



***REGISTRATION AUTHORITY (RA) & LOCAL
REGISTRATION AUTHORITY (LRA)
ORIENTATION GUIDELINES***

Return this form (Appendix A, B, and C) to Project Manager

DATE: August 5, 2026

VERSION: 7.4

REVISION HISTORY

VERSION	DATE	REASON FOR CHANGE
2.0	March 23, 2011	Formatting changes Addition of Organization and CA DN verification procedures Addition of requirement for recording and signing of subscriber hardware destruction and re-initialization Addition of requirement for RA and LRA to notify CA of any changes to certificate contents
3.0	August 31, 2011	Formatting changes Separation of vetting charts to individual CAs Enhancement of vetting instructions in charts
3.1	September 24, 2012	Add provisions for Basic Assurance in forms
3.2	December 13, 2013	Added TA, RA, LRA Check box on Appendix A
4.0	April 13, 2016	Revised Company Logo/Branding and formatting
5.0	May 13, 2020	Corrected date from 201_ to 20
6.0	September 14, 2022	Annual Review
7.0	September 1, 2023	Annual Review
7.1	June 17, 2024	Annual Review, minor edits for formatting
7.2	June 17, 2025	Major Update – new structure, updated learning points for the reader, alignment with current policies & practices
7.3	June 22, 2026	Annual Review and Update
7.4	August 5, 2026	Minor edits as requested by GSA

Signature

This document is authorized by the Entrust Policy Authority (PA).

Signed by:

Jim Trovato

89D32B44D9C945B...

Jim Trovato,

Entrust Policy Authority, Date: August 5, 2026

Contents

Signature	2
Purpose	4
Using this Document	4
INTRODUCTION	5
1.1 Scope	5
Authority	5
SECTION 1 - UNDERSTANDING FPKI	6
The Roots of FPKI Authority	6
The Federal PKI Policy Authority (FPKIPA)	6
FPKI Policies & Practices: Key FPKI Documentation	6
Entrust, an FPKI Affiliate SSP	6
Entrust Policies & Practices: Entrust Documentation	7
The Registration Authority (RA)	7
Local Registration Authority (LRA)	8
Policies and Practices: Key RA Documentation	8
Subscribers	8
Entrust – Key Roles	9
RA – Key Roles	9
FPKI COMPLIANCE: AN OVERVIEW	11
A Shared Cascade	11
The RA Compliance Guide	12
GUIDANCE FOR THE REGISTRATION AUTHORITY ORGANIZATION (RA)	13
The RA Policy Management Authority	13
The Registration Authority Agreement	13
An Overview of the Registration Practices Statement	13
A Trusted Role Overview	14
Annual Assessment	14
Section Summary	14
GUIDANCE FOR RA/LRA PERSONNEL	15
Registration Authority Guidance	15
Registration Authority (RA) Responsibilities:	15
Local Registration Authority	16
Local Registration Authority (LRA) Responsibilities:	16
Compliance with the RA RPS	16
Maintaining Audit Evidence	16
Managing Subscribers	17
Subscriber Responsibilities	17
Devices: Human Sponsor Responsibilities	17
Role-based certificates	17
REQUIRED FORMS	18
Acceptable Forms of ID for Verification	18
Appendix A – ENTRUST MANAGED SERVICES SUBSCRIBER AGREEMENT	19
Appendix B - ENTRUST MANAGED SERVICES SUBSCRIBER IDENTITY VERIFICATION	22
Appendix C - SUBSCRIBER IDENTITY VERIFICATION	23

Purpose

This document is intended to provide clear guidance for US Federal Agencies and Organizations that act in the RA role:

- For SSP and/or Derived Credential RA Organizations, requirements are defined in the [Common Policy Framework \(Common Policy CP\)](#)
- For NFI RA Organizations, requirements are defined in the [Federal Bridge Certificate Policy \(FBCP\)](#)
- FPKI program requirements are posted by the GSA at: <https://www.idmanagement.gov/fpki/>

Entrust Certificate Policy Certification Practices Statements for SSP & NFI (ETPKISSP CPS & EMS-NFI CPS) build on those requirements. Requirements are subject to change at any time. In case of discrepancy between the requirements and this guide, the current Common Policy CP, GSA requirements, and Entrust SSP CPS or Entrust NFI CP and CPS documents shall be deemed accurate for defining requirements.

Using this Document

This document references sections from various Certificate Policy (CP), Certification Practices Statement (CPS), and Registration Practices Statement (RPS) documents. All documents within the FPKI private trust environment follow the RFC 3647 structure. As a result, when a section number is referenced, the subject matter is consistent across all documents:

- **Certificate Policy (CP):** Defines policy requirements (what must be done).
- **Certification Practices Statement (CPS):** Describes how Entrust meets CP requirements and establishes compliance requirements for Registration Authority Organizations (RAs) (how Entrust meets the policy and what RAs must follow).
- **Registration Practices Statement (RPS):** Describes how an RA implements practices to comply with the CPS requirements.

For example, a reference to **Section 5.3 – Personnel Controls** allows the reader to:

- Consult the **CP** to understand the policy requirements (e.g., background checks, training, job rotation, and access controls),
- Review the **CPS** to see how Entrust addresses these requirements and what is required of RAs, and
- Examine the **RPS** to understand how the RA implements those requirements in practice.

Together, these documents provide a complete, end-to-end compliance cascade.

Introduction

Welcome to the Entrust RA Orientation Guide for US Federal Government Agencies and Organizations that enter a Registration Authority (RA) relationship with Entrust. The purpose of this guide is to support a powerful on-boarding experience that positions the relationship for on-going and compliant operational success.

