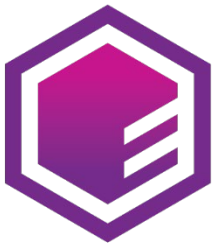


ENTRUST

Registration Authority (RA) & Local Registration Authority (LRA) Orientation Guidelines

***Return form (Appendix A &/or C) to Project Manager**

DATE: June 17, 2025

VERSION: 7.2

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

DISCLAIMER

This document is intended to provide clear guidance for US Federal Agencies and Organizations that act in the RA role. Requirements are defined in Common Policy Framework (Common Policy CP) with program requirements posted by the GSA at: https://www.idmanagement.gov/FPKI/#audit-information-for-the-FPKI-management-authority. Entrust Certificate 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 NFI CP and CPS documents shall be deemed accurate for defining requirements.

Using this Document

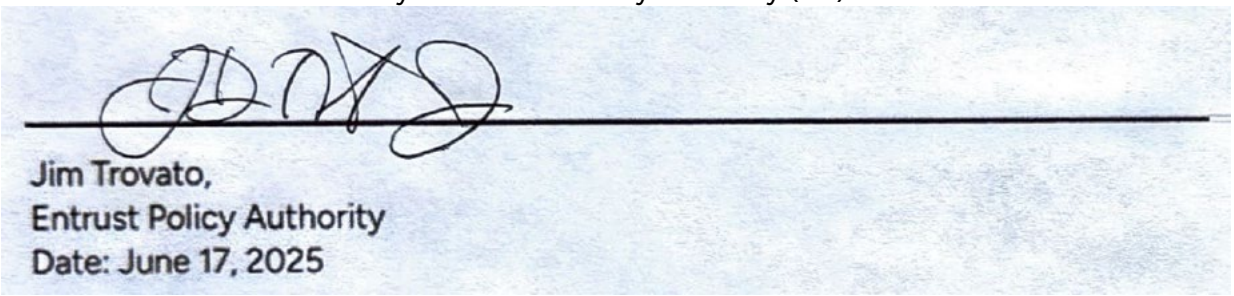
This document contains references to Sections of various CP/CPS and RPS documents. All such documents in the FPKI private trust environment adhere to RFC 3647. Where a section number is referenced, the content subject matter will be consistent across documentation.

- A Certificate Policy (CP) defines the policy requirements (The CP defines *what* we have to do).
- A Certification Practices Statement (CPS) defines the practices used by Entrust to address CP requirements, and the compliance requirements for RA Organizations (RAO) (The CPS defines *how* Entrust meets policy requirements and sets requirements for the RAO).
- A Registration Practices Statement defines *how* your organization, as an RA, employs practices that are compliant with the CPS requirements.

For example, a reference to "Section 5.3 – Personnel Controls" allows the reader to explore the CP, to identify the policy requirements around issues like background checks, training and re-training, job-rotation, managing unauthorized access, and more. The CPS, defining how Entrust approaches each issue from a practices perspective, and what is required of an RA. The RPS, defining how the RAO addresses the requirements captured in the CPS. Leverage each document to explore subjects from a 360-degree perspective.

SIGNATURE

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



Contents

1. 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.

1.1 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
- Key Forms – templates

When finished, a reader will understand the FPKI landscape, participating organizations and their roles, how Entrust can support each step of the RA journey, the major building blocks of implementation success, the obligations of each organization, and the roles of the RA Organization and Trusted Role staff. An overview of the Compliance cascade will build an understanding of the shared responsibility and organizational posture required by FPKI and Entrust. And finally, our goal is to ensure that you are connected to the Entrust team, who are dedicated to your success.

1.2 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.

2. Understanding FPKI

2.1 The Roots of FPKI Authority

The Federal Public Key Infrastructure (FPKI) provides the government with a trust framework and infrastructure to administer digital certificates and public-private key pairs. This private trust framework was established by the Federal Chief Information Officer (CIO) Council, comprised of the Chief Information Officers of all cabinet level departments and other independent agencies as the Federal PKI (FPKI), and oversees the operation of the organizations responsible for governing and promoting its use. The X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, known as the Common Policy CP, was established under the authority and approval of the Federal CIO Council. (Reference: Common Policy CP 1.3.1.1)

2.2 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 Common Policy CP 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)

2.2.1 FPKI Policies & Practices: Key FPKI Documentation

- Font FPKI Program information is available at: https://www.idmanagement.gov/fpki/
- The FPKIPA maintains the X.509 Certificate Policy for the U.S. FPKI Common Policy Framework, which defines the compliance requirements for each PKI participant.

2.3 Entrust, an SSP Affiliate

Entrust maintains an Authority to Operate as an FPKI Affiliate Shared Services Provider. From an RA perspective, this really includes three service models.

