



Federal Public Key Infrastructure Policy Authority
Charter for Operations

Version 2.2

September 20, 2011

Record of Changes

Date	Version	Change
DD MM YYYY	1.0	Original
09 July 2002	1.1	Non interoperable changes, no affect to current compliant members
10 September 2002	1.2	Changes made to accommodate comments received from FPKIPA participants between 9-28 July 2002
10 February 2004	1.3	Adding information concerning federal agencies using Shared Service Providers
23 March 2004	1.4	Editorial correction to input text in Section 6.1 that was supposed to be part of the changes made for Version 1.3.
08 February 2005	1.5	Changes made to address changes in the FPKIPA voting process, the use of proxies, and the FPKIPA meeting planning standards.
09 August 2005	1.6	Changes made to resolve inconsistencies within the Charter, and with the FPKIPA By-Laws and Operational Procedures and Practices
26 September 2005	1.7	Two new sections (2.2 and 2.3) were added and subsequent sections were re-numbered.
04 October 2005	1.7	Review comments
10 November 2005	1.8	Format and textual emendations per comments
13 December 2005	1.8	Review comments
23 January 2006	1.8	Added voting requirement for re-issuance of a cross-certification (Table 1) and language allowing a member to declare him/herself an <i>ex officio</i> member at any time (3.1.4)
1 March 2006	1.8	Qualifying the voting requirement in Table 1
10 March 2006	1.8	Added new sub-section, 3.1.5
5 April 2006	1.8.1	Added language explaining Charter Membership
27 March 2007	1.9	Modified to reflect changes in Crits & Methods
10 July 2007	2.0	Annual Review and Document Reorganization
6 August 2009	2.1	Annual review and update
3 August 2011	2.2	Annual review and update including removal of references to C4CA and inclusion of references to the E-Governance Trust Services (EGTS).

Table of Contents

1.0 BACKGROUND AND PURPOSE	1
1.1 Background	1
1.2 Purpose	1
2.0 RESPONSIBILITIES OF THE FEDERAL PKI POLICY AUTHORITY	1
2.1 CP/CPS Change And Approval	2
2.2 Approval of Entity Cross-Certification	2
2.3 Maintain Compliance	2
2.4 Agreement With FEDERAL PKI Management Authority	2
2.5 Interoperability Practices	2
2.6 Charter and By-Laws	3
3.0 MEMBERSHIP AND ORGANIZATION	3
3.1 Membership	3
3.1.1 Voting Membership	3
3.1.2 Non-Voting Membership	3
3.1.3 Temporary non-Voting Status for Cross-Certified Agencies	4
3.2 Observers	4
3.3 Committees/Working Groups	5
4.0 OFFICERS	5
4.1 Chair	5
4.2 Secretariat	5
5.0 OPERATIONS	5
5.1 Meetings	5
5.2 Voting	6
5.2.1 Proxies	7
5.2.2 Electronic Voting	7
6.0 CHARTER REVISIONS	7
7.0 NOMENCLATURE	8

1.0 BACKGROUND AND PURPOSE

1.1 BACKGROUND

The Federal Bridge Certification Authority (FBCA) enables discrete Public Key Infrastructures (PKI) to trust digital certificates issued by other entities with which it has been policy-mapped and cross-certified at known Levels of Assurance. The Common Policy CA, cross-certified with the FBCA (as well as the SHA-1 Federal Root CA), serves as the Federal Government's trust anchor and root certification authority for trusted third party providers operating under the Certified PKI Shared Service Provider (SSP) program; and, for those FBCA legacy Entities that have cross-certified with the Common Policy. The E-Governance Trust Services (EGTS) facilitates the use of federated identity throughout the Federal Government and between the Federal Government and external partners. The EGTS includes the E-Governance Certification Authorities (EGCA) and the E-Governance metadata authority. The EGTS is needed to support the backend attribute exchange, identity providers, relying party applications, trusted metadata, and legacy E-Authentication programs.

The Federal Public Key Infrastructure Policy Authority (FPKIPA) is comprised of entities operating enterprise PKIs cross-certified with the FBCA or the Federal Common Policy Framework Certification Authority (FCPCA); or who have acquired PKI services under the SSP Program; and who have demonstrated their interest in participating in the work of the FPKIPA.

1.2 PURPOSE

The FPKIPA sets policy governing operation of the FPKI Trust Infrastructure; approves applicants for cross certification with the FBCA including PIV-I (for non-federal organizations); and provides oversight for the Certified PKI SSP program. It operates under authority of the Identity, Credential, and Access Management (ICAM) Subcommittee (ICAMSC) of the Federal Chief Information Officer (CIO) Council's Information Security and Identity Management Committee (ISIMC). It serves the interest of U.S. Government organizations as relying parties, and promotes interoperability between federal and non-federal entities.

