Towards Secure IP-Communication in the Maritime Industry*

Using the Example of Maritime Safety Information

Julius Möller†
University of Oldenburg, Oldenburg, Germany, julius.moeller@uni-oldenburg.de

Sibylle Fröschle
OFFIS - Institute for Information Technology, Oldenburg, Germany, sibylle.froeschle@offis.de

Axel Hahn
University of Oldenburg, Oldenburg, Germany, axel.hahn@uni-oldenburg.de

* Place the footnote text for the title (if applicable) here.

† Place the footnote text for the author (if applicable) here.

ABSTRACT

…

KEYWORDS

…

1 Introduction

The maritime industry is a big sector of today's economy. Thousands of vessels are constantly underway in inland waterways, coastal waters or the open sea. To sail within their environment safely there is a continuous need for communication. This could be for example communication with surrounding vessels for collision avoidance, contacting vessel traffic 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]. Often the way of obtaining the above-mentioned information can also 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 unsecure communication methods, in which the validity and the propriety of the data cannot be verified.

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 channels [3]. Actually there is no established mechanism to ensure cyber security.

Contrarily, a development of new communication technologies for the maritime sector could be observed in the past years: IP-based 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 will be part of the well-known **Global Maritime Distress and Safety System** (GMDSS) in the near future [7].

The fact that a set of important information can only be obtained from a lot of different sources with their own standards, channels and technologies makes gathering of information complicated and also expensive. Especially safety-relevant data like the MSI 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.

This paper demonstrates who to distribute information in the maritime environment using secure IP-based communication. The layer model of the internet protocol opens new possibilities for a separation of services and communication channel. A concept for distributing navigational warnings as a part of MSI over a secure IP-connection will be shown here.

2 Normative Background

2.1 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 systems intention 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 providers like Inmarsat is a recent development and opens the possibilities to reach ships in distant locations via an IP-connection [7]. As a part of GMDSS these services must fulfill the approved safety and security standards regulated by the SOLAS Convention too.

2.2 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 1: The MSI is sent to an abstraction layer of the available broadcast services. 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]

2.3 S-100 Standards and S-124

S-100 short introduction…

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 at its usage in the above describe mediums (NAVTEX and SafetyNET). [10]

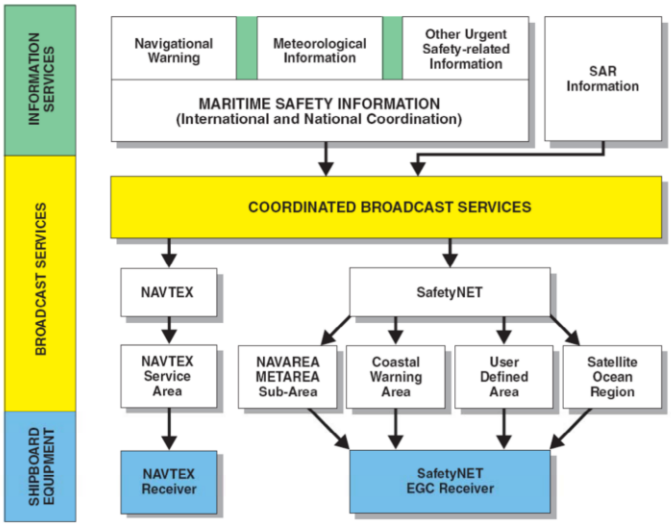

Figure 1: Distribution of the MSI - Information, Broadcast Services and Shipboard Equipment [3]

2.4 S-100 Online Data Exchange

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.

The S-100 Standard suggests 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).

