# IALA GUIDELINE

## G-XXXX

## GUIDELINE ON WEB SERVICE BASED S-100 DATA EXCHANGE

**Edition 1.0**

**Date (of approval by Council)**

10, rue des Gaudines - 78100 Saint Germain en Laye, France
Tél. +33 (0)1 34 51 70 01- Fax +33 (0)1 34 51 82 05 - contact@iala-aism.org
www.iala-aism.org

International Association of Marine Aids to Navigation and Lighthouse Authorities
Association Internationale de Signalisation Maritime

# DOCUMENT REVISION

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 |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# CONTENTS

# 1. INTRODUCTION

## 1.1. SCOPE

e-Navigation and Maritime Services have been defined by IMO as the means of providing electronic information in a harmonized way for the maritime domain. This requires common standards, specifications and guidelines on different levels. The standardisation of a common Web Service interface for exchange of S-100 based products will enable wider technical interoperability where the same service interface can be used for exchanging information regardless of operational use, i.e. common for several Maritime Services.

Accordingly, the purpose of the guideline is to:

- Provide guidance on standardized service exchange of information part of Maritime Services e.g. MSI/Navigational Warnings Route Plans and Chart updates
- Facilitate interoperability between maritime systems/eco-systems
- Reduce the need to support many different (proprietary) service designs
- Utilize the benefits of Service Oriented Architecture e.g. episodic tight coupling to allow a ship to interact with a port even though it is the first call to that specific port

Furthermore, it provides guidance on the application of *reliable and efficient* online Web Service based communication for the exchange of S-100 data. With the introduction of section 14 in the S-100 standard an alternative mechanism for efficient, fine-grained S-100 data exchange is available. This data exchange model allows frequent transmission of data to enable continuous information exchange between e-Navigation applications and efficient usage of available (limited / expensive) bandwidth and complements the classic file exchange of S-100 data. This creates flexibility towards future application of S-100 data exchange as needs for data exchange grow, for instance for e-Navigation and in in the development of autonomous shipping (MASS, Maritime Autonomous Surface Ships). It is an important building block especially for technical services for the implementation of Maritime Services in the context of e-Navigation. The realization of Service Oriented Architectures (SOA) using S-100 is also facilitated by this guideline. In the Appendix an example of the implementation of a Web Service for the provision of Maritime Safety Information using S-124 is shown.

This guideline is intended for service providers, system architects and developers, who are designing S-100 based technical services and implementing Maritime Services in the context of e-Navigation.

*Note*: This is one of several guidelines associated with Recommendation R-1019 (on the Provision of Digital VTS and AtoN Maritime Services in the context of e-Navigation in the domain of IALA). In particular, this document describes how IALA members can meet the following recommendations in R-1019:

2 Provide Maritime Services in digital formats, using international standards.

4 Ensure harmonisation 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).

## 1.2. RELATED DOCUMENTS AND RELATIONS TO THESE

Below, a list of related documents can be found. This guideline introduces the topic of Web Service based S-100 data exchange. It should be understood as an overview of available technologies, standards and guidance

documents and provide knowledge on the general aspects of the topic. For the underlying data model of a S-100 Web Service, refer to **IHO's S-100 Standard.** For explicit implementation of a S-100 Web Service API, refer to **IEC 63173-2 ED1: Maritime navigation and radiocommunication equipment and systems – Data interface – Part 2: Secure exchange and communication of S-100 based products (SECOM)** and for specification of such services, refer to **IALA Guideline 1128: SPECIFICATION OF e-NAVIGATION TECHNICAL SERVICES.** Refer to the IMO documents for further information on the definition of the terms *Maritime Service* and *e-Navigation*. In the following sections of this guideline, these documents and the other documents in the list below are placed into context and guidance is given on when to refer to which document.

**List of related Documents**

IHO S-100 Standard v. 4.0.0

The IALA Guideline 1128: SPECIFICATION OF e-NAVIGATION TECHNICAL SERVICES

IEC 63173-2 ED1: Maritime navigation and radiocommunication equipment and systems – Data interface – Part 2: Secure exchange and communication of S-100 based products (SECOM)

IMO MSC.467(101) on Guidance on the definition and harmonization of the format and structure of Maritime Services in the context of e-navigation

IMO MSC.1/Circ.1610 INITIAL DESCRIPTIONS OF MARITIME SERVICES IN THE CONTEXT OF E-NAVIGATION

ISO/IEC 7491- Open Systems Interconnection – Basic Reference Model

OAuth 2.0 Framework - RFC 6749

## 1.3. BACKGROUND

The maritime industry is a big sector of today's economy. Hundreds of thousands of vessels are constantly underway on inland waterways, coastal waters or on the open sea. To sail within their environment safely there is a continuous and increasing need for communication. This could be communication with surrounding vessels for collision avoidance, contacting vessel traffic service operators in port areas, obtaining weather data for the planned route or receiving Navigational Warnings to name only a small selection.

Until now most of these processes and services use several different types of communication channels [1]. The way of obtaining the above-mentioned information can also often differ depending on the location of the services. This makes the acquisition of relevant information more difficult in many situations. Especially safety-relevant data can be a problem when using communication methods, in which the validity and the propriety of the data cannot be verified. In an unprotected setup, an attacker could aim at injecting invalid information into navigational systems to create a misleading assessment of the environmental and navigational situation on vessels.

Contrarily, a technical trend consisting of new communication technologies for the maritime sector could be observed in the past years: IP-based communication technologies are increasingly rolled out and made available to the end-user. **Low Earth Orbit** (LEO) Satellite Networks, who can provide real-time IP-based communication [4] are currently emerging and are expected to find applications in several areas [5]. Also terrestrial technologies like **LTE** are expected to play an important role for the maritime industry in the future [6]. In addition to that, satellite providers like Inmarsat are going to launch broadband IP services that would be part of the well-known **Global Maritime Distress and Safety System** (GMDSS) in the near future [7].

The problem that a set of important information can sometimes only be obtained from a lot of different sources with their own standards, channels and technologies makes the gathering of information complicated and expensive. Especially safety-relevant data like the MSI, Ship-to-Shore reporting, Vessel Traffic Management or Pilot services should be easy to distribute and easy to receive. The developments in IP-based communication for maritime applications can be seen as an opportunity to make important services easier available and more secure.

The layered model of the internet protocol opens new possibilities for a separation of services and communication channels (see section 2.1).

This guideline gives guidance on how to distribute information in the maritime environment using web services that are transported over encrypted protocols using IP networks. It can be applied to any digital maritime service and especially to those exchanging S-100 data.

The **Maritime Safety Information (MSI) Service** is a GMDSS service for providing information which is needed for safe navigation of vessels [2]. It is a good example for a set of data that needs to be distributed to vessels frequently with a service-bound communication-path: The service is currently realized e.g. by a specific terrestrial (NAVTEX) as well as a satellite (SafetyNET) communication channel [3]. There is no established mechanism to ensure the integrity of these messages. A basic example on how this service can be realized conforming with this guideline is presented in the ANNEX A.

# 2. NORMATIVE COMPONENTS

## 2.1. IP-BASED COMMUNICATION IN MARITIME ENVIRONMENTS

The stack of communication technologies in the maritime industry is comprehensive. Technologies like LTE, VHF, AIS, Wireless networks, etc. are commonly used on ship bridges. The IP-Protocol is a widespread network layer protocol and abstracts from data link and physical communication layers (in ISO's OSI reference model, see ISO/IEC 7498-1:1994). Different Technologies that are already used in maritime applications can provide the underlying layers of the IP-Protocol. Satellite communication, 3GPP's LTE or IEEE 802.11, for example, can be utilized for that. The abstraction from these low-level standards opens new possibilities for always-available-services without the need of specific implementations for several low-level communication channels.

Especially in the maritime industry IP communication is opening opportunities for new business models, applying more standards 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 set of Maritime Services is imaginable. These services are implemented on top of the IP-Protocol and therefore do not need to deal with low-level communication issues. These services can be reached by Wi-Fi in port areas, LTE or cellular technologies in coastal areas or satellite communication at sea to make the most efficient way of communication possible respectively. Although the availability of IP based communication continuously increases, IP based communication is not always available to any service consumer. This should be kept in mind when designing IP based services.

Figure 1 shows an instance of ISO's OSI reference model, in which IP and technologies built on top of IP are abstracted from low-level communication channels. Layers can be stacked on top of IP to provide additional functionalities like data loss protection, encryption, session-based communication etc. This stack of technologies can then be used to transport the actual S-100 data from the service provider to its consumers.

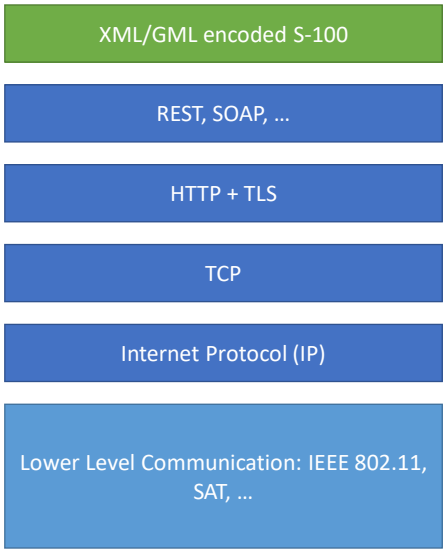



***Figure 1: Layer Model for the Abstraction of low-level Communication Technologies.***

Upcoming cyber-security risks are currently relevant (see [12]). Additionally, some low-level maritime technologies, such as AIS, are completely open and can be misused easily. IP-based communication allows the use of well-established encryption mechanisms and protocols. The IP protocol in itself is not the answer to security concerns but helps the maritime industry to easily integrate secure communication that enables reliable and integer information exchange.

