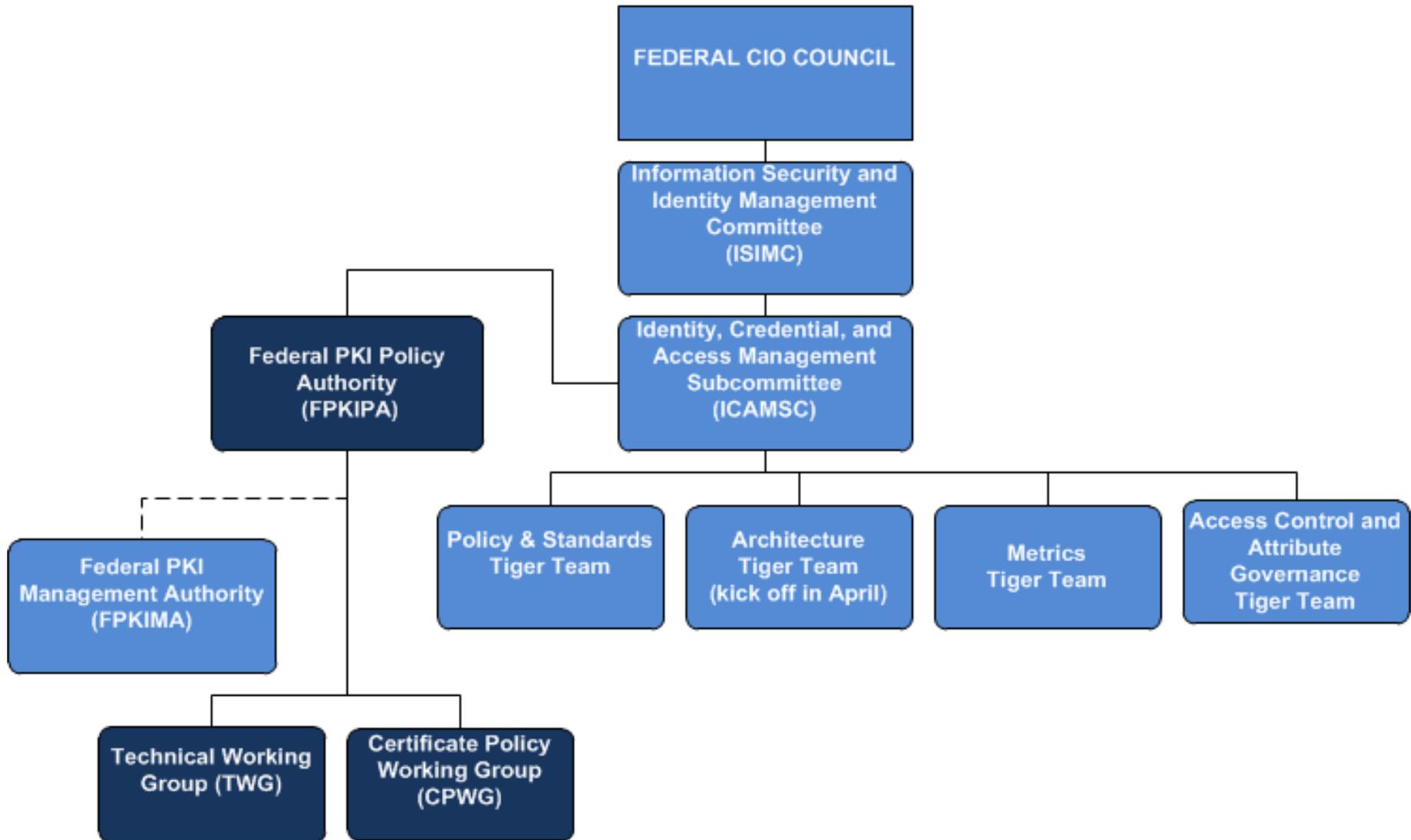
➤ The Federal PKI

- Serves the interest of U.S. Federal Government organizations
- Enables trust of certificate based credentials through standardized policies, profiles, and procedures
- Promotes interoperability between federal and non-federal entities.