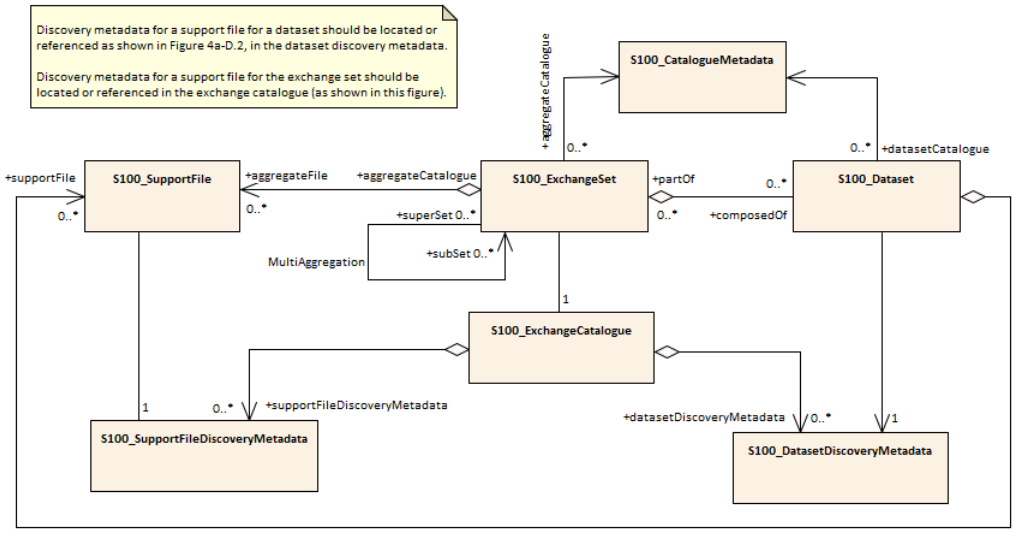

Figure 2: S100 Exchange Set Model for exchanging S100 Datasets with their Metadata

When it comes to continuous data exchange nowadays, Webservices with publicly available APIs are often utilized for interchanging information. Webservice Technologies like REST or SOAP allow a fine-grained and efficient exchange of information. For this reason, Part 14 of the S-100 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.

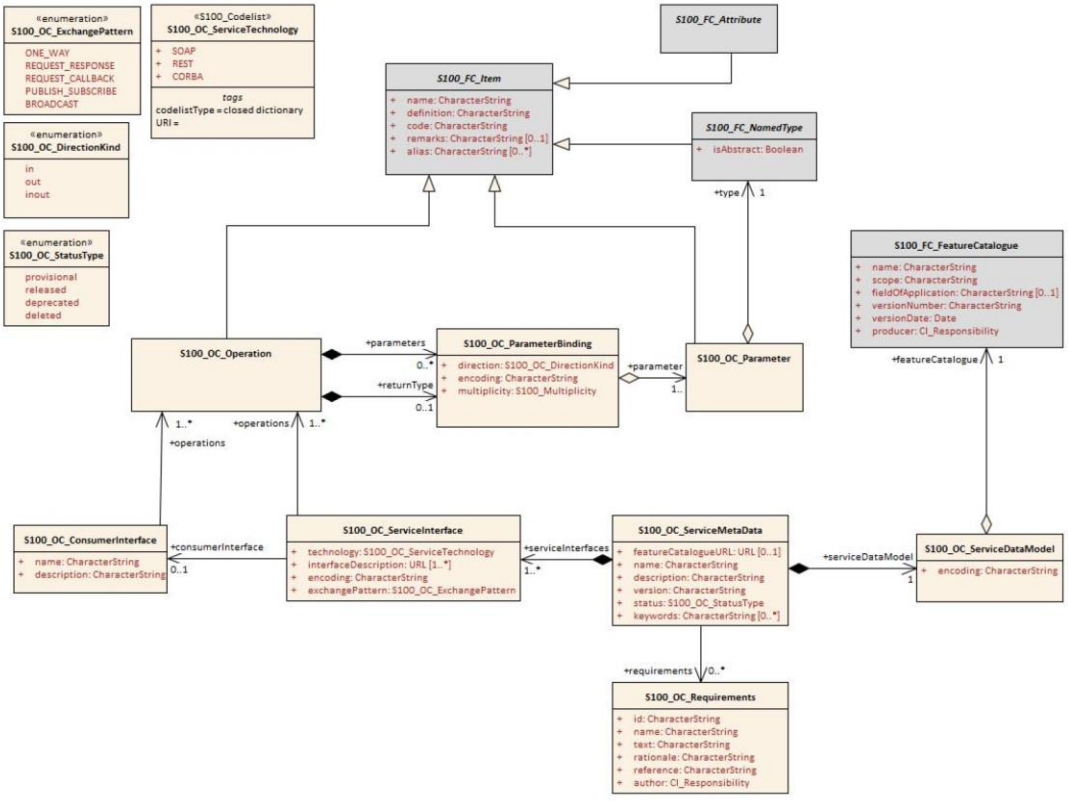

Figure 3: S-100 Part 14: Data Model to describe a Service

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 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 service has the possibility to reduce the amount of 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 the Service: Firstly, if Metadata needs to be added to the datasets, 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.

