CONNECTED SERVICES FRAMEWORK

Part 1: Framework

Connected Services Framework

An open transport framework for the UK telecommunications industry

Part 1 of the Connected Services Framework — the management and architecture volume — issued to the Telecom Technical Architecture Group (TAG) for review.

Document Title	**Connected Services Framework — Part 1: Framework**
Framework Reference	CSF v2.0.2 — UK Telecommunications Industry
Document Type	Framework Specification — Part 1 of 2 (Management & Architecture)
Version	2.0.2
Status	**FINAL**
Date of Issue	29 April 2026
Owning Body	**Telecom Technical Architecture Group (TAG)**
Audience	Senior management, solution architects, programme managers, and the TAG steering group

Maintained by the Telecom Technical Architecture Group (TAG).

About this Document

This document is **Part 1 of the Connected Services Framework (CSF) v2.0.2** — the management and architecture volume — assembled for review by the Telecom Technical Architecture Group (TAG) and its observers.

The CSF is an **open, free, peer-to-peer transport framework** for the UK telecommunications industry. It defines how Managed Access Providers (MAPs) exchange messages on behalf of Communications Providers (CPs), without dependency on any centralised hub or administrative authority.

Scope of this Document

Part 1 sets out **what the CSF is, why it exists, and how it works at a conceptual level**. It is intended for senior management evaluating adoption, solution architects designing CP or MAP implementations, and programme managers planning Switching for Business (SfB) delivery.

Part 2 — the implementation volume — provides the technical detail required to build against the CSF: API specifications, code examples, JSON schemas, and integration guidance. Part 2 is published separately.

Reading Order

The document is intended to be read in order, but each chapter stands alone. Decision-makers may find the Overview, Introduction (Chapter 1), and Background (Chapter 2) sufficient. Architects and programme managers should also read Chapters 3 to 6. Implementers and operators will benefit from Chapters 7 to 10 as well as Part 2.

Status and Authority

> **This is the v2.0.2 released version of CSF Part 1.** This published CSF specification is the authoritative source. Comments and proposed further amendments are recorded through the TAG steering group's weekly call. Draft versions are only shared with TAG Group members.

Document Control

Version History

This document is maintained under TAG change control. Each material change results in a new version entry.

Version	Date	Description	Status
1.0.5	14 Nov 2025	Last Word document version (Part 2 — Implementation).	Superseded
1.0.5	07 Jan 2026	Last Word document version (Part 1 — Framework).	Superseded
2.0	24 Apr 2026	Comprehensive rewrite in Markdown. Restructured into separate Part 1 (Framework) and Part 2 (Implementation) documents with deduplication, consistent terminology, and improved technical accuracy.	Superseded
2.0.1	29 Apr 2026	Content additions: new MAP Onboarding & Testing Process handbook with the TAG Baseline Test Suite; expanded CP Transitions §7.3–§7.4 with detailed step descriptions, suggested in-flight order export routine, full RCPID Status export schema, and Step 6 sign-off checklist; new optional `map.status` enum (`ACTIVE` / `TEST` / `SUSPEND`) in the Directory API; tightened telemetry rules in §10.6 (collection limited to `ACTIVE` participants, `auditData.test=true` exclusion); new auditData conventions in the Letterbox doc; bundled GPLB-SG SfB Message Specification v3.0 PDF as the authoritative low-level reference.	Superseded
2.0.2	**29 Apr 2026**	**Governance §10.6 ratified by the TAG steering group on 29 April 2026 — the controls move from review draft to operational baseline.** §10.6.1 formalised: **60% quorum** of currently onboarded MAPs (recorded proxies allowed); **one MAP, one vote** irrespective of size; simple majority for operational decisions, supermajority for specification changes; vote tally added to mandatory decision-record fields; observer status clarified as non-voting and non-quorum. §10.6.3 minimum support window made concrete (six months from release date, no longer indicative). §10.6.4 Tier 3 escalation now mandatorily refers disputes to OTA2 as the standing CSF adjudicator with binding effect. §10.6.5 breach notification re-aligned to UK GDPR /	**Issued**

Version	Date	Description	Status
		DPA 2018 Article 33 — single 72-hour window covering MAPs, TAG and affected CPs, with prescribed notification content. §10.6.7 telemetry rules tightened with explicit **`ACTIVE`** participant filtering and **`auditData`** test-marker exclusion. §10.2.3 GPLB-SG header and lead-in updated to record the GPLB → SfB renaming.	

Distribution

This document is circulated to the TAG steering group, observer organisations attending TAG meetings, and stakeholders involved in the CSF's adoption (MAPs, Communications Providers, OTA2, TOTSCo, GPLB-SG, FCS, Ofcom). Released versions are published on the https://csf-uk.org website.

Change Control

Changes follow the CSF documentation change control process described in §10.3 — proposal, review at the weekly TAG steering group, consensus, publication, and incremental adoption by MAPs through API versioning and feature releases.

Contributors

The CSF is developed and maintained by the TAG. The following individuals and organisations have contributed to the framework:

Name	Organisation
Dave Stubbs	Zentive Limited
David A Wilson	iconectiv
Marcel Horst	CWP
Mark Delo	NowYoYo Limited
Shanmugavel Krishnan	iconectiv
Simon Phillips	ICUK Computing Services Limited
Stephen Breen	iconectiv
Steven Pearce	NowYoYo Limited
Susan Mangini	iconectiv

Index

Section numbering follows the structure of CSF Part 1. Subsections are listed under their parent chapter.

CSF Overview

An open transport framework for the UK telecommunications industry — version 2.0.2, published by the **Telecom Technical Architecture Group (TAG)**.

What is the CSF?

The Connected Services Framework (CSF) is a free, open, and decentralised messaging framework that enables UK Communications Providers (CPs) to exchange messages securely and efficiently through Managed Access Providers (MAPs) — without reliance on a centralised hub or administrative body.

Built on established internet standards (TLS 1.3, OAuth 2.0, DKIM/PKI via RFC 6376) and the industry-standard JSON Asynchronous Messaging Specification (JAM), the CSF provides a peer-to-peer transport layer that any CP or MAP can adopt at zero licensing cost.

Why CSF?

The table below summarises the key differences between the centralised hub model and the CSF's distributed model.

Capability	Centralised Hub Model	CSF (Distributed Model)
Cost	Ongoing per-message or subscription fees	Free to operate — no licensing or transaction charges
Independence	All parties depend on a single operator	Each MAP operates autonomously
Speed of change	Change requests go through a single vendor	TAG consensus enables rapid iteration
Resilience	Single point of failure	Distributed — no single point of failure
Scalability	Hub capacity limits all participants	Each MAP scales independently
CP freedom	CPs may be locked to a provider	CPs control their MAP choice via DNS
Security	Trust delegated to hub operator	End-to-end PKI signing verifiable by any party
Onboarding	Central registration and approval	Peer-sponsored onboarding — operational in hours
Market entry	Barriers to becoming a provider	Any CP can become a MAP of 1

Initial Use Case: Switching for Business (SfB)

The CSF's first application is delivering **Switching for Business** (SfB), formerly known as Gaining Provider Led Business Switching (GPLB). Unlike One Touch Switch (OTS) for residential customers, Ofcom has not mandated a single technical solution for business switching — enabling the industry to adopt this open, distributed approach.

The framework is not limited to SfB. It is designed to support any industry messaging process, including future applications such as number porting and bilateral communications.

Documentation Structure

The CSF documentation set is organised in two parts plus a small set of standalone reference documents.

Reference Documents

Document	Description
Definitions & Terminology	Consolidated reference for all acronyms, abbreviations, and CSF-specific terminology.
CP Rights Charter	Plain-language summary of CP rights under the CSF — standalone, no technical background required.
MAP Onboarding & Testing Process	Practical handbook for developers, implementers, and testers — environments, status model, NowYoYo PKI test harness, and the TAG Baseline Test Suite.

Part 1 — Framework (Management & Architecture)

For decision-makers, solution architects, and programme managers — this document.

Document	Description
Introduction (Ch. 1)	Purpose, scope, and value proposition of the CSF.
Background (Ch. 2)	OTS history, SfB context, and regulatory landscape.
Principles & Requirements (Ch. 3)	Gathered requirements with MoSCoW prioritisation.
Architecture Overview (Ch. 4)	Layered model, message flow, and entity definitions.
CP Registry, Master Registry & Directory (Ch. 5)	Three-tier distributed registry model and synchronisation.
Security Overview (Ch. 6)	TLS 1.3, OAuth 2.0, and PKI/DKIM at a conceptual level.

Document	Description
Onboarding (Ch. 7)	MAP sponsorship and CP registration processes.
RCPID Management (Ch. 8)	UUIDv4 identifiers — allocation, transitions, and rationale.
Operational Excellence (Ch. 9)	Resilience, SLAs, monitoring, and deployment patterns.
Governance (Ch. 10)	Standards bodies, MoU, and change control.
Glossary	Abbreviations and definitions.

Part 2 — Implementation (Technical)

For developers, integration engineers, and technical architects — published separately.

Document	Description
Getting Started	Prerequisites and onboarding checklist.
OAuth 2.0 Implementation	Token requests, responses, and error handling.
PKI & DKIM Signing	DKIM process, CSF headers, worked examples, and error codes.
Message API	Letterbox API, HTTP codes, message delivery failures, and the `auditData` conventions for test flagging and match-session sequencing.
Directory API	Registry JSON schema, MAP-level (`map.status`) and per-CP (`processSupport[].status`) status fields, and field reference.
TOTSCo Integration	Hub interoperability and dual-endpoint configuration.
CP Transitions	Six-step migration process, RCPID Status export schema, suggested in-flight order export routine, Step 6 sign-off checklist, and conflict resolution.
Commercial Scenarios	MAP failure, CP mergers, and administration handling.
Operations	Monitoring, malicious behaviour, regulatory and industry reporting (with the proposed distributed telemetry collection model), and risk register.
FAQs	Combined Q&A from the GPLB Steering Group and TOTSCo integration.
Appendix: OpenAPI Specification	Full OpenAPI 3.0.3 spec for the Letterbox API.

Standards & External References

The CSF builds on and references the following industry standards:

- **JSON Asynchronous Messaging Specification (JAM)** — published on the OTA2 website (https://www.offta.org.uk/).
- **RCPID Standards** — published on the OTA2 website.
- **TOTSCo Hub API Specification v2.0** — the industry-standard letterbox and directory API for SfB, used by TOTSCo and supported by the CSF for hub interoperability (https://totsco.org.uk/wp-content/uploads/2026/04/TOTSCo-API-specifications-v2-Clean.pdf).
- **Switching for Business Process Documents** — published on the FCS website (https://www.fcs.org.uk/gaining-provider-led-business-switching/).
- **GPLB-SG Switching for Business Message Specification v3.0** — the authoritative low-level SfB message specification, published by the GPLB-SG via FCS and bundled with the CSF documentation.
- **TOTSCo Process & Technical Documents** — published on the TOTSCo website (https://totsco.org.uk/process-technical-documents/).

Key RFCs

RFC	Usage in CSF
RFC 8446	TLS 1.3 — mandatory transport encryption.
RFC 6376	DKIM — message signing and verification.
RFC 6749	OAuth 2.0 — authorisation framework.
RFC 4122	UUIDv4 — RCPID format.
RFC 8463	Ed25519 for DKIM — alternative signing algorithm.

Licence

The Connected Services Framework is an open transport framework, free for any Communications Provider or Managed Access Provider to use for any purpose. There are no licensing fees or transaction charges. Participation is governed by the Memorandum of Understanding (MoU) agreed among participating MAPs and CPs.

