

Feasibility study

An IALA instance of the Maritime Connectivity Platform

DLA PIPER



Background & context

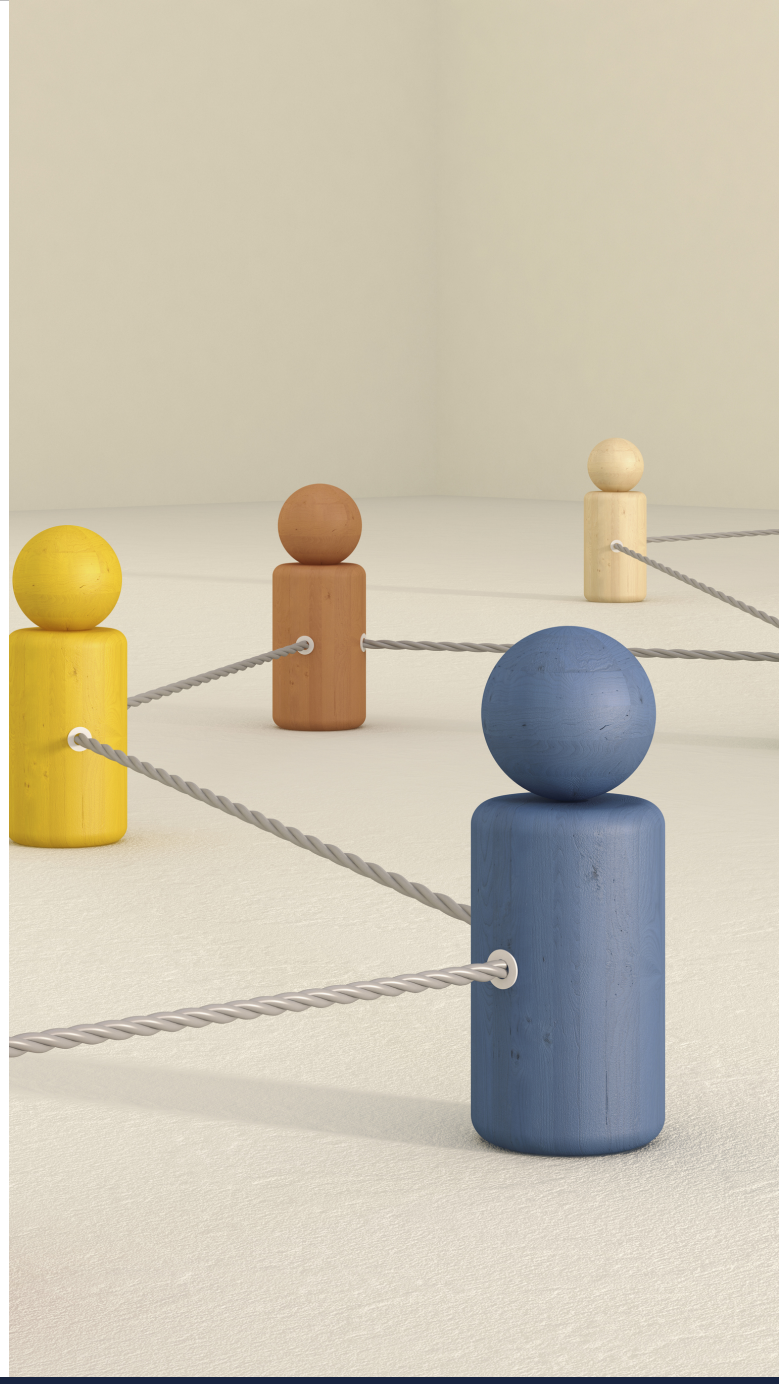
Why digital maritime connectivity needs trust

- **Shift:** from document-centric, manual information exchange to digital, service-based and near real-time exchange
- **Drivers:** S-100 data products, SECOM-based exchange, digital route exchange and IP connectivity between ship and shore
- **Need:** users must find authoritative services, trust the provider and know the data has not been manipulated
- **MCP:** a decentralised trust and service-discovery infrastructure – no single operator controls all services or data
- **MIR:** trusted maritime identities
- **MSR:** catalogue to publish and discover maritime services, incl. global search across MCP instances

Key stakeholders

Who shapes, operates and uses an IALA MCP instance

- **IALA:** intergovernmental organisation: governance, strategic direction and the participant framework
- **National authorities:** maritime administrations, coast guards, VTS, hydrographic offices and ports – identity holders and key publishers of public services.
- **Industry, service providers and end users:** equipment makers, software vendors, service providers, shipowners and operators
- **Host Member State (optional):** may provide facilities, funding and/or personnel to IALA



IALA MCP Instance – feasibility

The Study supports an IALA MCP instance

- **Scope assessed:** an IALA-operated or IALA-sponsored MCP instance regarding MIR and MSR
- **Legal benchmark:** EU law (e.g. GDPR, NIS 2, sanctions, competition)
- **Conclusion:** feasible in principle – legal, technical, operational and financial – subject to the decisions and measures identified
- **Key question:** not whether, but how – governance, responsibilities, risk, funding and contractual framework
- **Next steps:** further work and e.g. decision making on model, followed by implementation.