2.5 Maritime Connectivity Platform

MCP / Web-based communication, Identity Registry

3 Concept

3.1 IP-Technology in Maritime Environments

The stack of communication technologies in the maritime industry is comprehensive. Technologies like LTE, VHF, AIS, Wi-Fi, 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 the OSI layer-model). Different Technologies that are already used in maritime applications can provide the underlaying layers of the IP-Protocol. Satellite communication, LTE or 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.

With the new developments in IP-providing services like Inmarsat's Fleet One IP broadband communication with an exhaustive availability or LTE with a very high bandwidth, 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.

Also, upcoming issues with cyber-security are currently relevant (see [11]). Additionally, some maritime technologies, such as AIS are completely open and can be misused easily. In contrast to that, the layer model of IP-based communication enables security mechanisms on several different levels and therefore solves the problem of security issues in a much cleaner way. The IP-protocol is not the answer to all security related issues, but it provides the possibilities to create secure communication channels and is a technology that needs to be discussed in the

maritime industry in the future. The MSI is a good example for a service that can be deployed as an IP-based service.

3.2 Navigational Warnings Service

The technology that is proposed in this paper should be entitled to offer a lightweight broadcasting service for Navigational Warnings over a secure IP connection as a proof-of-concept. Additional considerations about the realization of such a service are discussed in section 4.

Currently, SafetyNET and NAVTEX use geographic Broadcasts to deliver Navigational warnings [3]. The distribution of the messages is realized by directional satellite signals or local terrestrial broadcasts. The idea of Geo-Broadcasts should remain in place when it comes to an IP-based solution. As broadcasting over IP is not supported in public networks, the broadcast idea needs to be emulated in a different way: The IP communication needs to be established by the consumer of the Navigational warnings. The Navigational Warning Service can then start to communicate and broadcast the information to all registered consumers. The most basic concept to realize such a mechanism is to deploy a set of local service providers, which are bound to geographical areas. The IP-addresses/hostnames of these services need to be publicly available to the consumers. When a consumer wants to subscribe to Navigational Warnings for a specific area, a simple table look-up can provide the hostname of the service provider for that area (see Figure 4).

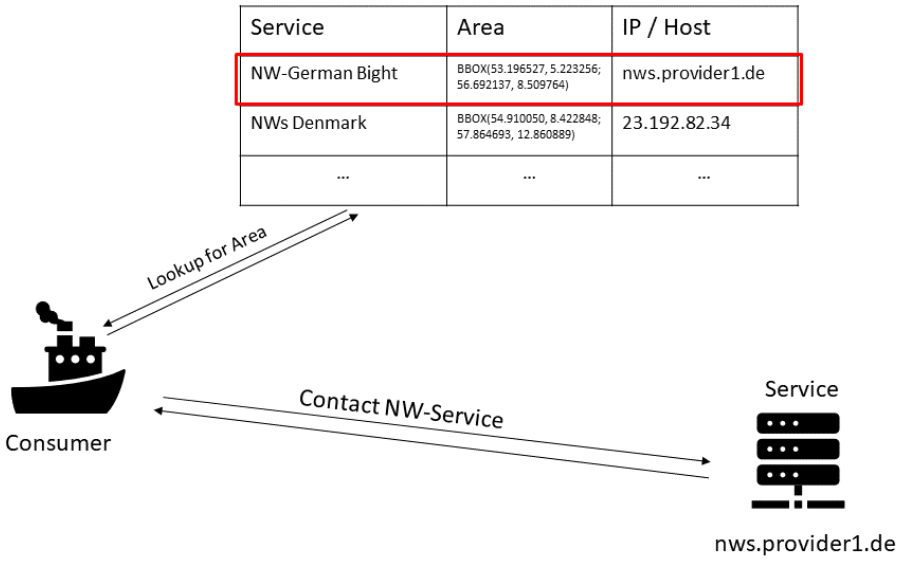

Figure 4: Table Look-Up of Navigational Warning Service Providers by Geographic Area