- The FPKI facilitates federated identity
 - Throughout the Federal Government; and
 - Between the Federal Government and external partners
- Includes the FPKI Trust Infrastructure
 - Federal Bridge Certificate Authority (FBCA)
 - Cross-certification assures comparability of certificate issuance policies
 - Incorporates multiple assurance levels
 - Federal Common Policy CA (FCPCA)
 - Trust Anchor for the U.S. Federal Government
 - E-Governance CAs (EGCA)
 - Supports various ICAM Programs
- The FPKI Policy Authority (FPKIPA) governs policies for operation of the FBCA, FCPCA, and EGCA
 - Operates under the authority of the Federal CIO Council



FPKI Structure



FPKI Structure

Working Group Name	Description
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKI governing body. It is an interagency body that develops digital certificates standards for trusted identity authentication across the federal agencies and outside bodies, such as universities, state and local governments and commercial entities.
Certificate Policy Working Group (CPWG)	Serves as the policy advisory group for the Federal FPKI. Addresses complex technical and policy issues encountered by Affiliates and evolves policy to maintain or enhance robustness of the FPKI trust fabric
FPKI Technical Working Group (FPKI TWG)	Discusses technical issues related to the usability of the PKI and future enhancements to the FPKI are brought to the TWG. It is focused on advancing PKI technology through collaboration, discussion and investigation. The FPKIPA Co-chairs this working group.
Tiger Teams as Needed	For example, the FISMA FPKI Overlay Tiger Team, Documentation Tiger Team.

- The FPKIPA is the policy arm of the Federal PKI
 - Manages policies, profiles, and procedures governing the FPKI
 - Approves applicants for cross certification with the Federal Bridge Certificate Authority (FBCA), including PIV-I issuers
 - Provides oversight for the Certified PKI Shared Service Provide (SSP) Program

- To accomplish these tasks, the FPKIPA has two fulltime working groups:
 - The Certificate Policy Working Group (CPWG)
 - Documentation Tiger Team (DTT)
 - The FPKI Technical Working Group (FPKI TWG)



➤ Federal mandates for implementing e-government and electronic signature technology. For example:

- Government Paperwork Elimination Act of 1998
- E-Sign Act of 2000
- E-Government Act of 2002
- Homeland Security Presidential Directive (HSPD 12)
- OMB Memorandum 04-04
- OMB Memorandum 05-05
- OMB Memorandum 11-11
- OMB VanRoekel Memorandum of October 2011
- NIST SP 800-63
- FIPS 201



