Federal Public Key Infrastructure (FPKI) Concept of Operations (ConOps)

Version 1.0.0

January 4, 2012

PREPARED BY PROTIVITI GOVERNMENT SERVICES
FOR GENERAL SERVICES ADMINISTRATION

Document History

Version	Date	Revision Details
v1.0.0	1/4/12	Initial publication

Editors

Matt King	Wendy Brown	Dave Silver
Jeff Jarboe		

Table of Contents

Figures

Tables

1 Introduction

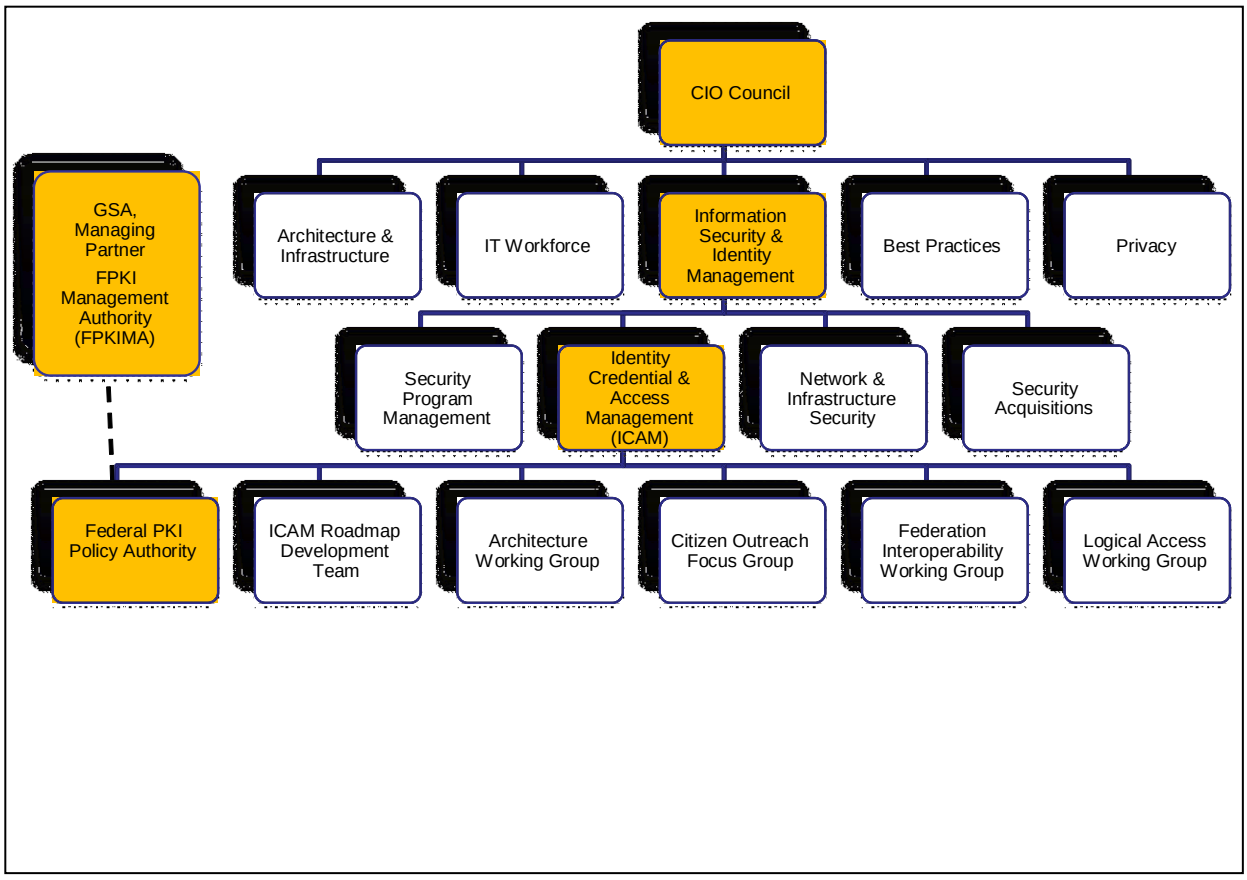
1.1 Background

The fundamental tenet of E-Government and E-Commerce is the trust of each party in a transaction that the other parties are indeed who they claim to be. A technology to assure this trust is based on asymmetric cryptography and digital certificates, which require establishment of a Public Key Infrastructure (PKI). PKI is a key factor in successfully implementing E-Government as called for by laws and executive directives such as the Government Paperwork Elimination Act (GPEA), the Government Paperwork Reduction Act, the Electronic Signatures in Global and National Commerce Act, the E-Government Act of 2002, Homeland Security Presidential Directive 7, and Homeland Security Presidential Directive 12 (HSPD-12). A crucial component to implementing E-Government and E-Commerce initiatives among government, citizens, and businesses is the Federal Public Key Infrastructure (FPKI). The purpose of the FPKI is to provide strong authentication, integrity, technical non-repudiation, and confidentiality services to government employees, contractors and business users. In addition, the FPKI provides a solid foundation for building authorization and advanced access control services, and provides the basis for Personal Identity Verification (PIV) and PIV Interoperable (PIV-I) credentials.

In recent years, identity management issues have been well-documented by the Government Accountability Office (GAO), National Science and Technology Council (NSTC), Office of Management and Budget (OMB), and most recently in the Cybersecurity Initiative, where the White House has laid out clear goals to make government more accessible to the American public while supporting the privacy and security of information and transactions. Identity, Credential and Access Management (ICAM) efforts within the federal government are a key enabler for addressing the nation‘s cybersecurity need. The Cyberspace Policy Review includes an entire section on the use of identity management in addressing cyber threats, which discusses recommendations such as improving authentication strength for individuals and devices, increasing the use of privacy-enhancing technologies, and extending the availability of identity management capabilities.

In September 2008, the Federal CIO Council established the Information Security & Identity Management Committee (ISIMC). The ISIMC is charged with overseeing government-wide activities related to Cybersecurity and Identity Management. In turn, the ISIMC established four subcommittees, including the Identity, Credential and Access Management Subcommittee (ICAMSC), which is co-chaired by the General Services Administration (GSA) and Department of Defense. The ICAMSC is tasked with aligning the Identity Management activities of government. The three other subcommittees address other cybersecurity issues. As Figure 1 depicts, the FPKI Policy Authority (FPKIPA), which governs the FPKI, is one of six ICAM working groups.

Figure 1. Federal ICAM Initiative Working Groups



1.2 Purpose

This Concept of Operations (ConOps) document provides a high-level description of the functions and processes used by the FPKI to provide trust services (e.g., cross-certification) for the benefit of the federal government. It identifies all stakeholders, and high-level functions and processes (e.g., managing certificate policies) and their corresponding interactions and information flows, as well as roles and responsibilities within the FPKI Community.

1.3 Audience

This is a public document intended for the entire FPKI Community.

1.4 Scope

The scope of this document is limited to the FPKI as it currently exists and operates.

2 Description of the Federal Public Key Infrastructure (FPKI)

The FPKI facilitates secure (trusted) physical and logical access, document sharing, and communications across federal agencies, and between federal agencies and outside bodies such as universities, state and local governments, commercial entities, and other communities of interest. To provide trust services, the FPKI uses a set of digital certificate standards, processes, and a mission-critical Trust Infrastructure to administer certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates (see Appendix A FPKI Trust Infrastructure for more detail). It uses a security technique called Public Key Cryptography to authenticate users and data, protect the integrity of transmitted data, and ensure technical non-repudiation and confidentiality.[1]

The FPKI is a key ICAM initiative. The FPKI Community is comprised of federal, industry, and state representatives who work collaboratively to leverage the FPKI, and to provide trust services for the benefit of the federal government.

The FPKI Policy Authority (FPKIPA) was created at the direction of the Federal Chief Information Officers (CIO) Council in 2000 to serve as the Federal Bridge governing body. The FPKIPA is an interagency body with voting membership limited to federal agencies who are Shared Service Provider (SSP) customers or who operate federal legacy PKIs. Other agencies, industry and state representatives participate in the FPKIPA as observers. The FPKIPA is supported by several policy and technical working groups. The E-Authentication Authorizing Official (EAO) is a special role within ICAM that decides policy for the EGCA and authorizes EGTS certificates.

The FPKI Management Authority (FPKIMA) is the operational arm of the FPKI that manages the FPKI Trust Infrastructure on a day-to-day basis. The FPKI Trust Infrastructure is the mission-critical federal system/environment that facilitates trust across the FPKI fabric via issuance and/or acceptance of PKI certificates. Certificates include cross-certificates[2] issued between the FPKI Community and the FPKI Trust Infrastructure, as well as non-person entity (NPE) certificates issued by the FPKI Trust Infrastructure's E-Governance Trust Services (EGTS). The FPKIMA manages an interoperability lab in support of the FPKI community and facilitates the FPKI Technical Working Group.

The remainder of the FPKI Community includes Entities such as federal and commercial PKIs, SSPs and federal agencies supported by SSPs, and community-of-interest Bridges. These FPKI Affiliates operate their own PKIs, or are served by PKIs, that have FPKIPA-approved trust relationships with the FPKI Trust Infrastructure. The approved trust relationships (at specified levels of assurance) allow trusted use of certificates issued by the FPKI Community.

In addition, the FPKI interfaces with external organizations whose actions may impact FPKI operations. This includes, but is not limited to commercial product and service vendors, Relying Parties (RPs), Identity Providers (IdPs), and government agencies and organizations that publish guidance, mandates, or specifications. Figure 2 summarizes the organizational composition of the FPKI.

[1] See also *The Realized Value of the Federal Public Key Infrastructure (FPKI)*.

[2] A cross-certificate is a certificate issued by one certification authority (CA) to another CA for the purpose of establishing a trust relationship between the two CAs.

