Federal Public Key Infrastructure Policy Authority Charter

Version 2.0

August 2021

Name

Federal Public Key Infrastructure Policy Authority

Background

In 2002, the Federal Public Key Infrastructure (FPKI) Policy Authority (PA) was created by the Federal Chief Information Officers (CIO) Council to serve as the Federal Public Key Infrastructure governance body.

The FPKI is the Federal trust framework for a set of PKI systems, certification authorities (CAs), and associated digital x509 certificates used for federated trust and mission delivery purposes.

The FPKI is comprised of technologies, policies, and personnel from the following entities:

- US Federal Government Departments and Agencies
- commercial Shared Service Providers (SSPs) operating PKI services on behalf of US Federal Government Departments and Agencies
- external PKI providers (referred to as “affiliates”).

The FPKI provides services that directly benefit federal agency mission needs and objectives. It encompasses the Federal Government's trust model for the Personal Identity Verification (PIV) credential, PIV-Interoperable (PIV-I) credential, and other PKI-based credentials for persons and devices.

As a result, the FPKI is essential for federal agency physical and logical access solutions.

Purpose

The purpose of the PA is to serve the interests of the US Federal Government.

The PA is a group of representatives from US Federal Government Departments and Agencies. A subset of these representatives have voting privileges as described in this charter and are collectively responsible for managing the policies governing the FPKI trust framework and approving or denying entities for certification into the trust framework. Certification into the trust framework is represented by the issuance of a digital x509 certificate, known as a cross-certificate.

The General Services Administration (GSA) Office of Government-wide Policy (OGP) provides the PA with secretariat support and oversight of the federally funded annual review and certification procedures. GSA OGP funds these activities via appropriations to GSA.

The GSA’s Federal Acquisition Services (FAS) operates the Management Authority program. The FPKI Management Authority (MA) operates and manages the CA systems that comprise the FPKI root certification authorities (Federal Common Policy CAs) and bridge certification authorities (Federal Bridge CAs) for the participating US Federal Government Departments and Agencies. The MA manages, issues, and revokes CA certificates as approved by the PA.

Authority

The PA operates under authority of the Federal Chief Information Security Officer Council (CISO Council) through the Identity, Credential, and Access Management Subcommittee (ICAMSC).

The PA and the FPKI support the following US Government policies and standards:

- Homeland Security Presidential Directive 12 (HSPD-12)
- Federal Information Processing Standard (FIPS) 201
- Office of Management and Budget Memorandum 19-17
- Office of Management and Budget Circular A-130
- E-Government Act of 2002
- Government Paperwork Elimination Act

The CISO Council, ICAMSC, or its assignee approves this charter and oversees responsibilities, work plans, and priorities.

Responsibilities

The PA has the following responsibilities:

Certificate Policy Management

- Approving FPKI Certificate Policies (CP), including revisions
- Approving FPKI Certification Practice Statements (CPS), including revisions
- Approving the criteria and methodologies used for cross-certification and other related requirements documents
- Creating, managing, and approving or denying change requests for FPKI artifacts
- Executing and maintaining all related Memorandums of Agreement (MOA)

Cross-Certification

- Establishing and administering the documented criteria for FPKI members and affiliates with a government mission need to be cross-certified by the FPKI
- Assessing government business cases, including the needs, costs, risks, and delegations of authority for approving an entity's PKI admission into the trust framework
- Evaluating comparability between FPKI CPs and those belonging to cross-certified entities and applicants for cross-certification
- Coordinating legal, policy, technical, and business practices and issues to facilitate government-wide PKI interoperability

Compliance

- Performing an initial and subsequent reviews of certified entities to ensure ongoing compliance or comparability with applicable FPKI requirements

Agreement with Federal PKI Management Authority

Establishing and maintaining a relationship with the FPKI Management Authority, to include:

- Authorizing CA certificate issuance and revocation activities for the Federal Common Policy CA and Federal Bridge CA
- Ensuring operation and maintenance of the Federal Common Policy CA and Federal Bridge CA in accordance with the CPs and CPSs
- Submitting documentation to the appropriate archives.

Leadership

There shall be three standing co-chairs. Co-chair role appointments will be affirmed biennially on February 1st.

Co-chairs are the following, all of whom must be federal employees with sufficient experience and program management knowledge of PKI, Key Management, or Identity Credential and Access Management (ICAM).