Scope

The intent of this guide is to address:

- Key participants
- Compliance overview
- Key program documentation
- How Entrust supports RA compliance
- Defining organizational roles and responsibilities
- What does an RA/LRA do?
- Guidelines for Subscriber Verification
- Certificate Management Systems (CMS) hosting guidelines for the RA
- Key Forms – templates

When complete, the reader will have a clear understanding of the FPKI landscape, the participating organizations and their respective roles, and how Entrust supports each stage of the RA journey. The reader will gain insight into the foundational building blocks required for successful implementation, the obligations assigned to each organization, and the specific responsibilities of the RA Organization and Trusted Role personnel. An overview of the compliance cascade will further establish an understanding of the shared-responsibility model and organizational posture required by both FPKI and Entrust. Finally, our objective is to ensure you are fully connected with the [Entrust team](#), who are committed to supporting your success.

Authority

This document was issued with the approval of the Entrust Policy Authority (PA) and the Entrust Policy Management Authority (EPMA) and is subject to change as required, and at a minimum is reviewed and if required, updated annually.

Section 1 - Understanding FPKI

The Roots of FPKI Authority

SSP and Derived: The Federal Public Key Infrastructure (FPKI) establishes the United States Government's trust framework and supporting infrastructure for the issuance and management of digital certificates and associated public and private key pairs. This government trust framework was established by the Federal Chief Information Officer (CIO) Council, which is composed of the Chief Information Officers of all Cabinet level departments and designated independent agencies. Operating as the Federal PKI (FPKI), the CIO Council provides oversight for the entities responsible for governing, operating, and promoting the use of the FPKI. The *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* (the "Common Policy CP") was developed and approved under the authority of the Federal CIO Council and serves as the foundational certificate policy governing trust relationships within the Federal PKI SSP. (Reference: *Common Policy CP §1.3.1.1*).

NFI: The *X.509 Certificate Policy for the U.S. Federal Bridge Certification Authority* (the "Federal Bridge Certificate Policy" or "FBCP") was developed and approved under the authority of the Federal Chief Information Officer (CIO) Council and establishes the certificate policy requirements governing cross certification and interoperation among participating PKI domains. In support of trust interoperability with the U.S. Federal Public Key Infrastructure, NFI operates in accordance with the requirements of the Federal Bridge Certificate Policy applicable to its role and policy mapping within the Federal PKI trust framework. (Reference: *Federal Bridge CP §1.3*)

The Federal PKI Policy Authority (FPKIPA)

The Federal Public Key Infrastructure Policy Authority (FPKIPA) is a sub-council comprised of U.S. Federal Government agency representatives and is chartered under the Federal Chief Information Security Officer (CISO) Council, under the Federal CIO Council. The FPKIPA owns the Certificate Policy documents and the maintenance of the FPKI Audit Boundary, which includes responsibility for approving Entrust documentation, the annual Audit Submission Package from Entrust and ensuring conformance of Entrust practices with the common policy framework and the practices captured in Entrust documentation. (Common Policy CP 1.3.1.2). PKI Participants can contact the FPKIPA team at fpki@gsa.com.

FPKI Policies & Practices: Key FPKI Documentation

- FPKI Program information is available at: <https://www.idmanagement.gov/fpki/>
- For SSP and Derived, the FPKIPA maintains the [X.509 Certificate Policy for the U.S. FPKI Common Policy Framework](#) (Common Policy CP), which defines the compliance requirements for each PKI participant. The Entrust SSP CPS is developed and maintained in compliance with the Common Policy CP.
- The NFI CP and CPS produced by Entrust are built and maintained in compliance with <https://www.idmanagement.gov/docs/fpki-x509-cert-policy-fbca.pdf>

Entrust, an FPKI Affiliate SSP

Entrust maintains an Authority to Operate (ATO) as a Federal Public Key Infrastructure (FPKI) Affiliate Shared Services Provider. From the Registration Authority (RA) perspective, Entrust supports three distinct service models:

- [Entrust PKI Shared Service Provider \(ETPKISSP\)](#)
Owned by the U.S. General Services Administration (GSA) and operated by Entrust, ETPKISSP



provides certificate services to U.S. Government employees, contractors, and devices (collectively, "Subscribers"). This service model leverages Shared Service Provider Issuing Certification Authorities (CAs) to issue credentials to Agency personnel and contractors, including those carrying Personal Identity Verification (PIV) cards.

- **Entrust Managed Services – Non-Federal Identities (EMSNFI)**
Owned and operated by Entrust, EMSNFI provides certificate services to nonfederal identities representing organizations authorized by the Federal PKI Policy Authority (FPKIPA) to participate in the Federal PKI trust framework. This service supports interoperability with the Federal PKI through applicable policy mappings and governance requirements.
- **Derived Credentials Management Service**
The Derived Credentials Management Service leverages existing PIV Cards for identity authentication and enables the derivation, issuance, and lifecycle management of derived certificates for use on mobile and other non-PIV-enabled devices.

Entrust Policies & Practices: Entrust Documentation

Entrust is responsible for maintaining the certificate policy and practice documentation governing its operations as a Shared Services Provider (SSP), Non-Federal Identity (NFI) provider, and Derived Credential Provider. These policy and practice documents are subject to review and approval by the Federal PKI Policy Authority (FPKIPA), with redacted CPS documents available at <https://www.entrust.com/legal-compliance/federal-pki>. Unredacted versions are available upon request to mpkipa@entrust.com.

From a compliance perspective, all documentation aligns with the Federal PKI framework and is evaluated for conformance against the *U.S. Federal PKI Common Policy Framework Certificate Policy* (Common Policy CP) or the *Federal Bridge Certificate Policy* (FBCP), as applicable to the service model. This governance structure reflects a shared responsibility within a private trust environment, whereby the FPKIPA establishes, manages, and enforces policy requirements through application of the Common Policy CP and oversight of an annual audit package submitted by Entrust, due no later than November 30 of each calendar year.

