Entrust FPKI RA Compliance Guide

Guidance for US Federal Government Agencies using Entrust ETPISSP, NFI and Derived Credentials

Abstract

This document captures FPKI requirements for Entrust and guidance for Agencies / Organizations who act in the RA/ LRA capacity.

DATE: June 17, 2025

VERSION: 1.0

REVISION HISTORY

Revision	Section	Description	Contributors
1.0	New Document – All sections	Capture compliance requirements for RA Agency/Organizations who subscribe to the Entrust ETPKISSP SSP Service for the US Federal Government.	K. Brown, P. Garritty, P. Dean, C. Pommier, L. Rahman, R. Barton, A. Walt, R. Boateng. Approval: J. Trovato

Audience

This document outlines the governance and compliance obligations for RA Agency/Organization (RAO) Policy Management Authority personnel, in alignment with the Federal Public Key Infrastructure Policy Authority (FPKIPA) and the Common Policy Certificate Policy (CP). It further details Entrust-specific compliance requirements for RAOs subscribing to the ETPKISSP Service.

About this Guide

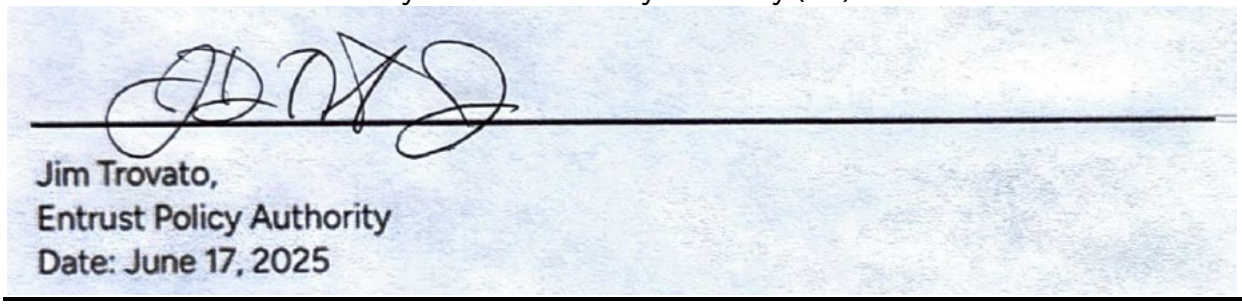
Although this guide can be printed, it relies on hyperlinks to other sections. It is best viewed and used electronically. Feedback and questions may be directed to the EPMA at mpkipa@entrust.com.

DISCLAIMER

This document is intended to provide clear compliance requirements 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 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 NFI CP and CPS documents shall be deemed accurate for defining requirements.

