



IALA GUIDELINE

G1157 WEB SERVICE BASED S-100 DATA EXCHANGE

Edition 2.0

December 2022

urn: mrn:iala:pub:g1157:ed2.0



DOCUMENT REVISION

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

Date	Details	Approval
December 2020	1 st issue	Council 72
July 2022	Edition 1.1 Editorial corrections.	
December 2022	Edition 2.0 Added additional information on the evaluation of third parties as suitable providers for IP-based communication. Added section on data set management to harmonize data set handling, query processing and subscription and to provide guidance on functional roles in the context of data production and (service) provision.	Council 76

CONTENTS

1. INTRODUCTION	5
1.1. Scope.....	5
1.2. Related documents and relations to these.....	6
1.3. Background	6
2. NORMATIVE COMPONENTS	7
2.1. IP-Based communication in maritime environments	7
2.2. S-100 online data exchange.....	8
2.3. Service architecture And environment.....	11
3. IMPLEMENTATION OF S-100 WEB SERVICES	11
3.1. Web service based S-100 data exchange	11
3.2. Making use of the session concept.....	13
3.3. Authentication mechanisms and encryption to ensure message integrity	14
3.4. Service specification	16
4. DATA SET MANAGEMENT	16
4.1. Functional Roles of Stakeholders.....	16
4.2. Dataset Packaging.....	17
4.3. Guidance on Data Set Management.....	17
4.4. Guidance on Query Processing	18
4.5. Guidance on Service Subscription	19
5. DEFINITIONS.....	19
6. ABBREVIATIONS	19
7. REFERENCES	20

List of Figures

<i>Figure 1</i>	<i>Layer Model for the Abstraction of low-level Communication Technologies.....</i>	<i>7</i>
<i>Figure 2</i>	<i>S-100 Exchange Set Model for exchanging S-100 Datasets with their Metadata.....</i>	<i>9</i>
<i>Figure 3</i>	<i>S-100 Part 14: Data Model to describe a Service</i>	<i>10</i>
<i>Figure 4</i>	<i>Example REST-POST-Request to retrieve Navigational Warnings.....</i>	<i>12</i>
<i>Figure 5</i>	<i>S-100 gml answer to the request shown in Figure 4.</i>	<i>13</i>
<i>Figure 6</i>	<i>Different types of Metadata: Message / Data Object Metadata is bound to a single message, Service Metadata is bound to a complete service instance.....</i>	<i>15</i>
<i>Figure 7</i>	<i>Streamable Exchangeset as (Signature-)Metadata-Container for S100-Datasets.....</i>	<i>15</i>
<i>Figure 1</i>	<i>Layer Model for the Abstraction of low-level Communication Technologies.....</i>	<i>7</i>

CONTENTS

<i>Figure 2</i>	<i>S-100 Exchange Set Model for exchanging S-100 Datasets with their Metadata.....</i>	<i>9</i>
<i>Figure 3</i>	<i>S-100 Part 14: Data Model to describe a Service</i>	<i>10</i>
<i>Figure 4</i>	<i>Example REST-POST-Request to retrieve Navigational Warnings.</i>	<i>12</i>
<i>Figure 5</i>	<i>S-100 gml answer to the request shown in Figure 4.</i>	<i>13</i>
<i>Figure 6</i>	<i>Different types of Metadata: Message / Data Object Metadata is bound to a single message, Service Metadata is bound to a complete service instance.....</i>	<i>15</i>
<i>Figure 7</i>	<i>Streamable Exchangeset as (Signature-)Metadata-Container for S100-Datasets.....</i>	<i>15</i>

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 standardization 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 the 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 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. Annexe A contains 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 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:

1. Provide Maritime Services in digital formats, using international standards.
2. Ensure harmonization and interoperability, by considering international standards and guidance for:
 - Digital maritime services
 - The communications infrastructure
 - System design and cyber security (e.g., availability, integrity, and confidentiality)

1.2. RELATED DOCUMENTS AND RELATIONS TO THESE

This Guideline introduces the topic of Web Service based S-100 data exchange and a list of related documents can be found below. The Guideline provides an overview of available technologies, standards and guidance documents and provides 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 radio communication 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 G1128 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.

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 and 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 (VTS) 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; safety-relevant data in particular 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 has been 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 that 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 Long Term Evolution (LTE) are expected to play an important role for the maritime industry in the future [6]. In addition, satellite providers like Inmarsat are going to launch broadband IP services that are expected to be part of the well-known Global Maritime Distress and Safety System (GMDSS) in the near future [7].

Gathering important information can be complicated and expensive due to multiple sources, each with individual standards, communication channels and technologies. Safety-relevant data like Maritime Safety Information (MSI), Ship-to-Shore reporting, data relating to 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 more readily available and more secure. The layered model of the Internet Protocol (IP) 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 such that data are transported over encrypted protocols using IP networks. It can be applied to any technical maritime service and especially to those exchanging S-100 data.

The Maritime Safety Information (MSI) Service is a GMDSS service for providing information that is needed for safe navigation of vessels [2]. It is a good example of a set of data that needs to be distributed to vessels frequently with a service-bound communication-path and also has specific requirements for message authentication. The service is currently realized, for example, by a specific terrestrial (NAVTEX) as well as a satellite (SafetyNET, SafetyCast) communication channel [3]. There is no established mechanism to ensure the integrity of these messages. A basic

example of how this service can be realized, conforming with this guideline, is presented in Annex A. Please note that the contents in this Guideline are generally applicable. In a similar way, an Inter-VTS Exchange service or a Route Exchange service could be designed with the guidance provided in this document.

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, for example, satellite communication, 3GPP's LTE or IEEE 802.11. 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.

In the maritime industry, IP communication is opening opportunities for new business models, applying more standards, 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 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 method of communication possible. 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.

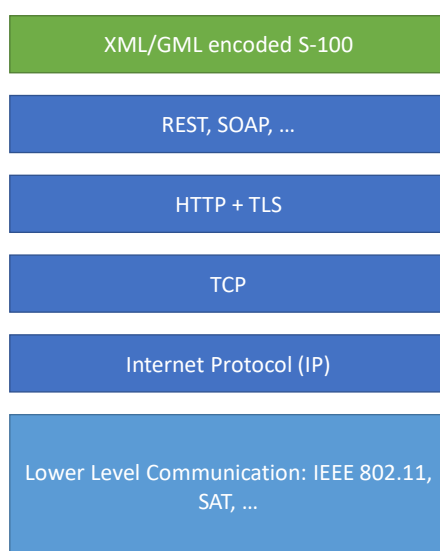


Figure 1 Layer Model for the Abstraction of low-level Communication Technologies.

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. Currently, the development of VDES is trying to address the shortcomings of AIS and also provide a higher-bandwidth communication mechanism. This low-level technology may also be used as a layer below IP.

It should be noted that IP-based communication often (but not necessarily) implies the use of an internet connection offered by an Internet Service Provider (ISP). It should be evaluated, if such an ISP is capable of providing the availability needed for S-100 data transmission, especially those used for warnings or emergency situations. This also applies to other dependencies on third parties and should be evaluated in each new use case for S-100 data 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 2). The metadata is encoded in an XML-file contained in a folder structure together with the S-100-Datasets.

In the case of continuous data exchange, Web Services with publicly available APIs are often utilized. 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 conformal way (see Figure 3). 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.