Determinations by the FPKIPA facilitate trust, but do not prescribe the criteria by which relying parties accept digital certificates from external sources for transactions. All entities are free to accept or reject any digital certificate issued by any other entity at their sole discretion, using available FPKIPA determinations to assist in making informed decisions.

2.0 RESPONSIBILITIES OF THE FEDERAL PKI POLICY AUTHORITY

The FPKIPA has the following responsibilities:

2.1 CP/CPS CHANGE AND APPROVAL

- Approving the [FBCA Certificate Policy \(CP\)](#), including revisions
- Approving the [FCPCA CP](#), including its revisions
- Approving the Federal PKI Trust Infrastructure Certification Practices Statements (CPS)

2.2 APPROVAL OF ENTITY CROSS-CERTIFICATION

- Establishing and administering the *Criteria and Methodology for Cross-Certification with the U.S. FBCA* [[CRITS&METHODS](#)] for entities wishing to cross-certify with the FPKI, including the approval of all entity cross-certifications and execution of resultant Memoranda of Agreement (MOA)
- Maintaining the Federal PKI (FPKI) Certification Applicant Requirements (mapping criteria for the FBCA) and the Common Policy CPS Evaluation Matrix to ensure continued accuracy and relevance in relation to the supported policies

2.3 MAINTAIN COMPLIANCE

Maintaining participant compliance with the ongoing requirements of the FPKI, including the determination and execution of remedies and actions for non-compliance and unacceptable risk:

- Ensuring cross-certified entities remain compatible with the FBCA CP (or the FCPCA CP for legacy CAs cross-certified with Common) by implementing the enforcement mechanism in the [[CRITS&METHODS](#)]
- Ensuring cross-certified entities are operationally compliant with their own policies by implementing the enforcement mechanism in the [[CRITS&METHODS](#)]
- Ensuring that Certified SSPs comply with the ongoing requirements for participation including requirements for maintaining compliance as described in the SSP Roadmap
-

2.4 AGREEMENT WITH FEDERAL PKI MANAGEMENT AUTHORITY

Establishing and maintaining a relationship with the Federal PKI Management Authority (FPKIMA), to include:

- Directing the FPKIMA concerning the issuance and revocation of cross-certificates
- Ensuring the FPKIMA continuing adherence to the FPKI Certificate Policies
- Providing documentation to the FPKIMA for archival

2.5 INTEROPERABILITY PRACTICES

Coordinating legal, policy, technical, and business practices and issues related to FPKI Trust Infrastructure interoperability.

2.6 CHARTER AND BY-LAWS

Establishing and maintaining a charter and bylaws for its own operations.

3.0 MEMBERSHIP AND ORGANIZATION

3.1 MEMBERSHIP

Membership in the FPKIPA is open to federal agencies that have cross-certified with the FBCA or FCPCA, federal agencies using PKI certificate services acquired through an approved SSP, cross-certified non-governmental PKIs and PKI bridges, and ex officio members as designated in Section 3.1.2.1.

Where the federal agency administering the PKI is a subordinate entity of either a Cabinet-level department or an independent entity of comparable stature, membership shall be vested in the superior organization, unless otherwise determined by the department or agency. It is intended that there will be one voting member per department or agency.

Membership terminates if and when the Entity ceases to operate its cross-certified CA or PKI shared service provider model or chooses not to participate in the FPKIPA.

3.1.1 Voting Membership

Voting membership on the FPKIPA is reserved for federal entities as follows:

3.1.1.1 FPKI Cross-Certified Federal Entities

All federal agencies, independent commissions and organizations that operate self-signed PKIs that have successfully completed the process of cross-certifying with the FPKI Trust Infrastructure in accordance with the [[CRITS&METHODS](#)] are eligible to be voting members of the FPKIPA.

3.1.1.2 Agencies Acquiring Certificate Services through a Certified PKI SSP

Federal agencies acquiring PKI certificate services from a Certified PKI SSP are eligible to be voting members of the FPKIPA.

3.1.1.3 General Criteria for All Voting Members

Voting membership in the FPKIPA for eligible federal entities is granted and maintained under the following circumstances:

- a) The agency expresses a desire to become a new voting member of the FPKIPA by submitting an application for membership
- b) The agency makes the requisite commitment of time and resources as evidenced by regular FPKIPA and working group participation

3.1.2 Non-Voting Membership

3.1.2.1 Shared Service Providers (SSPs)

Providers of cross-certified PKI certificate services to federal and non-federal organizations are recognized and included under the

FPKI trust infrastructure through the Certified PKI SSP and non-federal SSP programs; however, an SSP is a non-voting member unless it also meets the criteria for voting membership. The opinions and counsel of SSP members on issues before the FPKIPA are sought and considered prior to a vote.