SIGNATURE

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



Contents

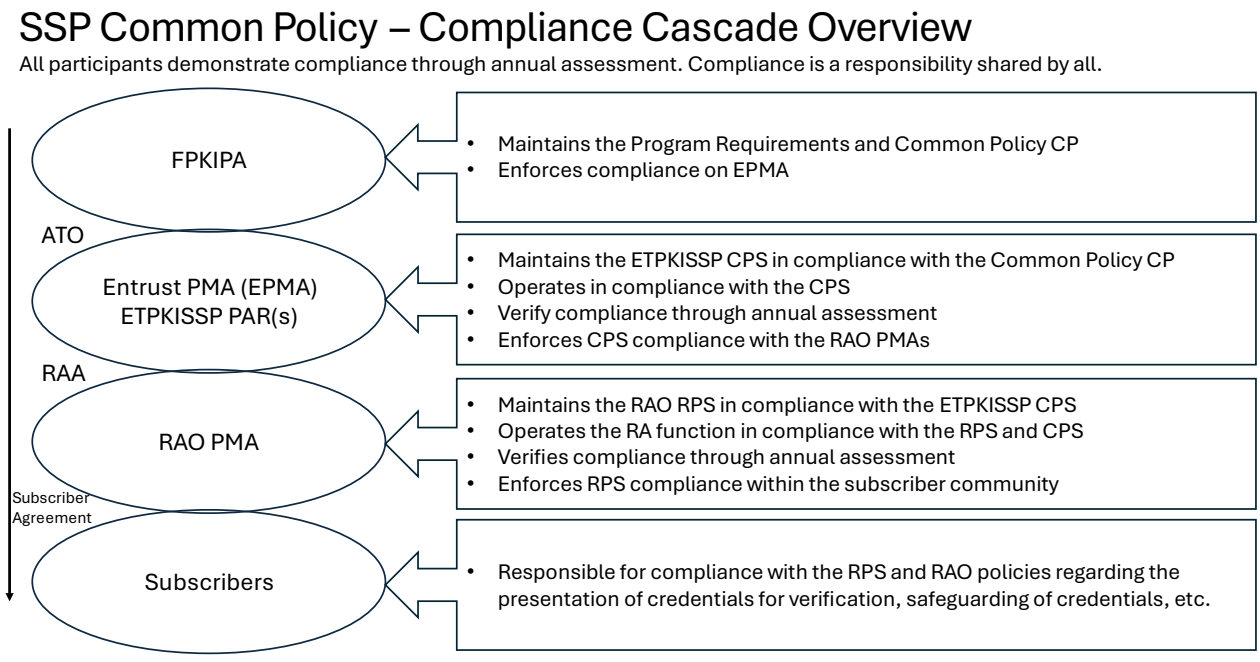
1. Introduction

Welcome to the 2025 Entrust PKI Shared Service Provider (ETPKISSP) RA Compliance Guide. Throughout 2024, Entrust experienced significant growth and transformation under new executive leadership, reinforcing a "compliance first" philosophy and implementing organizational changes to drive operational maturity. In 2025, our focus sharpens further with an emphasis on Compliance Excellence and a zero-tolerance approach to audit deviations, ensuring the highest standards of operational integrity across the FPKI environment.

The ETPKISSP is owned by the GSA and is part of the Entrust Managed PKI (mPKI) Services portfolio and Entrust hosts and operates the service in an environment dedicated to the US Federal Government. This document provides essential guidance for Agencies and Organizations operating as Registration Authorities (RAO – Registration Authority Organization), ensuring alignment with ETPKISSP operational practices and maintaining the integrity of the FPKI audit boundary, in accordance with requirements published at:

https://www.idmanagement.gov/FPKI/#audit-information-for-the-FPKI-management-authority.

This guide also outlines Entrust compliance requirements for all ETPKISSP Service subscribers.



2. Compliance Requirements

The FPKI Policy Authority defines and manages the compliance requirements for participation in the FPKI SSP program. Information regarding this program and the requirements for each participant are available online at: https://www.idmanagement.gov/FPKI/#audit-information-for-the-FPKI-management-authority.

The framework for compliance for ETPKISSP and service to the US Federal Government is the Common Policy CP, available at: https://www.idmanagement.gov/docs/FPKI-x509-cert-policy-common.pdf.

2.1 ETPKISSP Requirements

Entrust undergoes a tri-annual Authority to Operate (ATO) renewal process to maintain authorization for operating ETPKISSP as a Federal Public Key Infrastructure (FPKI) Shared Services Provider (SSP) under the Common Policy Framework.

As an FPKI SSP affiliate provider, Entrust develops and maintains the ETPKISSP Certificate Practices Statement (ETPKISSP CPS), a proprietary document that is subject to approval by the FPKI Policy Authority (FPKIPA). While the Common Policy Framework (Common Policy CP) defines what is required of an SSP CA provider, the ETPKISSP CPS specifies how Entrust operational practices meet these requirements.

In accordance with FPKI requirements (outlined here), Entrust also completes an annual independent third-party audit. This audit reviews documentation, data centers, and supporting evidence to verify that ETPKISSP operations comply with the Common Policy framework as implemented through the Common Policy CP and the ETPKISSP CPS.

As part of the annual audit process, ETPKISSP submits a compliance package to the FPKI Management Authority at fpki@gsa.gov, a process which includes:

- Preliminary review of the audit package with the FPKI team at the Annual Audit Kick-off meeting held at the beginning of November.
- Formal submission of the finalized audit package by November 30.

The annual submission includes an Assertion of Scope, which defines the ETPKISSP audit boundary. This boundary encompasses ETPKISSP data centers and Agencies/Organizations operating in Registration Authority (RA) or Local Registration Authority (LRA) roles. These organizations are identified in Appendix B of the ETPKISSP CPS and are individually referred to as a Registration Authority Organization, or RAO.