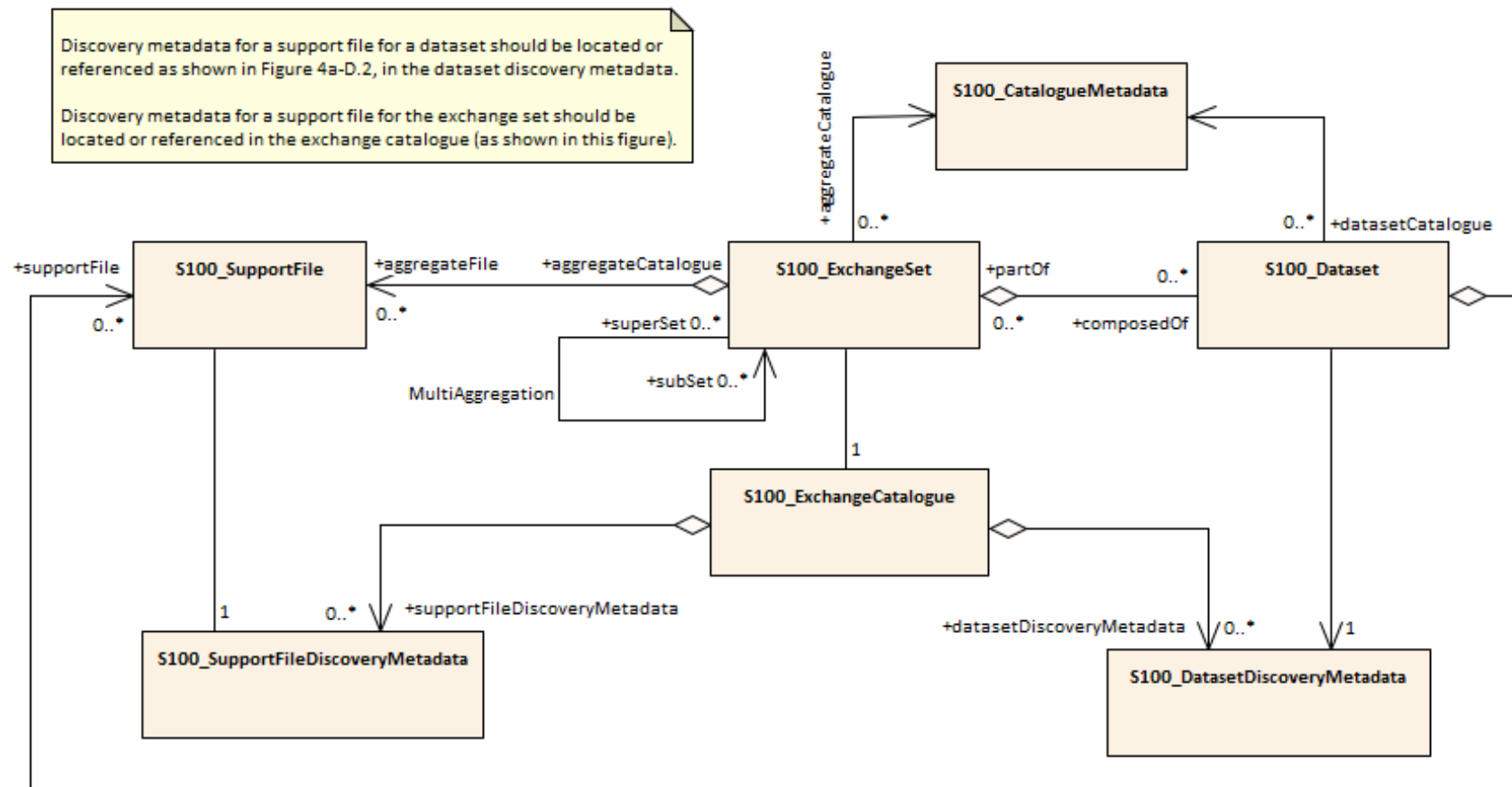


Figure 2 S-100 Exchange Set Model for exchanging S-100 Datasets with their Metadata

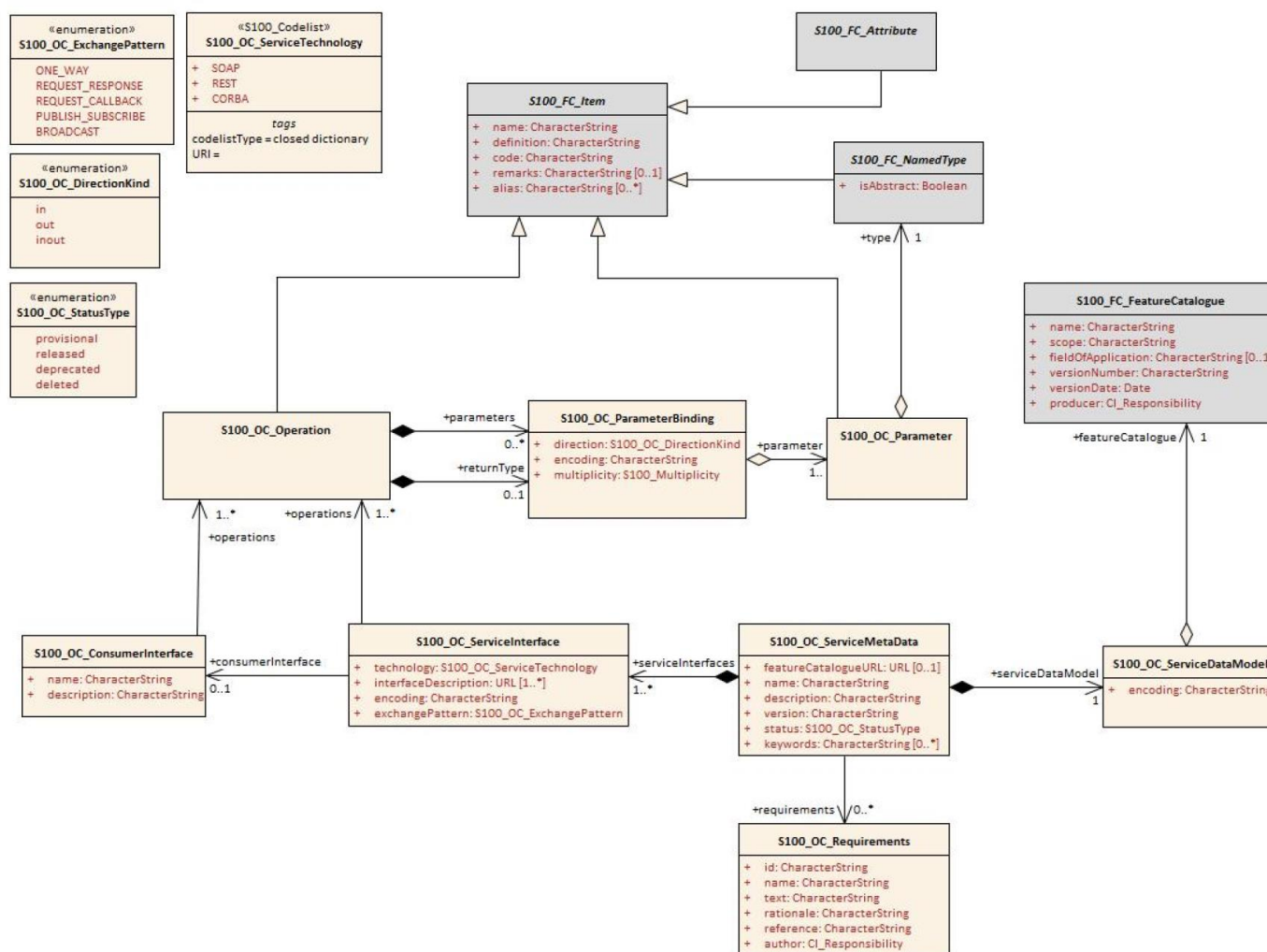


Figure 3 S-100 Part 14: Data Model to describe a Service

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 metadata 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 beforehand. 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-premises, 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 for by a commonly, agreed 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. 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 application 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 examples 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/EPSSG/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/EPSSG/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>
    </generalArea>
  </S124:NWPreamble>
</S124:DataSet>
```

```
<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 radio communication 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 the 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 independently 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 conformal 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. This can help to realize more complex data exchanges processes. 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 ENSURE 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. Another 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 authenticating 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 Ministry of Oceans and Fisheries (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 (typically a vessel at sea) is recommended to update the local certificate store whenever a good connection is available. 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, 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.

