|  |
| --- |
| IALA Guideline |

G-XXXX

GUIDELINE ON platforms to support the implementation OF maritime services IN THE CONTEXT OF E-NAVIGATION

Edition 1.0

Date (of approval by Council)

Revisions to this IALA Document are to be noted in the table prior to the issue of a revised document.

|  |  |  |
| --- | --- | --- |
| Date | Page / Section Revised | Requirement for Revision |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. INTRODUCTION 4

1.1. SCOPE 4

1.2. BACKGROUND 4

2. REQUIREMENTS OF PLATFORMS FOR MARITIME SERVICES IN THE CONTEXT OF E-NAVIGATION 4

2.1. HARMONISED 4

2.2. INTEROPERABLE 4

2.3. EFFICIENCY, ROBUSTNESS AND RESILIENCE 5

2.4. CYBERSECURITY 5

2.5. GOVERNANCE 6

2.6. MANAGEMENT OF SERVICE SPECIFICATION 6

2.7. APPLICATION PROGRAMMING INTERFACE 6

3. MARITIME CONNECTIVITY PLATFORM (MCP) – A CANDIDATE 6

3.1. WHAT IS THE MCP 6

3.1.1. web service based communications 7

3.1.2. The Maritime Identity Registry 7

3.1.3. the maritime service registry 7

3.1.4. the maritime messaging service 7

3.2. THE MARITIME CONNECTIVITY PLATFORM CONSORTIUM (MCC) 8

4. SUITABILITY OF MCP 8

5. ACRONYMS 9

# INTRODUCTION

## SCOPE

This guideline provides information on the establishment of harmonised platforms to support the implementation of VTS and AtoN maritime services in the context of e-navigation.

The platforms aim to enable efficient, secure, reliable and seamless electronic information exchange between all authorised maritime stakeholders using all available means of communications.

Although the initial focus is to enable VTS and AtoN services, the aim is to expand these platforms to accommodate all maritime services in the context of e-navigation.

This is one of several guidelines associated with Recommendation R-XXXX (on the Provision of Digital VTS and AtoN Maritime Services in the context of e-Navigation).

## BACKGROUND

Digitalisation in the maritime domain is advancing rapidly. The shipping industry is witness to increasing levels of digitisation and automation on board and ashore, growing electronic exchange of information and the advent of digital maritime services. These trends will lead to:

* The need for increased and improved connectivity
* Increased safety and efficiency of shipping and enhanced environmental protection.

# REQUIREMENTS OF PLATFORMS FOR MARITIME SERVICES IN THE CONTEXT OF E-NAVIGATION

Platforms for maritime services, must, as a minimum have the following features:

1. Authenticity
2. Mechanisms to verify trustworthy peers
3. Confidentiality, integrity and availability
4. Interoperability
5. Be based on sound governance principles

Additionally, platforms should also facilitate:

1. Service discoverability
2. IP-based communications
3. Web services
4. Robust, efficient and seamless connectivity

The above elements are explained in more detail below.

## HARMONISED

Broadly, harmonised means minimising redundant or conflicting standards or solutions. It also means that platforms need to operate the same fundamental principles (i.e. service oriented architecture and IP based).

## INTEROPERABLE

Interoperable means:

1. The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged[[1]](#footnote-1).
2. Orchestrate services to enable them to operate together effectively.
3. Compatible with other systems and services in platforms.
4. Ability for seamless information exchange across different systems.
5. Vendor agnostic.

## EFFICIENCY, ROBUSTNESS AND RESILIENCE

Efficiency[[2]](#footnote-2) represents the performance relative to the amount of resources used under stated conditions.

Robustness[[3]](#footnote-3) means the ability to cope with errors and function in less than optimum conditions. It also means the ability to reliably deliver information via unreliable physical communication channels.

Resilience[[4]](#footnote-4) is the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operations.

## CYBERSECURITY

Cybersecurity is the practice of protecting systems, networks and programs from digital attacks.[[5]](#footnote-5) The main attributes of cybersecurity are confidentiality, integrity and availability.

**Confidentiality** means the definition an enforcement of appropriate access levels of information.[[6]](#footnote-6) This includes the management of identities and their access rights and as an execution of the access control: the encryption of confidential data.

**Integrity** means the protection of data against modification or deletion by unauthorized parties.6

**Availability** means that all accessible parts of a system must be protected in such a way that the provision of information is working properly at any time. 6

Platforms need to have mechanisms for the identification and authentication of users, devices, objects and services. Additionally, there must also be mechanisms to inform involved parties about abuse of registered identities and stop entities from communicating with these.

Also, platforms should make use established, publicly available security standards and protocols such as X.509, OAuth 2.0, TLS as well as encryption techniques such as ECDSA or RSA as these promote interoperability and have already been exposed to public penetration testing for longer periods.

Traceability means

Guidance / standards (references to be provided)

## GOVERNANCE

Sound governance means adherence to the following principles:

1. Vendor agnostic
2. Non political
3. Not-for-profit
4. Open and transparent decision-making

A core responsibility of the governing body is to ensure a chain of trust among the entities registered on the platform (Rasmus will explain).