Figure 2. High-level Organization of the FPKI

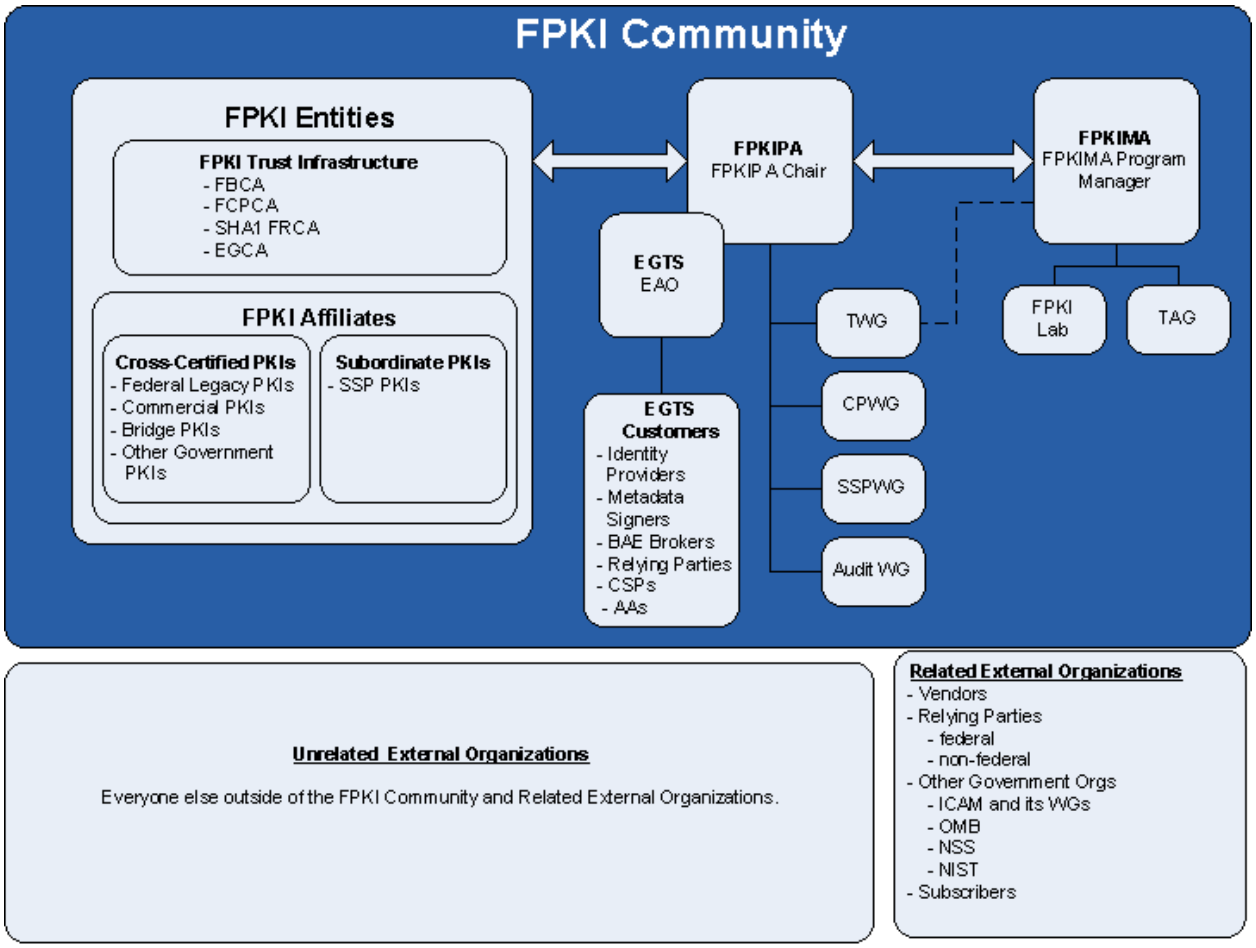


Figure 3 shows the Entities that currently comprise the FPKI. Figure 4 shows which federal agencies obtain services from which SSPs.[3]

[3] Both diagrams reflect the FPKI at the time of this writing. FPKI configuration changes infrequently. See http://idmanagement.gov/pages.cfm/page/Federal-PKI for the very latest FPKI information.

Figure 3. FPKI Entity Relationships to the FPKI Trust Infrastructure

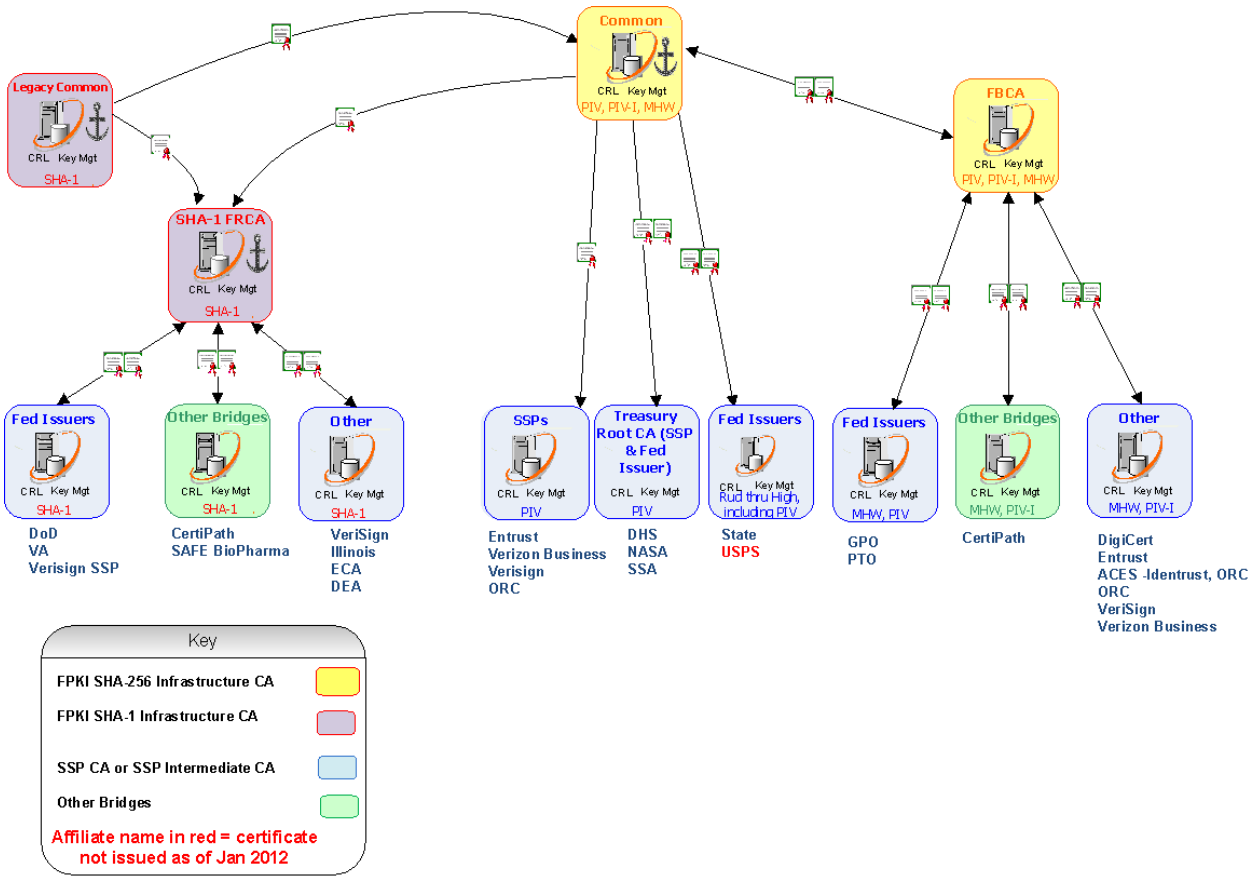
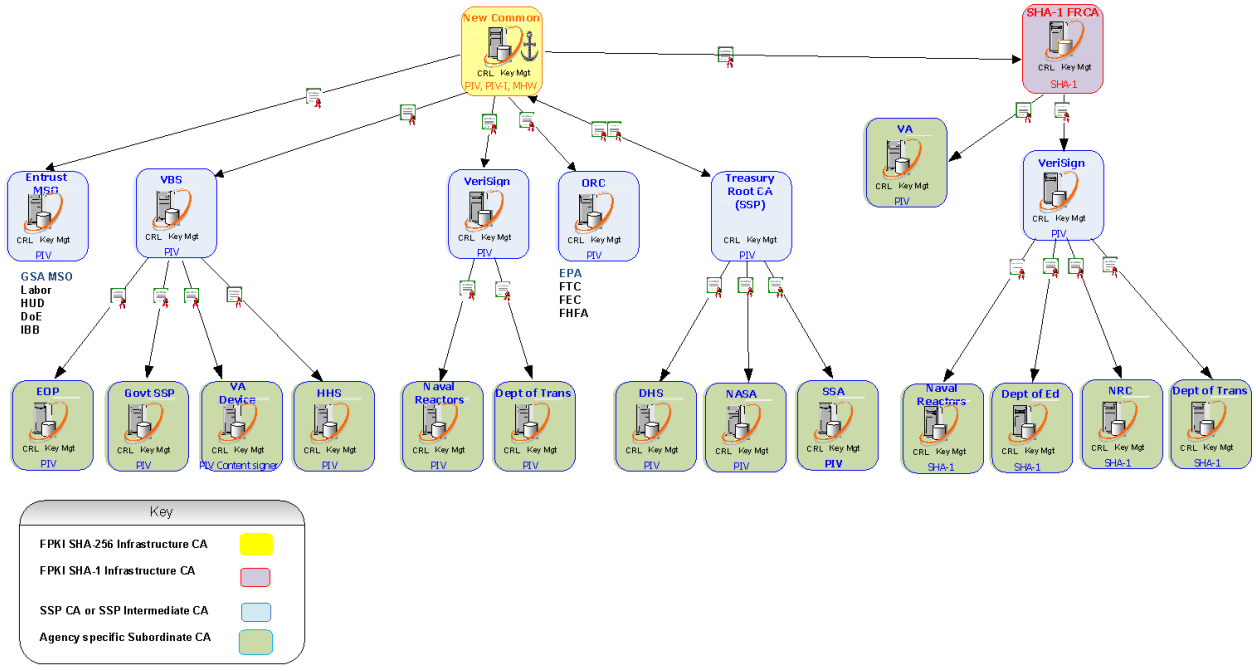


Figure 4. Federal Agencies supported by SSPs



In addition, the GSA Managed Service Office (MSO) provides SSP services to over 80 federal agencies. A detailed list can be found at http://fedidcard.gov/statistics.aspx

The following sections describe each FPKI Community member (i.e., description, roles and responsibilities, relationships).

2.1 FPKI Policy Authority (FPKIPA)

The FPKIPA is the FPKI governing body. It is an interagency body that develops digital certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies, such as universities, state and local governments and commercial entities. It does this by setting policy for the operation of the FPKI while considering the influence, direction, and guidance from external organizations that interact with the FPKI Community. According to the FPKIPA Charter, the FPKIPA has the following responsibilities:

- Facilitation of Certificate Policy (CP) / Certification Practice Statement (CPS) changes and approvals;
- Approval of Entity Cross-Certification;
- Monitoring compliance of all FPKI Entities;
- Directing the FPKIMA;
- Facilitation of Interoperability Practices; and
- Maintaining the Charter and Bylaws documents.

To execute these responsibilities, the FPKIPA, through the FPKIPA Chair, directs the FPKIMA and FPKI working groups to support the following functions:

- **Policy Management** – includes approval of all FPKI CP change proposals, CPSs, addition of new policies (e.g., PIV-I policies), and other policy-related approvals;
- **Governance** – includes providing direction and guidance to the FPKI:
    - *Approval of Governance Documents:* approving updates and maintenance of FPKIPA Bylaws and Operational Procedures and Practices, Criteria and Methodology, and other FPKI documents;
    - *Identification of Guidance Documents:* includes identification of the need for and development of specific guidance documents or white papers (e.g., SHA-256 FAQ, FPKI Security Profile);
    - *Approval of cross-certifications*: approving cross-certification applications in accordance with the process specified in the Criteria and Methodology document; and
    - *Compliance Enforcement* – ensuring FPKI Affiliates continue to comply with policy by ensuring Affiliates (a) submit annual audit letters that assert FPKI policy compliance, (b) provide delta mapping tables when CP changes are accepted, (c) provide the FPKIPA with a copy of their CP when it changes, and (d) notify the FPKIPA when they make changes to their architecture such as establishing new CAs or cross-certifying with additional partners.
- **Incident Response Strategy and Decisions** – approval of incident response strategy and tactical decisions.
- **Communications** – communications within the FPKI Community and with external organizations that interface with the FPKI (e.g., ICAM, RPs).

- **Strategic Operational Changes** – approves operational changes in support of policy that enhance FPKI security or performance.[4]

2.1.1 FPKIPA Chair

The FPKIPA Chair leads the FPKIPA by:

1. Representing the FPKIPA to external organizations and other government organizations and working groups;
2. Providing strategic direction in support of the FPKI;
3. Making tactical decisions related to incident response;
4. Establishing and directing strategic initiatives for the FPKI;
5. Approving establishment of specialized temporary working groups to address specific issues that impact the FPKI (e.g., SHA-256 Working Group);
6. Facilitating FPKIPA meetings; and
7. Signing Letters of Authorization (LOAs) to issue cross-certificates from the FPKI Trust Infrastructure.

