IALA

IALA GUIDELINE

G1161
EVALUATION OF PLATFORMS FOR THE PROVISION OF MARITIME SERVICES IN THE CONTEXT OF E-NAVIGATION

Edition 1.1

June 2021

urn:mrn:iala:pub:g1161:ed1.1

DOCUMENT REVISION

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

Date	Details	Approval
June 2021	First Issue	Council 73
July 2022	Editorial corrections	

CONTENTS

List of Figures

1. INTRODUCTION

This Guideline provides information for the evaluation of harmonized and suitable platforms for the provision of Marine Aids to Navigation (AtoN) services including VTS in the context of e-Navigation as recommended by Recommendation *R1019 Provision of Maritime Services in the Context of e_Navigation in the Domain of IALA*. For this purpose, regional, national and global platforms have to be considered. Of course, such platforms may be operated by national members themselves or be provided by industry.

Maritime Services and e-Navigation information are currently provided using a variety of legacy platforms. Navigational warnings and Maritime Safety Information in general, recommended routes, pilot routes, chart updates, weather routing, METOC data and other services are offered through websites maintained by regional and national authorities. They are also sometimes offered with Application Specific Messages (ASM) over the AIS network as well as by technology providers through proprietary network solutions. These legacy platforms have provided and continue to provide great value to all stakeholders. It is recognized however, that these legacy platforms have significant drawbacks in today's digital environment, e.g., most lack basic security capabilities. It is foreseen that these legacy platforms will continue to be useful for a number of years to come, but the maritime industry should start planning for the next generation of e-Navigation platforms that will offer a much more complete digital solution that will be harmonized and secured. In order to either develop a platform or select a suitable existing platform, specific requirements must be identified and defined.

This document concentrates on the required criteria for these next generation platforms which support the provision of Maritime Services in the context of e-Navigation and presents an overview of relevant requirements that should be considered for the distribution of maritime services. For the remainder of this document, the word "platform" will be used specifically in reference to these next generation platforms.

1.1. SCOPE

A platform is a system that facilitates the secure and reliable exchange of information and services between stakeholders. Platforms may have various security and reliability levels depending on their design implementation and users. Interoperability between all platform participants can be achieved through standardized data formats and access methods. A distributed ecosystem of Maritime Services and providers, as opposed to a centralized system, is foreseen in the maritime domain due to the international and decentralized nature of shipping. Although the focus is to enable VTS and AtoN services in the context of e-Navigation, it is the vision that these platforms may accommodate all Maritime Services in the context of e-Navigation and beyond (e-maritime, autonomous ships, etc).

As one of several guidelines associated with Recommendation *R1019 Provision of Maritime Services in the context of e-Navigation in the domain of IALA*, this document describes how the following recommendations in *R1019* can be met in order to:

- Ensure that a communications infrastructure to provide such digital maritime services is available in their area of responsibility.

- Ensure harmonization and interoperability by considering international standards and guidance for:

  a   Digital maritime services.

  b   The communications infrastructure.

  c   System design and cybersecurity (e.g., availability, integrity and confidentiality).

- Ensure their services are developed and harmonized with other and authenticated maritime services that are the responsibility of other domain coordinating bodies.

It is the intention that these platforms, together with various communication channels, will comprise the communication infrastructure mentioned above.

1.2.   BACKGROUND

As in other domains, digitalization advances rapidly in the maritime domain. The shipping industry is witness to increasing levels of digitization and automation onboard and ashore, growing electronic exchange of information and the advent of digital maritime services. These trends will lead to:

  a.   The need for increased and improved connectivity (onboard and ashore).

  b.   Approaches to exchange relevant information securely and in a timely manner despite volatile connectivity.

  c.   Increased safety and efficiency of shipping and enhanced environmental protection.

  d.   New maritime services using the opportunities of digitalization.

  e.   A global intention to exchange services and information with other stakeholders.

1.3.   AN EXAMPLE – THE PROVISION OF NAVIGATIONAL WARNINGS

In the case of navigational warnings, one way of providing this is through NAVTEX (other ways include satellite-based technologies). Here, providers of the information have an infrastructure with radio equipment and antennas enabling the transmission of this information on the frequency allocated to this purpose. On the receiver side, the user purchases a NAVTEX receiver, enabling the reception of this information on that specific frequency.