General Services Administration, Office of Government-wide Policy, Identity and Trusted Access Division Co-chair

A representative named by the GSA OGP Associate Administrator to provide:

- Oversight of the secretariat processes and federally funded annual review and certification procedures, to ensure efficient, effective and fiscally responsible execution in the best interests of government
- Insight into the policies, standards and delegations of authority for the PA, and other complementary federal enterprise cross-government sub-committees and communities of practices
- Communication of perspectives from non-CFO Act[1] agencies not represented by active voting members, including agency concerns and impacts on mission operations
- Policy and impact analysis support for proposed changes to certificate policies, practices, and procedures impacting federal IT

Department of Defense Co-chair

A Department of Defense representative nominated by the DoD ICAM Joint Program Integration Office, and approved by the DoD CIO and CISO Council or ICAMSC, to provide:

[1] Agencies, commissions and boards

- Insight into the technology and government wide standards to advance cross-government, efficient and effective procedures for issuance and acceptance of common PIV / CAC credentials between executive branch civilian agencies and defense agencies
- Insight into the policies, standards and delegations of authority for the PA, and other complementary federal enterprise cross-government sub-committees and communities of practices

At-Large Agency Co-chair

A representative from a US Federal Government Department or Agency outside of GSA and DoD, nominated by the Policy Authority, sponsored by their Agency CIO, and approved by the CISO Council or ICAMSC to provide:

- Additional agency perspectives, including agency issues and impacts on mission operations
- Technical subject matter expertise related to PKI, Key Management, or Identity Credential and Access Management (ICAM)

The term of the At-Large Agency Co-chair will be two years. If uncontested at the end of the two-year term, the At-Large Agency Co-chair may serve consecutive term(s) upon approval by PA voting members.

Co-chair Responsibilities

PA co-chairs shall be responsible for:

- Chairing PA meetings
- Ensuring the PA adheres to its approved responsibilities, delegations of authority, work plans, and priorities
- Signatory executor, on behalf of the PA, of all PA documents such as Certificate Policies, Memorandums of Agreement, and authorizations for certificate actions by the Management Authority
- Informing the CISO Council, ICAMSC, or its designees of PA activity, work plans, and priorities
- Recommending actions to be taken to maintain compliance with government wide statutes, policies, and standards for the PA to adhere to delegations of authority
- Recommending actions to be taken for noncompliance or unacceptable risk, or to restore FPKI interoperability following CA certificate revocation of an entity's certification authority systems
- Authorizing re-issuance of an entity's member's CA certification under extraordinary circumstances
- Sending compliance audit letter notifications

Membership

There are three categories of participants:

- Voting members
- Ex-officio members
- Observers

Voting membership for the PA is reserved for federal departments and agencies. All other participants are non-voting.

Voting Members

All federal departments, agencies, boards and commissions may designate a voting member representative and an alternate designee representative.

Only federal members vote. Federal agency voting members and alternate designee representatives must be federal employees.

Federal agency voting and alternate designee representatives shall be designated by their respective agency Chief Information Officer, Chief Information Security Officer, or similarly titled senior agency official(s) with delegated authorities for Information Technology and Information Security.

A Policy Authority co-chair may be designated by their agency to serve as a voting member. Regardless, each agency shall be represented by only one vote.

Voting members have the following responsibilities:

- Attending PA meetings or sending the alternate designee;
- Coordinating feedback and consensus among internal agency stakeholders;
- Designating personnel with the appropriate functional and technical knowledge to support working activities;
- Driving actions and activities stemming from PA decisions at their agency; and
- Acting as an authorized representative of their agency to vote (as permitted) on PA issues, actions, and deliverables.

Membership terminates when a member withdraws for any reason, fails to meet its membership responsibilities, or chooses not to participate in the PA.

Voting membership may be suspended for any organization that does not fulfill its meeting attendance obligations and fails to name a proxy for three consecutive meetings.

Ex-Officio Members

The following federal offices and / or members receive materials and notifications, and may attend all meetings, but do not have voting rights:

- Office of Management and Budget, Office of the Federal CIO representatives
- National Institutes of Standards and Technology, Computer Security Division representatives
- CISO council members and representatives
- ICAM Sub-committee co-chairs and representatives
- Federal PKI Management Authority program manager(s)
- Others as designated by the PA co-chairs or by quorum of the voting members

The PA shall seek and consider the opinions and counsel of ex-officio members prior to a vote.

Observer(s)

The following participants may receive materials and notifications, and may attend meetings as determined by the PA, but do not have voting rights:

- Commercial SSPs and affiliates with a signed agreement with the Federal PKI Policy Authority, or certified by a Federal PKI
- Third-party or internal government PKI compliance auditors

Procedures

Meetings

PA meetings shall be held on a regular schedule as specified by the PA co-chairs and agreed upon by the voting members. Meeting time and location may be modified as needed.

A quorum of two-thirds (2/3) of the voting membership is required for the PA to transact official business. A proxy to an attending member shall count toward a quorum. The FPKI PA Support Team maintains a record of the voting membership and ensures quorum requirements are satisfied for all votes.

The PA co-chairs or federal agency voting member representatives will identify meetings, discussions or voting activities not open to Observer, contractor, contracted personnel, or non-government participation.

Working Groups

The PA has the authority to establish working groups, or other bodies as necessary, to support its responsibilities, work plans, and priorities. Participation in working groups may include a broader set of participants such as representatives of other federal agency committees or councils and support contractors.

New working groups shall be chartered with a defined scope, expected outcomes and work products, participation requirements, expected time contributions, and timelines.