SSP: Key Documentation for SSP (including Derived Credentials) RAs	NFI: Key Documentation for NFI RAs
The Entrust Public Key Infrastructure Shared Services Provider "ETPKISSP" Certificate Practices Statement (ETPKISSP CPS)	Entrust Managed Services Non-Federal Identity (NFI) Public Key Infrastructure Certificate Policy (EMS-NFI CP)
	Entrust Managed Services Non-Federal Identity (NFI) Public Key Infrastructure Certification Practices Statement (EMS-NFI CPS)
Note: The ETPKISSP CPS and EMS-NFI CPS capture how Entrust and the RA collaborate for operational and audit success. It is the responsibility of Entrust to ensure that the RA maintains compliance with program requirements, the Common Policy CP and the relevant CPS.	

The Registration Authority (RA)

US Federal Agencies and Organizations approved for FPKI participation as a Registration Authority (RA) either:

- Are responsible for Subscriber credentials – verifying requests, maintaining audit information, and performing user administration through certificate management – issuing, suspending and restoring, revoking, recovery, and update; or

- Host on-premises RA or CMS software, for example, for Derived Credentials an on-premises component may be part of the RA architecture, hosted and operated by the RA and subject to annual assessment.

The RA, like Entrust, has requirements defined in the Common Policy framework, and addressed in Entrust documentation. A companion document to this document, the RA Compliance Guide, captures these requirements and provides guidance on each requirement. In summary, there are five essential requirements for the RA:

- Establish and maintain an RA Policy Management Authority (PMA) (Common Policy 1.3.1.5)
- Execute a Registration Authority Agreement with Entrust
- Maintain a current, approved Registration Practices Statement (RPS) that accurately reflects RA practices and make the RPS available upon request during internal assessments, external compliance audits, or other reviews required by Entrust, the applicable CP, CPS, or FPKI oversight authorities. Annually, submit PIV and PVI-I Card Test Reports
- Conduct an annual assessment (commonly called an RA Audit) (FPKI Memorandum – [click here](#))

The RA Compliance Guide supports the RA in establishing and maintaining the appropriate compliance posture, and guidance on how help and support is available through the appointed Policy Authority Representative for Compliance, available at mpkipa@entrust.com.

Local Registration Authority (LRA)

A Local Registration Authority (LRA) administers a specific group of users. An LRA is typically authorized by the RA where the scope of the Subscribers is specific to a physical location, or a specific team (group) of users. As a practical example, the LRA is a mechanism that can help the RA who has multiple locations. An LRA in a specific location is often best equipped to meet users in-person, verify their identities, execute the Subscriber agreement, respond with velocity where a security concern emerges, and maintain local audit records. An LRA may register other LRAs within the context of their locality or group of users and are not able to add RAs.

Policies and Practices: Key RA Documentation

The RA and Entrust are required to establish and maintain documentation specific to the RA role:

- The RA Registration Practices Statement (RA RPS) captures the practices employed by RA in compliance with Entrust documentation.

The RPS is a critical compliance document and is used during the annual assessment where the RA provides evidence of adherence. Note: When Entrust Professional Services is contracted to implement, creation of the required documentation is included in the SOW. For support in RPS creation and updates, contact mpkipa@entrust.com. See the RA Compliance Guide for more details.

Subscribers

The last link in the cascade represents the Subscribers. In general, this refers to humans being issued PIV card credentials, or Derived Credentials for mobile devices; the entity whose name appears as the subject in a certificate (Common Policy CP 1.3.6). The RA is responsible for the Subscribers: verifying the identity of the applicant, collecting a signed Subscriber agreement, and issuing the credential. Once verified and created, the RA is responsible for ensuring that Subscriber behavior aligns with policies, practices, and acceptable use, and finally, the RA is responsible for processing key management requests on behalf of their subscribers (e.g., revoke, suspend, restore, third-party

recovery, etc.).

Entrust – Key Roles

Success with PKI requires a balance of people, process, and technology. In compliance with the Common Policy framework, Entrust has established key roles to ensure RA success. The following table outlines these roles.

Role	Description
The Entrust Policy Management Authority (EPMA)	The Entrust Policy Management Authority (EPMA) holds responsibility for policy & compliance over all Entrust Services, including ETPKISSP & NFI. Comprised of a cross-functional group of the Entrust Senior Leadership Team and senior subject matter experts, the EPMA operates to a charter and is led by the Director, Product Compliance for Entrust mPKI, including the ETPKISSP service, as EPMA Chair. (CPS 1.3.1.3)
Policy Authority	The Policy Authority is the EPMA Chair and is responsible for compliance with all Entrust Managed Service Offerings and is the approver and signatory for CP, CPS and RPS updates.
Policy Authority Representative (PAR - Compliance)	The Policy Authority Representative - Compliance (PAR – Compliance) is responsible for ensuring compliance with the FPKIPA compliance requirements (CPS 1.1.3.4). This role is responsible for ensuring that Entrust and RA maintain the integrity of the FPKI audit boundary.
Policy Authority Representative (PAR Ops)	The Policy Authority Representative – Operations (PAR - Ops) is responsible for ensuring that the service is hosted and operated in compliance with FPKIPA requirements. The senior Trusted Role, the PAR Ops is a VP role at Entrust.
Operational Authority (OA)	The Operations Authority (OA) is the Director responsible for the Operations team and all aspects of ETPKISSP & NFI Operations. (CPS 1.3.1.6)
Service Manager, mPKI	The Service Manager is the business owner of ETPKISSP & NFI. Managing the go-to-market offering, service description and roadmap, pricing, service and customer advocacy, the Service Manager is a senior member of the Entrust Product Management team and the voice of ETPKISSP & NFI.
Technical Account Manager (TAM)	A Technical Account Manager (TAM) is an optional resource whose service may be procured by the RA Agency/Organization. Highly recommended by Entrust and the RAs who have engaged a TAM, these experienced PKI resources are valued by ETPKISSP customers.