## MANAGEMENT OF SERVICE SPECIFICATION

The platforms need to provide a service registry with the following functionality:

1. Register and retrieve specification of services (described in accordance with IALA Guideline G1128).
2. Ability to register artefacts described in G1128 (service specification, service design and service instance).
3. Ability to search a service registry using various criteria, such as key words, organisations and geographical coverage of service instances.

These functional requirements enable the unbiased selection of maritime service offers for service consumers. If services are described in a standardised way (with G1128), a service consumer with a need for a special service can query a service registry with its search criteria, obtain a list of available services, automatically select a service and contact a specific service instance. This automates the process of service setup and configuration and provides a centralized and standardised way of querying for maritime services. Service providers can use these functionalities to promote their services and make them available to a larger set of consumers.

## APPLICATION PROGRAMMING INTERFACE

An Application Programming Interface or API specifies how software components should interact. An API is the messenger that delivers your request to the provider from whom you are requesting a service. It can also be thought of as a user interface for machines (rather than humans).

It is important that the APIs of platforms are standardised.

APIs are used interchangeably with web services[[7]](#footnote-7). The difference is that a web service facilitates interaction between two machines over a network. An API acts as an interface between two different applications so that they can communicate with each other.

# MARITIME CONNECTIVITY PLATFORM (MCP) – A CANDIDATE

## WHAT IS THE MCP

The Maritime Connectivity Platform (MCP – [www.maritimeconnectivity.net](http://www.maritimeconnectivity.net)) is a communication framework enabling efficient, secure, reliable and seamless electronic information exchange between all authorized maritime stakeholders across available communication systems. The MCP supports digitalization across a wide maritime domain because it is an open-source solution that relies on the Internet concept of Web Services for identity management and service management and, as such, can support Maritime Services in the context of e-navigation. The MCP is vendor neutral and brings common internet standards to maritime navigation and transportation systems. Its platform structure enables easy and secure access to its users and supports machine-to-machine communication via a public and standardised API. The existence of multiple MCP instances operated by independent parties is part of the concept. Interoperability of Maritime Services in a Service-oriented architecture and the MCP instances is ensured by the standardisation of the MCP components by the MCP consortium.

The MCP comprises the following components:

### web service based communications

One of the core intentions of the MCP is to support secure and efficient Web Service based communication for Maritime Services. Web Services are services based on IP-communication, mainly HTTP(S). Especially in the maritime industry IP communication is opening opportunities for applying more standards to the communication and getting away from proprietary technologies. With the new developments in IP-providing services communication with an exhaustive availability (satellite) or with a very high bandwidth (LTE), a new generation of Maritime Services is coming. IP-based communication also enables to employ the standard security protocols built on top of IP and the layers above it (such as TCP) and therefore leads to a better abstraction from low-level communication channels. The MCP provides an infrastructure for the deployment of secure, interoperable Web Services and aims at the integration of existing standards for the exchange of maritime data such as S-100 datasets.

### The Maritime Identity Registry

The MIR is responsible for identity management and providing security functionality to the entities of the MCP. In particular, the MIR provides the following functionality:

* Firstly, Identity Management: The MIR enables that each maritime entity (such as a device, human, organization, service, or ship) can be registered as an entity of the MCP and be equipped with a unique identity (by assigning a Maritime Resource Name (MRN)).
* Secondly, Public Key Infrastructure (PKI): The MIR ensures that each MCP entity holds a corresponding cryptographic identity, i.e. a public/private key pair and a certificate with the public key bound to their identity.
* Thirdly, the MIR provides the infrastructure for authentication, which enables authorization and secure integration of web services, based on the established internet standards (OAUTH 2.0/OpenID Connect).

While the MIR will be distributed trustworthiness will be made transparent by the definition of MCP security profiles and the audited procedures MSP instance providers need to follow to adhere to them.

### the maritime service registry

The MSR does not provide actual maritime information but a specification of various services, the information that they carry, and the technical means to obtain it. An MSR instance contains service specifications according to a Service Specification Standard (which is identical to IALA Guideline 1128) and provisioned service instances implemented according to these service specifications.

The functionality of the MSR is twofold: service discovery and service management. It enables service providers to register their services in the MCP and allows an end-user to discover those services. Services and service instances can be searched via different criteria such as keywords, organizations, locations, or combinations, and more. The management of a service encapsulates the functions to publish a service specification and register / publish a service instance.

### the maritime messaging service

The MMS is a messaging service intended to offer transparent seamless information transfer across different communication links in a carrier agnostic and geolocation-context sensitive manner.

The MMS primarily addresses ship-shore communication based on internet connectivity, yet any number of alternative communication services may be connected to and utilized by the MMS via dedicated gateways. As an example, a message, sent by one specific ship using INMARSAT access to the MMS, may be received via a VSAT terminal on another ship, an HF data connection on yet another ship, or a VTS operator on a DSL landline internet connection. In the current implementation the MMS enables the transfer by using the MRN of an entity as an end-point address.