2.2 Agency Compliance Requirements

RAOs are also subject to annual requirements defined by the FPKIPA and available here: https://www.idmanagement.gov/FPKI/#annual-review-requirements-for-all-certification-authorities.

RA Agencies and RA Organizations are considered in-scope of the ETPKISSP annual review process where the RAO:

- Acts as the RA for Agency subscribers.

- Hosts on premise components that connect to the ETPKISSP.

Entrust ETPKISSP requires that RAOs fulfill the RA obligations and provide the required output to Entrust for inclusion in the annual audit package, and for audit preview, by September 30th each year. The following table summarizes the RA Agency obligations defined by FPKI in the Common Policy CP:

Item	Brief Description	More Information
Agency PMA	The RAO is required to appoint a RAO PMA to work as points of contact for the Entrust ETPKISSP PMA to communicate with. The RAO PMA is responsible for the RPS, the RA Audit, and for ensuring that Agency operations are compliant with the Agency RPS and the ETPKISSP CPS.	See the Section The *RA Agency /Organization PMA* later in this document.
RAA	Registration Authority Agreement – Signed by ETPKISSP and the RAO PMA, ensures alignment on the roles and requirements.	See the Section *The Registration Authority Agreement (RAA)* later in this document.
RPS	The Registration Practices Statement captures critical architecture and RA practices for the RAO and EMS PKI. A critical component of the annual RA Audit.	See the Section *The Registration Practice Statement (RPS)* later in this document.
RA Audit	The RAO PMA is responsible for completing an annual RA Audit (or approved alternative) and must provide the outcome to ETPKISSP on or before October 31, annually.	See the Section *The Annual RA Assessment* later in this document.

2.2.1 The RA Agency / Organization Policy Management Authority

The RAO is required to establish and maintain a Policy Management Authority per the Common Policy CP:

Policy Management Authority (PMA) (Section 1.3.1.5)

A PMA is an individual or group established by an organization or agency for the purpose of ensuring all PKI components are operated in compliance with an appropriate CPS and this CP. All organizations and agencies operating a PKI under this policy must establish a PMA. The PMA must identify an individual to serve as the liaison for that organization or agency to the FPKIPA.

The ETPKISSP CPS addresses this need:

Agency PMA (section 1.3.1.5)

Each agency is obligated to establish an Agency PMA, responsible for ensuring that any on premise PKI components and internal registration processes are run in compliance with the Common Policy CP and this CPS. The Agency PMA members serve as points of contact for the EPMA and provide directions for agencies, with details recorded in the RPS. The Agency PMA is responsible for establishing and maintaining the RPS, the annual RA audit or other compliant assessment, and providing the audit opinion evidence to Entrust on or before October 31, annually.

The EPMA, through the PAR, is responsible for coordinating with the Agency PMA to meet agency-specific requirements in compliance with the Common Policy CP and this CPS. The EPMA will communicate directly with the Agency PMA. Notifications may include service windows, unexpected outages, security bulletins, configuration changes, CPS Updates, or any other information that can affect normal operations.
For agencies utilizing the USAccess Program, the ETPKISSP provides any necessary notifications directly to the USAccess Project Management Office and sends email notifications to the RAO PMAs.
For the Department of Energy and the Department of Health and Human Services, agency PMAs are notified directly via email and/or telephone of any changes or service outages that may affect them.

"**Appendix B - Agency Contacts"** of this document provides a worksheet intended to help Agencies to identify current role holders. Once completed, the Agency PMA is asked to send the worksheet to the EPMA at mpkipa@entrust.com to facilitate timely and accurate communication.