For more information including a current list of role holders and contact information, contact the PAR-Compliance at mpkipa@entrust.com.

RA – Key Roles

Role	Description
Contract Signer	<ul style="list-style-type: none">• The individual who signed the mPKI Master Services Agreement with Entrust.• Appoints the Primary Point of Contact, may fill that role personally
Primary Point of Contact (PoC - Business)	<ul style="list-style-type: none">• By default, this is the Contract Signer unless someone else is assigned by the RA,• Appoints the First Registration Authority (RA). May fill that role personally.
First RA	<ul style="list-style-type: none">• The first administrative RA Account.• Verifies, adds and trains other RA and LRAs.• May be involved with training the RA Trusted Roles.

Role	Description
RA PMA Chair (CPS 1.3.1.5)	<ul style="list-style-type: none"> Chairs RA PMA Meetings, producing minutes as audit evidence. Collaborates with PAR-Compliance. Signatory for RPS, RAA and other relevant documents. Responsible for management of RA Trusted Roles – including documented periodic review and approval of staffing changes.
RA PMA– RA Assessment Audit prime	<ul style="list-style-type: none"> Manages the annual assessment option selected by the RA PMA. Collaborates with assessor and Entrust. Facilitates the assessor on-site visit. Provides Audit Opinion letter or equivalent to Entrust by September 30th each year.
RA PMA – Registration Practice Statement prime	<ul style="list-style-type: none"> Owens the RPS on behalf of the RA PMA. Collaborates with PAR-Compliance to produce final draft. Facilitates RA PMA Approval and Signature. Participates with PAR-Compliance in annual (at least) review.
Trusted Roles	<ul style="list-style-type: none"> As defined in the Common Policy CP and the Entrust CPS, Section 5.2.1. RA and LRA are Trusted Roles Trusted Agent, specifically, is NOT a Trusted Role and does not have system access.
RA personnel	<ul style="list-style-type: none"> Responsible for adding other RA and LRAs. Verifies Subscribers and Subscriber requests. Subscriber technical support. Enforcement of RPS and CPS practices. Maintains verification audit records.
LRA personnel	<ul style="list-style-type: none"> May add other LRAs within scope of the creating LRA's Subscriber view. Verifies Subscribers and Subscriber requests. Subscriber technical support. Enforcement of RPS and CPS practices. Maintains verification of Subscriber evidence, archived for audit.
Trusted Agents	<ul style="list-style-type: none"> TAs may only support verification of Subscribers. Does not have access to systems. Maintains verification of Subscriber evidence, archived for audit.

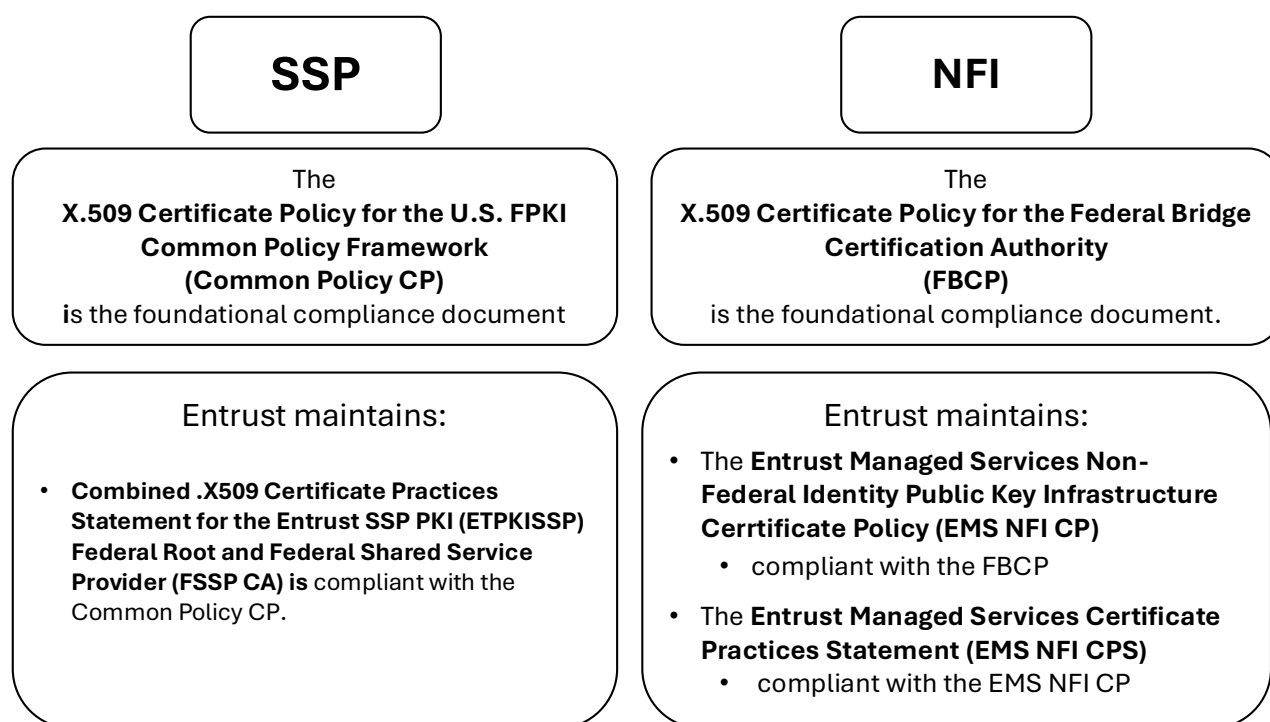
FPKI Compliance: An Overview

Consider the size and scope of the Federal PKI and the mandate for the FPKIPA and understand that they are responsible for compliance across the entire government landscape. In the US Federal Government private trust environment, it is critical that the Policy Management Authorities for each of the organizational participants strictly adhere to the applicable Policy Framework to ensure the integrity and security of the entire environment. Not only is it required to ensure the integrity of the FPKI audit boundary, but it is also a requirement for all participants as a condition of continued participation in FPKI.