2.1.2 FPKI Secretariat

The FPKIPA is supported by the FPKI Secretariat. The FPKI Secretariat function provides technical and administrative support for the FPKIPA. The Secretariat supports planning and facilitation of FPKIPA and working group meetings (e.g., agenda planning, meeting notes, scheduling). The Secretariat also manages the process flows between the FPKIPA and other FPKI Stakeholders.

2.1.3 FPKI Legal Counsel

Currently, the GSA attorney serves in the role of FPKI Legal Counsel. The FPKI Legal Counsel reviews Memorandums of Agreement (MOAs), reviews compliance audit letters, reviews legal agreements (e.g., contracts with vendors), vets Applicant organizations (e.g., verification that an organization is a legal entity), performs the legal portion of operational parameters reviews (identified in Criteria and Methodology), and offers opinions on other FPKI-related legal matters.

2.1.4 FPKIPA Working Groups

2.1.4.1 FPKI Technical Working Group (FPKI TWG)

The FPKIMA chairs and manages FPKI TWG meetings on behalf of the FPKIPA. The FPKI TWG includes technical participants from federal agencies and FPKI Entities, and is focused on advancing PKI technology through collaboration, discussion and investigation. Technical issues related to the usability of the PKI and future enhancements to the FPKI are brought to the TWG. The FPKI TWG:

- Addresses technical issues impacting the FPKI;
- Analyzes technical enhancement opportunities for the FPKI;
- Develops technical recommendations (noting potential policy impacts for Certificate Policy Working Group consideration) for the FPKIPA and other FPKI stakeholders; and
- Facilitates communication with vendors regarding technical-product issues.

[4] The FPKIMA is responsible for day-to-day and tactical operational changes such as security updates that do not require policy changes or FPKIPA approval.

In addition, the FPKI TWG reviews Path Discovery and Validation (PDVal) technology and the facilitation of bridge-enabled certificate validation. The FPKI TWG meets once per month

2.1.4.2 Certificate Policy Working Group (CPWG)

The CPWG addresses policy issues, reviews all FPKI CP change proposals, and provides policy-related recommendations to the FPKIPA. In addition, the CPWG oversees the cross-certification process,[5] which includes policy mapping, technical evaluation, and operational parameters review.

The CPWG Co-chairs are appointed by the FPKIPA Chair. The CPWG is comprised of participants from federal agencies and FPKI Entities. The CPWG may also review FPKI Entity compliance issues. The CPWG meets twice per month.

2.1.4.3 Shared Service Provider Working Group (SSPWG)

The SSPWG is similar to the CPWG, but focuses only on SSPs providing PKI certificate services to the federal government. The SSPWG determines the requirements, processes, and oversight provisions for selection of SSPs that will act on the government's behalf under the provisions of the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework Certificate Policy*. In addition, the SSPWG oversees the certification process,[6] which includes CPS Evaluation, Operational Capabilities Demonstration (OCD), and Government review of audit documentation.

The SSPWG was open to, and composed of federal agency representatives from federal agencies who are members of the FPKIPA, and who are not also SSPs themselves. The SSPWG also monitored SSP compliance. The SSPWG is currently dormant.

2.1.4.4 Audit Working Group (Audit WG)

The Audit WG was established to gain consensus on mutually-acceptable PKI audit practices in the commercial, government, and bridge environments, as well as to address and evaluate changes to FPKI audit requirements. The Audit WG is comprised of representatives from Entity PKIs and third-party auditors who may be invited to offer their expertise. The Audit WG meets as needed, develops audit guidance documents, and makes policy change recommendations to the CPWG.

2.1.5 E-Authentication Authorizing Official (EAO)

The EAO oversees the EGTS, which includes the E-Governance Certification Authority (EGCA). The EGTS offers services that facilitate the use of federated identity in a trusted manner throughout the federal government, and between the federal government and its partners (i.e., citizens, businesses, and other entities). The EAO:

1. Provides the FPKIPA with status of periodic EGCA compliance audits to demonstrate that the EGCAs are operating in compliance with the approved CPSs;
2. Approves the EGCA CP and CPS;
3. Approves EGCA compliance audit reports;
4. Authorizes issuance of certificates from the EGCA (by signing LOAs); and
5. Verifies the identity of sponsors of EGCA certificates.

[5] Governed by Criteria and Methodology.

[6] Governed by Shared Service Provider Roadmap: Navigating the Process to Acceptance

6. Authorizes the ICAM Lab to support testing of EGTS applications prior to approving the issuance of EGTS certificates

The *EGCA EGTS Certificate Application and Issuance* document details how EGTS certificates are requested and issued.

2.2 FPKI Management Authority (FPKIMA)

The FPKIMA manages, operates and manages the FPKI Trust Infrastructure on a day-to-day basis in accordance with the FPKI CPs and the CPSs approved by the FPKIPA. The FPKIMA operates under the direction of the FPKIPA. To operate and maintain the FPKI Trust Infrastructure, the FPKIMA performs the following functions:

- **Operations** – operates and maintains the FPKI Trust Infrastructure on a day-to-day basis in accordance with FPKI CPs, FPKI CPSs and FPKIMA Standard Operating Procedures;
- **Communications** – maintains and facilitates communications across the FPKI Community related to current and planned FPKI Trust Infrastructure operational status and monitors external organizations, technology, policies, and events that may affect the FPKI Community as its requirements evolve;
- **Testing** – performs testing in support of new Applicants, current Entity PKIs, and strategic or transition planning;
- **Helpdesk** - provides helpdesk and technical analysis services to address technical issues encountered by Entities; and
- **Incident Response Management** - manages security incidents impacting the FPKI Community.

2.2.1 FPKIMA Lab

The FPKIMA operates and maintains an FPKIMA Lab that consists of multiple environments, including a Community Interoperability Test Environment (CITE), and other environments for development and ad hoc testing to support the FPKI. In addition, the FPKI Lab conducts PDVal testing for vendor applications requesting to be included on the FPKI Qualified Validation List (QVL). An external lab, the ICAM Lab, develops pilots and performs testing at the direction of the ICAM, EAO, or FPKIPA. The ICAM Lab collaborates with the FPKI Lab to develop pilots and prototypes of planned FPKI services, support PIV-I testing, and developing utilities for the FPKI (e.g., AIA Crawler, and PKCS#7 tools).

2.2.1.1 The Community Interoperability Test Environment (CITE)

CITE provides the FPKI Community with a test environment to identify and resolve issues, and to ensure proper functionality prior to deploying hardware and/or software into the production environment. The FPKIMA maintains test versions of FPKI Trust Infrastructure components for CITE. The CITE Trust Infrastructure is available for cross-certification and interoperability testing with the FPKI Affiliates' test PKIs. In the same way that the FPKI includes the Repositories managed by each Entity PKI in addition to the FPKI Trust Infrastructure Repositories, CITE includes the Repositories managed by the FPKIMA in its test lab and the Repositories managed by the Entity PKIs participating in CITE. This integration of infrastructures makes up CITE. Some examples of testing conducted in CITE are:

1. Interoperability testing between cross-certified CAs;
2. Interoperability testing of chaining between Directories;

3. Testing transition to new algorithms (e.g., transition from SHA-1 to SHA-2);
4. PIV-I card interoperability testing (CITE provides the interagency cross-certification, while card interoperability testing is performed in the ICAM Lab);
5. Path discovery testing for a particular application; and
6. Path validation testing for a particular application.

2.2.2 FPKIMA Helpdesk

The FPKIMA maintains a helpdesk that is accessible via email or telephone. The helpdesk provides the FPKI Community the ability to report issues related to the FPKI Trust Infrastructure, and allow the FPKIMA to respond and provide immediate assistance. The helpdesk is also available to the FPKI Community and external (non-FPKI) parties for general requests and inquiries.

2.2.3 FPKIMA Working Groups

2.2.3.1 Technical Advisory Group (TAG)

In support of the FPKIMA's mission, the National Institute of Standards and Technology (NIST) provides technical recommendations and standards to the FPKIPA and at large to the federal government for public key services. NIST recommendations and standards are technology and standards focused. The FPKIMA established the TAG to provide operational and effective implementation expertise and perspectives on NIST recommendations, guidance, and standards. The TAG is a small focused group of practitioners considered experts in public key technology

2.3 FPKI Entities

2.3.1 The FPKI Trust Infrastructure

The FPKIMA operates and maintains the FPKI Trust Infrastructure, which is the backbone of the FPKI. It consists of several CAs and their supporting Repositories. The FPKI Trust Infrastructure CAs are:

- Federal PKI Common Policy Framework Certification Authority (FCPCA);
- Federal Bridge Certification Authority (FBCA);
- E-Governance Certification Authorities (EGCA); and
- SHA-1 Federal Root Certification Authority (SHA1 FRCA).

The FCPCA is the trust anchor for digital-authentication certificates for the PIV credentials. The FBCA provides the basis for mapping CPs between federal legacy PKIs, PIV, other government and commercial PKIs (including PIV-I) and other PKI Bridges. The EGCA is the source of various NPE credentials such as IdP credentials, RP credentials, metadata signer credentials, and backend attribute exchange (BAE) broker certificates. The SHA1 FRCA supports FPKI Community members that cannot yet support SHA-256.

2.3.2 FPKI Affiliates

There are five categories of FPKI Affiliates that are connected to the FPKI Trust Infrastructure:

- **Legacy PKIs –** a PKI run by a government organization that has successfully completed all steps required to become cross-certified with the FBCA, and has been issued a cross-certificate by the FBCA, FCPCA, or SHA1 FRCA, as opposed to obtaining PKI services and credentials from an

SSP subordinate to the FCPCA. Legacy PKIs were early adopters of PKI whose systems pre-date the issuance of the Office of Management and Budget (OMB) M-05-05 requiring the use of SSPs.

- **Bridge PKIs** – a CA that itself does not issue certificates to end entities (except those required for its own operations), but establishes unilateral or bilateral cross-certification with member PKIs similar to the FBCA. Bridge CAs currently cross-certified with the FBCA include SAFE/BioPharma and CertiPath. CertiPath has been approved as a PIV-I Bridge and can approve member PKIs to be PIV-I issuers.
- **SSP PKIs –** offer out-sourced PKI services to federal agencies (i.e., SSP Customers). This allows federal agencies to deploy digital credentials without the need to operate and maintain an Enterprise PKI. SSP PKIs adhere to the Common Policy CP and receive a cross-certificate from the FCPCA with no policy mapping extension, making them subordinate to the FCPCA. SSP Customers are part of the FPKI because they may operate components of the PKI service on behalf of their own agency, such as Registration Authorities (RAs) and Card Management Systems (CMS).
- **Commercial PKIs –** a PKI run by a commercial organization that has been issued a cross-certificate by the FBCA. Some commercial PKIs have been approved as PIV-I issuers. Some commercial PKIs are also approved as SSPs, but must operate under their own CP when cross-certified with the FBCA and under FCPCA for their SSP service.
- **Other Government PKIs** - a PKI run by a non-Federal government organization (e.g., state, local or foreign) that has been issued a cross-certificate by the FBCA.