Definitions & Terminology

The following abbreviations and key definitions are used throughout the CSF documentation. They are placed at the front of this document so subsequent chapters can refer to them in passing.

Abbreviations

Abbreviation	Full Term	Definition
CP	Communications Provider	An organisation participating in an industry process (for example, OTS, SfB) that creates or consumes messages and sends or receives them via a MAP. CPs include retailers, wholesalers, and agencies providing services on behalf of other CPs.
CSF	Connected Services Framework	A set of open message communication standards that define how MAPs exchange messages securely and efficiently on a peer-to-peer basis, without reliance on a centralised hub.
DDG	Detail Design Group	The original industry group that documented the requirements for the technologies and processes of switching residential customers' broadband and voice services (One Touch Switch).
DKIM	DomainKeys Identified Mail	A message authentication standard (RFC 6376) that uses PKI to verify the sender's domain identity and ensure that the message has not been altered in transit. The CSF adapts DKIM for HTTP message signing between MAPs.
DNS	Domain Name System	The internet system that resolves domain names to IP addresses. In the CSF, DNS TXT records are used to publish CP public keys and MAP associations.
GPLB	Gaining Provider Led Business Switching	The original name for the industry *process* for switching business telecommunications services, now branded as Switching for Business (SfB). Ofcom has not mandated a single technical solution for this process.
GPLB-SG	GPLB Steering Group	An independent body of industry stakeholders together with OTA2 that guides and facilitates the steering meetings and publication of the SfB process documentation via FCS. The group retains the historical "GPLB" label even though the process has been renamed to Switching for Business (SfB).

Abbreviation	Full Term	Definition
HMAP	Hub Managed Access Provider	A specialised MAP type that operates as a hub-and-spoke delivery mechanism (for example, TOTSCo). An HMAP accepts messages and forwards them among its subscribed members without engaging with the message payload.
JAM	JSON Asynchronous Message	The industry-wide messaging standard published on the OTA2 website. JAM defines the envelope format (addressing, routing, correlation) used by all CPs and MAPs regardless of the underlying transport.
MAP	Managed Access Provider	An organisation that facilitates message exchange on behalf of CPs by offering integration services, portals, and technical solutions. A CP can become a MAP of 1 (itself) by abiding by MAP rules.
MoU	Memorandum of Understanding	The agreement governing collaboration between MAPs and CPs participating in the CSF.
OTA2	Office of the Telecommunications Adjudicator	The industry body accountable for publishing and controlling RCPID Standards and the JSON Asynchronous Messaging Specification.
OTS	One Touch Switch	The Ofcom-mandated process for switching residential IAS and NBICS services between consumer CPs. All OTS messages must be routed via the TOTSCo Hub.
PKI	Public Key Infrastructure	A framework for managing cryptographic key pairs and digital certificates. In the CSF, PKI is implemented via DKIM (RFC 6376) to sign and verify messages between MAPs.
RCPID	Retail Communications Provider Identifier	A unique identifier assigned to a CP brand for the purpose of message exchange. In the CSF, RCPIDs use the UUIDv4 format (RFC 4122) and remain with the CP for life, even when changing MAPs.
RFC	Request for Comments	A publication series from organisations such as the IETF that defines internet standards, protocols, and technical specifications.
SfB	Switching for Business	The current branding for the GPLB process — the industry process for switching business telecommunications services.
TAG	Telecom Technical Architecture Group	A consortium of telecoms industry stakeholders responsible for the development, publication, and change control of the CSF. The TAG meets weekly via its steering group.

Abbreviation	Full Term	Definition
TLS	Transport Layer Security	A cryptographic protocol providing secure communication over networks. The CSF mandates TLS 1.3 (RFC 8446) for all connections.
TOTSCo	Telecoms One Touch Switching Company	The organisation operating the centralised hub for OTS message routing. TOTSCo also publishes OTS process and technical documentation. For SfB, TOTSCo may operate as an HMAP within the CSF.

Key Definitions

CP Registry

A JSON data structure published by each MAP containing detailed information about that MAP, its connected CPs, and their supported processes (including RCPIDs, brand names, PKI signing domains, resource URLs, and contact details). Both the MAP and each individual CP can include a `contact` array using the same structure — the MAP contact is for MAP-to-MAP technical issues, while each CP's contact is for CP-to-CP operational escalations (sales, support, technical). Each MAP publishes its own CP Registry and makes it available to other MAPs via an OAuth 2.0-protected API endpoint. The CP Registry is the outward-facing data that MAPs share with each other.

Master Registry

The private, consolidated view built by each MAP when it collects and converges all other MAPs' CP Registries. The Master Registry contains the full routing, PKI signing, and contact details for every CP across the entire CSF network. It is held privately by the MAP and used internally for message routing, DKIM signature verification, and CP-to-MAP resolution. Each MAP maintains its own copy of the Master Registry.

Directory

A filtered, cut-down version of the Master Registry that a MAP shares with its own CPs. The Directory lists the brand names and RCPIDs available to switch with — the information CPs need to populate drop-down lists, search-as-you-type fields, and message addressing. It excludes inter-MAP routing details, PKI signing domains, and other sensitive operational information. When a CP selects a destination from the Directory, the MAP uses the RCPID to look up the full routing and signing details in its private Master Registry.

Sponsor MAP

An onboarded MAP that is assigned (via round-robin rotation) to guide a new MAP through the onboarding process. The Sponsor MAP validates the new MAP's technical readiness, conducts testing, and acts as a gatekeeper to the CSF network.

New MAP

An organisation that wishes to join the CSF and begin exchanging messages with other MAPs. A New MAP must complete the sponsored onboarding process before it can publish its registry or exchange production messages.

Letterbox

The REST API endpoint used by MAPs to send and receive messages. The letterbox accepts JAM-formatted JSON messages over HTTPS (TLS 1.3) with OAuth 2.0 authentication and returns an HTTP 202 to acknowledge receipt.

Routing Group

A named collection of routing ID patterns (expressed as regular expressions) that determines which message types are accepted by a specific MAP service endpoint. For example, `businessSwitch.*` for SfB messages or `residentialSwitch.*` for OTS messages.

Feature Release

A mechanism within the CSF that allows MAPs to adopt new capabilities incrementally without requiring all MAPs to upgrade simultaneously. MAPs advertise their supported feature sets in the registry, enabling automatic negotiation of the highest compatible version between interacting parties.

1. Introduction

1.1 Purpose of This Document

This document defines the **Connected Services Framework (CSF)**, an open transport framework for the UK telecommunications industry. It establishes the technical and operational prerequisites, architectural design, and implementation strategy that enable Managed Access Providers (MAPs) to exchange messages securely and efficiently on behalf of their Communications Providers (CPs).

The CSF is free for any organisation to adopt. There are no licensing fees, transaction charges, or commercial dependencies on any single provider.

1.2 What the CSF Does

The CSF is a **transport layer** — it defines how messages are wrapped, signed, and delivered between MAPs. It does not define the content of those messages. Industry processes such as Switching for Business (SfB) or One Touch Switch (OTS) define the message content; the CSF delivers it.

In practical terms, the CSF provides:

- **Secure peer-to-peer message delivery** between MAPs using TLS 1.3, OAuth 2.0, and DKIM-based PKI signing.
- **A distributed registry model** where each MAP publishes a CP Registry of its CPs, all MAPs converge these into a private Master Registry, and each MAP derives a filtered Directory for its own CPs.
- **DNS-based CP verification** that puts CPs in control of which MAP represents them.
- **Standardised onboarding** through peer sponsorship, removing the need for centralised administration.
- **In-flight order portability** so CPs can change MAPs without disrupting active switching orders.

1.3 Who This Document Is For

Part 1 (this document) is written for:

- **Senior management and decision-makers** evaluating whether to adopt the CSF.
- **Solution architects** designing CP or MAP implementations.
- **Programme managers** planning SfB delivery.

Part 2 (Implementation) is written for developers and integration engineers who need API specifications, code examples, and JSON schemas.

1.4 Scope

The CSF covers:

- The definition of a decentralised messaging architecture independent of any centralised administrative authority.
- Requirements for interoperability, security protocols, and communication standards between MAPs.
- Protocols for onboarding new MAPs and transitioning CPs between MAPs.
- Guidelines for maintaining data integrity, ensuring secure communications, and managing exceptional scenarios such as MAP failures, CP migrations, mergers, and administration.

The CSF **does not** cover:

- How a MAP integrates with its own CPs (this is each MAP's commercial decision).
- The content of industry process messages (defined by OTS, SfB, etc.).
- The internal architecture of any MAP's platform.

1.5 The Case for a Distributed Model

The UK telecoms switching landscape currently operates through a centralised hub model for residential switching (OTS via TOTSCo). While this model served its purpose, it introduces constraints that are unnecessary for business switching.

Cost

A centralised hub requires ongoing funding — through per-message fees, subscriptions, or industry levies. The CSF eliminates these costs entirely. MAPs exchange messages directly with each other at no charge.

Independence

In a hub model, every CP and MAP depends on a single operator for message routing, change management, and availability. The CSF distributes these responsibilities across all participants.

Speed of innovation

Hub changes require approval from a single vendor's change control process. CSF changes are agreed by the TAG steering group and can be adopted incrementally by MAPs through versioning and feature releases.

Resilience

A centralised hub is a single point of failure. The CSF's peer-to-peer architecture means that an outage at one MAP affects only that MAP's CPs — not the entire industry.

CP freedom

The CSF gives CPs direct control over their MAP relationship through DNS. A CP can change MAP by updating two DNS records, and their RCPID stays with them for life.

Market access

Any CP can become a MAP of 1 (serving only itself) and exchange messages directly with the industry. This lowers barriers to entry and avoids monopolistic lock-in.

> **Note.** The CSF does not preclude the use of a centralised hub. TOTSCo can operate as a Hub MAP (HMAP) within the CSF, allowing CPs connected to the hub to exchange messages with CPs connected to other MAPs seamlessly.

1.6 Initial Application: Switching for Business (SfB)

The CSF's first industry application is **Switching for Business (SfB)**, formerly known as Gaining Provider Led Business Switching (GPLB).

Key differences from OTS:

- **No mandated hub.** Ofcom has not required a centralised technical solution for business switching.
- **Gaining-provider-led.** The switching process is initiated by the gaining provider.
- **Larger scale.** The industry expects a tenfold increase in RCPIDs compared to OTS.
- **Longer onboarding.** Industry-wide ramp-on is expected to span a considerably longer timeframe.

The CSF has been designed to support SfB as its initial use case, but is architected for any future industry messaging process — including number porting, bilateral communications, and processes not yet defined.

1.7 Document Structure

Chapter	Content
Background	History of OTS, the emergence of SfB, and the regulatory context.
Principles & Requirements	Industry-gathered requirements with MoSCoW prioritisation.
Architecture Overview	Layered model, message flow, and entity definitions.
CP Registry, Master Registry & Directory	The three-tier distributed registry model.
Security Overview	Multi-layered security architecture.
Onboarding	MAP sponsorship and CP registration.
RCPID Management	Identifier format, allocation, and lifecycle.
Operational Excellence	Resilience, SLAs, and deployment patterns.
Governance	Standards bodies and change control.

Chapter	Content
Glossary	Terms and abbreviations.

2. Background

2.1 The Evolution of UK Telecoms Switching

The United Kingdom's telecommunications sector has undergone significant evolution, driven by government policy objectives aimed at promoting a more competitive, consumer-focused market. Central to this transformation is the **Switching General Conditions**, a regulatory framework designed to streamline switching processes by minimising inefficiencies and eliminating procedural redundancies.

