



# **Federal PKI Policy Authority**

## **Charter For Operations**



## *Table of Contents*

|   |           |
|---|-----------|
| <b>1.0 BACKGROUND AND PURPOSE</b> .....   | <b>4</b>  |
| 1.1 FEDERAL PUBLIC KEY INFRASTRUCTURE POLICY AUTHORITY (FPKI POLICY AUTHORITY)..... | 4         |
| 1.2 FPKI POLICY AUTHORITY MISSION .....   | 4         |
| <b>2.0 RESPONSIBILITIES OF THE POLICY AUTHORITY</b> .....                           | <b>4</b>  |
| 2.1 CP/CPS CHANGE APPROVAL PROCESS .....  | 4         |
| 2.2 AGREEMENT WITH FBCA OPERATIONAL AUTHORITY .....                                 | 5         |
| 2.3 BUSINESS ISSUES .....   | 5         |
| 2.4 BYLAWS .....  | 5         |
| <b>3.0 MEMBERSHIP AND ORGANIZATION</b> .....  | <b>5</b>  |
| 3.1 MEMBERSHIP .....  | 5         |
| 3.1.1 <i>Charter membership</i> .....   | 5         |
| 3.1.2 <i>Cross certified Agency membership</i> .....                                | 5         |
| 3.1.3 <i>Ex Officio membership (non-voting)</i> .....                               | 6         |
| 3.2 OBSERVERS .....   | 6         |
| 3.3 COMMITTEES/WORKING GROUPS.....  | 7         |
| <b>4.0 OFFICERS</b> .....   | <b>7</b>  |
| 4.1 CHAIR .....   | 7         |
| 4.2 SECRETARY .....   | 7         |
| <b>5.0 OPERATIONS</b> .....   | <b>7</b>  |
| 5.1 MEETINGS .....  | 7         |
| 5.2 VOTING .....  | 7         |
| <b>ACTION REQUIRING FPKIPA VOTE</b> .....   | <b>8</b>  |
| <b>6.0 APPLICATION FOR INTEROPERATION WITH THE FBCA</b> .....                       | <b>9</b>  |
| 6.1 PROCEDURES .....  | 9         |
| 6.2 APPLICATIONS .....  | 9         |
| 6.2.1 <i>APPLICATION APPROVED, WITH NO CHANGES REQUIRED</i> .....                   | 10        |
| 6.2.2 <i>APPLICATION APPROVED, WITH CHANGES REQUIRED</i> .....                      | 10        |
| 6.2.3 <i>APPLICATION REJECTED</i> .....   | 10        |
| 6.3 NON-COMPLIANCE .....  | 10        |
| <b>7.0 CHARTER REVISIONS</b> .....  | <b>10</b> |
| <b>8.0 NOMENCLATURE</b> .....   | <b>11</b> |
| 8.1 “ORGANIZATION” .....  | 11        |
| 8.2 “APPLICANT” .....   | 11        |
| 8.3 “REPRESENTATIVE” .....  | 11        |
| 8.4 “VOTING MEMBER” .....   | 11        |
| 8.5 “CHARTER MEMBER” .....  | 11        |
| 8.6 “EX OFFICIO MEMBER” .....   | 11        |
| 8.7 “OBSERVER” .....  | 11        |

# Charter

## 1.0 BACKGROUND AND PURPOSE

### 1.1 FEDERAL PUBLIC KEY INFRASTRUCTURE POLICY AUTHORITY (FPKI POLICY AUTHORITY)

The Federal Public Key Infrastructure Policy Authority (FPKI Policy Authority) sets policy governing operation of the Federal Bridge Certification Authority (FBCA), and approves applicants for cross certification with the FBCA.

The FBCA allows discrete Public Key Infrastructures (PKI) to trust digital certificates issued by other entities that have been policy mapped and cross-certified with the FBCA.

The FPKI Policy Authority was created under the Federal CIO Council (and operates under the Architecture and Infrastructure Committee,) pursuant to Federal CIO Council authority. It serves the interest of U.S. Government organizations as relying parties, but does not prohibit interoperability among Non-Federal entities.

### 1.2 FPKI POLICY AUTHORITY MISSION

The FPKI Policy Authority is composed of organizations that wish to interoperate and exchange digital certificates that have been signed by their Certification Authority with the FBCA.