Best Practice Recommendations for RAO Policy Management Authorities (PMAs)

1) **Establish a PMA Charter.**
Agencies should develop a formal Charter to govern the PMA's activities. ETPKISSP offers a Charter template (click here), which includes the following elements:
    a. **Purpose** of the PMA.
    b. **Core Responsibilities**, including:
        i. Executing a Registration Authority Agreement (RAA) with Entrust.
        ii. Establishing and maintaining the Agency Registration Practices Statement (RPS), which must be reviewed, updated, and approved annually by the Entrust PMA.
        iii. Preparing for and completing the annual Registration Authority (RA) assessment and submitting results to Entrust by September 30 each year.
        iv. Receiving official communications from the Entrust PMA.
        v. Escalating compliance questions and concerns to the Entrust PMA.
    c. **Structure**, detailing the Executive Leader (the RAO PMA signatory), cross-functional membership, and the process for adding or removing members.
    d. **Voting vs. Non-Voting Roles**, defining member participation.
    e. **Operational Details**, including meeting cadence, documentation of meeting minutes, formatting standards, and audit record-keeping.
    f. **Compliance Oversight**, ensuring the RA service operates in accordance with the ETPKISSP CPS and the Agency's RAO RPS, while capturing evidence needed for the annual RA assessment.
2) **Conduct Regular PMA Meetings.**
Agencies should hold PMA meetings at least quarterly to maintain cross-functional communication. These meetings help ensure all members work from a shared understanding. A formal voting process is encouraged to collect feedback and achieve consensus on key changes. Voting also serves as critical audit evidence during assessments.

    Example:
    If a proposed change is reviewed by the PMA and most members vote to approve, but the legal representative votes against it due to a contractual conflict, the voting process

surfaces the legal concern. This allows the PMA to revise the proposal, hold a subsequent review, and conduct another vote, ensuring that consensus is achieved and documented properly.

3) **Maintain Detailed Meeting Records.**
Agencies must maintain comprehensive meeting minutes and an audit log to support the annual RA assessment process.

4) **Review Compliance Data Quarterly.**
Each quarterly meeting should include a review of compliance performance against the Agency's RPS to ensure RA services are executed in full alignment with policy requirements.

As Registration Authority Organizations (RAOs), Agencies serve as operational extensions of both the FPKI and ETPKISSP audit boundaries. The RAO PMA is the vehicle for managing Agency compliance requirements. Entrust stands ready to assist; the *US Federal PA Representative – Compliance* (mpkipa@entrust.com), will consult and support the RAO PMA and manage compliance inquires on behalf of the EPMA.

2.2.2 The Registration Authority Agreement (RAA)

The EPMA and the RAO PMA are required to counter-sign a Registration Authority Agreement, or RAA. This requirement from FPKI is identified in this memorandum: https://www.idmanagement.gov/docs/FPKI-ra-audit-guidance.pdf which stipulates:

> "**Guidance for Registration Authorities**
> Every agency managing RAs that verify certificate contents and submit Certificate Signing Requests (CSRs) to a CA for the purpose of issuing certificates to agency personnel, must submit supporting audit documentation on an annual basis to their CAs, for inclusion in the CA's annual review package. The Registration Authority Agreement (RAA) or other binding legal 1 agreement between the CA and RA (e.g., established contracts) should specify the responsibilities for the audits that support the annual package."

The ETPKISSP PAR – Compliance is responsible for executing the RAA with the RAO. New counter-signed RAAs will be submitted with the ETPKISSP Annual Audit Package, as required. The RAA is signed once and reviewed annually by ETPKISSP to determine whether an updated agreement is required.

2.2.3 The Registration Practice Statement (RPS)

From the Common Policy CP:

> **"1.5.3. Person Determining CPS Suitability for the Policy**
> The FPKIPA must approve the CPS for each CA that issues certificates under this policy.
> **1.5.4. CPS Approval Procedures**
> CAs issuing under this CP are required to meet all requirements. The FPKIPA will not issue waivers.
> The FPKIPA makes the determination that CPS complies with this policy. The CA and RA must operate under an approved CPS. RA practices are documented in the CPS or an associated Registration Practices Statement (RPS). In each case, the determination process must include an independent compliance auditor's results and recommendations.."

To establish and maintain the RAO RPS is a compliance requirement which serves as a fundamental document in the annual assessment. The assessment establishes that the RPS complies with the CPS, and that the RAO operates in compliance. An RPS is used by the RA Agency/Organization to define the practices used relative to:

1) How the RA function is carried out – verification of Agency subscribers (with associated records), admin practices, audit evidence.
2) How any ETPKISSP integrated components hosted on premise by the RA Agency/Organization are operated in compliance with the CPS.