Entity representatives are responsible for complying with evolving FPKI technical and policy requirements and actively participate in FPKI working groups. FPKI CPs and MOAs specify the incident reporting and change modification procedures for which each Entity is responsible. Entities identify policy or technical issues that require attention as well as enhancements to the FPKI without compromising interoperability. Additionally, Entity representatives collaborate with the broader FPKI Community to streamline requirements as the FPKI evolves and are responsible for passing information from the FPKI membership, as appropriate, to its own users and customers.

2.4 Related External Organizations

To execute its mission, the FPKI interfaces with, and depends upon various external organizations with whom there is no direct relationship. These organizations include:

- **Relying Parties** – Relying Parties (RPs) operate online applications that utilize digital certificates for authentication of electronic identities. RPs may use the FCPCA root certificate as a trust anchor, which enables their applications to trust digital certificates issued by any Entity PKI's cross-certified with the FPKI. RPs that take this approach can be assured that these certificates were issued following the CP rules for identity proofing the subject of the certificate defined by the FPKI policies. No other information is required for the RP to make that determination of trust.
- **Vendors –** commercial and other providers of components used by the FPKI Trust Infrastructure and FPKI Affiliate PKIs. This includes, but is not limited to software, hardware, and networking components. In addition, some vendors distribute the FCPCA Root Certificate in their CA certificate trust stores at the request of the FPKIMA.

- **Other Government Organizations –** the FPKIPA coordinates with other government organizations to address impacts of regulations, standards, and policy on the FPKI Community. These organizations include, but are not limited to the ICAMSC, ICAM working groups, OMB, the National Security Systems, and NIST.
- **Subscribers** – the end-entities to which FPKI Affiliate PKIs issue certificates. The FPKI Trust Infrastructure has no direct relationship to the subscribers, but relies on FPKI Affiliate PKIs to keep the subscriber informed of relevant information.

The actions of these external organizations may impact FPKI requirements. For example, government organizations such as NIST and OMB develop standards, guidance and directives that the FPKI must consider when developing or modifying its policies. In addition, ICAM and its working groups develop higher-level identity management initiatives, which may impact the FPKI. While direct lines of communication do not currently exist, understanding the needs of RPs is an important factor when making changes to the FPKI policies to ensure they support RP needs – especially the need for trust. Relationships with vendors are needed to communicate FPKI requirements to the vendors, and to understand how and when proposed capabilities will be supported in vendor products, enabling implementation of enhancements in operations or policy by the FPKI.

2.5 Unrelated External Organizations

Unrelated organizations are those that are neither in the FPKI Community nor a related FPKI external organization. Though these organizations have no ostensible relationship with or interest in the FPKI, the FPKI may ultimately be affected by actions (malicious or otherwise) of those organizations. An example of an unrelated external organization that may have affected the FPKI Community and/or related external organization is DigiNotar.[7]

[7] On July 19th 2011, DigiNotar detected an intrusion into its Certificate Authority (CA) infrastructure, which resulted in the fraudulent issuance of public key certificate requests for a number of domains, including Google.com. The major browser vendors had to action to remove or disable the DigiNotar CA from their Trust Stores.

3 High-level FPKI Process Flows

The process flow diagrams in this section depict the steps and information flows for some of the functions described in Section 2. Each high-level flow is important for the FPKI to achieve it mission. Table 1 lists the FPKI Processes and FPKI documents that provide detailed descriptions of the FPKI process flows.

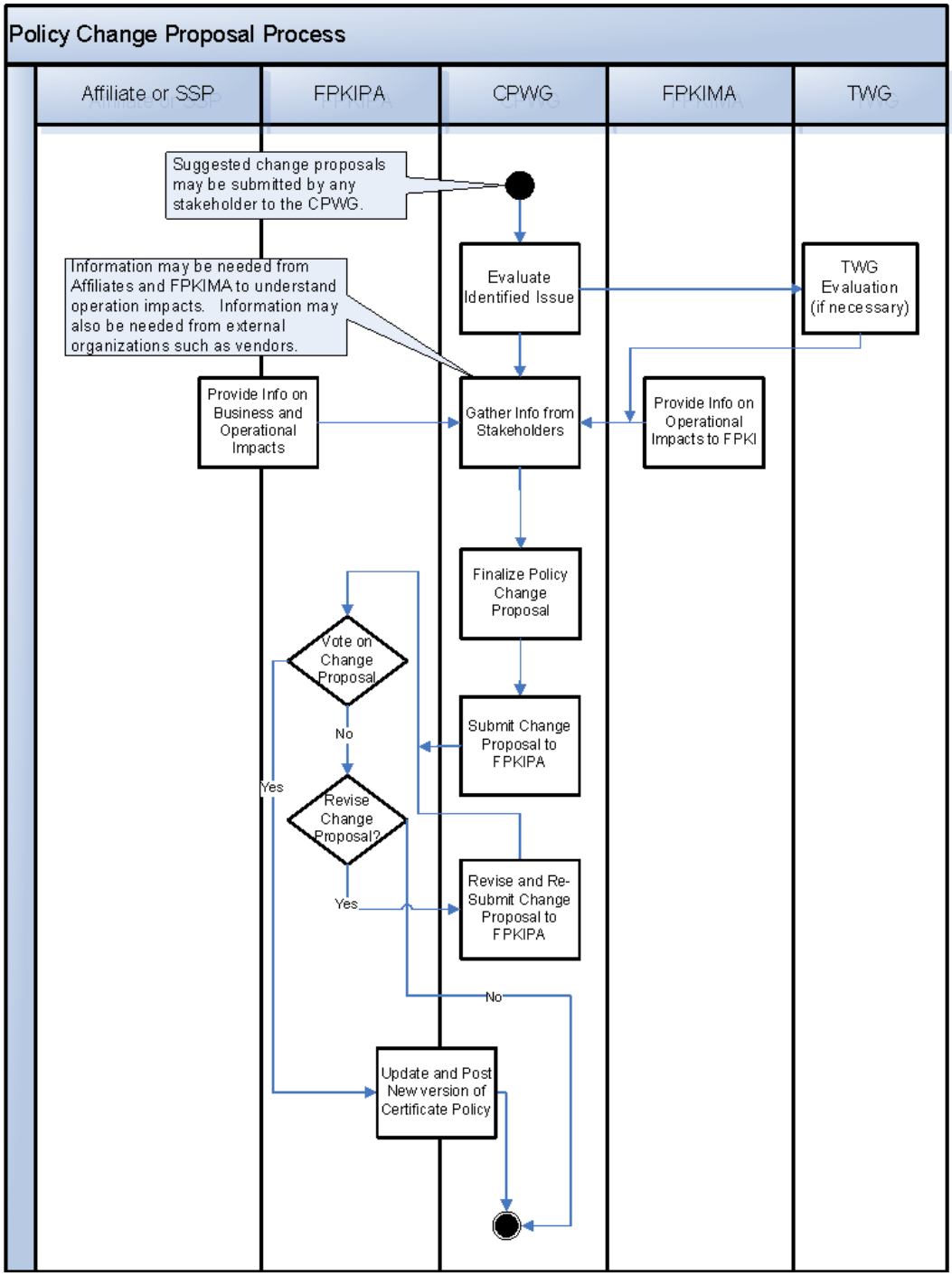
Table 1. FPKIPA Processes Categorized by Function

FPKI Function/Process	Reference Document	Description
Policy Management		
• Policy Change Proposals	Criteria and Methodology	Depicts the process for submitting and approving changes to all FPKI CPs.
Governance		
• Governance Document Approval	Charter and Bylaws	Depicts the process for submitting and approving changes to the FPKIPA Charter and Bylaws documents.
• Cross-Certification	Criteria and Methodology	Depicts the process for application for cross-certification through issuance of cross-certificates for an Entity PKI.
• SSP Approval	SSP Roadmap	Depicts the process for application to be accepted as an SSP through issuance of a subordination cross-certificate as an SSP PKI.
• Compliance Audit Maintenance	Criteria and Methodology	Depicts the process for approval of compliance audits.
• Re-Certification	Criteria and Methodology	Depicts the process for re-issuance of cross-certificates to existing Entity PKIs.
Incident Response Strategy		
• Response to Incidents	Incident Management Process	Depicts the process for Incident Management details in the FPKI Community Incident Management Process – document under development.
Strategic Operational Changes		
• Technical Issue Evaluation	No document necessary. Captured as a process step in Figure 13.	Depicts the process for submitting and evaluating technical issues that impact the operations and policy of the FPKI.

3.1 Policy Management

As the FPKI grows, requirements and capabilities change over time. These changes often require changes to FPKI policy. Changes in policy are not trivial because the entire FPKI Community must concur, otherwise interoperability can be threatened. Figure 5 depicts the process by which a policy change is proposed, reviewed by the CPWG and approved by the FPKIPA.

Figure 5. Policy Change Proposal Process



3.2 Governance

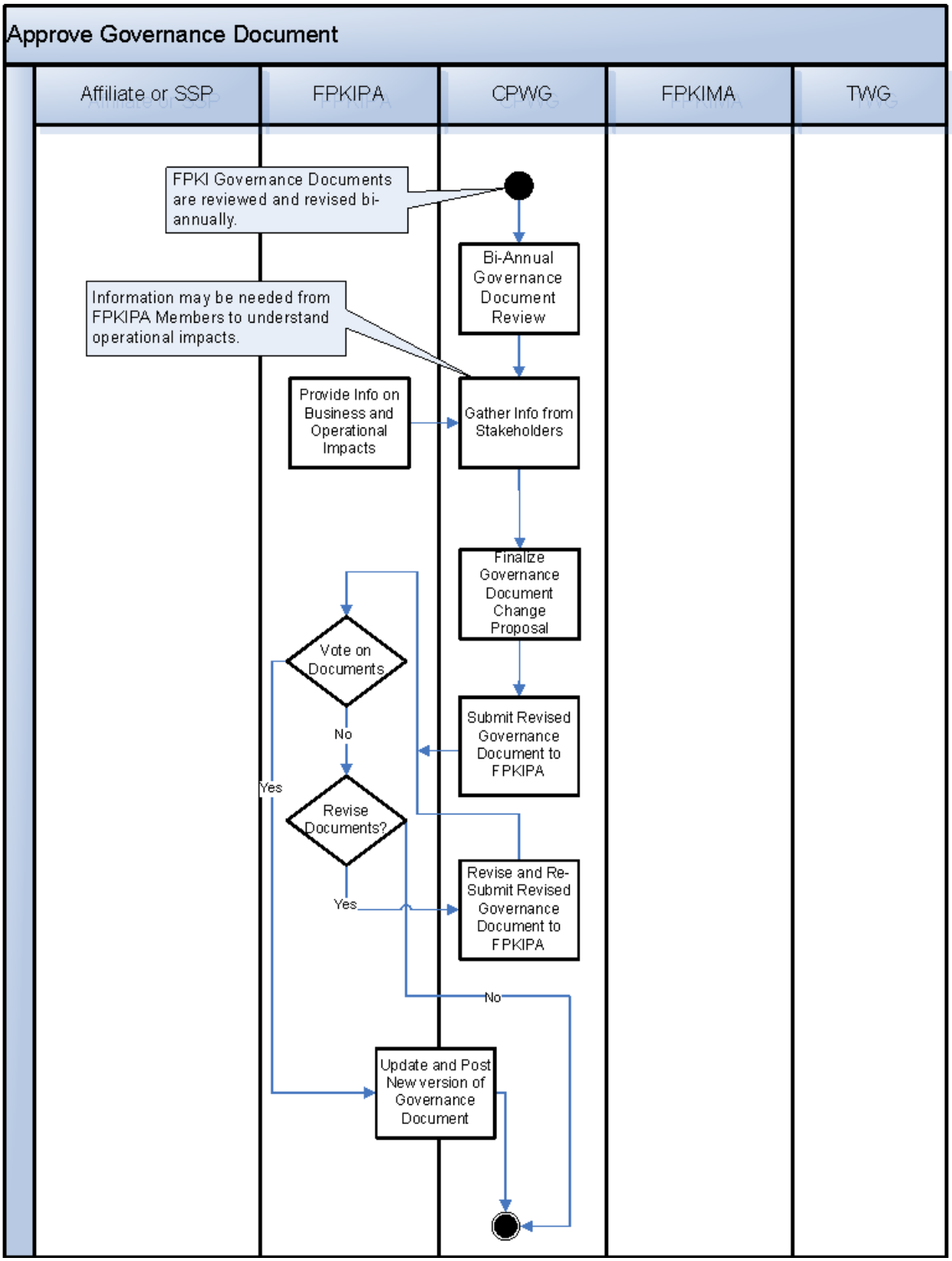
FPKI Governance Processes include:

- Governance Document Approval;
- Cross-Certification;
- SSP Approval;
- Compliance Audit Maintenance; and
- Re-Certification.