Determinations by the FPKI Policy Authority apply to the issuance of cross-certificates to approved participants but does not prescribe how those entities are to rely on digital certificates for transactions; all entities are free to accept or reject any digital certificate issued by any other entity at their sole discretion, using available FPKI Policy Authority determinations to assist in making informed decisions.

## 2.0 RESPONSIBILITIES OF THE POLICY AUTHORITY

The FPKI Policy Authority has the following responsibilities:

### 2.1 CP/CPS CHANGE APPROVAL PROCESS

Approving the FBCA Certificate Policy (CP) and Certification Practice Statement (CPS), including their revisions.

## **2.2 AGREEMENT WITH FBCA OPERATIONAL AUTHORITY**

Entering into an agreement with a government organization to operate the FBCA on behalf of the FPKI Policy Authority and its oversight bodies. This organization that operates the FBCA is referred to as the FBCA Operational Authority (FBCA OA). The agreement establishes that:

- (a) The FBCA OA will issue or revoke cross-certificates with Federal organizations, State, Local, Foreign Governments or private entities when and as directed by the FPKI Policy Authority; and
- (b) The FPKI Policy Authority may review FBCA OA activities for compliance with the FBCA Certificate Policy and Certification Practice Statement.

## **2.3 BUSINESS ISSUES**

Coordinating legal, policy, technical and business practices and issues related to FBCA interoperability.

## **2.4 BYLAWS**

Establishing and maintaining bylaws for its own operations.

## **3.0 MEMBERSHIP AND ORGANIZATION**

### **3.1 MEMBERSHIP**

Membership in the FPKI Policy Authority is limited to Federal Executive Branch agencies that have cross-certified with the Federal Bridge, Federal Executive Branch agencies using PKI services provided by vendors participating in approved, cross-certified Service Provider programs, the designated charter members, and ex officio members as designated in Section 3.1.3.

#### **3.1.1 Charter membership**

The following Federal organizations shall have Charter membership in the FPKI Policy Authority and be granted representation into the Certificate Policy Working Group, if desired:

1. Office of Management and Budget,
2. Department of Justice,
3. General Services Administration,
4. Department of the Treasury,
5. Department of Defense, and
6. Department of Commerce.

#### **3.1.2 Cross certified Agency membership**

Membership is also granted to Federal Executive Branch organizations authorized to cross certify with the FBCA in accordance with Section 6. This grants voting privileges for that organization in the FPKI Policy Authority.

Where the Federal Applicant administering the PKI is a subordinate entity of either a Cabinet-level Department or an independent entity of comparable stature as set forth in Section 8 below, Membership shall be vested in the superior organization, unless otherwise determined by the Department or Agency. Membership terminates if and when interoperation with the FBCA is terminated, for any reason.

#### 3.1.2.1 Agencies Acquiring Certificate Services from Service Providers Cross Certified with the FBCA

Vendors providing PKI certificate services are recognized and included under the e-Authentication architecture umbrella and the Common Policy Framework through both the GSA ACES program (Federal Employee Profile) and the Common Federal Policy Shared Service Provider program. In addition, some certificate service providers have themselves cross-certified with the Federal Bridge CA. Federal Agencies acquiring PKI certificate services using any of these mechanisms are eligible for voting membership on the PA under the following circumstances:

1. The Agency expresses a desire to be a voting member of the PA, evidenced by completion of an application for membership and submission of relevant documentation for review, as described below.
2. The Agency operates its own Registration Authority, with its own certification practices statement for the registration function.
3. The Agency maintains a policy management functionality that includes, but does not have to be limited to, authorizing and reviewing an independent, third party audit of the policies, procedures and operations of its RA functions in conformance with the Certificate Policy of the service provider.

#### 3.1.3 Ex Officio membership (non-voting)

The following FPKI Organizations shall have ex officio membership: the Chair of the Federal Identity Credentialing Committee, and the FBCA Operational Authority Project Manager. Ex Officio membership does not have voting privileges.

### 3.2 OBSERVERS

The FPKI Policy Authority recognizes the following organizations as Observers:

- Members of the Federal Identity Credentialing Committee;
- Entities that have cross certified with the FBCA;
- Organizations whose application for cross certification is under consideration; and
- Other entities at the discretion of the FPKI Policy Authority.