## 2.2. S-100 ONLINE DATA EXCHANGE

"The **S-100 Standard** is a framework document that is intended for the development of digital products and services for hydrographic, maritime and GIS communities. It comprises multiple parts that are based on the geospatial standards developed by the International Organization for Standardization, Technical Committee 211 (ISO/TC211)." [10]

The following section summarizes the data exchange sections of the S-100 standard. The proposed concept in section 3 is an implementation of the data exchange model of the S-100 standard. Of course, this guideline can be applied to all S-XXX specifications, e.g. S-201.

The S-100 Standard allows exchanging S-100-Datasets with the S100_ExchangeSet class provided in section 4a of the Standard. An important part of the Exchange Set Model is the aggregation of Metadata and support files. A complete S-100 Dataset, typically consisting of different files such as the Feature Catalogue or digital signatures should be exchanged with its Metadata in this way (see Figure 1). The Metadata is encoded in an XML-file contained in a folder structure together with the S-100-Datasets.

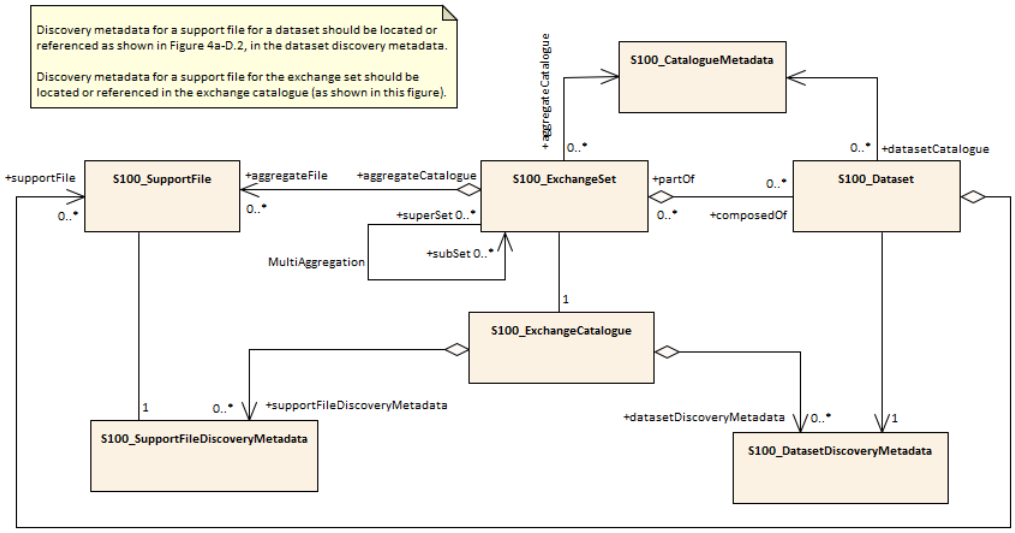



*Figure 2: S100 Exchange Set Model for exchanging S-100 Datasets with their Metadata*

When it comes to continuous data exchange nowadays, Web Services with publicly available APIs are often utilized for interchanging information. Web Service Technologies like REST or SOAP allow a fine-grained and efficient exchange of information. For this reason, Part 14 of the S-100 standard defines the usage of online services for the exchange of S-100 sets of data. Services themselves shall be modelled in a S-100 conform way (see Figure 2): The central class of the Service Data Model is the S100_ServiceMetaData which is composed of the Service Data Model including the S-100 Feature catalogue and the Service Interface which can be used to communicate with the Service.

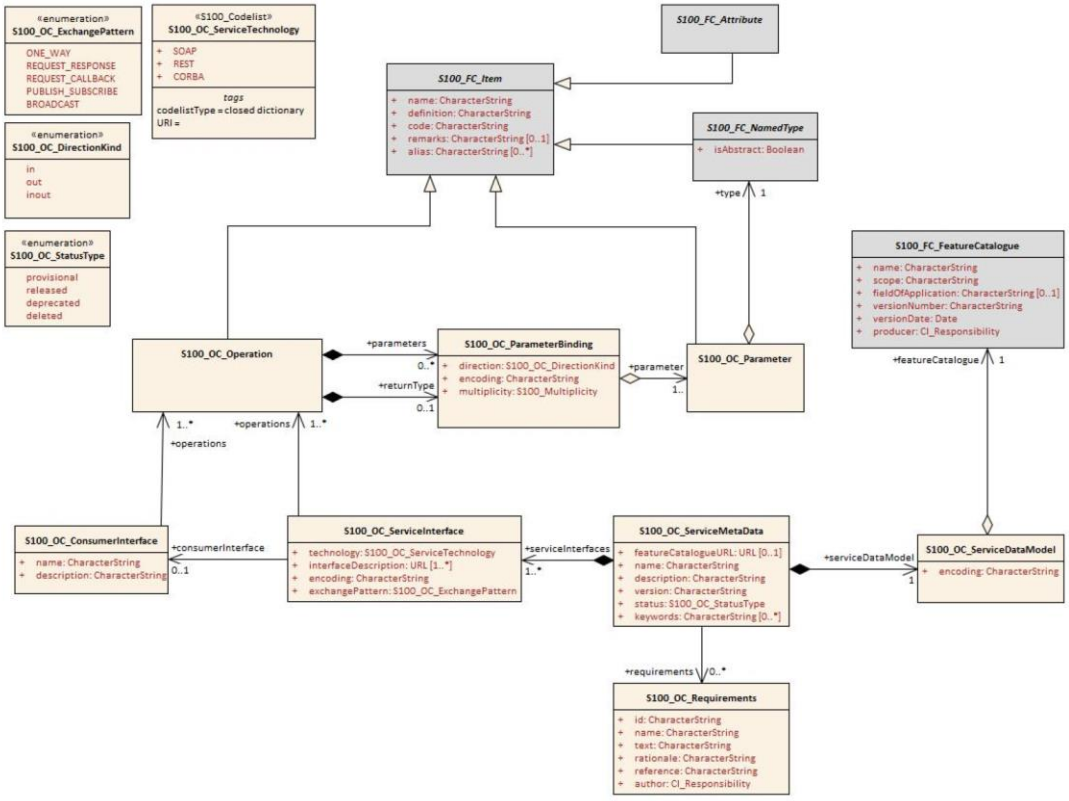



*Figure 3: S-100 Part 14: Data Model to describe a Service*

The Service Data Model does not contain all the fields used to describe the S100_ExchangeSet. This is due to the nature of a Service. A service is typically used to exchange multiple datasets or feature objects with multiple messages between service consumer and service provider as time passes.

Some information contained in the support files of the S100_ExchangeSet is dataset-specific and cannot be mapped to the general Service Metadata Model. A digital signature of a dataset, for example, is directly derived from the specific dataset and is different for every dataset. It has also kept in mind that a session-based service has the possibility to reduce the amount of transmitted data. Meta-Information such as the Feature Catalogue or the available operations only need to be transmitted once when a new consumer connects to the service and opens a new session. The service can keep track of the sessions and only submit new information, that is not already known to the consumer. This makes the continuous communication more efficient and lightweight in comparison to the S100_ExchangeSet if multiple datasets need to be transmitted over time.

The two aspects mentioned above should be considered when constructing the data model of a Web Service: Firstly, if Metadata needs to be added to single messages / data objects, either the data model itself needs additional fields for the description of Metainformation or a support class, similar to the S100_ExchangeSet needs to be constructed. Secondly, the Service communication scheme needs to be designed in such a way that the Service Metadata (not the dataset-specific Metadata) must be sent to the service consumer at the beginning of a session or the service metadata must be known to the consumer before. This is also prescribed by the S-100 Standard (section 14-4 to 14-6) and reduces the amount of transmitted data in comparison the S100_ExchangeSet, where Metadata such as the Feature Catalogue would be transmitted every time.

### 2.3. SERVICE ARCHITECTURE AND ENVIRONMENT

Theoretically, S-100 services can be deployed in several different setups: on-premise, in the cloud or as a hybrid solution. Although, to facilitate and enable discovery, authentication and identification of services and service providers some common principles need to be adhered to. Principles like standards for service description (like the IALA Guideline 1128, see also section 3.4), vetting procedures for service providers together with identification and authentication of services and service providers are important. These principles can be provided by a common, agreed upon Maritime Digital Infrastructure for Maritime services. Setting up a secure and efficient service for the exchange of S-100 datasets requires the existence of different resources: This can be the existence of any kind of identity provider, a way to enable service discovery for all involved parties or a message infrastructure. To provide these complex resources in an acceptable way is not an easy task for a single service provider. Upcoming platforms support the deployment of modern Maritime Services in the context of Service Oriented Architecture. Please refer to IALA Guideline XXXX: Guideline on Platforms to support the Implementation of Maritime Services in the Context of e-Navigation for further considerations on this topic and see Annex B for guidance on using the Maritime Connectivity Platform.