➤ Policy Drivers

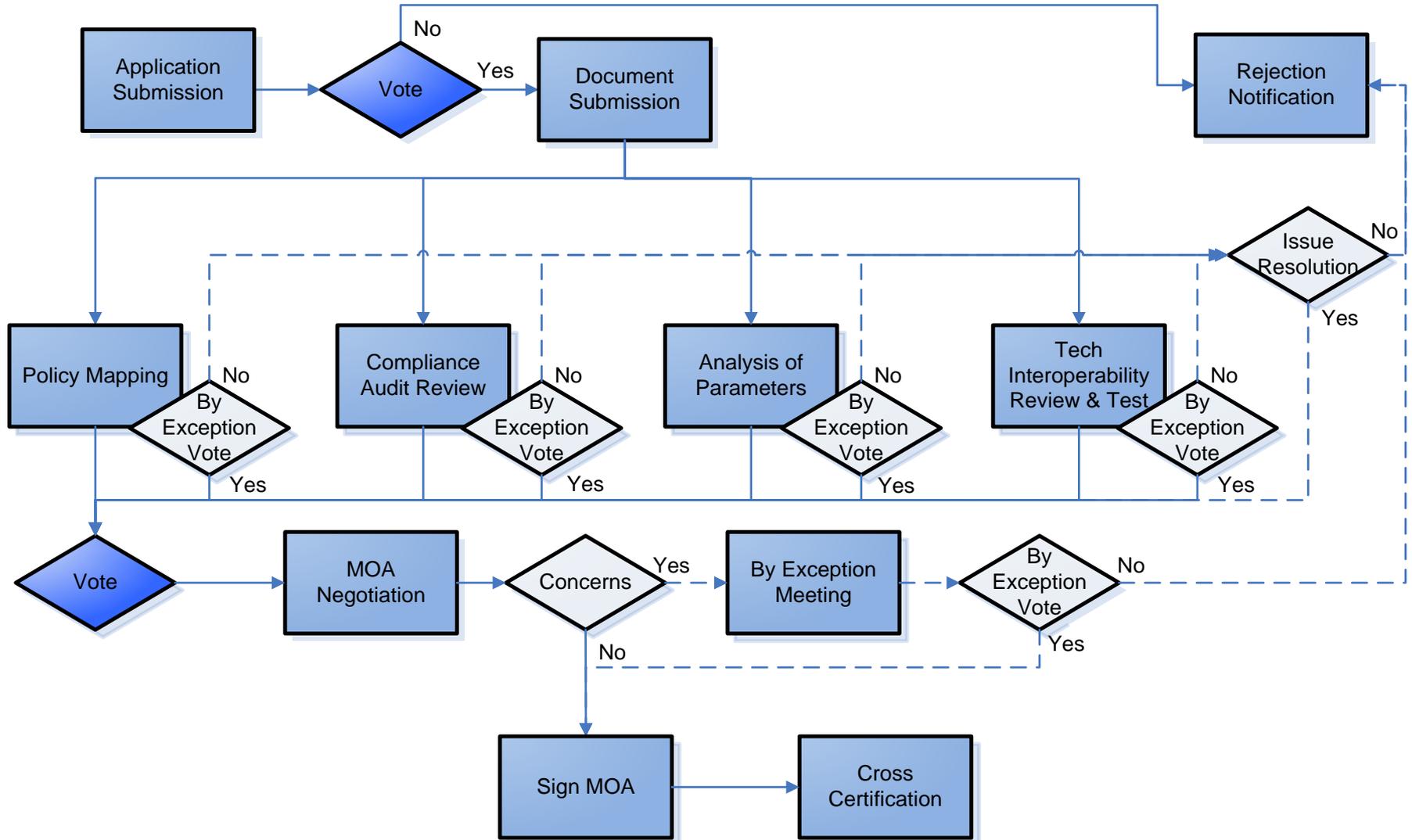
- FISMA
- OMB Circular No. A-130, Appendix III
- Federal PKI Certificate Policies

➤ Security Policies

- GSA IT Security Policy
- FPKIMA FISMA Compliance
- System Security Plan
- FPKI Security Overlay for NIST SP 800-53