The FPKI Policy Authority will permit Observers to participate in all activities, except for specifically designated members-only activities.

### **3.3 COMMITTEES/WORKING GROUPS**

The FPKI Policy Authority may create or have temporary or permanent subordinate committees or working groups as determined by a vote of the membership, to incorporate comments and support for operation of the FBCA.

## **4.0 OFFICERS**

### **4.1 CHAIR**

The FPKI Policy Authority shall have a Chair selected by majority vote of the membership and approved by the Chair of the Architecture and Infrastructure Committee of the CIO Council. The FPKI Policy Authority Chair shall serve a two-year term. The Chair may designate an alternate to perform the functions of this office in their absence.

### **4.2 SECRETARY**

The FPKI Policy Authority shall have a Secretary appointed by the Chair. The Secretary shall record minutes of all FPKI Policy Authority meetings and be responsible for administrative matters.

## **5.0 OPERATIONS**

### **5.1 MEETINGS**

FPKI Policy Authority meetings shall be held on a regular schedule as determined by the FPKI Policy Authority Chair. The Chair or, in his or her absence, the designated alternate, shall preside over all meetings and votes.

### **5.2 VOTING**

Voting may be performed at a FPKI Policy Authority meeting, or through remote means (teleconferencing, e-mail, or letter). A Member may grant a proxy voting status to another Member or to the FPKI Policy Authority Chair. Each Member shall be required to cast a vote, except when recusal is necessary owing to a conflict of interest.

Charter members shall not vote upon their own application for cross certification with the FBCA. Failure of a voting member to vote during the scheduled voting period will automatically grant that Member's proxy to the FPKI Policy Authority Chair.

All members will be given reasonable notification before any vote is to be called, all votes shall be recorded, and the results of voting will be published.

| Action Requiring FPKIPA Vote   | Votes Needed for Passage                                     |
|--|--|
| 1. Approve FPKIPA meeting minutes.   | majority   |
| 2. Approve FPKIPA Charter revisions.   | 75% majority   |
| 3. Approve FBCA Certificate Policy and changes.  | 75% majority   |
| 4. Approve FBCA CPS and changes.   | 75% majority   |
| 5. Approve FPKIPA CP Plan. (FBCA CP s.8.1)   | 75% majority   |
| 6. Approve FBCA OA Operating Agreement. (Charter)  | majority   |
| 7. Approve FBCA Application and process  | majority   |
| 8. Elect FPKIPA Chair, Vice-Chair  | majority   |
| 9. Establish subordinate committees/work groups  | majority   |
| 10. Approve FPKIPA procedures for actions/remedies to address non-compliance. (CP s.2.7.5)   | majority   |
| 11. Directions to FBCA OA to revoke FBCA certificates. (CP s.4.4.1.2)  | 75% majority   |
| 12. Requests to external organizations for input/review of Agency Interoperability Applications.   | Majority   |
| 13. Following recommendations from Application Interoperability Review Committee:<br>a. Referral back to Committee for further review.<br>b. Referral to external organization for review. | majority<br>majority   |
| 14. Acceptance of Entity Cross Certification Application   | majority   |
| 15. Approval of Entity Cross Certification, including:<br>a. Policy Mapping;<br>b. Compliance Audits;<br>c. Interoperability testing; and<br>d. Memorandum of Agreement.                   | 75% majority<br>75% majority<br>75% majority<br>75% majority |
| 16. Determination of remedies/actions to be taken for CP, CPS noncompliance.   | 75% majority   |
| 17. Determination of remedies/actions to be taken for unacceptable risk.   | 75% majority   |
| 18. Determination to restore FBCA interoperability following cross-cert revocation   | 75% majority   |
| 19. Fee Assessment (CP s.2.5)<br>a. Amount<br>b. Fee mechanism   | 75% majority<br>75% majority                                 |

## **6.0 APPLICATION FOR INTEROPERATION WITH THE FBCA**

### **6.1 PROCEDURES**

The FPKI Policy Authority shall develop and maintain application procedures to be used by Entities wishing to apply for interoperability with the FBCA. This completed application form covers:

- (a) How the Applicant proposes to map its Principal CA Certificate Policy to the FBCA Certificate Policy respecting certificate levels of assurance, security, and trust. In the case of an Agency acquiring certificate services from a recognized provider (see 3.1.2.1), the Applicant must show how it proposes to map its RA functions to the FBCA Certificate Policy or the X.509 Certificate Policy for the Common Policy Framework; and
- (b) What duties the Applicant will have if it is accepted for interoperability with the FBCA, expressed in the form of a Memorandum of Agreement (MOA) between the FPKI Policy Authority and the Applicant.