## 3. IMPLEMENTATION OF S-100 WEB SERVICES

### 3.1. WEB SERVICE BASED S-100 DATA EXCHANGE

A Web service technology such as HTTP — originally designed for human-to-machine communication — is used for transferring machine-readable data formats such as XML and JSON or in our case GML describing S-100 data. In practice, a Web service commonly provides a Web-based interface to a maritime technical service, utilized for example by a mobile app or bridge equipment, that provides a user interface to the end user.

The communication always consists of a request message from one machine (client) to another machine (server) and a reply message from the server to the client. The message can contain S-100 data encoded in GML. Different types of requests are named operations. Figure 4 and Figure 5 show an example of such a communication.

| |
|---|
| **POST** /Get_NW_Messages HTTP/1.1 |
| **HOST:** nw-service.com |
| **Content-Type:**text/xml |

```
<?xml version="1.0" encoding="UTF-8"?>
 <gml:boundedBy

    xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance

    xmlns:gml="http://www.opengis.net/gml/3.2">
  <gml:Envelope srsName="http://www.opengis.net/def/crs/EPSG/0/4326">
   <gml:lowerCorner>53.602678 6.934154</gml:lowerCorner>
   <gml:upperCorner>53.922239 7.528269</gml:upperCorner>
  </gml:Envelope>
 </gml:boundedBy>
```

***Figure 4: Example REST-POST-Request to retrieve Navigational Warnings.***

```
<?xml version="1.0" encoding="UTF-8"?>
 <S124:DataSet
 xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
 xmlns:gml="http://www.opengis.net/gml/3.2"
 xmlns:S100="http://www.iho.int/s100gml/1.0"
 xmlns:S100EXT="http://www.iho.int/s100gml/1.0+EXT"
 xmlns:s100_profile=http://www.iho.int/S-100/profile/s100_gmlProfile
 xmlns:S124="http://www.iho.int/S124/gml/cs0/0.1"
 xmlns:xlink="http://www.w3.org/1999/xlink">
  xsi:schemaLocation="http://www.iho.int/S124/gml/cs0/0.1 .../S124.xsd" gml:id="ds">
  <gml:boundedBy>
   <gml:Envelope srsName="http://www.opengis.net/def/crs/EPSG/0/4326">
    <gml:lowerCorner>53.602678 6.934154</gml:lowerCorner>
    <gml:upperCorner>53.922239 7.528269</gml:upperCorner>
   </gml:Envelope>
  </gml:boundedBy>
  <S124:References gml:id="references">
   <messageSeriesIdentifier>
    <nameOfSeries>Navigational Warnings</nameOfSeries>
    <warningNumber>0</warningNumber>
    <warningType>local Navigational Warning</warningType>
    <year>2019</year>
    <productionAgency>000</productionAgency>
   </messageSeriesIdentifier>
   <referenceCategory>in-force</referenceCategory>
   <noMessageOnHand>false</noMessageOnHand>
   <theWarning xlink:href="#preamble"/>
  </S124:References>
  <S124:NWPreamble gml:id="preamble">
   <messageSeriesIdentifier>
    <nameOfSeries>Navigational Warnings</nameOfSeries>
    <warningNumber>0</warningNumber>
    <warningType>local Navigational Warning</warningType>
    <year>2019</year>
    <productionAgency>000</productionAgency>
   </messageSeriesIdentifier>
   <publicationDate>2019-05-04T18:13:51.0</publicationDate>
   <generalArea>
    <locationName>
     <text>Norderney</text>
    </locationName>
    <locationName>
     <text>Langeoog</text>
    </locationName>
   </generalArea>
   <theWarningPart xlink:href="#warning"/>
  </S124:NWPreamble>
  <S124:NavigationalWarningFeaturePart gml:id="warning">
```

```
<geometry><S100:pointProperty>
 <S100:Point gml:id="pnt1">
 <gml:pos>53.731420 7.397681</gml:pos>
 </S100:Point>
</S100:pointProperty></geometry>
<warningHazardType>uncharted rock</warningHazardType>
<warningInformation>
 <headline>Uncharted Rock</headline>
 <text>An uncharted rock was discovered between Langeoog and Norderney islands...</text>
</warningInformation>
<header/>
</S124:NavigationalWarningFeaturePart>
</S124:DataSet>
```

***Figure 5: S-100 gml answer to the request shown in Figure 4.***

A more elaborated example of transfer of S-124 data is provided in ANNEX A.

As the S-100 standard is applied in several different areas of the maritime domain for modelling and distribution of data, an equally large number of services for the distribution of these datasets is imaginable. To make these services interoperable, a harmonized definition of APIs of these services is required. The IEC 63173-2 ED1: Maritime navigation and radiocommunication equipment and systems – Data interface – Part 2: Secure exchange and communication of S-100 based products (further referred to as SECOM) defines a standardized way for the specification of these APIs. It is recommended to also refer to this document for the explicit implementation of S-100 Web Services and their associated infrastructure.

## 3.2. MAKING USE OF THE SESSION CONCEPT

It can be useful to make use of the *session concept* for a Web Service based S-100 data exchange. A Session precisely incorporates all or part of the communication between service provider and service consumer and helps service provider and service consumer to maintain an information state about messages that have been sent between them in the past in a specific session. A session starts at a certain point in time and can be terminated later. This allows an efficient exchange of data: Service-related Metadata does not need to be sent with each dataset, but only at the beginning of a session. It is then evident to service consumer and service provider, that the Metadata is known by both parties. Also, sessions can be used to manage different states of communication. In a service setup with multiple consumers, the service provider can keep track of which information already has been made available to which client.

This session must not be confused with the term “session” in the context of communication protocols, like a TCP session, which operates independently from the Web Service session and serves another purpose. Web-Service sessions can be used independent from lower level communication and do not require a continuous connection.

The operations StartSession (to create a new session), EndSession (to terminate the current session), KeepAlive (to keep the current session alive, if a session time-out is configured) and GetMetaData (to retrieve Metadata) are the minimal requirements for a S-100 conform session-based service specification as stated in section 14-9 of the S-100 standard. Here, sessions are specifically utilized to keep an internal state of which consumer has received which S-100 data. When querying the service again, the service can identify the consumer by a sessionID and for example only transmit new data objects. This is an important factor to minimize the traffic and ensure that every consumer is aware of any relevant data.

Note that GetMetaData returns the ServiceMetaData instance, defined in Figure 3. Hence, GetMetaData is the only command that must be known to the consumer to discover the services capabilities.

Of course, it is also possible to implement S-100 Web Services without the usage of sessions. Such services are called *stateless* or *session-less* services. This can be useful to reduce the complexity of the communication with a service and is thus also implemented by SECOM.

## 3.3. AUTHENTICATION MECHANISMS AND ENCRYPTION TO ENSCURE MESSAGE INTEGRITY

To secure the exchange of the S-100 data, two options are available. One option is to require that each transmitted fragment of data is digitally signed by its originator. Thereby it is possible to guarantee origin and message authenticity without any trust assumptions on intermediary communication points, but care must be taken to prevent replay attacks. The second option is to ensure that the communication between the consumer and service is carried out via a secure connection, e.g. via TLS. The TLS Protocol is very common in HTTPS communication. However, the consumer must trust that the service provider distributes authentic and timely S-100 data only, and it lies with the service provider to ensure this. The two options can of course also be used in combination.

Both solutions require the existence of a Public Key Infrastructure (PKI) including a certificate authority (CA) that issues certificates for the participants of the proposed communication pattern. These certificates prove that a cryptographic key used for encryption or digital signatures belongs to a certain Identity of a person, a service, etc. These keys can be used in different contexts: For signing a dataset, encrypting a communication channel or authenticate a specific entity. A consumer-defined lookup-table can be configured with a list of CAs that are trusted by the consumer. Suitable PKIs are currently set up by operators of the Maritime Connectivity Platform (e.g. by the Navelink Consortium or the MOF in Korea). SECOM also considers the standardization of maritime PKIs.

As it is not always possible or intended to contact the CA for each message that is broadcasted by the service provider, the consumer (which is typically a vessel at sea) is recommended to update the local certificate store whenever in charge of a good connection. This aims to optimize the usage of the potentially limited bandwidth at sea.

An alternative approach is to make use of the established chains of trust as used on the internet. This mitigates the need to establish a PKI and CA and has an updated local trust store mechanism in all modern systems. This approach does not necessarily imply that communication takes place over the internet.

In either approach, it is highly recommended that systems and protocol requirements are updated regularly as TLS certificates get updated and revoked, encryption techniques are advancing, and encryption requirements change as a result. It is suggested that system updates are performed on a monthly basis or more frequently.

The service provider should carefully consider the offered encryption mechanisms. While some older mechanisms (e.g. TLS v1.0) are not considered secure enough at a certain point in time, the service consumer might use systems that have not been updated for a while (which is not uncommon for ships) and does not support anything better than that older mechanism.

If support metadata such as digital signatures needs to be transmitted with each message or transmitted data object, additional changes need to be made to the transmitted data. Current solutions in the S-100 including ServiceMetaData (section 4a-5.7) and the S-100 ExchangeSet do not offer the possibility to add such information to every message without using support files in a predefined folder structure which is not suitable for the realization in a Web Service. Figure 6 shows the difference between Service Metadata and Message / Data Object Metadata.

