Registration Authority (RA) Requirements

1.0 Registration Authority Overview

Pursuant to the definition contained in the Federal Common Policy[1] the Registration Authority is defined as *an entity that is responsible for identification and authentication of certificate subjects but does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of an authorized CA).*

This document provides an overview of the Registration Authority (RA), and the relationship of the PKI Shared Service Providers (SSPs) with the RA function. The RA function shall be conducted by the respective Federal agency contracting for services under the provisions of the Federal Common Policy, as overseen by the Federal PKI Policy Authority (FPKIPA). A PKI SSP may provide infrastructure components, which is discussed within this document; however the Registration Authority is deemed to be an inherently government function[2] and only the Contracting Federal Agency[3] may act as the Registration Authority.

The guidance contained in this document takes into consideration that Federal agencies have common minimum requirements for RA services. However, there is no single best approach for the provision of RA functions and components: Federal agencies have differing functions; may be subject to different laws and regulatory considerations; and can have different business cases for implementing PKI services[4].

At the same time, it is essential that the Federal government establish a common approach that supports mutual reliance and provides for a common trust environment. The basis for reliance and trust is provided for in the emerging Authentication and Identity Policy Framework for Federal Agencies[5]. This framework will be comprised of three core policy documents which are reviewed below, and are directly related to the provision of RA services, and minimum expectations.

The guidance in this document also notes the unique structure of the Federal common trust anchor, where the Policy Authority neither belongs to the CA function or the RA

[1] The Federal Common Policy is formally entitled the X.509 Certificate Policy for the Common Policy Framework, and is the Certificate Policy for the Federal common trust anchor.
[2] The term "inherently governmental function" comes from OMB Circular A-76, Performance of Commerical Activities. The RA function is deemed to be an inherently governmental function; and as such a government Program Manager shall be assigned to oversee and manage the RA function. However, the LRA function may be contracted.
[3] The context of Contracting Federal Agency includes the federal Program Manager, the Program Manager's federal employees, and any support staff contracted by the Program Manager as trusted agents of the Federal agency. The PKI SSP is not authorized to act as a trusted agent for the purposes of this agreement, except where they may be authorized to provide LRA duties under the supervision of the RA, as deemed appropriate by the SSPWG.
[4] A government organization that has healthcare considerations may have additional or different requirements than an agency with financial considerations dictated by business parties that are relying parties.
[5] These policy documents are overseen by OMB.

function[6]. To address this, the Shared Service Provider Working Group (SSPWG) has determined that a Registration Authority Practice Statement (RPS)[7] may be required to properly define the roles and relationships, and this is provided for in the Federal Common Policy[8]. The RPS should properly delineate the RA roles and responsibilities[9], and is subject to approval by the FPKIPA, as well as compliance audits and certification and accreditation (C&A)[10].

2.0 Registration Authority Purpose

The Registration Authority (RA) is the entity that enters into an agreement with a Certification Authority (CA)[11] to collect and verify each Subscriber's identity and information to be entered into his or her public key certificate. The RA performs its function in accordance with the Federal Common Policy and the approved CPS, and any other relevant agreements or policy documents such as those published by the SSPWG under the Authentication and Identity Policy Framework for Federal Agencies. Areas and activities overseen by the RA include, but are not limited to:

- In person proofing
- Verification and validation of identity documents
- Enrollment and registration
- Credential issuance
- Credential usage
- Credential revocation
- Post issuance updates and additions
- Credential re-issuance

The RA may, at the discretion of the Contracting Federal Agency, delegate functional roles and duties within the organization to a LRA. Such delegation must be consistent with Federal Policy, including the Federal Common Policy, the approved CPS, the RPS

[6] The Federal PKI Policy Authority description can be found www.cio.gov/fpkipa. The FPKIPA derives authority through the Federal CIO Council and the OMB Office of E-Government, as provided for in the E-Government Act of 2002.

[7] The Registration Practice Statement incorporates similar considerations that would exist in a Registration Authority Agreement, as identified in related literature on PKI implementation, management, and audit.

[8] The Federal Common Policy defines the RPS as a statement of the practices that an RA employs in determining identity, for the issuing, suspending, revoking, and renewing certificates, in accordance with specific requirements (i.e., requirements specified in this CP or requirements specified in a contract for services).

[9] The following documents are provided as a reference, but are not mandatory: Appendix A – ANS X.9.79-1: 2001, Part 1: PKI Practices and Policy Framework, Appendix B – ABA PKI Assessment Guidelines related to the RA evaluation, and Appendix C – ABA PKI Assessment Guidelines related to defined roles that can be delegated by the CA to the RA function. These references are provided for guidance only. The FPKIPA, CA and RA must determine, in the context of the Federal Common Policy and Federal mandates, how to properly structure any related agreements.

