Document: MCP Gen 4
Version: 1.0

Requirements for MCP identity service providers

1. INTRODUCTION

This document describes what it means to be an MCP (Maritime Connectivity Platform) identity service provider, and what the requirements are for being such. The document is high-level but other than this informative introduction is mostly normative.

The intended audience of this document includes:

Non-technical people in organisations that wish to be MCP identity service providers

Non-technical people in organisations that wish to rely on a MCP identity service provider for authentication

This document makes references to documents that are geared towards a technical audience, mainly the IALA Guideline 1183 'the provision of Maritime Connectivity Platform (MCP) identities' - G1183.

The goal of the MCP specifications is to enable easier development and deployment of network-based services for the maritime domain. This is achieved by specification of:

- Maritime Resource Names, MRNs, that identify a vessel, service, person, etc.
- an MCP Maritime Identity Registry (MIR), which assigns MRN's to vessels, services, persons, etc., and service providers. A MIR can issue X509 certificates that binds the assigned MRN to the holder of the private key associated with the public key in the certificate. A MIR can also act as a federated authentication service, minting tokens for use at a particular service.
- an MCP Maritime Service Registry (MSR), that allows parties to search for services that meet certain criteria, for example those that offer up-to-date AtoN information in a particular geographic area.
- an MCP Maritime Messaging service (MMS) allowing authorized maritime stakeholders to send and receive messages in an efficient, reliable and seamless manner within the MCP to solve problems of the current maritime wireless data communication system.

Various services can then choose to rely on a MIR to authenticate users. Services that are specified by the MCP consortium, such as a MSR or MMS, will always rely on a MIR for authentication. Importantly, also services specified elsewhere can do so. For example, a local AtoN information service, when itself registered with a MIR, can now require that its users authenticate with their MIR issued certificate, or with a token minted by a MIR.

One or more MIRs can establish a "hierarchy of trust", where a root MIR has registered subordinate MIR providers. A "root" MIR in turn may be endorsed by the MCP consortium. This way a vessel registered with a shipping company MIR which in turn is registered with an endorsed MIR in e.g. Korea, might be able to use (might be trusted by) an agent service registered with a port MIR which in turn is registered with a Finnish endorsed MIR. Likewise, that same vessel might trust a Finnish service that provides up-to-date AtoN information about a fairway into Helsinki, because that service can proof that is registered (possibly indirectly) with an endorsed MIR. See The MIR hierarchy of trust

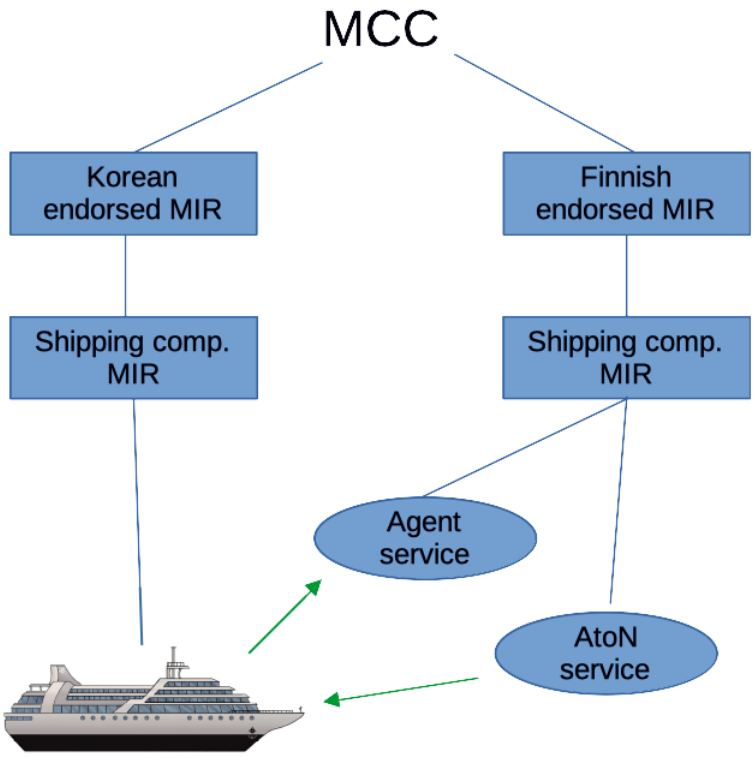

Figure 1: The MIR hierarchy of trust

The remainder of this document specifies what is required from a party that wishes to operate a MIR, MSR or MMS, such that the scenarios sketched out above are indeed possible.