Finding the navigational warning information, therefore, is simply a matter of listening to the right frequency. The authenticity (proof of identity) of the information provider is to some extent given by the fact that the provider has the equipment which is able to transmit the signal, although some rogue entity in principle, could have the same equipment and transmit malicious information for some devious purpose. Strictly speaking, the information provider is not authenticated, the identity of the information provider is not proven and the integrity of the information provided is not guaranteed (i.e., it is not guaranteed that the information has not been tampered with).

Using contemporary technology a provider would expose a service on the internet and the service consumer would connect to that service and receive the data, i.e., the navigational warnings. This, of course, requires that the recipient is connected to the internet, which is not a given fact for all vessels at all times.

Having the provider of navigational warnings deliver the information over the internet means that the provider needs to be authenticated e.g. via a certificate from a trusted authority. On the internet, anyone can provide anything from anywhere very easily, requiring nothing more than a connected computer or smartphone. Therefore, authentication becomes essential.

In addition, it is very difficult to find the correct information from authenticated providers on the internet - it is not just a matter of tuning into a specific frequency and thus, service discoverability becomes an issue. Users or vessels will need to connect to different providers depending on where they are in the world and as they will require navigational warnings, and other relevant information, only for those areas. Transmitting the information using NAVTEX gives a kind of regional relevance because the NAVTEX transmitters have limited coverage, but on the internet, information is available from anywhere in the world.

This example illustrates that although NAVTEX is a legacy platform, which is harmonized worldwide, additional features, such as service discovery and encryption will be beneficial to all next generation platforms.

2. CRITERIA REGARDING PLATFORMS FOR THE PROVISION OF MARITIME SERVICES

Criteria to consider when evaluating platforms:

a. Authentication and authorization (cf. section 2.1).

b. Service specification management features (cf. section 2.2).

c. Efficiency, robustness and resilience (cf. section 2.3).

d. Cybersecurity (cf. section 2.4).

By realizing the raised criteria, secure and trustworthy communication can be assured during the exchange of services. Additionally, the use of current technological trends within the platform should simplify and enable the development of modern maritime services. The defined criteria are explained in more detail below.

2.1. AUTHENTICATION AND AUTHORIZATION

2.1.1. AUTHENTICATION

Authentication is a process in which the identity of a user (human or machine) is verified (i.e., to confirm whether you are who you claim to be, like a passport). This corresponds to the written signature and official stamp on paper. In accessing various Maritime Services, authenticity is vital for establishing a trustworthy communication. As such, a platform is committed to facilitate means of identification and functionality for the management of identities.

2.1.2. AUTHORIZATION

In managing identities, authorization is also important. Authorization is the process of determining a set of permissions that is granted to a specific trusted identity. Platform support for authorization may be required if there is a need to limit access to certain sensitive information or restricted services.

2.2. SERVICE SPECIFICATION MANAGEMENT FEATURES

2.2.1. SERVICE DISCOVERABILITY

Service discoverability is another possible feature of a platform, to enable searching for relevant services in a catalogue of published services. Since efficient service discovery is most likely handled by machine to machine communication, service descriptions are required to be standardized and machine readable. The IALA Guideline *G1128 The Specification of e-Navigation Technical Services*, describes such a format. Furthermore, the quality of published services can be evaluated in using a common description as *G1128* specifies.

The platforms may provide a service registry with the following functionality:

a. Register and retrieve specification of services (described in accordance with IALA Guideline *G1128*).

b. Ability to register artefacts described in *G1128* (service specification, service design and service instance).

c. Ability to search a service registry using various criteria, such as key words, organizations and geographical coverage of service instances.

d. Ability to endorse services according to agreed levels of quality and importance.

These functional requirements enable the unbiased selection of maritime service offers for service consumers. If services are described in a standardized 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 standardized 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.

2.3. EFFICIENCY, ROBUSTNESS AND RESILIENCE

Efficiency[1] represents the performance relative to the amount of resources used under stated conditions.

Robustness[2] means the ability to cope with errors, and to function in less than optimum conditions, like the volatile connectivity at sea. It also means the ability to reliably deliver information via unreliable physical communication channels.

Resilience[3] is the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operations.

A common baseline to evaluate platforms regarding efficiency, robustness and resilience should be established so that stakeholders can find a combination of solutions that meet their requirements and expected service level.

2.4. CYBERSECURITY

Cybersecurity is the practice of protecting systems, networks and programs from digital attacks.[4] In general, there are many aspects of cybersecurity, and there are existing guidelines on cybersecurity within the maritime domain from organizations like IMO, CIRM and BIMCO. However, certain elements of cybersecurity need to be handled by platforms such as those discussed in this document. This pertains to confidentiality, integrity and availability.