The EPMA provides support for the RPS requirement:

1) A RAO-specific RPS draft will be derived from the CPS and previous customer documents..
2) The PA Representative (PAR) will work through a workshop with the RAO PMA to help minimize the time required.
3) Once the RPS draft is complete, the PAR will submit it to the EPMA for approval.
4) Once approved, the PAR will retain a copy of the latest approved RPS for inclusion in the annual audit package submission, or to be made available to the FPKIPA upon request.
5) The RAO will provide the latest approved RPS to the auditor during the RA audit.
6) The PAR and the RAO PMA will review the document at least annually to ensure continued compliance.

2.2.4 The Annual RA Assessment

RA & CA Responsibilities

The requirement for each RAO to complete an annual assessment is captured in the program documentation available at https://www.idmanagement.gov/FPKI/#audit-information-for-the-FPKI-management-authority. In October 2022, the FPKIPA clarified the requirements, including assessment options, and requirements of the Agency PMA and the Entrust PMA, posting this memorandum:

- "RA Audit Guidance Memorandum (PDF, October 2022 – *This FPKIPA Memorandum reiterates the necessity of RA audits in supporting PKI operations, normalizes differing terminology used across various references, and provides options for reducing potential duplication of RA audit efforts, as applicable to PIV issuers.*"
- Also from the memorandum: "**Background -** *CAs that participate in the FPKI community are required to receive an annual audit, and to share the results of that audit with the FPKI Policy Authority (FPKIPA), to remain in good standing with the FPKI community. The scope of the annual audit includes all aspects of the CA/RA operation. While CAs are ultimately responsible for submitting the review package, RAs are subject to the compliance audit requirements and must ensure that a compliance audit is performed and the results of the audit submitted to the FPKIPA along with the rest of the annual review package.*"

The memo clarifies that the RAO is responsible for an annual RA assessment:

- Procurement and budgeting for the RA Audit or equivalent.
- Execution of the assessment on an annual basis.

- Provision of assessment outcome to the EPMA for inclusion in the annual Entrust audit submission to the FPKIPA.

The same memo clarifies the responsibilities and requirements of the EPMA:

- Submit an annual audit package to the FPKIPA for assessment.
- Include the assessment outcome as provided by the RAO PMA.

FPKIPA has determined that the RAO PMA has options to satisfy the annual assessment:

1) A formal RA Audit – in this instance an independent, qualified third-party auditor will examine the RAO RPS and examine evidence to ensure that the RAO is:
    - Maintaining an up-to-date RPS which is compliant with the ETPKISSP CPS.
    - Operating in compliance with the ETPKISSP CPS, and the RAO RPS.
2) A copy of an ATO letter provided under the requirements of SP 800-79, together with an attestation letter (see Appendix A) signed by an agency authority that the agency complies with the Key Recovery, if applicable, and audit and archive requirements of the relevant CPS.

The RAO PMA determines which option to employ and captures the approach in the RPS. While the RAO is required to perform the annual assessment, the requirement for Entrust to include the output in the annual package makes it a shared responsibility. The EPMA can help facilitate option 1 above by adding the RA Audit to the annual renewal of the RAO subscription to ETPKISSP and:

- Engaging our 3rd-party Auditor partner.
- Participating in an RA Audit readiness review with the RAO.
- Supporting the RAO and the auditor through the process: documentation review and communication, remediation consulting, Audit Opinion Letter (the output), and inclusion in the annual Entrust package.

Appendix B – RAO PMA includes a table listing the available options. The PMA can select the option that it will employ. Where Entrust is supporting, the table is used to identify the preferred annual cycle to assist in scheduling, and the RAO PMA prime for the audit.

2.3 Compliance Requirements and Non-Compliance Consequences

The audit package must be submitted annually by the EPMA to the FPKIPA by November 30th. This submission must include RA Audit evidence from all RAOs. Any deviation from this requirement poses an unacceptable risk to the FPKIPA, the Entrust PMA, and the RAO PMA. Failure to comply could result in the Entrust submission being assessed as **out of compliance** by the FPKIPA. The consequences of such a determination are outlined here:

- **Non-Compliance Management Framework for the Federal Public Key Infrastructure (FPKI)** (PDF, January 2016), this document provides guidance on how the FPKIPA addresses failures by FPKI FBCA members to meet Memorandum of Agreement (MOA) obligations.