### **6.2 APPLICATIONS**

Upon receipt of an application form, the FPKI Policy Authority shall determine whether this application is in the interest of the Federal Government. If accepted, the FPKI Policy Authority, or its delegates, shall perform the following actions:

- Review the applicant's Certificate Policy, or RA Policy addendum, in the case of an Applicant acquiring services through a recognized provider (see 3.1.2.1), to determine an appropriate policy mapping with the FBCA Certificate Policy or the X.509 Certificate Policy for the Common Policy Framework;
- Review the applicant Compliance audit, or in the case of an Applicant acquiring services through a recognized provider (see 3.1.2.1), review the applicant RA function compliance audit to verify the applicant's PKI is operated in accordance with a suitable Certification Practice Statement;
- Perform interoperability testing; and
- Establish a memorandum of agreement between the Applicant and the FPKI Policy Authority.

Upon completion of these actions, the FPKI Policy Authority shall make a determination, from the following choices:

1. Approve it, with no changes required,
2. Approve it, with changes required (such as a different policy mapping or assurance level than proposed in the applicant), or
3. Reject it, for reasons stated in a formal FPKI Policy Authority response.

#### **6.2.1 APPLICATION APPROVED, WITH NO CHANGES REQUIRED**

If the application is approved without changes, the Applicant and the FPKI Policy Authority Chair shall mutually sign the Memorandum of Agreement (MOA) for this relationship. Then the FPKI Policy Authority Chair shall instruct the FBCA Operational Authority, in writing, to issue a cross certificate to the applicant PKI.

#### **6.2.2 APPLICATION APPROVED, WITH CHANGES REQUIRED**

If the application is approved but with changes required by the FPKI Policy Authority, the Applicant will be apprised of the discrepancies or issues, and if they agree with the proposed or expanded changes, the process in 6.2.1 shall be followed.

#### **6.2.3 APPLICATION REJECTED**

If the application is rejected, the FPKI Policy Authority shall apprise the Applicant of the reasons for the rejection. The Applicant may then decide to address these issues and revise its application and re-apply without prejudice, if desirable.

### **6.3 NON-COMPLIANCE**

If an entity that has cross-certified with the FBCA is found to be or admits that it is in noncompliance with the MOA, the FPKI Policy Authority shall terminate interoperability and notify the entity. The Applicant in question shall have full access to, and ample opportunity to, participate in these deliberations, and may be issued a new cross certificate after taking corrective actions.

## **7.0 CHARTER REVISIONS**

Revisions to this Charter may be made upon at least a 75% majority vote of the voting membership, with each agency having one vote. 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.

## **8.0 NOMENCLATURE**

### **8.1 “ORGANIZATION”**

Any Executive or Federal Agency as defined in 5 U.S.C. § 105. It shall include independent executive departments, but not subordinate elements within an Agency.

### **8.2 “APPLICANT”**

Any entity that has applied for membership or interoperability with the FBCA.

### **8.3 “REPRESENTATIVE”**

The person (primary or alternate) who has been chosen by an organization to attend meetings of the FPKI Policy Authority as a Member or Observer.

### **8.4 “VOTING MEMBER”**

Any Federal organization that has been determined to be eligible to vote on FPKI Policy Authority or FBCA matters as set forth in Section 3.1.

### **8.5 “CHARTER MEMBER”**

The initial members of the FPKI Policy Authority as set forth in Section 3.1.2.

### **8.6 “EX OFFICIO MEMBER”**

The non-voting members of the FPKI Policy Authority as set forth in Section 3.1.3.

### **8.7 “OBSERVER”**

Any entity that has been approved by the FPKI Policy Authority to attend its meetings, as set forth in Section 3.2.