The Common Policy CP and FBCP (Section 1.3.1.5) defines the requirement for each organization that participates in FPKI to establish and maintain a Policy Management Authority (PMA) to maintain compliance.

A Shared Cascade

ETPKISSP is hosted/operated by Entrust for the GSA, and as an FPKI Affiliate provider Entrust owns and operates EMS-NFI:



The Common Policy CP and FBCP frameworks for SSP and NFI contemplate compliance as a cascading responsibility shared by all organizations participating in FPKI. The cornerstone of compliance in each organization is the PMA.

PKI Participant	Compliance Mission
The Federal PKI Policy Authority (FPKIPA)	<ul style="list-style-type: none">Owns the Common Policy CP.Owns the FPKI CA – the root of FPKI Trust.Enforces policy on the Entrust PMA.
The Entrust Policy Management Authority (EPMA)	<ul style="list-style-type: none">Owns the NFI policy and SSP and NFI practices documentation that defines how Entrust and the RA Agency/Organizations (RA) operate in compliance with the Common Policy CP.

	<ul style="list-style-type: none"> • Responsible for Operational Compliance. • Annual assessment – Entrust submits the complete FPKI audit package to the FPKI GSA team on November 30th each year.
The Registration Authority Policy Management Authority (RA PMA)	<ul style="list-style-type: none"> • Owns the RA RPS, supported by Entrust. • Responsible for Operational Compliance.
Subscribers – Users and Devices	<ul style="list-style-type: none"> • <i>Subscribers is a term used to describe</i> subscribers or non-person entities such as computing and communications devices (routers, firewalls, servers, etc.). • Named as certificate subjects in the Certificate Distinguished Name (DN). • Devices must have a human sponsor who has been vetted to at least the assurance level required for the device.

The RA Compliance Guide

Compliance is ongoing, and the RA Compliance Guide, issued by the EPMA, provides the RA with guidance for establishing and maintaining the required compliance posture. The guide provides the requirement, the source of the requirement, and what that means to the RA. It also puts focus on how Entrust, through the TAM and PAR-Compliance roles, can provide support. In a shared services environment like FPKI, there is a dependence on collaboration and shared responsibility, and the guide outlines how Entrust is there to support the RA with every step.

Guidance for the Registration Authority (RA)

To this point we have focused on laying a foundation for orienting those new to FPKI and Entrust. We have described the organizations involved in FPKI, provided an overview of the shared responsibility for the compliance cascade, and identified resources to support the RA. In the following sections, we focus on the RA Organization and provide guidance on organizational responsibilities.

The RA Policy Management Authority

A CP requirement, the RA will appoint an RA PMA and implement a Charter to guide behavior and expectations. Complete information is available in the RA Compliance Guide, with direct support available from the PAR-Compliance, as needed.

The Registration Authority Agreement

Counter-signed by Entrust and the RA, the Registration Authority Agreement is an FPKI requirement that creates the agreement for Entrust to act as Service Provider and the RA to operate as a Registration Authority for their users. Complete information is available in the RA Compliance Guide.

An Overview of the Registration Practices Statement

A primary responsibility of the RA PMA is ownership of the RA Registration Practices Statement (RA RPS). While the Common Policy or Federal Bridge CP serve as the foundational FPKI policy documents, all Entrust CP and CPS documents are developed and maintained in alignment with those frameworks and the RA RPS builds upon the CPS by defining the specific practices used by the RA and RA personnel to operate in compliance.

The RA RPS documents RA specific practices, including but not limited to:

- The process by which subscribers are verified prior to issuing or managing credentials.
- Maintenance of identity verification records to support annual assessments.
- Subscriber support activities.
- Architecture and operational documentation for any on-premises components.

Although the RA PMA retains ownership of the RPS, its development and maintenance is a shared responsibility, and Entrust provides support in several ways:

- When implementation is performed by Entrust Professional Services, creation of the RA RPS is included in the applicable Statement of Work (SOW).
- The PAR-Compliance team can also provide direct support; assistance can be requested via mpkipa@entrust.com.
- The PAR-Compliance team meets at least annually (and ideally more often throughout the year) with the RA PMA prime to review and update the RA RPS. To set expectations, Entrust uses internal automated tools to generate an initial draft RA RPS. The RA PMA prime and PAR-Compliance then work collaboratively to review and refine the draft. The finalized RPS is submitted to the RA PMA and then the Entrust Policy Authority for final approval.

For the RA, the RPS serves multiple purposes:

- Providing RA personnel with clearly defined Rules of Behavior.
- Ensuring required audit evidence is systematically collected.
- Serving as the primary document for annual RA audit and internal assessments.
- Aligning the compliance posture between the RA and Entrust.
- Forming part of the annual audit package submitted by Entrust each year.

The RA is required to maintain a current, approved Registration Practices Statement (RPS) that accurately reflects RA practices and shall make the RPS available upon request during internal assessments, external compliance audits, or other reviews required by Entrust, the applicable CP, CPS, or FPKI oversight authorities.

A Trusted Role Overview

In a private trust environment such as the FPKI, where the scope is extremely broad, trust is sustained through a balanced application of people, processes, and technology. The model's greatest vulnerability exists at the Registration Authority (RA) level, underscoring the need to establish, comply with, and regularly audit Registration Authority Officer (RA) practices. This begins by ensuring that individuals with access to systems used to issue and manage credentials are properly vetted, trained, and formally appointed to Trusted Roles, as defined in CP documents in Section 5.

The roles designated as Trusted Roles under the CP and the Entrust CPS are managed by the RA PMA and documented in the applicable Registration Practice Statement (RPS). Evidence of Trusted Role management is an assessment requirement owned by the RA PMA. Entrust maintains a mature Trusted Role Management process, and the PAR-Compliance team is available to support the RA PMA, as needed.