2.2 One Touch Switch (OTS): Establishing the Foundation

Through the Switching General Conditions, the industry formed a Detail Design Group (DDG) to establish the requirements for switching residential customers' broadband and voice services — what Ofcom termed "One Touch Switch."

The DDG established several foundational principles that the CSF builds upon:

1. **JSON message format.** A standardised format separating delivery instructions (the envelope) from the message content (the body).
2. **Shared directory.** A directory of all participating CPs that could be shared by all participants.
3. **Common connectivity.** A standardised way for CPs to connect, send, and receive messages.
4. **Multiple delivery platforms.** Support for multiple solutions — hub, portal, and direct integration — provided by what are now known as Managed Access Providers (MAPs).

These principles now form the basis of the **JSON Asynchronous Messaging Specification (JAM)**, published on the OTA2 website and used by both OTS and SfB.

Limitations of the OTS Implementation

To guarantee timely delivery of OTS, certain original design principles were not fully implemented:

- Ofcom mandated that all OTS messages be routed through a single centralised hub (TOTSCo), limiting direct MAP-to-MAP exchange.
- Industry processes for CP transitions between MAPs were not addressed.
- RCPID management — where the CP, not the MAP, owns the identity — was not fully resolved.
- The directory model, while distributed in concept, remained dependent on a central operator.

These gaps created the need for the TAG and the CSF.

2.3 Switching for Business (SfB): Removing Restrictions

Mandated by Ofcom, the business switching process was established on principles similar to OTS, with one critical distinction: **Ofcom has not mandated that all messages be routed through a centralised hub**.

This removal of the routing restriction enables MAPs and individual CPs to exchange messages directly with one another, rather than through a central intermediary.

The Switching for Business process:

- Establishes the **gaining-provider-led model** as mandated by Ofcom.
- Adopts the **Switching for Business (SfB) process** — stewarded by the GPLB Steering Group (GPLB-SG) — uniformly across the industry.
- **Decouples** CPs from the constraints of any specific transport mechanism.
- Represents the **first industry process** designed to streamline direct inter-provider messaging.

2.4 The Telecom Technical Architecture Group (TAG)

The TAG is a consortium of telecom industry stakeholders — including MAPs, System Integrators, and CPs — convened to:

1. Identify gaps in the OTS messaging infrastructure.
2. Establish core requirements for extending the OTS foundation to support SfB and future processes.
3. Design and maintain the Connected Services Framework.

The TAG collaborates closely with the GPLB Steering Group (GPLB-SG) and references the Switching for Business process documentation published on the FCS website.

Before designing any solution, core requirements were gathered from all MAPs, System Integrators, and related CPs. These requirements — covering cost reduction, security enhancement, and message exchange processing — form the foundation of the CSF as documented in *Principles & Requirements (Chapter 3)*.

2.5 From OTS to CSF: What Changed

Aspect	OTS	CSF
Routing	All messages via TOTSCo Hub	Direct MAP-to-MAP (peer-to-peer)
Hub dependency	Mandatory	Optional (TOTSCo can operate as HMAP)
Directory	Centralised at TOTSCo	Each MAP publishes its own registry
RCPID format	4-character codes (e.g., RGXD)	UUIDv4 for scalability and uniqueness

Aspect	OTS	CSF
CP identity	Managed by MAP/Hub	CP controls via DNS records
Message signing	Hub validates	DKIM-based PKI — any recipient can verify
Onboarding	Central registration	Peer-sponsored, self-service
Cost model	Hub subscription/per-message fees	Free — no charges between MAPs
CP portability	Limited	Built-in: RCPID follows the CP for life
Change control	Hub vendor process	TAG steering group (weekly)

3. Principles and Requirements

3.1 How Requirements Were Gathered

The requirements documented in this chapter were explicitly gathered from Managed Access Providers (MAPs), Systems Integrators (SIs), and their associated CPs. The purpose was to define how MAPs communicate with each other efficiently, reliably, and securely to facilitate messaging solutions on behalf of their CPs for any industry process.

The intention is that modifications stipulated within the CSF will not impact solutions already developed by CPs in support of OTS. However, MAPs may need to implement changes to fully support distributed messaging for processes such as SfB.

3.2 Requirements

Requirements are prioritised using the MoSCoW method:

- **Must** — non-negotiable; the CSF cannot function without this.
- **Should** — important but not blocking; deviation requires justification.
- **Could** — desirable if achievable without significant cost or complexity.
- **Won't** — out of scope for the current version.

Connectivity and Routing

Ref	Requirement	Priority
R.01	MAPs MUST be free to acquire and manage their own customers without a technical or commercial dependency on, or imposed by, another MAP. No centralised administration is required.	**Must**
R.02	MAPs MUST make their customers available for message exchange with any other requesting MAP without applying a commercial or technical barrier.	**Must**
R.03	Unless required by regulation or an agreed industry process, no single party SHALL be a dependency for routing messages to any other MAP and their CPs.	**Must**
R.04	All OTS messaging MUST continue to be routed via TOTSCo to meet Ofcom compliance requirements.	**Must**
R.05	Direct routing MUST NOT be mandated between MAPs. A MAP can choose who they route through unless required by regulation or an agreed industry process.	**Must**
R.06	MAPs MUST ensure they have peering capabilities to reach all CPs in the directory.	**Must**

Ref	Requirement	Priority
R.07	Any MAP MAY choose to provide routing services to another MAP (e.g. TOTSCo), but MUST NOT route to another routing MAP as circular routes MUST be avoided.	**Must**
R.08	MAPs MUST meet the requirements of the industry processes in delivering messages and meeting CP SLAs.	**Must**
R.09	SLAs MUST be defined for all MAP-to-MAP transactions.	**Must**
R.10	MAPs MUST maintain a secure networking environment between all MAPs and their CPs.	**Must**
R.11	MAPs MUST ensure they only accept messages from authenticated CPs and MAPs.	**Must**
R.12	Every MAP MUST provide the same guaranteed delivery capability to its CPs, including retry mechanisms and failure reporting.	**Must**
R.13	A mechanism is REQUIRED to allow auto-discovery of CPs by onboarded MAPs.	**Must**
R.14	The solution MUST support message sending and receiving in compliance with supported industry processes (e.g., OTS, SfB).	**Must**
R.15	The solution MUST be as simple as possible to implement.	**Must**

Directory Management

Ref	Requirement	Priority
R.17	A centralised directory SHOULD NOT be a dependency or requirement.	**Should**
R.18	Every MAP MUST provide its customers with access to a complete directory list in support of their messaging processes.	**Must**
R.19	Every MAP is responsible for maintaining and publishing the CP Registry entries of its own CPs.	**Must**
R.20	All MAPs MUST be able to issue their own unique RCPIDs.	**Must**
R.21	A new MAP MUST have a sponsor and be onboarded before being added to the network.	**Must**
R.22	Any shared directory model MUST be openly extensible.	**Must**

Messaging

Ref	Requirement	Priority
R.23	Messages SHOULD be capable of being encrypted end-to-end.	Could
R.23a	All messages exchanged between MAPs MUST be digitally signed using DKIM (RFC 6376) so that the receiving MAP can verify the message has not been tampered with in transit and that it originated from the claimed source CP.	Must

Operations

Ref	Requirement	Priority
R.24	No MAP MAY charge for connectivity and routing of messages from or to another MAP, or levy charges to another MAP's customers.	Must
R.25	Every MAP MUST ensure they have connectivity to exchange and route messages.	Must

Other

Ref	Requirement	Priority
R.26	Linking RCPIDs (e.g., association of OTS and SfB RCPID if a CP uses one for each process).	Could

CP Right to Move

Ref	Requirement	Priority
R.27	Every CP MUST have the right to change to another MAP.	Must
R.28	No MAP SHALL actively prevent a CP from moving to a new MAP.	Must
R.29	No MAP SHALL deliberately prevent access to switching for a CP while still under contract when the CP is switching to another MAP.	Must
R.30	A CP MUST be able to choose their service status within the MAP's directory, regardless of account status (e.g., ACTIVE, TEST, SUSPENDED).	Must

3.3 Summary of Principles

Taken together, these requirements establish that the CSF must:

1. **Ensure MAP independence** — no commercial or technical dependency on any other MAP.
2. **Guarantee interoperability** — secure routing of messages between all MAPs.

3. **Remove barriers** — MAPs provide connectivity without imposing technical or commercial barriers.
4. **Maintain security** — authenticated message exchanges using OAuth 2.0, PKI, and DNS-based validation.
5. **Enable auto-discovery** — decentralised discovery of MAPs and CPs through shared directory structures.
6. **Guarantee delivery** — consistent message delivery with retry mechanisms and failure reporting.
7. **Empower CPs** — freedom and autonomy to switch MAPs without disruption or obstruction.
8. **Enforce SLAs** — MAP-to-MAP service-level agreements for consistency and reliability.
9. **Comply with regulation** — all MAP activities must comply with relevant industry regulations.
10. **Reward good behaviour** — the framework encourages good actors and discourages bad actors without requiring centralised enforcement.

These principles support operational excellence, regulatory compliance, and industry-wide interoperability, fostering an environment conducive to innovation and dynamic market competition.

4. Architecture Overview

4.1 Layered Architecture

The CSF operates as a layered messaging stack. Each layer has a distinct responsibility, and together they provide a complete, secure message delivery pipeline.

Layer	Role	Standards / Mechanisms
Process Layer	Defines the business message content (e.g., SfB Switch Match, Switch Order).	Open industry process message formats (defined by GPLB-SG, OTS-DDG, etc.).
JAM Routing Layer	Defines addressing, message correlation, and routing.	JSON Asynchronous Messaging Specification (RCPID addressing, envelope headers).
CSF Security Layer	Handles message signing, encapsulation, and verification.	PKI/DKIM (RFC 6376), OAuth 2.0, DNS-based validation.
Transport Layer	Ensures secure delivery over the network.	HTTPS over TLS 1.3 (RFC 8446).

The process layer and JAM routing layer are industry-wide standards that exist independently of the CSF. The CSF's contribution is the security layer and the operational framework that binds everything together.

4.2 Entity Definitions

4.2.1 Communications Provider (CP)

A CP is any party participating in an industry process — creating or consuming messages and sending or receiving them from other CPs. CPs include retailers, wholesalers, and agencies providing services on behalf of other CPs.

The CP involved will vary based on the industry process. A CP does not need to understand how the CSF works — it creates messages according to the industry process specification and hands them to its MAP for delivery.

4.2.2 Managed Access Provider (MAP)

A MAP facilitates message exchange on behalf of one or more CPs. MAPs provide integration services, portals, technical solutions, and the operational infrastructure to send and receive messages over the CSF.

Within the CSF, a MAP is the **only entity** authorised to exchange messages with other MAPs, because MAPs are responsible for:

- Publishing and maintaining their CP registry.
- Applying PKI signing to outbound messages.
- Verifying PKI signatures on inbound messages.
- Establishing and maintaining OAuth 2.0 credentials with other MAPs.
- Guaranteeing message delivery with retry mechanisms.

A MAP may serve multiple roles concurrently for its clients (insourced, technical, fully managed), and the CSF imposes no restrictions on this. There are no charges or licensing requirements mandating specific MAP definitions.

4.2.3 MAP of 1

Any CP can become a "MAP of 1" — operating as its own MAP. This allows CPs to exchange messages directly with the industry for free, maintaining full control of all messages sent and received from their own infrastructure. The CP must abide by all MAP rules when implementing.