2. DEFINITIONS

The *MCP consortium* (MCC) is the organization that authors the MCP specifications and endorses MIR services.

An *MRN* is a Maritime Resource Name.

An *MCP service* is one of: an MCP Maritime Identity Registry (MIR), an MCP Maritime Service Registry (MSR), or an MCP Maritime Messaging Service (MMS).

An *MCP service provider* is an organization that offers one or more MCP services.

A MIR can be *endorsed* by the MCC. This means that the MCC has deemed that the MIR service is operated according to the specifications and other requirements set forth in this document; and has issued an MRN to the MIR and signed the root certificate of the MIR.

A party is *registered* when it has been issued an MRN by a MIR that itself is registered.

A MCP service is deemed to be in *good status* if it is registered with a MIR that is currently in good status, or if it is currently endorsed by the MCC. Informatively, good status is achieved if the chain of trust is rooted in a currently endorsed MIR.

The key words *MUST*, *MUST NOT*, *REQUIRED*, *SHALL*, *SHALL NOT*, *SHOULD*, *SHOULD NOT*, *RECOMMENDED*, *MAY*, and *OPTIONAL* in this document are to be interpreted as described in RFC2119.

3. REQUIREMENTS FOR A MIR SERVICE

A MIR service assigns MRN's to maritime parties, and issues a X509 certificate to such parties, but only after appropriate vetting of each party.

This chapter describes the requirements a MIR service provider must meet, and processes it must adhere to, in order to operate a MIR service that can be registered with another MIR, or endorsed by the MCP consortium.

3.1. Compliance with MCP Specifications

A MIR service provider MUST ensure that each entity to which its MIR service assigns an MRN has been vetted according to the procedures specified in MCP Gen 5.

A MIR service MUST assign MRN's that are compliant with Chapter 4 of G1183 'Identity Management'. Before the MIR service is put into operation it MUST either register with a MIR in good status, or obtain endorsement from the MCC. This is to ensure that the IPID part of the MRN of the (new) MIR will be globally unique.

Digital certificates issued by a MIR service MUST be compliant with the requirements put forth in Chapter 5 of G1183 'Public Key Infrastructure'.

A MIR service provider MUST adhere to applicable data protection rules such as the EU General Data Protection Regulation (GDPR) and any other applicable laws.

3.2. Requirements for endorsement by the MCC

A MIR service provider that wishes for its MIR service to be endorsed:

- MUST have a public certificate practice document compliant with RFC3647.
- MUST follow the vetting procedures in MCP Gen 5, when enrolling organisations into their identity registry, and keep records of the results of applying vetting procedures for potential future assessment.

3.3. Physical operations

MCP identity service providers are encouraged to use renewable energy sources for their operations.

4. ENDORSEMENTS

Upon request the MCC secretariat, or a party appointed by the MCC secretariat, will assess the MCP service provider to verify compliance with the requirements of the relevant sections of this document. As part of this assessment the service provider will be subject to the vetting procedure specified in MCP Gen 5.

Having made this assessment, the secretariat makes a recommendation to the MCC board on whether or not to endorse the service, and the board makes the final decision on this.

Endorsed MCP services will be listed on the MCC web page, and root certificates of endorsed MIR services will be included in a list which will be digitally signed by one of the MCC host members.

4.1. Revocation of endorsement

When it is evident that an endorsed MCP service no longer complies with the requirements of this document the MCC board can revoke the endorsement of that service.

In case there is reasonable doubt that an endorsed MCP service no longer complies with the requirements of this document the MCC board may request the service provider for clarification and can ask the MCC secretariat to re-assess the service provider. Having made this assessment, the secretariat makes a recommendation to the MCC board on whether or not to revoke the endorsement of the service, and the board makes the final decision on this.

5. UPDATES OF SPECIFICATIONS

When new versions of the MCP specifications are approved and published by the MCC the MCC will publish a date by which MCP services are expected to have adopted the new version(s). The MCC may revoke the endorsement of services that are not compliant with the new versions by that date.

6. REFERENCES

MCP Gen 5: Vetting procedure for MCP instance providers, version 1.2.

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

RFC2119: Key words for use in RFCs to Indicate Requirement Levels. S. Bradner. The Internet Society, March 1997.

RFC3647: Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework. S. Chokani et al. The Internet Society, November 2003.