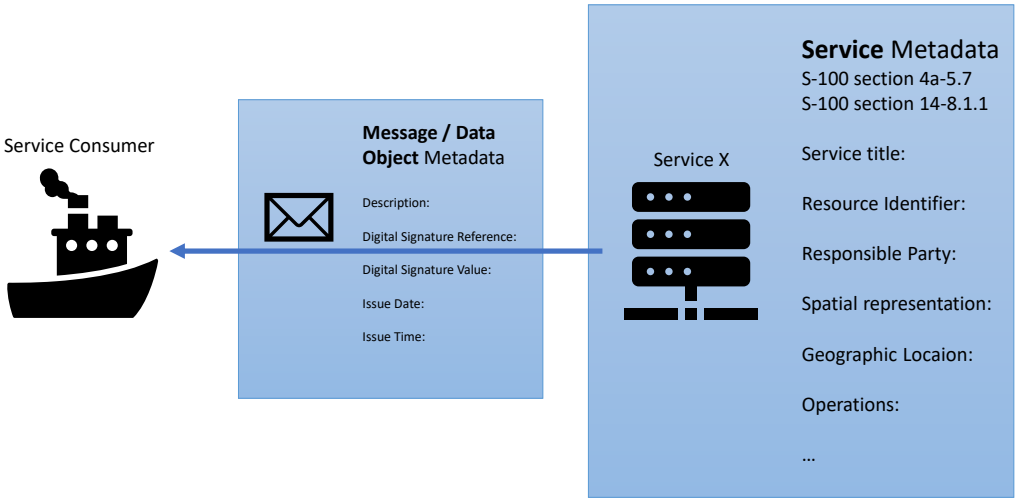



*Figure 6: Different types of Metadata: Message / Data Object Metadata is bound to a single message, Service Metadata is bound to a complete service instance.*

An approach for the solution of this problem is shown in Figure 7: The Streamable_Exchange set complements the ServiceMetaData with data-specific information such as a digital signature that is directly derived from the data and therefore needs to be generated for each data object individually. The Streamable_ExchangeSet is inspired by the SupportFile-section of the ExchangeSet model of the S-100 standard. It can easily be extended with additional dataset-specific metadata without making changes to the S-XXX data models. The Streamable_Exchangeset may also be extended with further parameters and attributes to encapsulate service-related content that is not directly associated with the S-100 data. Please note that SECOM treats the problem in a similar way in its standardized API definition. For explicit implementation, it is recommended to follow the more detailed models of SECOM.

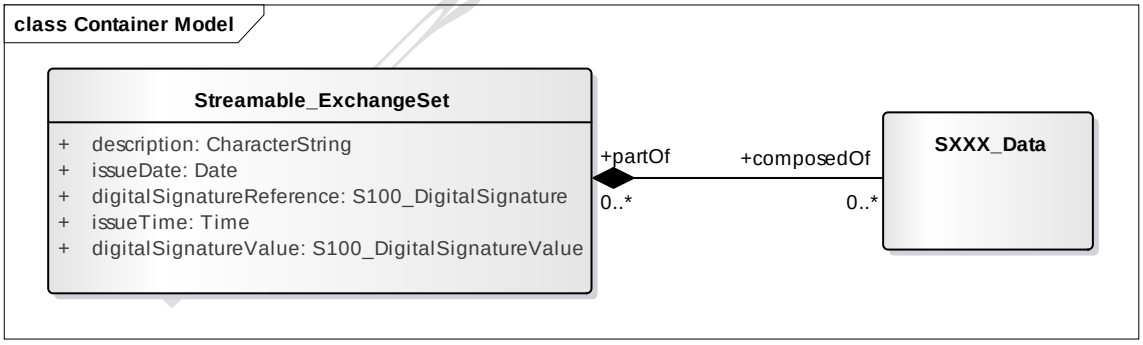



*Figure 7: Streamable Exchangeset as (Signature-)Metadata-Container for S100-Datasets.*

In S-100 section 15 the mechanism for assigning digital signatures to files is described. The approach described here makes use of its features (S100_DigitalSignature, S100_DigitalSignatureValue) but the signatures are assigned to datasets. In addition, to ensure the timeliness of S-100 datasets the data set must also contain a timestamp (i.e. date and time) so that the receiver of the dataset can check whether the data is sufficiently up-to-date. Otherwise an attacker could eavesdrop and record a signed dataset and replay it later, perhaps in a context when the data will cause misinformation or confusion. It is crucial that the signature spans both the dataset and the timestamp. Otherwise replay attacks will still be possible: The attacker could extract the signed dataset from the overall message and combine it with a timestamp valid for the intended time of replay. Also note that separately signing

the dataset and the timestamp is not sufficient because the attacker could eavesdrop on any current message, extract its signed timestamp, and combine the current signed timestamp with an earlier signed dataset. Hence, it is crucial that S-100 dataset and timestamp are cryptographically bound together.

Moreover, it is crucial for security that the clocks of the sender and receiver are synchronized and that the time window in which the receiver accepts a message as valid is sufficiently precise. The first is easy to realize since in the maritime context we can assume that senders and receivers are equipped with GPS. The choice of the time window for acceptance is less straightforward to determine. Different types of datasets might come with different margins of when it might become unsafe to accept and act upon them. In our context of IP-based communication we also must keep in mind that the routing of messages does not come with any real-time guarantees. It is recommended that the time window will be defined specifically for each type or sub-groups of S-100 dataset following a safety impact analysis.

Also, it is highly recommended to implement IP based communication in such a way that no UDP/TCP -Ports are opened at the service consumer side at any time. Open ports increase the attack surface and make consumer systems more vulnerable to an attacker. This can be due to undiscovered security gaps in parts of the consumer side implementation that are listening to these ports. Also, the usage of HTTPS instead of HTTP as a communication protocol always must be preferred as is fulfils all of the proposed recommendations. As an additional measure for security, a VPN connection can be used.

### 3.4. SERVICE SPECIFICATION

As the digitalisation of the maritime industry advances rapidly, a whole set of new digital Maritime Services is expected to be established soon. These systems may bring new challenges of interoperability and harmonisation with them. Therefore, the IALA is developing and publishing standards, recommendations and guidelines for the specification of Maritime Services. The IALA Guideline 1128: SPECIFICATION OF e-NAVIGATION TECHNICAL SERVICES describes a standardized approach for the specification of Maritime Services for the e-Navigation. The Guideline differs between the actual service specification, technical designs and instance descriptions. All parts of the guideline are characterized by a fixed scheme. This opens the possibility for the standardized specification of services in a Service Oriented Architecture. It is highly recommended to refer to the Guideline 1128 for the specification and SECOM for the technical realization of Maritime Services.

## 4. REFERENCES


[1] F. Bekkadal, 'Emerging maritime communications technologies', Oct. 2009.

[2] 'Resolution A.705(17) - Promulgation of Maritime Safety Information'. International Maritime Organization, 06-Nov-1991.

[3] 'Manual on Maritime Safety Information (MSI)'. International Hydrographic Organization, Jul-2009.

[4] G. Maral, J.-J. de Ridder, B. G. Evans, and M. Richharia, 'Low earth orbit satellite systems for communications', *International Journal of Satellite Communications*, 01-Jul-1991. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/sat.4600090403. [Accessed: 08-Jul-2019].

[5] H. Tsunoda, K. Ohta, N. Kato, and Y. Nemoto, 'Supporting IP/LEO Satellite Networks by Handover-Independent IP Mobility Management', *Sel. Areas Commun. IEEE J. On*, vol. 22, pp. 300–307, Mar. 2004.

[6] I. Maglogiannis, S. Hadjiefthymiades, N. Panagiotarakis, and P. Hartigan, 'Next generation maritime communication systems', *IJMC*, vol. 3, pp. 231–248, Jan. 2005.

[7] 'Inmarsat receives IMO approval for Fleet Safety', *Inmarsat*. .

[8] K. Korcz, 'GMDSS as a Data Communication Network for E-Navigation', *TransNav Int. J. Mar. Navig. Saf. Od Sea Transp.*, vol. 2, no. 3, Sep. 2008.

[9] E. Tzannatos, 'GMDSS Operability: The Operator-Equipment Interface', *J. Navig.*, vol. 55, pp. 75–82, Jan. 2002.

[10] 'THE S-100 UNIVERSAL HYDROGRAPHIC DATA MODEL', 2017. [Online]. Available: http://s100.iho.int/S100/. [Accessed: 05-Sep-2019].

[11] International Hydrographic Organization, 'IHO Geospatial Standard For Navigational Warnings - Special Publication No. S-124 (Working Draft)'. 31-Oct-2018.

[12] L. Jensen, 'Challenges in Maritime Cyber-Resilience', *Technol. Innov. Manag. Rev.*, vol. 5, pp. 35–39, Apr. 2015.

[13] Maritime Connectivity Platform, 'MMS: Concepts, Design and Usages'. .

# ANNEX A IP BASED EXCHANGE OF MSI (S-124)

This section is an example on how to implement a reliable and efficient IP based service following this guideline.