4.2.4 Hub Managed Access Provider (HMAP)

An HMAP is a specialised MAP designed to facilitate integration for proxy hubs such as TOTSCo. An HMAP:

- Accepts messages and forwards them among its subscribed members using a hub-and-spoke model.
- Does **not** engage with the message payload — it routes based on addressing information.
- When interfacing with the CSF, uses its Master Registry (built from collected CP Registries) to locate the destination CP and dispatches the message to the appropriate MAP.
- Is **not required** to implement PKI/DKIM signing when exchanging messages on behalf of its CPs (to minimise integration cost).
- Is **strongly recommended** to implement the full CSF CP Registry format for SfB, as its CP clients benefit significantly from the additional information it provides.

> ✓ **Best Practice.** MAPs on the CSF should provide a dedicated endpoint exclusively for HMAPs, separate from the endpoint used by other CSF MAPs. This allows rapid CSF iteration without disrupting established hub exchange networks.

4.3 Message Flow

The diagram below illustrates the end-to-end message flow through the CSF.

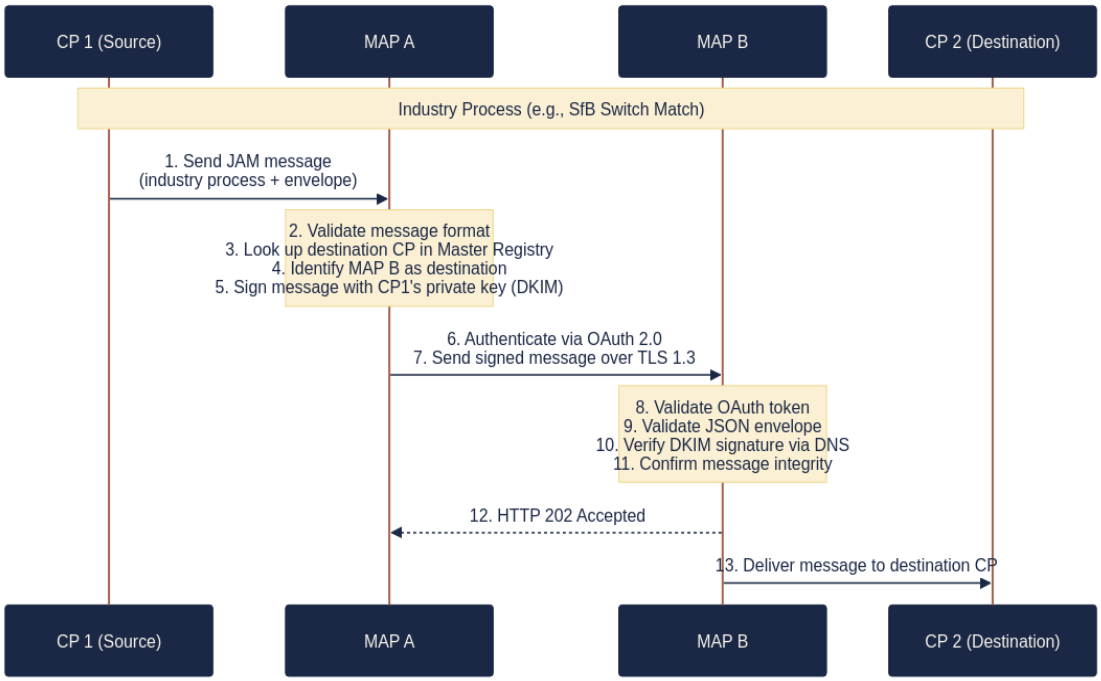

Figure 4.1 · End-to-end message flow through the CSF.

Step-by-Step Workflow

1. **CP creates message.** The CP creates a message according to the industry process specification (for example, SfB) and wraps it in a JAM envelope with RCPID addressing, using directory information provided by its MAP.
2. **CP sends to MAP.** The CP sends the message to its MAP using whatever integration method the MAP provides (API, portal, BSS integration). MAP-to-CP integration is outside the scope of the CSF.
3. **MAP validates.** The MAP validates the message structure, format, and addressing. Unlike a hub model, MAPs **can** read the full CP payload and validate compliance before signing.
4. **MAP discovers route.** Using its Master Registry, the MAP identifies which MAP serves the destination CP.
5. **MAP signs message.** The MAP signs the message with the source CP's private key using DKIM (RFC 6376). The signature is placed in HTTP headers — the message body is not altered.
6. **MAP authenticates.** The sending MAP authenticates with the receiving MAP via OAuth 2.0.
7. **MAP delivers.** The signed message is sent over TLS 1.3 to the receiving MAP's letterbox endpoint.
8. **Receiving MAP verifies.** The receiving MAP validates the OAuth token, checks the JSON envelope, retrieves the source CP's public key from DNS, and verifies the DKIM signature to confirm the message is authentic and unaltered.

9. **Receiving MAP acknowledges.** On successful validation, the receiving MAP returns HTTP 202 (Accepted) — indicating the message has been accepted for processing but processing has not yet completed.
10. **Receiving MAP delivers.** The receiving MAP delivers the message to the destination CP.

> **Note.** If both CPs use the same MAP, the CSF is typically not needed as there is no inter-MAP exchange. However, MAPs operating multiple instances or solutions may elect to use the CSF for their own internal interconnections.

4.4 CSF Networks

Message exchanges are conducted solely between MAPs. The CSF may be employed across diverse industry processes, and the network adapts its size to the specific process in use.

Each MAP must:

1. **Undergo sponsored onboarding** with an existing MAP that supports the relevant industry process.
2. **Establish secure connectivity** with all other MAPs (OAuth 2.0 credentials, endpoint registration).
3. **Publish its CP Registry** detailing its CPs and supported processes.
4. **Retrieve all other MAPs' CP Registries** to build its Master Registry.

Feature-based services are advertised in the CP Registry, allowing certain MAPs to utilise additional functionalities for bilateral and advanced communication. This design ensures MAPs transmit only messages that the receiving MAP can process.

4.5 API Versioning and Feature Releases

The CSF supports incremental evolution through two mechanisms.

API Versioning

MAPs can support multiple API versions simultaneously, allowing new features to be adopted without disrupting existing integrations. When both parties support the latest version, they automatically use advanced features. Where compatibility varies, messages default to the highest compatible version.

Feature Discovery

A MAP queries the directory to identify the supported feature set of another MAP. This enables:

- **Backward compatibility.** All MAPs maintain compatibility with earlier API versions.
- **Flexible adoption.** MAPs can adopt new features at their own pace.
- **Rapid iteration.** The TAG can release new capabilities without requiring industry-wide synchronisation.

By implementing versioning and feature discovery, the CSF enables rapid feature adoption while reducing the constraints of traditional messaging protocols.

4.6 What the CSF Does Not Prescribe

The CSF is deliberately silent on:

- **MAP-to-CP integration.** How a MAP connects to its CPs is a commercial decision (API, portal, BSS plugin, etc.). Typically, MAPs will attempt to offload or shield CPs from as much of the heavy lifting for a process like SfB as possible, and this is often used to differentiate between MAPs, but this is a technical-commercial decision outside the scope of this framework.
- **Internal MAP architecture.** MAPs are free to use any technology stack.
- **CP message creation.** CPs create messages according to industry process specifications, not CSF specifications.
- **Commercial arrangements.** MAPs and CPs establish their own commercial relationships independently of the CSF.

5. CP Registry, Master Registry & Directory

5.1 Overview

The distributed registry model is a foundational pillar of the CSF. Unlike a centralised model where a single operator maintains the master list of all CPs, the CSF distributes this responsibility across all MAPs using a three-tier approach.

Each MAP:

1. **Publishes a CP Registry** — a JSON document listing its own CPs and their metadata, made available to other MAPs via an OAuth 2.0-protected API endpoint.
2. **Collects all other MAPs' CP Registries** — via those same API endpoints.
3. **Converges these into a Master Registry** — a private, consolidated view containing full routing, PKI, and contact details for all CPs across the entire CSF network.
4. **Derives a Directory for its CPs** — a filtered, cut-down version of the Master Registry listing just the brand names and RCPIDs available to switch with.

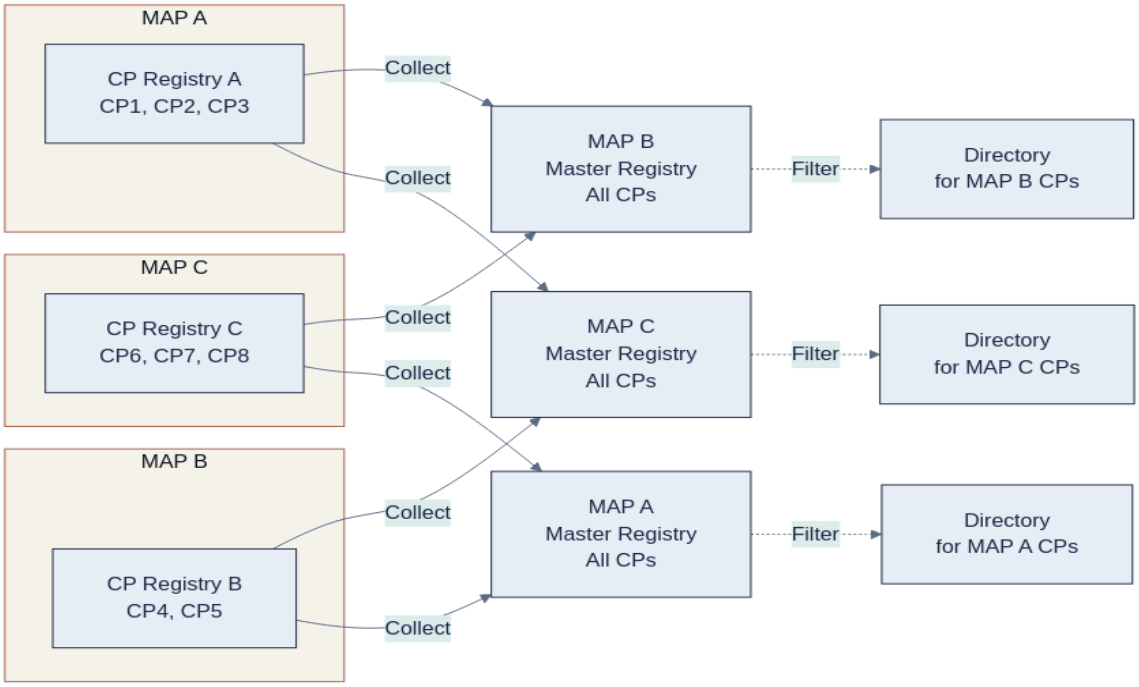

Figure 5.1 · How CP Registries are collected and converged into per-MAP Master Registries, then filtered into Directories shared with each MAP's own CPs.

How the Three Tiers Work Together

1. A CP selects a destination brand from the **Directory** (for example, a drop-down list in the MAP's portal).
2. The MAP uses the selected RCPID to look up the full routing and signing details in its private **Master Registry**.

3. The Master Registry tells the MAP which MAP serves the destination CP, which endpoint to send to, and which PKI domain to use for verification.
4. The destination CP's details originally came from that MAP's **CP Registry**, which was collected and converged into the Master Registry.

5.2 CP Registry Structure

Each MAP's CP Registry contains two main sections.

MAP Section

Comprehensive metadata about the MAP itself:

- **Identity.** MAP name, version timestamp.
- **Contact information.** Phone, email, URL with availability hours and days.
- **Connectivity.** CP Registry API endpoint URL, OAuth token URL, messaging service endpoints.
- **Routing groups.** Which message types (for example, `businessSwitch.*`, `residentialSwitch.*`) are accepted at which endpoint.
- **Connections.** List of other MAPs this MAP has established connectivity with.
- **Registration URI.** Where new CPs or MAPs can apply to register.
- **Service status.** URL and API endpoint for checking operational status and planned changes.