2.4.1. CONFIDENTIALITY

Confidentiality means the definition and enforcement of appropriate access levels of information.[5] This includes the management of identities and their access rights and as an execution of the access control: the encryption of confidential data. Confidentiality ensures that no one else than the intended recipient can read and understand the content of the document. Confidentiality corresponds to the sealed envelope.

2.4.2. INTEGRITY

Integrity means the protection of data against modification or deletion by unauthorized parties. Integrity corresponds to the difficulties in changing printed text on paper.[6]

2.4.3. AVAILABILITY

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]

2.4.4. NON-REPUDIATION

Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data.[6]

---

1   ISO 25010

2   ISO 22300-2018

3   ISO 22300-2018

4   https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

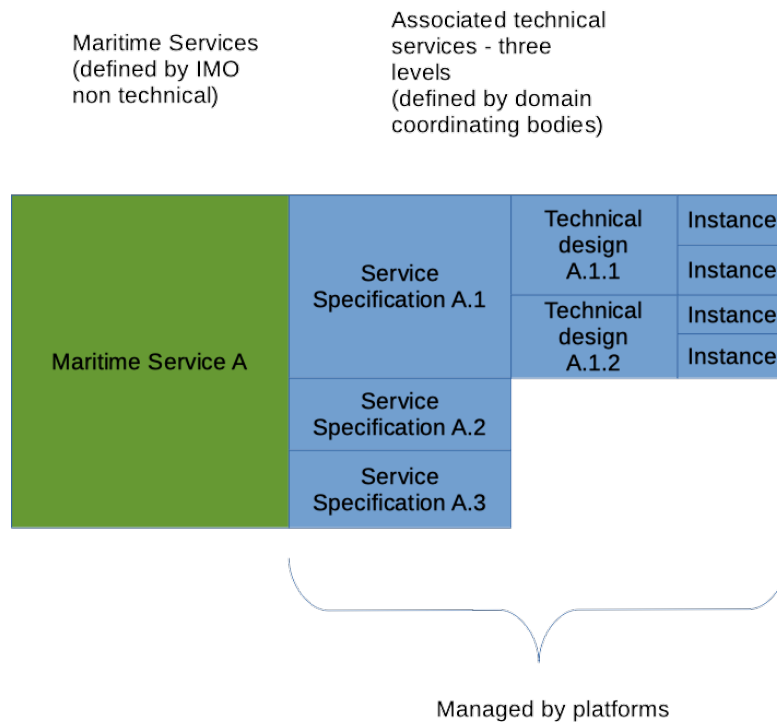5   The CIA Triad, Chad Perrin, https://www.techrepublic.com/blog/it-security/the-cia-triad/, 12.02.2020

6   FAQ Cryptomathic, https://www.cryptomathic.com/products/authentication-signing/digital-signatures-faqs/what-is-non-repudiation

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

Furthermore, it is also possible that the platform facilitates traceability for non-repudiation purposes when transferring messages between services. This is important for messages which might have a significant impact on legal liability. For instance, protection against a ship's false denial of having created the route content and of having sent the route to a provider of route optimization services. Although the platform can facilitate this, it is solely the choice of the service provider and service consumer whether to implement such functionality or not. The platform should not impose such requirements by introducing centralized functions for traceability. 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.

3. PLATFORMS IN THE CONTEXT OF E-NAVIGATION

Platforms need to handle technical e-Navigation services following IALA Guideline *G1128*. These services are specified on three levels (service specification, service technical design and service instance) and the platforms may need to handle the service descriptions on these independent levels.

The Maritime Services and the service specifications (two first columns) are technology agnostic. The Service specifications defines the data model - usually by reference to an S-100 product specification. The technical designs describe how the service is implemented using a specific technology.

Figure 1   *Relationship of services on various levels*

IMO resolution *MSC.467(101) Guidance on the definition and harmonization of the format and structure of maritime services in the context of e-Navigation* defines services in the context of e-Navigation. This resolution defines four levels of services: Maritime Services (in the context of e-Navigation) and technical services, with the technical services having three levels corresponding to the three levels described in *G1128* (Figure 2 and 3 in *G1128*). Thus, the platforms may manage the three levels of the technical services defined in the IMO resolution.