3.2.1 Governance Document Approval Process

The FPKIPA Charter and Bylaws govern how the FPKIPA operates. Bi-annual review of these documents is self imposed to ensure the documents are maintained. Figure 6 shows the process for reviewing and approving these documents on a bi-annual basis.

Figure 6. Governance Document Approval Process



3.2.2 Cross-Certification Process

The process for cross-certification with the FBCA is detailed in the Criteria and Methodology document. The following figures provide an overview of the cross-certification process. Figure 7 is an overview of the process as depicted in Criteria and Methodology. Figure 8 shows the roles of involved FPKI Community members as an Applicant moves through the application, policy mapping, testing, audit compliance, and approval steps required before cross-certification with the FBCA.

Figure 7. FBCA Cross-Certification Process

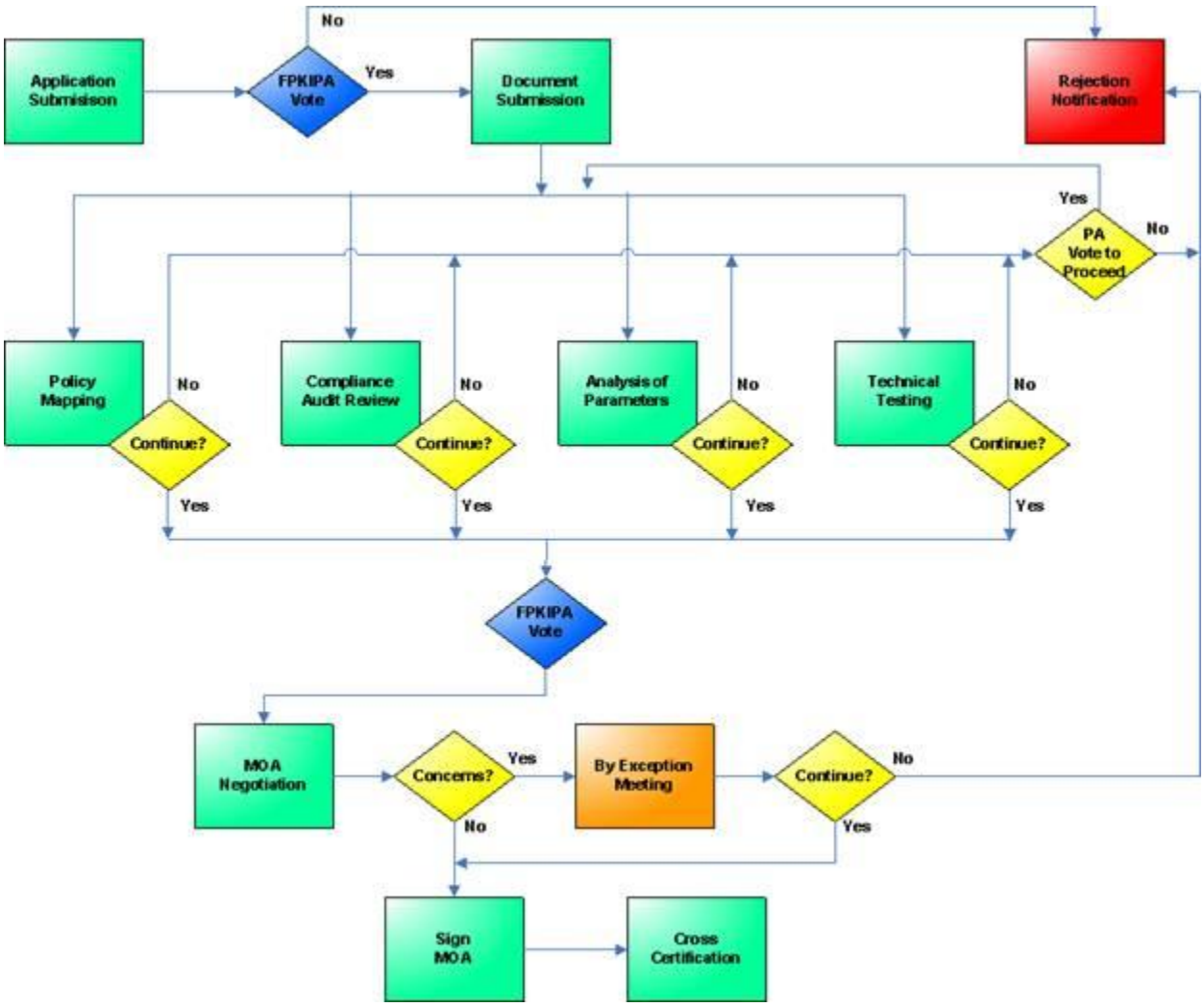
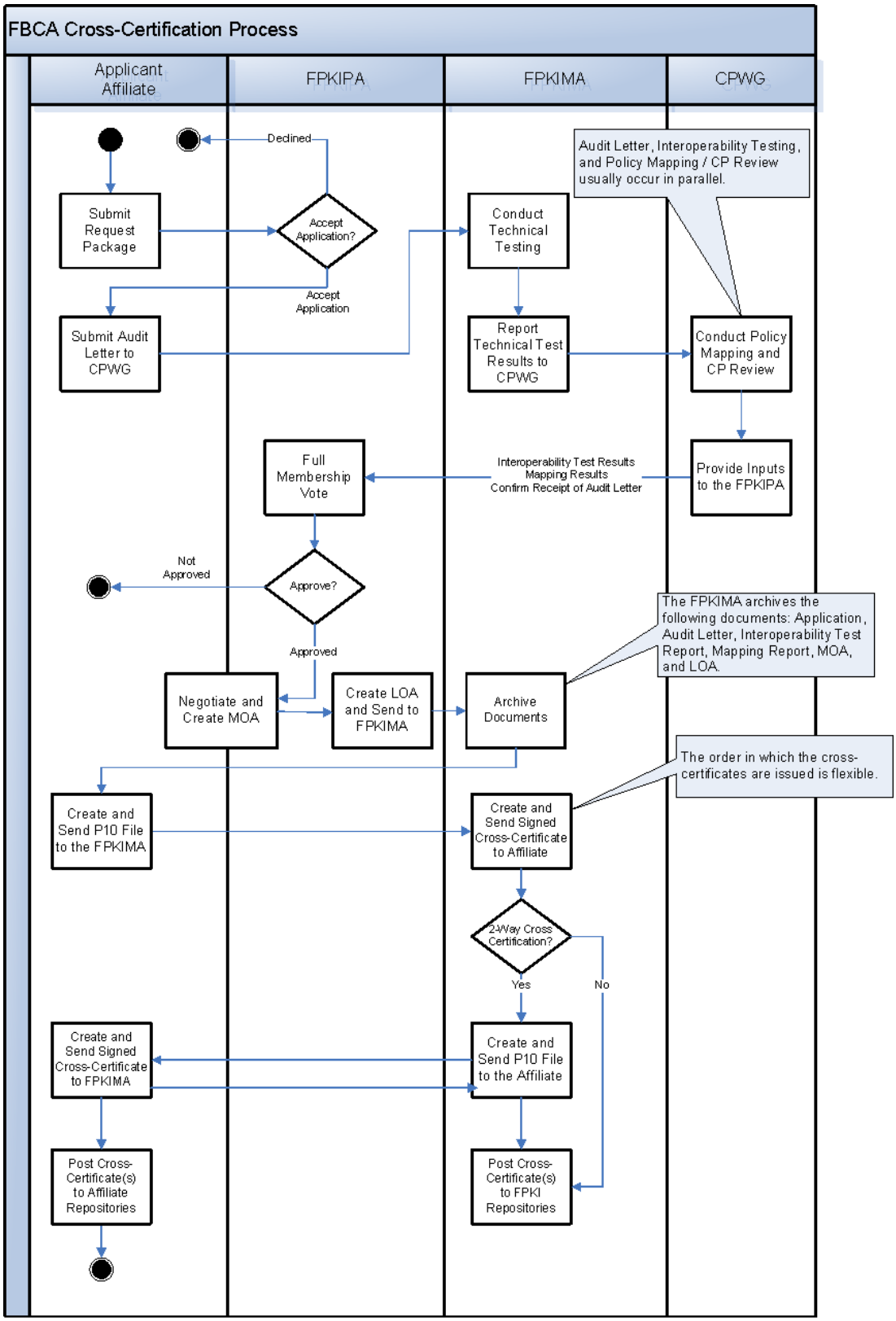


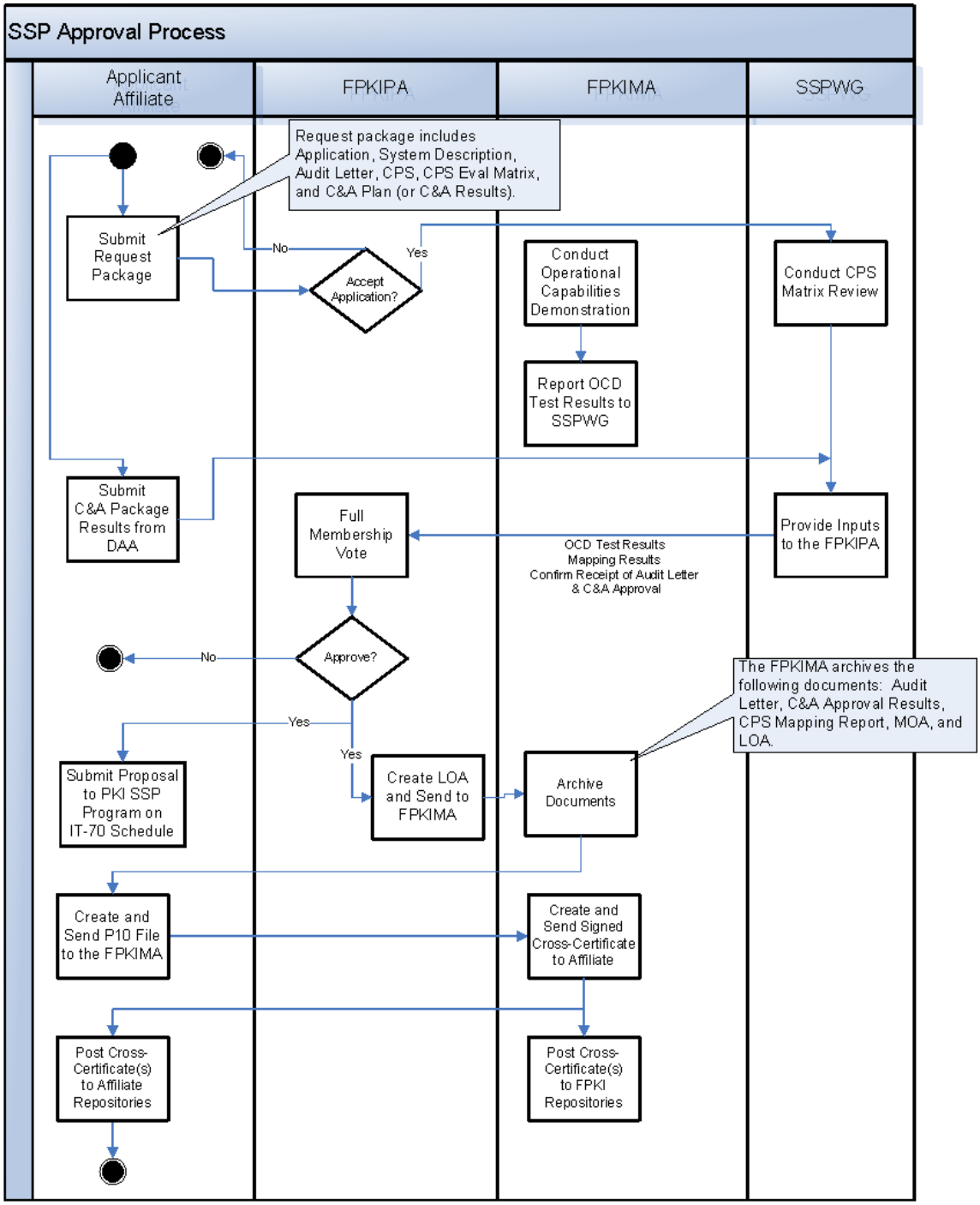
Figure 8. FBCA Cross-Certification Process Roles