To secure the exchange of the Navigational Warnings, two possibilities are imaginable: Either each navigational warning dataset is signed by a trustworthy

organization or the communication itself between consumer and service is encrypted. Both these solutions require the existence of a Public Key Infrastructure including a certificate authority (CA) that issues certificates for the participants of the proposed communication pattern. The service lookup-table can be extended with a list of CAs that are trusted by the consumer. The advantage of the IP-protocol here is the abstraction of different communication layers and the availability of many different technologies for securing the communication: The TLS Protocol is very common in Webservice communication and can also be implemented in the presented scenario. Additionally, the Digital Signature Algorithm (DSA) can be used on a second layer to generate a signature for any Navigational Warning dataset that can be verified later by the consumer to ensure the message was created by a trustworthy service provider.

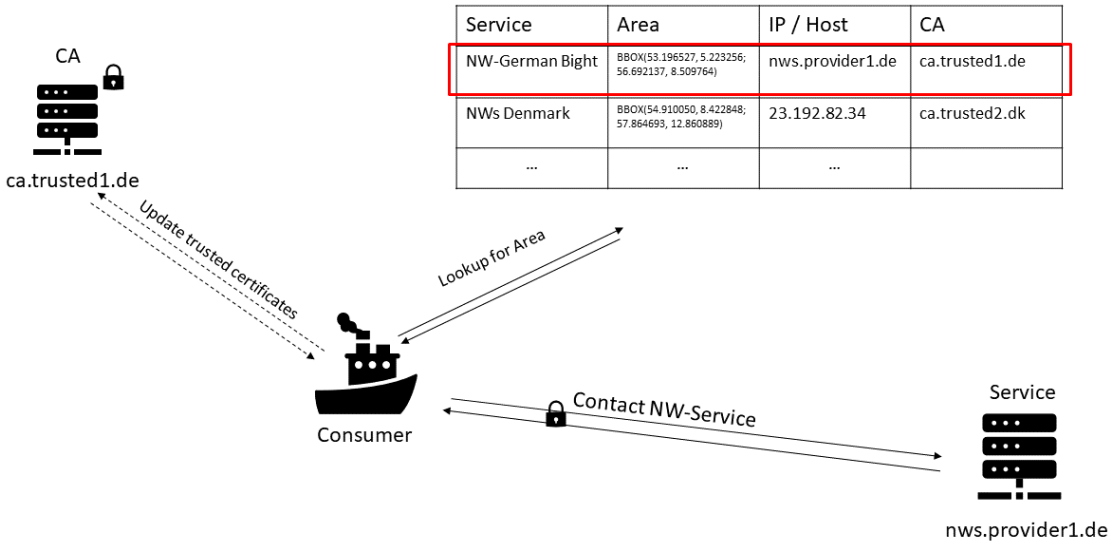

Figure 5: Extension of the concept with Certificate Authorities to secure the exchange of Navigational Warnings.

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.

3.3 S-124 as WebService

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 2.4. Figure 6 shows the instantiation of the 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 data model of the service can be described by the (XML-) Feature Catalogue of the S-124 Standard.

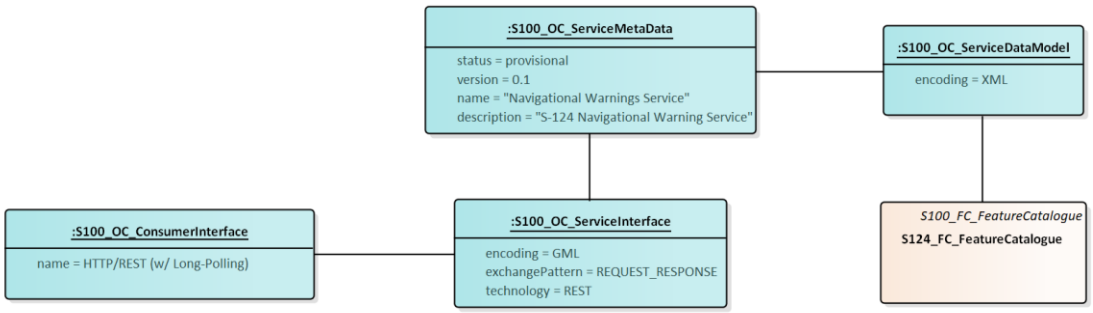

Figure 6: Service Specification of the Navigational Warnings Service

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:

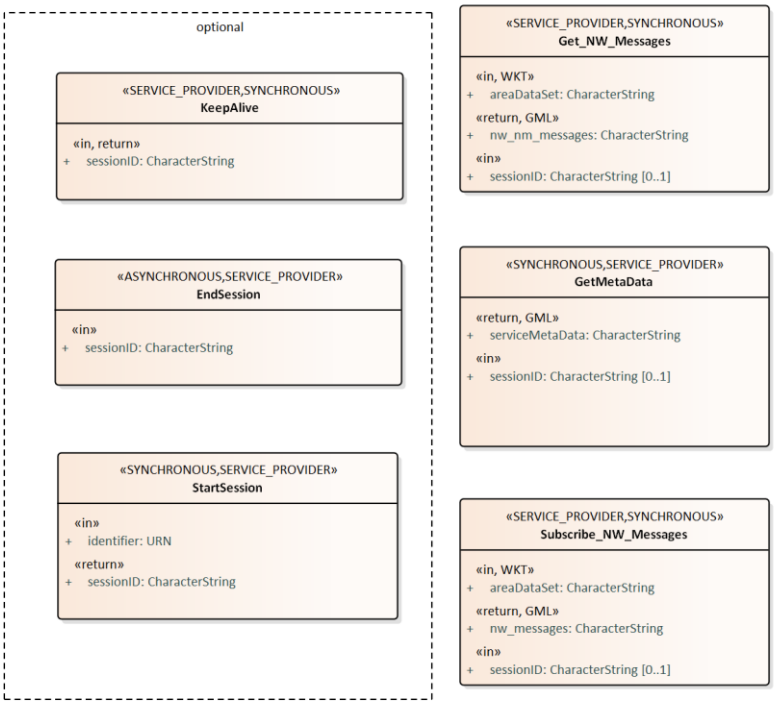

Figure 7: Available Operations of the Navigational Warning Service

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.

Note that GetMetaData returns the ServiceMetaData instance, defined in Figure 6. Hence, GetMetaData is the only Command that must be known to the consumer to discover the services capabilities.

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 area definition	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 8) is a simple polling pattern. After starting the session and transmitting the metadata, the consumer can use the Get_NW_Messages command to receive all navigational warnings. 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 client repeats the Get_NW_Messages command in fixed periods.

The second possible pattern is the long-polling pattern (shown in Figure 9). After opening the session and receiving the 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.