4.   POTENTIAL BENEFITS OF STANDARDIZATION

As explained in the previous sections, it will be of importance to utilize platforms that provide certain features such as authentication and service discoverability when implementing technical e-Navigation services. However, such features could be implemented in multiple ways and undoubtably would. Thus, we will have various techniques to achieve the various features mentioned. This will mean that providers and consumers of otherwise harmonized services will still have to implement different techniques to achieve, for instance, authentication to service providers and possibly service consumers (if required).

It would be advantageous to standardize features in the same way as the technical services themselves are standardized like the work in progress in the *IEC 63173-2 SECOM*. This would include standardized interfaces to platforms that would enable:

- Authentication, authorization, encryption, integrity
- Service discoverability like it is defined in *S-100* (global i.e., the ability to lookup all standardized e-Navigation services from all providers in all regions of the world)
- Service management (registration, endorsement etc.)

Once this has been achieved, all service providers and consumers would only have to implement the mentioned features once. This would introduce the same benefits as introduced by standardization of the individual services, but on another level.

Introducing standardization on this level would obviously be a great benefit, but would also require a new level of governance to develop and maintain the necessary standards.

Analogous to the criteria from section 2, the following criteria must be considered for realizing standardized platforms:

a.   Harmonization and interoperability (cf. section 4.1).

b.   Open and standardized interfaces (API's) (cf. section 4.2).

c.   Governance (cf. section 4.3).

Each of these criteria is further defined in the following subsections. Instead of having an arbitrary number of standardized platforms that cannot communicate with each other, the same could be achieved by a decentralized interoperable platform architecture as explained in section 4.4

4.1.   HARMONIZATION AND INTEROPERABILITY

Having harmonized platforms using standards is the only way to ensure that interoperability is achieved. Interoperability in the context of shipping is quite unique in the sense that a ship might call an arbitrary port and still expect to be served with the same level of service as calling a scheduled port. This puts special requirements on interoperability, so that there needs to be mechanisms in place to handle episodic tight coupling between maritime actors.

Interoperability achieved through harmonization and using standards in the context of platforms means:

a. The ability of two or more platforms or applications to exchange information and to mutually use the information that has been exchanged[7].

b. Orchestrated services to enable them to operate together efficiently.

c. Compatibility with other platforms and services in platforms.

d. Ability for seamless information exchange between users of different platforms provided that the users trust those platforms.

e. Vendor agnostic.

To achieve interoperability, the independent platforms must be harmonized with each other by using standards. Harmonized means minimizing redundant or conflicting standards or solutions. It also means that platforms need to operate the same fundamental principles (e.g., service-oriented architecture and IP based). Harmonization is a key aspect in supporting inter platform communication since there will not be one single platform implementing Maritime Services, rather a variety of different platforms possibly specialized in various areas of the maritime industry. So, in requiring harmonization there need to be clear and precise standards defined for inter-platform services like authentication, service discovery and synchronization of entities.

4.2.   OPEN AND STANDARDIZED INTERFACES (APIs)

Platforms must use open and standardized interfaces. Application Programming Interfaces (APIs) and web services are examples of such interfaces.

An 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 standardized to facilitate interoperability.

APIs are often used interchangeably with web services[8]. 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. In other words, a web service is only one type of API.

An API also decouples the actual application from the outside world thus wrapping the functionality of the application which can facilitate changes in the application without affecting information exchange across different systems.

4.3.   GOVERNANCE

Governance of a platform relates to establishing rules, norms and standards that will be used by that platform. Sound governance may mean enforcing adherence to the following principles in the usage of the platform, by all stakeholders:

a. Vendor agnostic, standard based interfaces.

b. Internationally defined standards and formats to exchange information.

c. Not-for-profit or freely available access to the platform.

d. Open and transparent decision-making.

The rationales for the above statements are summarized below:

---

7   ITU Rec.Y.101

8   https://medium.com/@programmerasi/difference-between-api-and-web-service-73c873573c9d

- A platform should strive to provide standard interfaces that offer vendor interoperability to promote market competitiveness in the devices and tools required to access the platform, e.g., any AIS transceiver, from any manufacturer, should allow you to receive ASM messages.

- Furthermore, in order to gain global recognition, the governing body should strive to use internationally defined standards and formats for the exchange of information on the platform.

- A core responsibility of the governing body is to ensure a chain of trust among the entities registered on the platform. This implies that the governing body ensures that all identities are validated to the same level of assurance. Thus, there is a unified trust in all identities in the platform.