Annual Assessment

Each RA is responsible for an annual assessment (commonly referred to as an RA Audit) and is further required to provide the outcome of that assessment (commonly, an RA Audit Opinion Letter) to Entrust for inclusion in the annual audit submission. In turn, Entrust is required to include such evidence from all the RA Organizations who work with Entrust with the audit submission. The RA Compliance Guide provides details on the annual assessment options and support available. The Entrust CPS requires that the RA PMA designates a primary point of contact (PoC) to own and manage the annual assessment process.

Section Summary

Once the topics outlined in these sections have been addressed, the RA Organization is prepared for production success and a compliant security posture. The net outcome is:

- The RA and Entrust have executed the necessary RAA to formalize the relationship with FPKI.
- RA PMA is in place, chartered, and has appointed primary points of contact, and shared this information with Entrust.
- Trusted Roles have been designated, staff identified and trained, and the RA PMA is actively managing the roster of Trusted Roles.
- An RPS has been approved, defining the practices used by the RA in accordance with the Common Policy Framework, repositories for required documentation are established and actively managed and an annual review with the PAR-Compliance has been scheduled.
- The RA is ready to undergo annual assessment and provide the outcome to Entrust.

The RA can leverage this document, the RA Compliance Guide, and the direct support of the PAR-Compliance to ensure organizational success. Contact mpkipa@entrust.com.

Guidance for RA/LRA personnel

The Registration Authority (RA) role is among the most critical roles in a private trust environment, as RAs serve as gatekeepers of the audit boundary and interact directly with Subscribers. Within the FPKI, each RA Organization employs RAs who are responsible for verifying Subscribers and issuing credentials that may be interoperable across the full scope of the FPKI. Alternatively, Agencies who prefer may work with an external authorized RA, such as US Access, to provide these services.

The RA PMA selects and verifies RA personnel, who are then trained, required to acknowledge applicable Subscriber Agreements, and formally appointed to Trusted Roles in accordance with the applicable Registration Practice Statement (RPS). Trusted Roles are defined in Section 5 of the Common Policy CP and the Entrust CPS.

Credentials may also be deployed to Certificate Management Systems (CMS) to support automated Subscriber credential issuance and management workflows.

The following sections provide guidance applicable to Registration Authority (RA) personnel.

Registration Authority Guidance

A Registration Authority (RA) is appointed by the RA PMA, who in turn is required to maintain and share the RA RA/LRA list with Entrust. Of note:

- There may be more than one RA.
- An RA may also perform LRA duties.
- Entrust is responsible for verification and enrollment of the first RA, who in turn can create the remaining required RA/LRA identities.
- RA credentials may be deployed to Certificate Management Systems (CMS).
- The First RA may be the Contract Signer, another qualified employee, or a third party authorized by the RA PMA to perform tasks on behalf of the RA.

Registration Authority (RA) Responsibilities:

- Maintain, through the RA PMA, a current and accurate list of authorized RA and LRA personnel.
- Submit, through the RA PMA, any digitally signed change requests for modifications to baseline certificate contents or applicable security policies.
- Maintain, through the RA PMA, a current approved Registration Practices Statement (RPS) and make it available upon request during internal assessments, external compliance audits, or other authorized compliance reviews.
- Perform LRA duties in accordance with the applicable CP, CPS, approved RA RPS, and Entrust-issued compliance requirements.
- Register and onboard new Registration Authorities (RAs) and Local Registration Authorities (LRAs).
- Train RAs and LRAs in Subscriber identity verification and in the issuance, renewal, revocation, suspension, restoration, and recovery of certificates.
- Where applicable, train Trusted Agents in Subscriber identity verification procedures. All personnel performing PKI trust functions, including but not limited to RAs, LRAs, and Trusted Agents, SHALL perform their assigned duties in strict compliance with the applicable CP, CPS, approved RA RPS, and Entrust-issued compliance requirements.
- Create and maintain a repository of verification records for each LRA, including verification evidence as defined in the RA Registration Practices Statement (RPS).

- Securely communicate approval of certificate requests to Entrust.
- Distribute activation data, certificate download instructions, and installation guidance to support LRA enrollment.
- Provide operational support to Subscribers.
- Verify and process certificate revocation, suspension, and restoration requests.
- Approve the issuance of certificates for network device Non-Person Entities (NPEs).
- Register individuals authorized to approve and receive role-based certificates.

Local Registration Authority

The **Local Registration Authority (LRA)** is the person or entity appointed by the RA PMA to perform certain functions on behalf of customer, including approving or rejecting subscriber application for a certificate license, based on information verified by the LRA, and instructing Entrust from time to time to issue, renew, or revoke certificates.

Local Registration Authority (LRA) Responsibilities:

- Perform LRA duties in accordance with the applicable CP, CPS, approved RA RPS, and Entrust-issued compliance requirements.
- Approval, communicated securely to Entrust, of certificate requests.
- Creating and maintaining verification records for each LRA, including verification evidence as defined in the RA RPS.
- Performing any verification function allocated to a Trusted Agent.
- Distributing activation data, certificate download instructions and installation details for LRA enrollment.
- Registering other LRAs and Subscribers.
- Providing operational support for Subscribers.
- Verification and processing of Revocation, Suspension, or Restoration requests.
- Approving issuance of certificates to network NPEs.
- Registering individuals to approve and receive role-based certificates.

