FPKIPA - Federal Public Key Infrastructure Policy Authority


FPKI REGISTRATION AUTHORITY AGREEMENT   
TEMPLATE AND GUIDANCE

v.1.0 – April 13, 2017

Abstract

This template is for use by members of the Federal PKI when the organization that performs enrollment/registration services is separate and distinct from the organization that operates and maintains the Certification Authority that issues certificates based on these enrollment/registration services.

Table of Contents

[I. Introduction I](#_Toc479250782)

[II. Intended Audience I](#_Toc479250783)

[III. Intended Use II](#_Toc479250784)

[ATTACHMENT 1](#_Toc479250785)

[1. Purpose 1](#_Toc479250786)

[2. Rights of the Parties 1](#_Toc479250787)

[3. Responsibilities of the Parties 1](#_Toc479250788)

[4. Dispute Resolution 3](#_Toc479250789)

[5. Termination 3](#_Toc479250790)

[6. Effective Date 3](#_Toc479250791)

[7. Signature 3](#_Toc479250792)

[Appendix: Registration Authority Requirements 4](#_Toc479250793)

[A-1 Architecture 4](#_Toc479250794)

[A-2 Documentation 4](#_Toc479250795)

[A-3 Certificate Identification 4](#_Toc479250796)

[A-4 Initial Identity Validation 5](#_Toc479250797)

[A-5 Authentication of Users 5](#_Toc479250798)

[A-6 Special Considerations for PIV Certificates 5](#_Toc479250799)

[A-7 Special Considerations for PIV-I Certificates 5](#_Toc479250800)

[A-8 Authentication of Devices 6](#_Toc479250801)

[A-9 Security Controls 6](#_Toc479250802)

# Introduction

The purpose of this document is to identify and explain the roles and responsibilities of an organization other than the Certification Authority (CA) acting as an enrollment/registration agent for the issuance of digital certificates to Federal agencies under the Federal PKI COMMON Policy Framework.

Federal Public Key Infrastructure (FPKI) Shared Service Providers (SSP) are required to submit a third-party audit on an annual basis, in accordance with Section 8 of the FPKI COMMON Certificate Policy, which states:

CAs operating under this policy shall have a compliance audit mechanism in place to ensure that the requirements of their CPS are being implemented and enforced. The SSP PMA shall be responsible for ensuring audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated."

When the CA does not perform the enrollment/registration activities, a Registration Authority Agreement (RAA) demonstrates that there is a clear understanding of which party will be responsible for each aspect of the infrastructure and has the responsibility to see that the audits are conducted and audit letters available to the FPKI SSP Policy Management Authority (PMA) for inclusion in the required annual audit package.

Note: This requirement extends to PIV-I and other PKI certificate services acquired by Federal Agencies from service providers cross-certified with the Federal Bridge Certification Authority (FBCA).

In general, the enrollment/registration component includes:

* In person identity proofing
* Verification and validation of identity documents
* Enrollment and registration
* Card printing and personalization (for specific credential types)
* Credential issuance
* Credential revocation
* Post-issuance updates and additions
* Credential re-issuance

The PKI Service Provider must provide the enrollment/registration agent with guidance concerning the requirements for operating in accordance with the applicable CP and CPS for inclusion in the RAA between the two entities. The attached template contains the recommended RAA stipulations, and the registration authority practices that must be described are identified in the associated Appendix.

# Intended Audience

1. Federal Agencies that acquire PIV, PIV-Interoperable (PIV-I) or any other PKI token services from a Federal PKI Shared Service Provider.
2. FPKI SSPs operating under the Federal PKI COMMON Certificate Policy
3. PKI providers cross certified with the Federal Bridge CA Certificate Policy that issue PIV-I certificates on behalf of a Federal agency.
4. Any organization that takes responsibility for any portion of the enrollment/registration activities associated with digital credential issuance to/on behalf of Federal agencies.

# Intended Use

PKI Service Providers must undergo an annual review that includes submission of an independent compliance audit encompassing all aspects of its operations, including those activities conducted by a customer (issuing organization) or by a third party. The attached RAA template and addendum attachment shall be executed between the PKI Service Provider and the issuing organization or other third party and included in the Annual Review document submission whenever all or any portion of the enrollment/registration/issuance activities are conducted by the customer or other third-party. In addition, the RAA shall be assessed during the compliance audit review for conformance to the applicable CP and CPS, and against the referenced operations.

Note: The requirements of the RAA may be incorporated into a memorandum of agreement or a contract, provided the language clearly addresses the requirements in the attachment and its appendix.