4.4. PLATFORMS VS. PLATFORM – THE NEED FOR A DECENTRALIZATION

Due to the global characteristics of the maritime domain, it is necessary to achieve nearly global coverage with the offered services. So that safety-critical services can be obtained at any time from anywhere in the world. Security-critical services are pointless if they can only be used in certain places on earth on global routes.

To achieve this, a decentralized platform architecture is essential. Only in this way each authority does have the option of setting up its own platform instance with individual regulations e.g., to comply with national legal requirements. Additionally, each instance provider gets the opportunity to trust only certain authorities and organizations. While the concept of a single central platform is less complex and easier to implement, a centralized solution is not likely to be trusted by everyone globally. Therefore, there need to be several platforms (or instances of the same platform) so that each stakeholder can on a case by case basis chose which platform should be used. This can increase the trust and acceptance for the platform so that as many stakeholders as possible can also benefit from the offered services.

However, the decentralized architecture of the platforms makes it even more important to harmonize them with each other so that they can be exchanged by stakeholders seamlessly e.g., when entering other sea areas. The platform instances required to support the maritime services need to be harmonized and interoperable as described in section 4.1 This level of harmonization and interoperability needs to be absolutely perfect such that the platforms must outwardly behave identically and interface identically (cf. 4.2). This is because users (and machines) should be able to use these platforms interchangeably. For instance, an ECDIS on a vessel should be able to authenticate to a service using any platform it trusts without the software on the ECDIS needing to be changed in any way.

5. ACRONYMS

API	Application Programming Interface
ASM	Application Specific Message
ECDSA	Elliptic Curve Digital Signature Algorithm
G1128	IALA Guideline G1128 – The Specification of e-Navigation Technical Services
IP	Internet Protocol
OAuth	OAuth is a standard protocol for authorization.
PKI	Public Key Infrastructure
RSA	RSA is a public-key cryptosystem.
TLS	Transport Layer Security
X.509	X.509 is a standard for PKI for the creation of digital certificates.

APPENDIX 1   EXAMPLES OF PLATFORMS – MARITIME CONNECTIVITY PLATFORM

The Maritime Connectivity Platform (MCP – www.maritimeconnectivity.net) is concept of a communication framework enabling efficient, secure, reliable and seamless electronic information exchange between all authorized maritime stakeholders across available communication systems. It is presented here solely for the purpose of illustration how a mature platform fulfils the above mentioned requirements. This is therefore only an example of a current candidate for consideration.

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 standardized 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 standardization of the MCP components by the MCP consortium.

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 moving 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 approaching. IP-based communication also enables employment of 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 is defined by a set of standard specifications. Independent implementations of these standards provide 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 MCP consists of specifications for three basic components - the "Maritime Identity Registry", the "Maritime Service Registry" and the "Maritime Message Service" (cf. Figure 2) which can be used as parts of an e-Navigation platform.
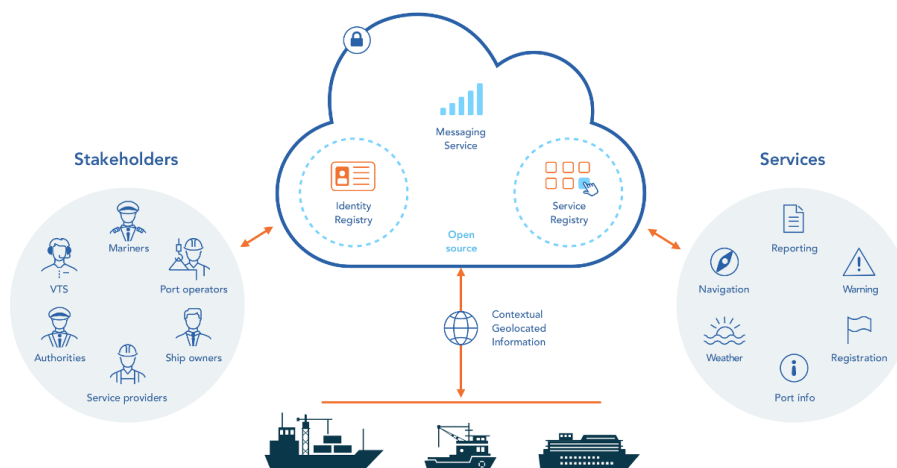

Figure 2   *Figure 1 MCP Components for setting up a platform for the provision of maritime services in the context of e-Navigation*

Further information can be retrieved from https://maritimeconnectivity.net/.