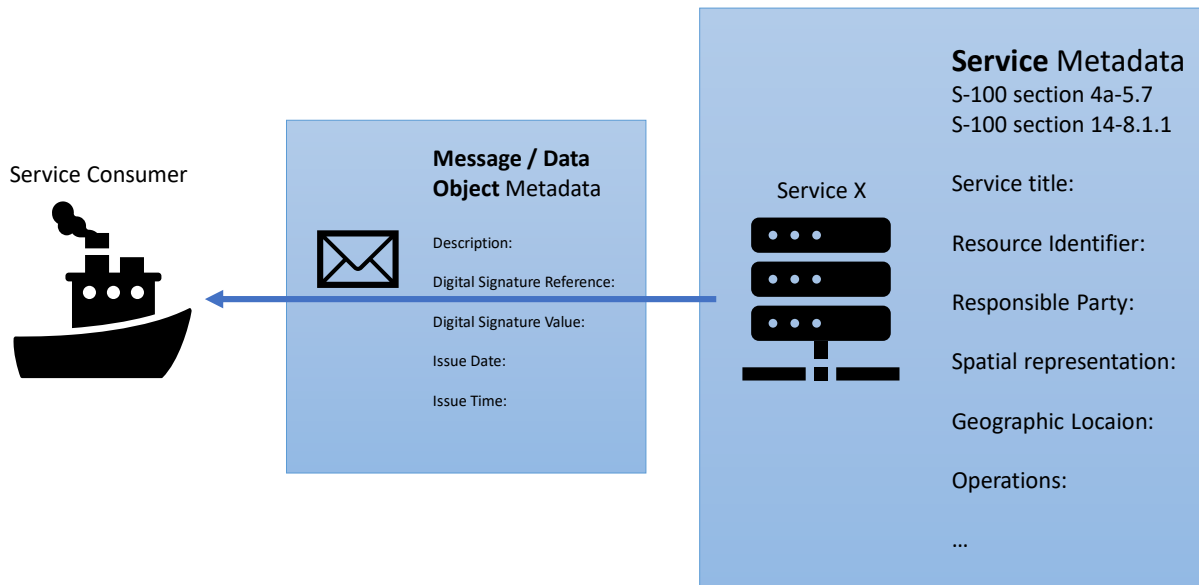


Figure 6 Different types of Metadata: Message / Data Object Metadata is bound to a single message, Service Metadata is bound to a complete service instance.

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.

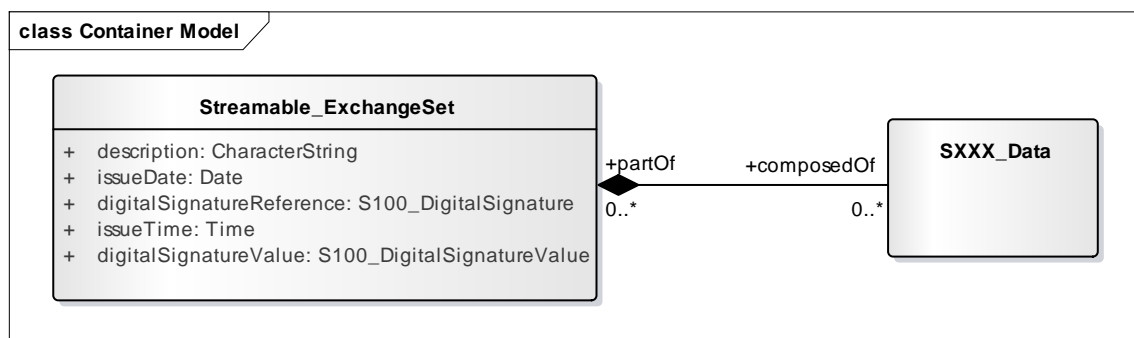


Figure 7 Streamable Exchangeset as (Signature-)Metadata-Container for S100-Datasets.

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. Senders and receivers in the maritime context are usually equipped with GPS (or even resilient PNT services) which can be used if a higher-precision clock is required. 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 product specifications 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 it fulfils all the proposed recommendations. As an additional measure for security, a VPN connection can be used.

3.4. SERVICE SPECIFICATION

As the digitalization of the maritime industry advances rapidly, a whole new set of Maritime Services is expected to be established soon. These systems may bring new challenges of interoperability and harmonization with them. Therefore, IALA is developing and publishing standards, recommendations, and guidelines for the specification of Maritime Services. The IALA Guideline *G1128 Specification of e-Navigation Technical Services* describes a standardized approach for the specification of Maritime Services for 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 *G1128* for the specification and SECOM for the technical realization of Maritime Services.

4. DATA SET MANAGEMENT

A common problem encountered in the development of S-100 services is the handling of S-100 data sets (or data products) in combination with the dynamic communication behaviour of the technical services. The following sections provide guidance on the harmonization of interfaces and implementation of these services regarding S-100 data set handling and the involved stakeholders in these processes.

4.1. FUNCTIONAL ROLES OF STAKEHOLDERS

In the context of technical services, different functional roles are typically required to process data sets and provide them to service consumers. Depending on the use case and local regulations, the following functional roles might be carried by a single or multiple stakeholders:

- *Data producer* The data producer is the original producer of the data and stores the data in its original form in any type of information system for further processing by other entities.

- **Data provider** The data provider gathers data from the data producer and provides them in a standardized data format (typically S-100). The data provider is also responsible for signing the data and held responsible for the content of the data. This is also referred to as the authoritative source of the data.
- **Service provider** The service provider provides a standardized way for the exchange of the data and handles the communication with the service consumer.

For example, during the production of ENC's, a hydrographic office might hire a company (data producer) to survey hydrographic data. The data is then processed by the hydrographic office (data provider) and then released as S-101 data. It is finally distributed by an ENC distributor (service provider) to the end-users. As another example an AtoN authority may establish a new aid and produce the data related to this aid (coordinates, type, colour, lights, etc.), which is published then in an AtoN information service. In this case, the AtoN authority can be perceived as a data producer, data provider and service provider at the same time.

4.2. DATASET PACKAGING

Existing data management systems utilize S-100 data sets to organize entities by specific properties such as their spatial geometry (e.g., all AtoN information of a specific geographical area is contained in a single data set for this area). On the other hand, technical services that make the data available to end-users providing the functionality to query for specific data (which will then be delivered as a “user-defined” data set).

In comparison to the static organization of S-100 data sets in the classical sense, services might need to dynamically package data sets based on query parameters that are supplied by a service consumer. This could be the case if, e.g., data is required only for a specific route or limited geographic area. The dynamic generation of data sets increases efficiency of communication as a service consumer would only receive the requested data. It can also support a less cluttered portrayal of information as irrelevant features are not retrieved. However, this depends on the service and may not be applicable to all services (e.g., ENC provision).

In the case that data sets are *packaged statically*, the service provider only provides original data sets, as received by the data provider.

In the case of *dynamically packaged* data sets, the service provider has the freedom to (re-)package the data sets and provide a user-defined subset of the original data.

Depending on operational, legal, or other requirements, it might not always be possible to provide a service with dynamically packaged data, even though it could be beneficial for the service consumers. In these cases, it could be beneficial to provide statically packaged data in smaller, more easily transmissible units while complying with the framework conditions. Another possibility is to offer a service that uses dynamic packaging as an additional (and optional) service.

The following sections focus on the implementation of procedures for the provision of data by service providers.

4.3. GUIDANCE ON DATA SET MANAGEMENT

The following procedures are suggested for services that utilize *statically packaged* data sets:

- If no query parameters are supplied in a data request by the service consumer, the service should either return all original data sets or an empty response (if querying all data once is not an intended functionality of the service).
- If query parameters are specified, they are interpreted on a per data set basis. This can happen on the metadata level via the S100_DataSetDiscoveryMetadata or via a custom analysis of the data entries. Either way, if there is a match with the metadata or an entry of a dataset, the whole data set must be returned in its original version.