CP List Section

For each CP registered with the MAP:

- **RCPID.** The CP's unique identifier (UUIDv4).
- **Brand name.** The human-readable name shown in search/drop-down lists.
- **Process support.** Which industry processes the CP participates in (OTS, SfB) and their status (ACTIVE, SUSPENDED, TEST).
- **Resources.** Customer assist URLs, sales assist URLs, switch support contacts — backward compatible with OTS resource fields.
- **Signing information.** The DNS domain used for PKI key lookup and which routing IDs should be signed with that domain.
- **Contact details (optional).** A `contact` array using the same structure as the MAP contact object — phone, email, URL with availability hours, days, and purpose (sales, support, technical). This allows each CP to advertise its own preferred contact methods for operational escalations, independent of the MAP's contacts.

> 💡 For the full JSON schema and field reference, see *Part 2: Directory API*.

5.3 CP Registry Synchronisation

MAPs retrieve other MAPs' CP Registries via HTTP GET requests to each MAP's registry API endpoint, authenticated with OAuth 2.0 credentials established during onboarding.

Frequency

- There is no mandatory synchronisation interval — MAPs can pull as frequently as needed.
- A maximum frequency of approximately **60 seconds** is recommended to avoid unnecessary load.
- MAPs MUST retrieve CP Registries regularly and in near-real time, particularly as new CPs are onboarded continuously throughout the day.

Building the Master Registry

Each MAP independently converges the collected CP Registries into its own private copy of the Master Registry. The Master Registry contains:

- **Full routing information.** Endpoint URLs, OAuth token URLs, and routing group definitions for every MAP.
- **PKI signing domains.** The DNS domains used for DKIM signature verification for every CP.
- **Contact details.** MAP and CP contact information for operational support and escalations.
- **Service status.** Real-time availability indicators for each MAP.

Deriving the Directory

From the Master Registry, each MAP creates a Directory for its own CPs. The Directory contains only the information CPs need to address messages:

- **Brand names** and **RCPIDs** — for drop-down lists and search-as-you-type.
- **Supported processes** — which CPs support OTS, SfB, etc.
- **Resource URLs** — customer assist and sales assist URLs (backward compatible with OTS).

The Directory excludes inter-MAP routing details, PKI signing domains, OAuth endpoints, and other sensitive operational information. How the MAP presents the Directory to its CPs (portal, API, BSS integration) is the MAP's commercial decision.

5.4 Advantages of the Distributed Model

Benefit	Description
Data accuracy	Each MAP is the authoritative source for its own CPs, reducing inaccuracies.
Real-time updates	New CPs can be onboarded and advertised in seconds, without central approval.

Benefit	Description
Scalability	Each MAP manages only its own CP Registry — the network scales naturally.
No single point of failure	If one MAP is offline, all other MAPs continue to operate.
Extensibility	The CP Registry schema can be extended without breaking existing implementations.
CP control	CPs control their MAP association via DNS, not through a central register, which means CPs stay in control at all times, not the MAP.
Transparency	Every MAP can see the full network state by converging all CP Registries into its Master Registry.

5.5 Conflict Resolution

When a CP appears in more than one MAP's CP Registry simultaneously (typically during a CP transition between MAPs), the conflict is resolved using DNS:

1. The MAP performs a DNS lookup on the CP's `_mapkey` record.
2. The DNS record indicates the CP's current MAP endpoint.
3. The MAP routes messages to the MAP indicated by DNS, regardless of which CP Registry listed the CP.
4. The MAP marks the conflicting entry as being in "conflict" in its Master Registry.

This DNS-based resolution ensures that the CP — not the MAP — has ultimate control over routing.

> 💡 For detailed conflict resolution procedures, see *Part 2: CP Transitions*.

5.6 TOTSCo Compatibility

The CSF CP Registry structure is backward compatible with the TOTSCo OTS directory. The same fields used in OTS (RCPID, brand name, customer assist URL, sales assist URL) are preserved in the CSF CP Registry using the same structure.

TOTSCo can collect CSF MAPs' CP Registries and either merge them into its own Master Registry or maintain them separately. The CP Registry is JSON-formatted, making convergence straightforward.

For details on consuming the TOTSCo Directory API, see *Part 2: TOTSCo Integration*. The TOTSCo Hub API Specification v2.0 (https://totsco.org.uk/wp-content/uploads/2026/04/TOTSCo-API-specifications-v2-Clean.pdf) defines the standard directory and letterbox interfaces used by TOTSCo and supported by the CSF for hub interoperability.

6. Security Overview

6.1 Security Architecture

The CSF implements a multi-layered security architecture combining three established standards. Together, they deliver end-to-end encryption, authenticated access, and verifiable trust for every connection, credential, and message.

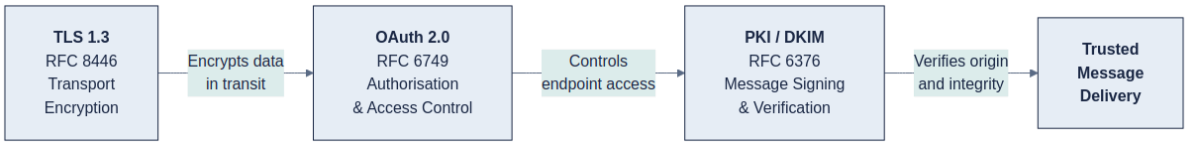

Figure 6.1 · The three-layer CSF security stack: TLS 1.3 transport, OAuth 2.0 access control, and PKI/DKIM message integrity.

Layer	Standard	Purpose
Transport	TLS 1.3	Encrypts all data in motion, protecting against interception and tampering.
Access Control	OAuth 2.0	Ensures only authorised MAPs and CPs can interact with API endpoints.
Message Integrity	PKI / DKIM	Digital signatures verify message authenticity and that content has not been altered.

This combination delivers a **zero-trust, cryptographically assured trust boundary** across networks and services.

6.2 Transport Layer Security (TLS 1.3)

TLS is a cryptographic protocol providing secure communication over computer networks. It ensures that data transmitted between MAPs remains confidential, authentic, and integrity-protected.

What TLS 1.3 Provides

- **Encryption.** Protects data from eavesdropping using symmetric encryption after a secure handshake.
- **Authentication.** Verifies server identity using digital certificates from trusted Certificate Authorities.
- **Integrity.** Ensures data has not been tampered with during transit through message authentication codes.

Why TLS 1.3 Specifically

TLS 1.3 (RFC 8446) is mandated by the CSF because it:

- Removes legacy insecure algorithms (RSA key exchange, SHA-1, static DH).
- Reduces handshake latency from two round-trips to one.
- Mandates **forward secrecy** — session keys cannot be recovered even if a server's private key is compromised.
- Supports only strong, modern encryption (AES-GCM, ChaCha20-Poly1305).
- Encrypts more of the handshake, hiding metadata from passive observers.
- Has growing support for Post-Quantum cryptography (NTRU, ML-KEM, etc.).

> ✓ **CSF Requirement.** TLS 1.3 is mandatory for all CSF deployments. Earlier TLS versions **MUST NOT** be used.

6.3 OAuth 2.0

OAuth 2.0 is the authorisation framework used by the CSF to control access to API endpoints. It provides token-based security with granular permissions.

How OAuth 2.0 is Used in the CSF

The CSF uses the **Client Credentials flow** — the machine-to-machine (M2M) flow — because CSF communication is between MAP servers, not end users.

Each MAP:

1. Registers with other MAPs during onboarding, receiving a `client_id` and `client_secret`.
2. Requests a time-limited access token from the other MAP's OAuth token endpoint.
3. Includes the bearer token in API requests to the other MAP's endpoints.
4. The receiving MAP validates the token's signature, issuer, audience, and expiry on every request.

CSF OAuth 2.0 Requirements

- All token exchanges **MUST** use HTTPS / TLS 1.3.
- Token scope and lifetime **MUST** be limited.
- Client secrets **MUST NOT** be exposed in logs or client-side code.
- Token signature, issuer, and audience **MUST** be validated on every request.

> 📝 **OAuth 2.0** mirrors the approach used by TOTSCo for OTS, making it the most compatible option across the industry. MAPs that already have TOTSCo OAuth credentials may be able to reuse them for CSF connectivity.

6.4 API Key Authentication

API key authentication is a simpler mechanism where a client includes a unique secret key in each request. In the CSF context:

- API keys are recommended for **MAP-to-CP** communication, where full OAuth 2.0 would be excessive.
- API keys **MUST NOT** be used for **MAP-to-MAP** communication over the CSF — OAuth 2.0 is mandatory.
- All API key exchanges **MUST** use TLS 1.3.
- Keys **MUST** be stored securely, rotated regularly, and granted minimal access.

6.5 PKI and DKIM Message Signing

Public Key Infrastructure (PKI) provides the cryptographic framework for message signing and verification. The CSF implements PKI through DKIM (DomainKeys Identified Mail, RFC 6376), a standard originally designed for email authentication but ideally suited to federated, distributed messaging.

Why DKIM?

DKIM is ideal for the CSF because it:

- Provides **message integrity** — the message body cannot be tampered with undetected.
- Provides **domain-level authentication** — the signature confirms which domain (and therefore which CP) authorised the message.
- Uses **DNS for public key distribution** — no centralised certificate authority is needed.
- Gives **CPs control** — a CP's DNS records determine which MAP is authorised to sign on their behalf.
- Is a **proven standard** used at internet scale for email authentication.

How It Works (Conceptual)

1. When a MAP sends a message, it creates a cryptographic hash of the message body and selected headers.
2. The hash is encrypted (signed) with the source CP's **private key** — held securely by the MAP.
3. The signature is placed in the HTTP header `X-CSF-SIGNATURE` — the message body is not modified.
4. The receiving MAP retrieves the source CP's **public key** from a DNS TXT record.
5. The receiving MAP recalculates the hash and verifies it against the decrypted signature.
6. If the hashes match, the message is authentic and unaltered; if not, the message is rejected.

DNS Records for Each CP

Each CP maintains two DNS TXT records that establish their identity and MAP association:

- **`[RCPID]._domainkey.[cp-domain]`** — contains the CP's public key for signature verification.

- **`[RCPID]._mapkey.[cp-domain]`** — contains the URL of the CP's MAP message endpoint.

These records are controlled by the CP, ensuring that:

- Only the MAP indicated in DNS can sign messages on the CP's behalf.
- The CP can change MAP by updating these DNS records.
- Any receiving MAP can independently verify the message origin without relying on a central authority.

> 💡 **For implementers.** Detailed DKIM implementation guidance, worked code examples (Java and C#), CSF HTTP headers, signing algorithms, and error codes are provided in *Part 2: PKI & DKIM Signing*.

6.6 Security Summary

The CSF protects every interaction with:

- **TLS 1.3** — encrypting all data in transit between MAPs.
- **OAuth 2.0** — controlling who can access which endpoints.
- **PKI / DKIM** — verifying that every message is authentic, unaltered, and authorised by the source CP.

No single layer is sufficient on its own. Together, they provide **confidentiality** (data cannot be read), **authentication** (identities are verified), **authorisation** (access is controlled), and **integrity** (content cannot be tampered with).

7. Onboarding

7.1 Overview

The CSF uses a peer-sponsored onboarding model. There is no centralised registration authority. Instead, existing MAPs take responsibility for validating and onboarding new participants, ensuring quality and compliance without the cost and complexity of a central governing body.

A minimum of **two MAPs** is sufficient for a basic bilateral exchange. This eliminates the need for a "big bang" approach — MAPs and CPs can be onboarded incrementally.