## 1. NORMATIVE BACKGROUND

### 1.1. GMDSS

**The Global Maritime Distress and Safety System (GMDSS)** was designed to alert rescue authorities as well as near vessels in case of an emergency event. The goal is to provide help to the ship in distress as fast as possible. It is also used for the distribution of Maritime Safety Information (MSI) and was introduced by the SOLAS Convention in 1992. [8]

The GMDSS uses several different communication methods realized by satellite or terrestrial services. Radar transponders and emergency position indicating radio beacons are also used sometimes for locating survivors after an accident. Depending on the location of the ship in distress, different channels are used for an automated establishment of communication. [9]

The addition of IP-based communication to the GMDSS via satellite is a recent development and opens the possibility to reach ships in distant locations via an IP-connection [7]. As a part of GMDSS these services must fulfil the approved safety and security standards regulated by the SOLAS Convention too.

### 1.2. MSI

As defined by the Resolution A.705 by the International Maritime Organization (IMO), the Maritime Safety Information Service is

*"[…] an internationally coordinated network of radio broadcasts containing information which is necessary for safe navigation, received in all ships by equipment which automatically monitors the appropriate frequencies and prints out in simple English only that information which is relevant to the ship".* [2]

The MSI service is also a part of the GMDSS. In addition to providing information about Navigational Warnings, the MSI service is used for the distribution of meteorological forecasts and warnings or other safety-related information. The process of the distribution is visualized in Figure 8: The MSI is sent to an abstraction layer of the available broadcast service. Depending on the location of the affected ships either NAVTEX or SafetyNET is selected to transmit the information. The GMDSS-equipped ship needs separate equipment for receiving the MSI either by satellite (SafetyNET) or terrestrial (NAVTEX) communication channels. [3]

### 1.3. S-124 STANDARD

The **S-124 Standard** is a product specification of the S-100 family, managed by the International Hydrographic Organization (IHO). It standardizes the Navigational Warnings with a S-100 conforming Data Model. Its intention is to describe and encode Navigational Warning data for the usage in navigation. The standard aims to its usage in context of NAVTEX and SafetyNET. As a submission of S-124 data is not considered possible, a direct translation from S-124 data to the proprietary technologies is planned. Moreover, S-124 is not limited to these channels and also expected to be used in context of consumer-available Web Services. [11]

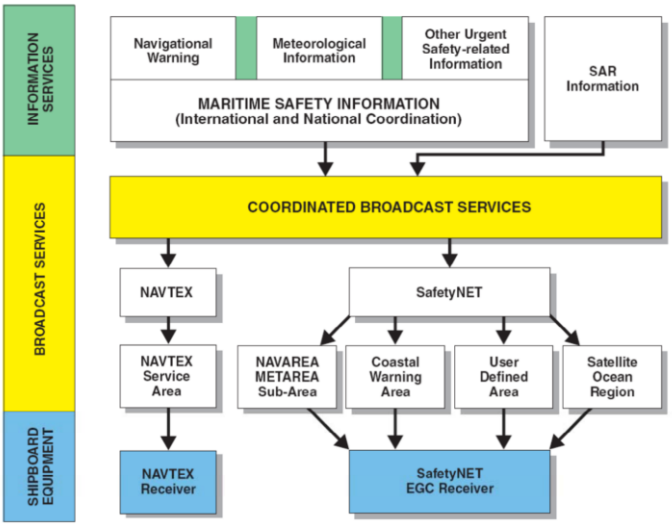



*Figure 8: Today's Distribution of the MSI - Information, Broadcast Services and Shipboard Equipment [3]*

## 2. REALIZATION OF A WEB SERVICE FOR MARITIME SAFETY INFORMATION

The following section describes the realization of a Navigational Warnings service. The service specification is an instance of the S-100 Service Data Model as introduced in section 2.2. Please note, that this only a very minimal specification of a S-124 Web Service. The S-124 Working Group is currently working on a complete G1128 service specification for the exchange of Navigational Warnings with S-124. Existing Web Services for the distribution of navigational warnings already have been established experimentally (Baltic / Pacific Web, Danish Maritime Authority).

Figure 9 shows the instantiation of the S-100 model. The ServiceMetaData provides the central structure and provides information about the service itself. The ServiceInterface in combination with the ConsumerInterface specifies the way consumers can interact with the service. The S-124 data model of the service can be represented by the (XML-) Feature Catalogue of the S-124 Standard.

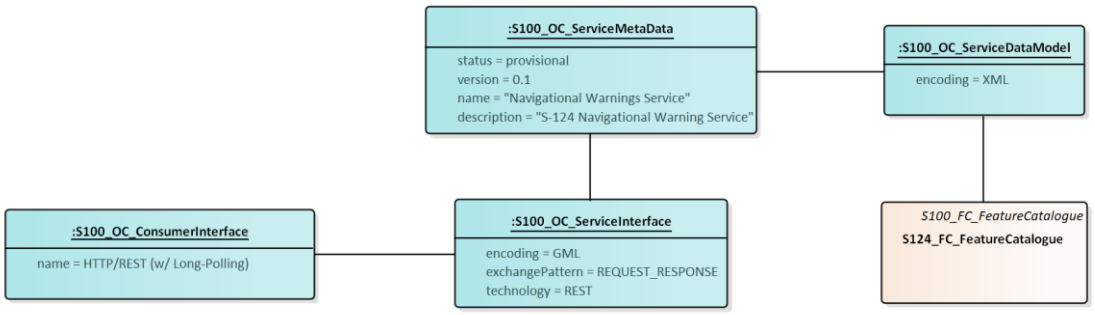



*Figure 9: Service Specification of the Navigational Warnings Service*

The operations of the service, which are also instances of the Service Data Model are illustrated in a separate diagram for the sake of clarity. Please note, that for demonstration only a subset of the proposed operations in the S-124 Standard, section 11.2.2 is implemented.

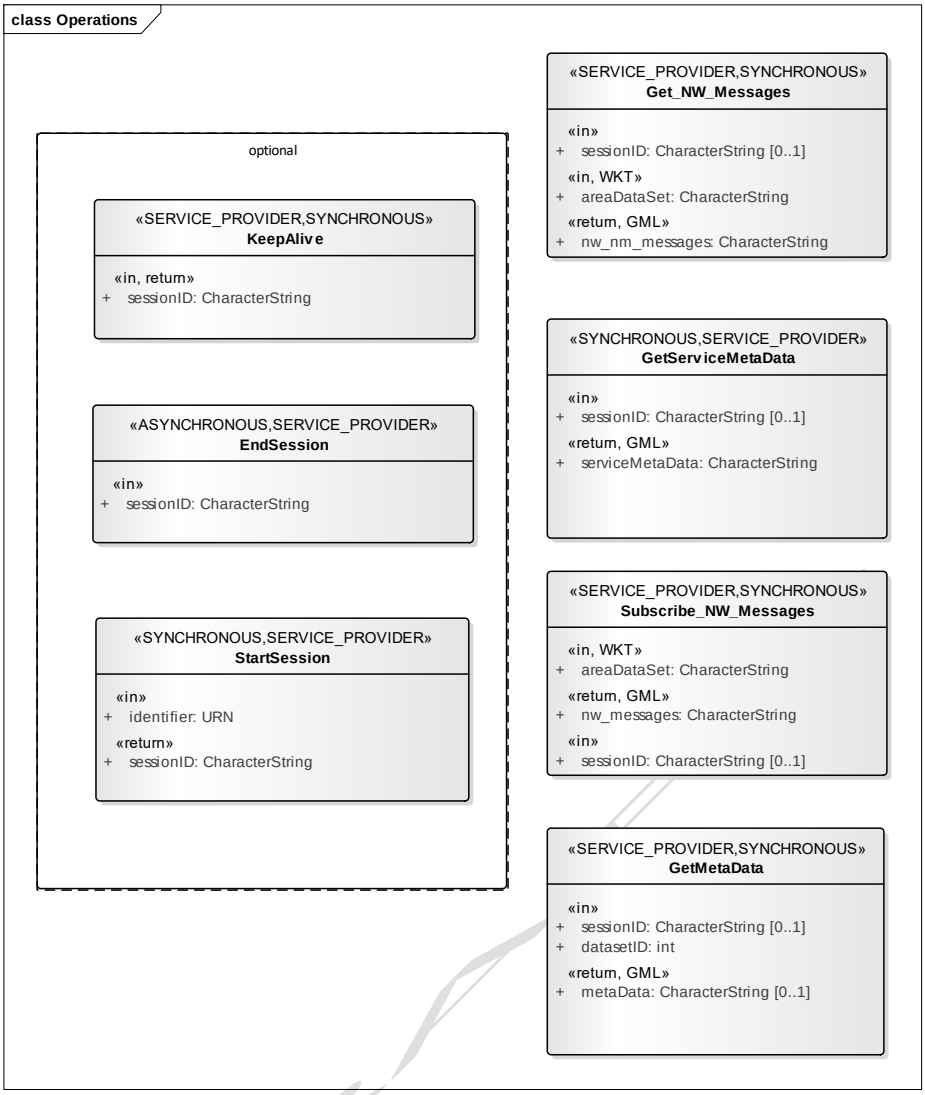



*Figure 10: Available Operations of the Navigational Warning Service*

The operations StartSession, EndSession, KeepAlive and GetMetaData are the minimal requirements for a S-100 conform **session-based service** specification as stated in section 14-9 of the S-100 standard. Sessions are utilized to keep an internal state of which consumer has received which warning. When querying the service again, the service can identify the consumer by the sessionID and only transmit new Navigational Warnings. This is an important factor to minimize the traffic and ensure that every consumer is aware of any relevant warnings.