- Entrust PKI Shared Service Provider (ETPKISSP), owned by GSA and operated by Entrust, provides certificates issued to government employees and devices (known as Subscribers). This service leverages Shared Service Provider Issuing CAs to issue credentials to Agency Employees or Contractors carrying PIV cards.
- Entrust Managed Services – Non-Federal Identities (EMS-NFI) is owned and operated by Entrust, providing certificates issued to non-federal identities for organizations approved by the FPKIPA for FPKI participation.
- The Derived Credentials Management Service leverages PIV Cards for authentication to derive, create, and distribute derived certificates to mobile devices.

2.3.1 Entrust Policies & Practices: Key Entrust Documentation

Entrust is responsible for the policy and practices documentation which governs operations as an SSP Provider. These documents are subject to review and approval by the FPKIPA. From a compliance perspective, all documentation must align with the FPKI framework, and is reviewed for compliance against the Common Policy CP. This highlights the shared responsibility of compliance in a private trust environment; the PKIPA manages and enforces compliance through the Common Policy CP and review of an audit package submitted by Entrust annually on November 30th.

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

Whereas ETPKISSP is owned by GSA, and hosted/operated by Entrust, as an FPKI Affiliate provider Entrust owns and operates EMS-NFI. The EMS-NFI CP defines the policies for NFI operations in alignment with the Federal Bridge Certification Authority (FBCA) CP, and the EMS-PKI NFI CPS Captures the practices used by Entrust and the RAO to align NFI practice and policy.

2.4 The Registration Authority (RA)

US Federal Agencies and Organizations approved for FPKI participation as a Registration Authority (known as RA Organizations, or RAO) 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 software, for example, for Derived Credentials an on-premises component may be part of the RA architecture, hosted and operated by the RAO and subject to annual assessment.

The RAO, 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 RAO:

- Establish and maintain an RAO PMA (Common Policy 1.3.1.5)
- Execute a Registration Authority Agreement with Entrust (online- click here)
- Establish and maintain a Registration Practices Statement (RPS) (online reference – click here)
- 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.

2.4.1 Local Registration Authority (LRA)

A Local Registration Authority (LRA) administers a specific group of users. An LRA is typically employed by the RAO 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 RAO 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 and are not able to add RAs.

2.4.2 Policies and Practices: Key RAO Documentation

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

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

The RPS is a critical compliance document and is used during the annual assessment where the RAO 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.

2.5 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 (revoke, suspend, restore, third-party recovery, etc.)

2.6 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 for all Entrust Managed Service Offerings.
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 Agency/Organizations maintain the integrity of the FPKI audit boundary. The PAR – Compliance reports to the EPMA and is a direct report to the Director, Compliance (Entrust PA).
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.

Role	Description
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 RAOs 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 mpki@entrust.com.

2.7 RAO – Key Roles

Role	Description
Contract Signer	• The individual who signed the mPKI Master Services Agreement with Entrust. • Appoints the Primary Point of Contact, may fill that role personally
First RA	• A cornerstone in the on-boarding process • Adds and trains additional RA
Primary Point of Contact (PoC)	• Appoints the First Registration Authority (RA). May fill that role personally. • By default, PoC is the Contract Signer unless someone else is assigned by the RAO PMA. • To appoint new RA's the POC will need to fill out Appendix C and return it to Entrust.
First RA	• The first administrative RA Account • Verifies and Creates other RA and LRAs • Typically involved in training Trusted Roles and other RA/LRA personnel
RAO PMA Chair (CPS 1.3.1.5)	• Chairs RAO PMA Meetings, producing minutes as audit evidence • Collaborates with PAR-Compliance • Signatory for RPS, RAA and other documents • Responsible for RAO Trusted Role management
RAO PMA– RA Assessment Audit prime	• Manages the annual assessment option selected by the RAO PMA • Collaborates with assessor and Entrust • Facilitates assessor on-site visit • Provides Audit Opinion letter or equivalent to Entrust by September 30th each year
RAO PMA – Registration Practice Statement prime	• Owns the RPS on behalf of the RAO PMA • Collaborates with PAR-Compliance to produce final draft • Facilitates RAO PMA Approval and Signature • Participates with PAR-Compliance in annual (at least) review
Trusted Roles	• As defined in the Common Policy CP and the Entrust CPS.

Role	Description
RA personnel	• May add other RA and LRAs • Verifies Subscribers and Subscriber requests • Subscriber technical support • Enforcement of RPS and CPS practices • Maintains verification audit records
LRA personnel	• 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	• Engaged by the RAO when support is required for verification of Subscribers. • Does not have access to systems • Maintains verification of Subscriber evidence, archived for audit

3. 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 landscape. In the US Federal Government private trust environment, it is critical that the Policy Management Authorities for each of the organizational participants to strictly adhere to the Common 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 (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.