7.2 Onboarding a New MAP

7.2.1 Sponsorship Framework

New MAPs are onboarded through a structured, multi-phase process guided by a **Sponsor MAP** — an existing, onboarded MAP assigned through round-robin rotation.

Key principles:

- **Rotating sponsorship.** Sponsor MAP responsibilities are distributed equally among all onboarded MAPs using a sequential rotation. The current Sponsor MAP is published in the registry using a token-based approach.
- **Capped costs.** A Sponsor MAP may charge the new MAP for time and effort during onboarding, but this charge is capped at **£3,000** to avoid discouraging new market entrants.
- **Gatekeeper role.** The Sponsor MAP acts as a gatekeeper to the CSF network, ensuring operational performance and compliance.
- **Evolving criteria.** The TAG continuously updates entry criteria to reflect the latest maturity levels and address known issues identified through industry testing and operational working groups.

7.2.2 On-Ramp Process

The onboarding process follows five phases:

> **1. Select Sponsor MAP → 2. Initial Assessment → 3. Integration & Testing → 4. Operational Validation → 5. Full Operations**

Phase 1 — Sponsor MAP Selection and Agreement

- The new MAP identifies and selects an existing MAP as its sponsor (or is assigned one via rotation).
- The Sponsor MAP verifies the request is legitimate.
- Both parties agree on technical, operational, and compliance criteria.

Phase 2 — Initial Assessment and Registration

- The Sponsor MAP conducts a capability assessment covering technical readiness, security, and compliance.
- The new MAP registers essential details: endpoint URLs, PKI credentials, and directory synchronisation preferences.

Phase 3 — Integration and Testing

- Secure communication channels are established using OAuth 2.0 and PKI.
- Credentials at this stage provide **provisional / restricted access** — directory information should contain limited, obfuscated data to prevent disclosure of client information until testing is complete.
- Testing verifies secure, authenticated message exchanges and directory synchronisation.
- Once basic connectivity is proven, access levels are raised to **test** — the directory will now contain information to facilitate test communications (with CP consent or using test CPs).

Phase 4 — Operational Validation

- The Sponsor MAP verifies adherence to operational requirements: message delivery reliability, retry mechanisms, and SLA compliance.
- Validation tests ensure interoperability with other MAPs and CPs.
- Each other MAP performs additional sanity testing as they establish their own OAuth 2.0 connections with the new MAP.

Phase 5 — Full Operations

- The Sponsor MAP formally approves the onboarding and notifies all other MAPs.
- Connectivity is upgraded to **full access**.
- The new MAP freely shares its complete CP Registry with other MAPs.
- The new MAP commences independent, full operational integration.

> 📝 The detailed testing process, entry criteria, and exit criteria are set out in the separate "New MAP Onboarding & Testing Process" document maintained by the TAG.

7.3 Onboarding a CP

CP onboarding is a commercial matter between the CP and its chosen MAP. The CSF does not prescribe how MAPs select or charge their CPs. However, the CSF requires certain steps to be completed before a CP can exchange messages.

7.3.1 MAP Responsibilities

1. **Allocate a unique RCPID** — a UUIDv4 identifier, verified against the directory to prevent collisions (see *RCPID Management (Chapter 8)*).
2. **Generate PKI key pair** — create the public/private key pair for the CP.
3. **Guide DNS setup** — assist the CP in creating the two required DNS TXT records:

- `[RCPID]._domainkey.[cp-domain]` — containing the public key.
- `[RCPID]._mapkey.[cp-domain]` — containing the MAP's message endpoint URL.

4. **Collect customer data assets** — ensure the MAP has sufficient data to perform timely Switch Match responses without relying on the CP being online.
5. **Validate compliance** — ensure the CP meets the requirements of the industry process they wish to participate in.
6. **Publish in registry** — add the CP to the MAP's registry with all mandatory fields.

7.3.2 When a CP Can Exchange Messages

No messages can be exchanged until other MAPs verify that the CP is correctly associated with the MAP in its directory. This verification happens automatically when MAPs pull the updated registry and cross-reference it against the CP's DNS records.

A MAP can register a new CP and advertise it to other MAPs **within seconds**. However, the CP controls when it is ready to exchange by managing its DNS entries and service status (ACTIVE, TEST, SUSPENDED).

7.4 Testing in Production

The CSF supports testing in production during onboarding:

- All test traffic **MUST** be explicitly marked as test in the audit record held in the JAM envelope.
- The onboarding MAP **MUST** override the test flag until the CP has passed exit criteria — even if the CP sets it.
- A published set of test data assets is available for entry criteria testing, performed locally with the MAP using a Virtual Test Host.
- A hidden set of unit tests forms the exit criteria before the CP is granted production status.
- PKI verification tools are available to assist with setup and testing.

> 📝 **Note.** Not all CPs will have SIT/UAT environments. The CSF is designed to support continuous onboarding throughout core business hours, with strict protocols and test-flagging to prevent test traffic from affecting production operations.

7.5 Memorandum of Understanding (MoU)

MAPs and CPs that collaborate on the CSF are bound by a Memorandum of Understanding that outlines the terms of participation. The MoU is designed to be simple to join, reflecting the CSF's nature as an open standard that is licence-free for any CP or MAP to use for any purpose.

8. RCPID Management

8.1 What is an RCPID?

A Retail Communications Provider Identifier (RCPID) is a unique identifier assigned to a CP brand for the purpose of message exchange. Each RCPID maps 1:1 to a human-readable brand name that appears in search and drop-down lists used by CPs when initiating a Switch Match.

8.2 Why UUIDv4?

The CSF adopts **UUIDv4** (RFC 4122) as the RCPID format, replacing the 4-character alphanumeric codes used by OTS.

Problems with the OTS Format

The OTS format (Rxxx — for example, RGXD, RYHC) has several limitations:

- **Collision risk.** With only 4 characters, the probability of duplication increases as more CPs join for business switching (expected tenfold increase over OTS).
- **Human confusion.** Similar codes are easily mistaken (for example, RYHC and RYCH are different brands but commonly confused — and they can exist in the same MAP).
- **MAP coupling.** If prefixes are tied to MAPs, changing MAP requires changing RCPID, which is costly and disruptive.
- **Scalability.** The format does not scale for business switching where CPs may have multiple brands requiring separate identifiers.

Benefits of UUIDv4

UUIDv4 addresses all of these issues:

- **Virtually zero collision risk.** With 122 bits of randomness, the odds of collision between any two UUIDs are 1 in 2.71 × 10^18. One would need to generate 1 billion UUIDs per second for 85 years to have a 50% chance of a single collision.
- **Self-allocation.** MAPs can generate RCPIDs independently without central coordination.
- **No human bias.** Machine-generated identifiers eliminate human-readable confusion.
- **Portability.** The RCPID stays with the CP for life, regardless of which MAP they use.
- **Data continuity.** All historical data (time-series, audit records, reporting) remains consistent as CPs move between MAPs.

Example RCPID: `d8322d80-92c8-4906-a408-f1d2daf7e03d`

Compatibility with OTS

The UUIDv4 format does not preclude any CP or MAP (including TOTSCo) from continuing to use the OTS Rxxx format internally. MAPs can maintain a mapping between their internal codes and the UUIDv4 RCPID used for SfB message exchange.

The SfB Message Specification defines the source and destination identity fields as strings with a maximum length of 256 characters. UUIDv4 (36 characters including hyphens) fits well within this constraint.

8.3 Allocation Process

1. The MAP generates a UUIDv4 for the new CP brand.
2. The MAP provisionally allocates it to the CP.
3. Before going live, the MAP pulls all other MAP directories and checks for collisions.
4. If no collision is detected, the MAP publishes the RCPID in its registry.
5. If a collision is detected (extremely unlikely), the MAP generates a new UUID and repeats.

> **Responsibility.** It is the MAP's responsibility to ensure no duplication or collisions occur. The MAP **MUST** check the generated ID against the directory before allocating it to a CP and advertising it as live.

8.4 RCPID Lifecycle

Allocation

An RCPID is allocated to a CP brand and remains associated with that brand **for life**. This helps with:

- CPs moving between MAPs.
- Future brand consolidation or growth.
- Mergers and acquisitions.
- Consistent time-series data and historical reporting across all MAPs.

MAP Transitions

When a CP moves between MAPs:

1. The RCPID **does not change** — it remains constant and unique across the network.
2. The new MAP adds the existing RCPID to its CP Registry.
3. The old MAP removes the RCPID from its CP Registry.
4. Other MAPs detect the change through CP Registry synchronisation and DNS verification.

This ensures seamless continuity for in-flight orders and network-wide consistency.

Retirement

When a CP brand is dissolved or merged, the RCPID is retired and retained in an archived state for historical reporting purposes. It **MUST NOT** be reused for a different brand.

8.5 Handling Exports During Transitions

When a CP moves to a new MAP, the in-flight order data must be transferred:

1. **Export with ID mapping.** On a valid "RCPID Status" request, the old MAP provides a standardised JSON export of all in-flight orders for the specified RCPID.
2. **Validation.** The request is validated by checking that the RCPID's DNS entry now points to the MAP making the request.
3. **CP Registry updates.** The old MAP removes the CP from its CP Registry before responding, ensuring no duplicate entries exist.
4. **Verification.** The new MAP verifies the accuracy of the RCPIDs and ensures no collisions.

> 💡 For the complete transition process including in-flight order handling, see *Part 2: CP Transitions*.

8.6 Summary

Aspect	OTS (Legacy)	CSF
Format	4-character alpha (Rxxx)	UUIDv4 (36 characters)
Allocation	Centralised or MAP-specific	MAP self-allocates
Collision risk	Moderate (grows with scale)	Negligible (1 in 2.71 × 10^18)
Portability	Tied to MAP (prefix-based)	Follows the CP for life
Human readability	Confusing (RYHC vs RYCH)	Not human-readable (by design)
Scalability	Limited for business switching	Unlimited

9. Operational Excellence

9.1 Core Principles

The CSF is built on three operational cornerstones:

- **Security.** Strong encryption, robust authentication, and digital signing.
- **Efficiency.** Accurate and timely telecom service transitions.
- **Reliability.** Resilient architecture ensuring continuous availability.

9.2 Availability Target

MAPs **MUST** target **99.999% availability** (five nines) for switching services. This equates to no more than approximately 5 minutes of unplanned downtime per year.

9.3 High Availability and Redundancy

MAPs MUST:

- Deploy **multiple geographically distributed** instances (subject to GDPR) to eliminate single points of failure.
- Implement **automatic failover** mechanisms capable of instantly transitioning operations to backup systems without noticeable service disruption.
- Maintain **fully redundant network paths** and infrastructure components.

9.4 Continuous Operations During Maintenance

MAPs MUST implement rolling updates and upgrades to ensure that maintenance activities — including software updates and security patching — do not impact service continuity.

Recommended deployment strategies:

- **Blue-Green Deployment.** Maintain two identical production environments. Deploy updates to the inactive environment, validate, then seamlessly switch traffic. This enables rapid rollback if issues are discovered.
- **Canary Deployment.** Gradually roll out updates to a small subset of traffic, monitor performance, and incrementally increase exposure based on positive outcomes.

MAPs SHOULD clearly communicate planned maintenance activities — even when designed to have no service impact — to maintain transparency and stakeholder confidence.

9.5 Monitoring and Alerting

MAPs MUST provide:

- **Real-time, proactive monitoring** with automated alerting capable of detecting and addressing issues before they affect availability.

- **Mandatory status indication** in the MAP Registry when an incident occurs, including clearly recorded planned changes highlighting any periods of potential risk.

MAPs SHOULD provide:

- A transparent, real-time **status dashboard** accessible by connected providers, showing platform health and operational metrics.