GetMetaData returns the Exchange set Metadata for a specified dataset. GetServiceMetaData returns the ServiceMetaData (S-100, section 4a-5.7).

### *Operations Description*

StartSession, EndSession, KeepAlive and GetMetaData are implemented as described in S-100 section 14-9.

Get_NW_Messages

OPERATIONTYPE: SYNCHRONOUS

OPERATIONOWNER: SERVICE_PROVIDER

| Role Name | Name | Description | Mult | Type | Direction | Encoding |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| Operation | Get_NW_Messages | Provides Navigational Warning messages for a specific area | - | - | - | |
| Parameter | sessionID | To identify the active session | 1 | CharacterString | in | |
| Parameter | areaDataSet | The NW coverage area | 0..1 | CharacterString | in | WKT |
| Parameter | nw_nm_messages | The messages returned for the area | 1 | CharacterString | return | GML |

Subscribe_NW_Messages

OPERATIONTYPE: SYNCHRONOUS

OPERATIONOWNER: SERVICE_PROVIDER

| Role Name | Name | Description | Mult | Type | Direction | Encoding |
|---|---|---|---|---|---|---|
| Operation | Get_NW_Messages | Opens a long-polling Subscription. The service provides Navigational Warning updates as Response. | - | - | - | |
| Parameter | sessionID | To identify the active session | 1 | CharacterString | in | |
| Parameter | areaDataSet | The area definition | 0..1 | CharacterString | in | WKT |
| Parameter | nw_nm_messages | The messages returned for the area | 1 | CharacterString | return | GML |

The implemented operations open the possibility for keeping track of the consumers by the service via the session id.

### *Communication Patterns*

The described operations allow two communication patterns between service and consumer. The first pattern (shown in Figure 11) is a simple polling pattern. After starting the session and transmitting the service metadata, the consumer can use the Get_NW_Messages command to receive all Navigational Warnings for the specified area. As this is only a minimal example, the selection of sub-areas of Navigational Warnings is not included here. The area could be for example a polygon containing the planned route. The Service can keep track of the messages that are known to the consumer via the session ID and only submit messages updates, when the consumer repeats the

Get_NW_Messages command in fixed periods. The consumer can also optionally ask for dataset metadata with the GetMetadata operation.

The second possible pattern is the long-polling pattern (shown in Figure 12). After opening the session and receiving the service metadata, the consumer executes Get_NW_Messages once, to get the current set of Navigational Warnings. After that, the consumer opens a long-polling request with Subscribe_NW_Messages. This is a simple request that is answered by the server only after an update of the Navigational Warnings set is published. This solution ensures that the consumer immediately gets notified, when an update is available. That means there is no fixed time period which must pass before a new request is executed as realized by the polling pattern. After an update was received, the consumer directly starts a new Subscribe_NW_Messages command to wait for the next update.

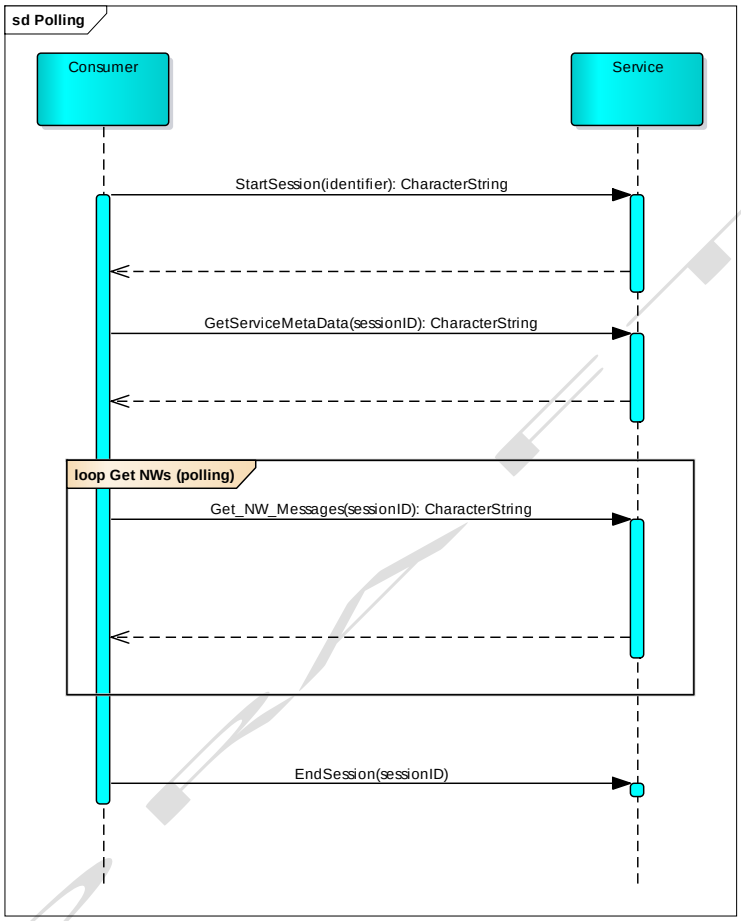



*Figure 11: Polling of the Navigational Warning Messages*

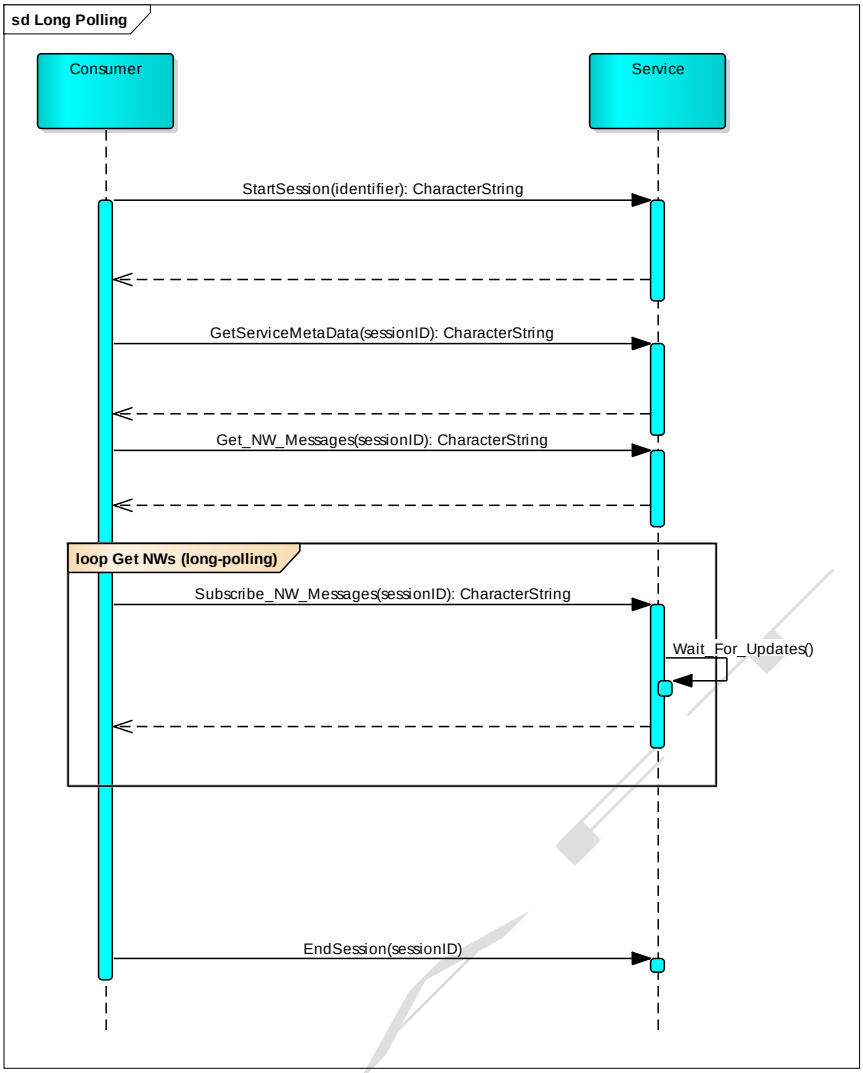



*Figure 12: Long-Polling of the Navigational Warning Messages*

Both patterns are mandatory for the service. Although the long-polling is preferable because of the immediate notification, it is not always possible to realize such a long lasting connection on the client side. Bad connections can be a cause of connections failures. Also, the polling method is an easy way to keep implementations of the consumer component simple.

Note that both patterns can also be used session-less (without executing the session commands) theoretically to provide a more lightweight communication pattern. In this case the service does not keep track of the transmitted warnings and the information state of the consumer.

# 3. SERVICE SPECIFICATION OF THE TECHNICAL SERVICE

The MSI technical service is specified in the following form according to G-1128.

## 3.1. SERVICE IDENTIFICATION

| | |
|---|---|
| Name | Navigational Warning Service |
| ID | urn:mrn:iala:service:specification:msi:1230.1 (to be assigned) |
| Version | 0.1 |
| Description | This service delivers Maritime Safety Information (MSI) / Navigational Warnings to its consumers. |
| Keywords | MSI, maritime safety information, Navigational Warnings, s-124, warnings service |

| | |
|---|---|
| Architects | Axel Hahn, Sibylle Fröschle, Julius Möller |
| Status | provisional |

## 3.2. OPERATIONAL CONTEXT

For a high-level description of the service see ANNEX A section 2.

