Procedure for endorsing MCP identity service providers

Document Revision

ID: MCP Gen 7			
Version	**Author(s)**	**Nature of change**	**Date of adoption**
1.0	Thomas Christensen	Initial version	General assembly meeting #5 December 6, 2021
1.1	Thomas Christensen	• Step 7 – one or more IPID's instead of just one • Recurrence section added • Added step 4 regarding data privacy	
1.2 DRAFT	Julius Moeller	Full rewrite – clarified roles, reordered steps, added Board guidance and detailed checklists	
1.3 draft	Thomas Christensen	Inserted changes from "other" version 1.2. Problem with versioning.	
1.4 draft	Thomas Christensen, Jakob Svenningsen	Editorial changes and minor clarifications in the endorsement procedure.	

Purpose

This document defines the mandatory process for endorsing MCP identity service providers. It establishes responsibilities, sequencing, and evaluation criteria to ensure that only MCP identity 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, issues MRN domain(s), 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 MCP identity service providers 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). Discuss and vote. Decision requires simple majority. Possible outcomes: *Approve*, *Reject*.	Board resolution
9	Secretariat	Notify applicant of decision within 3 working days.	Notification letter
10	Secretariat	If approved, **issue MRN domain(s)**, publish root certificate in trusted list, 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 identity 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 IDENTITY 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. MCP IDENTITY SERVICE PROVIDERS MUST ALSO NOTIFY THE SECRETARIAT OF ANY SIGNIFICANT CHANGES, SUCH AS UPDATES TO THEIR CP/CPS OR KEY ROLLOVER. THE SECRETARIAT WILL CONDUCT AN IMPACT

ASSESSMENT AND ESCALATE THE MATTER TO THE BOARD IF NECESSARY.ANNEX A – REQUIRED ARTIFACTS FOR INITIAL APPLICATION

1. Evidence required to validate the organisation's identity in accordance with MCP Gen 5 vetting.
2. The organisation’s written vetting procedure for enrolling organisations in its identity registry.
3. A written declaration that the organisation follows applicable data-privacy practices (e.g. GDPR).
4. Certificate Policy (CP) document.
5. Certificate Practice Statement (CPS) document.
6. Proposed MCP MRN domain(s) (IPID) for the organisation.
7. Root certificate of the organisation’s MCP PKI (PEM format).
8. Two example end-entity certificates for each MCP entity type, including the full certificate chain – one active and one revoked.
9. Endpoints (URLs) for the certificate revocation list (CRL) and for OCSP.
10. URL of the organisation's OIDC Well-Known configuration information endpoint.

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. Vetting Procedure Review – verify that the submitted vetting procedure meets or exceeds MCP Gen 5.
3. Data-Privacy Declaration – verify the presence and adequacy of the GDPR (or equivalent) compliance declaration.
4. CP/CPS Existence Check – ensure the Certificate Policy and Certificate Practice Statement are present and not empty.
5. Certificate Compliance – confirm the two sample certificates for every MCP entity type comply with IALA G1183 Chapter 5 MCP PKI.
6. CRL Freshness & Content – retrieve the CRL from the provided endpoint, confirm it is current and includes the revoked certificates while excluding active ones.
7. OCSP Response Accuracy – query the OCSP endpoint and confirm correct revocation status for all sample certificates.
8.

REFERENCES

G1183: IALA Guideline 1183 'The provision of Maritime Connectivity Platform (MCP) identities'