3.2.3 SSP Approval Process

SSPs must follow a process similar to FBCA cross-certification approval. Because SSPs operate systems on behalf of the government, there are some differences in the process, which include submission and review of certification and accreditation (C&A) documentation. Figure 9 shows the process flow.

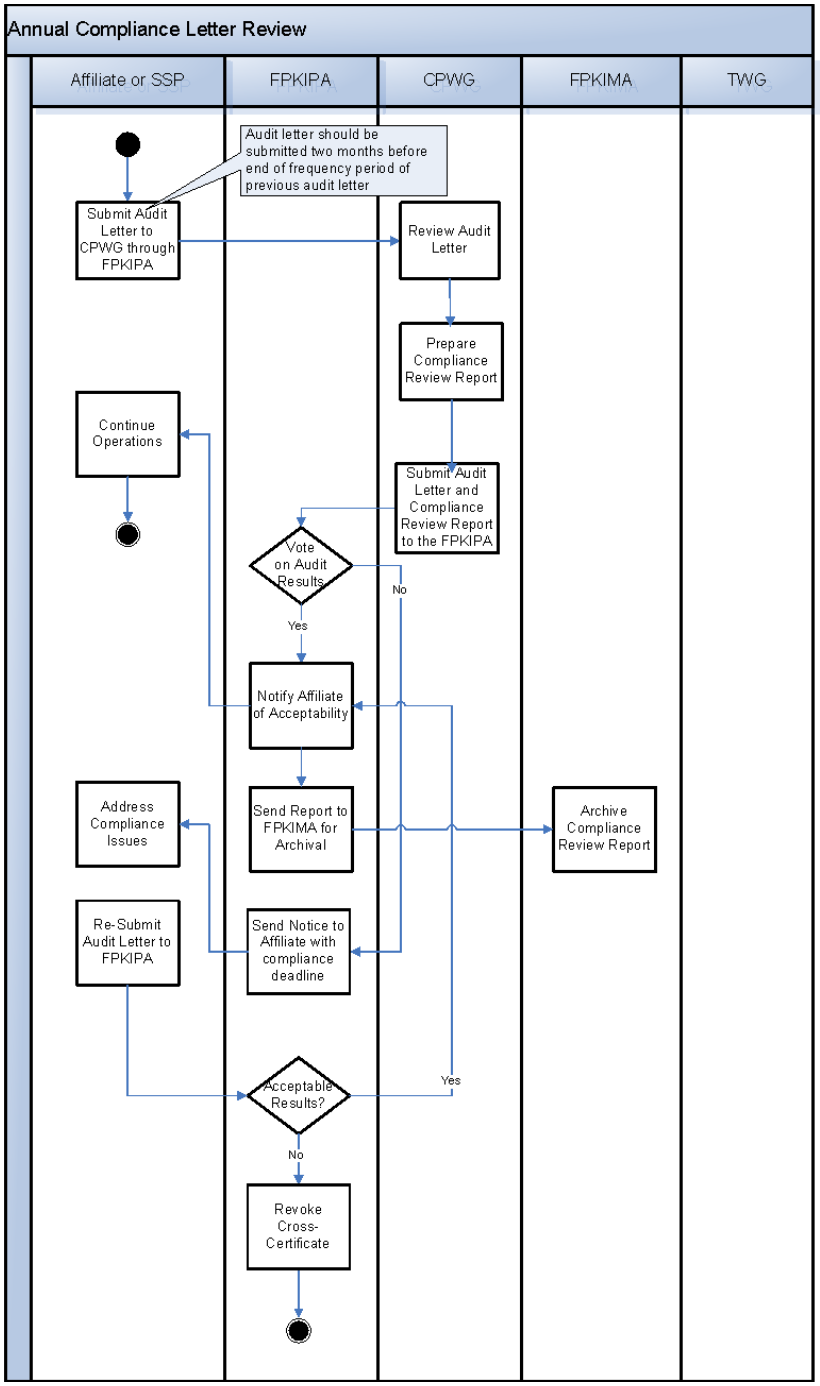
Figure 9. SSP Approval Process



3.2.4 Compliance Enforcement Process

To ensure Entity PKIs continue to operate in compliance with current FPKI policies, Entity PKIs must keep their CPs aligned with applicable FPKI CPs. In addition, Entity PKIs must undergo audits conducted by third-party auditors, and submit letters asserting that their operations are compliant with their CPs. Figure 10 shows the process flow.

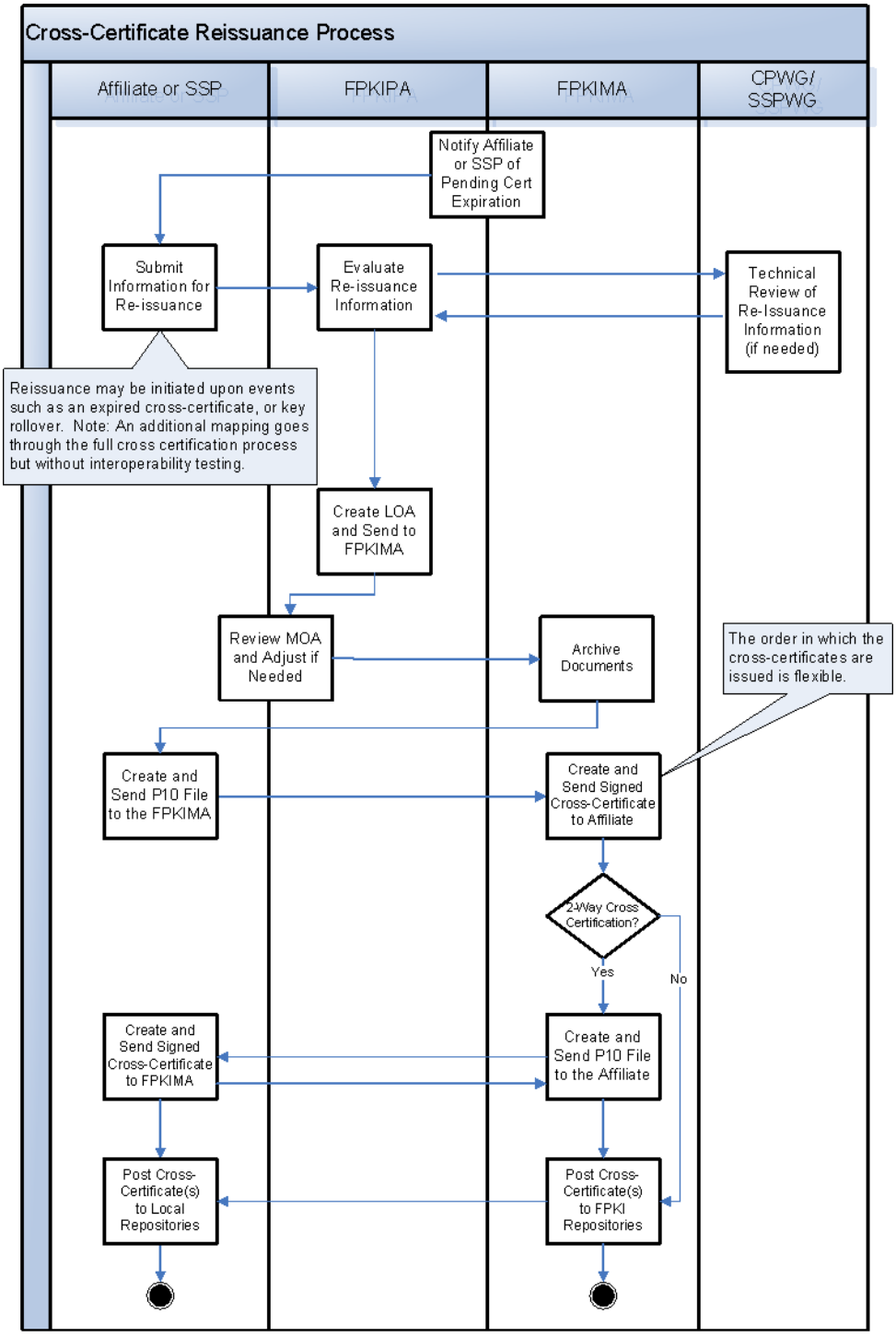
Figure 10. Compliance Audit Maintenance Process



3.2.5 Re-Certification Process

Before certificates issued from the FPKI to an Entity PKI expire, the FPKI must perform certain checks to ensure the Entity PKI is still in compliance with policy. Figure 11 shows the steps necessary before a new cross-certificate is issued to an Entity PKI to replace a cross-certificate that is about to expire.