Each communication service will impose technology and situation specific limitations in terms of restrictions to capabilities, bandwidth availability, size of transferrable data packages, latencies, etc. – but basic transfer of text or structured data (e.g. using XML) will be possible.

The Maritime Identity Registry facilitates authenticity, integrity and confidentiality, and the Maritime Service Registry together with the Maritime Messaging Service facilitates efficient and robust connectivity. Therefore, the MCP is a potential solution that addresses the above stated compelling need. For further considerations on the suitability of the MCP see section 4.

## THE MARITIME CONNECTIVITY PLATFORM CONSORTIUM (MCC)



Figure 1The Maritime Connectivity platform Consortium

The MCP is governed by the MCP consortium (MCC). The consortium was setup in the beginning of 2019 with a structure inspired by the world wide web consortium (W3C). As such, the “founding fathers” of the consortium are all non-profit organisations named “host” organisations. These hosts populate the board – which is the central coordinating body of the consortium. Other organisations (including commercial – for profit -organisations) may become regular members. Host organisations together with regular members comprise the general assembly of the consortium. This is the highest decision body of the consortium, where all members can vote, but hosts have the possibility of vetoing decisions. This is because the hosts are expected to safeguard the original vision of the MCP within the consortium. In addition to the board and the general assembly, the consortium has a number of working groups undertaking the activities of the consortium and an advisory board for relevant international organisations.

The MCC takes the following responsibilities:

Developing and maintaining all standards (SOP’s, API’s, PKI structure etc.) relating to the MCP

Developing and maintaining reference source code for the MCP

Running instances of the MCP for testing purposes and a public demonstration instance

Defines criteria’s for running operational MCP instances

Endorses organisations running operational MCP instances

It is important to note, that the consortium itself is not a legal body, and have no resources on its own. Thus, all activities are carried out by consortium members on behalf of the consortium.

# SUITABILITY OF MCP

The following section examines how the MCP meets the requirements defined in section 2.

|  |  |
| --- | --- |
| **Criteria** | **Suitability of MCP** |
| Authenticity | The available instances of the MCP are known to the MCC and must fulfil several requirements (profiles) to operate in an authentic, MCC approved manner. |
| Mechanisms to verify trustworthy peers | The MCP offers a Public Key Infrastructure which is closely integrated into the Maritime Identity Registry. These functionalities, in combination with the service registry can be used to verify trustworthy peers in a common, standardised way. |
| Confidentiality, integrity and availability | The MCP supports common standards and protocols for authorization (OAuth, X.509 Certificates) and offers the Maritime Identity Registry as a central component for the management of identities. Cryptographic keys that are bound to MIR identities can be used for the protection of data. The service registry permanently supervises the availability of maritime services. |
| Interoperability | The MCP is interoperable by design: MCP registered services need to be specified in the standardised G1128 format and can therefore be subdivided into specifications, technical designs and instances. Different instances of the MCP are also interoperable regarding identities, messaging and service registration. |
| Be based on sound governance principles | The MCP is governed by the non-political, vendor agnostic, not-for-profit and transparent MCP Consortium (see section 2.5) consisting of several members from the fields of maritime industry, research and governmental observers. |
| Service discoverability | Service discoverability is one of the core functionalities of the MCP. It is realized by the Maritime Service Registry. |
| IP-based communications | The MCP enhances IP-based communication with common technologies and is also mainly based on this technology. |
| Web services | The MCP fully supports Web Services. |
| Robust, efficient and seamless connectivity | The MCP is constantly being developed by the MCC and its contributors. An operational MCP instance is required to provide at least two MCP environments for testing and production. Further regulations on downtime, technical requirements, security standards and support must be fulfilled to be recognized as an official instance. |
| Presence of APIs | The MCP uses publicly available, open-source APIs for any type of machine-to-machine interaction. |
| Compatibility with G1128 | The MCP is fully compatible with G1128 service specifications. |

# ACRONYMS

MCP – Maritime Connectivity Platform

MCC – Maritime Connectivity (Platform) Consortium

MIR – Maritime Identity Registry

MSR – Maritime Service Registry

MMS – Maritime Messaging Service

G1128 – IALA Guideline G1128 – The Specification of e-Navigation Technical Services

IP – Internet Protocol

API – Application Programming Interface

X.509 – X.509 is a standard for PKI for the creation of digital certificates.

OAuth – OAuth is a standard protocol for authorization.

TLS – Transport Layer Security

ECDSA – Elliptic Curve Digital Signature Algorithm

RSA – RSA is a public-key cryptosystem.

MRN – Maritime Resource Name

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. ITU Rec.Y.101 [↑](#footnote-ref-1)
2. ISO 25010 [↑](#footnote-ref-2)
3. ISO 22300-2018 [↑](#footnote-ref-3)
4. ISO 22300-2018 [↑](#footnote-ref-4)
5. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html [↑](#footnote-ref-5)
6. The CIA Triad , Chad Perrin, <https://www.techrepublic.com/blog/it-security/the-cia-triad/>, 12.02.2020 [↑](#footnote-ref-6)
7. https://medium.com/@programmerasi/difference-between-api-and-web-service-73c873573c9d [↑](#footnote-ref-7)