# ATTACHMENT

Registration Authority Agreement Template

*The RAA should clearly identify where the responsibility for each of the functions associated with the management/operation of the PKI and the issuance of certificates. This Template is a representative example that should be customized for each RAA.*

# Purpose

The purpose of this document is to summarize the Registration Authority roles and functions that will be provided by *[Issuing Organization]* as defined in the *[PKI Service Provider]* CPS.

# Rights of the Parties

**PKI Service Provider/Certification Authority**

The enrollment/issuing organization grants the PKI Service Provider the following:

* The rights set forth in the applicable CP/CPS, including appropriate access to information in order to deliver the PKI service
* If at any time the PKI service provider determines that the issuing organization is not operating in accordance with the Registration Authority Agreement (RAA), it shall notify the issuing organization and may unilaterally suspend PKI services until such time the issuing organization is once more operating in compliance with the RAA.

**Enrollment/Registration Services (Issuing Organization)**

The PKI Service Provider grants the enrollment/issuing organization the following:

* The rights set forth in the applicable CP/CPS, including appropriate access to information and systems in order to perform enrollment and registration services
* If at any time the issuing organization determines that the PKI service provider is not operating in accordance with the RAA, it shall notify the PKI service provider and may unilaterally cease enrollment and issuance activities until such time the PKI service provider is once more operating in compliance with the RAA.
* In the event the PKI service provider’s non-compliance results in the termination of its relationship with the Federal PKI (i.e. revocation of the certificates issued to the PKI Service Provider by the Federal PKI), the RAA is terminated.

# Responsibilities of the Parties

**PKI Service Provider/Certification Authority**

The PKI service provider is responsible for the following:

* The policy, practices, baselines and guidance pertaining to the CA that ensure the issuance and key management functions of the CA are conducted in accordance with the applicable CP[[1]](#footnote-1), to include:
  + Key management functions: Generation of CA key pairs, the secure management of CA private keys, and the distribution of CA public keys
  + Issuance and Revocation of certificates
  + Card personalization and printing, as applicable for the credential type (i.e. PIV, PIV-I)
  + Publication of Certificate Revocation Lists (CRL) and revocation information
  + Audit and Archive System event logs
* Conformance to the Key Recovery System (KRS) that ensure the escrow and recovery of key management keys are conducted in accordance with the applicable Key Recovery Policy (KRP), when applicable.[[2]](#footnote-2)

**Enrollment/Registration Services (Issuing Organization)**

The Issuing Organization is responsible for the following:

* The practices, baselines, and guidance that ensure the enrollment and issuance activities are in material compliance with the applicable CP and CPS at all times.
* Timely corrective action to address any deficiencies, including termination or suspension of specific activities, when warranted.
* For Federal agencies, Federal information security requirements that pertain to the enrollment and issuance activities, to include the System Security Plan, Risk Management Plan, Continuity of Operations Plan, and related documentation and processes required under the Federal Information Security Management Act (FISMA) and a FISMA Authority to Operate (ATO).
* For PIV and Derived PIV Credentials, an audit) shall be completed that conforms to NIST SP 800-79-2, and an authority to operate shall be granted by the Agency’s Designated Authorizing Official for each issuing facility. This also applies to PIV-I credentials issued by Federal agencies.
* The management, operational and technical controls over the enrollment and issuance activities, in compliance with the applicable CP, CPS, and other associated documents.
  + Establish and maintain a secure environment and procedures for certificate applicants
  + Identify and authenticate individuals (or entities) applying for a certificate
  + Approve or reject certificate applications
  + Initiate certificate revocations
  + Audit and archive enrollment system event logs on a regular and continual basis
* The management, operational and technical controls associated with key recovery requests, in compliance with the applicable KRP/KRPS, when applicable.
* Annual third party Audit of enrollment and issuance processes.

# Dispute Resolution

Any dispute arising under this RAA shall be resolved by the Parties.

# Termination

This RAA remains in effect for the duration of the contract between the parties and will terminate upon the termination of said contract.

# Effective Date

This RAA enters into effect upon the signatures of both Parties.

