Procedure for endorsing MCP MSR service providers

Document Revision

ID: MCP Gen 9			
Version	**Author(s)**	**Nature of change**	**Date of adoption**
x	Thomas Christensen, Jakob Svenningsen	Initial version	

Purpose

This document defines the mandatory process for endorsing MCP MSR service providers. It establishes responsibilities, sequencing, and evaluation criteria to ensure that only MCP MSR service providers adhering to MCP security, privacy and interoperability requirements are trusted.

1 ROLES AND RESPONSIBILITIES

Role	Responsibilities
Applicant	Submits complete application package and responds to information requests.
Secretariat	Manages the workflow, performs completeness checks, conducts the detailed technical and operational assessment, maintains records and schedules renewals.
Board	Provides strategic oversight, nominates rapporteurs, reviews Secretariat's report and decides on endorsement, conditional endorsement or rejection.
Board Rapporteur	One Board member assigned per application; perform high-level review against strategic goals, independence and risk; coordinate questions to Secretariat.

2 PROCEDURE

The process of endorsing an MCP MSR service provider consists of the following steps:

Step	Actor	Action	Output / Decision
0	Secretariat	Optional pre-application meeting to explain requirements.	–
1	Applicant → Secretariat	Submit application form plus artefacts listed in Annex A.	Application package
2	Secretariat	Completeness check within 5 working days.	Application package accepted/rejected (incomplete)
3	Secretariat → Board Chair	Forward application package and request nomination of one rapporteur.	–
4	Board Chair	Appoint rapporteur within 3 working days.	Rapporteur confirmed
5	Rapporteur	Strategic & governance review using Board Checklist (Annex B). May request clarifications via Secretariat.	Preliminary recommendation
6	Secretariat	Technical & operational assessment (Annex C). Produce detailed report and compliance matrix.	Assessment report
7	Secretariat → Board	Circulate assessment report and all artefacts at least 14 days before the decision meeting.	–
8	Board	Rapporteur presents their preliminary recommendation and outcome of the assessment (step 6). Possible outcomes: *Approve*, *Reject*.	Board resolution
9	Secretariat	Notify applicant of decision within 3 working days.	Notification letter
10	Secretariat	If approved, update website and repository.	Publication completed
11	Secretariat	Archive dossier and set renewal reminder (12 months minus 30 days).	Renewal task scheduled

3 RECURRENCE AND CHANGES AFTER ENDORSEMENT

Endorsement of an MCP MSR service provider remains valid for a period of 12 months from the date of Board approval. To maintain continuity, the Secretariat must initiate a renewal review prior to expiry. This review consists of repeating the technical and operational assessment outlined in Appendix C.

If the reassessment identifies no material deviations or concerns, the endorsement is automatically renewed for another 12--month term without requiring additional Board action.

However, if the Secretariat identifies any material deviation from the original approval criteria, including procedural changes, technical non-compliance, or security concerns, a report will be escalated to the Board. The Board must then decide whether to suspend, revoke, or grant a waiver for continued endorsement.

In the event of suspension or revocation, the change in status will be published immediately to ensure transparency and the integrity of trust.

Additionally, a re-assessment of any endorsed MCP MSR service provider may be triggered at any time if the board decides on such action. In that case, the procedures outlined in this document apply accordingly.

4 OPERATIONAL REQUIREMENTS

The following list describes the operational requirements an MCP MSR service provider must comply with:

1. An MCP MSR service provider must implement the requirements described in IALA G1191.
2. An MCP MSR service provider must only provide services with a valid identity issued by an MCC endorsed MCP identity service provider.
3. An MCP MSR service provider must participate in the global search network as described in IALA G1191 to enable service discoverability across different service registries.

ANNEX A – REQUIRED ARTIFACTS FOR INITIAL APPLICATION

1. Evidence required to validate the organisation's identity in accordance with MCP Gen 5 vetting.
2. A written declaration that the organisation follows applicable data privacy practices (e.g. GDPR).
3. A testable endpoint (URL) for the purpose of testing that the MSR implementation fulfils the requirements in IALA G1191.

ANNEX B – BOARD REVIEW CHECKLIST (RAPPORTEUR)

1. Alignment with MCP objectives and community needs.
2. Independence from existing identity providers (conflict of interest).
3. Adequacy of organisational governance.
4. Risk profile (e.g., legal, cybersecurity, geopolitical – as appropriate).
5. Completeness and clarity of provided documents at policy level.

ANNEX C – SECRETARIAT TECHNICAL & OPERATIONAL ASSESSMENT

The Secretariat must perform the following checks:

1. Identity Validation – confirm the organisation’s identity under MCP Gen 5 vetting.
2. Data -Privacy Declaration – verify the presence and adequacy of the GDPR (or equivalent) compliance declaration.
3. Implementation validation – Using the testable endpoint (URL) to verify compliance with interfaces described in IALA G1191, Section 4.

REFERENCES

G1191: IALA Guideline 1191 ‘Maritime Service Registry (MSR) Technical Specification'