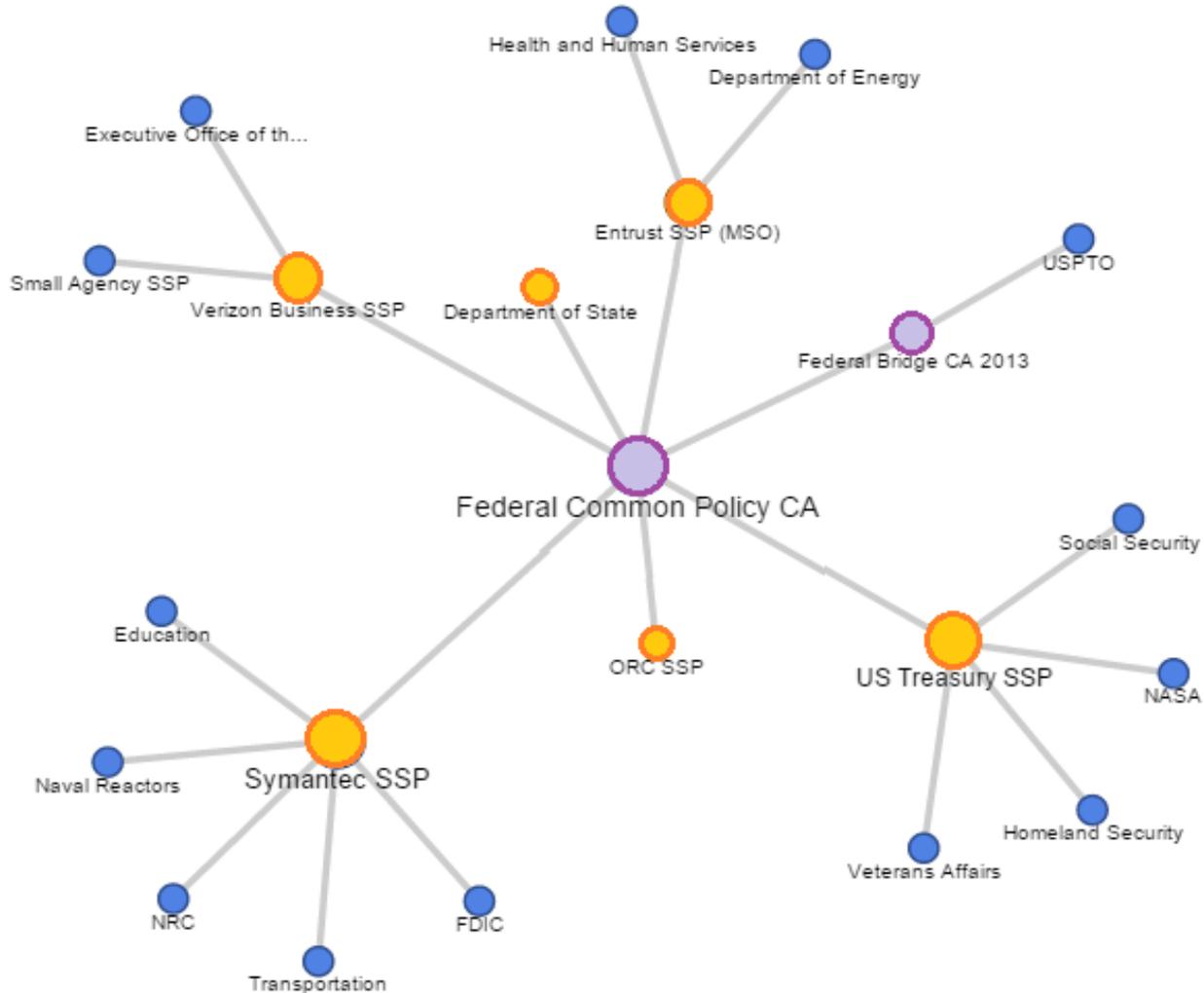


Cross-Certification Process



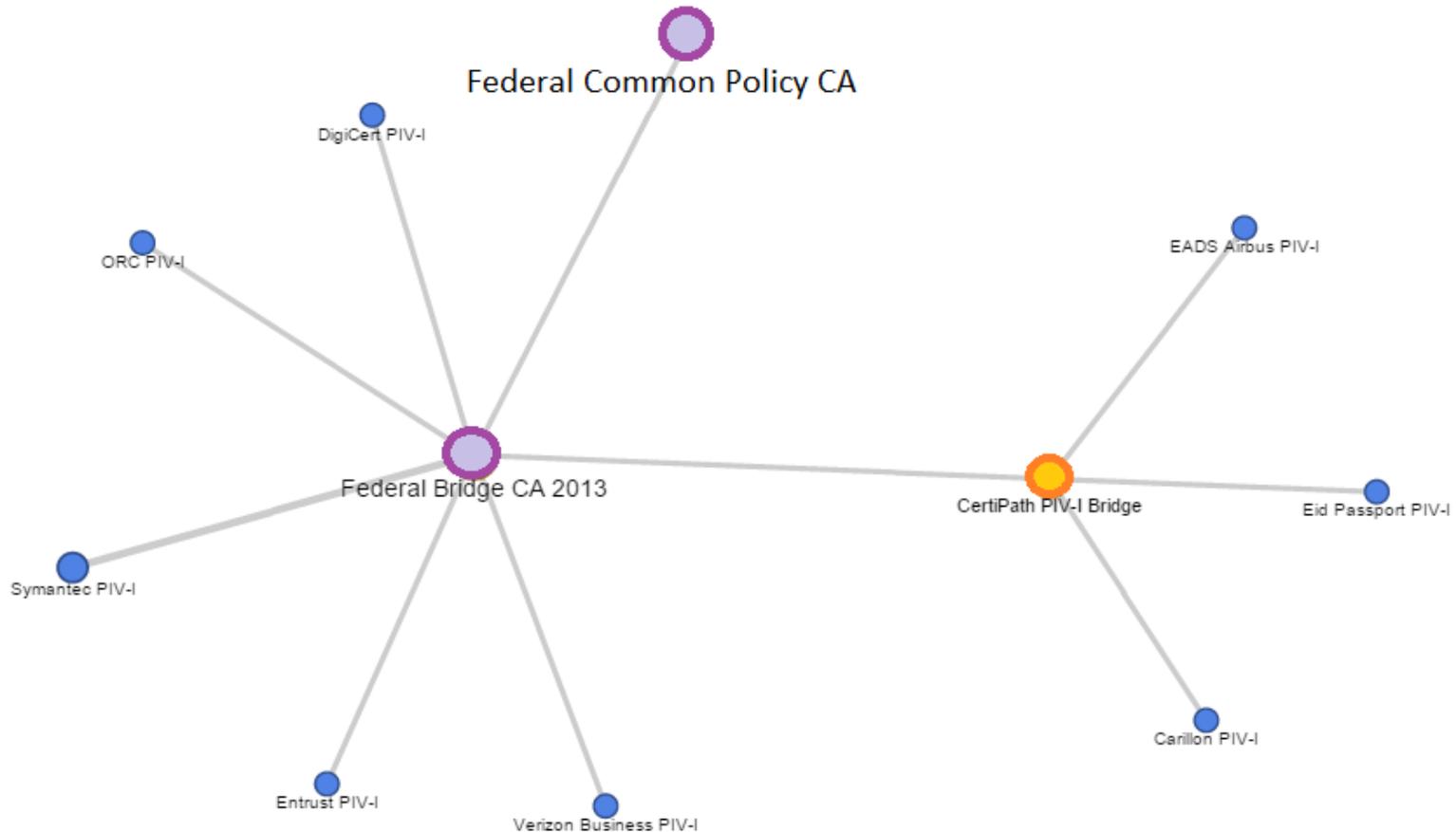
PIV Certification Authorities

- ✓ 17 PIV Issuing CAs
- ✓ 4 Commercial Shared Service Providers



PIV-I Certification Authorities

- ✓ 8 Commercial PIV-I Service Providers
- ✓ 1 Industry Bridge



- *Note: 2 additional bridges pending successful PIV-I card testing of members and FPKIPA approval*

2015 FPKIPA Prioritized Docket (Draft)



PA Focus Area	2015 PA Docket	Related Projects / Initiatives	Q1	Q2	Q3	Q4
Member Management	Affiliate Tracking & Reporting	Review annual audits for all SSP and Affiliates				
		Re-baseline cross-certified members (10 in 2015)				
		Re-baseline CPS of the shared service providers (5 in 2015)				
		Approve new trusted issuers				
		Enhance status reporting dashboards				
		Improve scheduling of Affiliate Compliance reviews				
		Develop metrics to monitor the health and use of the FPKI Trust Fabric				
Policy Management	Policy & Procedures Updates (Bridge, Common, EGCA)	Both Bridge and Common CPs – review and align the bridge and common policy				
		Update EGCA CP				
		Certificate Profiles				
		NIST SP overlays				
		Applicable policies in support of mobile requirements				
	Policy - Criteria and Methodology (Including Noncompliance, Increased Trust New Affiliates)	Criteria and Methodology				
		Clarification on PIV-I testing requirements				
		Update processes to provide more clarity about business case and sponsorship requirements				
		Adding concrete requirements to evaluate the security and business approach of new applicants				
		Consider creating interim approval				
Policy - Audit Guidelines	Audit guidelines					
	Review Audit Scope of Current Members					
Analysis & Issue Response	Respond to technical issues, emerging technology, and new standards	Develop guidance for government NPE certificate use				
		Prepare for transition to ECC algorithm				
		Develop Code Signing Strategy				
Communications & Outreach	Liaise with governmental groups and committees	Report progress to the ICAMSC/CIO Council				
		Better Alignment with CIO Council				
	Communicate with Stakeholders & Credential Users	Create communication aids by developing case studies of the value the FPKI has brought through use of PKI				
		Give strategic, proactive speeches at applicable conferences				
		Participate in the Four Bridges Forum				
		Create a communication plan for active outreach to RPs				
		Improve Idmanagement.gov website to allow for external communications with relying parties				
		Coordinate with NIST, industry, and other standards international organizations				
		Work with industry to promote the inclusion of the FPKI Trust Anchor in commercial trust stores				