9.6 Disaster Recovery

MAPs MUST:

- Regularly **test and validate** disaster recovery procedures, including full failover scenarios and restoration processes.
- Establish **Recovery Time Objectives (RTO)** and **Recovery Point Objectives (RPO)** that align with the commitment to continuous availability.

9.7 Security and Compliance

MAPs MUST:

- Maintain rigorous security standards and apply timely patches without disrupting ongoing service.
- Adopt **secure-by-design** principles to ensure resilience includes robust protections against cyber threats.
- Conduct **regular security audits** and vulnerability assessments to identify and mitigate risks proactively.

9.8 Guaranteed Message Delivery

Pre-Send Verification

Before sending a message, the originating MAP SHOULD verify the resilience status of the receiving MAP using information from the MAP Directory. This includes checking:

- Whether the receiving MAP is currently online.
- Whether they are in a known period of planned change or experiencing an incident.

Retry Policy

If the originating MAP does not receive a synchronous HTTP 202 acknowledgement (for example, receives a 400, 500, or timeout), it MUST:

1. Automatically retry message delivery at pre-defined intervals using **exponential backoff** to avoid overwhelming the recipient MAP.
2. Log and escalate incidents if repeated delivery attempts fail within agreed thresholds.
3. Maintain comprehensive **audit trails** of all message exchanges, delivery attempts, and outcomes.

4. Define **maximum retry periods** and implement alerting mechanisms to trigger operational intervention when delivery consistently fails.

Asynchronous Error Handling

The CSF employs asynchronous error codes (8xxx series) to signal and assist MAPs during message processing. These codes are designed for self-healing and promoting good practices, complementing the industry-standard 9xxx codes used by OTS/TOTSCo.

> 💡 For details on error codes and message delivery failure formats, see *Part 2: Message API*.

9.9 Service Level Agreements

> Specific SLAs for MAP-to-MAP activity are to be formalised. The following indicative levels have been agreed:

Category	Target
Platform availability	24×7 high availability (queue and retry during unavailability).
Directory freshness	Near-real-time updates (never delete the last compiled directory).
Working hours	Core business hours for support.
Planned maintenance	Outside business hours (with objective of minimal planned outages).
MAP-to-MAP response time	1 working day.
Priority 1 (MAP unavailable)	Fix within 4 working hours.
Priority 2 (CP unavailable)	Fix within 1 working day.
Priority 3 (Service degradation)	Fix within 2 working days.
Priority 4 (Change requests)	Actioned within 1 working week.

9.10 Capacity Planning

> MAPs should scale their infrastructure to align with their CP base. The following minimum rate calculation is recommended:

Messages per second = Total Switchable Asset Base / 1,000

With an **absolute minimum of 2 messages/second**.

Examples:

- **MAP with 5,000 switchable assets:** 5,000 / 1,000 = 5 msg/s.
- **MAP with 20,000 switchable assets:** 20,000 / 1,000 = 20 msg/s.

MAPs can enhance acceptance rates using hardware acceleration and internal queuing, as SLAs for business switching are significantly longer than the 60-second Switch Match response times required by OTS.

10. Governance

10.1 Standards Landscape

The CSF operates within a multi-layered governance structure. Each layer has its own standards body, documentation, and change control process. The CSF leverages these existing standards rather than duplicating them.

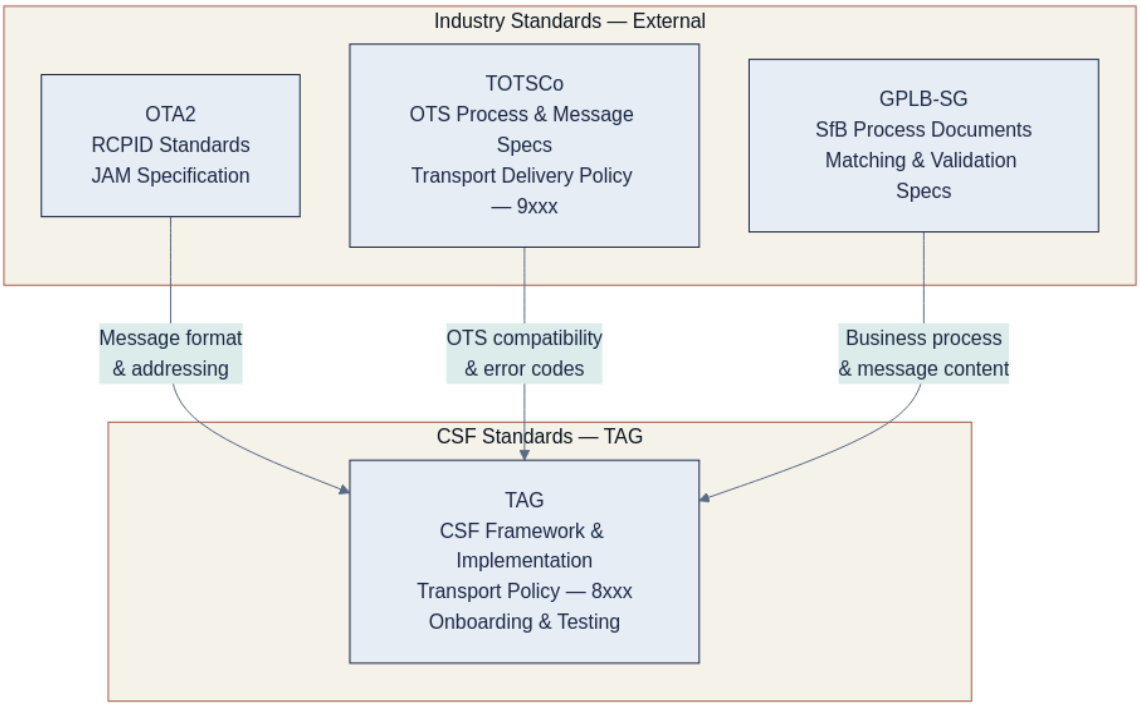

Figure 10.1 · Standards landscape and the CSF's position within it.

10.2 Standards Bodies

The following subsections set out the four standards bodies whose output the CSF depends upon or produces.

10.2.1 OTA2 — Office of the Telecommunications Adjudicator

Accountable for:

- RCPID Standards.
- JSON Asynchronous Messaging Specification (JAM Spec).

The industry has established RCPIDs and the JAM envelope as standards that **MUST** be implemented by all current and future transport providers, including TOTSCo and the CSF. These standards enable consistent addressing and routing of messages. The use of specific envelope fields may vary across industry processes (OTS, SfB) but the fields themselves are standardised.

All documentation is published on the OTA2 website (https://www.offta.org.uk/).

10.2.2 TOTSCo — Telecoms One Touch Switching Company

Accountable for:

- All OTS-related Message Process and Message Specification documentation.
- OTS Best Practice Guidance.
- Transport Delivery Policy and Response Codes (9xxx).
- TOTSCo Hub API Specification v2.0 (https://totsco.org.uk/wp-content/uploads/2026/04/TOTSCo-API-specifications-v2-Clean.pdf).

The Industry Process Group (IPG) and Operations Group (OG) generate original documentation and proposed changes. All documentation is under change control and published on the TOTSCo website (https://totsco.org.uk/process-technical-documents/).

10.2.3 GPLB-SG — GPLB Steering Group

The **GPLB Steering Group (GPLB-SG)** is an independent body of industry stakeholders working alongside the OTA2. It guides and facilitates the steering meetings and the publication of the Switching for Business (SfB) process documentation via FCS. The group retains the historical "GPLB" label even though the underlying *process* has been renamed from Gaining Provider Led Business switching to **Switching for Business (SfB)** to better describe the protocol.

Accountable for (via FCS publication):

- Switching for Business (SfB) Process documentation.
- Switching Open Orders specification.
- Matching Summary and Validation Process.
- **SfB Response Codes** and Asset List Guidance.
- Customer Matching Guidance.
- Best Practice Guide for Avoidance of Erroneous Transfers.
- SLAs.

All documentation is under change control from 30 September 2025 and published on the FCS website (https://www.fcs.org.uk/gaining-provider-led-business-switching/).

10.2.4 TAG — Telecom Technical Architecture Group

Accountable for:

- Connected Services Framework (CSF) — this documentation.
- CSF Transport Delivery Policy and Response Codes (industry 9xxx + CSF 8xxx enhancements).
- Testing and Onboarding of MAP documentation.
- Hub Implementation Overview Plan.

The TAG maintains autonomy to manage and iterate specific areas of the CSF. All changes to CSF documentation are undertaken by the TAG group, which meets via its steering group call **weekly**.

All documentation is under change control from 12 September 2025 and published on the CSF website (https://csf-uk.org/)

10.3 Change Control

CSF Documentation

All CSF documentation builds on existing OTS message exchange standards, including directory elements and TOTSCo 9xxx codes, to maintain consistency and avoid misunderstandings. Where additional response codes are required for security and signalling between MAPs and CPs, these are introduced using the **8xxx series**.

Changes to the CSF follow this process:

1. **Proposal**: any TAG member can propose a change.
2. **Review**: the TAG steering group reviews the proposal at its weekly meeting.
3. **Consensus**: changes require consensus among TAG members.
4. **Publication**: approved changes are published and versioned.
5. **Adoption**: MAPs adopt changes incrementally through API versioning and feature releases.

Industry Process Documentation

Changes to industry process documents (SfB process, JAM Spec, RCPID standards) follow the change control processes of their respective standards bodies (GPLB-SG, OTA2, TOTSCo). The CSF does not control these processes but references them.

10.4 Memorandum of Understanding

The MAPs and CPs that participate in the CSF are bound by a Memorandum of Understanding (MoU). The MoU:

- Makes it simple to join and contribute to the CSF.
- Reflects the CSF's nature as an open standard.
- Is licence-free for any CP or MAP to use for any purpose.
- Outlines the collaborative responsibilities of participants.

10.5 Decentralised Governance

The CSF deliberately decentralises governance responsibilities:

Principle	What it means in practice
No centralised administrator	Controls are distributed to CPs and MAPs.

Principle	What it means in practice
Self-regulation	The framework promotes good behaviour and discourages bad behaviour through its design (for example, DNS-based CP control, PKI verification, directory transparency).
Commercial independence	MAPs and CPs are free to establish their own commercial relationships; the CSF has no impact on these arrangements.
Cost reduction	Decentralising basic functions reduces costs for all parties and makes message exchange more transparent.

10.6 Governance Controls

The governance controls below were ratified by the TAG steering group on **2026-04-29** and form the operational baseline for the CSF's decentralised model. Each control leverages the framework's existing peer-to-peer architecture and the TAG's weekly steering group, without introducing heavy central administration.

10.6.1 TAG Decision-Making and Voting

The TAG steering group operates by consensus wherever possible. Where consensus cannot be reached, the following formal procedure applies:

- **Quorum.** A formal vote **MUST** be attended (in person or by recorded proxy) by at least **60% of currently onboarded MAPs**. A vote held below quorum is invalid and **MUST** be rescheduled.
- **Voting weight. One MAP, one vote**, regardless of MAP size, footprint, or seniority. A MAP that operates as a MAP-of-1 carries the same single vote as a MAP serving many CPs.
- **Voting threshold.** A **simple majority** of votes cast is sufficient for operational decisions. Specification changes (additions to or breaking changes in the CSF documents) require a **supermajority** of votes cast.
- **Decision records.** All TAG decisions **MUST** be recorded with the date, attendees, proposal summary, vote tally, outcome, and dissenting views. These records are accessible to all MoU signatories.
- **Observer status.** Organisations that are not yet MAPs but have a legitimate interest — for example, prospective MAPs, industry bodies, OTA2, TOTSCo — **MAY** attend TAG meetings as observers. Observers contribute to discussion but do not count toward quorum and have no voting rights.