The following procedures are suggested for services that utilize *dynamically packaged* data sets:

The original data at the service provider side may be organized into several statically packaged data sets given by the data provider (e.g., a data set may contain AtoN information for a specific waterway). In the following, these data sets are referred to as original data sets. An original data set typically contains multiple entries or features. To harmonize the handling of dynamically generated and original data sets, the following procedures are suggested:

- If query parameters are supplied that restrict the original data sets to only subsets, a single generated data set with all the matching entries should be provided.
- The derived metadata in a generated data set must be consistent with the data entries.
- The service provider must make sure that the signatures of the data are valid for the generated data sets.
- If not specified otherwise in the service specification, the service consumer is responsible for the management of generated data sets. This means that they need to keep track of which data they already requested and which data may need to be requested when entering a different waterway/area etc.

In addition, it should be considered whether a distinction between an original data set and those generated during runtime by user requests is desirable. A differentiation between the two (if any) can be defined at the technical service specification level, but a harmonized way of dealing with them is strongly advised. For example, a specific keyword in the S-100 data set file identifier or title could be employed.

Services might also provide different data based on the identity of the consumer (e.g., VTS information tailored to a specific type of ship). In these cases, it should be clearly stated in the service specification on what basis this decision is made.

4.4. GUIDANCE ON QUERY PROCESSING

To avoid confusion regarding the results of data queries, the following procedures for the interpretation of query parameters are proposed:

- If not defined otherwise in the service specification, a service should return all entries/data sets that fulfil a supplied filter criterion.
- If not defined otherwise in the service specification, a service should return all entries/data sets that *interact* with a supplied geometry parameter. This refers to all entries with geometry that are not disjoint with the provided filter geometry (cf. OGC 09-026r2, section 7.8.3).
- Dataset entries/data sets may only be valid in a specific time range. If this is the case, and it is not specified otherwise in the service specification
 - a service should only provide those entries/data sets, which are valid after a *validFrom* parameter. In the case that data entries/data sets are valid until cancelled by another entry/data set, all of those that were valid after *validFrom* and were not cancelled should be returned. A *validFrom* parameter in the future will only be accepted if data entries/data sets have explicit values for their validity period.
 - a service should only provide those entries/data sets, which are valid till a *validTo* parameter. In the case that data entries/data sets are valid until cancelled by another entry/data set, a *validTo* parameter will not be accepted.
- Dataset entries may only be valid in a specific numeric range. If this is the case, and it is not specified otherwise in the service specification

- a service should only provide those entries in a generated data set, which have values larger than the start value of the range.
- a service should only provide those entries in a generated data set, which have values smaller than the end value of the range.
- If filtering data by specific S-XXX data models, query parameters must use the format “SXXX” as defined in SECOM, section 5.6.7.

4.5. GUIDANCE ON SERVICE SUBSCRIPTION

Several services need to provide data that is continuously extended, modified, or removed. The following procedures should harmonize the way services deal with changes in data sets.

- If a service consumer subscribes to a service, they are responsible to pull the current version of the required data. The subscription only provides updates when the queried data sets change.
- The service provider must keep track of the query parameters of a subscription request and only provide updates to data entries/data sets that match the subscription query.

The following procedures are proposed for services that utilize *dynamically packaged* data sets:

- Updates in data sets are often done to a limited number of entries. This means that anytime data entries are updated, a data set (containing only the updated entries) is generated and sent to the subscribers of those entries.
- Deletions of data entries should be made available to the service consumers that have subscribed to a relevant dataset. Therefore, unless specified otherwise in the service specification, the employed data products should support a way of identifying deleted data entries.

5. DEFINITIONS

The definitions of terms used in this Guideline can be found in the *International Dictionary of Marine Aids to Navigation* (IALA Dictionary) and were checked as correct at the time of going to print. Where conflict arises, the IALA Dictionary should be considered as the authoritative source of definitions used in IALA documents.

6. ABBREVIATIONS

3GPP	3rd Generation Partnership Project
AIS	Automatic Identification System
API	Application Programming Interface
AtoN	Marine Aids to Navigation
CA	Certification Authority
GMDSS	Global Maritime Distress and Safety System
GML	Geography Markup Language
GPS	Global Positioning System
HTTP(S)	Hypertext Transfer Protocol (Secure)
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IHO	International Hydrographic Organization



IMO	International Maritime Organization
IP	Internet Protocol
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
LEO	Low Earth Orbit
LTE	Long Term Evolution
MASS	Maritime Autonomous Surface Ship
MCP	Maritime Connectivity Platform
MIR	Maritime Identity Registry (MCP)
MMS	Maritime Messaging Service (MMS)
MOF	Ministry of Ocean and Fisheries (Korea)
MRN	Maritime Resource Name
MSI	Maritime Safety Information
MSR	Maritime Service Registry (MCP)
NAVTEX	Navigational Text Messages
OSI	Open Systems Interconnection
PKI	Public Key Infrastructure
PNT	Position Navigation Timing
REST	Representational State Transfer
SECOM	Secure exchange and communication of S-100 based products (IEC 63173-2)
SOA	Service-oriented Architecture
SOAP	Simple Object Access Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VDES	VHF Data Exchange System
VHF	Very high frequency
VTs	Vessel traffic service
XML	Extensible Markup Language

7. REFERENCES

Informative references

- [1] F. Bekkadal, 'Emerging maritime communications technologies', Oct. 2009.
- [2] IMO 'Resolution A.705(17) - Promulgation of Maritime Safety Information'. International Maritime Organization, 06-Nov-1991.
- [3] IHO. 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] 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] IHO. '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'.

Normative references

- [14] IHO S-100 Standard v. 4.0.0
- [15] IALA. Guideline G1128 Specification of e-Navigation Technical Services
- [16] IEC. 63173-2 ED1: Maritime navigation and radio communication equipment and systems – Data interface – Part 2: Secure exchange and communication of S-100 based products (SECOM)
- [17] 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
- [18] IMO. MSC.1/Circ.1610 Initial descriptions of maritime services in the context of e-navigation
- [19] ISO/IEC. 7491- Open Systems Interconnection – Basic Reference Model
- [20] OAuth. OAuth 2.0 Framework RFC 6749

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

This section provides an example of how to implement a reliable and efficient IP based service following this guideline. S-124/MSI is presented because of its illustrative nature as a maritime service. It requires the realization of near-real-time message delivery, usage of digital signatures for message authentication, enables the logical breakdown of requested data into geographical areas, has an easy to understand dynamic behaviour, is widely known to the public and an existent realization (NAVTEX / SafetyNET) is available for comparison. However, the example in this section only depicts a simplified version of the service for better understanding and is not intended to be applied to real-world use cases.

A.1. NORMATIVE BACKGROUND

A.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 quickly as possible. It is also used for the distribution of Maritime Safety Information (MSI) and was introduced by the SOLAS Convention in 1992.

The GMDSS uses several different communication methods realized by satellite or terrestrial services. Radar transponders and emergency position indicating radio beacons (EPIRBs) 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.

A.1.2. MSI

As defined by Resolution A.705 of 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 A1: 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]

A.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 Navigational Warnings with a S-100 conforming Data Model. Its intention is to describe and encode Navigational Warning data for use in navigation. The standard aligns to its usage in the 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. However, S-124 is not limited to these channels and it is also expected to be available via Web Services [11].