2015 Docket – Initiated in Q1

PA Focus Area	2015 PA Docket	Related Projects / Initiatives	Q1	Q2	Q3	Q4
Member Management	Affiliate Tracking & Reporting	Review annual audits for all SSP and Affiliates				
		Re-baseline cross-certified members (10 in 2015)				
		Re-baseline CPS of the shared service providers (5 in 2015)				
		Approve new trusted issuers				
		Enhance status reporting dashboards				
		Improve scheduling of Affiliate Compliance reviews				
		Develop metrics to monitor the health and use of the FPKI Trust Fabric				
Policy Management	Policy & Procedures Updates (Bridge, Common, EGCA)	Both Bridge and Common CPs – review and align the bridge and common policy				
		Update EGCA CP				
		Certificate Profiles				
		NIST SP overlays				
		Applicable policies in support of mobile requirements				
	Policy - Criteria and Methodology (Including Noncompliance, Increased Trust New Affiliates)	Criteria and Methodology				
		Clarification on PIV-I testing requirements				
		Update processes to provide more clarity about business case and sponsorship requirements				
		Adding concrete requirements to evaluate the security and business approach of new applicants				
		Consider creating interim approval				
Policy - Audit Guidelines	Audit guidelines					
	Review Audit Scope of Current Members					
Analysis & Issue Response	Respond to technical issues, emerging technology, and new standards	Develop guidance for government NPE certificate use				
		Prepare for transition to ECC algorithm				
		Develop Code Signing Strategy				
Communications & Outreach	Liaise with governmental groups and committees	Report progress to the ICAMSC/CIO Council				
		Better Alignment with CIO Council				
	Communicate with Stakeholders & Credential Users	Create communication aids by developing case studies of the value the FPKI has brought through use of PKI				
		Give strategic, proactive speeches at applicable conferences				
		Participate in the Four Bridges Forum				
		Create a communication plan for active outreach to RPs				
		Improve Idmanagement.gov website to allow for external communications with relying parties				
		Coordinate with NIST, industry, and other standards international organizations				
		Work with industry to promote the inclusion of the FPKI Trust Anchor in commercial trust stores				

- Qualitative Benefits¹:
 - Trusted interoperability with Federal Agencies
 - Strong digital signature;
 - Support for technical non-repudiation;
 - Strong authentication;
 - Strong Encryption; and
- Quantitative benefits (measured by return on investment):
 - Synergy with HSPD-12 (PIV and PIV-I);
 - Multi-factor authentication;
 - Network security; and
 - PK-enabled applications.

¹ <http://www.idmanagement.gov/sites/default/files/documents/RealizedValueFederalPKI.pdf>

- Overview of the FIPS 201 Evaluation Program
 - APL Vision
 - APL Overview
 - GEN2 Cards and PKI
 - Updated SINs (Schedule 70 & 84)
 - A look Ahead
 - Summary
- Overview of the FPKIPA Program
 - About the Program
 - 2015 Docket
- Summary



Summary

➤ Testing Program:

- 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

➤ FPKIPA:

- The FPKIPA is a core component of the Federal Government's ICAM Initiatives with responsibility for all FPKI Policy management and oversight.
- The FPKI has become even more critical as demand for strong authentication credentials increases within the Government



- Overview of the FIPS 201 Evaluation Program
 - APL Vision
 - APL Overview
 - GEN2 Cards and PKI
 - Updated SINS (Schedule 70 & 84)
 - A look Ahead

- Overview of the FPKIPA Program
 - About the Program
 - 2015 Docket

- Summary

