Input paper: [[1]](#footnote-1) ENAV22-8.2.8

Input paper for the following Committee(s): check as appropriate Purpose of paper:

**□** ARM **□** ENG **□** PAP **□** Input

**x** ENAV **□** VTS **x** Information

Agenda item [[2]](#footnote-2) (from agenda) 8

Workplan Task Number / Technical Domain 2 1.2

Working Group TBD

Author(s) / Submitter(s) OFFIS

Ensuring Authenticity and Integrity of e-Navigation Service Descriptions

# Summary

Hostile attacks to the Maritime Connectivity Platform can end up in manipulated service descriptions and manipulated service instance descriptions. Currently there are no measures implemented, which ensure authenticity and integrity of service (instance) descriptions registered with the Maritime Service Registry. The service specification should be enhanced to allow inclusion of digital signatures.

* 1. **Purpose of the document**

This document motivates the need for authenticity and integrity checking of technical e-Navigation Services based on IALA Guideline 1128. Ensuring authenticity and integrity is the basis for the establishment of trust within the involved actors such as service provider and service consumer.

* 1. **Related documents**
* IALA Guideline 1128 For Specification Of Technical e-Navigation Services
* The Guidelines on Cyber Security Onboard Ships

# Background

The establishment and the raising complexity of maritime digitization through e-Navigation but also regional and national initiatives lead to the establishment of global wide accessible platforms such as the Maritime Connectivity Platform (MCP) for the usage of digital maritime services by different actors. The MCP is an approach for a globally uniform communication framework to support efficient, secure, reliable and seamless electronic communication exchange between all authorized stakeholders. It is based on a service-oriented approach and enables global identity management by the Maritime Identity Registry (MIR) and service management by the Maritime Service Registry (MSR). MIR and MSR are core components of the MCP. For the provision of technical services, IALA Guideline 1128 ("Specification for technical e-Navigation Services”) provides rules for a uniform specification of such services over multiple specification levels.

Beside all benefits, the establishment of the MCP and other approaches have to deal with security and safety issues. Provided e-Navigation services are highly relevant for the optimization of a safe navigation berth to berth and may be connected with systems such as an ECDIS onboard a ship, this requires the establishment of an extended handling of cyber security and safety in order to prevent cyber-attacks.

The remainder of this paper motivates therefore the need to identify safety and security related requirements, which need to be handled in the aforementioned environment.

# Potential threats and vulnerabilities

With the establishment and usage of the MCP, the maritime actors have to deal with additional cyber security and safety scenarios. Hostile attackers that gain unauthorized access to the MSR either by attacking the MSR hosting provider, a service provider or that register hostile services instances of a broadly used service might exploit the service consumer with malicious software or provide manipulated data through the service with the intention to influence a vessel’s passage. Malicious service instance descriptions might also remain cached at a service consumer ending up in continuous use of malicious service instances even though such an instance has already been identified and removed from the MSR.

The infrastructure and resulting operational processes of the MCP for user authentication and the registration of new services requires the correct specification of those services for a harmonized usage. IALA Guideline 1128 provides rules for a harmonized specification of technical services. Nevertheless, once a service has been registered with Maritime Service Registry service consumers are require to trust the MSR as in the current state no further checks for authenticity and service integrity have been established so far.

Potential vulnerabilities are the upload of new service instance descriptions in the MSR via unauthorized access or the manipulation of a documented service endpoint in order to redirect the service consumer and intentionally provide him with incorrect information. A use case is the redirection of users of a safety relevant weather service to another endpoint in order to send incorrect weather information. Moreover, on the service provider-side, it may be the case, that through unauthorized access, attackers send malware and exploits for specific onboard systems (e.g. a specific ECDIS) for various cases. Therefore, iterative and continuous checks of registered services are necessary.

The inclusion of a digital signature into the service description specification, the service instance description specification and optionally to the related service documentation would significantly increase trust and security for service providers and consumers respectively.

Public Key Cryptography Standards have been widely adopted in IT infrastructures such as for app stores and telecommunication services in general. XML signature defines for instance an XML syntax for digital signatures and is specified in the W3C recommendation “XML Signature Syntax and Processing”. It has been already successfully used by various Web technologies such as SOAP, SAML, and is suitable for ensuring service specification authenticity and integrity for the MSR as well.

# Outlook

Reviewing or eliminating the above threats through the provision of trustworthy services leads to a safer e-navigation environment. According to Bimcos Guideline on Cyber Security onboard ships, cyber security should be guided by appropriate standards. Such standards must also be defined and applied in the context of the MCP environment.

In order to make this possible, the IALA Guideline 1128 and the interfaces of the MCP have to be adapted. This includes:

* Analysis of potential threats to the MCP environment and offered e-navigation services
* Development of suitable technical and organizational measures with the purpose of monitoring systems.
* Integration of these systems in the MCP environment
* Continuous monitoring of registered services and MCP components
* Define a review process to further evolve the processes above

# Action requested of the Committee

The committee is invited to note the information paper and provide comments when appropriate.

1. Input document number, to be assigned by the Committee Secretary [↑](#footnote-ref-1)
2. Input papers should be assigned to a work task as listed in the Committee work plan which is available in input papers. Leave open if uncertain but consider how the paper is to be processed if not relevant to a work task [↑](#footnote-ref-2)