The EPMA has directed the ETPKISSP team to ensure that all compliance risks are fully mitigated to uphold the Entrust commitment to Compliance Excellence and the integrity of the FPKI audit boundary.

Significant Compliance Risk for RA Agencies/Organizations

The FPKIPA defines the audit boundary, and the annual assessment verifies that the boundary remains intact and operates in accordance with the Common Policy CP and FPKIPA requirements. The EPMA uses the audit package to demonstrate this compliance. Missing RA audits is a violation of compliance requirements. If an annual assessment is not completed on time, the EPMA cannot assert the integrity of the audit boundary and must take corrective action.
As outlined in the ETPKISSP CPS, RA Agencies/Organizations are required to:

1. Establish and maintain an RAO PMA
2. Maintain a current ETPKISSP subscription
3. Execute a Registration Authority Agreement (RAA) with the Entrust PAR
4. Establish and maintain a Registration Practices Statement (RPS)
5. Maintain required audit data as defined in the RPS
6. Conduct the annual assessment and submit results to mpkipa@entrust.com
7. Operate in accordance with the ETPKISSP CPS and the RPS

The EPMA is responsible for enforcing compliance to maintain the integrity of the audit boundary. Sanctions for non-compliance are defined in the CPS and include:

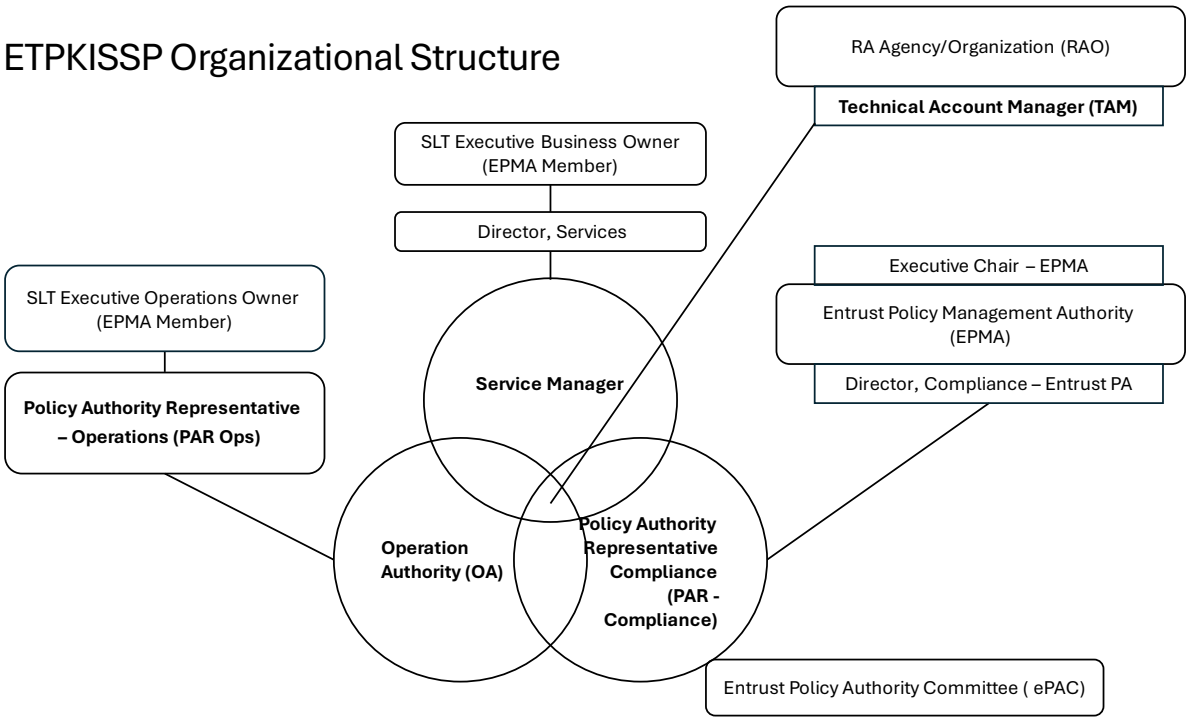
- **30-Day Notification:** The EPMA will notify the RAO PMA when they are 30 days away from a compliance deadline. The notification will detail the compliance issue.
- **Non-Compliance Notification:** If the issue is not resolved within 30 days, the EPMA will issue a formal notice of non-compliance to the RAO PMA. This notice will include details of the issue, the date, required remediation steps, and possible sanctions until compliance is restored.
- **Suspension Notification:** Should circumstance dictate, the EPMA will issue a formal suspension or reduction of service notification. This notice will include details of the issue and the sanction being imposed including communication history and required remediation steps for service restoration. Included will be requirements to avoid action, and an appeals process for the RAO.