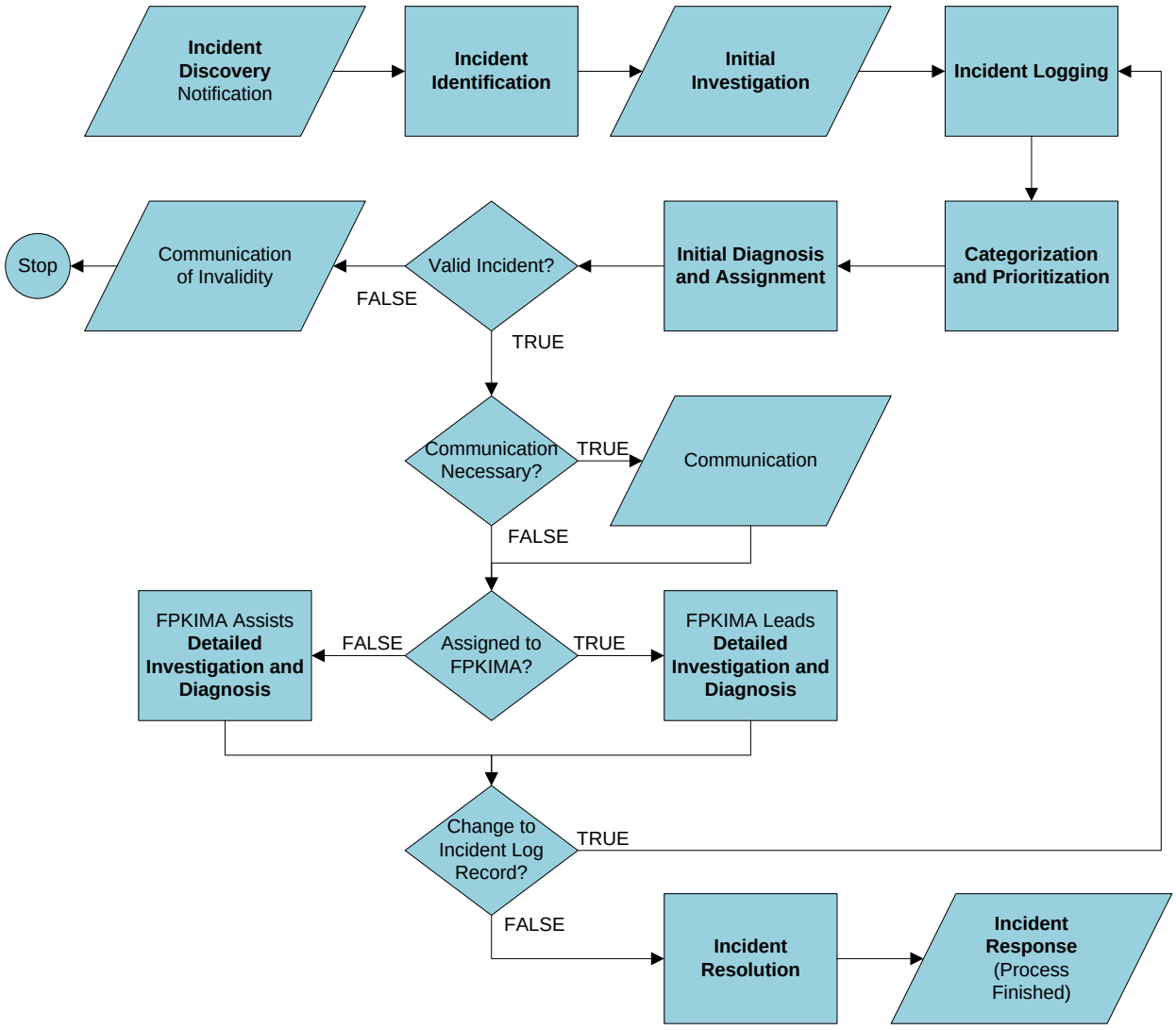
Figure 11. Re-certification Process



3.3 Incident Response Strategy

The FPKI Incident Management Process is currently being defined by the FPKI TWG. This process defines how the FPKI will respond to incident that impact the FPKI Community. Figure 12 shows the planned process.

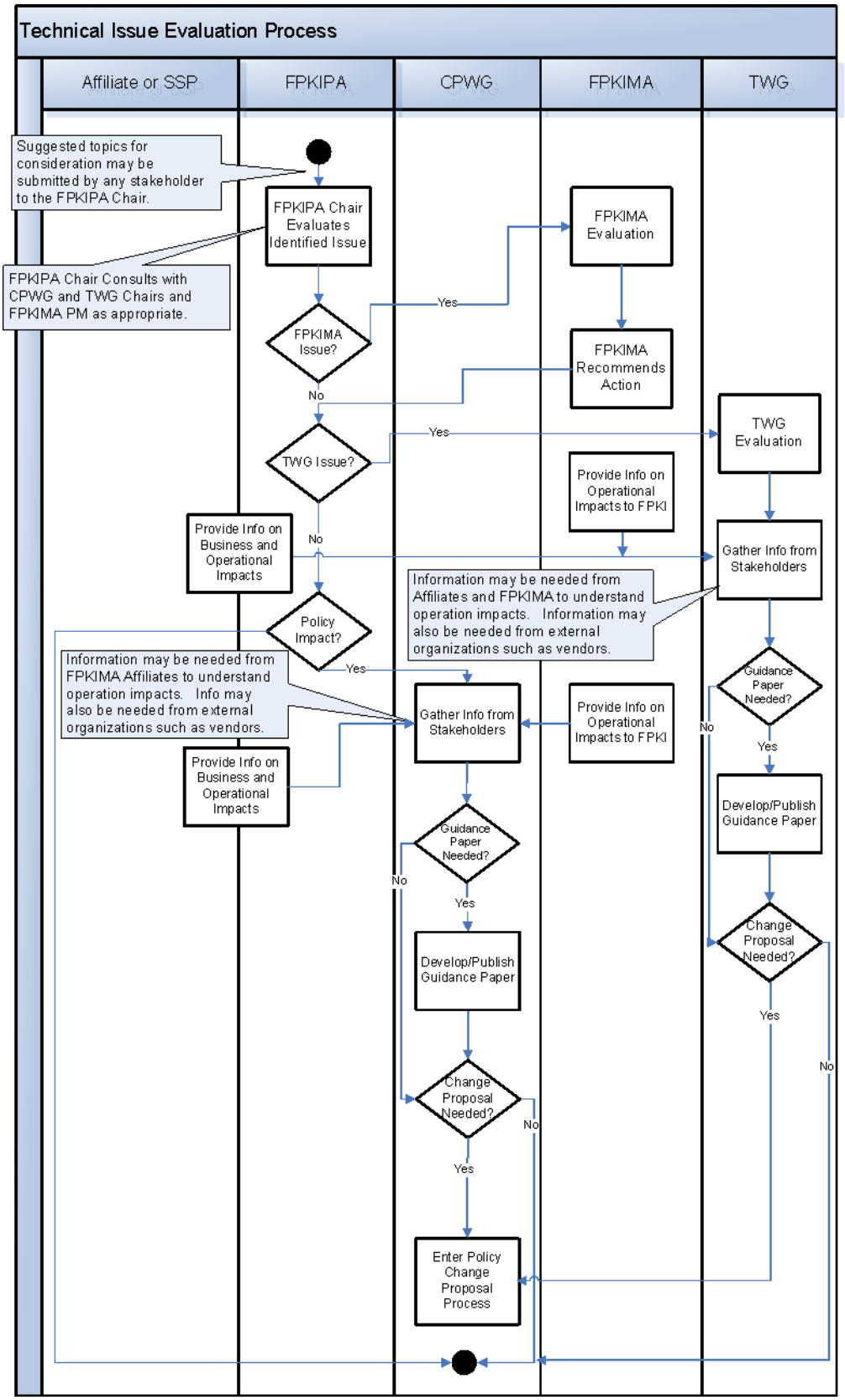
Figure 12. FPKI Incident Management Process



3.4 Strategic Operational Changes

The requirements of the FPKI evolve over time, in response to newly-identified threats and newly-defined FPKI capabilities. Figure 13 depicts how technical issues are introduced to the FPKI, and addressed by the TWG and/or CPWG with the goal of enhancing the overall FPKI.

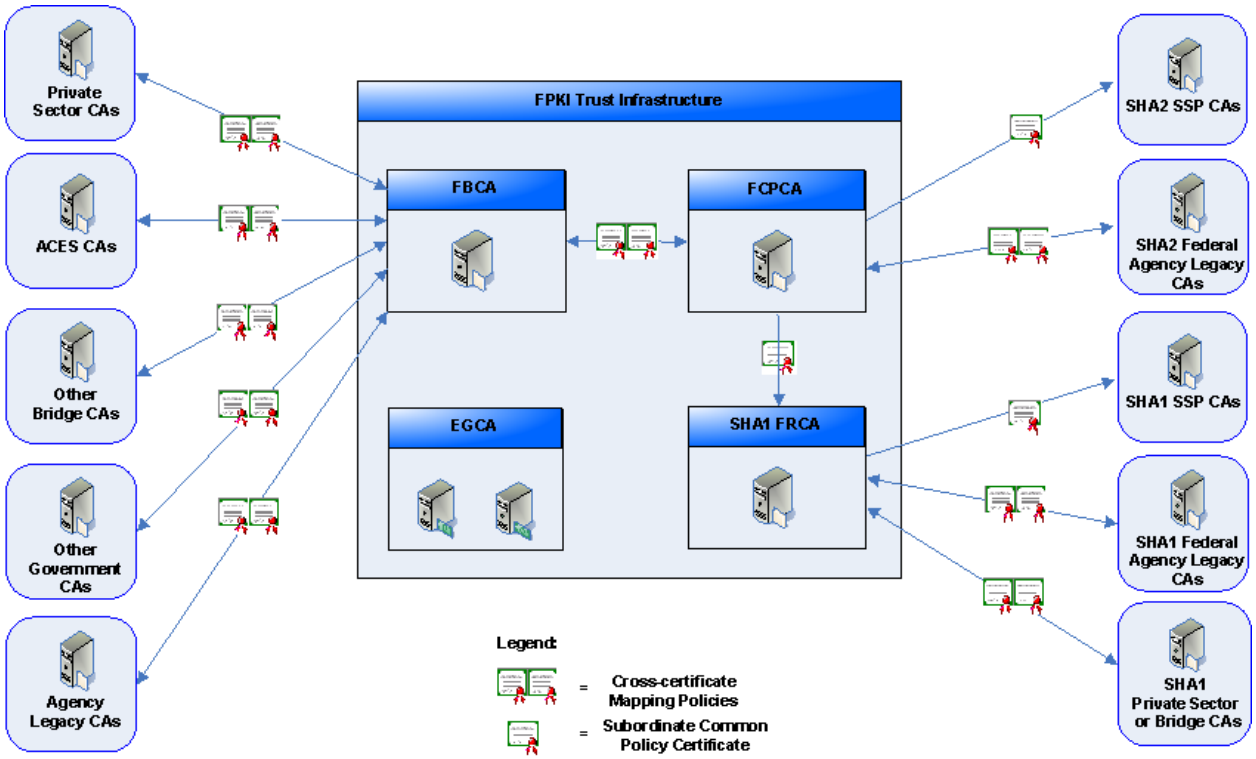
Figure 13. Technical Issue Evaluation Process



Appendix A FPKI Trust Infrastructure

The FPKI Trust Infrastructure consists of six CAs (FBCA, FCPCA, SHA1 FRCA, EGCA CSP2, EGCA RP, and EGCA TS) and the Repository services to support them.[8] All cross-certificates and Certificate Revocation Lists (CRLs) issued by FPKI Trust Infrastructure CAs, and all cross-certificates issued to FPKI Trust Infrastructure CAs are published in the FPKI Trust Infrastructure Repositories. The FPKI Trust Infrastructure resides at the technology layer of the ICAM Segment Architecture. Figure 14 shows a high level view of the FPKI Trust Infrastructure.

Figure 14. High Level View of the FPKI Trust Infrastructure



3.4.1 A-1 Federal PKI Common Policy Framework (FCPCA)

The FCPCA was established to serve as the FPKI hierarchical trust anchor for federal agency CAs, in support of HSPD-12 and PIV cards. FCPCA customers are SSP CAs that issue and manage PIV cards for federal agencies that do not have their own PIV-issuing PKIs. In addition, federal legacy PKIs can choose to directly cross-certify with the FCPCA rather than FBCA.