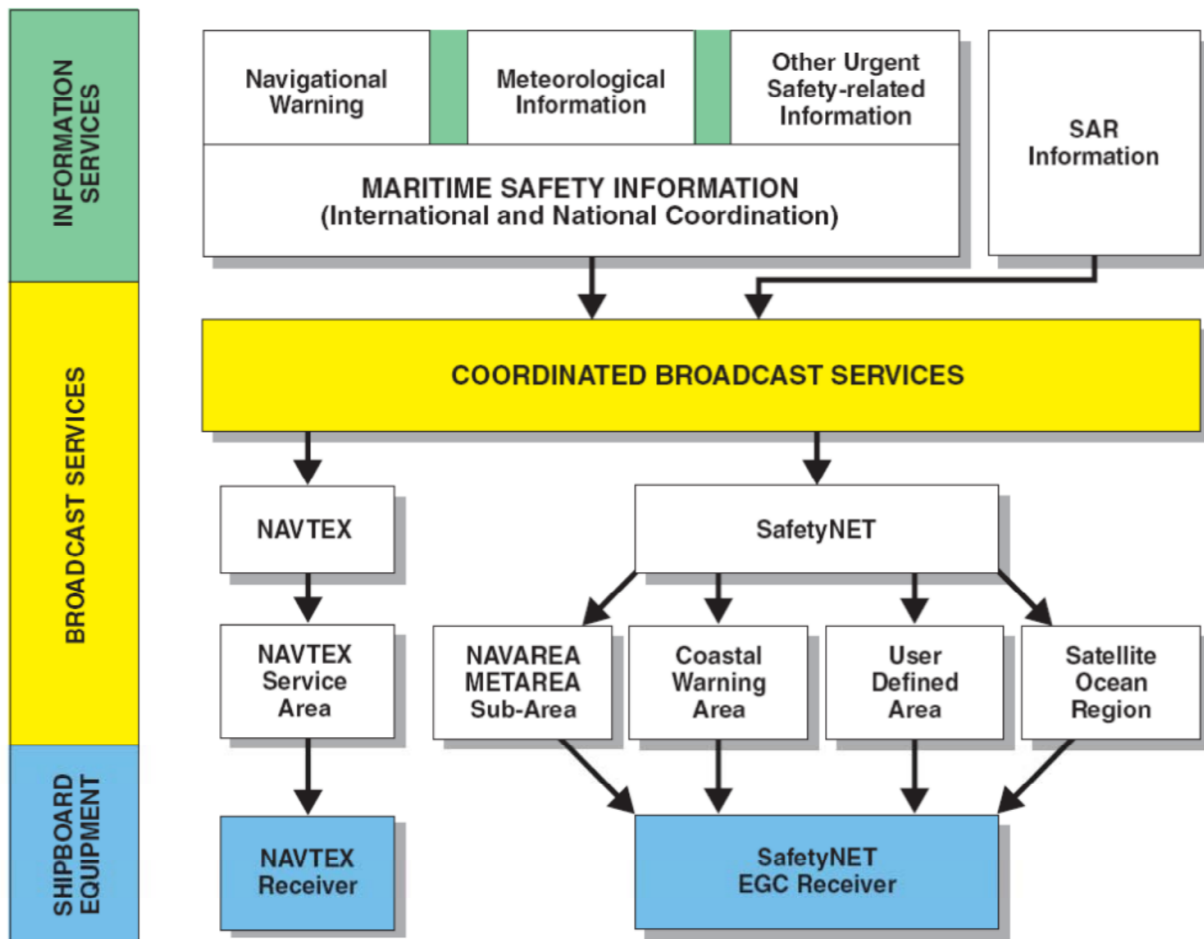


Figure A1: Today's Distribution of the MSI - Information, Broadcast Services and Shipboard Equipment [3]

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

The service specification is an instance of the S-100 Service Data Model as introduced in section 2.2. Please note, that this is 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 experimental Web Services for the distribution of navigational warnings already have been established (Baltic/Pacific Web, Danish Maritime Authority).

Figure A2 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*.

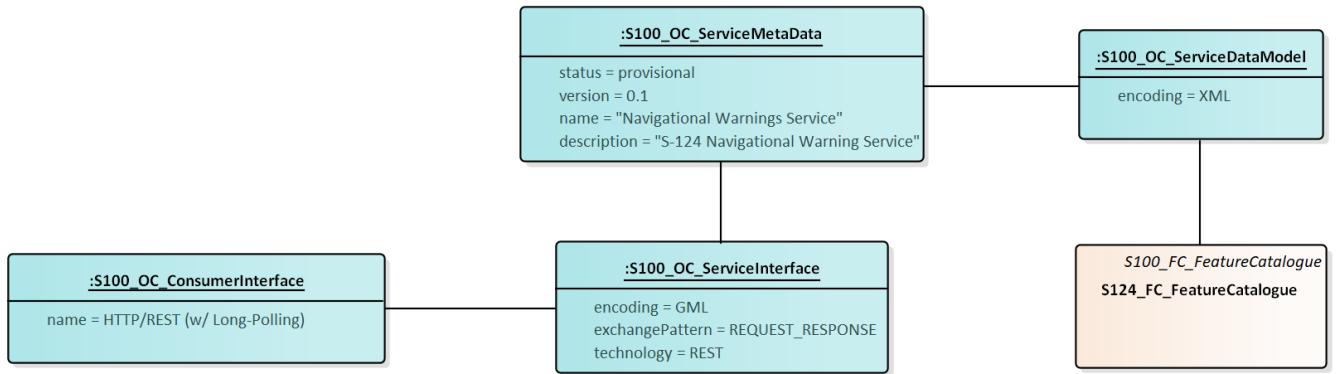


Figure A2: Service Specification of the Navigational Warnings Service.

The operations of the service, which are also instances of the Service Data Model are illustrated in Figure A3. For demonstration purposes only a subset of the proposed operations in the *S-124 Standard* (section 11.2.2) is implemented.