# Signature

**PKI Service Provider**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*[Name]*

*[Title]*

*[Phone]*

*[Email]*

**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Issuing Organization**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*[Name]*

*[Title]*

*[Phone]*

*[Email]*

**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Appendix: Registration Authority Requirements

*Note: If a Registration Practices Statement exists, it will take the place of this Appendix, but should cover the contents listed here.*

# A-1 Architecture

*[Provide a brief description of the architecture of the PKI that identifies the components and which organization, FPKI SSP or Issuing Organization, has responsibility for each. At a minimum the architecture description should include the following components and their relationships:*

* *Issuing CA and its hierarchy, if applicable, what types of certificates are issued from each CA in the hierarchy*
* *Enrollment/Registration Workstation(s) and its (their) components*
* *Credential Management System (mandatory for PIV and PIV-I, optional for all others)*
* *Repositories*
* *OCSP Servers/Responders*

*Include a diagram that identifies the components and their relationships. This diagram should be detailed enough to show the peripheral components that provide technical system security for the PKI.]*

# A-2 Documentation

*[Identify the governing documents and the organization responsible for each. At a minimum, this will include:*

* *Architecture*
* *Certificate Policy*
* *Certification Practices Statement (if a separate Registration Practice Statement is used, this needs to be identified)*
* *Key Recovery Policy (when applicable)*
* *Key Recovery Practices Statement (when applicable)]*
* Certificate uses

# A-3 Certificate Identification

*[Provide a list of the policy object identifiers (OID) and their common names that will be included in certificates provided by the FPKI SSP to the issuing organization. Include any limitations or special requirements associated with each.]*

*[See Federal PKI CP. Identify the naming convention for the certificates. Certificates may be issued in one of two forms: a geo-political name or an Internet domain component name.]*

*[See FBCA CP to determine specific naming requirements for PIV-I certificates Include the distinguished name details for each type of end user certificate that will be issued (PIV-I Auth, PIV-I CardAuth, PIV-I Content Signing, etc.]*

# A-4 Initial Identity Validation

Initial identity validation for the purpose of issuing a PKI credential to a subscriber is the responsibility of the issuing organization.

# A-5 Authentication of Users

The issuing organization policy management authority shall ensure that the applicant’s identity information is verified in accordance with the process established by the applicable CP and CPS as follows:

* *[Describe the identity proofing process used by the registration/enrollment officers (See FPKI CP Section 3.2). This must include the following:*
  + Identity of the individual performing the identity proofing, date the proofing was performed, and a signed declaration under penalty of perjury that the identity of the applicant was verified as required.
  + For in person identity proofing, the unique identifying number(s) from the proof(s) of identity presented by the applicant or a facsimile (scan) of the identity documents.
  + A declaration of identity signed by the applicant in the presence of the individual performing the identity proofing using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).
* *Describe how the information used to assert identity is verified.*
* *Indicate whether role-based or group certificates are permitted and under what circumstances]*

# A-6 Special Considerations for PIV Certificates

*[Describe how the following requirements as specified in FIPS 201-2 are satisfied:*

* *Enrollment officer verifies:*
  + *Request for certificate issuance was submitted by an authorized agency sponsor*
  + *Request was approved by an official separate and distinct from the individual that sponsored the applicant.*
  + *An approved background investigation (NACI or higher) exists for this individual. If none exists, verification that one has been initiated and the NAC portion has been completed is required.*
* *Applicant presents two (2) forms of government-approved identification as specified in FIPS 201-2.*
* *The enrollment officer collects biometrics as specified in FIPS 201-2.]*

# A-7 Special Considerations for PIV-I Certificates

*[Describe how the following requirements are satisfied:*

* *For PIV-I, credentials required are two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document shall be a valid State or Federal Government-issued picture identification (ID). For PIV-I, the use of an in-person antecedent is not applicable.*
* *Biometric data shall be collected during the identity proofing and registration process, and shall be formatted in accordance with [NIST SP 800-76]*

# A-8 Authentication of Devices

*[This section applies if the issuer intends to issue certificates to devices. Each device must have a human sponsor. This human sponsor will have an identity credential that contains PKI certificates issued at a level that is equivalent or higher than the device’s certificate.*

* *Describe the identity verification requirements for the human sponsor and the processes used to ensure the device certificate application is valid and authorized.*
* *Describe how the device certificate accountability is maintained in the event the human sponsor is changed.]*

# A-9 Security Controls

*[Describe how the registration/enrollment workstations are protected from unauthorized access (logical and physical).]*

*[Describe how the exchange of information between the enrollment/registration workstations and the CA is protected. If the enrollment/registration workstation exchanges information with any other system include these network security controls.]*

*[Describe the process for reviewing and archiving the audit logs of the registration/enrollment workstations.]*

1. . For FPKI Shared Service Providers, the applicable CP is the X.509 Certificate Policy for the Federal Common Policy Framework (COMMON). For all other PKI Shared Service Providers (PIV-I etc.), this is the X.509 Certificate Policy used to cross certify the provider with the FBCA. [↑](#footnote-ref-1)
2. Key Recovery is an optional service that, when provided, must be accompanied by a Key Recovery Policy and Key Recovery Practices Statement, or incorporated into the appropriate CP and/or CPS. [↑](#footnote-ref-2)