[10] See NIST Special Publication 800-37, Guide for the Certification and Accreditation of Federal Information Systems.

[11] Each PKI SSP is responsible for providing the Certification Authority (CA), and the associated infrastructure and resources required to operate the CA in accordance with acceptable practices. Such operation must be in accordance with Authentication and Identity Framework for Federal Agencies, and must be validated by an Operational Capabilities Demonstration (OCD) conducted by the FICC.

and associated agreement(s) with the approved PKI SSP. The RA is responsible for the standards, training, oversight and audit of the LRA entities operating at the direction of the RA. As such, each RA must establish policy, standards, baselines, and guidance that ensure that the approved LRA is in material compliance at all times. The RA shall ensure that timely corrective action is taken to address any LRA deficiency, including the termination or suspension of specific LRA entity duties, when warranted.

3.0 Registration Authority Roles and Responsibilities

The following roles and responsibilities are identified, in addition to the provisions of traditional references used to define the roles and responsibilities of a RA.

3.1 Shared Service Provider Working Group (SSPWG)

The SSPWG is responsible for the following areas, including policy development and management, and providing guidance where appropriate.

- Acts in accordance with the FPKIPA Charter, as approved[12].
- Determines the standards and evaluation criteria for PKI SSPs, and is the Federal entity responsible for conducting the Operational Capabilities Demonstration (OCD) used to validate the qualification and suitability of a perspective PKI SSP. This includes the ability to support Federal agency RA functions in the manner required to achieve compliance with Federal policy and guidance. The OCD is conducted with the participation of the SSPWG.
- Establishes and oversees the subcommittees required to develop policy, procedures, and guidance for Federal agencies.

3.2 Federal PKI Policy Authority

The FPKIPA acts to establish, monitor and evaluate the Federal common trust anchor, as provided for in the Federal Common Policy.

- Responsible for the compliance audit for PKI SSP vendors, and the respective RA entities operating by the Contracting Federal Agencies. Provisions and controls related to compliance audit are contained in the Federal Common Policy.
- Responsible for the review and acceptance of the CPS and RPS documents directly related to the Federal Common Policy.
- Responsible for the implementation, operating, audit and oversight of the Federal Common Policy root CA, used to sign the subordinate CA operated by a PKI SSP vendor in support of a Contracting Federal Agency. This includes provisions for compliance audits and C&A of the Federal Common Policy root CA.

3.3 PKI Shared Service Provider

[12] The FPKIPA Charter can be found at http://www.cio.gov/fpkipa/documents/fpkipa_charter.pdf for review.

Each PKI SSP is responsible for the following areas, as it pertains to the RA function.

- Each PKI SSP is responsible for working with the SSPWG, the FPKIPA, and the Contracting Federal Agency to provide for compliance audits, as provided for in the Federal Common Policy.

- Each PKI SSP is responsible for the maintenance, and warranty communications with the vendors providing the RA components listed in the Registration Authority Component Requirements section.

3.4 Contracting Federal Agency

Each Contracting Federal Agency is responsible for the following areas, as it pertains to the RA function.

- Responsible for any Federal information security requirements, such as compliance audits or contracting for C&A services, where required. This includes creation of a System Security Plan, Risk Management Plan, Continuity of Operations Plan, and related documentation and processes required by the Federal government.

- Identification and management of the authoritative data source used to create digital credentials.

- The management, operational and technical controls over the RA, in compliance with the Federal Common Policy, the CPS, the RPS, and associated agreements. This includes any LRA delegated functions.

4.0 Registration Authority Practice Statement

A RPS is required between a PKI SSP that has completed an Operational Capabilities Demonstration (OCD) and a Contracting Federal Agency. The agreement must be approved by the SSPWG prior to commencement of services. The following documents must be considered in the formulation of the RPS, and are part of the emerging Authentication and Identity Policy Framework for Federal Agencies:

- **X.509 Certificate Policy for the Common Policy Framework –** This policy document, known as the Federal Common Policy, conforms to the general structure for a Certificate Policy (CP) as outlined in RFC 2527, Certificate Policy and Certificate Practice Statement Framework.

- **Federal Smart Card Policy –** A policy document issued by the Federal Identity Credentialing Committee (FICC), and based on the work accomplished by the Smart Card Manager's Interagency Advisory Board (IAB), it outlines considerations for life cycle management of Federal Identity Cards (FIC).

- **Federal Identity Assurance Policy –** This document will establish the minimum standards for identity assurance, which is a core consideration in the RA function. If the identity assurance requirements specified in this document exceed those defined in the Common Policy, agencies will be required to meet the new higher standard.