Compliance with the RA RPS

For the RA and LRA community, consistent application of the practices approved by the RA PMA and documented in the RA Registration Practices Statement (RPS) is the most critical factor for RA program success. All personnel acting in a trusted PKI role, including but not limited to Registration Authorities (RAs), Local Registration Authorities (LRAs), and Trusted Agents, SHALL perform their assigned duties in strict compliance with the applicable Certificate Policy (CP), Certification Practice Statement (CPS), and approved RA RPS. Adherence to the RA RPS ensures:

- Preservation of the integrity of the FPKI audit boundary.
- Issuance of credentials only to Subscribers who meet applicable eligibility and verification requirements.
- Avoidance of operational disruption resulting from non-compliance.
- Successful completion of required annual reviews and audits.

The RA PMA is responsible for monitoring RA/LRA activities to ensure compliance with the RA RPS.

Maintaining Audit Evidence

During the annual RA assessment, an external independent auditor will examine records to determine that the RPS is compliant with the applicable CP and the Entrust CPS. When an RA/LRA verifies a Subscriber identity, evidence related to the verification process must be produced, archived securely,

and provided to the auditor in alignment with the practices captured in the RPS.

Managing Subscribers

The term Subscribers refers to qualified, verified, human users or non-human entities including devices (routers, firewalls, servers, etc.). Where a device is to be issued a certificate, there must be a Human Sponsor vetted to at least the assurance level of the device.

Subscriber Responsibilities

- Apply in person for credentials, providing appropriate identification for identity verification and approval.
- Should the Subscriber detect a need to revoke, suspend, restore, or recover certificates, a request must be presented to the RA/LRA.

Devices: Human Sponsor Responsibilities

The Human Sponsor assumes accountability for the associated device certificate and provides the information required to verify the request and issue the device certificate:

- Device Serial # or application identification (e.g. DNS name).
- Device or application Public Keys.
- Device or application authorization and attributes.
- Contact information to facilitate communication with the Human Sponsor.
- Should the Human Sponsor detect a need to revoke, suspend, restore, or recover certificates, a request must be presented to the RA/LRA.
- In-person registration by the PKI sponsor who has previously been vetted in accordance with these guidelines at an assurance level as high as the assurance level being requested.

Role-based certificates

A subset of human subscribers will be issued role-based certificates, which identify a specific role on behalf of whom the subscriber is authorized to act. Rather than the subscriber's name, role-based certificates are issued in the interest of supporting accepted business practices. Normally, it will be issued in addition to an individual subscriber certificate. The RA/LRA will authenticate Subscribers authorized to use the PKI in the name of an organization (PKI Sponsor). In addition, the RA/LRA will verify that the PKI sponsor applying for a role-based certificate is authorized to act in this role. The RA/LRA will request the certificate from the CA on behalf of the applicant and notify the applicant that the request has been made.

A specific role may be identified in certificates issued to multiple subscribers however, the key pair will be unique to each individual role-based certificate (i.e. there may be four individuals carrying a certificate issued in the role of "Secretary of Commerce" however, each of the four individual certificates will carry unique keys and certificate identifiers). Roles for which role-based certificates may be issued are limited to those that are held by a unique individual within an organization (e.g., *Chief Information Officer*; is a unique individual whereas *Program Analyst* is not).

Required Forms

For RA/LRAs, forms must be completed and submitted to Entrust prior to the issuance of the credential:

- a) Subscriber Agreement – Required: for each RA/LRA, and Trusted Agent if applicable. See Appendix A of this document for a copy of the Entrust Managed Services Subscriber Agreement.
- b) Identity verification is completed and signed in alignment with the RPS, and must be completed and signed for each RA, LRA, TA and Subscriber End-entity prior to digital credential issuance. See Appendix B for the Verification Form template and instructions.
- c) Where the RA engages a Trusted Agent to perform user verification, the form in Appendix C is used.

Acceptable Forms of ID for Verification

Photo ID (select only one) Column A	-or- Government IDs (select one from each column B and C)	
	Column B	Column C
Federal Government photo ID	State-issued driver's license	US social security card issued by the Social Security Administration
Entrust employee photo ID	State-issued photo identification card	Original or certified copy of birth certificate issued by a state, municipal or county agency and bearing an official seal
US Passport (unexpired or expired)		
Certificate of US Citizenship		
Certificate of Naturalization		
US Military ID card		

Appendix A – ENTRUST MANAGED SERVICES SUBSCRIBER AGREEMENT

Please select the box that best describes the purpose of filling out the form:

☐ Initial Issuance ☐ Certificate Recovery ☐ Certificate Update ☐ Certificate Revocation ☐ LRA ☐ RA ☐ TA

Your sponsoring organization has subscribed to certain public key encryption and digital signature services offered by Entrust, Inc. Accordingly, as an employee or contractor, you have been authorized to receive a digital certificate containing a public key. In addition, you will receive a private key that corresponds to the public key listed in your digital certificate. The private key will enable you to digitally sign documents, identify yourself to gain access to systems, or to decrypt data that has been encrypted for you. Other persons, organizations and/or applications will use your public key to verify your digital signature; to identify you for access control purposes or to encrypt data for you so only you can decrypt it.

Your Obligations

As a user of the public key encryption and digital signature service, you agree to the following:

- a) You will comply with your employer's security policies, rules, and regulations regarding the use of any software and/or digital certificate provided to you, and which includes the protection and safeguarding of any passwords and private keys in a secure manner.
- b) You will use any digital certificates and private keys provided to you by your employer only for employer-related business transactions.
- c) You acknowledge that the use of a private key shall be deemed to be an acceptance of the related public key and associated certificate and the terms and conditions of the issuing CA's certificate policy.
- d) As soon as you become aware of, or suspect the compromise of your private keys, passwords and/or software, you will promptly report this to your employer.
- e) You will always make true representations regarding the information in your digital certificate and the information provided to your employer. You must notify your employer if your personal information changes (name change, organization change, email address change, etc.) throughout the duration of your use, so the certificate information is correctly updated.
- f) You represent and warrant that you are not located in, under the control of, or are a national or resident of any country to which the export of the cryptographic hardware and/or software or related information would be prohibited by applicable export laws (including, but not limited to, the laws of the United States of America and Canada).