10.6.2 MAP Compliance and Periodic Review

Onboarding validates a MAP at a point in time, but ongoing compliance must also be assured:

- **Annual self-certification.** Each MAP **SHOULD** submit an annual self-certification to the TAG confirming continued compliance with the CSF requirements, including PKI key hygiene, SLA adherence, and CP Registry accuracy.

- **Peer review.** The TAG **SHOULD** establish a lightweight peer review process where MAPs periodically verify each other's CP Registry accuracy, DNS record consistency, and endpoint availability. This can be automated through existing registry collection and DNS verification mechanisms.
- **Evolving exit criteria.** As the TAG updates onboarding entry and exit criteria to reflect new use cases and lessons learned, existing MAPs **SHOULD** be required to demonstrate compliance with material changes within an agreed adoption window.

10.6.3 Version Adoption Policy

API versioning enables incremental change, but without adoption timelines the network could fragment:

- **Minimum support window.** When a new CSF version is released, MAPs **MUST** continue to support the previous version for **six months from the release date**, to allow all participants to upgrade.
- **Deprecation notice.** The TAG **MUST** provide at least three months' notice before deprecating a CSF version.
- **Adoption tracking.** The TAG **SHOULD** track which CSF version each MAP supports (visible in the CP Registry) and follow up with MAPs that have not adopted within the agreed window.

10.6.4 Dispute Resolution

Disputes between MAPs — for example, over CP ownership, message delivery failures, or onboarding decisions — need a resolution path that does not require legal action as a first resort:

Tier	Mechanism	Detail
Tier 1	**Direct resolution**	The MAPs involved attempt to resolve the dispute directly using the contact details published in their CP Registries.
Tier 2	**TAG mediation**	If direct resolution fails within 5 working days, either party can escalate to the TAG steering group, which will mediate at its next meeting. The TAG may appoint a subset of uninvolved MAPs to review the facts.
Tier 3	**Independent adjudication**	If TAG mediation fails, the dispute **MUST** be referred to **OTA2** as the standing independent adjudicator for the CSF. OTA2's adjudication is binding on the parties to the dispute. OTA2's role and history as a UK telecoms adjudicator is summarised in §10.2.1; the TAG will engage OTA2 directly and provide the case file, supporting evidence, and the result of Tier 1 and Tier 2 attempts.

> **Interim measures.** During any dispute, both MAPs **MUST** continue to exchange messages normally. A dispute **MUST NOT** be used as a reason to block or degrade service to CPs.

10.6.5 Incident Response Coordination

While each MAP manages its own security, coordinated response to network-wide incidents is essential:

- **Security contact.** Each MAP **MUST** publish a dedicated security contact in its CP Registry (separate from general support) for reporting vulnerabilities and incidents.
- **Coordinated disclosure.** If a MAP discovers a vulnerability that affects the CSF specification or other MAPs, it **MUST** notify the TAG within 24 hours. The TAG will coordinate disclosure and remediation across all MAPs.
- **Breach notification.** If a MAP suffers a data breach that could affect CP data or message integrity, it **MUST** notify all connected MAPs, the TAG, and affected CPs within **72 hours of becoming aware**, in alignment with the wider industry standard set by UK GDPR / Data Protection Act 2018 Article 33 personal-data breach notification. Notifications **MUST** include the nature of the breach, categories and approximate volume of data affected, the likely consequences, and the mitigations taken or proposed.
- **Post-incident review.** Significant incidents **SHOULD** trigger a post-incident review at the TAG steering group to identify systemic improvements.

10.6.6 MAP Suspension and Removal

The CSF must have a clear, proportionate process for dealing with MAPs that persistently fail to meet their obligations or act maliciously:

Stage	Trigger	Consequence
Warning	TAG issues a formal written warning identifying the non-compliance and a remediation deadline.	Typically 10 working days.
Probation	Failure to remediate within the warning period.	MAP status flagged in other MAPs' Master Registries. Voting rights in TAG decisions suspended.
Suspension	Serious or persistent non-compliance.	TAG votes to suspend. Suspended MAP's CPs treated as if the MAP were in distress; the CP emergency migration process applies and CPs are encouraged to move to another MAP.
Removal	Suspended MAP does not remediate within 30 days.	Permanent removal by TAG supermajority vote. CP Registries no longer collected by other MAPs.

> **CP protection.** At every stage, the priority is CP continuity. No enforcement action against a MAP should leave CPs unable to exchange messages for longer than necessary. The CSF's built-in ability to migrate CPs — including their in-flight orders — between MAPs via the RCPID Status export process is an integral safeguard here. Where a MAP is suspended or removed, the TAG **SHOULD** proactively

> coordinate with affected CPs and receiving MAPs to ensure that the CP emergency migration process is initiated promptly, in-flight order exports are completed before the MAP is taken offline, and CPs are re-established on new MAPs with minimal disruption to end consumers.

10.6.7 Anti-Competitive Safeguards

The CSF's open, free-to-use nature must be actively protected:

- **No exclusionary behaviour.** No MAP or group of MAPs may act to exclude a legitimate new entrant from the CSF. Sponsor MAPs **MUST NOT** unreasonably refuse or delay onboarding.
- **No preferential routing.** MAPs **MUST NOT** give preferential treatment to their own CPs' messages over messages routed on behalf of other MAPs' CPs.
- **No information misuse.** Information obtained from other MAPs' CP Registries — CP lists, contact details, switching volumes — **MUST NOT** be used for competitive advantage, marketing, or customer solicitation.
- **Telemetry collection.** Every MAP **MUST** collect telemetry data for all messages sent and received **between `ACTIVE`-status MAPs and on behalf of `ACTIVE`-status CPs only**, including: message type (routingID), date/time, source CP (RCPID), destination CP (RCPID), source MAP, destination MAP, and delivery outcome (success, failure code). Messages where either endpoint MAP carries `map.status = TEST` or `SUSPEND`, where either CP carries `processSupport[].status = TEST` or `SUSPEND`, or where the JAM envelope's `auditData` carries the explicit test marker (`{ "name": "test", "value": "true" }`) **MUST** be excluded from telemetry counted toward industry statistics. This ensures that onboarding traffic, bilateral test runs, and post-incident soak testing never pollute reporting or KPIs. Telemetry data **MUST** be stored securely and handled in accordance with GDPR and the data retention policies agreed by the TAG. Test-flagged messages **MAY** still be logged separately for audit and onboarding evidence, but **MUST** be tagged as such and held outside the production telemetry corpus. See *Onboarding & Testing Process §5* for the audit-flag rules and *§4 Status Model* for status semantics.
- **Transparency.** The TAG **SHOULD** publish an annual summary of CSF network activity — including aggregated message volumes by message type, number of active MAPs and CPs, onboarding activity, and delivery success rates — to demonstrate openness and healthy competition. Each MAP **MUST** contribute its aggregated telemetry to this summary, **drawn solely from production traffic between `ACTIVE` participants** as defined above. Individual CP-level data, message content, or commercially sensitive patterns **MUST NOT** be disclosed — only aggregated, anonymised statistics are published. See the *REVIEW document* for options on how telemetry can be collected and shared without revealing sensitive data or breaching GDPR.

10.6.8 CP Representation

While the CSF primarily governs MAP-to-MAP interactions, CPs are the ultimate beneficiaries and should have a voice:

- **CP feedback channel.** The TAG **SHOULD** establish a mechanism for CPs to raise concerns or propose improvements, either directly or through their MAPs.

- **CP rights charter.** The **CP Rights Charter** is published as a standalone document, written in plain language, so CPs can understand their entitlements without reading the full CSF specification. It is derived from the formal requirements in *Principles & Requirements — CP Right to Move (Chapter 3)*.

10.6.9 Documentation and Transparency

- **Public documentation.** The CSF specification (this documentation) **SHOULD** be publicly accessible to any interested party, not restricted to MoU signatories. Transparency builds trust and encourages adoption.
- **Change log.** All changes to the CSF specification **MUST** be recorded in a versioned change log with dates, descriptions, and the TAG meeting reference where each change was agreed.
- **Archived versions.** Previous versions of the CSF specification **MUST** be retained and accessible so that MAPs running older versions can reference the specification they implemented against.

10.7 Supporting Documents

The following documents support the CSF and are maintained separately. They are listed here for reference; their content and change control remain with the owning body.

Document	Version	Maintainer
MAP Onboarding and Testing	Draft	TAG
PKI Overview	Draft	TAG
Use-Cases and Examples	Draft	TAG
TOTSCo Integration — Implementation Plan	v1.1	TAG
TOTSCo Integration — Overview Slides	v1.0	TAG
JSON Asynchronous Messaging Specification	v1.0	OTA2
Principles of Use for RCPID	v1.0	OTA2
TOTSCo Hub API Specification	v2.0	TOTSCo

Glossary

Quick-reference abbreviations used throughout this document. The full Definitions & Terminology section at the front of the document provides extended definitions for the key concepts (CP Registry, Master Registry, Directory, Sponsor MAP, New MAP, Letterbox, Routing Group, Feature Release).

Abbreviation	Term
CP	Communications Provider
CSF	Connected Services Framework
DDG	Detail Design Group
DKIM	DomainKeys Identified Mail (RFC 6376)
DNS	Domain Name System
GPLB	Gaining Provider Led Business Switching
GPLB-SG	GPLB Steering Group
HMAP	Hub Managed Access Provider
JAM	JSON Asynchronous Message
MAP	Managed Access Provider
MoU	Memorandum of Understanding
OTA2	Office of the Telecommunications Adjudicator
OTS	One Touch Switch
PKI	Public Key Infrastructure
RCPID	Retail Communications Provider Identifier
RFC	Request for Comments
SfB	Switching for Business
TAG	Telecom Technical Architecture Group
TLS	Transport Layer Security (RFC 8446)
TOTSCo	Telecoms One Touch Switching Company

Copyright & Disclaimer

The Connected Services Framework ("CSF") is an open technical standard maintained by the **Telecom Technical Architecture Group (TAG)**. The CSF operates within the broader UK telecoms standards ecosystem and references, but does not control, the work of OTA2, TOTSCo, and GPLB-SG as described in §10.2.

Copyright and Permitted Use

The CSF is published as an open standard. Subject to the terms of the Memorandum of Understanding (§10.4) and the permissions set out below, any Communications Provider (CP) or Managed Access Provider (MAP) may:

- Store, reproduce and distribute the CSF specification in its entirety, without modification, for the purposes of implementing or participating in the framework.
- Quote short extracts with attribution to the Connected Services Framework and a reference to the document (title, version and date).
- Incorporate references to the CSF into their own technical documentation, commercial agreements, and regulatory submissions, with attribution.

Any other reproduction, adaptation, or commercial use not contemplated by the MoU requires the prior written consent of the TAG.

Relationship to Other Standards

This document refers to, and depends upon, materials maintained by OTA2, TOTSCo, and GPLB-SG. Copyright in those materials remains with their respective owning bodies. Where this document summarises or references those materials, it does so under the terms applicable to each body's publications.

Status of this Document

> **This is the v2.0.2 released version of CSF Part 1 — assembled for TAG review.** It is provided on an "as-is" basis and does not constitute legal, regulatory, commercial or technical advice. This published CSF specification is the authoritative source; where this document and other drafts diverge, this published specification prevails. The TAG accepts no liability for any loss or damage arising from reliance on this document.

Review Forum and Contact

This document is reviewed at the **TAG steering group's weekly call**. Comments, questions, and proposed amendments should be directed to the TAG editorial owner via the standing TAG communication channels.