The EPMA is committed to supporting RAO PMAs to avoid compliance issues and possible service disruption. For assistance, please contact the ETPKISSP PAR – Compliance at **mpkipa@entrust.com**.

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

Appendix A – ENTRUST ETPKISSP ORGANIZATION

The diagram below provides the organizational structure for ETPKISSP. The key visible and active roles are in bold. Together, the Service Manager, PARs, and the OA are responsible for all aspects of ETPKISSP as appointed by the EPMA. A brief description of each role is provided below:



Key Roles and Responsibilities

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.

The **Policy Authority** is the EPMA Chair and is responsible for compliance of all Entrust Managed Service Offerings.

The **Service Manager** is the business owner of ETPKISSP. 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.

The **Operations Authority (OA)** is the Director responsible for the Operations team and all aspects of ETPKISSP & NFI Operations.

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.

The **Policy Authority Representative - Compliance (Par – Compliance)** is responsible for ensuring compliance with the FPKIPA compliance requirements. 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 as a direct report to the Director, Compliance.

A **Technical Account Manager (TAM)** is an optional resource whose service may be procured by the RA Agency/Organization. Highly recommended by Entrust, these experienced PKI resources are valued by ETPKISSP customers. A full description of TAM service is available here.

Many of these roles are more deeply defined in the ETPKISSP and NFI CPS documents.

Contacting the Entrust Policy Management Authority

The RAO PMA may connect directly with the PAR – Compliance at mpkipa@entrust.com.

Appendix B – RA AGENCY / ORGANIZATION DETAILS

RAO PMA

ETPKISSP and the RAO are required to maintain up-to-date records. In this exercise, ETPKISSP is asking for an updated list of RAO PMA membership, specifically identifying the executive leader(s), the PMA Signatory(s) able to counter-sign RAAs and RPS updates on behalf of the RAO PMA, and anyone who the organization considers Prime Point of Contact (PPC) roles. Note that one person may handle multiple roles. Group email addresses may be listed.
Under communication, please select the desired options:

- **Emergencies** – The EPMA will contact these contacts when a service-impacting issue occurs.
- **Notifications** – Service windows, Policy updates, etc.
- **Bulletins** – From the Service Manager, providing updates on release dates, roadmap, etc.
- **Portal** – ETPKISSP is releasing a customer portal. In selecting this option, we will send updates regarding this release and put the member in the queue for Portal access.

The last line of the table is intended for the RAO to specify any instructions. For example, a PMA may have an executive leader and signatory, but the operational team may wish to specify that the leader is not to receive communication directly from ETPKISSP, and that escalation will occur internally as required.

PMA Member Details						**Communication**			
Name	**Email**	**Role(s)**	**Chairperson**	**Signatory**	**RA Audit**	**Emergencies**	**Notifications**	**Bulletins**	**Portal**
Communication requirements as defined by the RAO PMA:									

Annual Assessment

In this section, the RAO PMA indicates which annual assessment option will be used, and the Prime contact for the PAR – Compliance to engage with.

Select	Assessment Option (Required: Choose 1 of 3)
☐	The RAO will leverage an 800-79 assessment and attestation letter, with outcome submitted to mpkipa@entrust.com by September 30th, annually.
☐	The RAO will contract directly an independent, qualified auditor to perform an RA Audit and provide the Audit Opinion Letter to mpkipa@entrust.com on or before September 30th.
☐	The RAO will procure an RA Audit through Entrust, who will bring in their independent 3rd-party auditor, support the process and receive the Audit Opinion letter before September 30th annually.

Please indicate the RAO PMA member(s) who will prime the annual assessment exercise:	
Please indicate the RAO PMA member(s) who will prime ownership of the RPS:	

Please submit completed forms to mpkipa@entrust.com