Please note, that for demonstration we only implement a subset of the proposed operations in the S-124 Standard, section 11.2.2.

*Requirements*

| Requirement Id | **NWS-RQ1** |
|---|---|
| **Requirement Name** | Get Datasets |
| **Requirement Text** | The service must provide a list of current Navigational Warnings. |
| **Rationale** | |

| Requirement Id | **NWS-RQ2** |
|---|---|
| **Requirement Name** | Get Metadata |
| **Requirement Text** | The service must provide metadata for the Navigational Warning datasets. |
| **Rationale** | |

| Requirement Id | **NWS-RQ3** |
|---|---|
| **Requirement Name** | Subscribe Warnings |
| **Requirement Text** | The service must provide an interface for subscription of Navigational Warnings. The service consumer needs to be notified when a new Navigational Warning is created. |
| **Rationale** | |

| Requirement Id | **NWS-RQ4** |
|---|---|
| **Requirement Name** | Message signing |
| **Requirement Text** | Navigational warning datasets must be signed. |
| **Rationale** | Security |

*Operational Nodes*

| Operational Node | **Remarks** |
|---|---|
| **Vessels** | Vessels at sea. |
| **NW-Service providers** | Service providers that publish MSI. |
| **Certification Authorities** | Certification Authorities that issue certificates to sign the datasets. |

## 3.3. SERVICE OVERVIEW

The following diagram gives an overview of the main elements of the service.

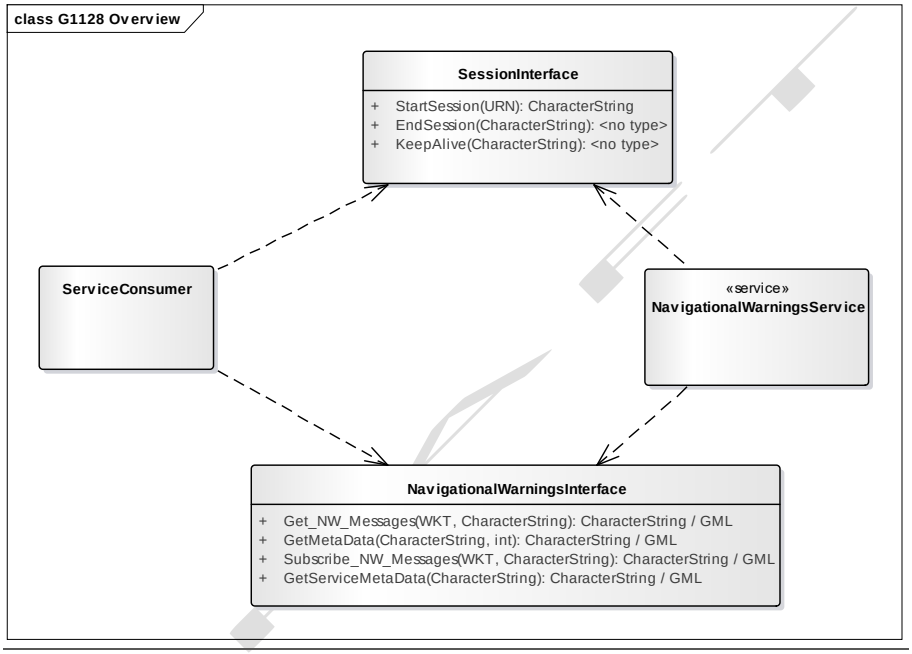



***Figure 13: Navigational Warnings Service Interface Definition Diagram.***

| Service Interface | Role (from service provider point of view) | ServiceOperation |
|---|---|---|
| **SessionInterface** | provided | StartSession, EndSession, KeepAlive |
| **NavigationalWarningsInterface** | provided | Get_NW_Messages, Subscribe_NW_Messages, GetMetaData, GetServiceMetaData |

## 3.4. SERVICE DATA MODEL

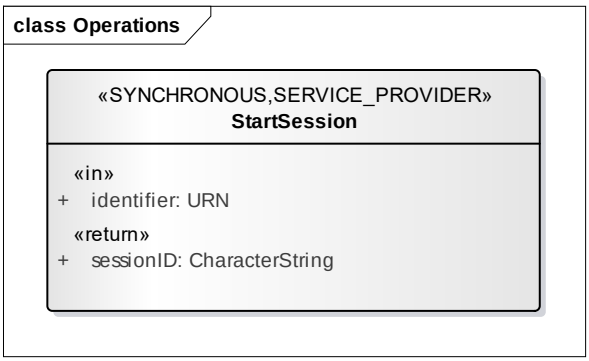
The service uses an external data model, which is described by the S-124 standard. Additions to the S-124 data model regarding security are discussed in section 3.3.

## 3.5. SERVICE INTERFACE SPECIFICATIONS

*SERVICE INTERFACE SessionInterface*

*The session interface provides functionalities for starting, ending or keeping alive a session. Sessions are used for keeping track of the current information state of each consumer of the service. The use of sessions is not mandatory, but it can help minimizing the traffic between service and consumer.*

**OPERATION** StartSession

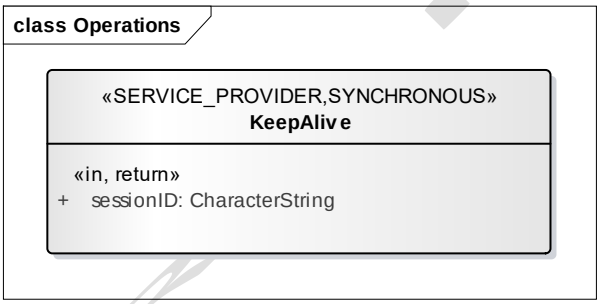



**OPERATION FUNCTIONALITY**: Starts a new session.

**OPERATION PARAMETERS**:

| Parameter | Type | Direction | Description |
|---|---|---|---|
| identifier | URN | In | An URN (MRN) identifying the consumer of the service. |
| sessionID | CharacterString | Out | An ID to identify the new session. |

**OPERATION KeepAlive**

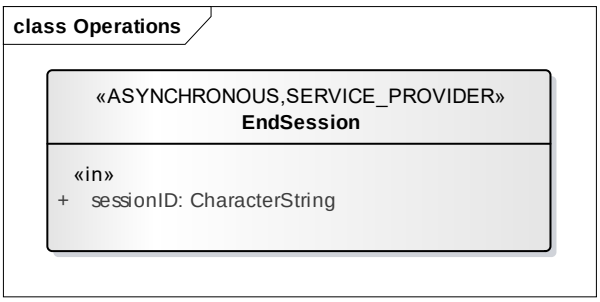



**OPERATION FUNCTIONALITY**: Keeps the current session alive. The service session time-out is reset.

**OPERATION PARAMETERS:**

| Parameter | Type | Direction | Description |
|---|---|---|---|
| sessionID | CharacterString | In | The current session ID. |
| sessionID | CharacterString | Out | The current session ID. |

**OPERATION EndSession**



**OPERATION FUNCTIONALITY**: Ends the current session.

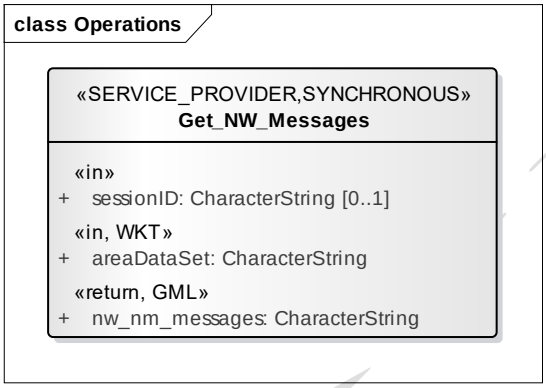
**OPERATION PARAMETERS:**

| Parameter | Type | Direction | Description |
|---|---|---|---|
| sessionID | CharacterString | In | The current session ID. |

### *SERVICE INTERFACE NavigationalWarningInterface*

The NavigationalWarningInterface provides the core functionality of this service. Consumers can request a list of Navigational warnings or subscribe to Navigational Warning updates. An operation for obtaining MetaData is also available.