Revocation of Digital Certificates

Your certificate may be revoked at any time and without notice. The reasons for such revocation include, but are not limited to, the following:

- Your private key is lost, stolen, or suspected of having been compromised
- Your private keys or certificates become unavailable, and no recovery is possible
- Your identifying information contained in the digital certificate is no longer valid
- You are suspected of fraud or other adverse behavior
- You violate this Subscriber Agreement

Liability

By signing this Subscriber Agreement, you agree that Entrust, Inc. and its subsidiary companies have no liability to you arising out of or relating to your use of any digital certificates issued to you. This includes any liability for any expenses, losses and/or damages, whether direct or indirect, incidental, compensatory, consequential, special, or punitive.

Registrar				
By signing below, the undersigned Registrar avers that he or she has personally: (1) verified the eligibility of the Applicant/Subscriber to receive certificates; (2) verified the identity of the Applicant/Subscriber in accordance with procedures defined in the applicable Certification Practices Statement (CPS); (3) witnessed the Applicant/Subscriber sign this form. I affirm that the foregoing is true and correct.				
Title:				
Date:	Time:			
PRINT NAME:				
<i>(First Name, Middle Initial, Last Name)</i>				
City / County:	State:	ZIP:		
Registrar Signature:				

Applicant/Subscriber	
I have read and understand this Subscriber Agreement and I agree that I will abide by the terms and conditions of this Subscriber Agreement and will meet my obligations as set forth therein. I acknowledge receipt of the Token as indicated below. I affirm that the foregoing is true and correct.	
Per:	
<i>(Authorized Signature)</i>	
Name:	
<i>(Print Name)</i>	
PKI Role:	
Employer:	
Date:	Time:
Include details below as required for Subscriber's Assurance	

Identity Verification	
Type of Identification	
Issuing Authority	
Identification Number	

Identity Verification (if necessary)	
2 nd Type of ID	
Issuing Authority	
Identification Number	

Token Issuance		
☐ USB Token	☐ Smartcard	☐ None
Model:		
Serial Number:		
CA Name:		

Digital Photo	
Camera Serial Number:	
Media Identification Number:	
Digital Image Number:	

Appendix B - ENTRUST MANAGED SERVICES SUBSCRIBER IDENTITY VERIFICATION (by Local Registration Authority)

This form provides Entrust, Inc. with evidence that the authorized applicant's identity has been verified. This form must be completed in its entirety and signed by either an existing vetted customer LRA or an Entrust-designated TA. The RA or its designated representative shall personally verify the applicant's identity, including any information to be included in the certificate. The verifier shall record the process that was followed for issuance of each certificate.

Device Certificates:

Device certificates shall be assigned to an individual who will be responsible for the use of the Device certificate. The following information is required for authenticating these requests:

- The user shall follow the authentication mechanism stipulated in this section to establish their identity. Alternatively, if this user already has a certificate issued by Entrust Managed Services, they may submit a digitally signed request for a device certificate that is of an equal or lower assurance level.
 - Equipment (e.g., serial number) or application identification (e.g., DNS name);
 - Equipment or application Public Keys;
 - Equipment or application authorization and attributes (if they will be included in certificate); and
 - Contact information to enable the CA or RA to communicate with the Sponsor

RA shall ensure that records are maintained for all certificate Applicants. Copies of the identification information including any biometric information about the applicant shall be recorded, attached to the application, and maintained by the RA/LRA. Such information may include fingerprints, retina scans, photographs, facial scans, or other physical characteristics. Once the identity of the applicant/subscriber has been verified, the signed identity verification form and attached photocopies must be archived for a minimum of 10.5 years, for audit purposes, by the party verifying the identity of the applicant/subscriber.

For questions regarding the subscriber identity verification process, please contact Entrust, Inc. at:

Phone: 1-877-754-7878 (toll-free)

E-mail: support@Entrust.com



Appendix C - SUBSCRIBER IDENTITY VERIFICATION (by Local Registration Authority)

PRINT NAME: _____
(First Name, Middle Initial, Last Name)

Subscriber E-mail Address: _____

Business Address: _____

City: _____ State/Province: _____ Zip/Postal Code: _____

Business Phone Number: _____

Date of Birth (optional, for use as verifying information): _____

I hereby represent that all above information is true and accurate.

Signature: _____
(Sign in the Presence of a Customer LRA or Entrust-designated Trusted Agent)

I hereby declare that on this day of _____, 20__ , _____ personally appeared before me as the signer and subject of the above form, who signed or attested to the same in my presence, and presented one form of identification (if issuing Basic Assurance certificates) or two forms of identification (if issuing Medium Assurance certificates) from the following list as proof of his or her identity (check IDs reviewed):

- ☐ *Driver's License or Government/Company-Issued ID Card*
- ☐ *Social Security Card or Social Insurance Number*
- ☐ *Passport*
- ☐ *Birth Certificate*
- ☐ *Military ID Card*

Customer LRA or Trusted Agent - Registrar		
<p>By signing below, the undersigned Registrar avers that he or she has personally: (1) verified the eligibility of the Applicant/Subscriber to receive certificates; (2) verified the identity of the Applicant/Subscriber in accordance with procedures defined in the applicable Certification Practice Statement; (3) witnessed the Applicant/Subscriber sign this form. I affirm that the foregoing is true and correct.</p>		
Title:		
Date:	Time:	
PRINT NAME:		
<i>(First Name, Middle Initial, Last Name)</i>		
City / County:	State:	ZIP:
Registrar Signature:		

Device Certificate Details:	
Equipment serial # or application identification (DNS name, MS GUID as applicable);	
Equipment or application Public Keys;	
Equipment or application authorization & attributes (if to be included in the certificate):	
Contact info to enable CA or RA to communicate with the Sponsor:	