Federal mandates also require consideration of applicable NIST publications[13], including Federal Information Processing Standards (FIPS) and Special Publications such as those that provide for System Security Plans, or the documents that identify federal standards and guidance for PKI systems.

Additional documents that may be useful in the development of the RPS are listed below. These documents are optional and should be considered in the context of specific Agency requirements.

- **American Bar Association PKI Assessment Guide (PAG) –** This document is an industry reference used to help assess and facilitate interoperable trustworthy public key infrastructures. Development was conducted by the Information Security Committee. It addresses technical and business requirements for PKI components within a legal framework.

- **Industry Specific References –** Agencies that work closely with specific industries may have to meet industry specific requirements in addition to Government requirements. Examples may include ASTM standards intended to address industry specific considerations, including certificate profiles and life cycle management that have a bearing on relying party agreements. Note that agencies must meet the more restrictive of Federal and Industry requirements. That is, weak Industry requirements do not justify failure to meet Federal requirements.

- **ANS X9.79-1: 2001, Part 1: PKI Practices and Policy Framework –** This document, published by the American National Standards Institute is principally intended for the financial services industry.

5.0 Registration Authority Component Requirements

The following component requirements comprise the RA function, and are evaluated during the Operational Capability Demonstration (OCD) conducted as part of the approval process for a PKI SSP candidate review.

The PKI SSP must be able to demonstrate the ability to interoperate with the RA function and services as outlined in the Operational Capability Demonstration Criteria. The PKI SSPs are encouraged to provide components that conform to the Common Criteria

[13] NIST publications are available for review at the Computer Security Resource Center internet website (csrc.nist.gov), and includes links to other associated websites.

Certificate Issuance and Management Components (CIMC) Protection Profile, specifically the role separation considered in the CIMC.

The PKI SSP is required to provide an automated end-to-end RA function, which the Contracting Federal Agency may or may not elect to utilize[14]. The automated RA function will be evaluated against the Identity and Authentication Policy Framework for Federal Agencies, which includes the Federal Common Policy; the Federal Smart Card Policy, and; the Federal Identity Assurance Policy. Specific components and functionality incorporated into the RA shall include:

- Automated certificate issuance and management software supporting:
  - Certificate issuance where key pair generation is performed on a GSC-IS compliant smart card;
  - Out-of-band management requests for issuance of digital credentials, and post issuance life cycle management;
  - Secure communications with an authoritative data source and Certification Authority (CA) used for the purposes of issuing certificates;
  - The ability to perform post issuance updates and management of hardware tokens (smart cards form factor).

The use of knowledge based authentication[15] for purposes such as PIN resets shall be identified in the CPS and RPS documents, and shall be consistent with applicable government mandates, regulations and guidance as published by the Federal government.

Additionally, the PKI SSP is encouraged to offer the Contracting Federal Agencies the following optional components related to key management, validation, storage, and support which may be treated as contract options.

- An automated key history and reporting facility. This component must provide for secure communications by the RA and any LRA to identify and generate reports on current and historical key records. Examples would include the number of currently issued keys, the number of keys that will expire within a given period, and the types of keys issued and overseen by the RA function.

- Key Recovery services for key establishment keys (i.e., RSA key transport keys).

- Post issuance services such as smart card unlock features. This includes the ability to store and manage smart card unlock codes in a secure manner.

[14] The Contracting Federal Agency may propose a different solution to provide end-to-end RA functions. However, this requires acceptance by the PKI SSP vendor and the SSPWG, and must be identified in the RPS.

[15] Knowledge based authentication guidance is currently being developed by the Federal government. This form of authentication relies on a challenge response approach that only the intended individual should be able to successfully complete. Examples of knowledge based authentication include the use of a series of questions that would be difficult for an entity to successfully guess, and are commonly used for self-service password administration in e-commerce web-based systems.

- A PKI Help Desk function, with automated tracking that allows the Contracting Federal Agency the opportunity to manage and monitor PKI Help Desk events.

Contracting Federal Agencies may elect to require that their PKI solution is operated on dedicated systems. There are a variety of reasons associated with this, including Federal C&A considerations, disaster recovery, or integration requirements that would extend network functionality[16].

Contracting Federal Agencies may elect to provide these components separately, noting that government provided components must be in compliance with the Federal Common Policy, and CPS, and other relevant considerations. The PKI SSP may evaluate the government provided components to ensure acceptability against compliance audit criteria and industry best practices.

[16] An example may include a PKI SSP offering for a Windows 2003 Certificate Server that is integrated into the Contracting Federal Agency enterprise network, and may be used to provide device certificates under a separate CP and CPS.