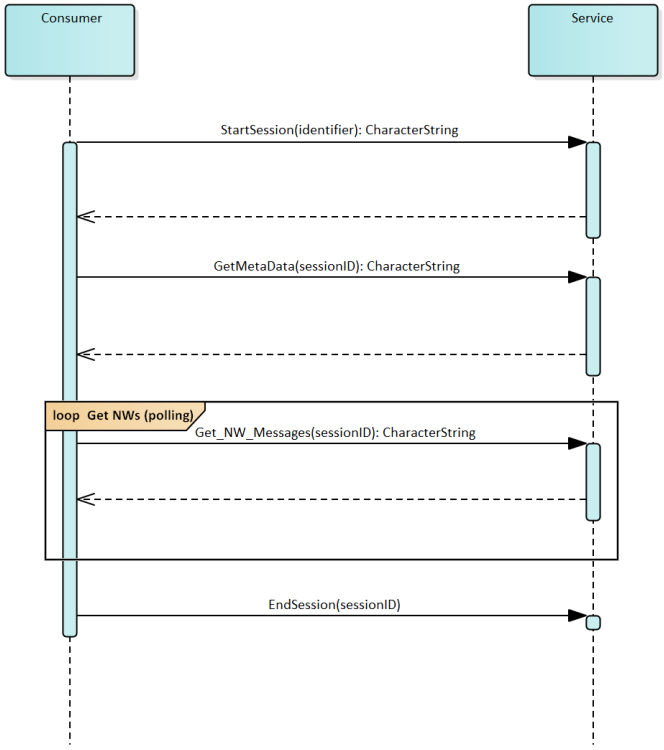

Figure 8: Polling of the Navigational Warning Messages

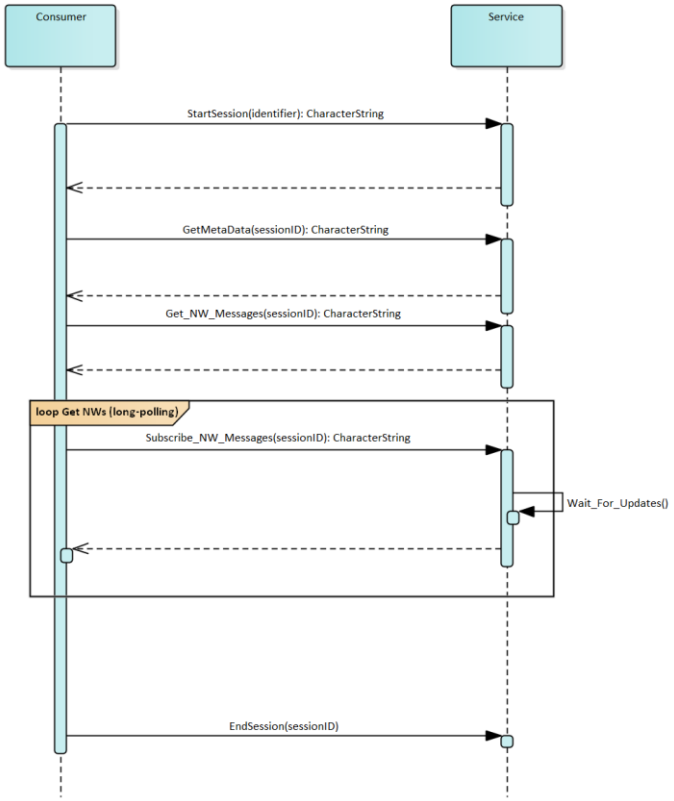

Figure 9: Long-Polling of the Navigational Warning Messages

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) 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.

3.4 Security

As pointed out in section 2.4, if support metadata needs to be transmitted with each dataset, additional changes need to be made to the transmitted data. In this paper, two possibilities will be proposed for that.

The first solution is shown in Figure 10: The Streamable_Exchange set complements the ServiceMetaData with dataset-specific information such as a digital signature that is directly derived from the dataset and therefore needs to be generated for each dataset 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 S124-Standard.

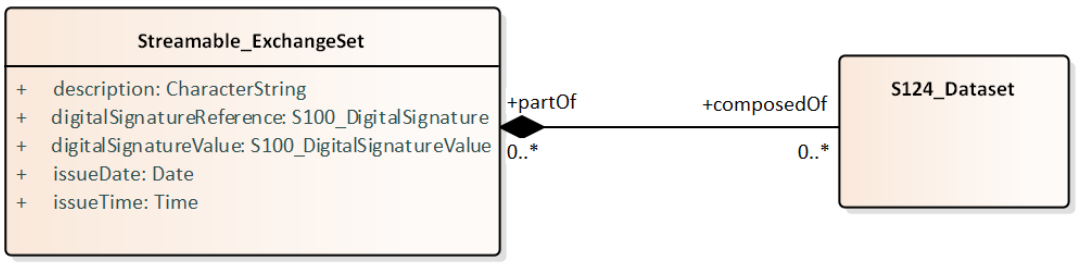

Figure 10: Streamable Exchangeset as (Signature-)Metadata-Container for S124-Datasets.

The second solution is a little bit more specific: Modifying the Data Model of the S-124 can also be a way to store additional metadata. The S-124 class S124_NWPreamble (see Figure 11) is defined to hold the meta-information of the dataset encapsulating the navigational warning. This class could be extended with additional attributes such as the digitalSignatureValue. This seems to be a less flexible solution because the Data Model of S-124 itself would have to be modified.