3.1.2.2 Ex Officio Membership

The following have ex officio membership:

- (1) Co-chairs of the ICAMSC and ISIMC
- (2) Program Manager, FPKIMA
- (3) Office of Management and Budget (OMB)

Ex officio membership does not confer voting privileges. However, the opinions of ex officio members are valued by the FPKIPA and considered prior to vote. In addition, ex officio members are welcome to participate on working groups and subcommittees at their discretion.

3.1.2.3 Non-Federal Entities

Non-federal PKIs and PKI bridges that cross-certify with the FBCA (including PIV-I cross certification) and/or the FCPCA through the procedures described in [\[CRITS&METHODS\]](#) are non-voting members. Their opinions on issues under consideration by the FPKIPA are valued and considered prior to vote. Non-voting, cross-certified members are encouraged to provide representatives to the FPKI Certificate Policy Working Group (CPWG).

3.1.3 Temporary non-Voting Status for Cross-Certified Agencies

Agencies that do not satisfy Federal PKI annual audit requirements, or who allow their cross-certificates to expire, will have their voting privileges temporarily suspended.

An agency may voluntarily place itself in this status prior to the date that either of these events occurs, or the FPKIPA Chair shall notify the agency that they have been involuntarily placed in this status after the respective dates.

An agency may return to full voting membership whenever the circumstances that led to suspension have been resolved.

3.2 OBSERVERS

The FPKIPA recognizes the following organizations as Observers:

- Members of the ICAMSC and ISIMC
- Members of other Bridges cross-certified with the FBCA
- Organizations whose application for cross-certification are under consideration
- Certified PKI SSP and, non-federal PKIs cross-certified with the FBCA
- Other entities invited at the discretion of the FPKIPA Chair.

The FPKIPA will identify those activities not open to Observer participation.

Observers do not have voting privileges on the FPKIPA.

3.3 COMMITTEES/WORKING GROUPS

The FPKIPA may create, participate in, or have temporary or permanent subordinate committees or working groups to support its policy and technical activities.

4.0 OFFICERS

4.1 CHAIR

The FPKIPA shall have a Chair selected by majority vote of the voting membership. The FPKIPA Chair must be a federal employee from a voting member organization of the FPKIPA and shall serve a two-year term. A sitting Chair may, by a majority vote, be allowed to hold the position for additional two-year terms. However, voting members shall be given 30 days in which to nominate a different candidate prior to expiration of the current term.

The Chair shall designate an alternate to perform the functions of this office in his or her absence.

The Chair may step down. In doing so, the Chair shall give at least 60-days notice, except in emergency situations, in which case the Chair shall designate an interim replacement to perform the functions of this office until an emergency election can be held. Such emergency elections shall be held as soon as practicable following the effective date of the outgoing Chairperson's resignation.

The Chair shall, at a minimum, be responsible for:

- Chairing FPKIPA meetings
- Directing and coordinating all FPKI activities
- Promoting the use of PKI to serve the interests of the Federal Government
- Representing the FPKIPA to other organizations, including international organizations

4.2 SECRETARIAT

The FPKIPA shall have a Secretariat. The Secretariat shall record, seek the Chair's approval and distribute agendas, documents for review, and the minutes of all FPKIPA meetings to participants, and be responsible to the Chair for all administrative matters.

5.0 OPERATIONS

5.1 MEETINGS

FPKIPA meetings shall be held on a regular schedule as determined by the FPKIPA. The Chair or, in his or her absence, the designated alternate, shall

Federal Public Key Infrastructure Policy Authority Charter for Operations

preside over all meetings and votes. The standard meeting date is the second Tuesday of each month from 9:30 a.m. to 12:00 p.m. The meeting time and location maybe modified when situation dictates.

At least five business days' prior public notice shall be given for all FPKIPA meetings. FPKIPA meeting documentation shall be emailed to all FPKIPA members at least five working days' in advance of the regularly scheduled FPKIPA meeting.

The quorum necessary for the FPKIPA to transact official business shall be two-thirds (2/3) of the voting membership. A transmitted proxy to an attending member shall also count towards a quorum. The FPKIPA may meet to discuss business without a quorum; however, formal decisions shall not arise from such a meeting.