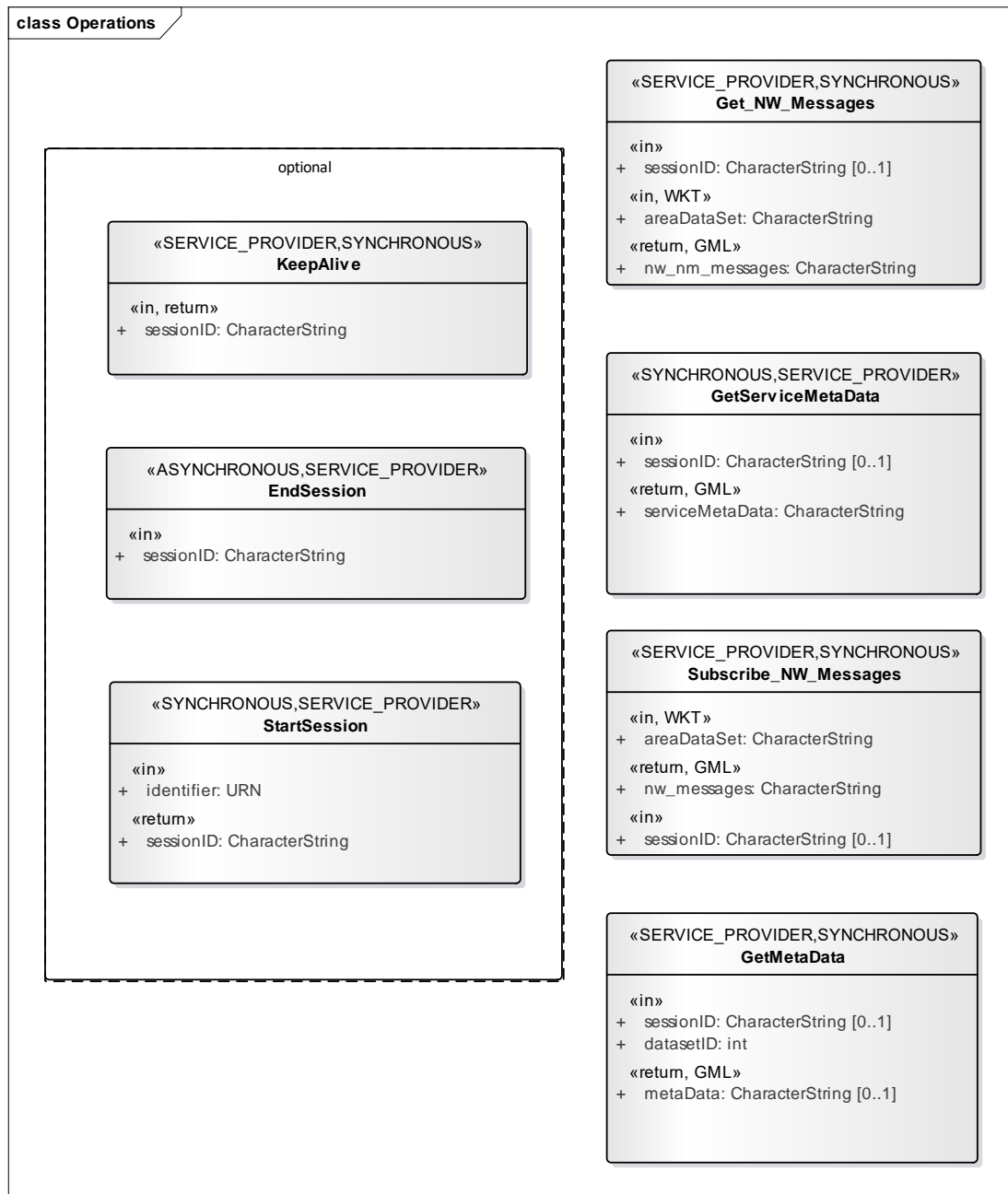


Figure A3: Available Operations of the Navigational Warning Service.

The operations *StartSession*, *EndSession*, *KeepAlive* and *GetMetaData* are the minimal requirements for a S-100 conformal 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).



A.2.1. 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.

A.2.2. COMMUNICATION PATTERNS

The described operations allow two communication patterns between service and consumer. The first pattern (shown in Figure A4) 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 A5). 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 notified immediately 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.

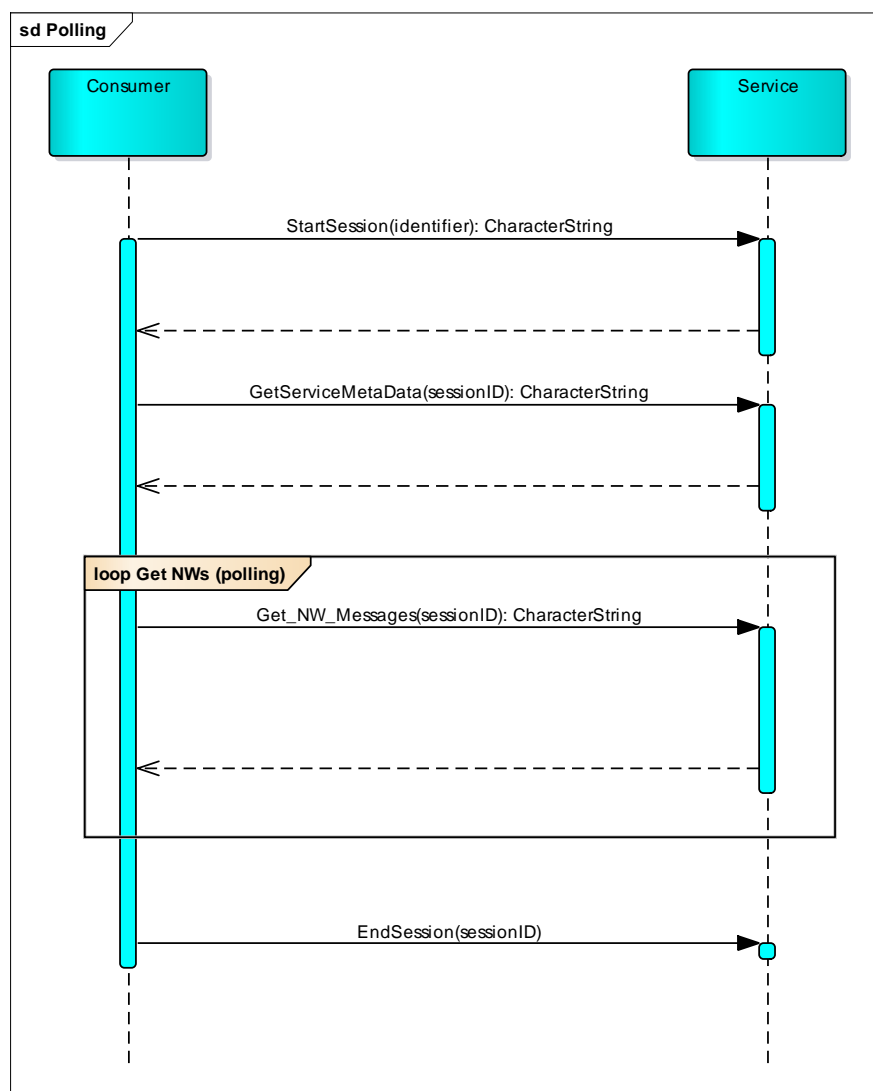


Figure A4: Polling of the Navigational Warning Messages.

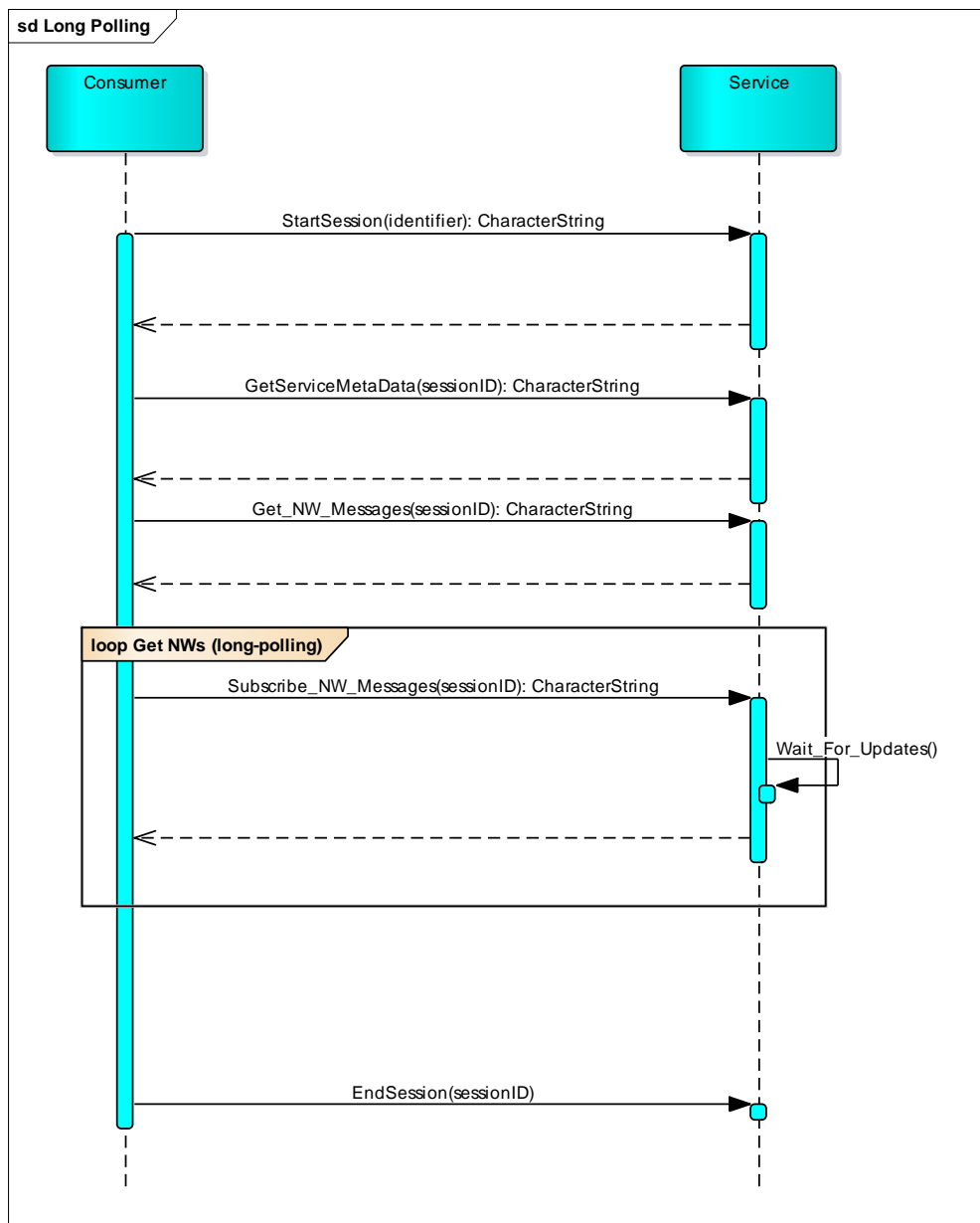


Figure A5: Long-Polling of the Navigational Warning Messages.