The two workable models

Tender model or IALA model

- **Model 1 (Tender):** a contractor establishes and operates; IALA keeps strategic governance via the tender contract
- **Model 2 (IALA):** IALA operates; development, hosting and maintenance can be outsourced

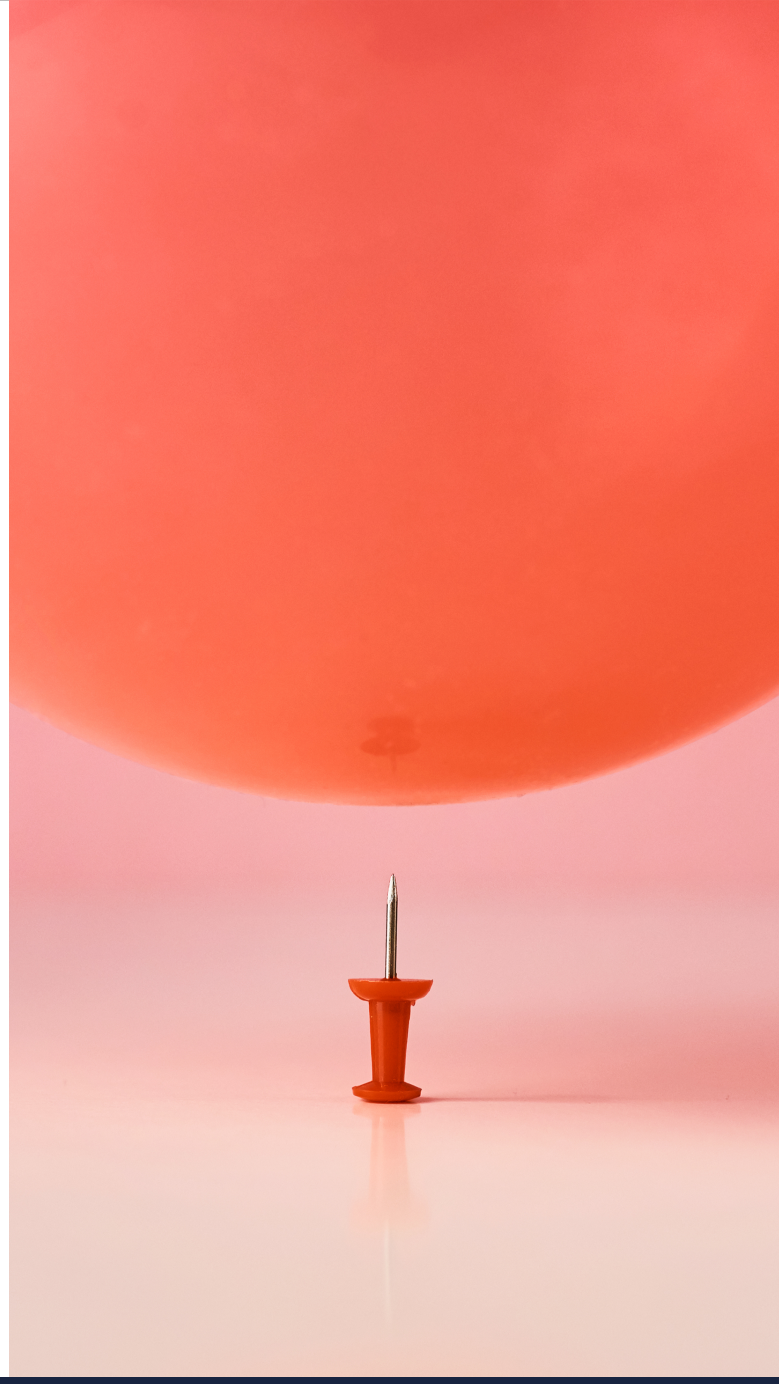
- **Host Member State:** can provide facilities, funding and/or personnel; IALA name and governance are kept (IHO infrastructure centre precedent)

- **Timeline:** approx. 12–24 months from decision to implementation

Key legal risks

A question of mitigation

- **Legal basis:** international legal personality and capacity to contract (Convention Art. 14)
- **Benchmarks:** GDPR, NIS 2, EU sanctions and fair, non-discriminatory access
- **Regulatory issues:** Data protection, cybersecurity, sanctions and export control, competition law and tax are matters of design, not obstacles.
- **Principal risks:** identity validation, service/data integrity, availability, cybersecurity, third-party claims to be managed with suitable contractual measures
  - **Allocation:** responsibility follows control – service providers answer for content; the operator for platform functions
  - **Contractual measures:** platform terms, contracts, interoperability agreements





Selected topics

Further insights into relevant areas

- **Third-party defects:** generally the Technical service provider; platform failures sit with whoever operates the function
- **Incorrect identity validation:** Model 1 – the contractor under the tender contract; Model 2 – IALA directly exposed
- **Public procurement:** no mandatory regime identified; a thorough, voluntary tender is recommended
- **Contractual framework:** T&Cs for providers and consumers, operator/supplier contracts and agreements with other MCP instances
- **Non-contractual claims:** to be managed contractually (indemnities)

Costs, funding and roadmap

From feasibility to operation

- **Funding:** hybrid model is under consideration
- **Roadmap:** six phases with various decision gates
- **First step:** an early IALA "Initial test" instance linked to the IHO test MCP and the MCP Public Demonstrator



Questions?