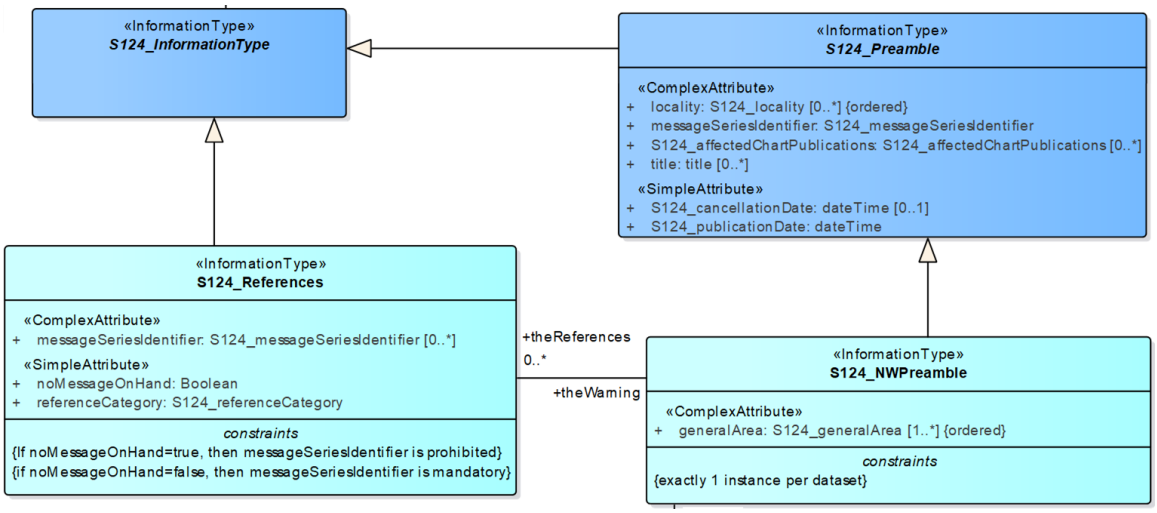

Figure 11: S-124 Datamodel for Navigational Warning Metadata

3.5 Example: Get_NW_Messages

The following communication between service and consumer shows an example for the exchange of navigational warnings information. The container approach from section 3.4 was used to encapsulate the digital signature. The consumer sends a POST request to the REST-API of the service (Figure 12) and retrieves a S100-gml response (Figure 13), describing navigational warnings in the requested area.

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

<areaDataSet>
        POLYGON((6.77490234375 53.51144930919295,8.14697265625
53.63090618774243,8.013916015625 53.99616127810512,6.6845703125
53.887507349745036,6.77490234375 53.51144930919295))
</areaDataSet>
```

Figure 12: Example REST-POST-Request to retrieve navigational warnings for a specific area.

```
<?xml version="1.0" encoding="UTF-8"?>
<Streamable_ExchangeSet 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:xlink="http://www.w3.org/1999/xlink">
  <description>Navigational Warning Dataset provided by NW-Service XY</description>
  <issueDate>2019-05-04</issueDate>
  <issueTime>18:13:52.0</issueTime>
  <digitalSignatureValue>
   <S100:DigitalSignature>
302C021433796C6647CC1C55A67DC72FA7C6E157A6594B2B02145D3768B44F3A6ABA11A77178B738AD3
B6A0DE344
   </S100:DigitalSignature>
```