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.

A.3. SERVICE SPECIFICATION OF THE TECHNICAL SERVICE

The MSI technical service is specified in the following form according to *G1128*:

A.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

A.3.2. OPERATIONAL CONTEXT

For a high-level description of the service see annex A, section A.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.

A.3.3. SERVICE OVERVIEW

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

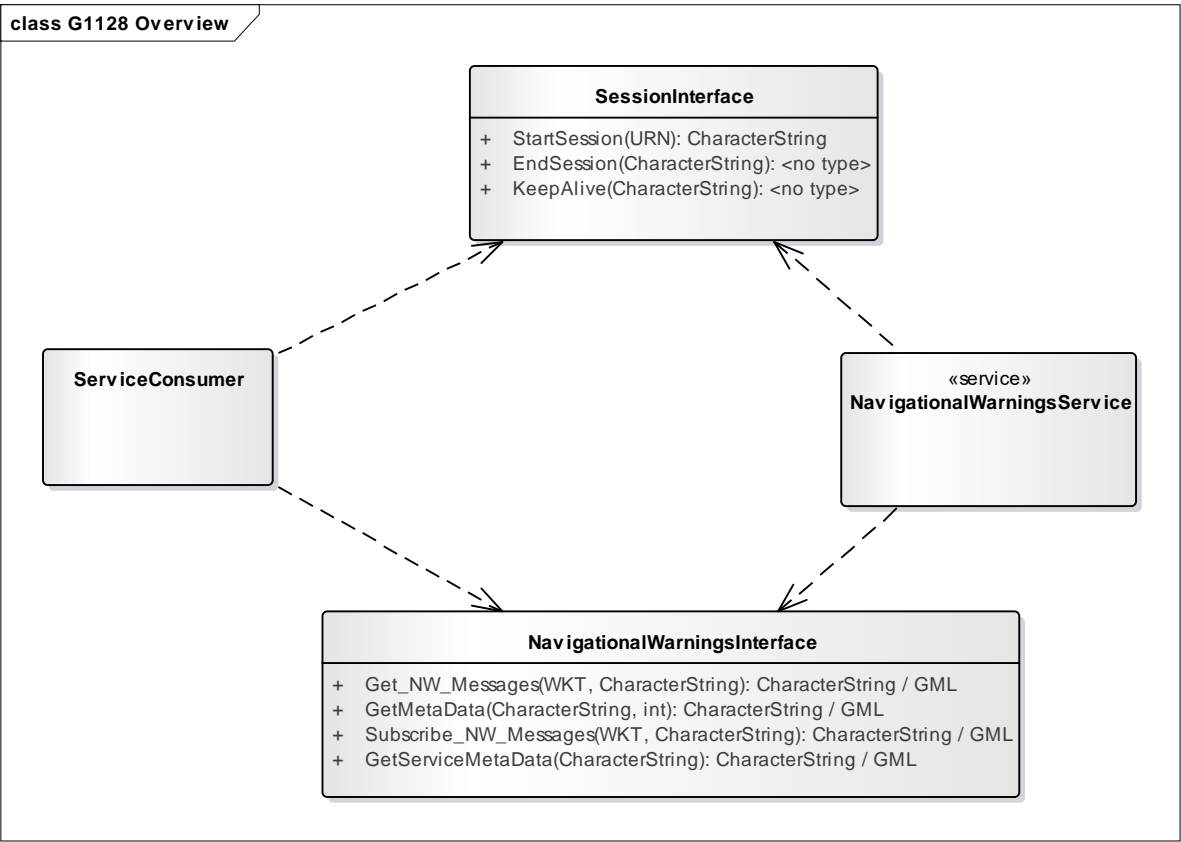


Figure A6: Navigational Warnings Service Interface Definition Diagram.

Table A 1 Service Operation by Service Interface

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

A.3.4. SERVICE DATA MODEL

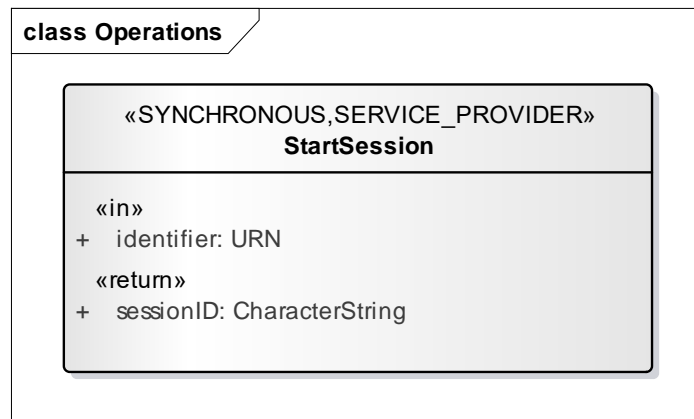
The service uses an external data model, which is described by the S-124 standard. The recommended *Steamable_ExchangeSet* is used as an extension of this data model to transport digital signature information.

A.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 minimize the traffic between service and consumer.

OPERATION StartSession

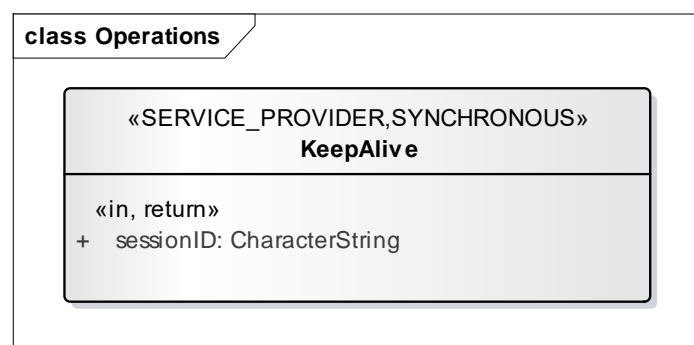


OPERATION FUNCTIONALITY: Starts a new session.

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

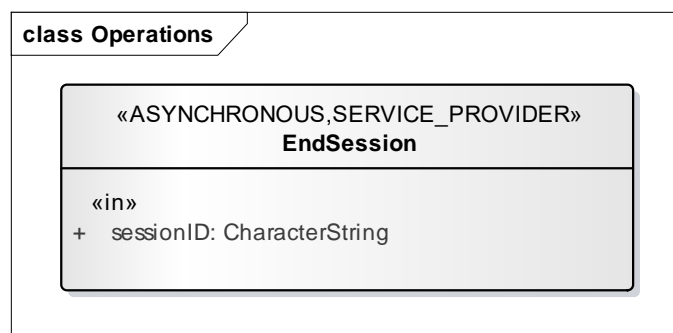


OPERATION FUNCTIONALITY: Keeps the current session alive. The service session time-out is reset.

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.