Prior to establishing new working groups, the PA co-chairs, voting members and ex-officio members shall research needs and coordinate with representatives of other federal agency committees or councils. It is in the best interests of the government and the public to coordinate, collaborate and share. Working groups shall not be established that duplicate other active cross-government working groups or expected work products, or impinge on the efforts and responsibilities delegated to a government office or official.

The PA co-chairs shall designate working group leadership, at least one of whom shall be a federal employee. All aspects of a new working group shall be communicated to the full PA prior to its first discussion.

Working group participants shall have the following responsibilities:

- Actively participating on behalf of their agency;
- Contributing content and ideas and driving progress towards timelines;
- Coordinating reviews of working group products with stakeholders across their agency; and
- Communicating and coordinating to ensure policy and implementation alignment.

The PA co-chairs or superior committee or council may terminate, or request termination of, a working group.

In the event that industry input is desired to contribute to a working group product, it will be conducted in a manner wholly compliant with the Federal Advisory Committee Act. Any plan to include industry must be vetted and approved by the appropriate authorities including, but not limited to, the GSA General Counsel and Office of Management and Budget. The PA must make every reasonable effort to ensure that when industry input is to be included for an official working group product, there is an open, fair, and transparent process to ensure that all industry participants, regardless of size, are able to participate when appropriate. However, such attendees cannot participate in PA deliberations to accept a work product, publish any work products, or voting.

Standing working groups include:

- **FPKI Certificate Policy Working Group (CPWG)**

  Reviews cross-certification applications, Certificate Policies, Certificate Policy change proposals, auditor reports of entities applying for or seeking to maintain cross-certification with the FPKI, and provides recommendations to the PA for acceptance or rejection of those items. The CPWG also reviews FPKI administrative and guidance documents and recommends changes to those documents as needed.

- **FPKI Technical Working Group (TWG)**

  Reviews and provides advice about technical issues related to the FPKI at the request of the PA, CPWG, or Federal PKI MA.

Voting

Votes shall be held for proposed updates or changes in FPKI Certificate Policies, the approval of new FPKI members or affiliates, and outcomes associated with the annual review processes.

Votes shall also be held when voting members cannot reach consensus, or when otherwise as determined by the PA co-chairs. Voting and ex-officio members may also request a vote.

The PA co-chairs shall decide when and how a vote occurs. For example, a vote may occur during a meeting via roll-call, or outside a meeting via email.

For non-immediate votes, voting members shall have at least five business days to vote. The PA co-chairs may specify a shorter time frame as necessary.

Concurrence of at least two-thirds (2/3) of the voting membership is required for the PA to approve a motion. When votes are taken, each authorized agency shall get one vote. However, a voting member may provide a proxy to another voting member.

Amendments

This charter may be amended upon request and approval of the PA and coordinated with the ICAM Sub-committee, CISO Council and CIO Council. At a minimum, this charter will be reviewed on a biennial basis.

Effective Date

This charter is effective as of the date signed and remains in effect until modified or rescinded.

DocuSigned by:
Nandini Diamond
75CE0BE9E1B04B5...

Nandini Diamond, ICAMSC Co-Chair Date

RAMON BURKS Digitally signed by RAMON BURKS
Date: 2021.08.19 08:56:32 -04'00'

Ramon Burks, ICAMSC Co-Chair Date

Appendix: Definitions

a. Public Key Infrastructure ("PKI") is a set of policies, processes, and information technology systems used for the purpose of creating, maintaining and revoking certificates and public-private key pairs. A PKI certificate is considered trusted based on the security requirements of the systems, the adherence to the agreed upon set of issuance procedures for asserting a claimed set of identity attributes in the public certificate, and protection of the associated private key. The certificate policy or Object Identifier ("OID") asserted in the public certificate is a public assertion of adherence to the requirements defined in a Certificate Policy ("CP") and implementation practices stated in a Certification Practice Statement ("CPS").

b. Federal Public Key Infrastructure ("FPKI" or "Federal PKI") is an implementation of a set of PKI policies, processes and information technology systems that provides the US Government with a common baseline to administer certificates and public-private key pairs. Federal PKI is one of several trust frameworks supporting federated trust of government devices and persons used by the US Federal Government.

c. Federal Public Key Infrastructure Policy Authority ("PA" or "Policy Authority") is the Federal trust framework governance body for a set of PKI systems and associated certificates used for federated trust across and between Federal agencies and with entities that are not a US Federal Government agency for mission delivery purposes. The Policy Authority is a group of representatives from US Federal Government agencies (including cabinet-level departments) established pursuant to a charter under the Federal CIO council. It manages the policies governing the FPKI trust framework and approves or denies entities for certification into the trust framework.

d. Federal Public Key Infrastructure Management Authority ("MA" or "Management Authority") is governed under the PA. The MA operates and manages the certification authorities ("CA") that comprise the FPKI root certification authorities and/or bridge certification authority for the participating Federal agencies.

e. Entity is the organization operating a certification authority or non-federal trust framework certified by the Federal PKI Policy Authority.