5.2 VOTING

Voting maybe performed at a FPKIPA meeting, or through remote means (teleconferencing, e-mail, or letter). Each member is expected to cast a vote, except when recusal is necessary owing to a conflict of interest.

Voting members must be federal employees.

Members failing to vote when a vote is called shall be recorded as "Absent." If as a result, the final vote tally, including proxies, lacks a quorum, the vote will be rescheduled.

All members will be given five business days' notification before any vote is to be called, except in case of an emergency or after a discussion at a FPKIPA meeting. All votes shall be recorded and the results of voting will be published in the minutes of the FPKIPA meetings.

Table 1--Required Majorities

Action Requiring FPKIPA Vote	Votes Needed for Passage
1. Approve FPKIPA meeting minutes.	Majority of votes cast
2. Approve FPKIPA Charter revisions.	75% majority of all voting members
3. Approve FPKI Certificate Policies and changes.	75% majority of all voting members
4. Approve FPKI CPS and changes.	75% majority of all voting members
5. Approve FBCA, PIV-I Non Federal Issuer (NFI), and FCPCA Application.	Majority of votes cast
6. Elect FPKIPA Chair.	Majority of all voting members
7. Establish subordinate committees/work groups.	Majority of votes cast
8. Vote to revoke cross-certificates for non-administrative circumstances. (FBCA CP § 4.9.3)	75% Majority of votes cast

Action Requiring FPKIPA Vote	Votes Needed for Passage
9. Approval of Entity Cross Certification, including: a. Policy Mapping; b. Operational Parameters (“white space”) mapping; c. Compliance Audits; d. Interoperability testing; and e. MOA	75% majority of votes cast
10. Approval of Guidance Documents.	Majority of votes cast
11. Determination of remedies/actions to be taken for CP, CPS noncompliance.	75% majority of all voting members
12. Determination of remedies/actions to be taken for unacceptable risk.	75% majority of all voting members
13. Determination to restore FBCA interoperability following cross-certificate revocation.	75% majority of votes cast
14. Vote to re-issue a member’s cross-certification*.	75% majority of votes cast
15. Vote to reinstate a member’s voting privileges.	75% majority of votes cast

*A vote to re-issue a member’s cross-certificate is required only under extraordinary circumstances and for cause as determined by the FPKIPA. Routine reissuance of cross-certificates does not require a vote.

5.2.1 Proxies

A member may grant a voting proxy to another voting member, to another federal employee in their agency, or to the FPKIPA Chair. The proxy must specify whether it is for a particular issue or is a blanket proxy; and whether it is for a single meeting or remains valid until revoked in writing.

Proxies may be submitted to the Chair, to another federal employee in their agency, or to the designated member. The proxy must be presented to the Secretariat and to FPKIPA Chair prior to any vote in which the proxy is used.

If the voting member who issued the proxy is present at the covered or subsequent meeting, he or she may revoke the proxy by informing the Chair and the Secretary in open session. If a voting member is not present and has not provided a proxy, the vote shall show that the member is absent.

5.2.2 Electronic Voting

When a member votes by electronic means (e.g., email), the electronic vote shall be signed to indicate the member’s intent to vote and confirm that member’s identity. The electronic vote shall contain a valid PKI digital signature. Failure to use the above methods shall cause the electronic vote to be considered invalid and not counted in the tally.

6.0 CHARTER REVISIONS

The FPKIPA shall review this Charter bi-annually, and shall update it as often as necessary. The bi-annual review should preferably begin in January of each year, but in no case later than the regularly scheduled meeting in March. Once approved changes have been accepted, the “Record of Changes” section of this document will reflect the date, revision, and changes accepted for historical tracking of this living document.

7.0 NOMENCLATURE

PKI Certificate Services

Any or all aspects of the digital certificate life-cycle management of a PKI.

Vendor

Within the context of this document, any commercial entity that provides PKI certificate services for a fee.

[Federal] Agency

Any independent federal government entity as defined in 5 U.S.C. § 105. It shall include legislative and judicial branch agencies.

Applicant

Any organization that has applied for cross-certification with the FBCA or subordination to the FCPCA .

Representative

The person (primary or alternate) who has been chosen by an entity to attend meetings of the FPKIPA as a Member or Observer.

Voting member

Any federal organization that has been determined to be eligible to vote on FPKIPA matters as set forth in Section 3.1.1

Ex Officio member

The non-voting members of the FPKIPA as set forth in Section 3.1.2.1.

Observer

Any entity that has been approved by the FPKIPA to attend its meetings, as set forth in Section 3.2, or contractor support to any Voting, *Ex Officio*, or Observer entity.