3.2 A Shared Cascade

The Common Policy framework contemplates 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)	• 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)	• Owns the policy and practices documentation that defines how Entrust and the RA Agency/Organizations (RAO) operate in compliance with the Common Policy CP • Operational Compliance • Annual assessment – Entrust submits the FPKI audit package on November 30th each year
The Registration Authority Organizational Policy Management Authority (RAO PMA)	• Owns the RAO RPS, supported by Entrust. • Operational Compliance
Subscribers – Users and Devices	• *Subscribers is a term used to describe* 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

3.3 The RA Compliance Guide

Compliance is ongoing, and the RA Compliance Guide, issued by the EPMA, provides the RAO with guidance for establishing and maintaining the appropriate posture. The guide provides the requirement, the source of the requirement, and what that means to the RAO. It also puts focus on how Entrust, through the TAM and PAR-Compliance, 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 RAO with every step.

4. Guidance for the Registration Authority Organization (RAO)

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 RAO. In the following sections, we focus on the RA Organization and provide guidance on organizational responsibilities.

4.1 The RAO Policy Management Authority

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

4.2 The Registration Authority Agreement

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

4.3 An Overview of the Registration Practices Statement

One of the prime responsibilities of the PMA is ownership of an RAO Registration Practices Statement (RAO RPS). Where the Common Policy CP is the core FPKI policy document and all Entrust CP and CPS documents are developed and maintained in accordance with the framework, the RAO RPS builds on the CPS, defining the practices that the RAO and RA personnel use to operate in compliance. These are practices specific to the RAO for responsibilities such as:

- Verification of users prior to issuing or managing credentials.
- Maintenance of verification records for annual assessment.
- Subscriber support.
- Architecture documentation for any on-premises components.

Although owned by the RAO PMA, establishing an RPS is a shared responsibility and Entrust provides support for the RAO:

- Where the implementation has been done by Entrust Professional Services, the creation of the RPS is contained in the SOW.
- The PAR-Compliance can support you directly, contact mpkipa@entrust.com.

The PAR-Compliance will meet annually with the RAO PMA prime to review and update the RPS. To set expectations, Entrust has automated tools we use to derive a draft RAO RPS. The RAO PMA prime and the PAR-Compliance meet to work through the draft. The final is submitted to the RAO PMA and the Entrust Policy Authority for approval. For the RAO, the RPS may be used:

- To provide RA personnel with the Rules of Behavior
- To ensure the collection of required audit evidence
- As the core document for an RA Audit or Annual Assessment
- As the document which aligns the compliance posture for the RAO and Entrust.
- As an element of the annual audit package, Entrust Submits each November 30th.

4.4 A Trusted Role Overview

In a private trust environment like FPKI where the scope is extremely broad, trust is maintained by a balance of people, process and technology. The greatest vulnerability to the model exists at the RA level, reinforcing the need to establish, comply with, and audit RAO practices. It starts by ensuring the people who can access the systems that issue and manage credentials have been verified, trained and appointed to Trusted Roles as defined in the Common Policy CP Section 5.3

The roles that the RAO PMA designates as Trusted Roles under the Common Policy CP and the Entrust CPS are managed by the RAO PMA and identified in the RPS. Evidence of Trusted Role management is an assessment requirement owned by the RAO PMA. Entrust has a mature Trusted Role Management process, and the PAR-Compliance is available to consult with the ROA PMA for support if needed.

4.5 Annual Assessment

Each RAO is responsible for an annual assessment and is further required to provide the outcome of that assessment 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 RAO PMA designates a primary point of contact (PPC) to own and manage the annual assessment process.

4.6 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 RAO and Entrust have executed the necessary RAA to formalize the relationship with FPKI.
- RAO 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 RAO PMA is actively managing the roster of Trusted Roles.
- An RPS has been approved, defining the practices used by the RAO in accordance with the Common Policy Framework, and an annual review with the PAR-Compliance has been scheduled.
- The RAO is ready to undergo annual assessment and provide the outcome to Entrust.

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

5. Guidance for RA/LRA personnel

The RA role is the most important role in the entire private trust environment because they are the gatekeepers of the audit boundary and interact directly with users. Across FPKI, each RA Organization has RAs verifying Subscribers and issuing credentials with interoperability across the entire scope of FPKI. The RAO PMA selects and verifies RA personnel, who are subsequently trained, sign a Subscriber Agreement, and are appointed to the Trusted Role as per the RPS. Trusted Roles are defined in Section 5.3 of the Common Policy CP and the Entrust CPS. The following Sections provide Guidance for Registration Authority (RA) personnel.

