|  |
| --- |
| 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 5

2.3. EFFICIENCY, ROBUSTNESS AND RESILIENCE 5

2.4. CYBERSECURITY 5

2.5. GOVERNANCE 5

2.6. MANAGEMENT OF SERVICE SPECIFICATION 6

2.7. APPLICATION PROGRAMMING INTERFACE 6

3. MARITIME CONNECTIVITY PLATFORM (MCP) – A CANDIDATE (MCP CONSORTIUM will provide text before ENAV 25) 6

3.1. WHAT IS THE MCP 6

3.1.1. web service based communications 6

3.1.2. The Maritime Identity Registry 6

3.1.3. the maritime service registry 7

3.1.4. the maritime messaging service 7

3.2. THE MARITIME CONNECTIVITY PLATFORM CONSORTIUM (MCC) 7

4. SUITABILITY OF MCP 7

5. ACRONYMS 7

# 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. Trust between all entities
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 to provide services to and accept services from other systems[[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.

Platforms need to have mechanisms for the identification and authentication of users, devices, objects and services.

Confidentiality means (something here about identity management and encryption)

Integrity means

Availability means

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 the service registry using various criteria, such as key words, organisations and geographical coverage of service instances.

*Need to explain in more words to explain why we have the functional requirements – e.g. a ship moving around, which provider to get info from.*

## 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[[6]](#footnote-6). 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 (MCP CONSORTIUM will provide text before ENAV 25)

## WHAT IS THE MCP

The Maritime Connectivity Platform (MCP) is a communication framework enabling efficient, secure, reliable and seamless electronic information exchange between all authorized maritime stakeholders across available communication systems.

The MCP is an open source, vendor neutral technology in the digital maritime domain. It brings common internet standards to maritime navigation and transportation systems. It comprises the following components:

### web service based communications

Text

### The Maritime Identity Registry

For secure and reliable identity information, it provides a single login to all services, using identity information provided by trusted stakeholders.

### the maritime service registry

For registering, discovering and using all relevant e-Navigation and e-Maritime services, commercial and non-commercial, authorised and non-authorised, for free and against payment. It can be seen as a sophisticated yellow pages phone book or the equivalent of an App Store.

### the maritime messaging service

Maritime Messaging Service is a messaging component that allows authorized maritime stakeholders to send and receive message in an efficient, reliable and seamless manner within the MCP to solve the problems of the current maritime wireless data communication system.

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.

## THE MARITIME CONNECTIVITY PLATFORM CONSORTIUM (MCC)

The MCP is governed by the MCP consortium (MCC).

The MCC governs the standards relating to MCP, including the MCP source code. The MCC operates a testbed for MCP (done by a member on behalf of the consortium), but does not operate an operational instance of the MCP. Rather, the MCC authorises other organisations to run operational instances of the MCP.

The definitions of terms used in this Guideline can be found in the International Dictionary of Marine Aids to Navigation (IALA Dictionary) at http://www.iala-aism.org/wiki/dictionary and were checked as correct at the time of going to print. Where conflict arises, the IALA Dictionary should be considered as the authoritative source of definitions used in IALA documents.

# SUITABILITY OF MCP

How the MCP meets the requirements of Section 2

|  |  |
| --- | --- |
| **Criteria** | **Suitability of MCP** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# ACRONYMS

Kjg

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

1. ITU definition – add detail [↑](#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. https://medium.com/@programmerasi/difference-between-api-and-web-service-73c873573c9d [↑](#footnote-ref-6)