The FCPCA is public facing, and its root certificate is distributed by commercial vendors (by inclusion in an increasing number of commercial off the shelf product trust stores), enabling it to be the trust anchor for external RPs to trust PKI certificates issued by federal agencies. This facilitates PDVal for external

[8] The SHA1 FRCA was created to facilitate interoperability for PKIs unable to transition to SHA-256 by January 1, 2011. The SHA1 FRCA will only be operated until December 31, 2013.

RPs. The certificate policies defined in the FCPCA CP apply to federal employees, contractors, and other affiliated personnel requiring PKI credentials for access to unclassified federal systems that have not been designated by law as national security systems.

3.4.2 A-2 Federal Bridge Certification Authority (FBCA)

The FBCA is an identity trust hub that enables peer-to-peer transactions between its member organizations, both federal and non-federal.[9] The FBCA is cross-certified with the State of Illinois, and with two commercial PKI Bridges: CertiPath, which serves the Aerospace and Defense industry, and SAFE/BioPharma, which provides digital identity and signature standards for the pharmaceutical and healthcare industries. These partners have extended the reach of the FPKI well beyond the boundaries of the federal government. In addition, there are commercial PKI service providers cross-certified with the FBCA offering federally-trusted credentials to U.S. state and local governments and business entities.

3.4.3 A-3 SHA-1 Federal Root Certification Authority (SHA-1 FRCA)

The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011. However, there are some applications in use within the FPKI Community that cannot process certificates or certificate revocation information signed using SHA-256. Therefore, a new parallel SHA-1 FPKI was created to facilitate the interoperability for those unable to transition to SHA-256 by January 1, 2011 (i.e., for those FPKI organizations that are not yet technically capable of implementing the SHA-256 algorithm in their environment). Use of certificates asserting certificate policy Object Identifiers (OIDs) that identify the use of SHA-1 under this policy should be limited to applications for which the risks associated with the use of a deprecated cryptographic algorithm have been deemed acceptable and will only be asserted within the parallel SHA-1 FPKI. CAs that issue SHA-1 end entity certificates after December 31, 2010 may not also issue SHA-256 certificates.

The SHA1 FRCA will only be operated until December 31, 2013. By that time all federal agencies are expected to have fully transitioned to SHA-256.

3.4.4 A-4 E- Governance Certification Authorities (EGCA)

The EGCA supports a variety of NPE credentials. To support the legacy E-Authentication Federation, the EGCA issues OMB M-04-04 level of assurance (LOA) 1 and 2 PKI certificates to approved Credential Service Providers (CSPs) and federal RP systems to enable mutual authentication, and therefore mutual trust. These credentials establish secure communication links between recognized and trusted entities. Since only approved CSP and RP applications have EGCA credentials, the ability for a non-trusted entity to impersonate either identity or intercept the transaction is eliminated.

In addition, the EGCA supports EGTS, which facilitates the use of federated identity in a trusted manner throughout the federal government, and between the federal government and its partners (i.e., other governments, citizens, businesses, and other entities), by issuing eight PKI credentials. These include:

- Four CPs support OMB M-04-04 LOA 1-4 IdPs. IdPs are a new version of a CSP previously defined in the Legacy E-Authentication Federation;

[9] More specifically, the FBCA enables interoperability among Entity PKI domains in a peer-to-peer fashion.

- One CP supports BAE, which is a standard mechanism for RPs to obtain attributes directly from an authoritative source or attribute authority;
- One CP supports RPs that exchange information with IdPs and BAE Brokers[10]; and
- Two CPs support MetaData Signers. Metadata is the primary means of trust within ICAM.

The EGCA is not cross-certified with any other FPKI Trust Infrastructure CA.

[10] RPs are a new version of a agency applications previously defined in the legacy E-Authentication Federation.

Appendix B FPKI Document Summary

Table 2. Summary of FPKI Documents

FPKI Document	Description / Purpose	Maintained By	Link
FPKI Governance Documents			
Charter and Bylaws	Governs how FPKIPA is run.	**FPKIPA**	http://www.idmanagement.gov/fpkipa/documents/fpkipa_charter.pdf
Certificate Policies	Policies governing operation of PKIs operating within the FPKI. Includes polices for FBCA, FCPCA, and EGCA. Each of these CPs define a number of policies and the corresponding CP OIDs.	**CPWG (approved by FPKIPA)**	http://idmanagement.gov/pages.cfm/page/Federal-PKI-Policy-Authority-documentation
Certificate and CRL Profiles	Defines specific parameters for fields in certificates and CRLs issued under FPKI policies.	**CPWG**	http://idmanagement.gov/pages.cfm/page/Federal-PKI-Policy-Authority-documentation
Crits and Methods	Describes the complete process for Cross-certification with FBCA, including maintenance of the cross-certification relationship.	**CPWG**	http://www.idmanagement.gov/fpkima/documents/crosscert_method_criteria.pdf
SSP Roadmap	Describes the complete process for becoming an SSP, including maintenance of the relationship with the FPKI.	**SSPWG**	http://www.idmanagement.gov/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202.pdf
Certificate Practice Statements	Defines how a PKI will meet CP requirements.	**FPKIMA**	http://www.idmanagement.gov/pages.cfm/page/Federal-PKI-Policy-Authority-home-page

FPKI Document	Description / Purpose	Maintained By	Link
Incident Management Process	Describes how the FPKI will respond to incidents that impact or have the potential to impact the FPKI.	**FPKIPA**	http://idmanagement.gov/pages.cfm/page/Federal-PKI
Guidance Documents			
SHA-256 FAQ	Provides additional information about the transition from SHA-1 to SHA-256 within the FPKI.	**FPKIPA**	http://www.idmanagement.gov/fpkipa/documents/FPKI_Community_Transition_SHA256_FAQ.pdf
PIV-I FAQ	Provides additional information about the how PIV-I is used in the FPKI.	**FPKIPA**	http://www.idmanagement.gov/documents/PIV-I_FAQ.pdf
Trust Store Management Guidance	Provides guidance to agencies on proper approaches to trust store management (under development).	**TWG**	http://idmanagement.gov/library.cfm
PIV-I Card Test Plan	Provides information on testing required to become a PIV-I provider (currently under revision).	**FPKIPA**	www.idmanagement.gov/documents/PIVI_Test_Plan.pdf
Triennial Audit Guidelines	Provides guidance on Triennial Audit requirements.	**Audit WG**	http://www.idmanagement.gov/fpkipa/documents/TriennialAnnualAuditGuidance.pdf
Audit Cookbook	Provides specific guidance to navigate through an audit.	**Audit WG**	Appendix D in http://www.idmanagement.gov/fpkipa/documents/TriennialAnnualAuditGuidance.pdf

Appendix C Glossary

Term	Definition
Certificate Policy	A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Authority (CA)	A CA is a trusted entity that issues and revokes public key certificates.
Certification Practice Statement	A statement of the practices that a Certification Authority employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this Certificate Policy).
Cross-certificate	A cross-certificate is used to establish a trust relationship between two certification authorities (CAs).
Cross-certification	The act or process by which two certification authorities (CAs) each certify a public key of the other, issuing a public-key certificate to that other CA.
Federal Public Key Infrastructure (FPKI)	Facilitates secure (trusted) physical and logical access, document sharing, and communications across federal agencies, and between federal agencies and outside bodies such as universities, state and local governments, commercial entities, and other communities of interest. To provide trust services, the FPKI uses a set of digital certificate standards, processes, and a mission-critical Trust Infrastructure to administer certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. It uses a security technique called Public Key Cryptography to authenticate users and data, protect the integrity of transmitted data, and ensure technical non-repudiation and confidentiality.
FPKI Community	The FPKI Community is comprised of federal, industry, and state representatives who work collaboratively to leverage the FPKI, and to provide trust services for the benefit of the federal government.

Term	Definition
FPKI Concept of Operations (ConOps)	High-level description of the functions and processes used by the FPKI to provide trust services (e.g., cross-certification) for the benefit of the federal government.
FPKI Management Authority (FPKIMA)	The FPKIMA manages, operates and manages the FPKI Trust Infrastructure on a day-to-day basis in accordance with the FPKI certificate policies and the certification practice statements approved by the FPKIPA. To operate and maintain the FPKI Trust Infrastructure, the FPKIMA performs the following functions operations, communications with the FPKI Community, testing, helpdesk, and incident response management.
FPKI Policy Authority (FPKIPA)	The FPKPA is the FPKI governing body. It is an interagency body that develops digital certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies, such as universities, state and local governments and commercial entities. It does this by setting policy for the operation of the FPKI while considering the influence, direction, and guidance from external organizations that interact with the FPKI Community.
FPKI Trust Infrastructure	The FPKI Trust Infrastructure consists of six CAs (FBCA, FCPCA, SHA1 FRCA, EGCA CSP2, EGCA RP, and EGCA TS) and the Repository services to support them.[11] All cross-certificates and Certificate Revocation Lists (CRLs) issued by FPKI Trust Infrastructure CAs, and all cross-certificates issued to FPKI Trust Infrastructure CAs are published in the FPKI Trust Infrastructure Repositories.
Identity, Credential and Access Management (ICAM)	Federal imitative to enable trust across organizational, operational, physical, and network boundaries.
Public Key Cryptography	Encryption system that uses a public-private key pair for encryption and/or digital signature.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Subordinate Certification Authority (CA)	A Subordinate CA is a CA in a hierarchical PKI whose certificate signature key is certified by another CA, and whose activities are constrained by the policies of the certifying CA. In the FPKI, SSP CAs are subordinate to the FCPFCA.

[11] The SHA1 FRCA was created to facilitate interoperability for PKIs unable to transition to SHA-256 by January 1, 2011. The SHA1 FRCA will only be operated until December 31, 2013.

Appendix D Acronyms

Acronym	Definition
AIA	Authority Information Access
BAE	Backend Attribute Exchange
C&A	Certification and Accreditation
CA	Certification Authority
CIO	Chief Information Officer
CITE	Community Interoperability Test Environment
ConOps	Concept of Operations
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Credential Service Provider
DAA	Designated Authorizing Official
EAO	Authentication Authorizing Official
EGCA	E-Governance Certification Authorities
EGTS	E-Governance Trust Services
FAQ	Frequent Asked Questions
FBCA	Federal Bridge Certification Authority
FCPCA	Federal Common Policy Certification Authority
FPKI	Federal Public Key Infrastructure
FPKIMA	Federal Public Key Infrastructure Management Authority
FPKIPA	Federal Public Key Infrastructure Policy Authority
FRCA	Federal Root Certification Authority
GAO	Government Accountability Office

Acronym	Definition
GPEA	Government Paperwork Elimination Act
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
HSTC	National Science and Technology Council
ICAM	Identity, Credential and Access Management
ICAMSC	Identity, Credential and Access Management Subcommittee
IdP	Identity Provider
ISIMC	Information and Security &Identity Management Committee
IT	Information Technology
LOA	Letter of Authorization
MOA	Memorandum of Understanding
MSO	Managed Service Office
NIST	National Institute of Standards and Technology
NPE	Non-person Entity
NSS	Network Security Services
OCD	Operational Capabilities Demonstration
OID	Object Identifier
OMB	Office of Management and Budget
PA	Policy Authority
PDVal	Path Discovery and Validation
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification - Interoperable
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure

Acronym	Definition
QVL	Qualified Validation List
RA	Registration Authority
RP	Relying Party
SHA	Secure Hash Algorithm
SSP	Shared Service Provider
SSP WG	Shared Service Provider Working Group
TAG	Technical Advisory Group
TS	Trust Service
TWG	CPWG
WG	Working Group