5.1 Registration Authority Guidance

A Registration Authority (RA) is appointed by the RAO PMA, who in turn is required to maintain and share the RAO 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 enrolment of the first RA, who in turn can create the remaining required RA/LRA identities,
- The First RA may be the Contract Signer, another qualified employee, or a third party authorized by the RAO PMA to perform tasks on behalf of the RAO.

5.1.1 Registration Authority (RA) Responsibilities:

- Through the RAO PMA, maintain a current list of RAO RA/LRA personnel.
- Through the RAO PMA, submit any digitally signed change requests for modifications to baseline certificate contents or security policies.
- Adding new RA/LRAs
- Training other RAs and LRAs in Subscriber verification, and to issue, renew, revoke. suspend, restore and recover certificates.
- If applicable, training Trusted Agents in Subscriber verification.
- Creating and maintaining verification records for each LRA, including verification evidence as defined in the RAO RPS.
- Approval, communicated securely to Entrust, of certificate requests.
- Distributing activation data, certificate download instructions and installation details for LRA enrolment.
- Registering other RAs and LRAs.
- 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.

5.2 Local Registration Authority

The Local Registration Authority (LRA) is the person or entity appointed by customer 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.

5.2.1 Local Registration Authority (LRA) Responsibilities:

- Approval, communicated securely to Entrust, of certificate requests.
- Creating and maintaining verification records for each LRA, including verification evidence as defined in the RAO RPS.
- Performing any verification function allocated to a Trusted Agent.
- Distributing activation data, certificate download instructions and installation details for LRA enrolment.
- Registering other LRAs and Subscribers.
- 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.

5.3 Compliance with the RAO RPS

Consistent application of the practices that the RAO PMA has approved in the RAO RPS is, for the RA/LRA Community, the most important success factor for RAO success, ensuring:

- The integrity of the FPKI audit Boundary.
- Only users who qualify are issued credentials.
- Avoiding disruption due to non-compliance.
- Securing annual review success.

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

5.4 Maintaining Audit Evidence

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

5.5 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.

5.5.1 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.

5.5.2 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.

5.6 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 LRA will authenticate Subscribers authorized to use the PKI in the name of an organization (PKI Sponsor). In addition, the LRA will verify that the PKI sponsor applying for a role-based certificate is authorized to act in this role. The 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).

6. 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 Agents 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 per RPS practices. Must be completed and signed for each RA, LRA, TA and End- entity prior to digital credential issuance. See Appendix B for the Verification Form and instructions.
c) Where the RAO engages a Trusted Agent to perform user verification, the form in Appendix C is used.

6.1 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 Certificate 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:		
(First Name, Middle Initial, Last Name)		
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:	
(Authorized Signature)	
Name:	
(Print Name)	
PKI Role:	
Employer:	
Date:	Time:
Include details below as required for Subscriber's Assurance	

Identity Verification	
Type of Identification	
Issuing Authority	
Identification Number (last four digits only)	

Identity Verification (if necessary)	
2nd Type of ID	
Issuing Authority	
Identification Number (last four digits only)	

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

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

Appendix B - SUBSCRIBER IDENTITY VERIFICATION: RA GUIDANCE

(by Local Registration Authority)

Entrust requires evidence that the authorized Subscriber applicant's identity has been verified. The form in Appendix C must be completed and signed by either an existing vetted LRA or designated TA. The 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 prior to issuance of Subscriber certificates.

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

Subscriber Applications: Verification and Archival Requirements
RA shall ensure that records are maintained for all certificate Applicants. Under the practices in the Entrust CPS, it is forbidden to capture and retain copies of personal identification used in the verification process. Only the last four (4) digits of the unique identification number are required to represent, for example, that a Subscriber's driver's license with the last four digits of XXXX was presented to the RA/LRA/TA for verification purposes.
The RA Organization may use biometric information (including fingerprints, retina scans, photographs, facial scans, and other physical characteristics). Details of biometric use are captured in the RA Registration Practices Statement (RPS), which specifies how biometric information is captured, verified, and archived. Per the RPS:

- Biometric information about the applicant shall be recorded, attached to the application, and maintained by the RA/LRA.
- An archive of all verification information must be maintained and available for annual audit or assessment.
- Signed and executed Subscriber forms and associated verification information must be archived by the RA for 10.5 years and remain available for audit purposes.

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 the 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 two forms of identification from the following list as proof of 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		
By signing below, the undersigned Registrar avers that they have 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; (3) witnessed the Applicant/Subscriber sign this form. I affirm that the foregoing is true and correct.		
Title:		
Date:	Time:	
PRINT NAME:		
(First Name, Middle Initial, Last Name)		
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:	