Appendix A - ANS X.9.79-1: 2001, Part 1: PKI Practices and Policy Framework

ANS X9.79-1:2001 is a principal PKI reference in the financial services industry. Sections A.3 through A.6 of Appendix A identify the applicable governance of Registration Authority Operations, and Section A.8 articulates Practice Administration. The control objectives in Annex B of ANSI X9.79 represent baseline control criteria that must be considered in the formation of the Registration Authority Practice Statement. The control objectives (high level) include:

- Security management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Event Journaling
- Key Management Life Cycle Controls
  - CA Key Generation
  - CA Key Storage, Backup, and Recovery
  - CA Public Key Distribution
  - CA Key Escrow
  - CA Key Usage
  - CA Key Destruction
  - CA Key Archival
- Cryptographic Hardware Life Cycle Management
- CA-Provided Subscriber Key Management Services (if required)
- Certificate Life Cycle Controls
  - Subscriber Registration
  - Certificate Renewal (if required)
  - Certificate Rekey
  - Certificate Issuance
  - Certificate Distribution
  - Certificate Revocation
  - Certificate Suspension (if required)
  - Certificate Status Information Processing
  - Integrated Circuit Card Life Cycle Management (if required)

Appendix B – ABA PKI Assessment Guidelines

The American Bar Association publication PKI Assessment Guidelines was published on May 10, 2003 by the Information Security Committee. This guideline document is intended to help assess and facilitate interoperable trustworthy public key infrastructures. The sections relevant to establishing a RPS include, but are not limited to:

- B.6 PKI Assessment
- B.6.1 Participants
- B.6.2 Assessment Process
- C.5.2 Privacy and Personally Identifiable Information
- D.1.3 Community and Applicability
- D.1.3.1 Certification Authorities
- D.1.3.2 Registration Authorities
- D.1.3.3 End Entities
- D.2.1.1 CA Responsibilities and Liability
- D.2.1.2 Responsibilities and Liability of a Registration Authority
- D.2.1.3 Subscriber Responsibilities and Liability
- D.2.1.4 Relying Party Responsibilities and Liability
- D.2.1.5 Repository Responsibilities and Liability
- D.2.7 Compliance Audits
- D.2.8 Consumer Issues, Information Practices, Privacy
- D.2.9 Intellectual Property Rights
- D.3 Initial Validation of Identity, Authority and/or Other Attributes
- D.4 Certificate Life Cycle Operational Requirements
- D.5 Management, Operational and Physical Security Controls
- D.6 Technical Security Controls
- D.7 Certificate, CRL, and OCSP Profiles
- D.8 Specification Administration

Appendix C – Functional Role Assignments

The American Bar Association publication, PKI Assessment Guidelines, incorporates guidance on the permissible delegation of functional roles from the CA to the RA function. This information is provided as a reference, noting that the ABA may change their recommendations in the future, and this reference does not constitute a mandate. While it does reflect general industry views that are adopted by compliance auditors, only the FPKIPA has the authority to formally approve the delegation of roles.

Table C-1: CA and RA Functional Role Alternatives

Functional Area	Certification Authority	Registration Authority
Key management functions, such as the generation of CA key pairs, the secure management of CA private keys, and the distribution of CA public keys	YES	NO
Establishing an environment and procedure for certificate applicants to submit their certificate applications (e.g., creating a web-based enrollment page)	YES	YES
The identification and authentication of individuals or entities applying for a certificate	YES	YES
The approval or rejection of certificate applications	YES	YES
The signing and issuance of certificates in a repository, where certificates are made available for potential relying parties	YES	NO
The publication of certificates in a repository, where certificates are made available for potential relying parties	YES	NO
The initiation of certificate revocations, either at the subscriber's request or upon the entity's own initiative	YES	YES
The revocation of certificates, including by such means as issuing and publishing Certificate Revocation Lists (CRL) or providing revocation information via Online Certificate Status Protocol (OCSP) or other online methods	YES	NO
The identification and authentication of individuals or entities submitting requests to renew certificates or seeking a new certificate following a re-keying process, and processes set forth above for certificates issues in response to approved renewal or re-keying requests	YES	YES

According to the ABA PKI Assessment Guidelines, assessors should read the PKI's policy and practice documents to see how the functions are identified and allocated among various entities. Assessors should determine if the relevant entities are identified and if their respective roles are clear. Assessors should also review agreements to determine if all functions are accounted for and if they clearly state the respective roles of the entities performing the functions. To ensure a successful compliance audit, agencies should understand how the table above is represented in their CPS and RPS agreements.