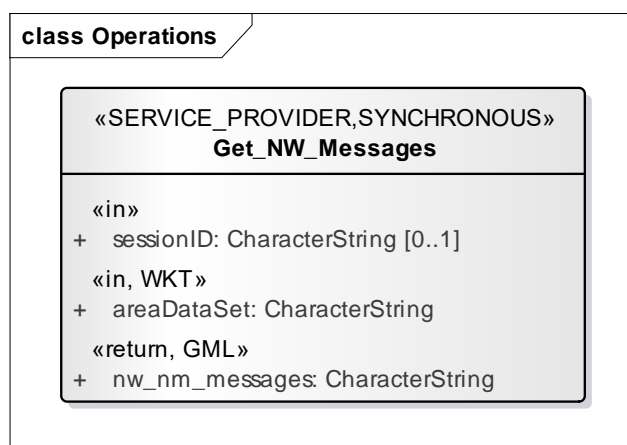
OPERATION PARAMETERS:

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



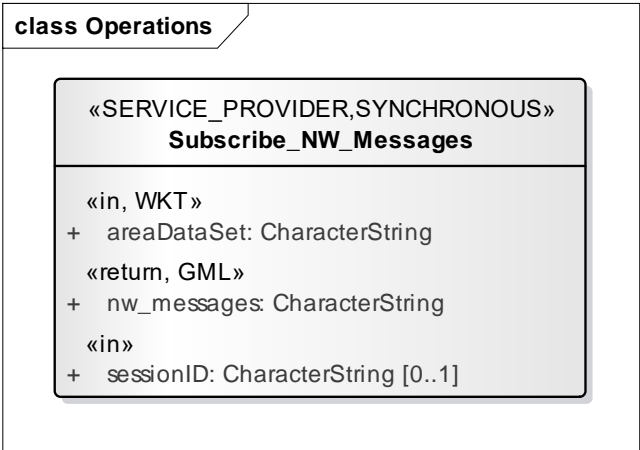
OPERATION FUNCTIONALITY: Returns a list of Navigational Warnings for a specified area.

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

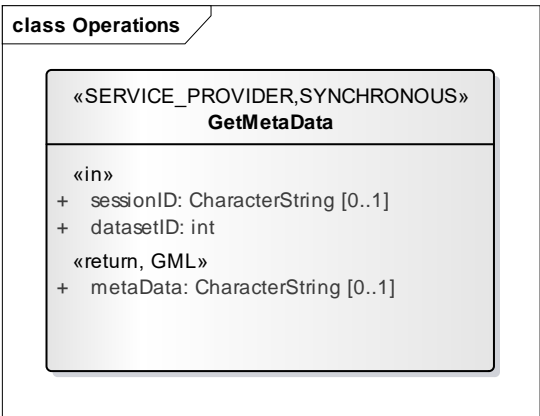


OPERATION FUNCTIONALITY: Subscription to updates on Navigational Warnings.

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

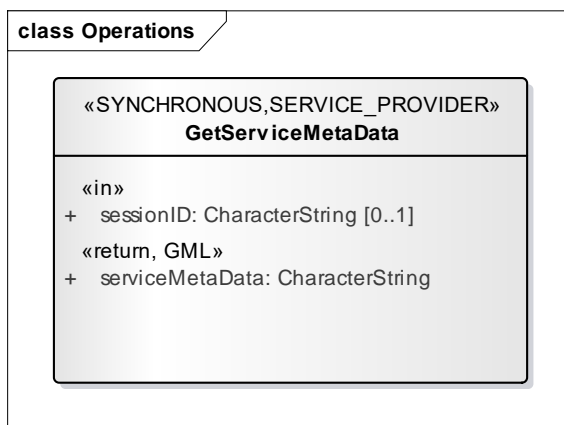


OPERATION FUNCTIONALITY: Provides Metadata for a dataset with a specified ID.

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.

A.3.6. SERVICE DYNAMIC BEHAVIOUR

The service dynamic behaviour is described in section A.2.2 (“Communication Patterns”).

ANNEX B USING THE MARITIME CONNECTIVITY PLATFORM

B.1. INTRODUCTION

The goal of the Maritime Connectivity Platform (MCP) is to allow information to 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 comprises 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.

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 OAUTH 2.0 and OpenID Connect standards.

B.2. USING MMS

The Maritime Messaging Service (MMS) is an information broker as part of the Maritime Connectivity Platform (MCP) 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 geo-casting of messages. Furthermore, the use of MRNs and the architecture of the MMS solve the problem of switching between different communication technologies and allow 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 B1 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. Ex) Hello World!		

Figure B1: Layout of an MMS-Message [13].

As every message is directly addressed to its receiver, the Web Service 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 B2. Specialized parameters for different operations can be included in the content part of the message.

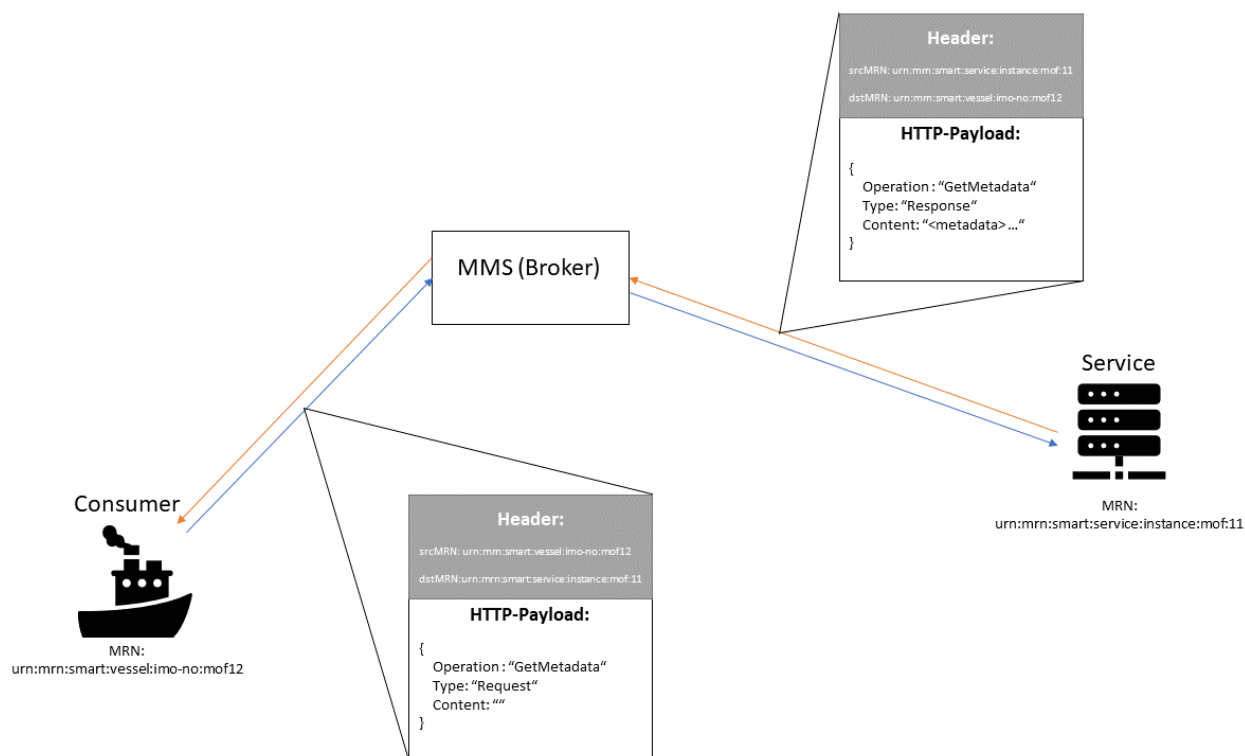


Figure B2: Simple exchange of messages using the MMS with a json-wrapper for the operations and types.

This usage of the MMS results in some changes that must be made to the methodology proposed in section **Erreur ! Source du renvoi introuvable.** and A.2.2 of ANNEX A. Since the consumers can now be identified by their MRN, which is known to the service, the session operations are no longer mandatory in the MMS setup. However, these commands can be kept for keeping track of consumers' interest in receiving 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 B2, 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 Service¹ [13].

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