SRTP System Architecture Overview Guidance

Sopra Steria Belgium

Homologation SEPA Request-to-Pay (SRTP) Scheme

Abstract	The present document provides some guidance for the creation and visualisation the SEPA Request-to-Pay (SRTP) system architecture overview.

Document reference	SSB-SRTP-15
Issue	Version 1.0 – FINAL
Date of Issue	17/11/2025
Produced by	Sopra Steria Benelux
Verified by	European Payments Council
Circulation	Public information

Table of Contents

1. Introduction

The purpose of SRTP homologation is to confirm that an SRTP Service Provider or Technical Solution Provider meets the technical, operational, security, and business continuity requirements necessary for exchanging SRTP messages, as outlined in the SRTP scheme rulebook and implementation guidelines. Assessing the technical infrastructure through an SRTP architecture overview is a critical component of this process.

This document provides guidance to Applicants and Technical Solution Providers on formalizing the SRTP architecture in clear, comprehensive overviews. The recommendations are based on industry best practices; however, alternative visualization methods that achieve the same objectives are also acceptable.

Applicants and TSPs may use any suitable diagramming tools. All architectural schematic overviews, whether following this guidance or a comparable approach, must be submitted as a **PDF slide deck** for SRTP homologation.

2. SRTP Architecture Overview

1 - One-Page Architecture Overview

The purpose of the high-level overview is to provide a functional, end-to-end view of the SRTP (Secure Request-to-Pay) ecosystem. This includes all actors involved in the SRTP message exchange, their trust boundaries, and the principal message flows.

The diagram should highlight:

- The ecosystem participants: **Payer Service Provider (Payer SP), Trusted Service Provider (TSP), Payee PSP,** and **Scheme/Directory services.**
- Core message flows for **SRTP Request** and **SRTP Response**, including **callback mechanisms**.
- Data movement and trust demarcations between domains.
- The full call sequence from **Payee PSP → TSP → Payer SP → Core → callback**.

This representation gives homologation assessors a concise but complete understanding of the SRTP interaction model across actors.

2 - System Context and Logical Architecture

The system-level architecture provides insight into the internal design of each actor (Payer SP or Payee PSP).
Its purpose is to describe the technical decomposition of the solution, the main functional components, and the logical flow inside the SP domain.

The architecture must illustrate:

- **Edge/WAF** components enforcing perimeter security.
- The **SRTP Orchestrator**, responsible for request validation, routing, and message transformation.
- **Consent management services**, including customer approval logic.
- **Core application components** performing business logic.
- **Data persistence layers** (DBs, encrypted stores).
- **Monitoring and observability services**.
- The logical flow across containers: **Edge → Orchestrator → Consent → Core → Data**.

This context ensures homologation teams understand how each SP or PSP manages SRTP flows internally.

3 - Network and Security Zones

The objective of this view is to demonstrate the network security posture.
It must reflect traffic segregation, firewall enforcement, and zoning models required for SRTP compliance.

The diagram should incorporate:

- A **DMZ** zone hosting WAF/Edge services.
- An **Application Zone**, containing orchestrators and internal APIs.
- A **Data Zone** with encrypted databases or vaults.
- A **Management Zone** for monitoring, observability, CI/CD, and administrative consoles.
- **Firewall layers** between zones.
- **VLAN separation** and traffic control rules.

This enables assessors to validate that SRTP traffic is isolated, controlled, and compliant with mTLS and segmentation requirements.

4 - Multi-Tenant Segregation (when applicable)

This view is required for **TSPs and banks offering SRTP** to multiple sub-institutions.

The architectural representation must clearly demonstrate how tenants are isolated at the infrastructure, network, and data layers, while still using shared SRTP-critical components.

Elements to illustrate:

- Shared **Edge Gateway** entry point.
- Separate **Tenant A** and **Tenant B** environments, each in its own VLAN, namespace, or container cluster.
- Isolated data stores (**DB_A, DB_B**), including encryption keys and secrets.
- **“No-connection” zones** showing strict tenant isolation.
- Shared but logically separated services such as **PKI**, observability, or directory lookups.

This ensures that tenant isolation is transparent and unambiguous for homologation.

5 - Disaster Recovery and Scalability Layout

This view demonstrates the resilience, high-availability, and continuity characteristics of the SRTP solution.

Points to visualise:

- Active-active or active-passive deployments.
- Replication mechanisms between **Primary Site** and **Secondary Site**, with the relevant **RPO/RTO** indicators.
- Auto-scaling components such as gateways, orchestrators, and container clusters.

- Clearly marked replication flows and failover triggers.

Homologation assessors must be able to confirm the ability to maintain SRTP operations under degradation or site failure.

3. Schematic Composition Guidelines

These guidelines must be applied consistently across all SRTP homologation diagrams.

1 - Layering

All diagrams must follow a consistent three-layer model:

1. **External Layer** – ecosystem actors (PSPs, TSP, directory, monitoring SaaS).
2. **Internal Layer** – application stack (Edge/WAF, Orchestrator, Core, DB).
3. **Infrastructure Layer** – network and security components (VLANs, firewalls, DR sites).

2 - Security Visualisation

Security elements must be visually explicit:

- **Red dashed lines** to delineate trust boundaries.
- **Shield icons** for mTLS-secured interfaces.
- **Firewall icons** to represent inter-zone filtering.
- **Lock icons** indicating encrypted data stores.
- **Padlock overlays** showing tenant-specific vaults or key sets.

3 - Scalability & Disaster Recovery

- Scalable components should be represented with **horizontal clustering indicators** (e.g., “×” markers or cluster icons).
- Secondary sites must be shown as **greyed-out clones**, with arrows indicating replication.
- RPO/RTO values should be annotated where applicable.

4 - Multi-Tenancy in a Single Visual

When multitenancy applies, the diagram must show:

- A single **shared Edge Gateway**.
- Distinct tenant spaces, each in a separate colour-coded zone or namespace.
- Fully separated databases.
- An explicit **no-connection barrier** between tenants.
- Shared services placed outside tenant boundaries (e.g., PKI, monitoring).

5 - Annotations and Legends

To keep diagrams readable, the use of long text must be minimal.
Use concise labels such as:

- *mTLS enforced*,
- *ISO 20022 JSON*,
- *Tenant A namespace*,
- *Encrypted store*.

A visual legend must be included, covering symbols for:

- Secured
- DR replication
- Load-balanced
- Tenant isolation