```
 </digitalSignatureValue>
 <digitalSignatureReference>dsa</digitalSignatureReference>
 <composedOf>
 <S124:DataSet
  xmlns:S124="http://www.iho.int/S124/gml/cs0/0.1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  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>
 </composedOf>
</Streamable_ExchangeSet>
```

Figure 13: S-100 gml answer to the request shown in Figure 12.

4 Architecture Proposal

The Maritime Messaging Service (MMS) is an information broker for exchanging messages via different communication channels in a maritime environment. 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 consumers and service providers. It acts as a middleware between the 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 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 consumer can obtain the MRN of a Service via the Maritime Service Registry (MSR) of the MCP.

The MCP offers a suitable basic architecture to deploy the S-124 WebService, constructed in section 3.3. However, some changes need to be made to the service itself to comply with the requirements of an MMS supporting service.

4.1 Communication via the MMS

As a first step, the navigational warning service needs an interface to understand the MMS-HTTP requests, that are generated by the MMS broker. 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. Ex) Hello World!		

Figure 14: Layout of an MMS-Message. [12]

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. We propose a simple json-like structure with the attributes: "operation", "type" and "content" that refer to the corresponding attributes of the S-100 service model. A basic message exchange with the wrapped operations is shown in Figure 15.

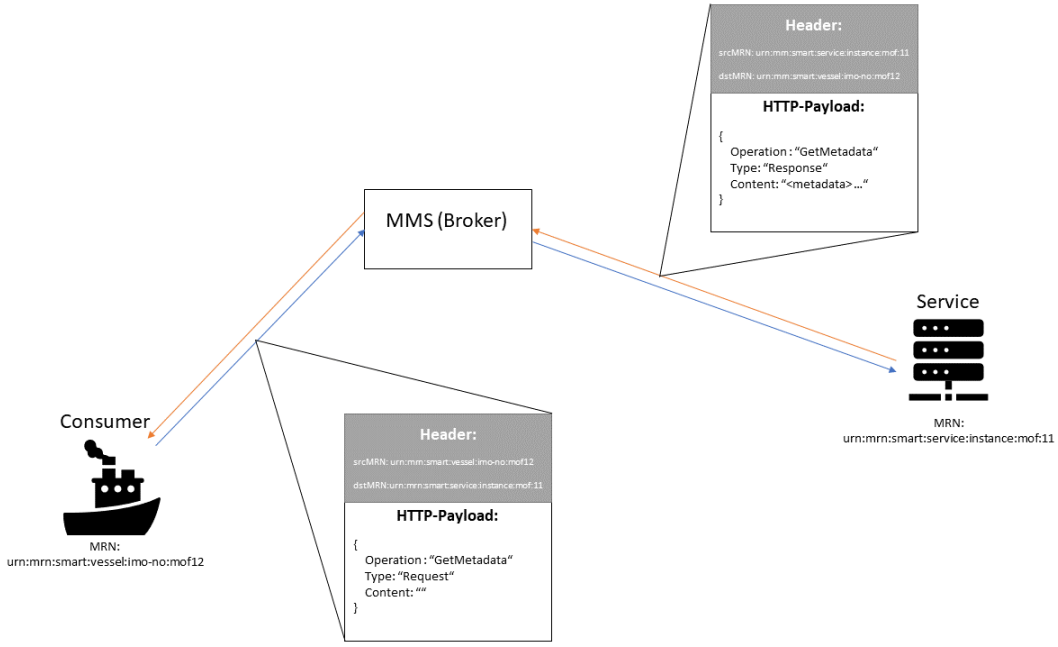

Figure 15: Simple exchange of messages using the MMS with a json-wrapper for the operations and types.

This usage of the MMS results in some changes that must be made to the instance of the S-100 model proposed in section 3.3: As the consumers can now be identified by their MRN, which is known to the service, the session operations are not mandatory anymore. However, these commands can be kept for keeping track of consumers interests to receive navigational warnings (ending the session may indicate that the consumer no longer wants to receive navigational warnings). Then, the GetMetadata and Get_NW_Messages operations can remain as they are. If receiving requests with one of these operations, the server reads the srcMRN header of the message and creates a "Response"-type MMS-Message, with the former srcMRN as destination and the S-100 datasets in the "Content" field.

Since the MMS supports geocasting, the Subscribe_NW_Messages can be replaced by a Broadcast_NW_Message operation. Whenever a new S-124 dataset is available to the service, it generates a geocast MMS-Message, with special HTTP-Headers that specify the geographical area of the warning and sends it to the MMS-Broker. The MMS-Broker knows the positions of the registered clients and casts the message to

each of them. More on geocasting with the MMS can be found in the high-level description document of the Maritime Messaging Service[1]. [12]

4.2 Service Registry and Security with the MMS

Todo

Use MSR for service selection

Solves security issues with MIR, because communication is secured by https and end-to-end encryption, also addresses low-bitrate problem and communication channel changes.

Web portal for organizations (like NAVTEX / SafetyNET solution) to create and distribute navigational warnings to specified areas. -> We can use the OAuth-mechanism from the MCP here to authenticate the organizations.

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.

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

[10] International Hydrographic Organization, 'IHO Geospatial Standard For Navigational Warnings - Special Publication No. S-124 (Working Draft)'. 31-Oct-2018.
[11] L. Jensen, 'Challenges in Maritime Cyber-Resilience', *Technol. Innov. Manag. Rev.*, vol. 5, pp. 35–39, Apr. 2015.
[12] Maritime Connectivity Platform, 'MMS: Concepts, Design and Usages'. .