**OPERATION Get_NW_Messages**

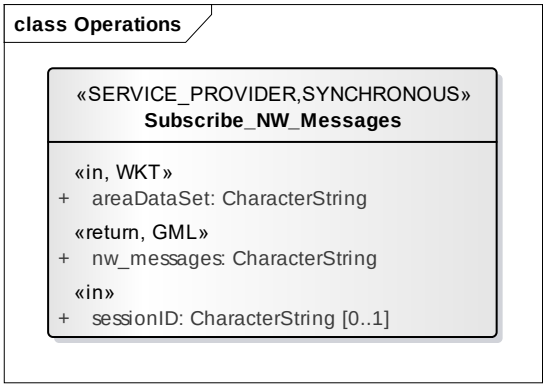



**OPERATION FUNCTIONALITY**: Returns a list of Navigational Warnings for a specified area.

**OPERATION PARAMETERS**:

| Parameter | Type | Direction | Description |
|---|---|---|---|
| areaDataset | WKT | In | The requested area for Navigational Warnings. |
| sessionID | CharacterString | In (optional) | The current session ID. |
| nw_nm_messages | CharacterString | Out | A S-124 Dataset with Navigational Warning, encoded in gml. |

**OPERATION Subscribe_NW_Messages**

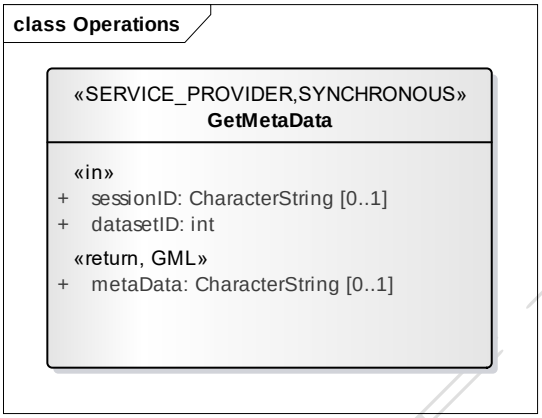



**OPERATION FUNCTIONALITY**: Subscription to updates on Navigational Warnings.

**OPERATION PARAMETERS**:

| Parameter | Type | Direction | Description |
|---|---|---|---|
| areaDataset | WKT | In | The requested area for Navigational Warnings. |
| sessionID | CharacterString | In (optional) | The current session ID. |
| nw_nm_messages | CharacterString | Out | A S-124 Dataset with Navigational Warning, encoded in gml. |

**OPERATION GetMetaData**

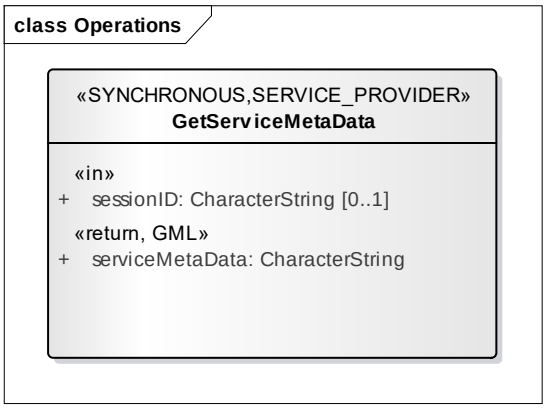



**OPERATION FUNCTIONALITY**: Provides Metadata for a dataset with a specified ID.

**OPERATION PARAMETERS:**

| Parameter | Type | Direction | Description |
|---|---|---|---|
| sessionID | CharacterString | In | The current session ID. |
| datasetID | Int | In | The ID of the dataset on which metadata is being requested. |
| metaData | CharacterString | Out | An S-100 metadata instance for the Navigational Warnings dataset encoded in gml. |

**OPERATION GetServiceMetaData**




**OPERATION FUNCTIONALITY**: Provides Metadata for the service.

**OPERATION PARAMETERS:**

| Parameter | Type | Direction | Description |
|---|---|---|---|
| sessionID | CharacterString | In | The current session ID. |
| metaData | CharacterString | Out | An S-100 service metadata instance for the Navigational Warnings service encoded in gml. |

## 3.6. SERVICE DYNAMIC BEHAVIOUR

The service dynamic behaviour is described in section **Error! Reference source not found.** (“Communication Patterns”).

# ANNEX B USING THE MARITIME CONNECTIVITY PLATFORM

## 1. INTRODUCTION

The goal of the **Maritime Connectivity Platform (MCP)** is to enable that information can be exchanged efficiently, securely, reliably and seamlessly between authorized maritime entities across diverse communication systems. To this end the MCP consists of three core components: The Maritime Identity Registry (MIR), the Maritime Service Registry (MSR), and the Maritime Messaging Service (MMS).

The MIR compromises three components that together provide the infrastructure necessary for secure communication services today. Firstly, Identity Management: Each MCP entity obtains a unique ID in terms of a Maritime Resource Name (MRN). Secondly, Public Key Infrastructure (PKI): Each MCP entity holds an electronic identity in terms of a public/private key pair and a certificate bound to their MCP ID. And thirdly, Authentication and Authorization for Web Services: MCP entities benefit from login, single sign-on, and authorization for API access of Web Services, as well as secure integration of Web Services based on the standards OAUTH 2.0 and OpenID Connect.

## 2. USING MMS

The Maritime Messaging Service (MMS) is an information broker as part of the Maritime Connectivity Platform (MCP, see section **Error! Reference source not found.**) for exchanging messages via different communication channels in a maritime environment. It is a more comprehensive approach than Web Services because it supports multiple communication patterns. It provides an abstraction Layer from low-level communication technologies and is – as it uses a HTTP Interface – based on IP-technology. The MMS uses MRNs to identify and authorize service consumers and service providers. It acts as a middleware between the service consumers and services and supports features like group- or geocasting of messages. Furthermore, the use of MRNs and the architecture of the MMS solve the problem of switching between different communication technologies and allow a continuous communication.

To use the MMS as a service provider, an MRN for the service is required. The service must register its MRN in the Maritime Identity Registry (MIR) which is also a part of the MCP. The registration of the service's MRN in the MIR is required later to authorize messages from the service. The service consumer, which is typically a vessel, also must use a registered MRN to communicate with the service via the MMS. In application, messages are then transmitted via HTTP with custom headers containing the MRN of the message source and destination. A service consumer can obtain the MRN of a Service via the Maritime Service Registry (MSR) of the MCP. Figure 14 shows the message layout of a message that is sent via the MMS.

| **HTTP Header** | | |
|---|---|---|
| Field Name | Description | Example |
| srcMRN | MRN of a sender | srcMRN: urn:mrn:smart:service:instance:mof:S11 |
| dstMRN | MRN of a receiver | dstMRN: urn:mrn:smart:vessel:imo-no:mof:12 |
| **HTTP Payload** | | |
| Message that a sender want to send.<br>Ex) Hello World! | | |

*Figure 14: Layout of an MMS-Message. [13]*

As every message is directly addressed to its receiver, the Webservice only needs a single interface that receives the messages addressed to its MRN. Additionally, the service needs to send MMS-HTTP requests to the MMS broker, to answer a consumer's request. Since the service only has one MRN, the selection of the operation required by the client needs to be wrapped into the message payload. A simple json-like structure with the attributes:

"operation", "type" and "content" that refers to the corresponding attributes of the S-100 service model is proposed. A basic message exchange with the wrapped operations is shown in Figure 15. Specialized parameters for different operations can be included in the content part of the message.

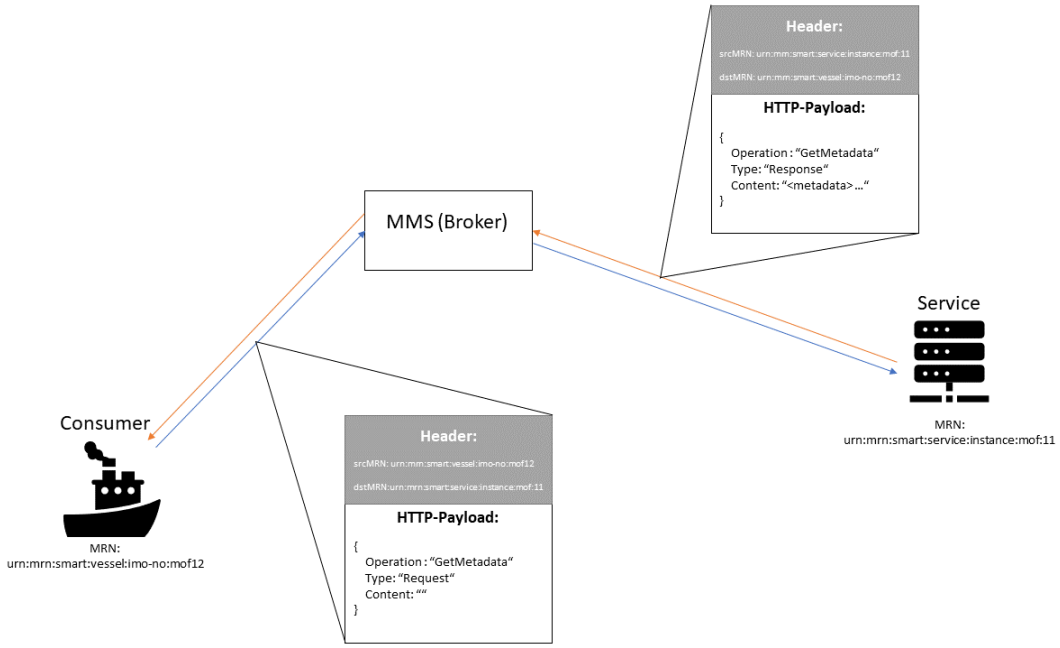



***Figure 15: Simple exchange of messages using the MMS with a json-wrapper for the operations and types.***

This usage of the MMS results in some changes that must be made to the methodology proposed in section 3.1 and 3.2: As the consumers can now be identified by their MRN, which is known to the service, the session operations are not mandatory anymore in the MMS setup. However, these commands can be kept for keeping track of consumers interests to receive new messages.

If the MMS is within the trust boundary of the client, the MMS could be used as a push-service gateway which enables the client to receive messages right after they arrive. When the MMS is trusted by service providers, the MMS could also be used as service-call proxy. As shown in Figure 15, the service endpoint is not accessed directly, but via the MMS Broker. Therefore, service endpoints do not need to be exposed to the client leading to better security. More on the MMS can be found in the high-level description document of the Maritime Messaging Service[1]. [13]

1 https://maritimeconnectivity.net/docs/MMS_Specification_0.8.3.pdf